



# System Center Data Protection Manager 2007 Operations Guide

---

Microsoft Corporation

Published: Sep 2007

## **Abstract**

This guide provides recommendations for monitoring and managing DPM servers, tape libraries, protected file servers and workstations, and protected servers running SQL Server, Exchange Server, and Windows SharePoint Services. The guide also provides instructions for disaster recovery.

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This White Paper is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from

Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

# Contents

---

Managing DPM Servers .....	9
Performing General DPM Server Maintenance .....	9
Using Windows Maintenance Tools on the DPM Server.....	10
Applying Operating System Updates to the DPM Server .....	11
Running Antivirus Software on the DPM Server.....	12
Performing DPM Server Management Tasks .....	13
Managing the DPM Database Volume .....	14
Finding DPM Servers in Active Directory Domain Services .....	14
How to Migrate a DPM Server to New Hardware .....	15
Restarting the DPM Server.....	16
Moving the DPM Server to a New Domain.....	16
Renaming the DPM Server.....	17
Changing the SQL Server Instance Used by DPM.....	17
Coordinating Protection Across Time Zones .....	17
How to Change the Time Zone of the DPM Server .....	19
Managing the Storage Pool.....	19
Adding Disks to the Storage Pool.....	20
How to Replace a Disk in the Storage Pool.....	21
Removing a Disk from the Storage Pool .....	22
Monitoring DPM Server.....	22
Establishing a Monitoring Schedule.....	23
Locating Information .....	23
Methods for Monitoring DPM.....	25
Monitoring with DPM Administrator Console.....	26
Monitoring with Reports and Alert Notifications .....	31
Monitoring with DPM Management Packs .....	32
Managing Protected File Servers and Workstations .....	33
Performing General Maintenance on File Servers and Workstations.....	33
Using Windows Maintenance Tools on File Servers and Workstations .....	34
Applying Operating System Updates on File Servers and Workstations .....	35
Running Antivirus Software on File Servers and Workstations .....	36
Performing File Server and Workstation Management Tasks .....	36
Changing the Path of a Data Source .....	36
Moving File Servers and Workstations Between Domains.....	37
How to Rename a File Server or Workstation .....	38
How to Change the Time Zone of a File Server or Workstation .....	39
Managing Clustered File Servers.....	39
Changing File Server Cluster Members .....	40
Changing Resource Groups on Clustered File Servers .....	40
Managing Protected Servers Running Exchange .....	41

Performing General Maintenance on Servers Running Exchange .....	41
Using Windows Maintenance Tools on Exchange Servers .....	42
Performing Exchange Maintenance Tasks .....	42
Applying Operating System Updates on Exchange Servers .....	43
Running Antivirus Software on Exchange Servers .....	43
Performing Exchange Server Management Tasks .....	43
Upgrading Exchange Server 2003 to Exchange Server 2007 .....	43
Moving Exchange Servers Between Domains .....	44
How to Rename an Exchange Server .....	45
Adding Storage Groups and Databases .....	45
Dismounting Databases .....	46
Changing the Path of a Database or Log File .....	46
Renaming Storage Groups .....	47
Moving Databases Between Storage Groups .....	47
Managing Clustered Exchange Servers .....	48
Changing Exchange Server Cluster Members .....	48
Changing Resource Groups on Clustered Exchange Servers .....	49
Recovering Exchange Data .....	49
How to Recover a Storage Group to its Original Location .....	50
How to Recover a Database to Its Original Location .....	51
How to Recover a Database to an Alternate Database .....	52
How to Copy Exchange Data to a Network Folder .....	53
How to Copy Exchange Data to Tape .....	54
Recovering Mailboxes .....	55
How to Recover an Exchange 2003 Mailbox .....	56
How to Recover an Exchange 2007 Mailbox .....	57
Recovering Data to Clustered Servers .....	60
Managing Protected Servers Running SQL Server .....	61
Performing General Maintenance on Servers Running SQL .....	62
Using Windows Maintenance Tools on SQL Servers .....	62
Performing SQL Maintenance Tasks .....	63
Applying Operating System Updates on SQL Servers .....	63
Running Antivirus Software on SQL Servers .....	63
Performing SQL Server Management Tasks .....	63
Upgrading SQL Server 2000 to SQL Server 2005 .....	64
Moving SQL Servers Between Domains .....	64
How to Rename a Computer Running SQL Server .....	65
Changing the Recovery Model of a Database .....	66
Replacing a Disk on a SQL Server .....	67
Adding Databases to a SQL Server .....	67
Changing the Path of a SQL Server Database .....	67
Renaming a SQL Server Database .....	67
Managing Clustered SQL Servers .....	67
Changing SQL Server Cluster Members .....	67

Changing Resource Groups on Clustered SQL Servers .....	68
Recovering SQL Server Data.....	68
How to Recover a SQL Database to Its Original Location .....	69
How to Recover and Rename a SQL Database.....	70
How to Recover a Database to a Different Instance of SQL Server .....	71
How to Copy a SQL Database to a Network Folder.....	72
How to Copy a SQL Database to Tape .....	73
How to Recover a SQL Database and Allow Additional Log Backups.....	74
Managing Protected Servers Running Windows SharePoint Services .....	75
Performing General Maintenance on Servers Running Windows SharePoint Services.....	75
Using Windows Maintenance Tools on Windows SharePoint Services Servers .....	76
Performing Windows SharePoint Services Maintenance Tasks .....	76
Applying Operating System Updates on Windows SharePoint Services Servers.....	76
Running Antivirus Software on Windows SharePoint Services Servers .....	77
Performing Windows SharePoint Services Management Tasks .....	77
Upgrading Windows SharePoint Services.....	77
Moving Windows SharePoint Services Servers Between Domains.....	78
How to Rename a Windows SharePoint Services Server .....	78
Changing the Front-End Web Server .....	79
Adding Databases to a Windows SharePoint Services Farm .....	80
Adding or Removing Servers in a Windows SharePoint Services Farm.....	81
Recovering Windows SharePoint Services Data.....	81
How to Recover a Windows SharePoint Services Farm .....	82
How to Recover a Windows SharePoint Services Site.....	83
How to Recover a Windows SharePoint Services Item.....	84
Managing Protected Virtual Servers.....	85
Performing General Maintenance on Servers Running Virtual Server .....	85
Using Windows Maintenance Tools on Virtual Server.....	86
Applying Operating System Updates on Virtual Server.....	86
Running Antivirus Software on Virtual Server .....	87
Performing Virtual Server Management Tasks.....	87
Moving Virtual Servers Between Domains .....	87
How to Rename Virtual Servers .....	88
Renaming Virtual Machines.....	88
Moving a Virtual Machine or Virtual Hard Disk.....	89
Protecting Application Data on Virtual Machines.....	89
Recovering Virtual Server Data.....	90
How to Recover the Virtual Server Host.....	90
How to Recover a Virtual Machine .....	91
How to Recover Virtual Machines as Files .....	92
Managing Performance .....	93
How DPM Operations Affect Performance .....	93
Replica Creation .....	94

Change Tracking.....	95
Synchronization .....	96
Consistency Check .....	96
Express Full Backup .....	97
Backup to Tape.....	97
DPM Processes .....	97
DPM and Memory .....	98
Performance Counters .....	98
Improving Performance.....	100
Modifying Workloads .....	101
Using Network Bandwidth Usage Throttling.....	102
Using On-the-Wire Compression .....	103
Staggering Synchronization Start Times .....	103
Scheduling Consistency Checks .....	104
Creating Replicas Manually.....	105
Increasing Capacity .....	105
Managing DPM Performance on a WAN .....	106
How Protection Group Changes Affect Jobs .....	106
Managing Tape Libraries.....	108
Updating Tape Library Information.....	108
Remapping Tape Drives .....	109
Disabling Tape Libraries and Tape Drives.....	110
Removing Tape Libraries .....	110
Managing the Tape Catalog.....	111
Cleaning Tape Drives.....	111
Managing Tapes.....	112
How to Add and Remove Tapes.....	112
How to Identify Tapes .....	113
How to Import Tapes .....	115
How to View Tape Contents .....	115
Rotating Tapes Offsite .....	116
How to Copy Tapes .....	116
How to Inventory Tapes.....	117
Recovering Data from Tapes .....	118
Disaster Recovery .....	118
Preparing for Disaster Recovery .....	119
Best Practices for Disaster Recovery .....	120
Backup of Protected Computer System State .....	121
Backup of DPM Servers .....	123
Backing Up DPM by Using a Secondary DPM Server .....	123
Backing Up DPM Databases to Tape.....	126
Backing Up DPM by Using Third-Party Software.....	127
Backup Using Non-Microsoft Software That Supports DPM .....	127
Backup Using Non-Microsoft Software That Supports VSS .....	128

Backup Using Non-Microsoft Software That Does Not Support VSS .....	129
Backup for Bare Metal Recovery .....	130
Installing DPM System Recovery Tool .....	131
Configuring Backups for Bare Metal Recovery .....	132
Recovery .....	132
Switching Protection If the Primary DPM Server Fails .....	133
Recovering Protected Computers.....	135
Recovering DPM Servers .....	137
How to Recover DPM Databases.....	137
How to Recover DPM Replicas .....	137
How to Reestablish Protection After Recovering the Primary DPM Server .....	138
How to Perform a Bare Metal Recovery .....	139
Using DpmSync .....	139
Using Pre-Backup and Post-Backup Scripts.....	141
Appendix A: Quick Reference to DPM Tasks.....	142
Appendix B: DPM 2007 Schema Extension .....	143
Appendix C: Custom Report Views .....	146





# Managing 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 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 DPM Server Management Tasks](#)

[Managing the Storage Pool](#)

[Monitoring DPM Server](#)

## See Also

[Disaster Recovery](#)

[Managing Performance](#)

[Managing Protected File Servers and Workstations](#)

[Managing Protected Servers Running Exchange](#)

[Managing Protected Servers Running SQL Server](#)

[Managing Protected Servers Running Windows SharePoint Services](#)

[Managing Protected Virtual Servers](#)

[Managing Tape Libraries](#)

## 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](#)

[Applying Operating System Updates to the DPM Server](#)

[Running Antivirus Software on the DPM Server](#)

## See Also

[Managing the Storage Pool](#)

[Monitoring DPM Server](#)

[Performing DPM Server Management Tasks](#)

## 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 2003. 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
<b>Disk Cleanup:</b> 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.
<b>Disk Defragmenter:</b> 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 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."

Windows Tool	Considerations
	For more information about this issue, see the Microsoft Knowledge Base article <a href="http://go.microsoft.com/fwlink/?LinkId=65210">Shadow copies may be lost when you defragment a volume</a> (http://go.microsoft.com/fwlink/?LinkId=65210).
<b>Chkdsk.exe:</b> Use to check the file system and file system metadata for errors and to display a status report of its findings.	Do not run chkdsk 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.

## See Also

[Applying Operating System Updates to the DPM Server](#)

[Running Antivirus Software on the DPM Server](#)

[Using Windows Maintenance Tools on File Servers and Workstations](#)

[Using Windows Maintenance Tools on SQL Servers](#)

[Using Windows Maintenance Tools on Exchange Servers](#)

[Using Windows Maintenance Tools on Windows SharePoint Services Servers](#)

[Using Windows Maintenance Tools on Virtual Server](#)

## 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," "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 prerequisite software. The prerequisite software is as follows:

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

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 that Microsoft Update is installed on.

