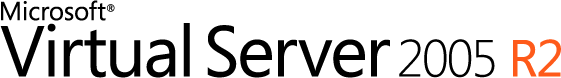


Deployment Cookbook: Hosted Backup



Microsoft® System Center Data Protection Manager 2007 & Microsoft® Virtual Server 2005 R2 Service Pack 1

Table of Contents

[Introduction 2](#_Toc174950517)

[Before You Begin 3](#_Toc174950518)

[Section 1: Install and Configure Virtual Server 15](#_Toc174950519)

[Section 2: Install and Configure Data Protection Manager 30](#_Toc174950520)

[Section 3: Back Up Data 47](#_Toc174950521)

[Section 4: Monitor and Report 64](#_Toc174950522)

[Section 5: Restore Data 70](#_Toc174950523)

[Appendix A: Back Up and Restore Data to a Running VM 86](#_Toc174950524)

[Appendix B: DPM Protocols and Ports 102](#_Toc174950525)

[Appendix C: Install IIS via Control Panel 103](#_Toc174950526)

[Appendix D: Virtual Server Security Considerations 107](#_Toc174950527)

[Appendix E: Install the iSCSI Initiator 108](#_Toc174950528)

[Related Links 114](#_Toc174950529)

Version 1.0

# Introduction

Most mid-sized and larger businesses may want to deploy Microsoft® System Center Data Protection Manager (DPM) 2007 within their infrastructure, especially where remote offices are involved. DPM provides centralized backup of branch offices, effectively making the company’s primary data center its disaster recovery site, as well as the hub for backups for the remote sites.

However, this will not work for all customers. Customers with less reachable alternate sites, or with one-site clients, need an alternate location. In these cases, their trusted systems integrator or channel partner is a logical choice for storing data.

### Intended Audience

This deployment cookbook is written for you, the IT generalist with a Microsoft channel partner, who seeks to become a Hosted Backup Provider (HBP) to your customers. The goal of this guide is to provide all of the steps and guidance necessary for you to successfully install and configure Microsoft® Virtual Server 2005 R2 SP1 and System Center Data Protection Manager 2007—and to provide this service to your customers.

### Using This Guide

This cookbook serves two purposes. First, you can follow the step-by-step instructions in a test environment to get a basic understanding of the concepts, techniques, and applications used in this scenario. Second, you can refer back to this cookbook as a how-to guide to performing specific tasks in a production environment.

To cover the bases, this cookbook probably contains more information than you need. In addition to the Table of Contents at the beginning of this guide, each section also includes its own table of contents so that you can easily find the steps that you need most. If you already have a component installed or a step completed, move on to the next step or section.

# Before You Begin

This cookbook assumes that you already have either Windows Server® 2003 Standard Edition, Enterprise Edition, Datacenter Edition, or later versions; or Windows Server® 2003 Standard x64 Edition, Enterprise x64 Edition, Datacenter x64 Edition, or later versions installed on your servers. This guide also assumes that you have the latest service pack for Windows Server 2003 installed on your server.

In this section, we will cover other prerequisites for you and your environment, as well as other specifics that will help you get the most out of this guide.

### Necessary Hardware to Follow Along

In order to learn the basics of using DPM deployed on virtual machines for data protection, you will need the following hardware in your test environment when going through this cookbook:

#### Two (2) physical servers

These servers will host the virtual machines that you will create while following this cookbook and each one must have one of the following operating systems installed on it:

* Windows Server 2003 Standard Edition, Enterprise Edition, Datacenter Edition, or later versions
* Windows Server 2003 Standard x64 Edition, Enterprise x64 Edition, Datacenter x64 Edition, or later versions
* Windows® Small Business Server 2003 Standard Edition or Premium Edition
* Windows® XP Professional Service Pack 2 (SP2)

To best ensure the responsiveness of the virtual machines that you will create and to shorten the wait time for installations to complete, both servers should have these recommended characteristics:

* 2 gigabytes (GB) RAM
* 1 GHz or faster CPU, such as an Intel® Xeon® processor
* 4.5 GB free hard drive space
* 1 NIC
* Processors with hardware-assisted virtualization technology such as Intel® Virtualization Technology. For more information on Intel Virtualization Technology, see [Intel Virtualization Technology Support](#_Intel_Virtualization_Technology_1) in the Virtual Server 2005 R2 SP1 section later in this document.

For specific system requirements and recommendation information, consult the [Virtual Server 2005 R2 SP1](#_Virtual_Server_2005) and [Data Protection Manager 2007](#_Data_Protection_Manager) sections later in this cookbook. See the [Bandwidth Considerations](#_Bandwidth_Considerations) section for more specific information on network cards for your physical server.

You may also consider deploying the solution outlined in this cookbook in your production environment on Intel Xeon quad-core processor-based servers. Quad-core technology provides you with significantly enhanced performance when compared with single-core or dual-core processors, particularly for virtualized workloads like the one described in this cookbook. This can allow you to run more virtual machines without having to buy, manage, and administer more physical servers.

#### One (1) virtual domain controller

The virtual machine that you will create while following this cookbook will need to be joined to an Active Directory® domain. In a production environment, this will be a customer domain. For testing purposes, this cookbook will lay out steps to create a virtual machine to serve as the domain controller. However, you can also set up a physical domain controller for this test scenario if you prefer.

In addition to being a domain controller, this virtual machine is also an Active Directory-integrated DNS server.

**Note:** Because the domain controller is running on a virtual machine, we recommend that you use two physical servers to follow the steps in this cookbook. Joining a physical server to a domain controller that is running on that physical server as a virtual machine is possible, but is technically complex.

#### One (1) computer to protect

You can use almost any computer in this role. This computer can either be a server or a client, and can be any computer on your domain (including the server hosting your DPM virtual machine, although doing this requires a more sophisticated implementation of Virtual Server than is provided in this cookbook).

Note that if you choose to use your domain controller as the computer that you protect, you will limit some of the scenarios that you can test, such as restoring the entire computer (as attempting this would break your domain and, by extension, your DPM virtual machine). In this scenario, we will not be protecting a domain controller.

#### One (1) virtual machine that is running DPM

We will create this virtual machine in this document, and join it to an Active Directory domain. We will then install DPM on it.

#### One (1) mass storage device or solution

Protecting data means storing backup data. In the case of the test environment you are working in should not be large: you control the size of the volumes and files of the computer you will practice protecting—in the interest of your own time, keep this as small as possible. However, this cookbook will take you through interacting with a mass storage apparatus like a storage area network (SAN) or a direct-attached storage (DAS) device. You can alter the steps presented in this cookbook to use hard drive space on the computer hosting your DPM virtual machine, but you will only be depriving yourself out of the vital experience of getting a virtual machine that you have made to work with mass storage as you would in a production setting.

Because your mass storage will have to work with virtual machines both in your test environment and in your production environment, your mass storage must use iSCSI. For a deeper discussion of the storage considerations for this deployment scenario, see the [Storage Type Considerations](#_Storage_Type_Considerations) section later in this guide.

### Test Network Topology

In the course of the going through this cookbook, you will create one virtual machine with two virtual hard drives, on which you will install DPM. You will also create a virtual machine to server as your domain controller. (You may also choose to create a virtual machine to protect with DPM.)

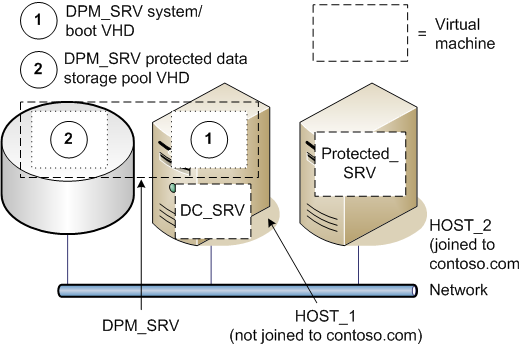


Figure Test network topology for this cookbook

Table 1 lists in greater detail the virtual machines created and the physical host computer used in the test environment for this cookbook.

Table Virtual machine and host computer configurations for cookbook test environment

|  | **DC\_SRV** | **DPM\_SRV** | **PROTECTED\_SRV** | **HOST\_1** | **HOST\_2** |
| --- | --- | --- | --- | --- | --- |
| **Operating System** | Windows Server 2003 R2 Standard Edition SP2 | Windows Server 2003 R2 Standard Edition SP2 | Windows  Server 2003 R2 Standard  Edition SP2 | Windows  Server 2003 R2 Standard Edition SP2 | Windows  Server 2003 R2 Standard Edition SP2 |
| **Memory** | 512 MB (assigned) | 1024 MB (assigned) | 256 MB (assigned) | 2048 MB (physical) | 1024 MB (physical) |
| **IP Addressing Information** | 192.168.10.10 | 192.168.10.11 | 192.168.10.12 | 192.168.10.250 | 192.168.10.20 |
| **Installed Services** | DNS  (domain IP addresses static) | None  (Virtual machine created and DPM installed in course  of cookbook) | None  (Virtual machine created and DPM agent installed in  course of cookbook) | None  (Virtual Server installed in course  of cookbook) | None  (Virtual Server and DPM agent installed in course  of cookbook) |
| **Physical or Virtual** | Virtual | Virtual | Virtual | Physical | Physical |
| **Host Server** | HOST\_1 | HOST\_1 | HOST\_2 | - | - |
| **Domain Name** | contoso.com | contoso.com | contoso.com | - | contoso.com |

### Production Network Topology

In a real-world production environment, the HBP deployment scenario for Virtual Server and DPM deploys DPM on a series of Virtual Server-based virtual machines running on the HBP’s host server or servers (see Figure 2). To maximize customer data isolation and security, each virtual machine running DPM is joined to the appropriate customer’s domain. This configuration has two advantages:

* By deploying Virtual Server, you can create multiple virtual machines that are entirely isolated from each other.
* By deploying Data Protection Manager inside of each virtual machine, each DPM system can fully participate in one particular client’s domain and Active Directory infrastructure, while ensuring that neither data nor security information is exposed to any other HBP client site.

Advances in server hardware make this topology attractive from a performance point of view. For example, Intel has created a set of hardware enhancements, called Intel Virtualization Technology, for Intel Xeon processor-based server platforms. Intel Virtualization Technology can improve software-based virtualization solutions, such as Virtual Server 2005 R2 SP1, with processor and input/output (I/O) enhancements that deliver more performance directly to virtual machines through an approach called *hardware-assisted virtualization*. For more information on Intel Virtualization Technology, see [Intel Virtualization Technology Support](#_Intel_Virtualization_Technology_1) in the Virtual Server 2005 R2 SP1 section later in this document.



