Deploying System Center Data Protection Manager 2007

Microsoft Corporation

Published: Sep 2007

Abstract

Deploying DPM 2007 provides step-by-step instructions for installing and configuring DPM 2007, and includes an introduction to the DPM user interface. Deploying DPM 2007 also provides information on troubleshooting your DPM installation and how to repair and uninstall DPM 2007.

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.

Contents

Deploying DPM 2007

This content provides instructions for deploying Data Protection Manager 2007.

In This Section

Installing DPM 2007

A System Center Data Protection Manager (DPM) 2007 installation is comprised of two primary tasks: installing the DPM prerequisite software and installing the DPM application. The DPM Setup Wizard guides you through the process of specifying the DPM installation settings, and automatically installs or provides links to install the prerequisite software as part of the integrated DPM installation process.

This section includes the following:

- System requirements for the DPM server.
- Instructions for specifying the non-default settings when installing the operating system before installing DPM.
- Step-by-step instructions for installing DPM.

If you want to use retail copies of one or more of the prerequisite products for your DPM installation, or if the automatic installation of one or more of the DPM prerequisite software products fails, you can use the information in this topic to help you install the prerequisite software manually.

In This Section

DPM 2007 System Requirements

Before you install System Center Data Protection Manager (DPM) 2007, you need to ensure that the DPM server and the computers and applications it is going to protect meet network and security requirements. You must also ensure that they are running on supported operating systems and that they meet the minimum hardware requirements and software prerequisites.

DPM is designed to run on a dedicated, single-purpose server that cannot be either a domain controller or an application server. The DPM server must not serve as a management server for Microsoft Operations Manager (MOM) 2005 or Microsoft System Center Operations Manager 2007; you can, however, monitor the DPM server and the computers that it protects in MOM or Operations Manager.

In This Section

Security Requirements

Network Requirements

Hardware Requirements

Software Prerequisites

Security Requirements

Following are the System Center Data Protection Manager (DPM) 2007 security requirements:

- Before you install DPM 2007, you must log on to the computer as a domain user who is a member of the local administrators group.
- After you install DPM, you must be a domain user with administrator access to use DPM Administrator Console.

See Also

Hardware Requirements

Network Requirements

Software Prerequisites

Network Requirements

Following are the System Center Data Protection Manager (DPM) 2007 network requirements:

- The DPM server must be deployed within a Windows Server 2003 Active Directory domain. The domain controllers can be running Windows Server 2000, Windows Server 2003, Windows Server 2003 R2 Server, or Windows Server 2008 operating system (pre-release version).

DPM 2007 running on Windows Server 2000 domain controllers does not support the following:

- Protecting computers across domains.
- Protecting a child Windows Server 2000 domain controller in a domain where Windows Server 2000 is the primary domain controller.
- Protecting computers running Exchange Server 2007.

DPM 2007 running on Windows Server 2003 domain controllers supports protecting computers across domains within a forest; however, you must establish two-way trust across the domains. If there is not two-way trust across domains, you must have a separate DPM server for each domain. DPM 2007 does not support protection across forests.

Active Directory Domain Services, an essential component of the Windows Server 2003 architecture, provides organizations with a directory service designed for distributed computing environments. Active Directory Domain Services allows organizations to centrally manage and share information about network resources and users while acting as the central authority for network security. In addition to providing comprehensive directory services to a Windows environment, Active Directory Domain Services is designed to be a consolidation point for isolating, migrating, centrally managing, and reducing the number of directories that companies require.

- The DPM server requires persistent connectivity with the servers and desktop computers it protects.

Note

If you are protecting data over a wide area network (WAN), there is a minimum network bandwidth requirement of 512 kilobits per second (kbps).

See Also

Hardware Requirements

Security Requirements

Software Prerequisites

Hardware Requirements

System Center Data Protection Manager (DPM) 2007 requires a disk that is dedicated to the storage pool and a disk that is dedicated to the following:

- System files
- DPM installation files
- DPM prerequisite software

- DPM database files

Note

You can install DPM on the same volume that the operating system is installed on, or you can install DPM on a different volume that does not include the operating system. However, you cannot install DPM on the disk that is dedicated to the *storage pool*, which is a set of disks on which the DPM server stores the replicas and recovery points for the protected data.

DPM owns and manages the disks in the storage pool, which must be dynamic. For purposes of DPM, *disk* is defined as any disk device manifested as a disk in Disk Management. For information about the types of disks that the storage pool supports and how to plan your disk configuration, see Planning the Storage Pool (http://go.microsoft.com/fwlink/?LinkId=91965).

If you want to manage your own additional disk space, DPM enables you to attach or associate custom volumes to data sources that you are protecting in a protection group. Custom volumes can be on basic or dynamic disks. Any volume that is attached to the DPM server can be selected as a custom volume; however, DPM cannot manage the space in custom volumes. Note that this release of DPM 2007 will not delete any existing volumes on the disk attached to the storage pool to make the entire disk space available.

Note

If you have critical data that you want to store, you can use a high-performance logical unit number (LUN) on a storage area network rather than the DPM-managed storage pool.

The following table lists the minimum and recommended hardware requirements for the DPM server. For information about planning DPM server configurations, see Planning for DPM Deployment (http://go.microsoft.com/fwlink/?LinkId=91848).

Note

We recommend that you install DPM on a 64-bit machine.

Component	**Minimum Requirement**	**Recommended Requirement**
Processor	• 1 gigahertz (GHz) or faster.	• 2.33 GHz Quad
Memory	• 2 gigabytes (GB) RAM For information about how DPM manages memory, see DPM and Memory (http://go.microsoft.com/fwlink/?LinkId=97938).	• 4 GB RAM
Pagefile	• 0.15 percent of the total DPM storage pool. For information about configuring the DPM pagefile size, in the DPM Operations Guide see Managing Performance	N/A

Component	Minimum Requirement	Recommended Requirement
	(http://go.microsoft.com/fwlink/?LinkId=91859).	
Disk space for DPM installation	- Program files drive: 410 megabytes (MB). - Database files drive: 900 MB. - System drive: 2650 MB. **Note** The system drive disk space requirement is necessary if you chose to install the instance of SQL Server from the DPM download package. If you are using an existing instance of SQL Server, this disk space requirement is considerably less.	- 2–3 GB of free space on the program files volume **Note** DPM requires a minimum of 300 MB of free space on each protected volume for the change journal. Additionally, before archiving data to tape, DPM copies the file catalog to a DPM temporary installation location; therefore, we recommend that the volume on which DPM is installed contains 2–3 GB of free space.
Disk space for storage pool **Note**	- 1.5 times the size of the protected data. For information about calculating capacity requirements and planning the configuration of the disks, in Planning a DPM 2007	- 2–3 times the size of the protected data

Component	Minimum Requirement	Recommended Requirement
The storage pool does not support Universal Serial Bus (USB)/1394 disks.	Deployment see Planning the Storage Pool (http://go.microsoft.com/fwlink/?LinkId=91965).	
Logical unit number (LUN)	N/A	• Maximum of 17 TB for GUID partition table (GPT) dynamic disks • 2 TB for master boot record (MBR) disks **Note** These requirements are based on the maximum size of the disk as it appears to the Windows Server operating system.

See Also

Network Requirements

Security Requirements

Software Prerequisites

Software Prerequisites

A complete installation of System Center Data Protection Manager (DPM) 2007 includes the DPM server operating system, the DPM prerequisite software, and the DPM application. Each computer that DPM protects must meet the protected computer software requirements.

In This Section

- DPM Server Operating System Prerequisites
- DPM Server Software Prerequisites
- Protected Computer Software Prerequisites
- Manually Installing Prerequisite Software

DPM Server Operating System Prerequisites

Before installing DPM on the required operating systems listed in this section, note the following:

- DPM supports Standard and Enterprise Editions for all supported DPM operating systems.
- DPM supports 32-bit and x64-bit operating systems. DPM does not support ia64-bit operating systems.
- There is a Volume Shadow Copy Service (VSS) non-paged pool limitation on x86 32-bit operating systems. If you are protecting more than 10 terabytes (TB) of data, the DPM server must be running on a 64-bit operating system. In addition, because VSS non-paged pool usage is based on the size of a single volume, we recommend that you do not protect a single volume larger than 4 TB of data on 32-bit operating systems.

The following are the System Center Data Protection Manager (DPM) 2007 operating system requirements:

- Windows Server 2003 with Service Pack 2 (SP2) or later.

  To download SP2 for Windows Server 2003, see Windows Server 2003 Service Pack 2 (http://go.microsoft.com/fwlink/?LinkID=90633).

  Caution

  DPM is designed to run on a dedicated, single-purpose server that cannot be either a domain controller or an application server.

- Windows Server 2003 R2 with SP2.
- Windows Storage Server 2003 with SP2.

  To obtain SP2 for Windows Storage Server 2003 or Windows Storage Server 2003 R2, contact your original equipment manufacturer.

- Windows Storage Server 2003 R2 with SP2.

For information about installing Windows Server 2003, see How to Install Windows Server 2003.

DPM Management Shell, an interactive command-line technology that supports task-based scripting is supported on the following operating systems:

- Windows XP Service Pack 2.
- Windows Vista.
- Windows Server 2003 Service Pack 2 (SP2) and subsequent versions.

Note

DPM Management Shell can be installed on computers other than the DPM server, enabling you to administer multiple DPM servers remotely.

See Also

Security Requirements

Network Requirements

Hardware Requirements

Software Prerequisites

How to Install Windows Server 2003

You must properly configure Windows Server 2003 to support a System Center Data Protection Manager (DPM) 2007 installation. If Windows Server 2003 is not installed on your computer, for more information about purchasing and installing Windows Server 2003, go to the Microsoft Windows Server Web site (http://go.microsoft.com/fwlink/?LinkID=64826).

Perform the following procedure to specify nondefault settings during an installation of Windows Server 2003 on a DPM server.

Procedures

To install Windows Server 2003

1. When Setup prompts you to format the Windows installation partition, choose the **NTFS** file system.
2. In the **Computer Name** dialog box, type a name for the DPM server. The name must be unique within the Active Directory domain.
3. In the **Workgroup or computer domain** dialog box, add the DPM server to the domain that contains the computers that you plan to protect.

   You can install DPM across domains within a forest if you establish a two-way trust across the domains. If there is not a two-way trust across domains, you must have a separate DPM server for each domain. DPM 2007 does not support protection across forests.

4. After installation is complete, apply all available Windows Server 2003 service packs and updates, including Windows Server 2003 Service Pack 2 (SP2).

   All Windows updates are available from Microsoft Windows Update (http://go.microsoft.com/fwlink/?LinkID=451).

   Windows Server 2003 SP2 is available from Windows Server 2003 Service Pack 2 (http://go.microsoft.com/fwlink/?LinkID=90633).

See Also

Hardware Requirements

Network Requirements

Security Requirements

Software Prerequisites

DPM Server Software Prerequisites

The System Center Data Protection Manager (DPM) server must be a dedicated, single-purpose server, and it cannot be either a domain controller or an application server. The DPM server cannot be the management server for Microsoft Operations Manager (MOM) 2005 or Microsoft System Center Operations Manager 2007.

Before you install DPM, you must install the following:

- Knowledge Base article 940349, "Availability of a Volume Shadow Copy Service (VSS) update rollup package for Windows Server 2003 to resolve some VSS snapshot issues" (http://go.microsoft.com/fwlink/?LinkId=99034).

Note

After installing Knowledge Base article 940349 and then restarting the DPM server and/or the protected server, we recommend that you refresh the protection agents in DPM Administration Console. To refresh the agents, in the **Management** task area, click the **Agents** tab, select the computer, and then in the **Actions** pane, click **Refresh information**. If you do not refresh the protection agents, Error ID: 31008 may appear because DPM only refreshes the protection agents every 30 minutes.

- Windows PowerShell 1.0 from http://go.microsoft.com/fwlink/?LinkId=87007.
- Single Instance Storage (SIS) on Windows Server 2008 operating system (Pre-release version). For information about installing SIS on Windows Server 2008, see Manually Install Required Windows Components.

If you want to manually install the required prerequisite software, you must follow the steps detailed in Manually Installing Prerequisite Software.

Following is the DPM server prerequisite software that DPM Setup installs before installing the DPM application:

- Windows Deployment Services (WDS) on Windows Server 2003 Service Pack 2 (SP2) servers.

  -OR-

  SIS on Windows Storage Server 2003 R2.

  Note

  If WDS and SIS are not already installed, DPM Setup prompts you for the Microsoft Windows Server 2003 product CD during the installation.

- Microsoft .NET Framework 2.0.
- Internet Information Services (IIS) 6.0 for Windows Server 2003. (IIS 6.0 is not installed on Windows Server 2003 by default.)
- IIS 7.0 for Windows Server 2008 (Pre-Release version). (IIS 7.0 is not installed on Windows Server 2008 by default. If IIS is not installed before installing SQL Server 2005, SQL Server will not install SQL Server Reporting Services.)

  Caution

  This release of DPM 2007 does not support a Windows Server 2008 installation in a production environment.

  Important

  In addition to the default components that IIS 7.0 installs, DPM requires all IIS 7.0 components. For more information, see "Installing the Required Components for Windows Server 2008" in Manually Installing Prerequisite Software.

- Microsoft SQL Server 2005 Workstation components.

  You can use an existing remote instance of SQL Server for your DPM database. If you choose to use a remote instance of SQL Server, you must install **sqlprep.msi**.

  To use an instance of SQL Server on a remote computer, run **sqlprep.msi**, which is located on the DPM product DVD in the **DPM2007\msi\SQLprep** folder.

  Verify that the user account you will be using to run the SQL Server service and the SQL Server Agent service has read and execute permissions to the SQL Server installation location.

Note

The remote instance of SQL Server cannot be on a computer that is running as a domain controller.

- Microsoft SQL Server 2005 with Reporting Services.

  If SQL Server Reporting Services is installed on the remote SQL Server, DPM Setup will use that Reporting Service. If SQL Server Reporting Services is not installed on the remote computer running SQL Server, you must install and configure the service on the remote computer running SQL Server.

Note

DPM 2007 contains the Standard Edition of SQL Server 2005.

- Microsoft SQL Server 2005 Service Pack 2.

See Also

Hardware Requirements

Network Requirements

Security Requirements

Protected Computer Software Prerequisites

Each computer that System Center Data Protection Manager (DPM) 2007 protects must meet the requirements listed in the following table. Protected volumes must be formatted as NTFS file system. DPM cannot protect volumes formatted as FAT or FAT32. Also, the volume must be at least 1 gigabyte (GB) for DPM to protect it. DPM uses the Volume Shadow Copy Service (VSS) to create a snapshot of the protected data, and VSS will create a snapshot only if the volume size is greater than or equal to 1 GB.

Before you install protection agents on the computers you are going to protect, you must apply hotfix 940349. For more details, see Microsoft Knowledge Base article 940349, "Availability of a Volume Shadow Copy Service (VSS) update rollup package for Windows Server 2003 to resolve some VSS snapshot issues" (http://go.microsoft.com/fwlink/?LinkId=99034).

Note

After installing Knowledge Base article 940349 and then restarting the DPM server and/or the protected server, we recommend that you refresh the protection agents in DPM Administration Console. To refresh the agents, in the **Management** task area, click the **Agents** tab, select the computer, and then in the **Actions** pane, click **Refresh information**. If you do not refresh the protection agents, Error ID: 31008 may appear because DPM only refreshes the protection agents every 30 minutes.