You can subscribe to Microsoft Update at any time on the [Microsoft Update Web site](http://go.microsoft.com/fwlink/?LinkId=41291) (<http://go.microsoft.com/fwlink/?LinkId=41291>).

## 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](#)

## See Also

[Managing the Storage Pool](#)

[Monitoring DPM Server](#)

[Performing General DPM Server Maintenance](#)

## 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 [Adsiedit Overview](#) on the Windows Server 2003 TechCenter (<http://go.microsoft.com/fwlink/?LinkId=50377>).

### ▶ 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.

▶ **To migrate a DPM server to new hardware,**

1. Install DPM on a new server. For more information, see [Installing DPM](http://go.microsoft.com/fwlink/?LinkId=91851) (<http://go.microsoft.com/fwlink/?LinkId=91851>).
2. Identify a protected computer to migrate and carry out the following steps:
  - a. On the existing DPM server, stop protection for all data, choosing to retain replicas for this protected computer, and uninstall the protection agent.
  - b. Restart the target computer.
  - c. Install the protection agent from the new DPM server to the selected computer.
  - d. Restart the protected computer.
  - e. Repeat for all protected computers.
3. Create protection groups on the new DPM server for the protected computers. For more information, see [Configuring DPM](http://go.microsoft.com/fwlink/?LinkId=91852) (<http://go.microsoft.com/fwlink/?LinkId=91852>).
4. 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

We recommend that you avoid changing the domain of the DPM server because doing so causes all protection and recovery operations to fail.

If it is essential that you change the domain membership of a DPM server, you must stop protection of the protection group members assigned to that DPM server and then restart protection of those data sources, either by adding them to protection groups on another DPM server or adding them to new protection groups on the same DPM server after you change its domain.



## See Also

[Performing DPM Server Management Tasks](#)

[Renaming the DPM Server](#)

## Renaming the DPM Server

We recommend that you avoid changing the name of the DPM server because doing so causes all protection and recovery operations to fail.

If it essential that you change the name of a DPM server, you must stop protection of the protection group members assigned to that DPM server and then restart protection of those data sources, either by adding them to protection groups on another DPM server or adding them to new protection groups on the same DPM server after you change its name.

## See Also

[Moving the DPM Server to a New Domain](#)

[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 choose a new instance of SQL Server. For more information, see [Installing DPM](#) (<http://go.microsoft.com/fwlink/?LinkId=91851>).
4. Restore DPMDB to the new instance of SQL Server, run DpmSync, and run a consistency check for the data sources protected by the DPM server.

The process depends on the availability of a backup of the DPM database. For more information about backing up and restoring the DPM database, see [Disaster Recovery](#).

## See Also

[Performing DPM Server Management Tasks](#)

[Installing DPM](#)

## 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 action 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](#)

## 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)

- Fibre 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, in the TechNet Library, see [Configuring DPM](#)

(<http://go.microsoft.com/fwlink/?LinkId=91852>).

## 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](#)

[Methods for Monitoring DPM](#)

## See Also

[Managing Performance](#)

[Managing the Storage Pool](#)

[Performing DPM Server Management Tasks](#)

[Performing General DPM Server Maintenance](#)

## 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](#) in DPM Help (<http://go.microsoft.com/fwlink/?LinkId=102159>). 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	<ul style="list-style-type: none"><li>• Critical and warning alerts</li><li>• E-mail notifications (if they are configured)</li><li>• Status report</li></ul>	Replica issues, synchronization and recovery point creation issues, agent issues, jobs waiting for tape, backup failures
Monthly	Reports: <ul style="list-style-type: none"><li>• Status</li><li>• Tape Management</li><li>• Disk Utilization</li></ul>	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:
<p>Does anything need my attention?</p> <p>Are there any changes on the protected computers that affect data protection?</p>	<ul style="list-style-type: none"> <li>• E-mail notifications of alerts, if you subscribe to them</li> <li>• <b>Monitoring</b> task area, <b>Alerts</b> tab</li> </ul>
<p>Did all the backups that were supposed to happen yesterday happen correctly?</p> <p>Is there an issue that keeps coming up?</p> <p>Are recovery goals being met?</p>	<ul style="list-style-type: none"> <li>• Status report</li> <li>• Protection report</li> </ul>
<p>Do I need to add disk space to the storage pool?</p>	<ul style="list-style-type: none"> <li>• <b>Management</b> task area, <b>Disks</b> tab</li> <li>• Disk Utilization report</li> </ul>
<p>When will a job run?</p> <p>How long did the last consistency check take?</p> <p>How much data was transferred by the most recent synchronization job?</p>	<p><b>Monitoring</b> task area, <b>Jobs</b> tab</p>
<p>How many recovery points are available for a data source?</p> <p>Are all replicas consistent?</p>	<ul style="list-style-type: none"> <li>• <b>Protection</b> task area, <b>Details</b> pane</li> <li>• <b>Recovery</b> task area</li> </ul>
<p>What tapes are available in the library?</p> <p>What data is on each tape?</p>	<p><b>Management</b> task area, <b>Libraries</b> tab</p>
<p>Did a recovery job complete successfully?</p>	<ul style="list-style-type: none"> <li>• <b>Monitoring</b> task area, <b>Alerts</b> tab</li> <li>• <b>Monitoring</b> task area, <b>Jobs</b> tab</li> <li>• E-mail notification (if you subscribe to e-mail notification when you initiate a recovery)</li> </ul>
<p>Is the DPM server able to contact each protected computer?</p>	<p><b>Management</b> task area, <b>Agents</b> tab</p>
<p>What is the status of the DPM service?</p>	<ul style="list-style-type: none"> <li>• Microsoft Management Console (MMC) Services snap-in</li> <li>• Event log, in case of service failures</li> </ul>
<p>What problems have occurred over the past month?</p>	<ul style="list-style-type: none"> <li>• Status report</li> <li>• <b>Monitoring</b> task area, <b>Alerts</b> tab,</li> </ul>



What do you want to know?	Look here:
	with <b>Show inactive alerts</b> selected
What is the status of each of my DPM servers and the computers that they protect?	MOM Operator console, <b>State</b> view
Why is recovery point creation failing for a protection group member?	Status report

## See Also

[Establishing a Monitoring Schedule](#)

[Managing Performance](#)

[Methods for Monitoring DPM](#)

## Methods for Monitoring DPM

To monitor protection activities, 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 e-mail. For instructions, see [How to Create or Modify Report Subscriptions](#) in DPM Help ( <http://go.microsoft.com/fwlink/?LinkId=102161>).
- Monitor operations for multiple DPM servers by using the System Center Data Protection Manager (DPM) Management Pack for Microsoft Operations Manager 2005 or System Center Operations Manager 2007.
- Monitor the instance of SQL Server that DPM installs by using the System Center SQL Server Management Pack for Microsoft Operations Manager 2005.

## In This Section

[Monitoring with DPM Administrator Console](#)

[Monitoring with Reports and Alert Notifications](#)

[Monitoring with DPM Management Packs](#)

## See Also

[Establishing a Monitoring Schedule](#)

[Locating Information](#)

[Managing Performance](#)

## 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](#)
- 



### 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 DPM Management Pack.

For more information, see the “Resolving Alerts” section in Data Protection Manager 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"](http://go.microsoft.com/fwlink/?LinkId=102085) in DPM Help (<http://go.microsoft.com/fwlink/?LinkId=102085>).

 **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"](http://go.microsoft.com/fwlink/?LinkId=102086) in DPM Help (<http://go.microsoft.com/fwlink/?LinkId=102086>).

**DPM Reports**

Report Name	Summary of Contents
Status	<p>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.</p> <p>Use this report to answer questions such as the following:</p> <ul style="list-style-type: none"> <li>• What happened yesterday? Last week? Last month?</li> <li>• What succeeded and what failed?</li> <li>• What is the trend of errors? Which errors occur most frequently?</li> <li>• Are we achieving the recovery point objective (RPO) established in our service level agreement (SLA)?</li> </ul> <p> <b>Note</b></p> <p>The Status report includes the error codes for any alerts recorded during the report period. To view the error message associated with an error code, see the <a href="http://go.microsoft.com/fwlink/?LinkId=91861">Error Code Catalog</a> (<a href="http://go.microsoft.com/fwlink/?LinkId=91861">http://go.microsoft.com/fwlink/?LinkId=91861</a>).</p>

Report Name	Summary of Contents
Tape Management	<p>The Tape Management report provides details for tape rotation and decommissioning, and it verifies that the free media threshold is not exceeded.</p> <p>Use this report to manage tape circulation between the library and your offsite location.</p>
Tape Utilization	<p>The Tape Utilization report provides trending of resource (disk/tape) usage over time to assist capacity planning.</p> <p>Use this report to make decisions about tape allocations and purchases.</p>
Protection	<p>The Protection report provides the commonly used metrics for backup success rolled up over long periods of time to track how backups are doing.</p> <p>Use this report to identify which computers or protection groups have been backed up successfully.</p>
Recovery	<p>The Recovery report provides the commonly used metrics for recovery success rolled up over long periods of time to track how recoveries are doing.</p> <p>Use this report to identify how well you performed against your service level agreements for recovery time objectives and recovery success guarantees.</p>
Disk Utilization	<p>Summarizes disk capacity, disk allocation, and disk usage in the DPM storage pool.</p> <p>Use this report to do the following:</p> <ul style="list-style-type: none"> <li>• Identify trends in disk usage</li> <li>• Make decisions about modifying space allocations for protection groups and adding disks to the storage pool</li> <li>• Identifying how much disk resource each computer is using on DPM</li> </ul>

**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

E-Mail Type	Subject Line
Notification of an alert	<ul style="list-style-type: none"><li>• DPM: Information (Protected computer name)</li><li>• DPM: Warning (Protected computer name)</li><li>• DPM: Critical (Protected computer name)</li><li>• DPM: Recovery (Protected computer name)</li></ul>
Notification of a resolved alert	<ul style="list-style-type: none"><li>• DPM: Resolved (Protected computer name)</li></ul>
Report	<ul style="list-style-type: none"><li>• Status Report from specified server</li><li>• Media Management Report from specified server</li><li>• Protection Report from specified server</li><li>• Recovery Report from specified server</li><li>• Tape Utilization Report from specified server</li><li>• Disk Utilization Report from specified server</li></ul>

**See Also**

[Managing Performance](#)

[Monitoring DPM Server](#)

[Monitoring with DPM Administrator Console](#)

[Monitoring with DPM Management Packs](#)

**Monitoring with DPM Management Packs**

The System Center Data Protection Manager 2007 Management Packs for Operations Manager enable an administrator to use a MOM Management 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 DPM Management Pack 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 DPM Management Packs are not included with the DPM product. You can download management packs at the [DPM Management Pack download site](http://go.microsoft.com/fwlink/?linkid=50208) (<http://go.microsoft.com/fwlink/?linkid=50208>).