Figure Hosted Backup infrastructure: Each group of protected computers and its associated DPM server is on its own customer Active Directory domain (colored yellow, blue, and red, respectively)

#### Storage and Network Isolation

Virtual Server ensures that each virtual machine running DPM is completely isolated from an operating system and data perspective. However, you should also isolate the individual DPM workloads from the storage and network perspectives. Isolate the storage for each DPM virtual machine by ensuring that each DPM machine accesses separate Logical Unit Numbers (LUNs)—separate disks or volumes in a storage disk set.

Isolate the network by ensuring that your router provides the customer only a view into the single DPM virtual machine that protects their infrastructure, but not into the rest of your segment or the other virtual machines.

#### Storage Type Considerations

The sheer volume of storage required to back up your customers’ data will necessitate a storage area network (SAN), network-attached storage (NAS), or direct-attached storage (DAS) appliance of some kind. However, because the virtual machines running your DPM servers cannot interact with the host bus adapters (HBAs) of high-speed interconnects such as Fibre Channel, you must use iSCSI or an Ethernet-based NAS appliance as your mass storage method for this scenario. If you use an iSCSI appliance, you will need to install an iSCSI initiator; instructions are provided in [Appendix E](#_Appendix_E:_Install). You will need to learn the specifics of the iSCSI target on your mass storage solution from your storage vendor.

#### Bandwidth Considerations

Over the network, DPM can only synchronize the data as fast as it can come from your customers’ production sites. There is a balance between the communications cost and the latency of the data. The specifics and the variables that go into this balance are too varied and numerous to be fully discussed in this guide. You will need to work with your ISP and your customers to arrive at this balance over time.

In order to help with this process, this cookbook will introduce you to the network bandwidth throttling, data compression, and backup scheduling functionality in DPM. Whatever the bandwidth realities you have to work with between your customers’ production sites and the DPM servers you are hosting for them, this functionality can help you best use the bandwidth available.

Depending on your network configuration, you may need to perform firewall configuration to enable communication between DPM, the file servers, and the domain controllers. To help with firewall configuration [Appendix B](#_Appendix_B:_) provides details about some of the protocols and ports used by DPM.

### Virtual Server 2005 R2 SP1

Virtual Server provides for the isolation of each server running DPM and makes it possible for those servers to be attached to customer domains. In this section, we will outline the requirements and considerations for this powerful technology.

#### Virtual Server 2005 R2 Glossary

Here are some of the basic terms concerning virtual machines in general and Virtual Server in particular that you will encounter repeatedly in this cookbook.

##### guest operating system

The operating system running on a virtual machine.

##### host computer

The physical computer running the Virtual Server service.

##### Internet small computer system interface (iSCSI)

A network protocol standard that allows the high-speed, parallel SCSI to transfer data by using the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol suite. In the context of Virtual Server, the iSCSI protocol standard provides virtual machines with a high-speed data connection to mass storage apparatuses.

##### logical unit number (LUN)

A logical partition (or volume) of a set of connected storage disks.

##### storage area network (SAN)

A set of interconnected devices (such as disks and tapes) and servers that are connected to a common communication and data transfer infrastructure such as iSCSI.

##### virtual hard disk

For Virtual Server and Virtual PC, a file, referred to as a .vhd file, which provides storage for a virtual machine. The .vhd file can reside on any storage topology that the host operating system can access, including external devices, storage area networks, and network-attached storage.

##### virtual machine

Essentially a computer within a computer, implemented in software. A virtual machine emulates a complete hardware system, from processor to network card, in a self-contained, isolated software environment, enabling the simultaneous operation of otherwise incompatible operating systems. Each operating system runs in its own isolated software partition.

##### Virtual Machine Additions

Software drivers that maximize performance and provide a better user interface (UI) experience within a virtual machine. Virtual Machine Additions are available for the following guest operating systems:

* Windows Server 2003 R2 (all versions)
* Windows Server 2003 (all versions)
* Windows XP (all versions)
* Microsoft® Windows® 2000 Server
* Microsoft® Windows® 2000 Professional
* Microsoft® Windows® Millennium Edition (ME)
* Microsoft® Windows® NT Server 4.0 with Service Pack 6a (SP6a)
* Microsoft® Windows® 98
* Microsoft® Windows® 95

##### Virtual Machine Remote Control (VMRC)

A feature of Virtual Server that enables a running virtual machine to be managed remotely.

#### Virtual Server 2005 R2 System Requirements

The server hosting your DPM virtual machines should conform to the following requirements and recommendations:

Table Requirements for the server hosting your DPM virtual machines

|  |  |
| --- | --- |
| **Minimum CPU speed** | 550 MHz |
| **Recommended CPU speed** | 1.0 GHz or higher |
| **Processor information** | Intel Celeron, Pentium III, Pentium 4, Xeon, or Core 2 Duo |
| **Supported host operating systems** | * Windows Server 2003 Standard Edition, Enterprise Edition, Datacenter Edition, or later versions * Windows Server 2003 Standard x64 Edition, Enterprise x64 Edition, Datacenter x64 Edition, or later versions * Windows Small Business Server 2003 Standard Edition or Premium Edition * Windows XP Professional SP2 or later (for non-production use only) |
| **Minimum RAM** | 256 MB (additional memory needed for each guest operating system) |
| **Required available hard-disk space** | 2 GB (additional disk space needed for each guest operating system) |
| **Other processor support** | AMD Opteron, Athlon, Athlon 64, or Athlon X2 |

**Note:** For this scenario, Virtual Server 2005 R2 SP1 should be installed on editions of Windows Server 2003 and Windows Server 2003 R2 for production purposes. Installation on Windows Small Business Server 2003 or Windows XP Professional SP2 is acceptable for test purposes or for purposes of evaluating the deployment and configuration steps outlined in this cookbook.

#### Licensing Considerations

The license for Windows Server 2003 Enterprise Edition, Windows Server 2003 Enterprise x64 Edition, or later versions on the server hosting your DPM virtual machines enables you to run up to four instances of Windows Server 2003 Standard Edition, Enterprise Edition, or later versions as the operating systems for those virtual machines, at no extra cost.

The license for Windows Server 2003 Datacenter Edition, Windows Server 2003 Datacenter x64 Edition, or later versions on the server hosting your DPM virtual machines enables you to run an unlimited number of instances of Windows Server 2003 Standard Edition, Enterprise Edition, Datacenter Edition, or later versions as the operating systems for those virtual machines, at no extra cost.

#### Intel Virtualization Technology Support

Service Pack 1 (SP1) for Virtual Server 2005 R2 includes a new feature that takes advantage of the hardware assistance for virtual machines provided by multi-core Intel Xeon processor-based servers through Intel Virtualization Technology.

Virtual Server takes advantage of this hardware assistance by controlling the virtual machine-specific operations of the processor, thereby allowing the virtual machine to run processor operations at the privilege level that the processor expects. These integrated features give virtualization software the ability to take advantage of offloading workload to the system hardware, enabling more streamlined virtualization software stacks and "near native" performance characteristics. In addition, Quad-Core Intel Xeon processor servers with virtualization hardware assistance offer additional application headroom, memory flexibility, and increased security for virtual and dedicated environments.

The performance improvements of virtual machines running on Virtual Server 2005 R2 SP1 with hardware assistance from Intel Virtualization Technology provide direct performance benefits. In this deployment scenario, for example, the increased performance makes running several DPM virtual machines on a single physical server possible, while maintaining performance.

# 

### Data Protection Manager 2007

Because you are running DPM on virtual machines, you have fewer system requirements to worry about for your DPM deployments. DPM is designed to run on a dedicated, single-purpose server—for example, a DPM server must not be a domain controller or an application server. Running as they are on dedicated virtual machines, these requirements for your DPM servers will not be a problem for you.

You will need to take into careful consideration the total memory and host server hard drive space requirements for all of the DPM virtual machines. The requirements and recommendations for the components of each DPM virtual machine break down as follows:

Table Individual DPM virtual machine requirements and recommendations

| **Component** | **Requirement** | **Recommendation** |
| --- | --- | --- |
| **Memory** | 512 MB RAM | 1 GB RAM |
| **Disk space for DPM virtual hard disks** | * System drive: 100 MB * Program files drive: 160 MB * Database files drive: 900 MB   **Total DPM virtual hard drive: 1,160 MB** | N/A |

**Note:** Because the multiple virtual hard disks of a virtual machine are generally hosted on the same physical host hard disk, DPM servers running on virtual machines do not improve performance by splitting their different drives between separate physical volumes. For this reason, this cookbook will have you create only two virtual hard disks for each virtual instance of a DPM server: one for the system, program, and database files, and one for the protected customer data files.

For example, in terms of memory, running four DPM virtual machines would require at least 2.3 GB RAM: 2 GB for the four instances of DPM running on the virtual machines, and 256 MB for Virtual Server (this figure does not take into account the memory needed by the operating system on the host server itself). The recommended memory on a server hosting four virtual machines running DPM would be closer to 5 GB RAM—4\*1 GB recommended for DPM virtual machines + 256 MB RAM for Virtual Server and additional memory for host server operating system.

Four virtual machines running DPM would require at least 4.6 GB of hard drive space on the host server—(100 MB+160 MB+900 MB)\*4. This does not include the mass storage space for protected customer data.

For the protected data storage pool disk space, DPM requires equal to 1.5 times the size of the protected data. However, Microsoft recommends having a storage pool two to three times the size of the customer data that you are protecting. For performance and size reasons, the virtual hard disk housing the protected data storage pool should reside on your SAN, NAS, or DAS appliance.

#### Data Protection Manager 2007 Glossary

Here are some of the basic terms concerning DPM 2007 that you will encounter repeatedly in this cookbook.

##### archive

The process by which an administrator copies the contents of the DPM server to tape by using tape backup software. Archiving the replicas provides for long-term storage and access to protected data. Archiving the DPM database and the Report database provides for restoring the DPM server in the event of disaster.

##### autodiscovery

The daily process by which DPM automatically detects new or removed servers on the network and discovers changes to protected file servers, such as the addition, removal, or renaming of shares and volumes.

##### consistency check

The process by which DPM checks for and corrects inconsistencies between a protected volume and its replica. A consistency check is performed only when normal mechanisms for recording changes to protected volumes, and for applying those changes to replicas, have been interrupted.