Protected Computer Requirements

Protected Computers	Computer Requirements
File servers	You can protect file servers on any of the following operating systems: • Windows Server 2003 with Service Pack 1 (SP1) or later • Windows Server 2003 x64 • Windows Server 2003 R2

Protected Computers	**Computer Requirements**
	• Windows Server 2003 R2 x64 • Windows Storage Server 2003 with SP1 or later **Note** To obtain SP1 for Windows Storage Server 2003, contact your original equipment manufacturer. • Windows Storage Server 2003 R2 • Windows Storage Server 2003 R2 x64 • Windows Server 2008 operating system (Pre-release version). **Note** DPM supports Standard and Enterprise Editions of all the required operating systems.
Computers running SQL Server	• Microsoft SQL Server 2000 with Service Pack 4 (SP4) - OR - • Microsoft SQL Server 2005 with SP1 or Service Pack 2 (SP2) **Note** DPM supports Standard, Enterprise, Workgroup, and Express Editions of SQL Server. **Important** You must start the SQL Server VSS Writer Service on computers running SQL Server 2005 SP1 before you can start protecting SQL Server data. The SQL Server VSS Writer Service is turned on by default on computers running SQL Server 2005. To start the SQL Server VSS Writer service, in the **Services** console, right-click **SQL Server VSS writer**, and then click **Start**.
Computers running Exchange Server	• Exchange Server 2003 with SP2 - OR - • Exchange Server 2007 **Note**

Protected Computers	Computer Requirements
	DPM supports Standard and Enterprise Editions of Exchange Server. • Before you can protect Exchange Server 2007 data in a Clustered Continuous Replication (CCR) configuration, you must install hotfix 940006. For more details, see Knowledge Base article 940006, "Description of Update Rollup 4 for Exchange 2007" (http://go.microsoft.com/fwlink/?LinkId=99291). **Important** • The eseutil.exe and ese.dll versions that are installed on the most recent edition of Exchange Server must be the same versions that are installed on the DPM server. • In addition, you must update eseutil.exe and ese.dll on the DPM server if they are updated on a computer running Exchange Server after applying an upgrade or an update. • For more information about updating eseutil.exe and ese.dll, see Eseutil.exe and Ese.dll.
Computers running Virtual Server	• Microsoft Virtual Server 2005 R2 SP1 **Note** To protect virtual machines for online backups, we recommend that you install version 13.715 of Virtual Machine Additions (http://go.microsoft.com/fwlink/?LinkId=84271).
Windows SharePoint Services	• Windows SharePoint Services 3.0 • Microsoft Office SharePoint Server 2007 Before you can protect Windows SharePoint Services (WSS) data, you must do the following: • Install Knowledge Base article 941422, "Update for Windows SharePoint Services 3.0" (http://go.microsoft.com/fwlink/?LinkId=100392). • Start the WSS Writer service on the WSS Server and then provide the protection agent with credentials for the WSS farm. For more

Protected Computers	Computer Requirements
	information, in Configuring DPM 2007, see "Starting and Configuring the WSS VSS Writer Service" (http://go.microsoft.com/fwlink/?LinkId=100247). • Update the instance of SQL Server 2005 to SQL Server 2005 SP2.
Shared disk clusters	• File servers • SQL Server 2000 with SP4 • SQL Server 2005 with SP1 • Exchange Server 2003 with SP2 • Exchange Server 2007
Non-shared disk clusters	• Exchange Server 2007
Workstations	• Windows XP Professional SP2 • All Windows Vista editions except Home (must be a member of a domain)

Eseutil.exe and Ese.dll

The versions of the Exchange Server Database Utilities (eseutil.exe) and ese.dll that are installed on the computer running the most recent edition of Exchange Server must be the same versions that are installed on the DPM server. For example, if you are protecting Exchange Server 2003 SP2, Exchange Server 2007, and Exchange Server 2007 SP1, you must copy eseutil.exe and ese.dll from the computer running Exchange Server 2007 SP1 to the DPM server.

The following scenarios determine the versions of eseutil.exe and ese.dll that you must install on the DPM server in the **<driver letter>:\Program Files\Microsoft DPM\DPM** folder.

Scenarios determining eseutil.exe and ese.dll versions

DPM Server Protecting:	DPM Processor type	Copy the Exchange Server Version of Eseutil.exe and Ese.dll from:
• Exchange Server 2007 (64-bit)	32-bit **Note** 64-bit DLLs cannot be used on a 32-bit computer.	Exchange Server 2007

DPM Server Protecting:	DPM Processor type	Copy the Exchange Server Version of Eseutil.exe and Ese.dll from:
• Exchange Server 2007 (64-bit) *And* • Exchange Server 2007 (64-bit) and Exchange Server 2003	32-bit **Note** The Exchange Server 2007 version binaries work with both versions of Exchange Server 2007 and Exchange Server 2003 databases.	Exchange Server 2007 (32-bit version) You can obtain this version from the Exchange Server 2007 Setup DVD or on the Exchange Server TechCenter Web site (http://go.microsoft.com/fwlink/?LinkId=83451).
• Exchange Server 2007 (64-bit) *Or* • Exchange Server 2007 (64-bit) and Exchange Server 2003	64-bit	Exchange Server 2007
• Exchange Server 2003	32-bit	Exchange Server 2003
• Exchange Server 2003	64-bit **Note** You can copy the 32-bit files from a computer running Exchange Server 2003 to a DPM server with a 64-bit processor.	Exchange Server 2003

See Also

Hardware Requirements

Network Requirements

Security Requirements

Software Prerequisites

Install DPM 2007

A System Center Data Protection Manager (DPM) 2007 installation involves installing the DPM prerequisite software and the DPM application. The DPM Setup Wizard guides you through the process of specifying the DPM installation settings, and it automatically installs or provides links to install the prerequisite software as part of the integrated DPM installation process. Throughout the installation process, DPM Setup provides status on the installation progress.

Important

> DPM 2007 requires a clean installation of DPM. Before you install DPM 2007, you must first uninstall System Center Data Protection Manager 2006 (DPM 2006) and its associated prerequisite software, as well as any previous versions of DPM. Because of the architectural differences between DPM 2006 and DPM 2007, you cannot directly upgrade a computer running DPM 2006 to DPM 2007. However, DPM 2007 includes an upgrade tool that enables you to migrate your DPM 2006 protection group configurations to DPM 2007. For more information about upgrading from DPM 2006 to DPM 2007, see Upgrading DPM 2006 to DPM 2007 (http://go.microsoft.com/fwlink/?LinkId=66737).

On a computer running the Windows Server 2003 operating system, if Internet Information Services (IIS) 6.0 and Single Instance Storage (SIS) are not already installed, DPM Setup prompts you for the DPM product DVD during the installation. By default, Windows Server 2003 does not install IIS or SIS after you install Windows Server 2003. If you are installing DPM on Windows Storage Server, SIS is installed by default.

Note

> This release of DPM 2007 does not support a Windows Server 2008 operating system (pre-release version) installation in a production environment.

The DPM Setup Wizard is designed to install DPM prerequisite software from the DPM product DVD. If you want to use retail copies of one or more of the prerequisite products for your DPM installation, install the products manually before you start the DPM Setup Wizard. For information about installation settings for prerequisite software, see Manually Installing Prerequisite Software.

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

Important

If you choose to install DPM or prerequisite software products from a shared folder, DPM Setup adds the Universal Naming Convention (UNC) path of the shared folder to the Internet Explorer local intranet security zone for the duration of the installation.

Note

You cannot install DPM 2007 on the same computer on which your Exchange Server is running.

DPM supports 32-bit and x64-bit operating systems. You can install the DPM 32-bit version only on a 32-bit operating system and the DPM 64-bit version only on an x64-bit operating system.

DPM Setup will stop the Removable Storage service, before installing DPM 2007.

To install DPM

1. Log on to the DPM server using a domain user account that is a member of the local administrators group.
2. Insert the DPM product DVD in the DVD-ROM drive. If the DPM Setup Wizard does not start automatically, double-click **Setup.exe** in the root folder of the DVD.

   -Or-

   If you are installing DPM from a network share, navigate to the installation share, and then double-click **Setup.exe** in the root folder of the share.
3. On the **Microsoft System Center Data Protection Manager 2007** screen, click **Install Data Protection Manager**.
4. On the **Microsoft Software License Terms** page, review the license agreement. If you accept the terms, click **I accept the license terms and conditions**, and then click **OK**.

   You can copy and paste the license agreement into a text editor, such as Notepad, for printing. After installation is complete, you can access the license agreement from DPM Administrator Console by clicking the product information icon on the navigation bar.

   Note

   DPM installs Microsoft .NET Framework 2.0 if it has not already been installed.
5. On the **Welcome** page, click **Next**.

   DPM begins a prerequisites check for all required hardware and software.
6. On the **Prerequisites Check** page, wait while DPM Setup checks the system to verify that it meets software and hardware requirements.

   - If all required components are present, DPM Setup displays a confirmation. Click **Next** to continue.
   - If one or more required or recommended components are missing or noncompliant, Setup displays a warning or error message.

     Warning. Indicates that a recommended component is missing or noncompliant. Review the warning and determine whether to resolve the issue now or continue with the installation. If you choose to continue with the installation, plan to resolve the issue as soon as possible.

Error. Indicates that a required component is missing or noncompliant. You must resolve the error before you can continue with the installation.

7. On the **Product Registration** page, enter your registration information. In the **Protection agent licenses** section do the following:

   a. In the **Standard licenses** box, type the number of licenses that you have purchased to authorize protection of file resources and system state.

   b. In the **Enterprise licenses** box, type the number of licenses that you have purchased to authorize protection of both file and application resources.

      Note

      If you purchase additional licenses after you set up DPM or reallocate licenses from one DPM server to another, you can update the number of available licenses for each DPM server in DPM Administrator Console. For information about updating your protection agent licenses, in DPM 2007 Help, see "How to Update DPM License Information".

8. On the **Installation Settings** page, in the **DPM Program Files** section, accept the default folder or click **Change** to browse to the folder in which you want to install DPM.

   You can install DPM only on a local drive, and you cannot install it in read-only folders, hidden folders, or directly to local Windows folders such as Documents and Settings or Program Files. (DPM can, however, be installed to a subfolder of the Program Files folder.)

   Important

   The installation partition must be formatted with the NTFS file system. To simplify recovery in the event of system partition failure, install DPM to a partition that is separate from the system partition.

9. On the **Installation Settings** page, in the **SQL Server settings** section, specify whether you want to install the MS$DPM2007$ instance of Microsoft SQL Server from the DPM product DVD or on a local or remote instance of SQL Server that already exists. For detailed instructions on how to install a remote instance of SQL Server, see Manually Install SQL Server 2005 (http://go.microsoft.com/fwlink/?LinkId=102396).

   If you want to use the MS$DPM2007$ instance that already exists, select the dedicated instance option to use the instance of SQL Server that is installed with DPM. If you want to use an instance other than the local MS$DPM2007$ instance, select a different instance of SQL Server 2005 on the **SQL Server Settings** page.

   If you are using an existing instance of SQL Server with the DPM installation, note the following:

   - The remote instance of SQL Server cannot be on a computer that is running as a domain controller.

   - The computer running SQL Server and the DPM server must be located in the same domain.

   - DPM Setup creates the DPMDBReaders$<DPM server name> and DPMDBAdministrators$<DPM server name> local groups on the remote instance of SQL Server. DPM administrators must be added to these groups to use the remote instance of SQL Server.
   - The remote instance of SQL Server must be running IIS 6.0 and SQL Server 2005 Standard or Enterprise Edition with SP2, including the SQL Server Database Engine and Reporting services components.

   We recommend you use the following settings on the remote instance of SQL Server:

   - Default failure audit setting.
   - Default Windows Authentication mode.
   - Assign a strong password to the **sa** account.
   - Enable password policy checking.
   - Install only the SQL Server Database Engine and Reporting Services components.
   - Run SQL Server by using the least-privileged user account.

10. On the **Installation Settings** page, the **Space requirements** section displays space availability on the specified destination drives. If you choose to change the installation folders, verify that the selected drives have enough space for the installation. Following are the minimum hardware requirements for the DPM server:

Component	**Minimum Requirement**
System drive	2650 MB **Note** This system drive disk space requirement is necessary if you chose to install the instance of SQL Server from the DPM download package. If you are using an existing instance of SQL Server, this disk space requirement is considerably less.
Program files drive	620 MB
Database files drive	900 MB

If you choose to use an existing instance of SQL Server instead of installing it from the DPM product DVD, the **SQL Server Settings** page appears.

- In the **Instance of SQL Server** box, type the name of the existing instance of SQL

Server that you want to use and the appropriate administrator credentials, and then click **Next**.

Note

If SQL Server Reporting Services is installed on the remote SQL Server, DPM Setup will use that Reporting Service. If SQL Server Reporting Services is not installed on the remote computer running SQL Server, you must install and configure the service on the remote computer running SQL Server before continuing with DPM Setup.

11. On the **Security Settings** page, specify and confirm a strong password for the restricted MICROSOFT$DPM$Acct and DPMR$<computer name> local user accounts, and then click **Next**.

    For security purposes, DPM runs SQL Server and the SQL Server Agent service under the MICROSOFT$DPM$Acct account, which DPM Setup creates during DPM installation. To securely generate reports, DPM creates the DPMR$<computer name> account.

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

    Note

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

12. On the **Microsoft Update Opt-In** page, specify if you want to sign up for the Microsoft Update service, and then click **Next**.

    You can change your Microsoft Update opt-in decision at any time after you install DPM 2007. To change your Microsoft Update opt-in decision, see the Microsoft Update Web site (http://go.microsoft.com/fwlink/?LinkId=74122).

13. On the **Customer Experience Improvement Program** page, specify if you want to enlist in the Customer Experience Improvement Program (CEIP), and then click **Next**.

14. On the **Summary of Settings** page, review the summary of installation settings. To install DPM using the specified settings, click **Install**. To change the settings, click **Back**.

    After the installation is complete, the **Installation** page displays the installation status.

15. Click **Close**, and then restart the computer to incorporate all of the changes made by DPM Setup.

Note

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

Manually Installing Prerequisite Software

If you want to use retail copies of one or more of the prerequisite products for your System Center Data Protection Manager (DPM) 2007 installation, or in the event that automatic installation of one or more of the DPM prerequisite software products fails, you can install the prerequisite software manually.

If you are installing a prerequisite product from the DPM product DVD, follow the instructions provided in this section. If you are installing a prerequisite product using a retail copy of the product, use the settings information provided in the instructions to configure the software properly for DPM.

You must install the following software in the order listed before installing DPM:

- Install Prerequisite Software
- Manually Install Required Windows Components
- Manually Install SQL Server 2005
- Manually Install SQL Server 2005 SP2

See Also

Hardware Requirements

Network Requirements

Security Requirements

Software Prerequisites

Install Prerequisite Software

Before installing the required Windows components and Microsoft SQL Server 2005, you must install Windows PowerShell 1.0 from http://go.microsoft.com/fwlink/?LinkId=87007.

Before you install protection agents on the computers you are going to protect, you must apply hotfix 940349. For more details, see Microsoft Knowledge Base article 940349, "Availability of a Volume Shadow Copy Service (VSS) update rollup package for Windows Server 2003 to resolve some VSS snapshot issues" (http://go.microsoft.com/fwlink/?LinkId=99034).

Note

After installing Knowledge Base article 940349 and then restarting the protected server, we recommend that you refresh the protection agents in DPM Administration Console. To refresh the agents, in the **Management** task area, click the **Agents** tab, select the computer, and then in the **Actions** pane, click **Refresh information**. If you do not refresh the protection agents, Error ID: 31008 may appear because DPM only refreshes the protection agents every 30 minutes.

See Also

Hardware Requirements

Network Requirements

Security Requirements

Software Prerequisites

Manually Install Required Windows Components

Before you install Microsoft SQL Server 2005, you must install the required Windows components.

This topic includes the procedures for installing Windows Server 2003 components and the Windows Server 2008 operating system (Pre-release version) components. The procedure for installing Windows components in Windows Server 2008 is very different from the procedures that you use in Windows Server 2003.

Installing the Required Components for Windows Server 2003

The following are the required Windows Server 2003 components:

- ASP.NET.
- Network COM+ access.
- Internet Information Services (IIS) 6.0 for Windows Server 2003. (IIS 6.0 is not installed on Windows Server 2003 by default.)

Note

If you do not install IIS before installing SQL Server 2005, SQL Server will not install SQL Server Reporting Services.

- Windows Deployment Services (WDS) on Windows Server 2003 Service Pack 2 (SP2) servers.

  - OR -

  Single Instance Storage (SIS) on Windows Storage Server R2.

To install required Windows Server 2003 components

1. In **Control Panel**, select **Add or Remove Programs**.
2. In the **Add or Remove Programs** dialog box, click **Add/Remove Windows Components**.
3. In the **Windows Components Wizard**, select **Application Server**, and then

click **Details**.

4. In the **Application Server** dialog box, select **ASP.NET**, select **Internet Information Services (IIS**), and then click **OK**.
5. If you are installing DPM on a Windows Server 2003 SP2 server, in the **Windows Components Wizard**, select **Windows Deployment Services**.

   - OR -

   If you are installing DPM on Windows Storage Server R2, select **Other Network File and Print Services**, click **Details**, click **Single Instance Storage**, and then click **OK**.
6. On the **Windows Components Wizard**, click **Next**.
7. When the installation is complete, click **Finish.**

Installing the Required Components for Windows Server 2008 (Pre-release version)

The following is the required Windows Server 2008 tools and work station components:

- PowerShell 1.0

  You must install Windows PowerShell 1.0 before installing IIS 7.0.
- IIS 7.0 for Windows Server 2008 operating system (Pre-release version). (IIS 7.0 is not installed on Windows Server 2008 by default.)

Note

If you do not install IIS before installing SQL Server 2005, SQL Server will not install SQL Server Reporting Services.

- Single Instance Storage (SIS)

To install Windows PowerShell 1.0

1. Click Start, point to **Administrative Tools**, and then click **Server Manager**.
2. Expand Server Manager to the **Features** node, and then select **Features**.
3. In the **Features** pane, click **Add Features.**
4. Select **Windows PowerShell**, and then click **Next**.
5. On the **Confirm Installation Selections** page, click **Install**.

In addition to the default components that are required for Windows Server 2008, DPM requires all IIS 7.0 components.