**See Also**

[Managing Performance](#)

[Monitoring DPM Server](#)

[Monitoring with DPM Administrator Console](#)

[Monitoring with Reports and Alert Notifications](#)



# Managing Protected 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 DPM.

## In This Section

[Performing General Maintenance on File Servers and Workstations](#)

[Performing File Server and Workstation Management Tasks](#)

[Managing Clustered File Servers](#)

## See Also

[Disaster Recovery](#)

[Managing DPM Servers](#)

[Managing Performance](#)

[Managing Protected Servers Running Exchange](#)

[Managing Protected Servers Running SQL Server](#)

[Managing Protected Servers Running Windows SharePoint Services](#)

[Managing Protected Virtual Servers](#)

[Managing Tape Libraries](#)

## Performing General Maintenance on File Servers and Workstations

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.

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.

► **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

[Using Windows Maintenance Tools on File Servers and Workstations](#)

[Applying Operating System Updates on File Servers and Workstations](#)

[Running Antivirus Software on File Servers and Workstations](#)

## See Also

[Managing Clustered File Servers](#)

[Performing File Server and Workstation Management Tasks](#)

## Using Windows Maintenance Tools on File Servers and Workstations

In general, you can continue maintenance on file servers and workstations protected by 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
<b>Disk Cleanup:</b> 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.
<b>Disk Defragmenter:</b> 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 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.
<b>Chkdsk.exe:</b> Use to check the file system and	Before you run <b>chkdsk /f</b> on a protected

Windows Tool	Considerations
file system metadata for errors and to display a status report of its findings.	<p>volume, verify that a consistency check of that volume is not being performed.</p> <p>Running <b>chkdsk /f</b> on a protected volume while a consistency check is being performed on that volume can cause 100% CPU utilization.</p> <p>Run synchronization with consistency check after running Chkdsk.exe on the protected computer.</p>

### See Also

[Applying Operating System Updates on File Servers and Workstations](#)

[Managing Protected File Servers and Workstations](#)

[Running Antivirus Software on File Servers and Workstations](#)

[Using Windows Maintenance Tools on the DPM Server](#)

[Using Windows Maintenance Tools on Exchange Servers](#)

[Using Windows Maintenance Tools on SQL Servers](#)

[Using Windows Maintenance Tools on Windows SharePoint Services Servers](#)

[Using Windows Maintenance Tools on Virtual Server](#)

## Applying Operating System Updates on File Servers and Workstations

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 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

[Managing Protected File Servers and Workstations](#)

[Running Antivirus Software on File Servers and Workstations](#)

[Using Windows Maintenance Tools on File Servers and Workstations](#)

## Running Antivirus Software on File Servers and Workstations

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 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](http://go.microsoft.com/fwlink/?LinkId=95113) (<http://go.microsoft.com/fwlink/?LinkId=95113>).

### See Also

[Applying Operating System Updates on File Servers and Workstations](#)

[Managing Protected File Servers and Workstations](#)

[Using Windows Maintenance Tools on File Servers and Workstations](#)

## 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 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](#)

### See Also

[Managing Clustered File Servers](#)

[Managing Performance](#)

[Performing General Maintenance on File Servers and Workstations](#)

## 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 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](#)

[Managing Protected 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](http://go.microsoft.com/fwlink/?LinkId=102087) (<http://go.microsoft.com/fwlink/?LinkId=102087>).

## 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](#)

[Managing Protected File Servers and Workstations](#)

## How to Rename a File Server or Workstation

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](http://go.microsoft.com/fwlink/?LinkId=102087) (http://go.microsoft.com/fwlink/?LinkId=102087).

## See Also

[Changing the Path of a Data Source](#)

[How to Change the Time Zone of a File Server or Workstation](#)

[Managing Protected File Servers and Workstations](#)

[Moving File Servers and Workstations Between Domains](#)

## How to Change the Time Zone of a File Server or Workstation

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](#)

[Managing Protected File Servers and Workstations](#)

[Moving File Servers and Workstations Between Domains](#)

## Managing Clustered File Servers

On planned failover of a cluster, 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](#)

[Performing General Maintenance on File Servers and Workstations](#)

## Changing File Server Cluster Members

When you make changes to a server cluster that is protected by 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](#)

[Performing General Maintenance on File Servers and Workstations](#)

## 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](#)

[Performing General Maintenance on File Servers and Workstations](#)

## **Managing Protected Servers Running Exchange**

---

All information in this section pertains to both Microsoft Exchange 2003 and Exchange 2007, unless otherwise specified.

### **In This Section**

[Performing General Maintenance on Servers Running Exchange](#)

[Performing Exchange Server Management Tasks](#)

[Managing Clustered Exchange Servers](#)

[Recovering Exchange Data](#)

## **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.

### ▶ 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

[Using Windows Maintenance Tools on Exchange Servers](#)

[Performing Exchange Maintenance Tasks](#)

[Applying Operating System Updates on Exchange Servers](#)

[Running Antivirus Software on Exchange Servers](#)

## Using Windows Maintenance Tools on Exchange Servers

Running Disk Cleanup, Disk Defragmenter, or Chkdsk.exe should have no adverse affect on performance or data protection.

### See Also

[Using Windows Maintenance Tools on the DPM Server](#)

[Using Windows Maintenance Tools on File Servers and Workstations](#)

[Using Windows Maintenance Tools on SQL Servers](#)

[Using Windows Maintenance Tools on Windows SharePoint Services Servers](#)

[Using Windows Maintenance Tools on Virtual Server](#)

## Performing Exchange Maintenance Tasks

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 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.

## Applying Operating System Updates on Exchange Servers

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 rollout 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 Exchange servers that are protected by Data Protection Manager (DPM). 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.

## Running Antivirus Software on Exchange Servers

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 Data Protection Manager (DPM) cannot detect. For instructions on configuring your antivirus software to delete infected files, see the documentation for your antivirus software.

For instructions on configuring firewalls on computers when installing protection agents, see [Installing Protection Agents](http://go.microsoft.com/fwlink/?LinkId=95113) (<http://go.microsoft.com/fwlink/?LinkId=95113>) in *Deploying DPM 2007*.

## Performing Exchange Server Management Tasks

This section provides instructions and guidelines for managing a protected Exchange server and making changes after the initial DPM configuration.

### In This Section

[Upgrading Exchange Server 2003 to Exchange Server 2007](#)

[Moving Exchange Servers Between Domains](#)

[How to Rename an Exchange Server](#)

[Adding Storage Groups and Databases](#)

[Dismounting Databases](#)

[Changing the Path of a Database or Log File](#)

[Renaming Storage Groups](#)

[Moving Databases Between Storage Groups](#)

## 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](http://go.microsoft.com/fwlink/?LinkId=72602) (<http://go.microsoft.com/fwlink/?LinkId=72602>).

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.

### ► 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](http://go.microsoft.com/fwlink/?LinkId=102087) (http://go.microsoft.com/fwlink/?LinkId=102087).

## How to Rename an Exchange Server

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](http://go.microsoft.com/fwlink/?LinkId=102087) (http://go.microsoft.com/fwlink/?LinkId=102087).

## 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.

## 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 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

We recommend that you do not change the name of a protected storage group. To change the name of a storage group, you must stop protection of the storage group, change the name, and then reprotect the storage group. You cannot do the following:

- Change the name of a protected storage group and continue protection without disruption.
- Change the name of a protected storage group, and associate the existing replica and recovery points with the storage group when it is reprotected.

### ► To change the name of a protected storage group

1. Remove the storage group from the protection group.  
If you retain the replica and recovery points, the data will remain accessible for administrative recovery until you delete the replica.
2. Change the name of the storage group.
3. Add the storage group to a protection group on the Data Protection Manager (DPM) server.

For instructions on tasks involving protection groups, see [DPM Help](http://go.microsoft.com/fwlink/?LinkId=102087) (<http://go.microsoft.com/fwlink/?LinkId=102087>).

## 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	Data Protection Manager (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

From	To	Result
		not on a protected volume, run the Modify Group Wizard. Run a consistency check for the protected storage group after the move.

## Managing Clustered Exchange Servers

On planned failover of a cluster, 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 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](http://go.microsoft.com/fwlink/?LinkId=97929)" (<http://go.microsoft.com/fwlink/?LinkId=97929>).

- **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](http://go.microsoft.com/fwlink/?LinkId=97929)" (<http://go.microsoft.com/fwlink/?LinkId=97929>).

- **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. 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 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](#)

[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](http://go.microsoft.com/fwlink/?LinkId=97929)" (<http://go.microsoft.com/fwlink/?LinkId=97929>).
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, 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 dismantled 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](http://go.microsoft.com/fwlink/?LinkId=97929)" (<http://go.microsoft.com/fwlink/?LinkId=97929>).

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](http://go.microsoft.com/fwlink/?LinkId=97929)" (<http://go.microsoft.com/fwlink/?LinkId=97929>).
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, 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**.

## See Also

[How to Copy Tapes](#)

[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](#)" (<http://go.microsoft.com/fwlink/?LinkId=97933>). To recover a deleted

mailbox, use the Exchange Management Shell or the Exchange Management Console. For instructions, see "[How to Recover a Deleted Mailbox](http://go.microsoft.com/fwlink/?LinkId=97934)" (<http://go.microsoft.com/fwlink/?LinkId=97934>).

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 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](http://go.microsoft.com/fwlink/?LinkId=96542)" (<http://go.microsoft.com/fwlink/?LinkId=96542>).

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.

## 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](http://go.microsoft.com/fwlink/?LinkId=83451) (<http://go.microsoft.com/fwlink/?LinkId=83451>). For more information on Exmerge.exe, see Knowledge Base article 174197, "[Microsoft Exchange Mailbox Merge program \(Exmerge.exe\) information](http://go.microsoft.com/fwlink/?LinkId=83459)" (<http://go.microsoft.com/fwlink/?LinkId=83459>).

### ▶ 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.
10. Complete the Recovery Wizard. DPM recovers the database.
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](http://go.microsoft.com/fwlink/?LinkId=97929)" (<http://go.microsoft.com/fwlink/?LinkId=97929>).

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.

### ▶ **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

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 Protected Servers Running SQL Server

---

This content applies to both Microsoft® SQL Server 2000 and SQL Server 2005, unless otherwise specified.

### In This Section

[Performing General Maintenance on Servers Running SQL](#)

[Performing SQL Server Management Tasks](#)

[Managing Clustered SQL Servers](#)

## Performing General Maintenance on Servers Running SQL

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 SQL Servers that are protected by 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 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.

### **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

[Using Windows Maintenance Tools on SQL Servers](#)

[Performing SQL Maintenance Tasks](#)

[Applying Operating System Updates on SQL Servers](#)

[Running Antivirus Software on SQL Servers](#)

## Using Windows Maintenance Tools on SQL Servers

Running Disk Cleanup, Disk Defragmenter, or Chkdsk.exe should have no adverse effect on performance or data protection.

You should not use other backup applications on a computer running SQL Server that is protected by DPM.

### **See Also**

[Using Windows Maintenance Tools on the DPM Server](#)

[Using Windows Maintenance Tools on File Servers and Workstations](#)

[Using Windows Maintenance Tools on Exchange Servers](#)

[Using Windows Maintenance Tools on Windows SharePoint Services Servers](#)

[Using Windows Maintenance Tools on Virtual Server](#)

## Performing SQL Maintenance Tasks

Coordinate with the SQL Server administrator to ensure that the following tasks are not scheduled at the same time as the express full backup performed by DPM:

- Check database integrity
- History cleanup
- Maintenance cleanup
- Rebuild index
- Reorganize index
- Shrink database
- Update statistics

Best practices for SQL Server include running a weekly database consistency check (DBCC). You should continue this practice for databases protected by DPM to avoid backing up a database with corruption issues.