##### data source

A share, volume, folder, or file that is a member of a protection group.

##### DPM Administrator Console

A Microsoft® Management Console (MMC) snap-in that provides access to the administrative functions of DPM. DPM Administrator Console allows administrators to configure data protection, perform data recovery operations, and monitor and report on these activities.

##### DPM database (DPMDB.mdf)

The Microsoft® SQL Server™ database that stores DPM settings and configuration information.

##### DPM File Agent

Software, installed on a file server, that records changes to protected data in a synchronization log, and transfers the log from the file server to the DPM server.

##### end-user recovery

A feature that enables an end user to independently recover data by retrieving a shadow copy. This feature requires the shadow copy client software.

##### network bandwidth throttling

A performance optimization in DPM that limits the percentage of network bandwidth that protection and recovery jobs can consume.

##### on-the-wire compression

A performance optimization in DPM that reduces the size of data transferred during replica creation and synchronization, thereby increasing the rate of data throughput without negatively affecting network performance.

##### protection

In DPM, the process of protecting data from loss or corruption by centrally creating and maintaining replicas and shadow copies of the data. DPM is designed to provide short-term disk-based backup, to support rapid and reliable recovery of data.

##### protection group

A collection of data sources that share the same protection configuration and schedule.

##### protection group member

A data source within a protection group. A protection group member can be a share, volume, or folder.

##### recovery

In DPM, the process by which an administrator or end user recovers previous versions of shares, volumes, folders, or files from the shadow copies on the DPM server.

##### recovery collection

The aggregate of all recovery jobs associated with a single recovery operation.

##### replica

A complete copy of the protected data on a single volume. Each volume in a protection group is associated with a replica on the DPM server.

##### replica creation

The process by which a full copy of data sources, selected for inclusion in a protection group, is transferred to the DPM storage pool. The replica can be created over the network from live data on the file server or from a tape backup system. Replica creation is an initialization process that is performed for each volume when the volume is added to a protection group.

##### Report database (ReportServer.mdf)

The SQL Server database that stores DPM reporting information.

##### restore

In DPM, the process by which an administrator retrieves a protected file or rebuilds a DPM server by using data that has been archived to disk or tape.

##### shadow copy

A point-in-time copy of files and folders that are stored on the DPM server. Shadow copies are sometimes referred to as snapshots.

##### shadow copy client software

Client software that enables an end user to independently recover data by retrieving a shadow copy.

##### storage pool

A set of disks that store replicas, shadow copies, and transfer logs for protected data.

##### synchronization

The process by which DPM transfers the synchronization log from the file server to the DPM server, and applies the changes stored in the log to the replica of the protected volume.

# Section 1: Install and Configure Virtual Server

Setting up Virtual Server consists of two steps—installing Microsoft® Internet Information Services (IIS), and installing Virtual Server. The instructions in this section will also lead you through delegating a given user’s credentials (to allow remote connections to the Virtual Server Administration Website) and through enabling Virtual Server to delegate the logged-on user’s credentials to another computer (so that Virtual Server can access data on other computers, such as disk images).

Steps covered in this section:

[Install IIS by using the Configure Your Server Wizard 16](#_Toc171320812)

Internet Information Services is a prerequisite for installing Microsoft Virtual Server. Microsoft Virtual Server uses a Web-based management console that depends on the Internet Information Server World Wide Web service.

[Install Virtual Server 2005 R2 SP1 17](#_Toc171320813)

The installation process will automatically set up the Virtual Server Administration Website, and also let you make the exceptions necessary for the computers that you will eventually protect, to access the DPM virtual machine across Windows® Firewall.

[Create a virtual machine 19](#_Toc171320814)

Here you will create the virtual machine on which DPM will run.

[Allow Virtual Server to delegate the credentials of the logged-on user to another computer 25](#_Toc171320815)

Allowing this delegation permits Virtual Server to access guest operating system installation files that may be stored on another computer.

[Install the guest operating system from a startup CD or image file 26](#_Toc171320816)

The virtual machine that you have created is analogous to a physical server that you have just taken out of the box; you will need to install an operating system on it before you can install DPM.

[Install Virtual Machine Additions 27](#_Toc171320817)

Virtual Machine Additions improves mouse cursor tracking and control, and also greatly improves overall performance of the guest operating system on the DPM virtual machine.

[Allow the Virtual Server host computer to delegate a user's credentials to the Virtual Server service 28](#_Toc171320818)

Allowing this delegation permits authorized users to access the Virtual Server Administration Website from remote workstations. If you do not delegate a user’s credentials to the virtual server service, then only local administration will be possible.

#### Install IIS by using the Configure Your Server Wizard

You must install the World Wide Web Service component of IIS so that you can use the Administration Website to manage Virtual Server. If you are following along in a test environment, do this on the **HOST\_1** and **HOST\_2** servers.

1. From the **Start** menu of the physical computer that will run the Virtual Server service, select **Programs** > **Administrative Tools** > **Manage Your Server**.
2. Under **Managing Your Server Roles**, click **Add or remove a role**.
3. Read the preliminary steps in the **Configure Your Server Wizard**, and then click **Next**.
4. Under **Server Role**, click **Application server (IIS, ASP.NET)**, and then click **Next**.

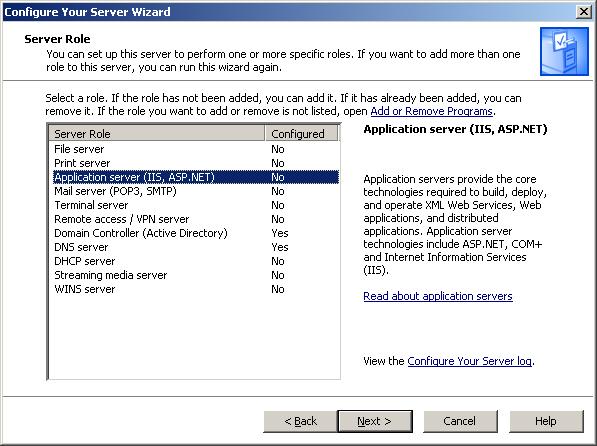


Figure Select Application Server in Configure Your Server Wizard

**Note:** By default, the wizard installs and enables IIS, COM+, and DTC. In addition, the Configure Your Server Wizard enables Microsoft® ASP.NET by default.

1. Read the summary, and then click **Next**. You will need the installation medium (CD, iso file, or network file share) for the operating systems of this computer to complete this step.
2. Complete the wizard, and then click **Finish**.

#### Install Virtual Server 2005 R2 SP1

You are now ready to install Virtual Server 2005 R2 with Service Pack 1 on the physical computer that will host your DPM virtual machine. In your test environment, do this on the **HOST\_1** and **HOST\_2** servers.

1. Start Microsoft Virtual Server 2005 Setup (Setup Wizard) from the Virtual Server 2005 CD-ROM.

**Note:** If you start the Setup Wizard manually, be sure to use Setup.exe.

1. Proceed through the wizard until you reach the **Setup Type** page.
2. On the **Setup Type** page, click **Complete**, which installs Virtual Server by using the default configuration, and then click **Next**.

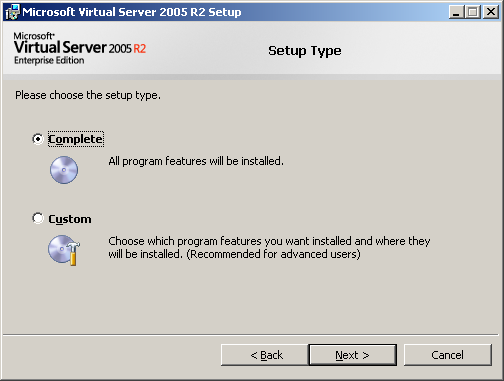


Figure 4 Virtual Server setup wizard, Setup Type page

1. On the **Configure Components** page, either accept the default Website port value of 1024, or type a new value for the port. In this example we will use the default value.

You have an additional choice to make:

* + If you plan to always run the Administration Website as the authenticated user—to access resource files only on the local computer—accept the default setting **Configure the Administration Website**.
  + If you plan to access resource files on a remote computer, select **Configure the Administration Website to always run as the Local System account**.

To allow the most flexibility in accessing resources (particularly in a production environment), we will select **Configure the Administration Website to always run as the Local System account,** and then click **Next**.

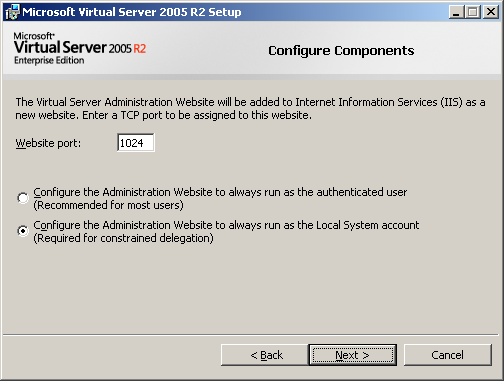


Figure 5 Virtual Server setup wizard, Configure Components page 1

**Note:** If you are installing the Administration Website on a computer running Windows XP SP2, the default Website port is 80.

1. On the second **Configure Components** page, leave the **Enable Virtual Server exceptions in Windows Firewall** check box selected.

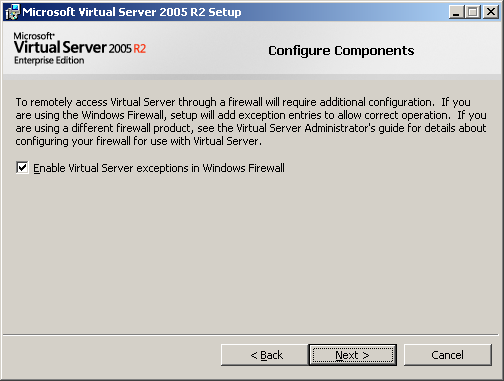


Figure 6 Virtual Server setup wizard, Configure Components page 2

With **Enable Virtual Server exceptions in Windows Firewall** selected, setup adds an exception for the Virtual Server service (vssrvc.exe) to every port on the computer. It also adds an exception to port 135 for Remote Procedure Call, which is required for the Distributed Component Object Model (DCOM)-based services upon which Virtual Server depends.

1. Click **Install** to begin the installation.
2. When the installation is complete, the **Setup Complete** page appears. Click **Finish** to close the page and exit the Setup Wizard.

**Note:** You can close the **Installation Summary** page that opens in Windows® Internet Explorer® when the installation is complete.