To install IIS 7.0 and the required services

1. Click Start, point to **Administrative Tools**, and then click **Server Manager**.
2. Expand Server Manager to the **Roles** node, and then select **Roles**.
3. In the **Roles** pane, click **Add Roles**.

4. In the **Add Roles Wizard**, on the **Before You Begin** page, click **Next**.
5. On the **Select Server Roles** page, select **Web Service (IIS)**.
6. In the **Add features required for Web Server (IIS)?** message box, click **Add Required Features**.

   Note

   Add the Windows Process Activation service (WAS) when prompted. WAS is the new process activation service that is a generalization of IIS features that work with non-HTTP transport protocols.

7. Click **Next**, and then click **Next** again.
8. On the **Select Role Services** page, select all of the role services.
9. Click **Next**, and then click **Install**.

To install SIS

1. From an administrator command prompt, type **start /wait ocsetup.exe SIS-Limited/quiet/norestart**.
2. After the installation is complete, you must restart the computer.

See Also

Hardware Requirements

Network Requirements

Security Requirements

Software Prerequisites

Manually Install SQL Server 2005

To install SQL Server 2005 Standard or Enterprise Editions, you can run Setup using the SQL Server 2005 Installation Wizard or you can install it from the command prompt. You can also add components to an instance of SQL Server 2005 or upgrade to SQL Server 2005 from a previous version of SQL Server.

We recommend a clean installation on the remote instance of SQL Server or when installing the dedicated instance of SQL Server for DPM, and that you use the following settings:

- Use the default failure audit setting.
- Use the default Windows Authentication mode.
- Assign a strong password to the **sa** account.
- Enable password policy checking.
- Install only the SQL Server Database Engine and Reporting Services components.

- Use the least-privileged user account on the computer running SQL Server.

To install SQL Server 2005

1. Insert the **Microsoft Data Protection Manager 2007** product DVD in the DVD drive.
2. In Windows Explorer, browse to **<DVD drive>:\SQLSVR2005\Servers**, and then run **setup.exe**.
3. On the **Microsoft SQL Server 2005 End User License Agreement** page, review the license agreement. If you accept the terms, click **I accept the licensing terms and conditions**, and then click **Next**.
4. On the **Installing Prerequisites** page, click **Install** to install the software that SQL Server requires, and then click **Next**. The **Microsoft SQL Server 2005 Setup Wizard** starts.
5. On the **Welcome to the Microsoft SQL Server Installation Wizard** page, click **Next**.
6. On the **System Configuration Check page**, verify that the configuration is successful, and then click **Next**.
7. On the **Registration Information** page, type your registration information, and then click **Next**.
8. On the **Components to Install** page, click **Advanced**.
9. On the **Feature Selection** page, select the following features:
   - **Database Services**.

     Expand the **Database Services** feature, and then select **Data Files**. Verify that **Shared Tools** is also selected.
   - **Reporting Services**.

     Select **Entire feature will be installed on local hard drive**.
   - **Client Components**.

     Expand the **Client Components** feature, and then select **Management Tools**.
10. Click **Next**.
11. On the **Instance Name** page, select **Named instance**, type **MS$DPM2007$**, and then click **Next**.

    You can use another instance name if you do not want to use the dedicated instance for DPM, or if you install SQL Server on a different computer.

    Note

    DPM supports pointing two DPM servers to two different instances of SQL Server on the same computer.
12. On the **Service Account** page, do the following:
    a. Select **Customize for each service account**.
    b. In the **Service** box, select **SQL Server**.
    c. Select **Use the built-in System account**, and then select a domain user account.

    d. In the **Service** box, select **SQL Server Agent**.
    e. Select **Use the built-in System account**, and then select a domain user account.
    f. In the **Service** box, select **Reporting Services**.
    g. Select **Use the built-in System account**, and then select **Network service**.
    h. In the **Service** box, select **SQL Browser**.
    i. Select **Use the built-in System account**, and then select a domain user account.

13. Click **Next**.
14. Follow the SQL Server wizard instructions on the remaining pages, and accept all default settings.
15. On the **Ready to Install** page, click **Install** to begin the installation.

After you have completed the installation, verify that SQL Server 2005 is running.

To verify that SQL Server 2005 is running

1. On the Start menu, point to **All Programs**, point to **Microsoft SQL Server 2005**, point to **Configuration Tools**, and then click **SQL Server Configuration Manager**.
2. In SQL Server Configuration Manager, verify that the **SQL Server (MS$DPM2007$)** service is running.

See Also

Hardware Requirements

Network Requirements

Security Requirements

Software Prerequisites

Manually Install SQL Server 2005 SP2

Microsoft SQL Server 2005 SP2 provides updates for SQL Server 2005 features.

To install SQL Server 2005 SP2

1. Insert the **Microsoft Data Protection Manager 2007** product DVD in the DVD drive.
2. In Windows Explorer, browse to:
    - 32-bit platform. **<DVD drive>:\SQLSVR2005SP2**, and then run **SQLServer2005SP2-KB921896-x86-ENU.exe**.
    - 64-bit platform. **<DVD drive:>\SQLSVR2005SP2**, and then run **SQLServer2005SP2-KB921896-x64-ENU.exe**.

    The **Microsoft SQL Server 2005 Service Pack 2 Setup Wizard** starts.

3. On the **Welcome** page, click **Next**.
4. On the **Microsoft SQL Server 2005 SP2 End User License Agreement** page, review the license agreement. If you accept the terms, click **I accept the licensing terms and conditions**, and then click **Next**.
5. Follow the SQL Server wizard instructions on the remaining pages, accept all default settings, and then on the **Ready to Install** page, click **Install** to begin the installation.

See Also

Hardware Requirements

Network Requirements

Security Requirements

Software Prerequisites

Repairing DPM 2007

This topic describes actions you need to take to repair System Center Data Protection Manager (DPM) 2007, including information about:

- What you should do before you reinstall DPM 2007
- What to do if you do not plan to reinstall DPM immediately
- What happens to protection jobs during the repair process
- The procedures you use to successfully repair DPM
- What to do after the installation is complete

In the unlikely event of corruption of the Microsoft Windows registry, system files, Internet Information Services (IIS), or the DPM binaries, you can repair DPM 2007 by reinstalling it. Reinstalling DPM 2007 involves uninstalling the application with an option to retain your data protection configuration and then re-running DPM Setup.

In most cases, you do not need to uninstall the DPM prerequisite software to reinstall DPM. However, if the Microsoft SQL Server 2005 binaries become corrupted, you might need to uninstall and reinstall SQL Server 2005 as well.

You do not need to uninstall the protection agents from the protected computers to reinstall DPM.

Important

> Before starting a reinstallation of DPM 2007, we strongly recommend that you archive the DPM database, Report database, and replicas to tape or other removable storage medium. For instructions, in the DPM Operations Guide, see Disaster Recovery (http://go.microsoft.com/fwlink/?LinkId=91860).

If you do not plan to reinstall DPM 2007 immediately after the uninstallation portion of the repair operation is complete:

1. Disable end-user recovery on the DPM server.
2. Run synchronization for each of the volumes in your protection groups.

These steps help ensure that users to whom you deny access to the server cannot access the replicas of those files on the DPM server.

Protection jobs cannot run successfully during a repair operation. Any jobs scheduled to run while a repair operation is in progress will not succeed. Any jobs that are in progress when the uninstallation portion of a repair operation begins are canceled. Upon completion of a repair operation, DPM automatically attempts to perform any canceled replica creation, synchronization, or consistency check jobs, but it does not attempt to perform canceled recovery point creation jobs.

You must perform the following procedures to successfully repair DPM:

1. Back up the DPM database.
2. Uninstall DPM.
3. Delete the DPM database.
4. Reinstall DPM.
5. Restore the DPM database.

To back up the DPM database

1. From the command prompt, run DPMBackup.exe -db, located at **<drive letter>:\Program Files\Microsoft Data Protection Manager\DPM\bin**.
2. In the console tree of the backup program, browse to **\Program Files\Microsoft Data Protection Manager\DPM\Volumes\ShadowCopy\Database Backups**. The file name of the DPM database backup is **DPMDB.bak**.
3. Select the media to which you want to back up the database.
4. Start the backup.

To uninstall DPM

1. In Control Panel, click **Add or Remove Programs**, and then click **Change or Remove Programs**.
2. Under **Currently installed programs**, select **Microsoft System Center Data Protection Manager 2007** and then click **Change/Remove**.
3. On the **Uninstallation Options** page, select the **Retain data** option, and then click **Next**.
4. On the **Summary of Options** page, click **Uninstall**.
5. When uninstallation is complete, click **Close**.

To delete the DPM database

1. On the **Start** menu, point to **Microsoft SQL Server 2005**, and then click **SQL Server Management Studio**.

2. Select the <*computer name*>\MS$DPM2007$ database, and then click **Connect**.
3. Expand **Databases**, right-click the **DPMDB** database, and then click **Delete**.
4. Click **Yes** to confirm the deletion.

To install DPM

- For information about installing DPM, see Installing DPM 2007.

To restore the DPM database using the DpmSync tool

1. From the command prompt, type **DpmSync -sync**.
2. After the new installation is complete and the database is restored, in DPM Administrator Console, in the **Monitoring** task area, check for protection jobs that failed during the repair operation. Manually restart any failed jobs.
3. After you restart the failed jobs you must perform a consistency check for all data sources. For instructions on how to perform a manual consistency check, in DPM 2007 Help, see "How to synchronize a replica".

Uninstalling DPM 2007

When you uninstall System Center Data Protection Manager (DPM) 2007, you can choose whether to remove or retain your existing recovery points and replicas. To continue accessing recovery points on the DPM server after you uninstall DPM, you must choose to retain your data protection configuration when you uninstall DPM.

Important

If you plan to retain your existing data protection configuration after uninstalling DPM, disable end-user recovery on the DPM server and run synchronization jobs for each data source in your protection groups before you start the uninstallation. These steps help ensure that users to whom you deny access to files on the server cannot access the replicas of those files on the DPM server.

Uninstall DPM 2007

Setup uninstalls only the DPM application. Setup does not remove the prerequisite software, protection agents, user settings, and Dr. Watson for Windows Server 2008 operating system. You must uninstall the DPM application, the prerequisite software, and the protection agents in the following order:

Note

After you uninstall the DPM system requirements, you must restart the computer to complete the uninstall.

Step 1: Uninstalling the DPM application

To uninstall DPM

1. In Control Panel, click **Add or Remove Programs**, and then click **Change or Remove Programs**.
2. Under **Currently installed programs**, select **Microsoft System Center Data Protection Manager 2007** and then click **Change/Remove**.

   The DPM Setup Wizard starts in uninstallation mode.
3. On the **Uninstallation Options** page, select either **Remove data** or **Retain data**, and then click **Next**.
4. On the **Summary of Options** page, click **Uninstall**.
5. When uninstallation is complete, click **Close**.

Step 2: Uninstalling the DPM prerequisite software

Following is the prerequisite software that you need to uninstall:

- **SQL Server 2005** (MS$DPM2007$) and SQL Server 2005 Reporting Services.
- **Internet Information Services (IIS) 6.0** for Windows Server 2003.

  -Or-
- **IIS 7.0** for Windows Server 2008 operating system (Pre-release version).

To uninstall SQL Server 2005 and IIS 6.0 on Windows Server 2003

1. In Control Panel, click **Add or Remove Programs**, and then click **Change or Remove Programs**.
2. Under **Currently installed programs**, select the prerequisite software, and then click **Remove**.
3. Click **Yes**, to confirm the deletion.

- **PowerShell 1.0**

To uninstall PowerShell 1.0 on Windows Server 2003

1. In Control Panel, click **Add or Remove Programs**, and then click **Change or Remove Programs**.
2. In the **Add or Remove Programs** screen, check **Show updates**.
3. Select **Hotfix for Windows Server 2003 (KB926139)**.

4. Under **Currently installed programs**, select the prerequisite software, and then click **Remove**.
5. Click **Yes**, to confirm the deletion.

To uninstall PowerShell 1.0 on Windows Server 2008

1. Click Start, point to **Administrative Tools**, and then click **Server Manager**.
2. Expand Server Manager to the **Features** node, and then select **Features**.
3. In the **Features** pane, click **Remove Features**.
4. Clear the **Windows PowerShell** checkbox and complete the uninstall.

- **Single Instance Storage (SIS)**

To uninstall SIS on Windows Server 2008

1. From an administrator command prompt, type **start /w ocsetup.exe SIS-Limited/uninstall/quiet/norestart**.
2. After the uninstall is complete, you must restart the computer.

Step 3: Uninstalling the protection agents

If you want to use DPM Administrator Console to uninstall protection agents deployed on protected servers, you must do so before you start uninstalling DPM. Alternatively, you can use **Add or Remove Programs** to uninstall protection agents from the servers locally after you complete uninstalling DPM.

Step 4: Uninstalling the User settings

To remove user settings, after you complete uninstalling DPM, delete the folder named:

<drive letter>:\Documents and Settings\<user name>\Application Data\Microsoft\Microsoft System Data Protection Manager 2007

Step 5: Uninstalling Dr. Watson

To uninstall Dr. Watson on Windows Server 2008, from the command prompt type one of the following commands:

- 32-bit operating system: **msiexec /x {95120000-00B9-0409-0000-0000000FF1CE}**
- 64-bit operating system: **msiexec /x {95120000-00B9-0409-1000-0000000FF1CE}**

Configuring DPM 2007

After you install System Center Data Protection Manager (DPM) 2007, you must perform a series of required configuration tasks before you can start protecting your data. You can also configure optional DPM features at this time, or you can wait and configure optional features at any time after you deploy DPM. The topics in this section provide instructions for opening DPM 2007 for the first time, and then performing each of the required and optional configuration tasks.

In This Section

- Getting Started with Configuring DPM
- Required Configuration Tasks
- Optional Configuration Tasks

Getting Started with Configuring DPM

Use the procedure in this topic to open DPM Administrator Console so that you can configure System Center Data Protection Manager (DPM) 2007.

For an introduction to DPM Administrator Console, see DPM Administrator Console in DPM 2007.

To open DPM Administrator Console

1. Log on to the DPM server under a domain user account that is a member of the local administrators group.
2. On the **Start** menu, point to **All Programs**, point to **Microsoft System Center Data Protection Manager 2007**, and then click **Microsoft System Center Data Protection Manager 2007**.

   –Or–

   If it is available, double-click the **Microsoft System Center Data Protection Manager 2007** icon on the desktop.

See Also

DPM Administrator Console in DPM 2007

Required Configuration Tasks

Before you can start protecting data by using System Center Data Protection Manager (DPM) 2007, you must verify that each computer that DPM is going to protect meets the protected computer software requirements. For information about the DPM 2007 software requirements, see Software Prerequisites (http://go.microsoft.com/fwlink/?LinkId=100242).

To successfully protect your data using DPM 2007, you must add one or more disks to the storage pool.

Note

Adding a disk to the storage pool is not a requirement if you are going to use custom volumes to protect your data sources, or if you are only going to use disk-to-tape protection.

- Configure tape libraries and stand-alone tape drives if you want to protect data on tape.
- Install a protection agent on each computer that you want to protect.
- Start and configure the Windows SharePoint Services VSS Writer service (WSS Writer service), and provide farm administration credentials for the protection agent.

  Note

  Perform this task only if you are protecting server farms on servers running Windows SharePoint Services 3.0 or Microsoft Office SharePoint Server 2007.
- Create one or more protection groups.

In This Section

- Adding Disks to the Storage Pool
- Configuring Tape Libraries
- Installing and Configuring Protection Agents
- Starting and Configuring the WSS Writer Service
- Creating Protection Groups

Adding Disks to the Storage Pool

The *storage pool* is a set of disks on which the System Center Data Protection Manager (DPM) 2007 server stores replicas and recovery points for protected data. Before you can start protecting data, you must add at least one disk to the storage pool. After configuration, you can add more disks to the storage pool.

Note

DPM does not support USB/1394 disks.

For more information and guidelines for choosing disk types and calculating capacity requirements for your storage pool, in "Planning a DPM 2007 Deployment", see Planning the Storage Pool (http://go.microsoft.com/fwlink/?LinkId=91965).

To help you estimate your storage space needs, download the DPM storage calculator (http://go.microsoft.com/fwlink/?LinkId=104370).

DPM 2007 requires a disk that is dedicated to the storage pool and a disk that is dedicated to the following:

- System files
- DPM installation files

- DPM prerequisite software
- DPM database files

Note

Adding a disk to the storage pool is not a requirement if you are going to use custom volumes to protect your data sources, or if you are only going to use disk-to-tape protection.

You can install DPM on the same volume that the operating system is installed on or on a different volume that does not include the operating system. However, a disk on which you install DPM cannot be added to the storage pool.

Caution

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 may have free space, DPM can use only space 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.

To add disks to the storage pool

1. In DPM Administrator Console, on the navigation bar, click **Management**, and then click the **Disks** tab.
2. In the **Actions** pane, click **Add**.