## Applying Operating System Updates on SQL Servers

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 computers running SQL Server that are protected by DPM. 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.

## Running Antivirus Software on SQL Servers

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. For instructions on configuring your antivirus software to delete infected files, see the documentation for your antivirus software.

## 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](#)

[Moving SQL Servers Between Domains](#)

[How to Rename a Computer Running SQL Server](#)

[Changing the Recovery Model of a Database](#)

[Replacing a Disk on a SQL Server](#)

[Adding Databases to a SQL Server](#)

[Changing the Path of a SQL Server Database](#)

[Renaming a SQL Server Database](#)

## 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](http://go.microsoft.com/fwlink/?LinkId=102087) (<http://go.microsoft.com/fwlink/?LinkId=102087>).

## How to Rename a Computer Running SQL Server

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](http://go.microsoft.com/fwlink/?LinkId=102087) (<http://go.microsoft.com/fwlink/?LinkId=102087>).

## 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, 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 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

New databases on a protected computer running SQL Server are not automatically added to an existing protection group. When a new database is created, you should manually add the database to an existing or new protection group to ensure the data is protected.

## 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 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.

## Managing Clustered SQL Servers

On planned failover of a cluster, 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](#)

[Changing Resource Groups on Clustered SQL Servers](#)

### Changing SQL Server Cluster Members

When you make changes to a server cluster that is protected by 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.

## 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](#)

[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 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 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.

### ▶ 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 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**.

### See Also

[How to Copy Tapes](#)

[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 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 \(Transact-SQL\)](http://go.microsoft.com/fwlink/?LinkId=104665) (<http://go.microsoft.com/fwlink/?LinkId=104665>).

### 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](#)

## Managing Protected Servers Running Windows SharePoint Services

---

This section provides instructions for managing protected servers running Windows SharePoint Services. All information in this section pertains to both Microsoft® Office SharePoint® Server 2007 and Windows SharePoint Services 3.0, unless otherwise specified.

### In This Section

[Performing General Maintenance on Servers Running Windows SharePoint Services](#)

[Performing Windows SharePoint Services Management Tasks](#)

[Recovering Windows SharePoint Services Data](#)

## Performing General Maintenance on Servers Running Windows SharePoint Services

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 Microsoft® Windows® SharePoint Services that are protected by System Center Data Protection Manager 2007 (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

[Using Windows Maintenance Tools on Windows SharePoint Services Servers](#)

[Performing Windows SharePoint Services Maintenance Tasks](#)

[Applying Operating System Updates on Windows SharePoint Services Servers](#)

[Running Antivirus Software on Windows SharePoint Services Servers](#)

## Using Windows Maintenance Tools on Windows SharePoint Services Servers

Running Disk Cleanup, Disk Defragmenter, or Chkdsk.exe should have no adverse effect on performance or data protection.

### See Also

[Using Windows Maintenance Tools on the DPM Server](#)

[Using Windows Maintenance Tools on File Servers and Workstations](#)

[Using Windows Maintenance Tools on Exchange Servers](#)

[Using Windows Maintenance Tools on SQL Servers](#)

[Using Windows Maintenance Tools on Virtual Server](#)

## Performing Windows SharePoint Services 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.

## Applying Operating System Updates on Windows SharePoint Services Servers

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 computers running Windows SharePoint Services that are protected by DPM. 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.

## Running Antivirus Software on Windows SharePoint Services Servers

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. For instructions on configuring your antivirus software to delete infected files, see the documentation for your antivirus software.

## Performing Windows SharePoint Services Management Tasks

This section provides instructions and guidelines for managing a protected server running Windows SharePoint Services and making changes after the initial DPM configuration.

### In This Section

[Upgrading Windows SharePoint Services](#)

[Moving Windows SharePoint Services Servers Between Domains](#)

[How to Rename a Windows SharePoint Services Server](#)

[Changing the Front-End Web Server](#)

[Adding Databases to a Windows SharePoint Services Farm](#)

[Adding or Removing Servers in a Windows SharePoint Services Farm](#)

## Upgrading Windows SharePoint Services

Windows SharePoint Services data, such as the configuration databases, content databases, and other databases and files that are part of the Windows SharePoint Services farm for Windows SharePoint Services 2.0 (WSS 2.0), can be protected by DPM as SQL Server databases.

If you protect WSS 2.0 data as SQL Server databases and then upgrade to WSS 3.0 or Microsoft Office SharePoint Server 2007, you must reconfigure protection of the data.

### ► To upgrade from Windows SharePoint Services 2.0 to Windows SharePoint Services 3.0 or Microsoft Office SharePoint Server 2007

1. Create a recovery point of the WSS 2.0 data that is protected as a SQL Server database.
2. Stop protection of the data, choosing the **Retain replica** option.
3. Upgrade the server running Windows SharePoint Services.

4. Add the upgraded Windows SharePoint Services farm to a protection group by selecting it as a Windows SharePoint Services data source.

Data in the retained replica remains available for recovery, but it is not associated with the upgraded Windows SharePoint Services farm.

## Moving Windows SharePoint Services 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](http://go.microsoft.com/fwlink/?LinkId=102087) (<http://go.microsoft.com/fwlink/?LinkId=102087>).

## How to Rename a Windows SharePoint Services Server

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](http://go.microsoft.com/fwlink/?LinkId=102087) (<http://go.microsoft.com/fwlink/?LinkId=102087>).

## **Changing the Front-End Web Server**

To protect a server farm on servers running Microsoft Windows SharePoint Services 3.0 or Microsoft Office SharePoint Server 2007, you start the Windows SharePoint Services VSS Writer service (WSS Writer service) and install the DPM protection agent on a single front-end Web server. 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 WSS 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.
5. On Server2, at a command prompt, change the directory to *DPM installation location\bin\* and run the following command:

#### **ConfigureSharepoint.exe**

A prompt appears requesting your Windows SharePoint Services farm administrator credentials. The administrator credentials you provide for the Windows SharePoint Services farm must be a local administrator on the server.

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.

## **Adding Databases to a Windows SharePoint Services Farm**

When a database is added to or removed from a Windows SharePoint Services farm, DPM will mark the replica as inconsistent and alert the administrator.



When a database is added, the alert includes a link to modify the protection group. After you complete the Modify Group Wizard, DPM performs a consistency check. Protection of the farm, including the added database, continues.

When a database is removed, you should stop protection of the server farm using the retain replica option, and then add the farm to the protection group again.

## Adding or Removing Servers in a Windows SharePoint Services Farm

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 [Changing the Front-End Web Server](#).

## Recovering Windows SharePoint Services Data

The following points apply to the recovery of Windows SharePoint Services data:

- Item details will not appear on the Recovery Wizard Summary page for Windows SharePoint Services sites and items. When you recover a Windows SharePoint Services farm, DPM recovers the configuration database of the farm but does not list this database in the item details on the Recovery Wizard Summary page.
- The administration content database is the first content database created with the administration central site when you set up your farm. Do not directly recover the administration content database because this could lead to data corruption in the Windows SharePoint Services farm.
- The recovery point times on the Browse tab may differ from the times on the Search tab for Windows SharePoint Services data. The Search tab lists the correct recovery point time for sites, documents, and folders. The Browse tab displays the backup time for the farm.
- Documents in Windows SharePoint Services could be in one of the following states if document versioning is enabled:
  - 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 Windows SharePoint Services data, only documents that are checked in, published, or approved are recovered. Documents that are not checked in will not be recovered as part of a site collection or document recovery. Documents that are in either the user Recycle Bin or the site collection Recycle Bin will not be recovered as part of a site collection or document recovery.

## In This Section

[How to Recover a Windows SharePoint Services Farm](#)

[How to Recover a Windows SharePoint Services Site](#)

[How to Recover a Windows SharePoint Services Item](#)

## How to Recover a Windows SharePoint Services Farm

To recover a Windows SharePoint Services 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 used when the recovery point was created.

### ▶ 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 used to protect the original farm, register the Windows SharePoint Services VSS Writer service (WSS Writer service) by running the following command at a command prompt:

```
stsadm -o registerwsswriter
```

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.

## See Also

[How to Recover a Windows SharePoint Services Site](#)

[How to Recover a Windows SharePoint Services Item](#)

## How to Recover a Windows SharePoint Services Site

To recover a Microsoft Windows SharePoint Services site, you must:

1. Create a farm to be used for the recovery.
2. Create a Web application for the recovery.
3. Use DPM to recover the site to the recovery farm.

The following requirements apply to a site recovery:

- The farm used for recovery should be a single server farm.
- If you protect a MOSS farm, then the recovery farm must also be MOSS.
- The features and templates installed on the recovery farm must match those of the target farm.

- If a service pack or update is installed on the protected farm, the recovery farm must have the same service pack or update installed or item-level restore operations could fail.
- Both the recovery and target farms must be in the same language and have the same language packs installed.
- The target farm must contain a site collection with the same path as the original protected site. If the site collection does not exist, you can create an empty site collection with the correct path on the target farm before you perform the recovery.

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.

### **To recover a site**

1. Create a farm that DPM can use for the recovery. To create a recovery farm, see the instructions at "[Deploy in a simple server farm](http://go.microsoft.com/fwlink/?LinkId=95150)" (<http://go.microsoft.com/fwlink/?LinkId=95150>).
2. Create a Web application and name it DPMRecoveryWebApplication. To create a new Web application, see the instructions at "[Create or extend Web applications \(Windows SharePoint Services\)](http://go.microsoft.com/fwlink/?LinkId=94374)" (<http://go.microsoft.com/fwlink/?LinkId=94374>).
3. 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. Double-click the farm item.  
The databases for the farm display in the **Recoverable item** pane.
6. Select a recovery point for the site you want to recover, and click **Recover** in the **Actions** pane.
7. On the **Select Recovery Type** page, select **Recover to original site**.
8. On the **Specify Recovery Farm** page, enter the information for the recovery farm you created in step 1, and then complete the wizard.  
DPM recovers the site to the original farm.

### **See Also**

[How to Recover a Windows SharePoint Services Farm](#)

[How to Recover a Windows SharePoint Services Item](#)

## **How to Recover a Windows SharePoint Services Item**

You can recover Windows SharePoint Services items, such as lists and documents, from a DPM recovery point to the original site or to an alternate site.

► **To recover an item**

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, double-click the content database, double-click the site, and then double-click the displayed items to navigate to the item that you want to recover.
5. Click **Recover** in the **Actions** pane, and then complete the wizard.

**See Also**

[How to Recover a Windows SharePoint Services Farm](#)

[How to Recover a Windows SharePoint Services Site](#)

## Managing Protected 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 DPM.

### In This Section

[Performing General Maintenance on Servers Running Virtual Server](#)

[Performing Virtual Server Management Tasks](#)

[Recovering Virtual Server Data](#)

## Performing General Maintenance on Servers Running Virtual Server

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 Virtual Server that are protected by System Center Data Protection Manager 2007 (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 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.

### ▶ 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

[Using Windows Maintenance Tools on Virtual Server](#)

[Applying Operating System Updates on Virtual Server](#)

[Running Antivirus Software on Virtual Server](#)

## Using Windows Maintenance Tools on Virtual Server

Running Disk Cleanup, Disk Defragmenter, or Chkdsk.exe should have no adverse effect on performance or data protection.