#### Create a virtual machine

Now that Virtual Server is installed, we can create the virtual machine that will run DPM. In your test environment, do this on the **HOST\_1** server.

1. If it is not already open, open the Virtual Server Administration Website. On the desktop of the computer running the Virtual Server service, click **Start** > **All Programs** > **Microsoft Virtual Server** > **Virtual Server Administration Website**.
2. In the left column of the Virtual Server Administration Website, under **Virtual Machines**, click **Create**.

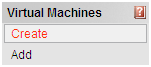


Figure 7 Create new virtual machine

1. In the **Virtual machine name** field, type a descriptive name for the virtual machine. If you do not want the virtual machine (.vmc) file to be created in the default configuration folder, specify a fully qualified path to the location where you want to create the virtual machine. The example provided in Figure 8 is **DPM\_SVR**. Feel free to use it in your own test environment, though it is not necessary to successfully create a virtual machine.

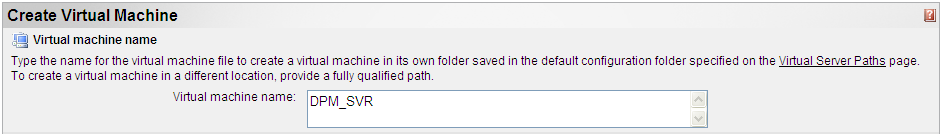


Figure 8 New virtual machine name

1. In the **Virtual machine memory** field, type a value in megabytes for the amount of RAM that is used by the virtual machine. Figure 9 shows **1 GB** of RAM allocated to the virtual machine; this is the minimum that you should commit for a virtual machine running DPM, particularly in a production environment.

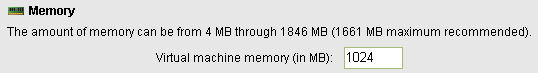


Figure 9 New virtual machine memory

1. In the **Virtual hard disk** section, select the **Create a new virtual hard disk** option. Next, to set the size of the virtual hard disk, specify a value in **Size**, and then select either **MB** for megabytes or **GB** for gigabytes. Because this virtual hard disk is going to house the DPM virtual machine’s system functions and information, it is okay to leave the virtual hard disk’s maximum size at 127 GB.

In the **Bus** drop-down menu, select **SCSI**. This is to improve disk input/output (I/O) performance. IDE is limited to one transaction at a time, regardless of whether the bus is physical or virtual. In this scenario, this means that if you attached both DPM virtual machine virtual hard disks to the IDE adapter, it would be limited to a single transaction for both disks, potentially degrading the DPM virtual machine’s performance in a production environment. By contrast, a SCSI adapter allows for multiple simultaneous transactions, which provides better performance than disks attached to the IDE adapter.

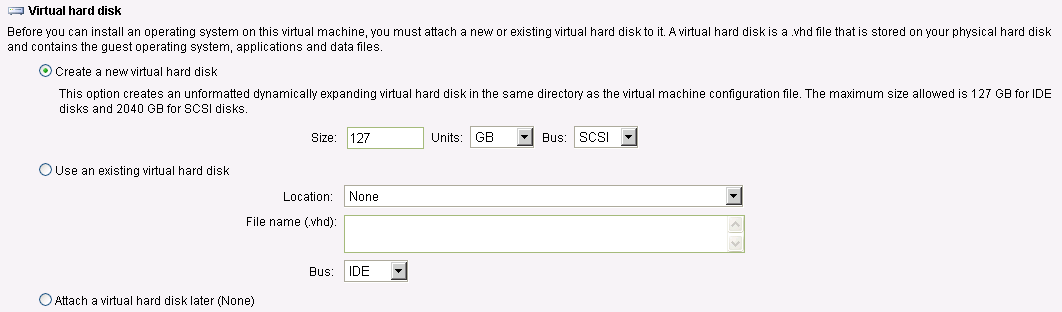


Figure 10 New virtual machine virtual hard disk

There are two other options in the **Virtual hard disk** section that we will not use in the steps laid out in this guide:

* + Select the **Use an existing virtual hard disk** option if you are creating a virtual machine that you want to use an existing .vhd file for its hard disk. If the virtual hard disk (.vhd) file is located in a directory included in Virtual Server Search Paths, you can select the .vhd file from the **Location** drop-down menu. Otherwise, in the **File name (.vhd)** field, type the complete path to the location of the .vhd file.
  + Select the **Attach a virtual hard disk later** optionto create a virtual machine without a virtual hard disk.

1. Under **Virtual network adapter**, select the host computer’s NIC (or the most appropriate one for your needs if you have multiple NICs on the server) from the **Connected to** drop-down menu.

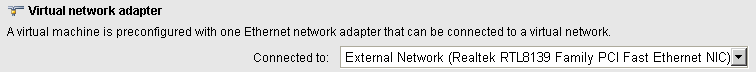


Figure 11 New virtual machine virtual network adapter

**Note:** The last section on this page is Virtual Machine Additions. We will address Virtual Machine Additions in the [Install Virtual Machine Additions](#_To_install_Virtual) section later in this guide.

1. Click **Create**.

**Note:** By default, hardware-assisted virtualization is enabled if it is enabled on the host computer. Support for Intel Virtualization Technology can also be specifically enabled or disabled on a per-virtual-machine basis by toggling the **Enable hardware-assisted virtualization if available** option in the general properties configuration page. However, you should refer to your Intel processor-based host server’s documentation on how to enable Intel Virtualization Technology in the Host system BIOS (if available on your server processor).

In order for DPM to function properly, we now need to create and attach a second virtual hard disk to the DPM virtual machine. This second virtual hard disk will serve as the DPM data protection pool for the computers you will eventually protect.

First we will create the second virtual hard disk independent of the virtual machine.

1. In the left column of the Virtual Server Administration Website, under **Virtual Disks**, point to **Create**, and then **Dynamically Expanding Virtual Hard Disk**.

A dynamically expanding virtual hard disk grows in size each time it is modified. This type of virtual hard disk starts as a 3 KB .vhd file and can grow as large as the maximum size specified when you create it. By selecting this type of virtual hard disk, you will not need to worry about running out of space on the virtual hard disk (so long as there is sufficient space on your mass storage apparatus), which is crucial to backing up your customers’ data.

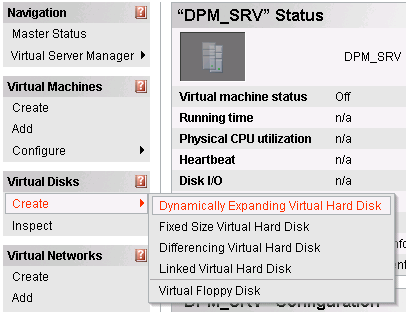


Figure Create new, dynamically expanding virtual hard disk

1. If this is your first time creating virtual hard disks, you will have to enter in the full path for the virtual hard disk in the **Virtual hard disk file name** field. Remember, this location should be on your mass storage device (particularly when doing this in a production environment). In this example we will use the path **S:\Protection\_pools\DPM\_SRV\_pool.vhd**

In the **Size** field, enter **2040**. 2,040 GB is the largest size possible for a Virtual Server virtual hard disk. Generally speaking, you want to allow the virtual hard disk housing the customer protected data to grow to the largest size it can. (However, you must ensure that enough space exists on the mass storage device for all of the data protection virtual hard disks that you will house on it.)

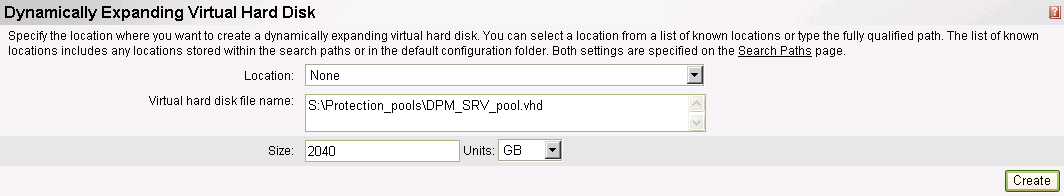


Figure Path and size of second virtual hard disk

1. Click **Create**.

Now we will attach this new virtual hard disk to the virtual machine.

1. In the left column of the Virtual Server Administration Website, under Virtual Machines, point to **Configure**, and then click the appropriate virtual machine. In Figure 14, this is **DPM\_SVR**.

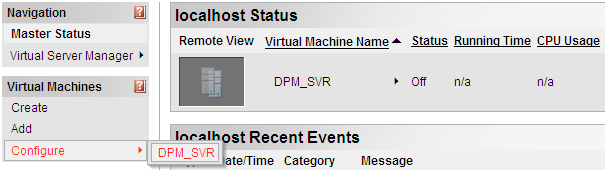


Figure Virtual Machine Administration Website, Configure virtual machine

1. Under **Configuration** for the DPM virtual machine, click **Hard disks**.

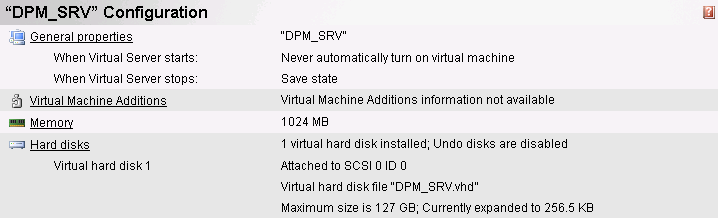


Figure Add additional virtual hard disks

1. Under **Virtual Hard Disk Properties** for the DPM virtual machine, click **Add disk**.

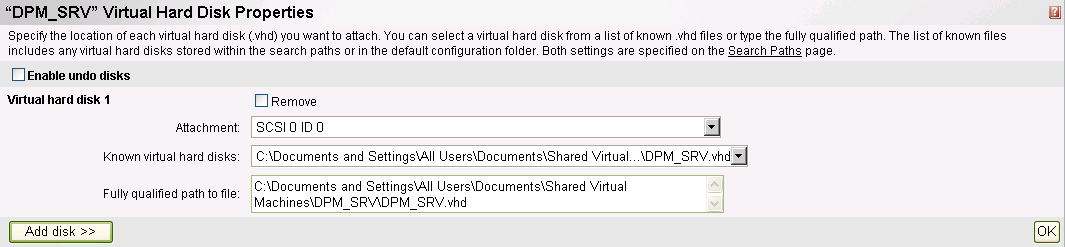


Figure DPM virtual machine virtual hard disk properties

1. From the **Attachment** drop-down menu, select **SCSI 0 ID 1**. (This is the next available virtual SCSI adapter.)   
   In **the Fully qualified path to file** field, enter the path to the virtual hard disk on the mass storage device that you created in step 9. (For example, in the Figure 17 that path is **S:\Protection\_pools\DPM\_SRV\_pool.vhd**.)