   The **Add Disks to Storage Pool** dialog box appears. The **Available disks** section lists the disks that you can add to the storage pool.
3. Select one or more disks, click **Add**, and then click **OK**.

See Also

Troubleshooting Protection Agent Installation Issues

Configuring Tape Libraries

You can add tape libraries and stand-alone tape drives to System Center Data Protection Manager (DPM) 2007 to enable short-term and long-term data protection on tape. The tape libraries and stand-alone tape drives must be physically attached to the DPM server.

After you attach a new tape library or stand-alone tape drive to your DPM server, you must perform a **Rescan** operation before the DPM server can identify them. When you perform a **Rescan** operation, DPM examines the tape libraries or stand-alone tape drives that are attached to the DPM server and updates the information that is displayed on the **Libraries** tab in DPM Administrator Console. The **Libraries** tab displays each stand-alone tape drive, and each tape library and its drives.

You use the **Rescan** operation on the **Libraries** tab to check for and refresh the state of all new tape libraries and stand-alone tape drives when you make changes to your hardware.

Note

> If the stand-alone tape drives listed on the **Libraries** tab in DPM Administrator Console do not match the physical state of your stand-alone tape drives, in the DPM 2007 Operations Guide see Managing Tape Libraries (http://go.microsoft.com/fwlink/?LinkId=91964). For example, if drives from a tape library are listed as stand-alone tape drives, or if a stand-alone tape drive displays incorrectly as a drive in a tape library, you need to remap the tape drive information.

To configure tape libraries

1. In DPM Administrator Console, on the navigation bar click **Management**, and then click the **Libraries** tab.
2. In the **Actions** pane, click **Rescan**.

   The **Rescan** operation might take several minutes to complete. DPM will add any library jobs to the queue that began during the **Rescan** operation. If a library job is already in progress when the **Rescan** operation begins, the **Rescan** operation will fail.

See Also

Managing Tape Libraries

Installing and Configuring Protection Agents

A *protection agent* is software installed on a computer that tracks changes to protected data and transfers the changes from the protected computer to the System Center Data Protection Manager (DPM) 2007 server. The protection agent also identifies data on a computer that DPM can protect and recover.

Before you can start protecting data, you must install a protection agent on each of the computers that contains data that you want to protect. After the protection agent is installed on a computer, the computer is listed as an unprotected computer in the **Management** task area of DPM Administrator Console. The data sources on the computer are not protected until you add them to a protection group. Each computer that you want to protect must meet the protected computer prerequisites. For more information, see Protected Computer Prerequisites (http://go.microsoft.com/fwlink/?LinkId=100473).

DPM supports protecting computers across domains within a forest; however, you must establish a two-way trust across the domains. If there is not a two-way trust across domains, you must have a separate DPM server for each domain. DPM 2007 does not support protection across forests.

If a firewall is enabled on the DPM server, you must configure the firewall on the DPM server. To configure a firewall on a DPM server, you must open port 135 to TCP traffic, and you must enable the DPM service (Msdpm.exe) and the protection agent (Dpmra.exe) to communicate through the firewall.

In This Section

- Configuring Windows Firewall on the DPM Server
- Installing Protection Agents
- Installing Protection Agents behind a Firewall
- Installing Protection Agents Using a Server Image
- Installing Protection Agents Manually

Configuring Windows Firewall on the DPM Server

The following procedures apply to a Windows Firewall configuration. If Windows Firewall is enabled on the DPM server when you install DPM, DPM Setup configures the firewall automatically. For more information about configuring other firewall software, consult the firewall documentation.

To configure Windows Firewall on a DPM server

1. In Control Panel, click **Windows Firewall**.
2. On the **General** tab, verify that Windows Firewall is turned on, and then verify that the **Don’t allow exceptions** check box is clear.
3. On the **Exceptions** tab, do the following:
    a. Click **Add Program**, click **Browse**, and then navigate to **<drive letter>:\Program Files\Microsoft DPM\DPM\bin**.
    b. Select **Msdpm.exe**, click **Open**, and then click **OK**.
    c. On the **Exceptions** tab, click **Add Program**, click **Browse**, and navigate to **<drive letter>:\Program Files\Microsoft DPM\DPM\bin**.
    d. Select **Dpmra.exe**, click **Open**, and then click **OK**.
4. Click **Add Port**, type any name you want for the port in the **Name** box, type **135** in the **Port number** box, verify that TCP is specified as the protocol, and then click **OK** to close the **Add a Port** dialog box.
5. Click **OK** to close the **Windows Firewall** dialog box.

Note

You must open port 5718 to enable communication with the agent coordinator and port 5719 to enable communication with the protection agent.

Installing Protection Agents

You use the Protection Agent Installation Wizard to install protection agents on servers that are members of the same domain and servers across trusted domains.

If you need to install protection agents on servers that reside behind a firewall, see Installing Protection Agents behind a Firewall in this topic.

Before you install protection agents on the computers you are going to protect, you must apply hotfix 940349. For more information about this hotfix, see Microsoft Knowledge Base article 940349, "Availability of a Volume Shadow Copy Service (VSS) update rollup package for Windows Server 2003 to resolve some VSS snapshot issues" (http://go.microsoft.com/fwlink/?LinkId=99034).

Note

After installing Knowledge Base article 940349 and then restarting the DPM server and/or the protected server, we recommend that you refresh the protection agents in DPM Administration Console. To refresh the agents, in the **Management** task area, click the **Agents** tab, select the computer, and then in the **Actions** pane, click **Refresh information**. If you do not refresh the protection agents, Error ID: 31008 may appear because DPM only refreshes the protection agents every 30 minutes.

If you are installing a protection agent and encounter network-related or permissions-related issues because of domain policies, we recommend that you install the protection agent manually. For information about manually installing a protection agent, see Installing Protection Agents Manually.

For information about installing a protection agent by using a server image on the computer without specifying the DPM server, see Installing Protection Agents Using a Server Image.

To install a protection agent on a server

1. In DPM Administrator Console, on the navigation bar, click **Management**, and then click the **Agents** tab.
2. In the **Actions** pane, click **Install**.

   The Protection Agent Installation Wizard starts and displays a list of available computers in the DPM server domain. If this is the first time you have used the wizard, DPM queries Active Directory to get a list of potential computers. After the first installation, DPM displays the list of computers in its database, which is updated once each day by the auto-discovery process.
3. On the **Select Computers** page, select one or more computers (50 maximum) from

the **Computer name** list, click **Add**, and then click **Next**.

If you know the name of a specific computer on which you want to install the protection agent, you can quickly find and select the computer by typing the name of the computer in the **Computer name** box, and then clicking **Add**. DPM will query Active Directory for the computer, and then add it to the **Selected computers** list. If you do not know the name of the computer, browse the list to find the computer.

To find a computer across a trusted domain, you must type the fully qualified domain name of the computer you want to protect (for example, **Computer1.Domain1.corp.microsoft.com**, where Computer*1* is the name of the target computer that you want to protect, and *Domain1.corp.microsoft.com* is the domain to which the target computer belongs.

> **Note**
>
> The **Advanced** button on the **Select Computers** page is enabled only when there is more than one version of a protection agent available for installation on the computers. If it is enabled, you can use this option to install a previous version of the protection agent that existed before you updated to the most recent version.

4. On the **Enter Credentials** page, type the user name and password for a domain account that is a member of the local administrators group on all selected servers.
5. In the **Domain** box, accept or type the domain name of the user account that you are using to install the protection agent on the target computer. This account may belong to the current or trusted domain.

   If you are installing a protection agent on a computer across a trusted domain, you enter your current domain user credentials. You can be a member of any trusted domain, and you must be an administrator on the target server that you want to protect.

   If you selected a node in a server cluster, DPM detects the additional nodes in the cluster and displays the **Select Cluster Nodes** page.

   - On the **Select Cluster Nodes** page, in the **Cluster node selection** section, select the option that you want DPM to use for selecting the remaining nodes in the cluster, and then click **Next**.
6. On the **Choose Restart Method** page, select the method you will use to restart the computers after the protection agent is installed. The computer must be restarted before you can start protecting data. This restart is necessary to load the volume filter that DPM uses to track and transfer block level changes between DPM and the computers it protects.

   If you select **No. I will restart the selected computers later**, after the restart is complete and if the protection agent installation status is not refreshed on the unprotected server, in the **Management** task area on the **Agents** tab, click **Refresh Information**.

   > **Note**
   >
   > You do not need to restart the computer if you are installing protection agents on

a DPM server.

If any of the servers you selected are clustered servers, an additional **Choose Restart Method** page appears that allows you to select the method you will use to restart the clustered servers.

You must install the protection agent on all nodes of the server cluster to successfully protect the clustered data. The servers must be restarted before you can start protecting data. Because of the time required to start services, it might take a few minutes after a restart is complete before DPM can contact the server.

Note

DPM will not restart a server that belongs to Microsoft Cluster Server (MSCS). You must manually restart a server in an MSCS cluster.

7. On the **Summary** page, click **Install** to begin the installation.
8. On the **Installation** page, the results appear on the **Task** tab to indicate whether the installation is successful. You can click **Close** before the wizard is finished performing the tasks, and then monitor the installation progress in DPM Administrator Console on the **Agents** tab in the **Management** task area.

If the installation is unsuccessful, you can view the alerts in the **Monitoring** task area on the **Alerts** tab.

Note

After you install a protection agent on a backend server to protect a Windows SharePoint Services farm, the server will not appear as protected in the **Management** task area on the **Agents** tab. However, DPM protects the back end server internally if the Windows SharePoint Services farm has data on the server.

Installing Protection Agents behind a Firewall

If you want to install protection agents on computers that reside behind a firewall, DPM provides an executable file named **DPM2007\Agents\DPMAgentInstaller.exe** that performs the following:

- Installs the protection agent prerequisites and the DPM protection agent.
- Configures the target computer to receive commands from the specified DPM server name.
- Configures the firewall to allow communication to come in.

Note

If you are using a language other than English, you can select the localized agent installer from **DPM2007\Agents\<language>\DPMAgentInstaller.exe**.

To install a protection agent on a server behind a firewall

1. On the computer on which you want to install the protection agent, from the Windows command prompt, from the DPM2007\Agents folder, type **DpmAgentInstaller.exe <DPM**

server name>.

Note

You can also run the executable using Microsoft Systems Management Server (SMS).

2. On the DPM server, from the DPM Management Shell prompt, type **Attach-ProductionServer.ps1 <DPM server name> <production server name> <user name> <password> <domain>**.

   The password parameter is not required and we recommend that you do not provide it. DPM will prompt you for a password, which will not appear on the screen. However, you can provide the password if you want to use the script to install a protection agent on a large number of computers.

   Note

   If you are attaching the protected computer on a different domain, you must specify the fully qualified domain name. For example, **Computer1.Domain1.corp.microsoft.com**, where Computer*1* is the name of the protected computer, and *Domain1.corp.microsoft.com* is the domain to which you are attaching the computer.

The required configurations to protect the server are created. DPM Administrator Console will now display the protected server. To display the correct protection agent status, in the **Monitoring** task area, on the **Jobs** tab, click **Refresh Job**.

Installing Protection Agents Using a Server Image

You can install a protection agent using a server image without specifying the DPM server using **DPMAgentInstaller.exe**. Once the image is applied to the computer and brought online, you run the **SetDpmServer.exe <DPM server name>** tool to complete the configurations and the firewall openings.

To install a protection agent using a server image

1. On the computer on which you want to install the protection agent, from the Windows command prompt, type **DpmAgentInstaller.exe**.
2. Apply the server image to a physical computer, and then bring it online.
3. Join the computer to a domain, and then log on as a domain user with the appropriate administrator credentials.
4. From the Windows command prompt, in the <drive letter>:\Program Files\Microsoft Data Protection Manager\bin directory, type **SetDpmServer.exe <dpm server name>** to

complete the configurations and firewall openings.

Specify the fully qualified domain name (FQDN) for the DPM server. For the current domain or for unique names across domains, specify only the computer name.

Note

You must run SetDpmServer.exe from <drive letter>:\Program Files\Microsoft Data Protection Manager\bin. If you run the executable from any other location, the operation will fail.

5. On the DPM server, from the DPM Management Shell prompt, type **Attach-ProductionServer.ps1 <DPM server name> <production server name> <user name> <password> <domain>**.

   The password parameter is not required and we recommend that you do not provide it. DPM will prompt you for a password, which will not appear on the screen. However, you can provide the password if you want to use the script to install a protection agent on a large number of computers.

   Note

   If you are attaching the production computer on a different domain, you must specify the fully qualified domain name of the production computer.

Installing Protection Agents Manually

You can install protection agents manually. To manually install a protection agent, use the command line options in the following procedure.

You can also install a protection agent independently using Microsoft Systems Management Server (SMS). To create an SMS package for the DPM protection agent, you must provide the following to the SMS administrator:

- A share to the **DpmAgentInstaller.exe** and **DpmAgentInstaller_AMD64.exe** packages.
- A list of servers on which you are installing the protection agents.
- The name of the DPM server.

To silently install the protection agent, from the command prompt, type **DpmAgentInstaller.exe /q <DPM server name>**.

To install a protection agent manually

1. On the computer on which you want to install the protection agent, from the command prompt, type **DpmAgentInstaller.exe <DPM server name>**.

   You can perform a non-interactive installation by specifying a **/q** parameter after the DpmAgentInstaller.exe command. For example, type **DpmAgentInstaller.exe /q <DPM server name>**.

2. To configure the protection agent for the appropriate DPM server and firewall settings, type **<drive letter>:\Program Files\Microsoft Data Protection Manager\bin SetDpmServer.exe**.

   This step is not required if you specified the DPM server in step 1.

3. On the DPM server, from the DPM Management Shell prompt, type **Attach-ProductionServer.ps1 <DPM server name> <production server name> <user name> <password> <domain>**.

   The password parameter is not required and we recommend that you do not provide it. DPM will prompt you for a password, which will not appear on the screen. However, you can provide the password if you want to use the script to install a protection agent on a large number of servers.

Note

> If you are attaching the protected computer on a different domain, you must specify the fully qualified domain name. For example, **Computer1.Domain1.corp.microsoft.com**, where Computer*1* is the name of the protected computer, and *Domain1.corp.microsoft.com* is the domain to which you are attaching the computer.

The required configurations to protect the production computer are created. DPM Administrator Console will now display the production computer.

Starting and Configuring the WSS Writer Service

Before you can start protecting server farms on servers running Windows SharePoint Services 3.0 or Microsoft Office SharePoint Server 2007, you must start and configure the Windows SharePoint Services VSS Writer service (WSS Writer service).

After you install the protection agent on the Windows SharePoint Services Web Front End (WFE) server, you must provide the protection agent with the credentials for the Windows SharePoint Services farm.

You perform the following procedure for a single WFE server. If your Windows SharePoint Services farm has multiple WFE servers, you must select only one WFE server when you configure protection in the Create New Protection Group Wizard.

To start and configure the WSS Writer service

1. On the WFE server, at the command prompt, change the directory to <DPM installation location>\bin\.
2. Type **ConfigureSharepoint.exe**.

3. When prompted, enter 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 WFE server.

   Note

   You must rerun **ConfigureSharepoint.exe** whenever the Windows SharePoint Services farm administrator password changes

Creating Protection Groups

A *protection group* is a collection of data sources that share the same protection configuration. *Data sources* within a protection group are referred to as protection group members or simply members.

The following table shows the data sources that System Center Data Protection Manager (DPM) 2007 protects and the level of data that you can recover by using DPM.

Product	Protectable Data	Recoverable Data
• Microsoft Exchange Server 2003 with Service Pack 2 (SP2) • Exchange Server 2007	• Storage group	• Storage group • Database • Mailbox
• Microsoft SQL Server 2000 with Service Pack 4 (SP4) • SQL Server 2005 with Service Pack 1 (SP1) or later	• Database	• Database
• Microsoft Office SharePoint Server 2007 • Microsoft Windows SharePoint Services 3.0	• Farm	• Farm • Database • Site • File or list
• Windows Server 2003 with SP1 • Windows Storage Server 2003 with SP1	• Volume • Share • Folder	• Volume • Share • Folder • File data
• Microsoft Virtual Server 2005 R2 SP1	• Virtual server host configuration • Virtual machines • Data for applications running in virtual machines	• Virtual server host configuration • Virtual machines • Data for applications running in virtual machines
• Workstations running Windows XP Professional SP2 • Windows Vista operating systems, except the Windows Vista Home Premium operating system (the computer running Windows Vista must be a member of a domain) **Note** DPM does not support file protection on portable computers running	• Volume • Share • Folder • File data	• Volume • Share • Folder • File data

Product	Protectable Data	Recoverable Data
Windows XP Professional SP2 and Windows Vista operating systems.		

Before you can start protecting data, you must create at least one protection group. For guidelines about protection groups, in Planning a DPM 2007 Deployment, see Planning Protection Groups (http://go.microsoft.com/fwlink/?LinkId=91849).