### See Also

[Using Windows Maintenance Tools on the DPM Server](#)

[Using Windows Maintenance Tools on File Servers and Workstations](#)

[Using Windows Maintenance Tools on Exchange Servers](#)

[Using Windows Maintenance Tools on SQL Servers](#)

[Using Windows Maintenance Tools on Windows SharePoint Services Servers](#)

## Applying Operating System Updates on Virtual Server

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 computers running Virtual Server that are protected by DPM and on virtual machines that are protected by DPM. 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.

## Running Antivirus Software on Virtual 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. For instructions on configuring your antivirus software to delete infected files, see the documentation for your antivirus software.

## 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](#)

[How to Rename Virtual Servers](#)

[Renaming Virtual Machines](#)

[Moving a Virtual Machine or Virtual Hard Disk](#)

[Protecting Application Data on Virtual Machines](#)

### 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.

For information about performing tasks involving protection agents and protection groups, see [DPM Help](http://go.microsoft.com/fwlink/?LinkId=102087) (<http://go.microsoft.com/fwlink/?LinkId=102087>).

## How to Rename Virtual Servers

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.

For information about tasks that involve protection agents and protection groups, see [DPM Help](http://go.microsoft.com/fwlink/?LinkId=102087) (<http://go.microsoft.com/fwlink/?LinkId=102087>).

## 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, 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](http://go.microsoft.com/fwlink/?LinkId=95298)" (<http://go.microsoft.com/fwlink/?LinkId=95298>).
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](http://go.microsoft.com/fwlink/?LinkId=95299)" (<http://go.microsoft.com/fwlink/?LinkId=95299>).
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.

For more information about protecting application data, see the topics on protecting specific data types, such as Exchange Server data or SQL Server data, in [DPM Help](http://go.microsoft.com/fwlink/?LinkId=102087) (<http://go.microsoft.com/fwlink/?LinkId=102087>).

# Recovering Virtual Server Data

## In This Section

[How to Recover the Virtual Server Host](#)

[How to Recover a Virtual Machine](#)

[How to Recover Virtual Machines as Files](#)

## 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 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](#)

# Managing Performance

---

The topics in this section define performance expectations and explain how to optimize 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

[How DPM Operations Affect Performance](#)

[DPM and Memory](#)

[Performance Counters](#)

[Improving Performance](#)

[Managing DPM Performance on a WAN](#)

[How Protection Group Changes Affect Jobs](#)

## See Also

[Disaster Recovery](#)

[Managing DPM Servers](#)

[Managing Protected File Servers and Workstations](#)

[Managing Protected Servers Running Exchange](#)

[Managing Protected Servers Running SQL Server](#)

[Managing Protected Servers Running Windows SharePoint Services](#)

[Managing Protected Virtual Servers](#)

[Managing Tape Libraries](#)

## How DPM Operations Affect Performance

As an administrator, one of your concerns will be the impact of 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 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. For more information, see [Creating Replicas Manually](#).

### See Also

[How DPM Operations Affect Performance](#)

[Managing Performance](#)

### Change Tracking

After the replica is created, the 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 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 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 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 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 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 (Microsoft\$DPM\$Acct.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.

DPM 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 information about modifying the pagefile size, see "[Change the size of the virtual memory paging pool](#)" (<http://go.microsoft.com/fwlink/?LinkId=95116>).

There is a Volume Shadow Copy Service (VSS) non-paged pool limitation on x86 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 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](#), (<http://go.microsoft.com/fwlink/?LinkId=47881>).



#### Note

You can use the DPM Management Pack for Microsoft Operations Manager 2005 (MOM) or System Center Operations Manager 2007 to centrally monitor the state, health, and performance of multiple DPM servers from an Operations Management server. For

information about downloading the DPM Management Pack, see the [Microsoft Management Pack and Product Connector Catalog](http://go.microsoft.com/fwlink/?LinkId=47215) (http://go.microsoft.com/fwlink/?LinkId=47215).

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.	<ul style="list-style-type: none"> <li>One or more applications are consuming large amounts of memory.</li> <li>Multiple DPM jobs are running simultaneously.</li> <li>The DPM server does not have sufficient memory to handle the current DPM workload.</li> </ul>
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.	<ul style="list-style-type: none"> <li>Multiple DPM jobs are running simultaneously. Synchronization with consistency check jobs are particularly CPU-intensive.</li> <li>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</li> </ul>

Performance Object and Counter	Description	Value That Might Indicate a Problem	Possible Causes
			<p>large processing load on both the protected computer and the DPM server.</p> <ul style="list-style-type: none"> <li>• A runaway process is exhausting system resources.</li> <li>• The DPM server does not have sufficient processing capacity to handle the DPM workload.</li> </ul>
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.	<ul style="list-style-type: none"> <li>• Multiple DPM jobs that are running simultaneously are placing a high demand on disk resources.</li> <li>• Disk performance needs tuning.</li> <li>• Disk resources on the DPM server are not sufficient for the current DPM workload.</li> </ul>

## 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

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 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 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 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 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. For instructions, see [How to Synchronize a Replica](#) in DPM Help (<http://go.microsoft.com/fwlink/?LinkId=102162>).

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.

For information about how to create a replica manually, see [How to Manually Create a Replica](#) in DPM Help (<http://go.microsoft.com/fwlink/?LinkId=102160>).

**See Also**

[Improving Performance](#)

[Modifying Workloads](#)

## Increasing Capacity

You can also improve performance by increasing the capacity of the 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 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.

### See Also

[Managing Performance](#)

## How Protection Group Changes Affect Jobs

Changes to the configuration of a 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
<ul style="list-style-type: none"><li>• Replica creation</li><li>• Consistency check</li><li>• Synchronization</li><li>• Create recovery point on disk</li><li>• Recovery from disk</li></ul>	<ul style="list-style-type: none"><li>• Create recovery point on tape</li><li>• Verification of data on tape</li><li>• Copy data to tape</li><li>• Back up to tape</li><li>• Recovery from tape</li></ul>

The following table lists the affects of protection group changes on active jobs. Jobs can be canceled for all members of the protection group ("protection group"), all data sources on the protected computer ("protected computer"), or 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 group

<b>Change to protection group</b>	<b>Job cancellations</b>
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 protection	Replica jobs for the protection group

## See Also

[Managing Performance](#)

# Managing Tape Libraries

---

This section explains how to manage tape libraries and stand-alone tape drives that are attached to the System Center Data Protection Manager 2007 (DPM) server, including routine maintenance tasks.

For hardware operations, maintenance, and troubleshooting, see the documentation for the tape drive product.

## In This Section

[Updating Tape Library Information](#)

[Remapping Tape Drives](#)

[Disabling Tape Libraries and Tape Drives](#)

[Removing Tape Libraries](#)

[Managing the Tape Catalog](#)

[Cleaning Tape Drives](#)

[Managing Tapes](#)

[Recovering Data from Tapes](#)

## Updating Tape Library Information

You can update tape library information by using **Rescan** on the **Libraries** tab in the **Management** task area. The Rescan operation performs the following tasks:

- Checks for new tape libraries and stand-alone tape drives attached to the DPM server.
- Refreshes the state of all tape libraries and stand-alone tape drives attached to the DPM server.

Rescan can take several minutes to complete. Any library jobs that begin during rescan will be queued until rescan completes. If a library job is already in progress when rescan begins, the rescan operation fails.

If a new tape library or stand-alone tape drive is identified during rescan, DPM adds its information to the **Libraries** tab.

If you installed a new tape library or stand-alone tape drive on the DPM server and it is not identified during rescan, try the following steps to troubleshoot the problem:

1. Ensure that the tape library and drives are properly connected.

2. For SCSI connections, ensure that the logical unit number (LUN) for each device is unique.
3. Ensure that Device Manager lists all tape libraries and stand-alone tape drives attached to the DPM server.
4. Ensure the proper drivers are installed for each device.

You should rescan to refresh the state of tape libraries and stand-alone tape drives attached to the DPM server only when changes have been made to the hardware.

## Remapping Tape Drives

The **Rescan** action on the **Libraries** tab in the **Management** task area 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.

To correct the tape drive mapping, you must create a file named DPMLA.xml with the correct information, and then click **Rescan**. A template file for drive remapping, LADriveRemappingTemplate.xml, is added to the DPM server when you install DPM.

To create DPMLA.xml, open LADriveRemappingTemplate.xml from Microsoft Data Protection Manager\DPM\Config in an XML editor or Notepad, follow the instructions in the template file, and then save the file as DPMLA.xml in the Microsoft Data Protection Manager\DPM\Config folder.



### 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 IsManuallyMapped="true">
    <DriveLibraryAssociation>
```

```
<Drive SerialNumber="HUL4B06579" SCSIPort="10" SCSIBus="23" SCSTargetId="80"
SCSILun="4" DriveBayIndex="0" />

<Library SerialNumber="2B41146637" SCSIPort="6" SCSIBus="5" SCSTargetId="0"
SCSILun="1" />