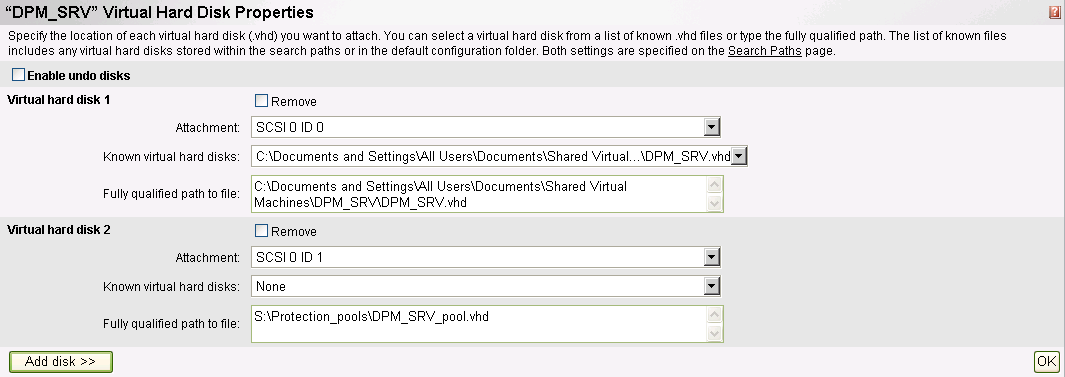


Figure 17 Second DPM virtual machine virtual hard disk

1. Click **OK**.
2. The DPM virtual machine now has both virtual hard disks attached. You are ready to install the operating system on the DPM virtual machine.



Figure DPM virtual machine with both virtual hard disks attached

**Note:** Because DPM requires at least 1.5 times as much space for storage as you have data to protect, a single 2,040 GB virtual hard disk can at most protect 1,360 GB of data. However, Microsoft recommends 2-3 times as much space for storage as you have data to protect, meaning that ideally a single 2,040 GB virtual hard drive would be used to protect 680-1,020 GB of data. The solution to this in a production environment is to create additional virtual hard drives, attach them to the DPM virtual machine (repeating steps 8-15 as many times as necessary), and add these to your storage pool as outlined later in the [Allocate storage for the DPM server](#_To_allocate_storage) section.

#### Allow Virtual Server to delegate the credentials of the logged-on user to another computer

**Note:** If you are following this guide step by step in your test environment, you may not be able to perform this step. This is because **HOST\_1**, the server hosting **DPM\_SRV**, may not be joined to any domain.

This process allows Virtual Server to access installation data on computers other than the computer running the Virtual Server service (that is, the computer hosting the DPM virtual machine). Allowing this delegation is only necessary if you are going to perform a network-based installation of the operating system on the virtual machine you created; you may skip it if you are going to use physical installation media or a local .iso file.

1. On the domain controller of the physical computer that is hosting the DPM virtual machine, open **Active Directory Users and Computers**.

**Note:** This delegation is to facilitate your administration of a service (Virtual Server) running on a physical computer joined to *your* domain. This should not be attempted via any of your customers’ domains.

1. In the console tree, under *DomainName*, click **Computers**. In this case, DomainName refers to the domain to which the computer hosting the DPM virtual machine is attached.
2. Right-click the computer that will host the DPM virtual machine, and then click **Properties**.
3. On the **Delegation** tab, click **Trust this computer for delegation to specified services only**.
4. Click **Use any authentication protocol**.
5. Click **Add**, and then click **Users and Computers**.
6. Type the name of the computer hosting the resource files, and then click **OK**.
7. From the list of available services, select **cifs**, and then click **OK.**

#### Install the guest operating system from a startup CD or image file

The virtual machine that you just created is now analogous to a bare-metal physical server that you just took out of the box. We need to install an operating system on it before we can install DPM on it.

1. If it is not already open, open the Virtual Server Administration Website. On the desktop of the computer running the Virtual Server service, click **Start** > **All Programs** > **Microsoft Virtual Server** > **Virtual Server Administration Website**.
2. In the left column of the Virtual Server Administration Website, under **Virtual Machines**, point to **Configure**, and then click the DPM virtual machine. In this example (Figure 19), this is **DPM\_SVR**.

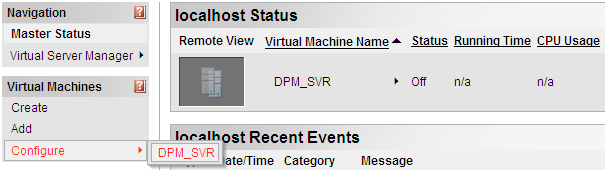


Figure Virtual Machine Administration Website, Configure virtual machine

1. In the **Configuration** section for the DPM virtual machine, click **CD/DVD** and do one of the following:
   * Insert the startup CD for the operating system into the CD drive on the physical computer running the Virtual Server service. On the **CD/DVD Drive Properties** page of the virtual machine that you are configuring, under **Capture**, click **Physical CD/DVD** **drive**. If necessary, select the corresponding CD or DVD drive letter from the drop-down menu.
   * On the **CD/DVD Drive Properties** page of the virtual machine that you are configuring, under **Capture**, click **Known image files**. If the image file containing a startup CD image is located in the default directory **(\Documents and Settings\All Users\Documents\Shared Virtual Machines\**), it is available from the drop-down menu. Otherwise, in the **Fully qualified path to file** field, type the complete directory path to the image file.

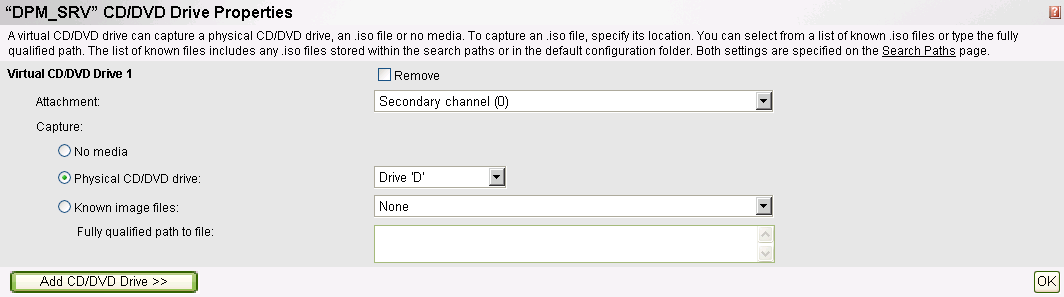


Figure DPM virtual machine CD/DVD drive properties

**Note:** Accessing operating system installation files on a remote computer requires constrained delegation and a software update to the host operating system of the local computer. For instructions, go to [Allow Virtual Server to delegate the credentials of the logged-on user to another computer](#_To_allow_Virtual) earlier in this guide.

1. After you have performed one of these two actions, click **OK**.
2. In the **Status** section for the virtual machine that you are configuring, point to the virtual machine name (**DPM\_SRV** in this example), and then click **Turn On**.



Figure Turn on the DPM virtual machine

1. When the virtual machine is turned on, point to the virtual machine name, and then click **Remote Control**.
2. When you are connected to the virtual machine, follow the instructions provided by the operating system to complete the installation.

If you are following these steps in a test environment, repeat this process of virtual machine creation and guest operating system installation to create the **DC\_SRV** virtual machine on the **HOST\_1** server. Install IIS and Virtual Server on the **HOST\_2** and use these steps to create **PROTECTED\_SRV** and install the guest operating system on it.

**Note:** Only **DPM\_SRV** requires two VHDs. **DC\_SRV** and **PROTECTED\_SRV** only require one.

In your test environment, promote **DC\_SRV** to be a domain controller. Join **DPM\_SRV**, **PROTECTED\_SRV**, and **HOST\_2** to your domain. In this cookbook, we use the example domain of **contoso.com**. You join virtual machines to Active Directory domains in the same way that you join physical computers to domain.

In a production environment, you would join the DPM virtual machine to the customer’s domain.

#### Install Virtual Machine Additions

Virtual Machine Additions is a very important component to running a virtual machine. Virtual Machine Additions improves mouse cursor tracking and control as well as greatly improving overall performance of the guest operating system on the DPM virtual machine.

In your test environment, do this on **DPM\_SRV** (you should also do this on **DC\_SRV** and **PROTECTED\_SRV**, but you will spend most of your time working with **DPM\_SRV**).

**Note:** Prior to installing Virtual Machine Additions, the mouse pointer may appear as a dot on the screen. The mouse still functions correctly; only the display of the pointer is affected.

1. If it is not already open, open the Virtual Server Administration Website. On the desktop of the computer running the Virtual Server service, click **Start** > **All Programs** > **Microsoft Virtual Server** > **Virtual Server Administration Website**.
2. In the navigation pane of the Virtual Server Administration Website, under **Virtual Machines**, point to **Configure**, and then click the appropriate virtual machine.
3. In the **Status** section for the virtual machine that you are configuring, point to the virtual machine name, and then click **Turn On**.
4. When the virtual machine has started, point to the virtual machine name, and then click **Remote Control**.
5. Log on to the virtual machine as an administrator or a member of the Administrators group.
6. When the guest operating system is loaded, press the HOST KEY (by default, the RIGHT ALT key) to release the mouse pointer, and then in the lower-left corner, under **Navigation**, click **Configure *virtual\_machine\_name*** where this is the name of the DPM virtual machine.
7. In the **Configuration** section, click **Virtual Machine Additions**, select the **Install Virtual Machine Additions** check box, and then click **OK**.
8. In the **Status** section for the virtual machine that you are configuring, point to the virtual machine name, and then click **Remote Control**.
9. Click in the **Remote Control** window to return to the guest operating system. The Virtual Machine Additions Installation Wizard will start. Proceed through the wizard.
10. When the wizard is complete, you will be prompted to restart the virtual machine to complete the installation.

#### Allow the Virtual Server host computer to delegate a user's credentials to the Virtual Server service

Allowing this delegation permits users authorized in Active Directory to access the Virtual Server Administration Website from a remote workstation. While being able to do this is a minor issue in a test environment, it is will make your DPM deployment easier to administer if you enable this in a production environment.

1. On the domain controller for the physical server that will host the DPM virtual machine, open **Active Directory Users and Computers**.