The Create New Protection Group Wizard guides you through the process of creating a protection group. Protection group creation involves making a series of decisions about how you want to configure the group.

Throughout the protection group creation process, the wizard provides default options that you can override if you choose.

In This Section

- Starting the New Protection Group Wizard
- Selecting Members for the Protection Group
- Specifying Exchange Protection Options
- Selecting a Name and Protection Method for the Protection Group
- Specifying Your Short-term Protection Goals
- Specifying Short-term Tape-based Recovery Goals
- Allocating Space for the Protection Group
- Specifying Your Long-term Protection Goals
- Selecting Library and Tape Details
- Choosing a Replica Creation Method
- Optimizing Performance
- Creating the Protection Group

Starting the New Protection Group Wizard

You start the Create New Protection Group Wizard to help guide you through the process of creating a protection group. To start the Create New Protection Group Wizard, you must open DPM Administrator Console.

To use DPM Administrator Console, you must be logged on to a DPM server with an account that has administrative privileges on that server.

Note

DPM supports multiple-user access to DPM Administrator Console using Remote Terminal server sessions.

To open DPM Administrator Console locally

- On the **Start** menu, point to **All Programs**, point to **Microsoft System Center Data Protection Manager 2007**, and then click **Microsoft System Center Data Protection Manager 2007**.

  - OR -

- Double-click the **Microsoft System Center Data Protection Manager 2007** icon on the desktop.

To start the Create New Protection Group Wizard

1. In DPM Administrator Console, click **Protection** on the navigation bar.
2. In the **Actions** pane, click **Create protection group**.

   The Create New Protection Group Wizard appears.
3. Review the **Welcome** page, and then click **Next**.

   Note

   If you do not want the wizard to display the **Welcome** page when you create protection groups in the future, select **Skip this page next time**.

Selecting Members for the Protection Group

You use the **Select Group Members** page to select the data sources you want to protect.

The computers that contain the members that DPM will protect must meet the protected computer requirements. For information about the protected computer software prerequisites, see Protected Computer Prerequisites (http://go.microsoft.com/fwlink/?LinkId=91851).

DPM does not support protection of some types of files and displays a warning of unsupported data in these cases. For more information about how to list the file types that DPM does not support, see "How to display warnings for unsupported data" in DPM 2007 Help.

DPM does not protect reparse points found in file systems or in application paths. If you select volumes, folders or applications in this protection group, DPM will protect all data except the reparse points. For more information about data types that are not protected, in "Planning a DPM 2007 Deployment", see Planning Protection Groups (http://go.microsoft.com/fwlink/?LinkId=91849).

▶ To select the data to protect

1. On the **Select Group Members** page, verify that all computers that store data you want to protect are displayed in the **Available members** box.
2. In the **Available members** box, expand the server nodes to display the available data sources on each server.

   Note

   If you have just installed the protection agent, you might experience a delay of up to several minutes before you can expand the node for the server and display its available data sources.
3. Place a check mark in the box next to each data source that you want to include in the protection group. As you select data sources, your selections appear in the **Selected members** box.

   For each for the data sources you want in the protection group, note the following:

   - Data sources that are members of other protection groups and unprotected data sources that reside on a volume already protected by another protection group are displayed but cannot be selected.
   - For file server data, you cannot include data sources from the same file server volume in different protection groups.
   - If a system volume contains user data that you want to protect, we recommend that you protect the relevant folders or shares individually rather than protecting the whole system volume.
   - You cannot include SQL Server 2005 database snapshots. Database snapshots appear as regular databases that you can select; however, DPM does not support protecting database snapshots for recovery. You can view database snapshots in the Microsoft SQL Server Management Studio in the Database Snapshots folder.
   - You cannot protect Windows SharePoint Services databases as a SQL Server data source. You must include the databases as part of the Windows SharePoint Services protection.
   - To protect clustered resources, expand the resource group name to select a clustered resource for protection.
   - If you have only a single stand-alone tape, use a single protection group to minimize the effort to change tapes. Multiple protection groups require a separate tape for each protection group.
   - To view a list of excluded folders, click the **View** link next to **Excluded folders**. To exclude a folder, expand the directory structure, and then clear the check box of the folder you want to exclude.
   - To exclude file types, click the **Exclude File** link, and in the **Exclude File Types** dialog box, type the file types you want to exclude, and then click **OK**.
4. After you have selected the members for the protection group, click **Next**.

Specifying Exchange Protection Options

If you selected an Exchange Server data source to protect, the **Specify Exchange Protection Options** page appears. You use this page to specify whether you want to check the integrity of the Exchange Server databases and to select the cluster node that you want to protect.

To specify Exchange protection options

1. On the **Specify Exchange Protection Options** page, select the **Run Eseutil to check data integrity** check box to check the integrity of the Exchange Server databases.

   The Exchange Server Database Utilities (Eseutil.exe) must be installed on the protected server for tape-based protection. For disk-based protection, you must also install Eseutil.exe on the DPM server. For more information about Eseutil.exe, see Eseutil (http://go.microsoft.com/fwlink/?LinkId=83451).
2. Select the type of node you want to protect for Cluster Continuous Replication (CCR) Exchange Server:
   - **Protect active node.** Select this option to select the active node as the node that DPM will protect.
   - **Protect passive node**. Select this option to select the active node as the node that DPM will protect.
   - **Protect only the specified node**. Select this option to specify the node that you want DPM to protect, and then select the protection node from the drop-down list.
3. Click **Next**.

Selecting a Name and Protection Method for the Protection Group

After you select the data you want to protect, you select your protection method. You can select short-term protection by using either disk or tape, or you can select long-term protection using only tape.

To select a name and protection method

1. On the **Select Data Protection Method** page, in the **Protection group name** box, accept the default name or type a new name for the protection group.

   Note

You can use special characters such as # ? @ \ $ () {} [] in your protection group name. However, you cannot use the following five special characters: & < > ‘ “

2. In the **Protection policy** section, select your protection method:
    - **I want short-term protection using**. Select this check box for short-term protection and then select the media you want to use from the drop-down list.

        Note

        If you do not have a tape library attached to the DPM server, only **Disk** is available for short-term protection.
    - **I want long-term protection using tape**. Select this check box for long-term protection.

    If you are using tape for both short-term and long-term protection, DPM creates copies of the latest short-term tape full backup to generate your long-term tape backup. Therefore, we recommend that you schedule your short-term protection full backup to run a day prior to your long-term protection. This scheduling enables your long-term tape backup to leverage the short-term tape backup that DPM created the day before. If you schedule the long-term tape backup to run prior to the short-term tape backup, the long-term backup will not take advantage of the latest short-term full backup.
3. Click **Next**.

Specifying Your Short-term Protection Goals

DPM generates a protection plan using your short-term recovery goals. You define your short-term recovery goals by selecting a retention range for your data, specifying how frequently you want the data synchronized, and scheduling the creation of your selected recovery points.
A *recovery point* is a snapshot or point-in-time copy of the data sources that are protected by your DPM server.

Retention range is the duration of time for which the data should be available for recovery. DPM retains recovery points for the duration specified in the retention range. Any day that the replica is not consistent does not count toward the retention range. When DPM protection is stopped temporarily because the replica is inconsistent, DPM does not delete expired recovery points until protection resumes.

To specify short-term protection goals

1. On the **Specify Short-Term Protection Policy** page, in the **Retention range** box, select the duration of time that you want the data to be available for recovery.

    You can select a retention range between 1 and 64 days for short-term disk-based protection.

2. In the **Synchronization frequency** section, do one of the following:

   - Select **Every**, and then select the frequency at which you want to synchronize the replica on your DPM server with the changes on your protected server. For application data protection, the synchronization frequency also determines the recovery point schedule. You can select a synchronization frequency interval of anywhere from 15 minutes to 24 hours.

     The default behavior is every 15 minutes, which means that the DPM server will never be more than 15 minutes behind the computer it is protecting. The average Recovery Point Objective (RPO) is 15 minutes from any event that critically impacts the computer or disk.

   - Select **Just before a recovery point** to synchronize the data just before a scheduled recovery point.

     When you select this option, recovery points for all protection group members are created according to the schedule you configure. The network traffic is potentially greater at the time of synchronization when you select this option.

     For more information about synchronization, in the "DPM 2007 Operations Guide", see Managing Performance (http://go.microsoft.com/fwlink/?LinkId=91859).

3. To specify the recovery points:

   - **Recovery points for files**. Click **Modify** to change the recovery point schedule for file data. Recovery points for files are created according to the schedule you configure.

   - **Application recovery points**. Click to create recovery points for application data after each synchronization. For data protection of applications that do not support incremental backups, such as SQL Server databases using the simple recovery model, the express full backup schedule determines the recovery point schedule

   - **Express full backup**. Click **Modify** to change the express full backup schedule. To enable faster recovery time, DPM regularly performs an express full backup, which is a type of synchronization that updates the replica to include the changed blocks.

     > **Note**
     >
     > Performing frequent express full backups may impact performance on the protected server. For more information about express full backups, in the DPM 2007 Operations Guide, see Managing Performance (http://go.microsoft.com/fwlink/?LinkId=91859).

     DPM can store a maximum of 64 recovery points for each file member of a protection group. For application data sources, DPM can store up to 448 express full backups and up to 96 incremental backups for each express full backup. To support end-user recovery, the recovery points for files are limited to 64 by Volume Shadow Copy Service (VSS).

4. On the **Modify Recovery Points** screen, specify the times of the day and the days of the week that you want to create a recovery point, and then click **OK**.

5. On the **Specify Short-term Objectives** page, click **Next**.

Specifying Short-term Tape-based Recovery Goals

If you chose to use short-term protection using tape, you need to specify your short-term tape-based recovery goals. Your recovery goals are defined by the configuration of retention range, synchronization frequency, and recovery point schedule. DPM provides default settings for the recovery goals; however, you can modify each or all of the settings.

To specify your short-term tape-based recovery goals

1. In the **Retention range** box, type or select how long you need your backup data available. You can select a retention range between 1 and 12 weeks for short-term tape-based protection.
2. In the **Frequency of backup** box, select how often you want to back up your data. You can select a backup frequency of daily, weekly, or biweekly depending on your retention range.
3. In the **Backup mode** box, select your backup type. For tape-based backup, instead of recovery points, you configure your type of backup as follows:
    - **Full and incremental backups**. (Available only when you select a daily backup frequency.)

        Important

        If you select this backup type, the retention range will be a maximum of one week longer than the one you specified, because of a dependency between full and incremental backups.
    - **Full backup only**. For more information about full and incremental backups, in the DPM Planning Guide see Planning Protection Groups (http://go.microsoft.com/fwlink/?LinkId=91849).
4. Select your daily backup schedule as follows:
    - **Full backup on**. When you select daily full backups, you specify the time. When you select weekly or every two weeks, only full backup is available. You specify the day and time.
    - **Incremental backup on**. (Available only when you select daily full and incremental backups). You specify the day and time for the full backup and for the incremental backup.
5. Select from the following performance options:
    - Select **Compress data** if you want to enable data compression on tape.

- Select **Encrypt data** to encrypt the data before it is written to tape.
- Select **Do not compress or encrypt data** if you do not want DPM to perform data compression or encryption.

6. Click **Next**.

Allocating Space for the Protection Group

When you select disk-based protection, you must allocate space on the storage pool for the replicas and recovery points for each data source that you want DPM to protect. You must also allocate space on protected file servers or workstations for the change journal. DPM recommends and allocates disk space for your protection group based on the size of the data to be protected. You can modify the disk space in the storage pool; however, there are guidelines you must follow to increase the allocated disk space. For more guidelines about allocating disk space, in the DPM Planning Guide, see Planning Protection Groups (http://go.microsoft.com/fwlink/?LinkId=91849).

To allocate space for the protection group

1. On the **Review Disk Allocation** page, review the space allocations that DPM recommends for the protection group. DPM lists the disk spaced that is allocated for your protection group based on the size of the selected data.

   Accept the default space allocations unless you are certain that they do not meet your needs.

2. On the **Review Disk Allocation** page, do the following:

   a. Accept the recommended allocations, or click **Modify** to change the disk space allocation on the DPM server and the protected computer, or to specify a custom volume.

   b. On the **Modify Disk Allocation** page, on the **DPM Server** tab, select from the following:

   - **Storage type**. Select the storage location. Your options are **Storage pool** or **Custom volume**.
   - **Replica Volume**. Type the disk space for the replica volume, or select the custom volume to use for the replica volume.
   - **Recovery Point Volume**. Type the disk space for the recovery point volume, or select the custom volume to use for the recovery point volume.
   - **Custom Volume**. Select the custom volume.

     Any volume that is attached to the DPM server can be selected as a custom volume except the volume that contains the system and program files

     Note

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

- **Calculate**. Click this link to calculate the data size for the data source.

3. When you finish specifying the new allocations, click **OK**, and then click **Next**.

Specifying Your Long-term Protection Goals

DPM creates a protection plan using your long-term recovery goals. You define your long-term protection plan by selecting a retention range for your data and a long-term backup schedule.

If you schedule your long-term backup on the same day that you create the protection group, the tape backup will run in the next calendar cycle. For example, if you create the protection group on January 1st, 2007 and schedule a yearly tape backup on the same day, the tape backup will not run until January 1st, 2008.

To create the protection group and to run the tape backup on the same day, in the **Protection** task area, in the **Actions** pane, click **Create recovery point - Tape**.

If you are not using long-term protection, skip to Choosing a Replica Creation Method.

To specify your long-term protection policy

1. On the **Specify Long-Term Protection** page, in the **Retention range** box, Type or select how long you need your backed-up data available. You can select a retention range between 1 and 99 years.
2. In the **Frequency of backup** box, select the backup frequency that you want. The backup frequency is based on the specified retention range, as shown in the following list:
   - When the retention range is 1–99 years, you can select backups to occur daily, weekly, bi-weekly, monthly, quarterly, half-yearly, or yearly.
   - When the retention range is 1–11 months, you can select backups to occur daily, weekly, bi-weekly, or monthly.
   - When the retention range is 1–4 weeks, you can select backups to occur daily or weekly.

   Note

   On a stand-alone tape drive, for a single protection group, DPM uses the same tape for daily backups until there is insufficient space on the tape. For multiple protection groups, DPM requires separate tapes. Therefore, we recommend that you minimize the number of protection groups that you create if you are using a stand-alone tape drive for your backups.

3. Click **Restore Defaults** to restore the defaults back to a three month retention range and a weekly backup frequency.
4. In the **Protection Objectives** section, click **Customize** to change the tape label and to customize the schedule of backup jobs for your recovery goals. This schedule will replace the default schedule.
5. To change the long-term backup schedule, click **Modify**. You have a number of scheduling options for long-term protection, depending on your retention range and backup frequency. For more information, see the following Changing Your Long-Term Backup Schedule section. If you are not modifying the long-term backup schedule, click **Next**.

Changing Your Long-Term Backup Schedule

You can use the **Modify Long-Term Schedule** screen to change your long-term backup schedule. The following table lists the backup frequency and the schedule you can change depending on the retention range you selected. After you modify the long-term backup schedule, click **OK**, and then click **Next**.

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

For this backup frequency	Depending on retention range, you can configure
	backup • Date and time for yearly backup
Yearly	• Date and time for yearly backup

Selecting Library and Tape Details

If you select protection using tape, you must specify the number of copies of each tape that DPM should create and the configuration options for the backup tapes. You also specify whether you want DPM to encrypt and compress the data, and if you want DPM to check the backup for data integrity.

If you are not using long-term protection, skip to Choosing a Replica Creation Method.

To select tape and library details

1. On the **Select Library and Tape Details** page, in the **Primary library** section, do the following:
   - In the **Library** box, select the library that you want to use for your tape backups.
   - In the **Drives allocated** box, select the number of drives you want to allocate for the tape backups.
2. In the **Copy library** section, select the library you want to use for multiple backup copies.

   Note

   Use **Copy library** only if you specified that you wanted multiple tape backup copies. If you did not specify multiple copies, accept the default library (same as the primary **Library**).
3. In the **Tape options for long-term protection** section, do the following:
   - Select **Check backup for data integrity** to check for data integrity between the backup copy versions.
   - Select the **Compress data** option to enable data compression on tape, which reduces the space needed on the tape and increases the number of backup jobs that can be stored on the same tape.
   - Select the **Encrypt data** option to encrypt the data before it is written to tape, which increases the security for archived data.
   - Select the **Do not compress or encrypt data** option if you do not want DPM to perform data compression or encryption.
4. Click **Next**.

Choosing a Replica Creation Method

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

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

On the **Choose Replica Creation Method** page, select when you want DPM to replicate your data.

To choose a replica creation method

1. Select the **Automatically** option to have DPM replicate the data across the network. For large replica creation jobs, you might want to schedule the job to run only during periods of light network traffic.
   - Select **Now** to have DPM immediately begin copying the data from the computers you are protecting to the DPM server.
   - Select **Later** to schedule the initial copy at a later time—most likely after business hours.
   - Select **Manually** to use tape, USB storage, or other portable media to transfer the baseline data to the DPM server.