</DriveLibraryAssociation>

</DriveReMapInfo>

</LAConfig>
```

## Disabling Tape Libraries and Tape Drives

You can temporarily disable a tape library or stand-alone tape drive in DPM to perform maintenance or repairs.

### ► To disable a tape library or stand-alone tape drive

1. In DPM Administrator Console, click **Management** on the navigation bar.
2. Click the **Libraries** tab.
3. In the **Display** pane, select the tape library or stand-alone tape drive that you want to remove, and then in the **Actions** pane, click **Disable**.

If any jobs are using the tape library or stand-alone tape drive, DPM will not disable the device until all jobs in progress complete.

If you disable the only tape drive installed on the DPM server, all jobs that are scheduled to use the tape drive will fail.

## See Also

[Removing Tape Libraries](#)

## Removing 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

[Disabling Tape Libraries and Tape Drives](#)

## Managing the Tape Catalog

DPM maintains metadata for each tape, referred to as the *tape catalog*, in a database. 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 automatically prunes 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.

### ► To specify tape catalog retention settings

1. In DPM Administrator Console, click **Protection** on the navigation bar.
2. Select a protection group.
3. In the **Actions** pane, click **Specify tape catalog retention**.
4. Select **For**, and then specify the duration. To use the default retention setting, select **For the duration of retention period specified for each protection group**.
5. Click **OK**.

The **Tape Catalog Retention** dialog box also lists the current size of the catalog in the database. You can modify the threshold at which DPM will alert you to the database size.

## Cleaning Tape Drives

To clean a stand-alone tape drive, load a cleaning tape and follow the hardware manufacturer's instructions. To clean a drive in a tape library using DPM, 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; you do not need to designate the tape as a cleaning tape.

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 fast inventory.

If a cleaning tape that 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 starts when DPM mounts this tape during the detailed inventory.

Follow the guidelines from the manufacturer of your tape device for cleaning frequency.

### ► To specify the cleaning tape

1. In DPM Administrator Console, click **Management** on the navigation bar.
2. Click the **Libraries** tab.

3. In the **Display** pane, select the tape to be used for cleaning, and then in the **Actions** pane, click **Mark as cleaning tape**.

#### **To clean a tape drive**

1. In DPM Administrator Console, click **Management** on the navigation bar.
2. Click the **Libraries** tab.
3. In the **Display** pane, select the drive to be cleaned, and then in the **Actions** pane, click **Clean drive**.



#### **Note**

If a cleaning tape is online and marked as a cleaning tape, you only need to run the cleaning job.

## Managing Tapes

On a stand-alone tape drive, DPM will use the same tape for daily backups of a specific protection group until there is insufficient space on the tape.

If a backup job requires more space than is available on a single tape, the job will begin, and then DPM will display an alert that a job is waiting for tape when you need to remove the full tape and add a blank tape.

DPM will not append backups from different protection groups on the same tape.

### In This Section

[How to Add and Remove Tapes](#)

[How to Identify Tapes](#)

[How to Import Tapes](#)

[How to View Tape Contents](#)

[Rotating Tapes Offsite](#)

[How to Copy Tapes](#)

[How to Inventory Tapes](#)

### How to Add and Remove Tapes

If your tape library has an insert/eject (IE) port, use the **Add tape (IE port)** and **Remove tape (IE port)** actions on the **Library** tab in the **Management** task area to add tapes or remove tapes from library slots.

If your tape library does not have an IE port, you must select the library on the **Library** tab in the **Management** task area, click **Unlock library door**, physically add or remove the tape, and then click **Lock library door**.



If you add or remove tapes to the tape library using **Unlock door** or **Add tape**, DPM will automatically inventory the library. If you add or remove tapes to the tape library without using **Unlock 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 hardware instructions, without using DPM Administrator Console.

## How to Identify Tapes

DPM identifies tapes by using the tape label. Tape labels for tapes used for long-term protection are assigned when you create a protection group. DPM assigns a default tape label in this format: **DPM - <ProtectionGroupName> - long-term tape <number>**. You can modify this label in the Create New Protection Group Wizard.

Each tape includes an on-media identifier (OMID), which is written to the start of the tape. DPM reads the tape OMID before performing an operation that uses the tape, to ensure that the tape is correct.

If your tape library includes a bar code reader, DPM displays the bar code of each tape in DPM Administrator Console. If the bar code on a tape starts with "CLN", such as bar code CLN0000812, DPM identifies the tape as a cleaning tape after a fast inventory.

## Identifying Unknown 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.
- A tape that has conflicting identification information, such as the bar code or the on-media identifier, DPM displays **Suspect** as the tape label.

### To identify unrecognized tapes

1. In DPM Administrator Console, click **Management** on the navigation bar, and then click the **Libraries** tab.
2. In the display pane, expand the tape library or stand-alone tape drive and select the unrecognized tape.
3. In the **Actions** pane, click **Identify unknown tape**.
4. In DPM Administrator Console, click **Management** on the navigation bar.
5. On the **Libraries** tab, select the unrecognized tape.
6. In the **Actions** pane, click **Identify unknown tape**.

## Managing Suspect Tapes

A *suspect* tape is a tape that has conflicting identification information. Tapes are marked as suspect in the following cases:

- Two tapes have the same bar code and different on-media identifiers (OMID)
- Two tapes have the same OMID and different bar codes
- Two tapes have same OMID, and one of the tapes does not have a bar code
- A non-cleaning tape is used for cleaning

DPM cannot use a suspect tape. To resolve the suspect status of the tape, perform the appropriate steps as listed in the following table.

Reason the tape is suspect	Resolution
Two tapes have the same bar code and different OMIDs	Change the bar code for one of the suspect tapes. After you resolve the issues for all suspect tapes, open a command prompt window and run the ResolveSuspectMedia.cmd script.
Two tapes have the same OMID and different bar codes -or- Two tapes have same OMID, and one of the tapes does not have a bar code	This indicates that one of the tapes is valid, while the invalid tape has the same OMID and is causing both tapes to be marked as suspect. <ol style="list-style-type: none"> <li>1. Remove both tapes that are marked suspect from the tape library.</li> <li>2. Open a command prompt window and run the ResolveSuspectMedia.cmd script. At this point the suspect tapes will no longer be labeled as <b>suspect</b>.</li> <li>3. Insert one of the tapes into the library.</li> <li>4. On the Libraries tab in the Management task area, click <b>Inventory library</b>. If the tape is labeled <b>suspect</b> after the inventory, this is the invalid tape and you should eject it. Re-run ResolveSuspectMedia.cmd, insert the other tape, and then run <b>Inventory library</b>. If the tape is not labeled <b>suspect</b> after the inventory, the other tape is the invalid tape.</li> </ol> After you determine the invalid tape, do not use it in this DPM server again without erasing it.
A non-cleaning tape is used for cleaning	Open a command prompt window and run the ResolveSuspectMedia.cmd script. Do not mark

Reason the tape is suspect	Resolution
	this tape as a cleaning tape again.
The bar code of a tape is changed after the OMID has been written.	Put back the old bar code, and then run ResolveSuspectMedia.cmd.
The OMID of the tape is changed or the tape is erased by software other than DPM.	Put a new bar code on the tape, and then run ResolveSuspectMedia.cmd.

You can download the ResolveSuspectMedia.cmd script at <http://go.microsoft.com/fwlink/?LinkId=96738>.

## 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, click **Management** on the navigation bar.
2. Click the **Libraries** tab, and then select the tape to import.
3. In the **Actions** pane, click **Recatalog imported tape**.

## How to View Tape Contents

If you find a tape that you cannot identify and are uncertain what to do with it, view the contents. When viewing the contents, you can copy the data that is on the tape to disk by clicking **Copy** in the tape contents dialog box. Using the **Copy** option is useful when you cannot use DPM to recover the data from the tape, such as when data spanned two tapes and only one tape can now be located.

### ▶ To view tape contents

1. In DPM Administrator Console, click **Management** on the navigation bar.
2. Click the **Libraries** tab, and then select the tape to view.
3. In the **Actions** pane, click **View tape contents**.

### ▶ To view the tapes associated with a protection group

1. In DPM Administrator Console, click **Protection** on the navigation bar.

2. In the **Display** pane, click a protection group.
3. In the **Actions** pane, click **View tape list**.

## 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 of time selected for the report.

When the data on a tape expires, return the tape to the tape library. Expired tapes not returned to the tape library will be 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.

## How to Copy Tapes

You can use DPM to copy data from a tape to disk, or from a disk or tape to tape.

### ▶ To copy the contents of a tape to disk

1. In DPM Administrator Console, click **Management** on the navigation bar.
2. Click the **Libraries** tab, 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 server 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.

You can view the progress of the copy job in the **Monitoring** task area on the **Jobs** tab.

### ▶ To copy data from disk or tape to tape

1. In DPM Administrator Console, click **Recovery** on the navigation bar.
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. **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** copies 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** reads from the source tape and copies 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** 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**.

## 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, click **Management** on the navigation bar.
2. Click the **Libraries** tab, and then select a library.
3. In the **Actions** pane, 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.

# 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 . 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 and Remove Tapes](#)

[How to Import Tapes](#)

[How to View Tape Contents](#)

[How to Copy Tapes](#)

# Disaster Recovery

---

Using Microsoft System Center Data Protection Manager 2007 (DPM) in your organization enables you to protect file and application data, and provides fast and efficient recovery of that data when the original data is lost or corrupted or mistakenly deleted. But what if the entire data center with all your critical servers is partially or completely destroyed? Or if the DPM server that is protecting the data is damaged or fails?

*Disaster recovery* refers to restoring your systems and data in the event of partial or complete failure of a computer because of 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, by using a combination of the features in DPM and the DPM System Recovery Tool.

The procedures for routine data recovery using DPM are in DPM Help and in the Operations sections for specific server types.

## In This Section

[Preparing for Disaster Recovery](#)

[Recovery](#)

[Using Pre-Backup and Post-Backup Scripts](#)

## See Also

[Managing Protected Servers Running Exchange](#)

[Managing Protected Servers Running SQL Server](#)

[Managing Protected Servers Running Windows SharePoint Services](#)

[Managing Protected Virtual Servers](#)

## Preparing for Disaster Recovery

When a computer is damaged or fails, your ability to restore that computer's functions and data depends on the actions you take before the disaster occurs.

If you use DPM for routine protection of file and application data and take no additional measures to prepare for disaster recovery, you can use DPM to recover the data after a protected computer is damaged or fails. However, you must first rebuild the computer manually by reinstalling the operating system, applications, and server configuration.

If the DPM server is damaged or fails, you must rebuild the DPM server manually and then reconfigure protection. Disk-based recovery points will not be recoverable; however, you can import existing tapes for data recovery. For more information, see [Importing Tapes](#) (<http://go.microsoft.com/fwlink/?LinkId=102163>).

If both the protected computer and the DPM server are damaged or fail, you can recover the latest backup from imported tapes after you rebuild the computers.

If both the protected computer and the DPM server are damaged or fail and you used only short-term disk-based protection, all data could be lost.

### Prepare for disaster recovery using the following methods:

1. **Back up the protected computer system state.** 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.
2. **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.

3. **Add a secondary DPM server.** A *secondary DPM server* can protect and restore a *primary DPM server*, which is a DPM server directly protecting file and application data sources. The secondary server can protect the databases of the primary DPM server, as well as the data source replicas that are stored on the primary DPM server. If the primary DPM server fails, you can restore the databases and replicas to the rebuilt primary DPM server from the secondary DPM server. You can restore data to protected computers directly from the secondary DPM server when the primary DPM server is unavailable. The secondary DPM server can also protect servers until the primary DPM server is available.
4. **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.



#### **Important**

Of these options, adding a secondary DPM server provides the greatest amount of protection. At a minimum, we strongly recommend that you back up the DPM databases regularly, either using DPM or non-Microsoft software.

## **In This Section**

[Best Practices for Disaster Recovery](#)

[Backup of Protected Computer System State](#)

[Backup of DPM Servers](#)

[Backup for Bare Metal Recovery](#)

## **See Also**

[Recovery](#)

## **Best Practices for Disaster Recovery**

Backups of data, whether by DPM or third-party software, rely on the integrity of the data being protected. To minimize the risk of data corruption, we recommend the following guidelines:

- 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.
- Use a secondary DPM server to provide additional protection and redundancy.



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.

On each protected computer, you should back up the scripting file, ScriptingConfig.xml, at \Program Files\Microsoft DPM\DPM\Scripting, and all pre-backup and post-backup scripts.

## See Also

[Backing Up DPM by Using a Secondary DPM Server](#)

[Using Pre-Backup and Post-Backup Scripts](#)

## Backup of Protected Computer System State

System state is a collection of system-specific data maintained by the operating system that must be backed up as a unit. It is not a backup of the entire system. 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.