**Note:** This delegation is to facilitate your administration of a service (Virtual Server) running on a physical computer joined to your own domain. This should not be attempted via any of your customers’ domains.

1. In the console tree, under *DomainName*, click **Computers**. In this case, DomainName refers to the domain to which the computer hosting the DPM virtual machine is attached.
2. Right-click the Web server (that is, the physical computer on which you installed Virtual Server), and then click **Properties**.
3. On the **Delegation** tab, click **Trust this computer for delegation to specified services only**.
4. Click **Use any authentication protocol**.
5. Click **Add**, and then click **Users and Computers**.
6. Type the name of the computer running the Virtual Server service, and then click **OK**.
7. From the list of available services, hold down the CTRL key while clicking **cifs** and **vssrvc**, and then click **OK**.
8. Repeat as necessary for additional computers hosting Virtual Server-based virtual machines**.**

# Section 2: Install and Configure Data Protection Manager

Now that you have created the DPM virtual machine, you can install the DPM software on it. You can install directly from the installation media, an .iso file, or copy the setup files from a shared network location.

A DPM 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 automatically installs or provides links to install the prerequisite software as part of the integrated DPM installation process.

Steps covered in this section:

[Install DPM prerequisites and DPM 30](#_Toc171321072)

The DPM installer gathers your input at the beginning of the setup process. In addition, the installer verifies prerequisites and installs dependent components that may not already be present, such as Internet Information Server.

[Allocate storage for the DPM server 39](#_Toc171321073)

The storage pool consists of one or more dynamic disk volumes that are used exclusively by DPM to store replicas, recovery points, and logs. Any volumes you use must be dedicated to DPM, but you do not have to dedicate an entire disk to DPM.

[Install the DPM agent on computers to be protected 41](#_Toc171321074)

A protection agent is software installed on a server that tracks changes to protected data and transfers the changes from the protected server to the DPM server. Before you can start protecting data, you must install a protection agent on each of the servers that contain data that you want to protect.

#### Install DPM prerequisites and DPM

The DPM installer has been optimized to gather all user input at the beginning of the setup process. When the interactive portion is complete, the installer verifies prerequisites and installs dependent components that may not already be present, such as Internet Information Server.

DPM includes Microsoft® SQL Server™ 2005 and SQL Server 2005 Reporting Services, allowing them to configure a dedicated SQL Server instance for their internal databases. However, if you already have a suitable SQL Server 2005 installation, you can configure the DPM installer to use your existing deployment.

1. If it is not already open, open the Virtual Server Administration Website. On the desktop of the computer running the Virtual Server service, click **Start** > **All Programs** > **Microsoft Virtual Server** > **Virtual Server Administration Website**.
2. In the navigation pane, under **Virtual Machines**, point to **Configure**, and then click the virtual machine on which you will install DPM. In this example, you will select **DPM\_SRV**.
3. In the **Status** section, point to the virtual machine name (**DPM\_SRV**) and then click **Turn On**.
4. When the virtual machine has started, point to the virtual machine name, and then click **Remote Control**.
5. Log on to the server on which you will install DPM (the virtual machine you created in Section 1), **DPM\_SRV**. Be sure to use a domain user account that is a member of the domain administrators group.

**Note:** You can install DPM by using a local administrator account. However, most configuration tasks require domain user privileges. Microsoft recommends installing DPM by using a domain account that is a member of the local administrators group.

1. Insert the Microsoft Data Protection Manager V2 Beta2 product DVD in the DVD-ROM drive. Within Virtual Server, click **Edit Configuration**, click on the **CD/DVD** section, and ensure that the physical drive where you inserted your DVD is selected. If the Setup wizard does not start automatically, double-click **Setup.exe** in the root folder of the DVD.

If you are installing DPM from a network share instead, navigate to the installation share, and then double-click **Setup.exe** in the root folder of the share. You can do this by clicking **Start > Run**,and then typing the location of the bits.

1. On the **Microsoft System Center Data Protection Manager V2 Beta2** screen, click **Install Data Protection Manager**.
2. 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**.

**Note:** DPM installs the Microsoft® .NET Framework version 2.0 if it has not already been installed.

1. On the **Welcome** page, click **Next**. DPM begins a prerequisites check for all required hardware and software.

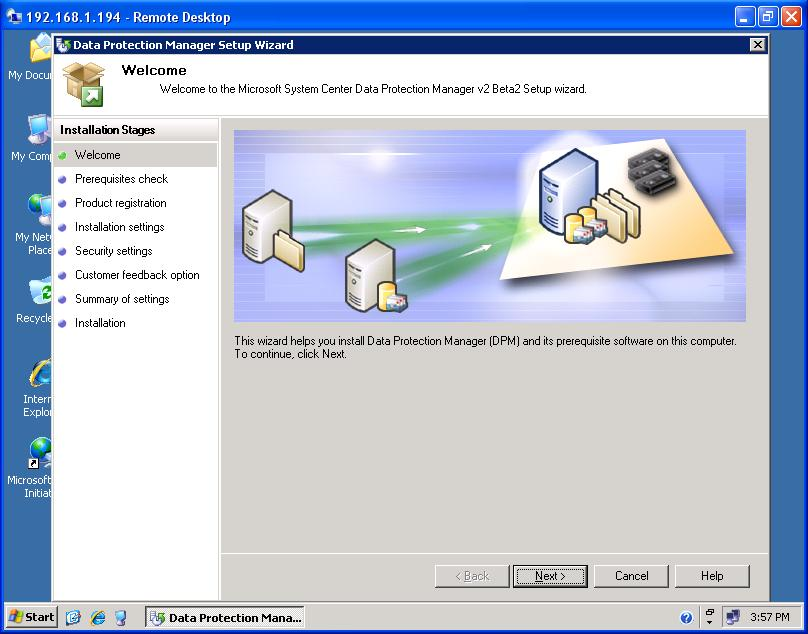


Figure Data Protection Manager Setup Wizard, Welcome page

1. On the **Prerequisites Check** page, wait while Setup checks the system to verify that it meets software and hardware requirements. If all required components are present, Setup displays a confirmation. Click **Next** to continue.

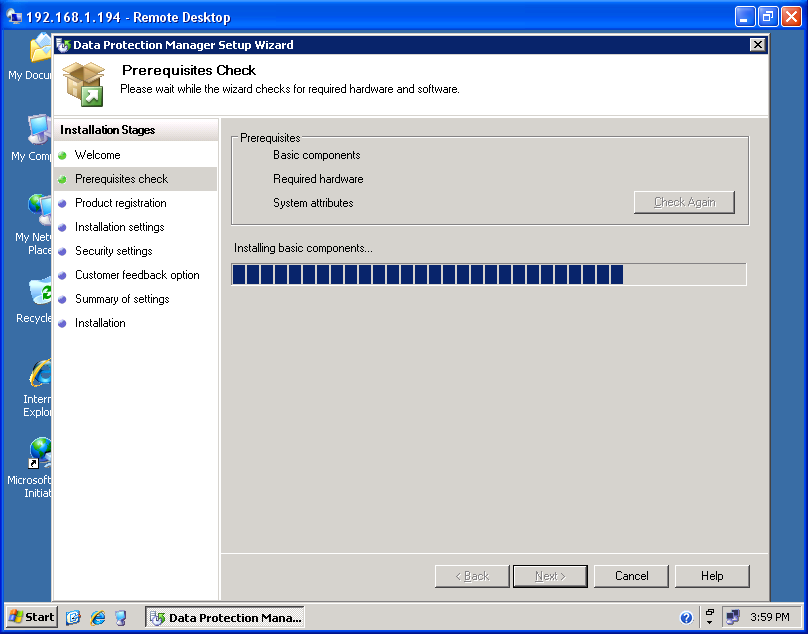


Figure Data Protection Manager Setup Wizard, Prerequisites Check page

**Note:** If one or more required or recommended components are missing or noncompliant, Setup displays a warning or error message. A 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. An error indicates that a required component is missing or noncompliant. You must exit the wizard and resolve the error before you can continue with the installation.

1. On the **Product Registration** page, enter your registration information, and then click **Next**.

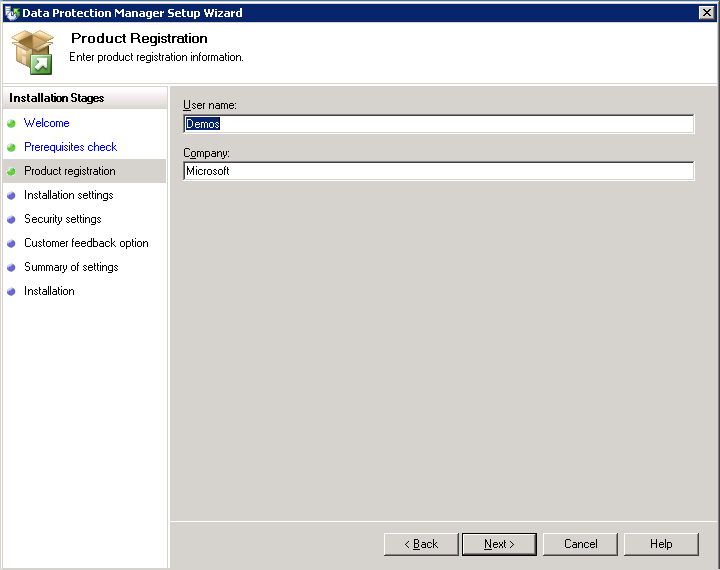


Figure Data Protection Manager Setup Wizard, Product Registration page

1. On the **Installation Settings** page, in the **DPM Program Files** section, accept the default folder, or browse to the folder in which you want to install DPM. In this example, we will use the default folder.

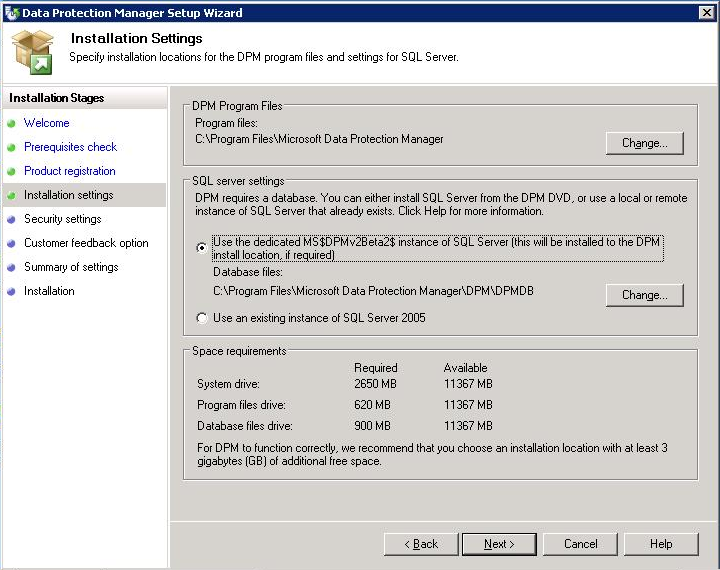


Figure Data Protection Manager Setup Wizard, Installation Settings page

**Note:** You can install DPM only on a local drive, and 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 be installed to a subfolder of the Program Files folder.)