     This is the preferred option when synchronizing large amounts of data across a slow WAN connection for the first time. For more information about manual replica creation, in the DPM 2007 Operations Guide, see "Creating Replicas Manually" in Managing Performance (http://go.microsoft.com/fwlink/?LinkId=91859).

     If you choose manual replica creation, you must know the details of the source (protected server) and the replica path (DPM server). It is critical that you retain the same directory structure and properties such as time stamps and security permissions for the data that you are protecting.
2. Click **Next**.

Optimizing Performance

DPM 2007 provides several methods you can use to modify protection workloads and optimize performance. To optimize the performance of the protection group, on the **Summary** page, click the **optimize performance** link to launch the **Optimize Performance** dialog box.

▻ **To optimize performance**

1. On the **Summary** page, click **optimize performance**.
2. In the **Optimize Performance** dialog box, on the **Network** tab, select **Enable on-the-wire compression** to reduce the size of the data transfer and increase CPU utilization on the DPM server and the protected servers.
3. In the **Start protection jobs** box, select the time of hour you want the protection job to start to balance the loads of synchronization jobs across protection groups, thus avoiding possible performance degradation.
4. On the **Consistency Check** tab, select **Schedule daily consistency check**, and then select the start time and maximum duration of the consistency check to prevent DPM from interfering with regular business use of your protected servers.
5. Click **OK**.

Creating the Protection Group

Before you create the protection group, review the tasks that DPM is set to perform. The tasks are based on the options that you specified while performing the steps in the wizard.

To optimize the performance of the protection group, on the **Summary** page, click the **optimize performance** link to launch the **Optimize Performance** dialog box.

▻ **To create the protection group**

1. On the **Summary** page, review the tasks that DPM is set to perform to create the protection group and then click **Create Group**.

   When the creation process is complete, DPM displays a confirmation page where you can view the results of creating the protection group task.
2. On the **Confirmation Page**, click **Close**.

Optional Configuration Tasks

You can enable optional System Center Data Protection Manager (DPM) 2007 features during initial configuration or at any time after you deploy DPM 2007. The topics in this section describe the optional features that you can configure.

In This Section

- Enabling End-User Recovery

- Installing the Shadow Copy Client Software
- Subscribing to Alert Notifications
- Configuring the SMTP Server
- Publishing DPM Alerts
- Installing DPM Management Shell

Enabling End-User Recovery

You can enable end-user recovery so that users can independently recover file data by retrieving shadow copies of their files. To enable end-user recovery, you must:

1. Configure Active Directory Domain Services (AD DS) to support end-user recovery.
2. Enable the end-user recovery feature on the DPM server.
3. Installing the shadow copy client software on the client computers.

For more information about installing the shadow copy client software, see Installing the Shadow Copy Client Software.

Note

> You do not need to download the shadow copy client software to enable end-user recovery on computers running Windows Vista.

You can use DPM end-user recovery or the Shadow Copies of Shared Folders client software on the protected computer, but you should disable Shadow Copies of Shared Folders on protected computers if you want to use DPM end-user recovery. When Shadow Copies of Shared Folders is enabled on the protected computer, the end-user recovery client will display shadow copies that are located on the protected computer rather than the shadow copies that are located on the DPM server. We recommend that you wait approximately a week after configuring protection before enabling end-user recovery to allow sufficient recovery points to be created on the DPM server.

You can use the following procedures to configure Active Directory Domain Services and enable end-user recovery on a Microsoft System Center Data Protection Manager (DPM) 2007 server.

Procedures

To configure Active Directory Domain Services and enable end-user recovery for schema and domain administrators

1. In DPM Administrator Console, on the **Action** menu, click **Options**.
2. In the **Options** dialog box, on the **End-user Recovery** tab, click **Configure Active Directory**.
3. In the **Configure Active Directory** dialog box, select **Use current credentials** or type the user name and password for an account that has both schema and domain

administrator privileges, and then click **OK**.

4. On the confirmation and notification prompts, click **Yes**, and then click **OK**.
5. After configuration of Active Directory Domain Services is complete, select the check box for the **Enable end-user recovery** option, and then click **OK**.

To configure Active Directory and enable end-user recovery for users who are not schema and domain administrators

1. Direct a user who is both a schema and domain administrator to configure the Active Directory schema by running **<drive>:\Program Files\Microsoft DPM\DPM\End User Recovery\DPMADSchemaExtension.exe** on a Windows Server 2003–based computer that is a member of the same domain as the DPM server.

   Note

   If the protected computer and DPM reside in different domains, the schema needs to be extended by running the DPMADSchemaExtension.exe tool on the other domain.
2. In the **Enter Data Protection Manager Computer Name** dialog box, type the name of the computer for which you want end-user recovery data in Active Directory Domain Services, and then click **OK**.
3. Type the DNS domain name of the DPM computer for which you want end-user recovery data in Active Directory Domain Services, and then click **OK**.
4. In the **Active Directory Configuration for Data Protection Manager** dialog box, click **OK**.
5. In DPM Administrator Console, on the **Action** menu, click **Options**.
6. In the **Options** dialog box, on the **End-user Recovery** tab, select the **Enable end-user recovery** check box, and then click **OK**.

See Also

Optional Configuration Tasks

Installing the Shadow Copy Client Software

Before end users can begin independently recovering previous versions of their files, the DPM shadow copy client software must be installed on their computers. If a client of Shadow Copies of Shared Folders is present on the computer, the client software must be updated to support Microsoft System Center Data Protection Manager (DPM) 2007.

The shadow copy client software can be installed on computers running Windows XP with SP2 or later, and Windows Server 2003 with or without SP2.

Note

You do not need to download the shadow copy client software to enable end-user recovery on computers running Windows Vista.

The following table shows the locations from which you can download the shadow copy client software for each supported operating system.

Operating System	Shadow Copy Client Software Location
Windows XP SP2	http://go.microsoft.com/fwlink/?LinkId=46064
The 64-bit version of Windows XP SP2	http://go.microsoft.com/fwlink/?LinkId=50683
Windows Server 2003	http://go.microsoft.com/fwlink/?LinkId=46065
Windows Server 2003 SP2	http://go.microsoft.com/fwlink/?LinkId=46067
The 64-bit version of Windows Server 2003 SP2	http://go.microsoft.com/fwlink/?LinkId=46068

Install the client software on users' workstations by using your usual software distribution method (for example, Group Policy Software Installation, Microsoft Systems Management Server, or shared folders). If your users install the client software on their own workstations, instruct them to copy the Setup program to any location on their computer, double-click the file name or icon, and then follow the instructions in the wizard.

See Also

Optional Configuration Tasks

Subscribing to Alert Notifications

You can configure System Center Data Protection Manager (DPM) 2007 to notify you by e-mail of critical, warning, or informational alerts, and the status of instantiated recoveries.

Note

Before you can subscribe to notifications, you must configure the Simple Mail Transfer Protocol (SMTP) server that you want DPM to use to send the notifications. For instructions, see Configuring the SMTP Server.

To subscribe to notifications

1. In DPM Administrator Console, on the **Action** menu, click **Options**.
2. In the **Options** dialog box, on the **Notifications** tab, do the following:
   - Select the types of alerts about which you want recipients to be notified (for example,

critical alerts, warning alerts, informational alerts, or any combination of these).

- Under **Recipients**, type the e-mail address for each recipient (including yourself) to whom you want DPM to send copies of the notifications. Use commas to separate the e-mail addresses.

3. To test the notification settings, click **Send Test Notification**, and then click **OK**.

Configuring the SMTP Server

System Center Data Protection Manager (DPM) 2007 provides options for subscribing to alert notifications and to reports by e-mail. If you plan to enable either of these features, you must first configure the Simple Mail Transfer Protocol (SMTP) server that you want DPM to use to send e-mail. Then specify which e-mail server you want to use.

For added security, the SMTP server can be configured as authenticated. When an SMTP server is authenticated, DPM requires a specified user name and password for the server when sending e-mail notifications and reports.

Note

DPM supports sending e-mail through both authenticated SMTP servers and unauthenticated SMTP servers.

Procedures

To configure DPM to use an SMTP server that does not require authentication

1. In DPM Administrator Console, on the **Action** menu, click **Options**.
2. In the **Options** dialog box, on the **SMTP Server** tab, type the SMTP server name, the SMTP server port, and the e-mail address you want to display in the **From** box of the e-mail messages that DPM sends.

   The e-mail address in the **From** box must be a valid e-mail address on the SMTP server.
3. To test the SMTP server settings, click **Send Test E-mail**, type the e-mail address to where you want DPM to send the test message, and then click **OK**.

To configure DPM to use an SMTP server that requires authentication

1. In DPM Administrator Console, on the **Actions** menu, click **Options** to display the **Options** dialog box.
2. On the **SMTP Server** tab, type the SMTP server name, the SMTP server port, and the e-mail address you want to display.
3. In the **Authenticated SMTP server** area, type a user name and password in the

appropriate boxes.

Note

The **User Name** must be the domain user name (for example, domain\user name). The **From** address must be the SMTP address of the user.

4. To test the SMTP server settings, click **Send Test E-mail**, type the e-mail address where you want DPM to send the test message, and then click **OK.**

See Also

Optional Configuration Tasks

Publishing DPM Alerts

You use the **Alert Publishing** option only if you have chosen to centrally monitor your Microsoft System Center Data Protection Manager (DPM) 2007 servers in Microsoft Operations Manager 2005 (MOM) or System Center Operations Manager 2007. You use this option to synchronize the DPM Alerts that are displayed in the DPM Administration Console with the MOM or System Center Operations Manager 2007 display.

The **Alert Publishing** option publishes to the DPM Alerts event log all existing actionable DPM alerts that might require a user action. The MOM or Operations Manager 2007 agent that is installed on the DPM server publishes the alerts in the **DPM Alerts** event log to MOM or Operations Manager 2007 and continues to update the display as new alerts are generated.

For information about the DPM Management Packs, see:

For information about centrally monitoring your DPM servers, see:

- DPM 2007 Management Pack Guide for Microsoft Operations Manager 2005 (http://go.microsoft.com/fwlink/?LinkID=66735)
- DPM 2007 Management Pack Guide for System Center Operations Manager 2007 (http://go.microsoft.com/fwlink/?LinkID=100474)

To publish existing DPM alerts

1. In DPM Administrator Console, on the **Action** menu, click **Options**.
2. In the **Options** dialog box, on the **Alert Publishing** tab, click **Publish Active Alerts**, and then click **OK**.

Installing DPM Management Shell

DPM Management Shell, based on Windows PowerShell, is an interactive command-line technology that supports task-based scripting.

Microsoft System Center Data Protection Manager (DPM) 2007 provides its own set of Windows PowerShell commands that can be used in addition to DPM Administrator Console to perform data protection management tasks. A DPM administrator can use DPM cmdlets to perform many of the administrative tasks that can be performed in the console.

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

Procedures

To install DPM Management Shell

1. Log on to the computer on which you want to install DPM Management Shell using a domain user account that is a member of the local administrators group.
2. Insert the Microsoft Data Protection Manager 2007 product DVD in the DVD drive. If the DPM Setup Wizard does not start automatically, double-click **Setup.exe** in the root folder of the DVD.

   -Or-

   If you are installing DPM from a network share, navigate to the installation share and then double-click **Setup.exe** in the root folder of the share.
3. On the **Microsoft System Center Data Protection Manager 2007** screen, click **Install DPM Management Shell**.

Installing the DPM System Recovery Tool

The DPM System Recovery Tool (SRT) is software provided with DPM to facilitate bare metal recovery for the DPM 2007 server and the computers that DPM protects. DPM SRT can be installed on a DPM 2007 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. We recommend that you place 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 place the primary file store on a separate volume on the same disk.

DPM SRT is not included on the DPM 2007 product DVD. It must be installed separately from the DPM System Recovery tool CD. For more information about installing DPM SRT, see the topics under the "Installation" node in the DPM System Recovery Tool Help (the .chm file) on the DPM SRT CD.

Troubleshooting Your DPM 2007 Installation

The topics in this section provide guidance for troubleshooting issues with your System Center Data Protection Manager (DPM) 2007 and protection agent installations.

In This Section

Troubleshooting DPM 2007 Installation Issues

Troubleshooting Protection Agent Installation Issues

Troubleshooting DPM 2007 Installation Issues

The following table provides guidance for troubleshooting issues that may occur when you are installing System Center Data Protection Manager (DPM) 2007.

DPM Installation Issues

Issue	Possible Cause	Resolution
A DPM installation interrupts non-DPM applications.	During DPM installation, Setup restarts the Windows Management Instrumentation (WMI) service. If you are running applications other than DPM and its prerequisite software on the DPM server, you may experience an interruption in the operation of those applications while the WMI	To prevent an interruption, shut down all other applications before you run DPM Setup.

Issue	Possible Cause	Resolution
	service is restarted.	
Error 812. Configuration of reports failed.	This problem occurs when both SQL Server Reporting Services and Windows SharePoint Services are installed in the same Internet Information Services (IIS) application pool.	To resolve this issue, perform one of the following tasks: • Uninstall Windows SharePoint Services by using **Add or Remove Programs**, uninstall DPM, and then install DPM again. -Or- • Configure a side-by-side installation of SQL Server Reporting Services and Windows SharePoint Services. For instructions, see Troubleshooting a Side-by-Side Installation of Reporting Services and Windows SharePoint Services (http://go.microsoft.com/fwlink/?LinkId=50877). **Note** The Rsactivate tool referred to in “Troubleshooting a Side-by-Side Installation of Reporting Services and Windows SharePoint Services” is located in the DPM installation path at Microsoft Data Protection Manager\Prerequisites\MSSQL\Reporting Services\ReportServer\RSReportServer.config.
The DPM installation fails.	An IIS installation failure occurs causing the DPM installation to fail.	Uninstall IIS using **Add or Remove Windows Components**, and then manually reinstall it. When the Windows Components Wizard prompts you for the IIS files, insert the Microsoft Windows Server product CD. To install IIS, note the following: • If you installed only the Windows Server 2003 operating system and then later updated to Service Pack 2 (SP2), you must provide the Windows Server 2003 CD. • If you slipstreamed Windows Server 2003 Service Pack 1 (SP1) with the operating system and then later updated to Windows Server 2003 SP2, you must provide the Windows Server SP1 slipstream CD. • If you slipstreamed Windows Server 2003 SP2 with the operating system, you must provide the Windows Server 2003 SP2 slipstream CD.
Error 810 or	If the DPM server	Verify that the DPM server can communicate with the

Issue	Possible Cause	Resolution
ID: 4315. The trust relationship between this workstation and the primary domain failed.	is unable to connect to the domain controller during installation, the DPM installation fails.	domain controller. In addition, verify that the DNS entries are for the domain controller and that they are correctly configured.
Error 820. Setup cannot query the system configuration while performing the prerequisite check on Windows Server 2008 operating system.	This issue occurs if IIS has been installed without all of the components that DPM requires.	To resolve the issue, remove IIS, and then run DPM setup again.

Remote SQL Server Issues

The following table provides guidance for troubleshooting remote SQL Server issues.

Remote SQL Server Issues

Issue	Possible Cause	Resolution
Error 812. Report deployment failed.	DPM setup fails if you choose an instance of SQL Server that is running on a Windows Server 2008 operating system x64 server.	To resolve this issue, do the following: 1. Uninstall DPM 2007. 2. On the Windows Server 2008 x64 computer running the remote instance of SQL Server 2005, follow the steps in Knowledge Base article 938245, "How to install and configure SQL Server 2005 Reporting Services on a computer running Windows Server 2008" (http://go.microsoft.com/fwlink/?LinkId=102

Issue	Possible Cause	Resolution
		506). 3. Run DPM setup again.

Troubleshooting Error ID 4307

The following table provides guidance for troubleshooting **Error ID 4307**. This error occurs when you are attempting to connect to a remote SQL Server database when installing System Center Data Protection Manager (DPM) 2007.

Troubleshooting Error ID 4307

Possible Cause	Resolution
Remote connection to the computer running SQL Server is disabled.	To enable the remote instance of SQL Server, do the following: 1. From the Start menu, point to **All Programs**, point to **Microsoft SQL Server 2005**, point to **Configuration Tools**, and then click **SQL Server Configuration Manager**. 2. In SQL Server Configuration Manager, in the console pane, expand **SQL Server 2005 Network Configuration**, and then select the network protocol for the DPM named instance. 3. In the details pane, if TCP/IP is disabled, right-click **TCP/IP** and click **enable**.
The SQL Server Browser service is disabled.	To start the SQL Server Browser service, do the following: 1. In SQL Server Configuration Manager, in the console pane, click **SQL Server 2005 Services**. 2. In the details pane, right-click **SQL Server Browser**, and then click **Properties**. 3. In the **SQL Server Browser Properties** dialog box, on the **Service** tab, select **Automatic** from the **Start Mode** drop-down list, and then click **OK**. **Note**

Possible Cause	Resolution
	By default, Microsoft SQL Server 2005 sets the SQL Server Browser service to start automatically.
The name of the remote instance of SQL Server is in the incorrect format.	Ensure that the remote SQL Server instance name is in the following format: *<Computer name>**<Instance name>* **Note** Only use *<Computer name>* for the default instance.
There is no network connectivity between the DPM server and the computer running SQL Server.	Ensure there is a connection between the DPM server and the computer running SQL Server.