DPM can protect the system state for any computer on which a DPM protection agent can be installed, except computers running Windows Vista or Windows Server 2008.

The system state of a protected 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).

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.

### Member Server and Desktop System State

When DPM backs up the system state of a member server or desktop, 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](http://go.microsoft.com/fwlink/?LinkId=90626)" (<http://go.microsoft.com/fwlink/?LinkId=90626>).

### **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.

## **To Change the Location of the Backup File**

The backup file of system state is created at %systemdrive%\DPM\_SYSTEM\_STATE.

### **▶ 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, if there is a protection group protecting the system state of the protected computer in step 1, run a consistency check.
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.

## **System State Backup Logs**

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.

## **See Also**

[Recovering Protected Computers](#)

## Backup of DPM Servers

You should protect the following components of a DPM server:

- The DPM database, which is required for DPM recovery.
- Replicas. Note that replicas are not required if the data sources are protected on tape, because tapes can be used to recover the data to the protected computers and to create initial replicas on a rebuilt DPM server.
- The \Program Files\Microsoft DPM\DPM\Config folder. This folder is required to protect the tape drive remapping file, DPMLA.xml.

A DPM server can protect its own database to tape. You can back up the recommended components of a DPM server by using a secondary DPM server or by using non-Microsoft software.

### In This Section

[Backing Up DPM by Using a Secondary DPM Server](#)

[Backing Up DPM Databases to Tape](#)

[Backing Up DPM by Using Third-Party Software](#)

### See Also

[Backup for Bare Metal Recovery](#)

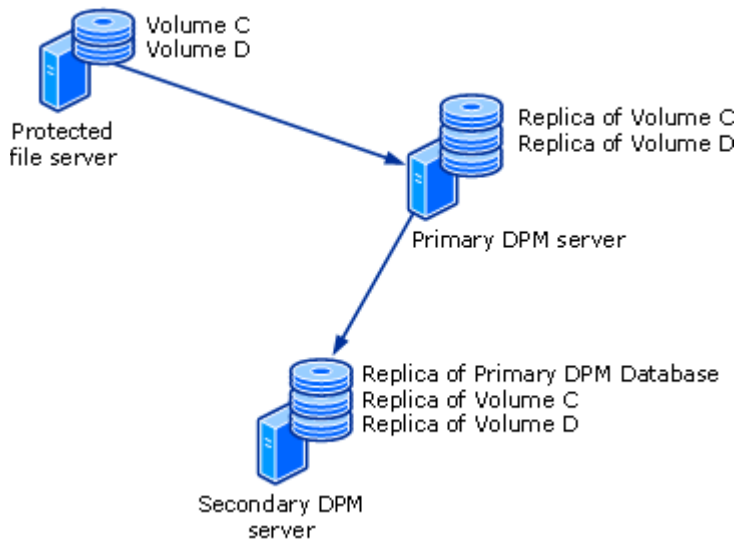
[Recovering DPM Servers](#)

### Backing Up DPM by Using a Secondary DPM Server

A DPM server can back up other DPM servers. A DPM server that protects data sources directly is called the *primary DPM server*. A DPM server that protects other DPM servers is called the *secondary DPM server*. The secondary DPM server can protect both the databases and the replicas on the primary DPM server. A DPM server can provide both secondary protection for another DPM server and primary protection for data sources.

The following illustration shows a sample topology using a primary DPM server and a secondary DPM server. In the illustration, the primary DPM server protects volumes C and D of the file server. The secondary DPM server protects the database of the primary DPM server, and also protects the replicas of volumes C and D of the file server.

#### Sample topology for backing up DPM



Using the topology shown in the illustration, if data loss occurs on the file server, you can recover the data from the primary DPM server. If the primary DPM server fails, the secondary DPM server can continue protection of the file server while the primary DPM server is unavailable, and you can recover the databases and replicas to the rebuilt primary DPM server from the secondary DPM server.

A DPM server that is providing secondary protection cannot be protected by another DPM server. For example, Server1 provides primary protection for Computer1, and Server2 provides secondary protection for Server1. Server1 cannot provide secondary protection for Server2.

A primary DPM server cannot be protected by more than one secondary DPM server.

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**.

#### **To back up a primary DPM server using a secondary 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. To enable protection of the replicas, you must establish communications between the secondary DPM server and the data sources protected by the primary DPM server. When local data sources are protected on a cluster node, you should enable protection for each cluster node in addition to the cluster. To establish communications, perform the following

steps:

- a. On the **Agents** tab in the **Management** task area, select a primary DPM server.
- b. In the **Details** pane, next to **Protected servers enabled for protection**, click **Modify**.
- c. In the **View details of protected computers** dialog box, select one or more computers, and then click **Enable protection**.
- d. Type the user name and password for a domain account that is a member of the local administrators group on all selected computers, and then click **OK**.

The **Protection enabled** column in the **View details of protected computers** dialog box will change to **Yes**.

3. You can use an existing protection group or create a new protection group for the primary DPM servers. On the **Select Group Members** page, the following data sources will be listed for each DPM server on which a protection agent is installed:
  - The databases in the instance of SQL Server on the primary DPM server
  - All volumes on the primary DPM server
  - All replicas on the primary DPM server, listed in the **Protected computers** item

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 DPM\DPM\Config folder, and the \Program Files\Microsoft DPM\DPM\Scripting folder.



**Note**

You cannot exclude file name extensions from protection for a replica.

4. On the **Select Data Protection Method** page, you can select short-term disk-based protection, long-term tape-based protection, or both. Short-term tape-based protection is unavailable when a primary DPM server is a member of a protection group.
5. 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.

**See Also**

[Switching Protection If the Primary DPM Server Fails](#)

[Recovering Protected Computers](#)

[Recovering DPM Servers](#)

## Backing Up DPM Databases 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.

### 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.

### 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 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.

### See Also

[How to Recover DPM Databases](#)

## [Using Reports](#)

### **Backing Up DPM by Using Third-Party Software**

The process for archiving the replicas and databases by using non-Microsoft software differs depending on whether the backup software supports DPM and the Volume Shadow Copy Service (VSS).

Backup software that supports DPM is specifically designed to work with DPM and will support the DPM VSS Writer service (DPM Writer).

Backup software that supports VSS uses VSS-enabled file system shadow copies but does not operate with the DPM Writer service. This software has two limitations compared to software that supports DPM:

- Archive and restore operations are more complex than they are when using software that supports DPM.
- The software that supports VSS organizes the archived replicas so that they appear to have been backed up directly from the DPM server. Organizing the backup in this way can make the process of restoring data less intuitive.

When you use backup software that does not support VSS, you cannot back up directly from the replicas. Instead, you must use the DPMBackup 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.

#### **In This Section**

[Backup Using Non-Microsoft Software That Supports DPM](#)

[Backup Using Non-Microsoft Software That Supports VSS](#)

[Backup Using Non-Microsoft Software That Does Not Support VSS](#)

#### **See Also**

[How to Recover DPM Databases](#)

[How to Recover DPM Replicas](#)

### **Backup Using Non-Microsoft Software That Supports DPM**

The optimal way to use non-Microsoft software to archive the DPM replicas and databases is to use backup software that is specifically designed to work with DPM. The principal advantages of software that supports DPM are:

- The archived data is organized 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.

▶ **To back up databases by using DPM-enabled backup software**

1. In the console tree of the backup program, browse to \Program Files\Microsoft DPM\DPM\, and select the DPMDDB folder. The file name of the DPM database file is DPMDDB2007.mdf.
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.

**See Also**

[How to Recover DPM Databases](#)

[How to Recover DPM Replicas](#)

**Backup Using Non-Microsoft Software That Supports VSS**

If your backup software supports VSS, you can back up data directly from the replicas at \Program Files\Microsoft 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 \Program Files\Microsoft DPM\DPM\, and select the DPMDDB folder. The file name of the DPM database file is DPMDDB2007.mdf.
2. In the console tree of the backup program, browse to \Program Files\Microsoft DPM\Prerequisites\, and select the Data folder. The file name of the Report database file will default to ReportServer.mdf.
3. Select the media to which you want to back up the databases.
4. 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 \Program Files\Microsoft 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.

### See Also

[How to Recover DPM Databases](#)

[How to Recover DPM Replicas](#)

### Backup Using Non-Microsoft 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 (DPMDB.mdf).

DPM creates a mount point of the backup shadow copies of the replicas on the DPM server in the folder \Program Files\Microsoft 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 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.  
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 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. 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 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.

**See Also**

[How to Recover DPM Databases](#)

[How to Recover DPM Replicas](#)

## **Backup for Bare Metal Recovery**

The DPM System Recovery Tool (SRT) is software provided with DPM to facilitate bare metal recovery for the DPM server and the computers that DPM protects. *Bare metal recovery* is a

feature that helps you recover a system that will not start. DPM SRT backs up the system volume and master boot record by copying the entire volume and using VSS writers to ensure all applications are in a consistent state for the copy.

## **Do you need bare metal recovery backup?**

The decision to add protection for bare metal recovery by using DPM SRT depends on your business needs. Your backup needs may be met adequately by disk-based and tape-based protection using DPM and a secondary DPM server. Application servers and file servers can be restored by installing the operating system and necessary applications, and then recovering the data from DPM recovery points. A DPM server can be restored by installing the operating system and necessary applications, and then recovering the DPM database from tape or the secondary DPM server.

Using DPM SRT to back up selected servers requires additional storage space. However, DPM SRT provides the ability to repair or roll back unstable systems, including unbootable systems. DPM SRT can back up a drive's master boot code, partition table, partition information, volume information, and the Logical Disk Management Database, allowing you to rebuild physically damaged or corrupted system drives.

## **In This Section**

[Installing DPM System Recovery Tool](#)

[Configuring Backups for Bare Metal Recovery](#)

## **See Also**

[How to Perform a Bare Metal Recovery](#)

## **Installing DPM System Recovery Tool**

DPM System Recovery Tool (SRT) can be installed on a DPM server or on a separate server.

When you install DPM SRT, you must specify the location for the primary file store, which will contain the DPM SRT Recovery Points. Ideally, you should locate the primary file store on a disk separate from the disk on which the operating system and DPM SRT are installed. If that is not possible, you can locate the primary file store on a separate volume on the same disk.

The amount of space required by the primary file store depends on the amount of system files you are trying to protect. For example, assume that you are protecting the system volumes of three computers running Windows Server 2003 and the average size of the system volumes is 6 GB. The storage space required would be 6 GB for one computer, and an additional 2 percent to 5 percent of space for each of the other computers. This requirement is because of DPM SRT's storage method, which stores only one copy of any file with a unique content address computed by a 128-bit MD5 cryptographic algorithm.

For more information about calculating the size of the primary file store and instructions for using the SRT Installation Wizard, open DPM SRT Help, which is the DPMSRT.chm file on the product

DVD, and view the topics "How Much Space Should I Allocate for the File Store?" and "Installation."

#### **See Also**

[Configuring Backups for Bare Metal Recovery](#)

## **Configuring Backups for Bare Metal Recovery**

You can use DPM System Recovery Tool (SRT) to back up DPM servers, file and application servers, and workstations for bare metal recovery.

To configure backups for bare metal recovery of a server, you create a *Recovery Point Schedule*. The Recovery Point Schedule specifies the computers to be backed up, the dates and times for the backup, and the Recovery Set, which is the definition of the volume entries to include in the Recovery Point.

DPM System Recovery Tool defines two Recovery Sets:

- **System Volumes**, which protects system files, system settings, and boot files
- **Disk Layout**, which protects disk information, including master boot code, partition table, partition, and volume information

You can create custom Recovery Sets in DPM SRT.

The DPM SRT agent must be installed on each computer that is backed up by DPM SRT. You can configure automatic installation of the agent when you create the Recovery Point Schedule, or you can install the agent manually.

For instructions about using DPM SRT, see DPM SRT Help, which is the DPMSRT.chm on the product DVD.

### **Custom Recovery Set for Front-End Web Server**

To back up a front-end Web server for a Microsoft Windows SharePoint Services farm, we recommend that you select the system volumes and disk layout Recovery Sets, and create a custom Recovery Set that protects the following data:

- Virtual directories that are not on the system volume
- The registry
- The Internet Information Services (IIS) metabase
- Windows SharePoint Services installation files if they are not on the system volume

#### **See Also**

[How to Perform a Bare Metal Recovery](#)

## **Recovery**

This section provides instructions for recovery in case of a disaster, such as a DPM server failing or a protected server failing. For instructions about routine data recovery using DPM, see DPM Help and the Operations sections for specific server types.

## In This Section

[Switching Protection If the Primary DPM Server Fails](#)

[Recovering Protected Computers](#)

[Recovering DPM Servers](#)

[How to Perform a Bare Metal Recovery](#)

[Using DpmSync](#)

## See Also

[Managing Protected Servers Running Exchange](#)

[Managing Protected Servers Running SQL Server](#)

[Managing Protected Servers Running Windows SharePoint Services](#)

[Managing Protected Virtual Servers](#)

## Switching Protection If the Primary DPM Server Fails

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 DPM server. You must also switch protection of the protected computers to the secondary DPM server to recover data directly from the secondary DPM server to the protected computer.

### Important

To recover Windows SharePoint Services data directly from the secondary DPM 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 DPM server.

### To switch protection to the secondary DPM server

- On the secondary DPM server, in DPM Management Shell, run the Start-ProductionServerSwitchProtection cmdlet.
- or-
- On the secondary DPM server, at a command prompt, run the SwitchProtection.ps1 script, using the following syntax:

```
SwitchProtection.ps1 dpmservername Name psname Name protectiontype Type  
username User password Password domain Domain
```

### SwitchProtection.ps1 Parameters

Parameter	Description
<b>-dpmservername</b>	The name of the server to which you are switching protection
<b>-psname</b>	The name of the protected computer for which you are switching protection
<b>-protectiontype</b>	The type of protection the server will provide: primary or secondary
<b>-username</b> <b>-password</b>	Credentials for an account with domain administrator privileges
<b>-domain</b>	The domain to which the protection computer belongs

When the primary DPM server is available again, you switch protection back to the primary DPM server to enable the primary DPM server to resume protection of the computers. You must also switch protection on the secondary DPM server to enable it to resume secondary protection of the data sources protected by the primary DPM server.

When you resume secondary protection, the replicas for the protected data sources will be inactive. You must add the data sources to a protection group on the secondary DPM server again, using the automatic replica creation option, and then the replicas will become active.



#### Note

After you resume secondary protection, if the replicas are not inactive, run `SwitchProtection.ps1` on the secondary DPM server again.

#### Example

In the following example, you switch primary protection for computer SQL1 to the secondary DPM server, DPM2, for recovery or continued protection, by running the following command on DPM2:

```
SwitchProtection.ps1 dpmservername dpm2 psname sql1 protectiontype  
primary username administrator password Password~1 domain dc990
```

In the following example, you switch primary protection for computer SQL1 back to the primary DPM server, DPM1.

First, you run the following command on DPM1:

```
SwitchProtection.ps1 dpmservername dpm1 psname sql1 protectiontype  
primary username administrator password Password~1 domain dc990
```

Second, you run the following command on DPM2:

```
SwitchProtection.ps1 dpmservername dpm2 psname sql1 protectiontype  
secondary username administrator password Password~1 domain dc990
```



## Note

The SwitchProtection.ps1 script is available on the DPM 2007 product DVD. During DPM setup, the script is installed to the installation path at \Microsoft DPM\DPM\bin.

## See Also

[Backing Up DPM by Using a Secondary DPM Server](#)

[Recovering Protected Computers](#)

## Recovering Protected Computers

This topic includes instructions for recovering system state to a protected computer and recovering data to a protected computer from the secondary DPM server.

### 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 DPM server is unavailable, you can recover data for protected computers from the secondary DPM server. To recover data to an alternate location from a secondary DPM server, you use the Recovery Wizard in DPM Administrator Console on the secondary DPM server with no additional steps required. To recover data to the original location from a secondary DPM server, you must first switch protection to the secondary DPM 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 DPM 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 DPM 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

If the server is inaccessible, set up a new server either by restoring the DPM server image using DPM System Recovery Tool (SRT) or installing the operating system and applications, including DPM, and then restoring the DPM database and replicas.

When you recover a primary DPM server, you must reestablish protection for the computers that were previously protected by the DPM server.

For more information about recovering a DPM server by using DPM SRT, see "Bare Metal Recovery" in DPM SRT Help.

### In This Section

[How to Recover DPM Databases](#)

[How to Recover DPM Replicas](#)

[How to Reestablish Protection After Recovering the Primary DPM Server](#)

### See Also

[Using DpmSync](#)

### How to Recover DPM Databases

When recovering the DPM database files, ensure that the location on the DPM computer where you restore the files is secure.

#### To recover the DPM database when the database is corrupt

1. Uninstall DPM and retain the disk-based replicas.
2. Delete the DPM database.
3. Install a new instance of DPM server.
4. Import the latest DPM tape backup and recover the database to an alternate location, or recover the database as a file from the secondary DPM server.
5. Run **DPMSync dbrestore dbloc *location***.
6. Run **DPMSync sync**.

DPMSync takes the DPM service offline and attaches the backed up database to SQL Server.

### See Also

[Using DpmSync](#)

### How to Recover DPM Replicas

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 invalid and not in a waiting manual load state.

#### ▶ **To recover replicas after the DPM database is recovered**

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.

#### **See Also**

[Backup of DPM Servers](#)

### **How to Reestablish Protection After Recovering the Primary DPM Server**

After you rebuild a primary DPM server, you must reestablish protection of the computers that were protected by the primary DPM server. Perform the following procedure on each computer that was protected by the primary DPM server.

#### ▶ **To reestablish protection after rebuilding the primary DPM 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 DPM server, in the format of *Domain/Name*, is a member of the following groups:
    - Distribute COM Users
    - DPMRADCOMTrustedMachines
    - DPMRADmTrustedMachines
  - c. If the primary DPM 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 DPM server is listed, the Access Control List (ACL) entry might be incorrect. Remove the entry, and then add the primary DPM server with full permissions.
  - If the primary DPM server is not listed, add the primary DPM server with full permissions.

## How to Perform a Bare Metal Recovery

If you use DPM System Recovery Tool (SRT) to back up the DPM server or a protected computer, you can perform a bare metal recovery in the case of a hardware failure.

For instructions about recovering a DPM server by using DPM SRT, see "Bare Metal Recovery" in DPM SRT Help.

### See Also

[Backup for Bare Metal Recovery](#)

## 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 **-Sync**

DpmSync **-DpmDbLoc** *location*

DpmSync **-DpmReportDbLoc** *location*

DpmSync **-ReallocateReplica**

DpmSync **-?**

### Parameters

Parameter	Description
<b>-Sync</b>	Synchronizes restored databases and reallocates missing replica volumes. You must run DpmSync –Sync after you restore the databases. After you run DpmSync –Sync, some replicas may still be marked as missing. To reallocate these replicas, on the <b>Disks</b> tab of the <b>Management</b> task area in DPM Administrator Console, remove the missing disks from DPM and then run DpmSync - reallocate replica.
<b>-DpmDbLoc</b> <i>location</i>	Identifies the location of backup of DPM database.
<b>-DpmReportDbLoc</b> <i>location</i>	Identifies the location of backup of Report database.
<b>-ReallocateReplica</b>	Reallocates all missing replica volumes without synchronization.
<b>-?</b>	Describes usage of the command.

### Example

To restore the DPM and Report databases from local backup media on the DPM server, you run the following commands:

**DpmSync -DpmDbLoc G:\DPM\Backups\2005\November\DPMDB.bak**

**DpmSync -DpmReportDbLoc G:\DPM\Backups\2005\November\ReportServer.bak**

After you restore the DPM and Report databases, to synchronize the databases, you run the following command:

**DpmSync -Sync**

After you restore and synchronize the DPM and Report databases and before you restore the replicas, you run the following command to reallocate disk space for the replicas:

**DpmSync -ReallocateReplica**

### See Also

[How to Recover DPM Databases](#)

[How to Recover DPM Replicas](#)

## 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.

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" </PreBackupScript>
    <PreBackupCommandLine>parameters</PreBackupCommandLine>
    <PostBackupScript>"Path\Script" </PostBackupScript >
    <PostBackupCommandLine>parameters</PostBackupCommandLine>
    <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.
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, ? for Virtual Server, and ? 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 execution status of the DPM backup job.

## 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
<ul style="list-style-type: none"> <li>• Manually synchronize a replica</li> <li>• Perform a manual consistency check on a replica</li> <li>• Manually create a recovery point</li> <li>• Remove a member from a protection group</li> <li>• Delete a replica</li> </ul>	The protected data source in the <b>Protection</b> task area
<ul style="list-style-type: none"> <li>• Modify the schedules for synchronization, express full backups, consistency checks, and recovery points</li> <li>• Enable compression</li> <li>• Add a member to a protection group</li> <li>• View a list of tapes</li> <li>• Stop protection of a group</li> </ul>	The protection group in the <b>Protection</b> task area
<ul style="list-style-type: none"> <li>• Configure tape catalog retention</li> </ul>	Either the protected computer or the protection

To perform this task	Select
	group in the <b>Protection</b> task area
<ul style="list-style-type: none"> <li>Modify disk allocation</li> </ul>	Either the protected data source or the protection group in the <b>Protection</b> task area
<ul style="list-style-type: none"> <li>Configure network bandwidth usage throttling</li> <li>Update, disable, enable, or uninstall a protection agent</li> </ul>	The protected computer on the <b>Agents</b> tab in the <b>Management</b> task area
<ul style="list-style-type: none"> <li>Lock or unlock the tape library door</li> <li>Rescan the tape library</li> </ul>	The tape library or stand-alone tape drive on the <b>Libraries</b> tab in the <b>Management</b> task area
<ul style="list-style-type: none"> <li>Clean a tape library drive</li> </ul>	The tape drive on the <b>Libraries</b> tab in the <b>Management</b> task area
<ul style="list-style-type: none"> <li>Run a fast or detailed inventory</li> </ul>	Any tape library, stand-alone tape drive, drive, slot, or tape on the <b>Libraries</b> tab in the <b>Management</b> task area
<ul style="list-style-type: none"> <li>Erase a tape</li> <li>Mark a tape as free</li> <li>Mark a tape as a cleaning tape</li> <li>View the contents of a tape</li> </ul>	A tape on the <b>Libraries</b> tab in the <b>Management</b> task area

## Appendix B: DPM 2007 Schema Extension

The DPMADSchemaExtension tool performs the following tasks to support end-user recovery:

- Extends the schema
- Creates a container (MS-ShareMapConfiguration)
- Grants the 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 Data Protection Manager (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
IDAPDisplayName	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



Attribute	Description
	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

Attribute	Value
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

Data Protection Manager 2007 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 2007.

**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
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 collected
EndDateTime	Date and time	Internal field
ScheduleType	Integer 0=Weekly 1=Monthly 2=Quarterly	The schedule period which this data represents

	3=Yearly	
--	----------	--

**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 identifier for the protection group to which this data source belongs
ServerId	GUID	The unique identifier 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
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 identifier 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 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
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 identifier generated by DPM for the replica volume
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 identifier 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 identifier 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 identifier for the protection group to which this data source belongs
ServerId	GUID	The unique identifier 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 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