1. On the **Installation Settings** page, in the **SQL Server Settings** section, select the **Install SQL Server from the DPM DVD** option, accept the default SQL Server database location or browse to the location of the DPM database, and then click **Next**. In this example, we will use the default location.
2. The Space requirements section of the page 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. In this example, we will use the default location.

* To change the specified installation locations, click **Change**.
* To accept the specified installation locations, click **Next**.

1. On the **Security Settings** page, specify a strong password for the Microsoft$DPM$Acct account, and then click **Next**.

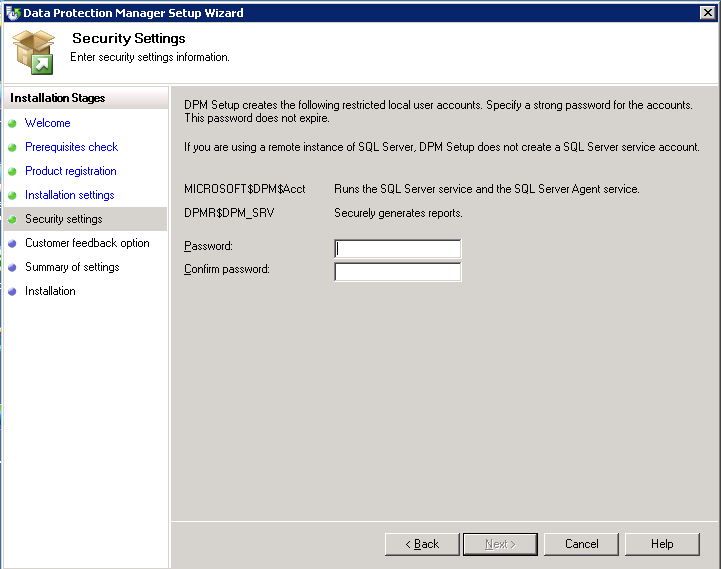


Figure Data Protection Manager Setup Wizard, Security Settings page

**Note:** For security purposes, during installation, DPM Setup creates the Microsoft$DPM$Acct account, which the DPM Writer service uses. DPM sets the system administrator (SA) password for SQL Server to the same password that you specify for the Microsoft$DPM$Acct 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. The password that you specify for these accounts does not expire.

1. On the **Customer Experience Improvement Program** page, if you want to provide Microsoft with information about your hardware and software configurations and usage patterns, click **Yes, I want to participate anonymously in this program**.

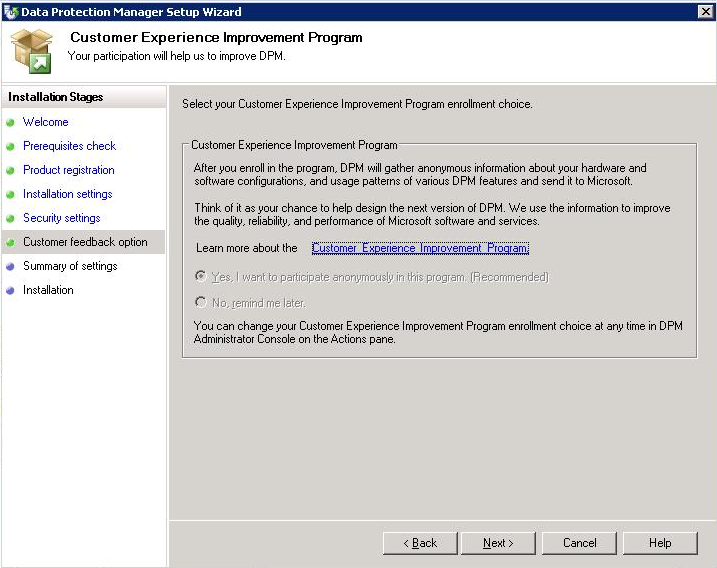


Figure Customer Experience Improvement Program page

**Note:** While participating in the DPM beta program, the only choice you can select is to participate in the Customer Improvement Program.

1. 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**.

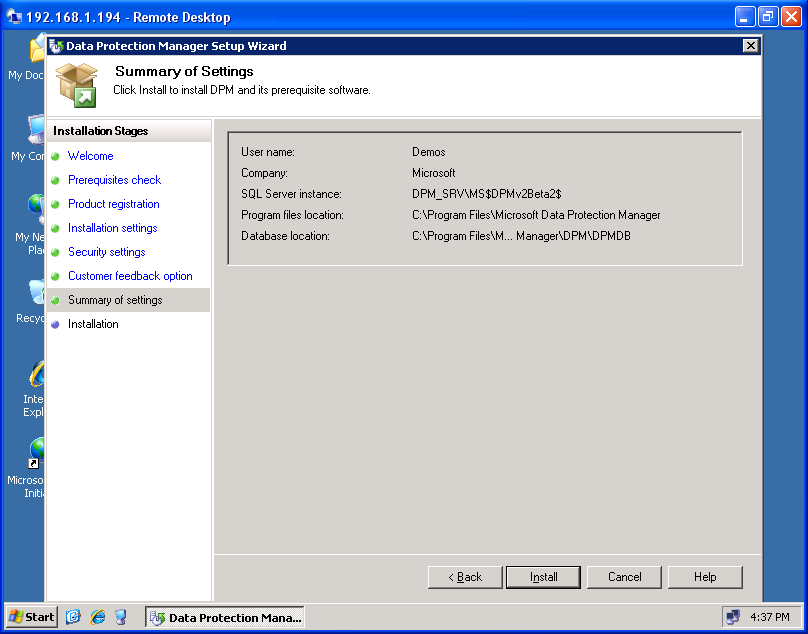


Figure Data Protection Manager Setup Wizard, Summary of Settings page

1. When prompted, insert the **Windows Server 2003** product CD, and then click **OK**. Set up prompts for the Windows Server 2003 CD because IIS and SIS are not already installed on the DPM server.



Figure Insert CD

1. When installation is complete, the **Installation** page displays the installation status. Click **Close**.

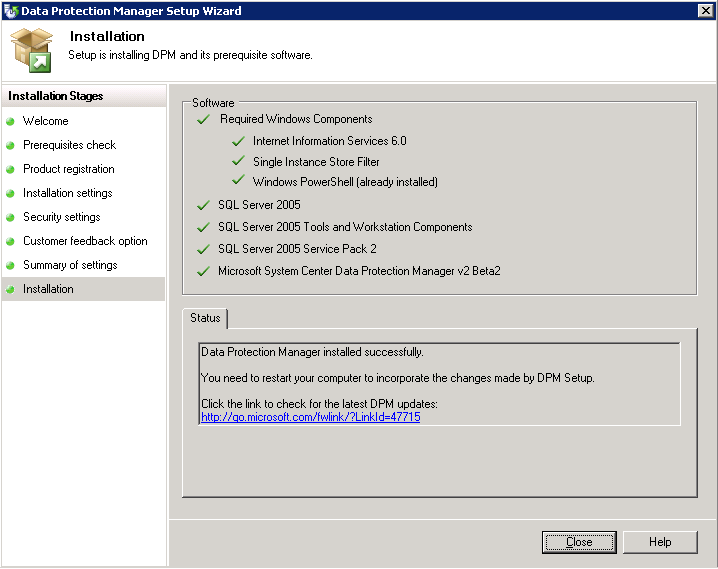


Figure Data Protection Manager Setup Wizard, Installation page

#### Allocate storage for the DPM server

The next step in deploying DPM is to create the storage pool. With DPM installed on a virtual machine, your storage pool will consist of one or more virtual hard disks residing on your mass storage device (such as the second virtual hard drive you created when you created the DPM virtual machine.)

**Note:** Virtual machines created with Virtual Server can only attach mass storage via Ethernet (including NAS, iSCSI SAN, or other appliances.) If you use iSCSI as your storage device, you will need to install an iSCSI initiator; see [Appendix E](#_Appendix_E:_Install) for instructions.

1. Open DPM Administrator Console (**Start**, **All Programs**, **Microsoft System Center Data Protection Manager**), click **Management** on the navigation bar, and then click the **Disks** tab.

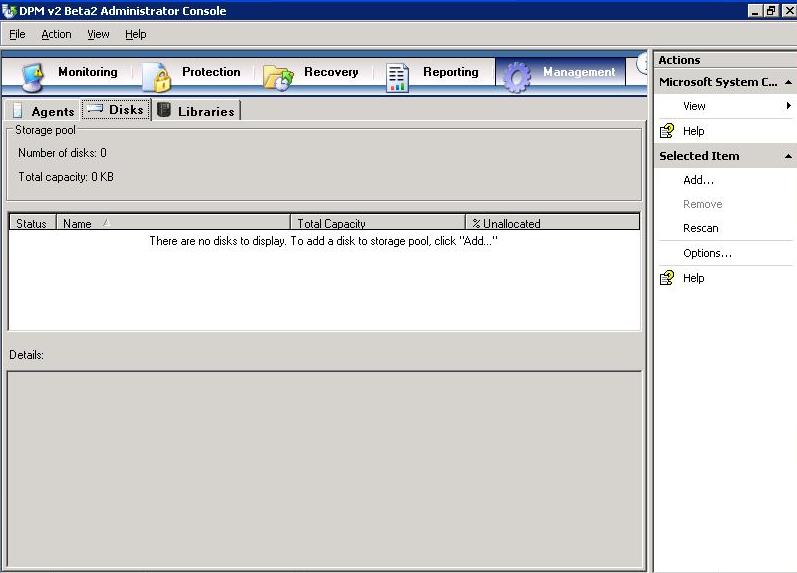


Figure Administrator Console, Management tab

1. To add disks to your DPM storage pool, click **Add** in the **Actions** pane. The example in Figure 32 shows adding the second virtual hard disk created earlier in this cookbook to the storage pool.