Troubleshooting Protection Agent Installation Issues

The following table provides troubleshooting guidance that supplements the specific error messages that you may encounter during protection agent installation.

Before beginning the troubleshooting process, we recommend that you first try to manually install the protection agents. For detailed instructions for installing the protection agents manually, see Installing Protection Agents Manually (http://go.microsoft.com/fwlink/?LinkId=100443).

Agent Installation Issues

Issue	Possible Cause	Resolution
Error 300: The agent operation failed because it could not communicate with the specified server.	• Incorrect firewall configuration requirements on the DPM server. • The Remote Procedure	To resolve this issue, do the following: • For firewall configuration requirements in the DPM Operations Guide, see Managing DPM Servers (http://go.microsoft.com/fwlink/?LinkId=91853). • For an unavailable RPC server, see Microsoft Knowledge Base article 224370, "Troubleshooting RPC Server is Unavailable in Windows" (http://go.microsoft.com/fwlink/?LinkId=458

Issue	Possible Cause	Resolution
	Call (RPC) server is unavailable.	17).
Error 303: Agent operation with specified server failed.	- Another installation is running on the specified server. - The boot volume on the server is formatted as file allocation table (FAT).	- Wait for the installation to complete, and then retry the operation. - Convert the boot volume to NTFS file system if you have sufficient space. For more information about using the **Convert** command for converting FAT volumes to NTFS, see Microsoft TechNet article Convert (http://go.microsoft.com/fwlink/?LinkId=50882). Review Microsoft Knowledge Base article 156560, "Free Space Required to Convert FAT to NTFS" (http://go.microsoft.com/fwlink/?LinkId=50883). - If neither of these actions resolves the problem, restart the specified server and then retry the operation.
Error 306: Agent installation failed because the specified server already has a different version of the protection agent installed.	This issue occurs when the protection agent has already been installed on a server, but the DPM database does not have a record of the protection agent being installed.	Perform the following steps to reinstall the protection agent. 1. Locally uninstall the protection agent from the server. 2. On the DPM server, in DPM Administrator Console, in the **Management** task area, on the **Agents** tab, select the server. In the **Actions** section, click **Refresh information**. The agent status will change to **Error**. 3. In the **Details** section, click **Remove the record of the server from this DPM computer**. 4. Reinstall the protection agent on the server.
Error 308: The agent operation failed	- Incorrect firewall	- For firewall configuration requirements, in the DPM Operations Guide, see Managing

Issue	Possible Cause	Resolution
because of a communication error with the DPM Protection Agent service on the specified server.	configuration requirements on the DPM server. - Internet Protocol Security (IPSec) configuration. - The RPC server is unavailable.	DPM Servers (http://go.microsoft.com/fwlink/?LinkId=91853). - IPSec may be configured to block particular IP traffic, such as on a particular port or to particular addresses. For assistance in troubleshooting IPSec, see IPsec Troubleshooting (http://go.microsoft.com/fwlink/?LinkId=50885). - See Microsoft Knowledge Base article 224370, "Troubleshooting RPC Server is Unavailable in Windows" (http://go.microsoft.com/fwlink/?linkid=45817).
Error 316: The agent operation failed because the DPM Protection Agent service on the specified server did not respond.	Incorrect firewall configuration requirements on the DPM server.	For firewall configuration requirements, in the DPM Operations Guide, see Managing DPM Servers (http://go.microsoft.com/fwlink/?LinkId=91853).
Error 319: The agent operation failed because of a communication error with the DPM Agent Coordinator service on the specified server.	Incorrect firewall configuration requirements on the DPM server.	For firewall configuration requirements, in the DPM Operations Guide, see Managing DPM Servers (http://go.microsoft.com/fwlink/?LinkId=91853).
Error 324: The agent operation failed because the DPM Agent Coordinator service on the specified server did not respond.	Incorrect firewall configuration requirements on the DPM server.	For firewall configuration requirements, in the DPM Operations Guide, see Managing DPM Servers (http://go.microsoft.com/fwlink/?LinkId=91853).
Error 341: Agent operation failed because credentials provided have insufficient privileges on the specified server.	- The account used does not have sufficient privileges	- Retry the operation with an account that has administrator privileges on the specified server. - Verify that system times on the DPM server and the server on which you are installing the agent are synchronized with

Issue	Possible Cause	Resolution
	on the server. - The system times of the DPM server, the server on which you are installing the agent, and the domain controller are not synchronized, and therefore the Kerberos authentication fails. - The DNS setting on the DPM server or the computer on which you are installing the protection agent is not correct.	the system time on the domain controller. - Verify that the DNS settings are correct.
Error 342: The agent operation failed because the DPM server could not communicate with the specified server.	Incorrect firewall configuration requirements on the DPM	For firewall configuration requirements, in the DPM Operations Guide, see Managing DPM Servers (http://go.microsoft.com/fwlink/?LinkId=91853).

Issue	Possible Cause	Resolution
	server.	
Error 348: An error occurred when the agent operation attempted to communicate with the DPM Agent Coordinator service on the specified server.	Incorrect security settings for the COM object on the computer.	Verify COM permissions on the server. Verify that the DCOM configuration settings are set as follows: **COM Security Default Access Permissions** • Local Access and Remote Access permitted to Self • Local Access permitted to System **COM Security Machine Access Restriction (Security Limits)** • Local and Remote Access permitted to NT AUTHORITY\ANONYMOUS LOGON • Local and Remote Access permitted to BUILTIN\Distributed COM Users • Local and Remote Access permitted to \Everyone **COM Security Default Launch Permissions** • Launch permitted to NT AUTHORITY\SYSTEM • Launch permitted to NT AUTHORITY\INTERACTIVE • Launch permitted to BUILTIN\Administrators **COM Security Machine Launch Restriction (Security Limits)** • Local Launch and Activate permitted to \Everyone • Local and Remote Launch, Local and Remote Activate permitted to BUILTIN\Administrators Local and Remote Launch, Local and Remote Activate permitted to BUILTIN\Distributed COM Users
Error 271: The user does not have administrator access. - Or -	The DCOM configuration settings did not meet the	Verify that DCOM is enabled. If DCOM is enabled, verify that the DCOM configuration settings are set as follows: **COM Security Default Access Permissions**

Issue	Possible Cause	Resolution
Error 377: The agent operation failed because the minimum requirements in the DCOM configuration were not met.	minimum requirements.	- Local Access and Remote Access permitted to Self - Local Access permitted to System **COM Security Machine Access Restriction (Security Limits)** - Local and Remote Access permitted to NT AUTHORITY\ANONYMOUS LOGON - Local and Remote Access permitted to BUILTIN\Distributed COM Users - Local and Remote Access permitted to \Everyone **COM Security Default Launch Permissions** - Launch permitted to NT AUTHORITY\SYSTEM - Launch permitted to NT AUTHORITY\INTERACTIVE - Launch permitted to BUILTIN\Administrators **COM Security Machine Launch Restriction (Security Limits)** - Local Launch and Activate permitted to \Everyone - Local and Remote Launch, Local and Remote Activate permitted to BUILTIN\Administrators - Local and Remote Launch, Local and Remote Activate permitted to BUILTIN\Distributed COM Users
System Error 1130: Not enough server storage is available to process this command. - OR - **Event ID 2011**: Not enough memory to complete the transaction. Close some applications and retry.	The configuration parameter "IRPStackSize" of the server is too small for the server to use a local device.	We recommend that you increase the value of this parameter. See Microsoft Knowledge Base article 177078, "Antivirus software may cause Event ID 2011" (http://go.microsoft.com/fwlink/?LinkId=73102).

Issue	Possible Cause	Resolution
The RPC server is unavailable.	A firewall is enabled on the remote computer.	If a firewall is enabled on the remote computer on which you are installing the protection agents, before installation you must run the **DPMAgentInstaller.exe** executable file. For more information, see Installing DPM 2007 Behind a Firewall (http://go.microsoft.com/fwlink/?LinkId=101313).
The agent operation failed while creating the local group DPMRADCOMTrustedMachines.	The protection agent installation fails when installing on two domain controllers that are in parallel replication.	The protection agent installations cannot occur simultaneously on the domain controllers that are in parallel replication mode. Wait for the replication to occur between the domain controllers before you install the protection agent on the second domain controller. You can also force the replication by doing the following: From the command prompt, type **repadmin /syncall**. The **repadmin** is a utility that you install with the Windows Server 2003 support tools. **Note** Two or more domain controllers in parallel replication mode must be protected by the same DPM server.
The Windows SharePoint Services farm backend server does not appear as protected in DPM Administrator Console.	After you install a protection agent on a backend server to protect a Windows SharePoint Services farm, the server does not appear as protected in the **Management** task area on the **Agents** tab.	No action is required. DPM protects the backend servers internally if the Windows SharePoint Services farm has data on the server.
The protection agent	If the Primary	To resolve this issue, upgrade the forest root

Issue	Possible Cause	Resolution
installation fails if you are installing it on a non-primary domain controller running Windows Server 2003.	Domain Controller (PDC) is running Windows Server 2000, the required Distributed COM Users group will be missing.	PDC emulator operations master role holder to Windows Server 2003, and then perform the protection agent installation again. For more information, see Knowledge Base article 827016, "Local service and other well-known security principals do not appear on your Windows Server 2003 domain controller" (http://go.microsoft.com/fwlink/?LinkId=101729).

DPM Administrator Console in DPM 2007

This content provides an overview of the DPM Administrator Console including a console tour that describes the DPM Administrator layout and explains where the controls for general tasks are located. The content also includes a description of the five task areas of DPM Administrator Console and their associated actions, and how to administer DPM.

Note

> If you are a member of a group other than the Administrators group, such as Backup Operator, you will not have access to DPM Administrator Console.

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

To administer multiple instances of DPM Administrator Console simultaneously, you can install DPM Management Shell on computers other than the DPM server. You can also install DPM Management Shell on desktop computers running Windows XP or Windows Vista

In This Section

How to Use DPM Administrator Console to Administer DPM 2007

Using DPM Administrator Console

Working with DPM Task Areas

Using DPM Administrator Console

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

Task Areas and Display Panes

A task area is a set of logically related functions grouped together in DPM Administrator Console. The console has five task areas: **Monitoring**, **Protection**, **Recovery**, **Reporting**, and **Management**. Each task area, except **Recovery**, consists of three panes: the display pane (unlabeled), **Details** pane, and **Actions** pane.

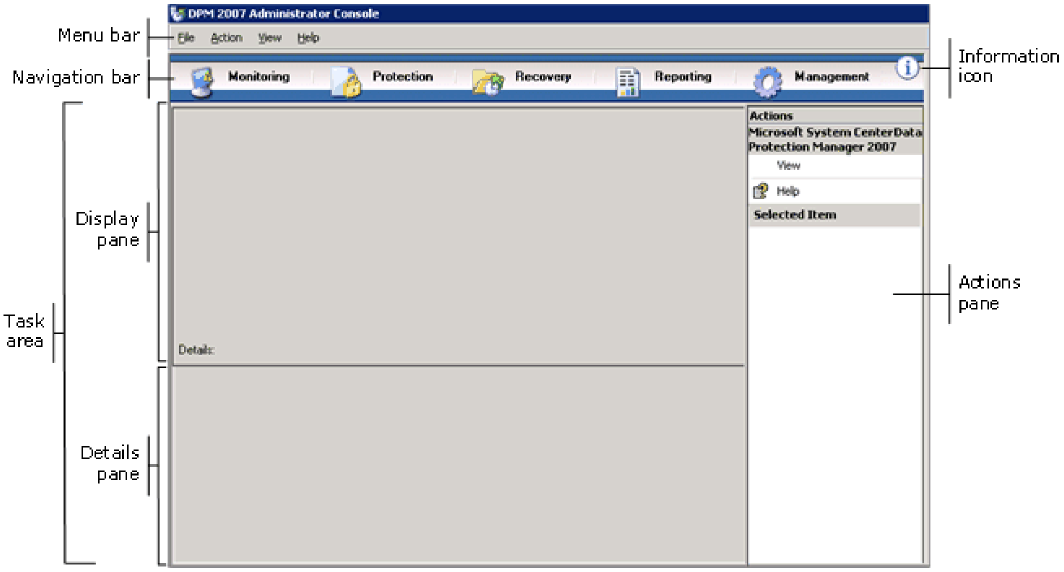
Note

The **Recovery** task area adds another pane for the browsing and searching functions.

Following are descriptions of the information that appears in each of the panes:

- **Display pane**. Lists items associated with the current task. For example, the display pane for the **Protection** task area displays the names of protection groups and lists the members of those groups. The display pane for some task areas is subdivided into tabs that group subsets of functionality. For example, the display pane for the **Management** task area is divided into three tabs: **Agents**, **Disks**, and **Libraries**.
- **Details pane**. Provides details, such as properties and status information, about items selected in the display pane. For example, the **Details** pane for the **Protection** task area displays status, recovery range, and other details about selected protection groups.
- **Actions pane**. Provides access to functionality associated with the current task and, in some cases, the item selected in the display pane. For example, the **Actions** pane for the **Protection** task area provides a command for creating protection groups. When a specific protection group is selected in the display pane, the **Actions** pane also provides a command for adding members to the group.

Layout of DPM Administrator Console



Navigation Bar

The navigation bar enables you to move between the five task areas of the console. To select a task area, click the name of the area.

Menu Bar

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

- **File menu**. Contains standard Microsoft Management Console (MMC) commands. For information about MMC, see MMC Help.
- **Action menu**. Contains the same commands as those displayed in the **Actions** pane, as well as an **Options** command and a **Help** command. The **Options** command enables you to set system-wide options, such as configuring end-user recovery, scheduling auto discovery, and subscribing to notifications. The **Help** command provides access to both DPM Help and MMC Help.
- **View menu**. Provides an alternative method for moving between the task areas of the console, a command for hiding the **Actions** pane, and a link to the DPM community Web site.
- **Help menu**. Provides access to both DPM Help and MMC Help. To access DPM Help from this menu, click **Help Topics**, and then click **Data Protection Manager Help**. The **Help** menu also provides version information for MMC and abridged version information for Microsoft System Center Data Protection Manager 2007.

Information Icon

The information icon provides access to complete version and product identification information for DPM, as well as a link to the Microsoft Software License Terms.

See Also

DPM Administrator Console in DPM 2007

Working with DPM Task Areas

DPM Administrator Console contains five task areas: **Monitoring**, **Protection**, **Recovery**, **Reporting**, and **Management**. The **Actions** pane provides access to functionality associated with the current task and, in some cases, the item selected in the display pane.

The following table provides details about the actions you can perform in each task area.

Task Area	Actions
Monitoring	Use the **Monitoring** task area to monitor the status of data protection, data recovery, and other DPM operations. The **Monitoring task** area contains the following tabs: • **Alerts**—Displays errors, warnings, and informational messages. You can group alerts by protection group, computer, or severity, and you can choose to display active alerts exclusively or to display both active alerts and a history of inactive alerts. You can also subscribe to notifications to receive alerts via e-mail. • **Jobs**—Displays the status of jobs and their associated tasks. You can group jobs by protection group, computer, status, or type, and you can filter jobs by time period. You can choose whether to include regularly scheduled synchronization operations in the list of jobs.
Protection	Use the **Protection** task area to do the following: • Create, rename, and manage members of

Task Area	Actions
	protection groups. - Manage protection schedules, disk allocations, and other options. - Run manual synchronization and consistency check jobs. - Manage recovery points. - Review and respond to results of Auto Discovery.
Recovery	Use the **Recovery** task area to find and recover data from recovery points. The **Recovery** task area contains the following tabs: - **Browse**—Enables you to browse for available recovery points by protected computer. - **Search**—Enables you to search for available recovery points based on data type, location, origin, and recovery point date.
Reporting	Use the **Reporting** task area to do the following: - Generate and view reports on DPM operations. - Schedule automatic report generation. - Manage Reporting Services settings.
Management	Use the **Management** task area to manage protection agents, storage pool disks, and tape libraries. The **Management** task area contains the following tabs: - **Agents**—Displays a list of protection agents deployed on computers and enables you to install, uninstall, and update the agents and agent licenses. - **Disks**—Displays a list of disks included in the storage pool and enables you to add and remove disks from the pool. - **Libraries**—Displays the tape libraries installed on the DPM server and enables

Task Area	Actions
	you to manage the tapes in the library.

See Also

DPM Administrator Console in DPM 2007

How to Use DPM Administrator Console to Administer DPM 2007

To use DPM Administrator Console, you must be logged on to the DPM server under a domain account that has administrator privileges.

Note

> You can also add DPM Administrator Console as a snap-in to a custom Microsoft Management Console (MMC). DPM Administrator Console is listed in the MMC Add/Remove Snap-in menu as **Microsoft System Center Data Protection Manager 2007**.

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

Procedures

To run DPM Administrator Console on the DPM server

- On the **Start** menu, point to **All Programs**, point to **Microsoft System Center Data Protection Manager 2007**, and then click **Microsoft System Center Data Protection Manager 2007**.

  -Or-

  Double-click the **Microsoft System Center Data Protection Manager 2007** icon on the desktop.

To access DPM Administrator Console remotely

1. On the **Start** menu, point to **All Programs**, point to **Accessories**, point to **Communications**, and then click **Remote Desktop Connection**.
2. In the **Remote Desktop Connection** dialog box, enter the name of the DPM server in the **Computer** box and then click **Connect**.
3. On the **Log On to Windows** dialog box, enter the login information for a domain user

account that has administrator privileges.

4. On the **Start** menu, point to **All Programs**, point to **Microsoft System Center Data Protection Manager 2007**, and then click **Microsoft System Center Data Protection Manager 2007**.

   -Or-

   Double-click the **Microsoft System Center Data Protection Manager 2007** icon on the desktop.

See Also

DPM Administrator Console in DPM 2007

Deployment Best Practices

This topic describes best practices related to the deployment of System Center Data Protection Manager (DPM) 2007.

DPM 2007 System Requirements

- Before you install System Center Data Protection Manager (DPM) 2007, you need to ensure that the DPM server and the computers and applications it is going to protect meet network and security requirements. You must also ensure that they are running on supported operating systems and that they meet the minimum hardware and software requirements.

  For information about DPM 2007 System Requirements, see DPM 2007 System Requirements (http://go.microsoft.com/fwlink/?LinkId=66731).

Network Requirements

- If you are protecting data over a wide area network (WAN), there is a minimum network bandwidth requirement of 512 kilobits per second (Kbps).

Hardware Requirements

- We recommend that you install DPM on a 64-bit machine.
- You can install DPM on the same volume that the operating system is installed on, or you can install DPM on a different volume that does not include the operating system. However, you cannot install DPM on the disk that is dedicated to the storage pool, which is a set of disks on which the DPM server stores the replicas and recovery points for the protected data.
- If you have critical data that you want to store, you can use a high-performance logical unit number (LUN) on a storage area network rather than the DPM-managed storage pool.

Software Requirements

- DPM is designed to run on a dedicated, single-purpose server that cannot be either a domain controller or an application server.
- To administer multiple DPM servers remotely, install DPM Management Shell on computers other than the DPM server.

Installing DPM 2007

- You must properly configure Microsoft Windows Server 2003 to support a DPM 2007 installation. For more information about installing Windows Server 2003, see How to Install Windows Server 2003 (http://go.microsoft.com/fwlink/?LinkID=100243).
- DPM 2007 requires a clean installation of DPM. Before you install DPM 2007, you must first uninstall System Center Data Protection Manager 2006 (DPM 2006) and its associated prerequisite software, as well as any previous versions of DPM. Because of the architectural differences between DPM 2006 and DPM 2007, you cannot directly upgrade a computer running DPM 2006 to DPM 2007. However, DPM 2007 includes an upgrade tool that enables you to migrate your DPM 2006 protection group configurations to DPM 2007.

  For more information about upgrading from DPM 2006 to DPM 2007, see Upgrading DPM 2006 to DPM 2007 (http://go.microsoft.com/fwlink/?LinkId=66737).
- If you choose to install DPM or prerequisite software products from a shared folder, DPM Setup adds the Universal Naming Convention (UNC) path of the shared folder to the Internet Explorer local intranet security zone for the duration of the installation.
- You cannot install DPM 2007 on the same computer on which your Microsoft Exchange Server is running.
- You can install DPM only on a local drive, and you cannot install it in read-only folders, in hidden folders, or directly to local Windows folders such as Documents and Settings or Program Files. (DPM can, however, be installed to a subfolder of the Program Files folder.)
- After installation is complete, apply all available Windows Server 2003 service packs and updates. All Windows updates are available from Microsoft Windows Update (http://go.microsoft.com/fwlink/?LinkID=451).

Use a Remote Instance of SQL Server

- We recommend a clean installation on the remote instance of Microsoft SQL Server or when installing the dedicated instance of SQL Server for DPM, and that you use the following settings:
  - Default failure audit setting.
  - Default Windows Authentication mode.
  - Assign a strong password to the **sa** account.
  - Enable password policy checking.
  - Install only the SQL Server Database Engine and Reporting Services components.

    - Run SQL Server by using the least-privileged user account.

- If SQL Server Reporting Services is installed on a remote SQL Server, DPM Setup will use that Reporting Service. If SQL Server Reporting Services is not installed on the remote computer running SQL Server, you must install and configure the service on the remote computer running SQL Server before continuing with DPM Setup.

DPM Server Software Requirements

- Before you install DPM, you must install the following:
    - Knowledge Base article 940349, "Availability of a Volume Shadow Copy Service (VSS) update rollup package for Windows Server 2003 to resolve some VSS snapshot issues" (http://go.microsoft.com/fwlink/?LinkId=99034).
    - After installing Knowledge Base article 940349 and then restarting the DPM server and/or the protected server, we recommend that you refresh the protection agents in DPM Administration Console.

      To refresh the agents, in the **Management** task area, click the **Agents** tab, select the computer, and then in the **Actions** pane, click **Refresh information**. If you do not refresh the protection agents, Error ID: 31008 might appear because DPM refreshes the protection agents only every 30 minutes.
    - Windows PowerShell 1.0 from http://go.microsoft.com/fwlink/?LinkId=87007.
    - Single Instance Storage (SIS) on Windows Server 2008 operating system (Pre-release version).

      For information about installing SIS on Windows Server 2008, see "Manually Install Required Windows Components" (http://go.microsoft.com/fwlink/?LinkId=10063).
    - You can use an existing remote instance of SQL Server for your DPM database. If you choose to use a remote instance of SQL Server, you must install **sqlprep.msi**.

Using a Remote Instance of SQL Server

- To use an instance of SQL Server on a remote computer, run **sqlprep.msi**, which is located on the DPM product DVD in the **DPM2007\msi\SQLprep** folder.
- Verify that the user account you will be using to run the SQL Server service and the SQL Server Agent service has read and execute permissions to the SQL Server installation location.
- The remote instance of SQL Server cannot be on a computer that is running as a domain controller.

Protected Computer Requirements

- Each computer that DPM 2007 protects must meet the protected computer requirements.

  For information about all protected computer requirements, see Protected Computer Requirements (http://go.microsoft.com/fwlink/?LinkId=100473).

- Protected volumes must be formatted as an NTFS file system. DPM cannot protect volumes formatted as FAT or FAT32.

  To simplify recovery in the event of system partition failure, install DPM to a partition that is separate from the system partition. Also, the volume must be at least 1 gigabyte (GB) for DPM to protect it. DPM uses the Volume Shadow Copy Service (VSS) to create a snapshot of the protected data, and VSS will create a snapshot only if the volume size is greater than or equal to 1 GB.

- Before you install protection agents on the computers you are going to protect, you must apply hotfix 940349. For more details, see Microsoft Knowledge Base article 940349, "Availability of a Volume Shadow Copy Service (VSS) update rollup package for Windows Server 2003 to resolve some VSS snapshot issues" (http://go.microsoft.com/fwlink/?LinkId=99034).

  After installing Knowledge Base article 940349 and then restarting the DPM server and/or the protected server, we recommend that you refresh the protection agents in DPM Administration Console.

  To refresh the agents, in the **Management** task area, click the **Agents** tab, select the computer, and then in the **Actions** pane, click **Refresh information**. If you do not refresh the protection agents, Error ID: 31008 might appear because DPM refreshes the protection agents only every 30 minutes.

Protection for computers running SQL Server 2005 Service Pack 1 (SP1)

- You must start the SQL Server VSS Writer Service on computers running SQL Server 2005 SP1 before you can start protecting SQL Server data.

  The SQL Server VSS Writer Service is turned on by default on computers running SQL Server 2005. To start the SQL Server VSS Writer Service, in the **Services** console, right-click **SQL Server VSS writer**, and then click **Start**.

Protection for computers running Exchange Server 2007

- Before you can protect Exchange Server 2007 data in a Clustered Continuous Replication (CCR) configuration, you must install hotfix 940006. For more details, see Knowledge Base article 940006, "Description of Update Rollup 4 for Exchange 2007" (http://go.microsoft.com/fwlink/?LinkId=99291).
- The eseutil.exe and ese.dll versions that are installed on the most recent edition of Exchange Server must be the same versions that are installed on the DPM server. In addition, you must update eseutil.exe and ese.dll on the DPM server if they are updated on a computer running Exchange Server after applying an upgrade or an update. For more information about updating eseutil.exe and ese.dll, see "Eseutil.exe and Ese.dll" in "Protected Computer Requirements" (http://go.microsoft.com/fwlink/?LinkId=100473).

Protection for computers running Virtual Server

- To protect virtual machines for online backups, we recommend that you install version 13.715 of Virtual Machine Additions (http://go.microsoft.com/fwlink/?LinkId=84271).

Protection for computers running Windows SharePoint Services

- Before you can protect Windows SharePoint Services (WSS) data, you must do the following:
    - Install Knowledge Base article 941422, "Update for Windows SharePoint Services 3.0" (http://go.microsoft.com/fwlink/?LinkId=100392).
    - Start the WSS Writer service on the WSS Server and then provide the protection agent with credentials for the WSS farm.
    - Update the instance of SQL Server 2005 to SQL Server 2005 SP2.

Repairing DPM 2007

- In most cases, you do not need to uninstall the DPM prerequisite software to reinstall DPM. However, if the Microsoft SQL Server 2005 binaries become corrupted, you might need to uninstall and reinstall SQL Server 2005 as well.
- You do not need to uninstall the protection agents from the protected computers to reinstall DPM.
- Before starting a reinstallation of DPM 2007, we strongly recommend that you archive the DPM database, Report database, and replicas to tape or other removable storage medium. For instructions, in the DPM Operations Guide, see Disaster Recovery (http://go.microsoft.com/fwlink/?LinkId=91860).

Uninstalling DPM 2007

- If you plan to retain your existing data protection configuration after uninstalling DPM, disable end-user recovery on the DPM server and run synchronization jobs for each data source in your protection groups before you start the uninstallation. These steps help ensure that users to whom you deny access to files on the server cannot access the replicas of those files on the DPM server.
- After you uninstall the DPM system requirements, you must restart the computer to complete the uninstall.

Configuring DPM 2007

- Before you can start protecting data by using System Center Data Protection Manager (DPM) 2007, you must verify that each computer that DPM is going to protect meets the protected computer software requirements.

  For information about the DPM 2007 software requirements, see Software Requirements (http://go.microsoft.com/fwlink/?LinkId=100242).
- To successfully protect your data using DPM 2007, you must complete the following configuration tasks:
    - Add one or more disks to the storage pool. (DPM does not support USB/1394 disks.)

- Adding a disk to the storage pool is not a requirement if you are going to use custom volumes to protect your data sources or if you are going to use disk-to-tape protection only.
- 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 only space 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.
- Configure tape libraries and stand-alone tape drives if you want to protect data on tape.
- Install a protection agent on each computer that you want to protect.
- Start and configure the Windows SharePoint Services VSS Writer Service (WSS Writer service), and provide farm administration credentials for the protection agent.
- Perform this task only if you are protecting server farms on servers running Windows SharePoint Services 3.0 or Microsoft Office SharePoint Server 2007.
- Create one or more protection groups.

Configuring Tape Libraries

- You use the **Rescan** operation on the **Libraries** tab to check for and refresh the state of all new tape libraries and stand-alone tape drives when you make changes to your hardware.

  If the stand-alone tape drives listed on the **Libraries** tab in DPM Administrator Console do not match the physical state of your stand-alone tape drives, in the DPM 2007 Operations Guide see Managing Tape Libraries (http://go.microsoft.com/fwlink/?LinkId=91964). For example, if drives from a tape library are listed as stand-alone tape drives, or if a stand-alone tape drive displays incorrectly as a drive in a tape library, you need to remap the tape drive information.

Installing and Configuring Protection Agents

- DPM supports protecting computers across domains within a forest; however, you must establish a two-way trust across the domains. If there is not a two-way trust across domains, you must have a separate DPM server for each domain. DPM 2007 does not support protection across forests.

  If a firewall is enabled on the DPM server, you must configure the firewall on the DPM server. To configure a firewall on a DPM server, you must open port 135 to Transmission Control Protocol (TCP) traffic, and you must enable the DPM service (Msdpm.exe) and the protection agent (Dpmra.exe) to communicate through the firewall.

Configuring Windows Firewall on the DPM Server

- If Windows Firewall is enabled on the DPM server when you install DPM, DPM Setup configures the firewall automatically.

You must open port 5718 to enable communication with the agent coordinator and port 5719 to enable communication with the protection agent.

Installing Protection Agents

- Before you install protection agents on the computers you are going to protect, you must apply hotfix 940349. For more information about this hotfix, see Microsoft Knowledge Base article 940349, "Availability of a Volume Shadow Copy Service (VSS) update rollup package for Windows Server 2003 to resolve some VSS snapshot issues" (http://go.microsoft.com/fwlink/?LinkId=99034).

  After installing Knowledge Base article 940349 and then restarting the DPM server and/or the protected server, we recommend that you refresh the protection agents in DPM Administration Console. To refresh the agents, in the **Management** task area, click the **Agents** tab, select the computer, and then in the **Actions** pane, click **Refresh information**. If you do not refresh the protection agents, Error ID: 31008 might appear because DPM refreshes the protection agents only every 30 minutes.
- If you are installing a protection agent and encounter network-related or permissions-related issues because of domain policies, we recommend that you install the protection agent manually. For information about manually installing a protection agent, see Installing Protection Agents Manually (http://go.microsoft.com/fwlink/?LinkId=100443).

Clustered Data

- You must install the protection agent on all nodes of the server cluster to successfully protect the clustered data. The servers must be restarted before you can start protecting data. This restart is necessary to ensure that the protection agent is installed correctly. Because of the time required to start services, it might take a few minutes after a restart is complete before DPM can contact the server.

  DPM will not restart a server that belongs to Microsoft Cluster Server (MSCS). You must manually restart a server in an MSCS cluster.

Starting and Configuring the WSS Writer Service

- Before you can start protecting server farms on servers running Windows SharePoint Services 3.0 or Microsoft Office SharePoint Server 2007, you must start and configure the Windows SharePoint Services VSS Writer Service (WSS Writer service).

  If your Windows SharePoint Services farm has multiple Web Front End (WFE) servers, you must select only one WFE server when you configure protection in the Create New Protection Group Wizard.

  You must rerun **ConfigureSharepoint.exe** whenever the Windows SharePoint Services farm administrator password changes.

Creating Protection Groups

- To use DPM Administrator Console, you must be logged on to a DPM server with an account that has administrative privileges on that server.

  Before you can start protecting data, you must create at least one protection group. For guidelines about protection groups, in Planning a DPM 2007 Deployment, see Planning Protection Groups (http://go.microsoft.com/fwlink/?LinkId=91849).

Long-Term Protection

- On a stand-alone tape drive, for a single protection group, DPM uses the same tape for daily backups until there is insufficient space on the tape. For multiple protection groups, DPM requires separate tapes. Therefore, we recommend that you minimize the number of protection groups that you create if you are using a stand-alone tape drive for your backups.

Replica Creation

- We recommend that you chose to manually create the replica when synchronizing large amounts of data across a slow WAN connection for the first time. For more information about manual replica creation, in the DPM 2007 Operations Guide, see "Creating Replicas Manually" in Managing Performance (http://go.microsoft.com/fwlink/?LinkId=91859).

  If you choose manual replica creation, you must know the details of the source (protected server) and the replica path (DPM server). It is critical that you retain the same directory structure and properties, such as time stamps and security permissions for the data that you are protecting.

Subscribing to Alert Notifications

- You can configure System Center Data Protection Manager (DPM) 2007 to notify you by e-mail of critical, warning, or informational alerts, and the status of instantiated recoveries.

  Before you can subscribe to notifications, you must configure the Simple Mail Transfer Protocol (SMTP) server that you want DPM to use to send the notifications. For instructions, see Configuring the SMTP Server.

Co-existing with Other Backup Applications

If you want DPM to co-exist with other backup applications (for example, while you are evaluating DPM, but still want to continue backups with your existing solution), we recommend that you adhere to the following guidelines.

DPM 2007 can co-exist with other SQL Server backup applications as long as the other backup applications perform only full backups. Only one application at a time can perform log backups on a SQL Server database. Therefore, administrators should ensure that they do full backups only with other backup applications. Full backups do not impact the log chain in any way, and therefore DPM backups can continue without any problems.