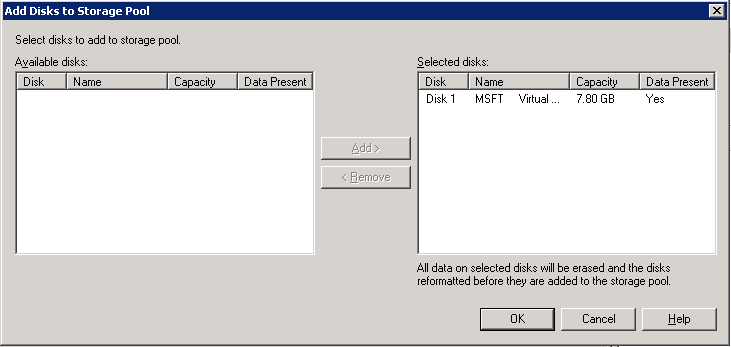


Figure Add Disks

1. In the **Add Disks to Storage Pool** window, you will see any available disks that are usable by DPM. Highlight one or more disks in the **Available disks** field, and then click **Add** to move them to the **Selected disks** field. When you have selected the desired disks, click **OK** to allocate these disks to the DPM storage pool.

#### Install the DPM agent on computers to be protected

A *protection* a*gent* is software installed on a server that tracks changes to protected data and transfers the changes from the protected server to the DPM server. Before you can start protecting data, you must install a protection agent on each of the servers that contain data that you want to protect. After the protection agent is installed on a server, the server is referred to as an unprotected server in DPM Administrator Console in the Management task area. The data sources on the server are not protected until you add them to a protection group.

**Note:** The Beta 2 release of DPM 2007 provides the license for only one protection agent. This means that while using the beta version of DPM 2007, each DPM server can only protect one computer.

After installation, DPM will scan Active Directory to find servers that it can protect. Simply choose the servers that you want to protect from the list that is presented in the Protection Agent Installation Wizard. You will need to deploy the DPM protection agent on the servers to be protected. You can install the DPM protection agent through DPM Administrator Console, System Center Configuration Manager 2007, Systems Management Server 2003, Active Directory Group Policy, or from the command line on the production server to be protected.

1. Turn on and log on to the virtual machine on which you have installed DPM (**DPM\_SRV**), if you have not already done so.
2. Open DPM Administrator Console: **Start > All Programs > Microsoft System Center Data Protection Manager**.
3. Click **Management** on the navigation bar, and then click the **Agents** tab. In the **Actions** pane, click **Install**. The Protection Agent Installation Wizard appears.

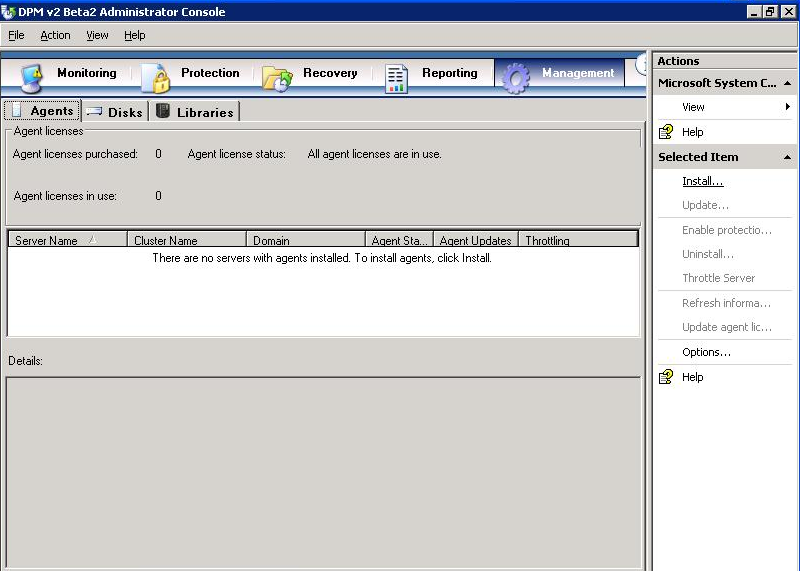


Figure Administrator Console

1. The first time that you use the wizard, DPM assembles a list of potential servers from Active Directory. The daily autodiscovery process creates a stored list of servers that is used for subsequent installations. On the **Select Servers** page, select up to the hard-coded number of servers (50), and then click **Add**. Here we will choose **PROTECTED\_SRV**. You can also specify a server by typing its name in the **Server** name box and clicking **Add**. When you are finished adding servers, click **Next.**

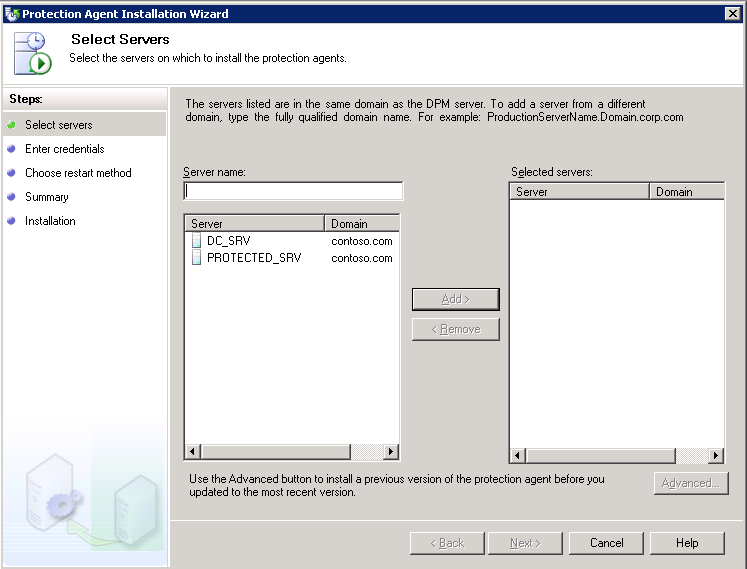


Figure Protection Agent Installation Wizard, Select Servers page

**Note:** Windows Firewall is included with all editions of Windows Server 2003 SP1 and later versions, as well as with SP2 for Windows XP and with Windows Vista™. If Windows Firewall is enabled on a computer that you want to protect, you must disable the firewall before you can install the DPM File Agent. After you have installed the file agent, configure Windows Firewall by opening port **135** to TCP traffic coming from the protected computer to the DPM server and then specifying the file agent (**Data Protection Manager\DPM\bin\MsDpmFsAgentCA.exe**) as an exception to the Windows Firewall policy.

1. On the **Enter Credentials** page, type the user name and password for the domain account to use during the agent installation. Due to the nature of the hosted backup solution, this account must be a member of the domain administrators group on all selected servers. Click **Next**.

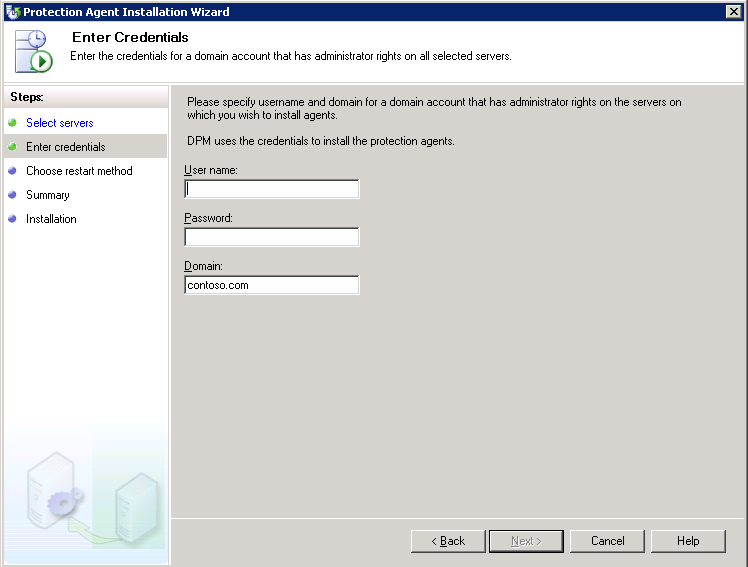


Figure Protection Agent Installation Wizard, Enter Credentials page

1. On the **Choose Restart Method** page, click the option indicating how you want the selected server to restart when the protection agent is installed. If you are following this scenario in your test environment, select **Yes, Restart the selected servers after installing the protection agents** and click **Next.**

(In your production environment, remember that nothing will be protected until you have restarted the machine. If you do not restart now, be sure to do so later.)

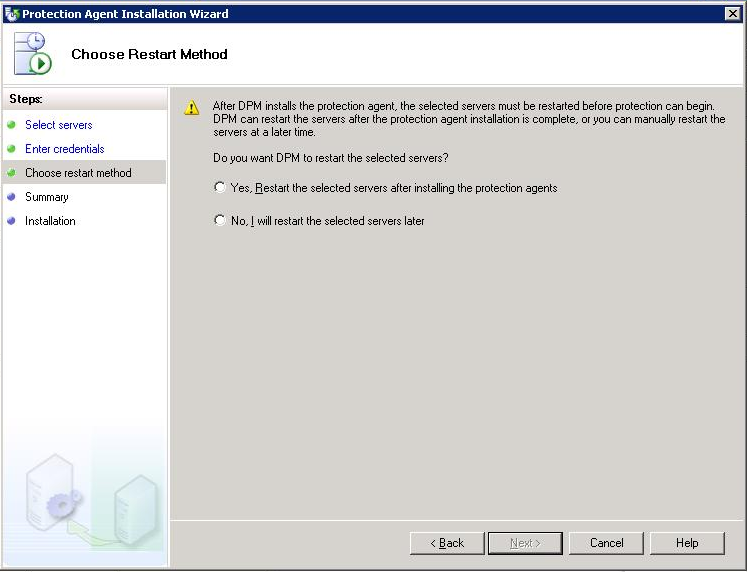


Figure Protection Agent Installation Wizard, Choose Restart Method page

**Note:** If any of the servers that you selected are clustered servers, an additional **Choose Restart Method** page appears that enables you to select the method that you will use to restart the clustered servers. 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 may 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 or a Windows Server cluster. You must manually restart a server in clusters such as these.

1. On the **Summary** page, review the summary, and then click **Install Agents** to proceed with the installation.
2. The results of the process appear on the **Task** tab of the wizard. You can monitor the installation progress in the **Management** task area on the **Agents** tab in DPM Administrator Console. If the installation is unsuccessful, you can view the alerts in the **Monitoring** task area on the **Alerts** tab.
3. After the installation is complete, click **Close**.

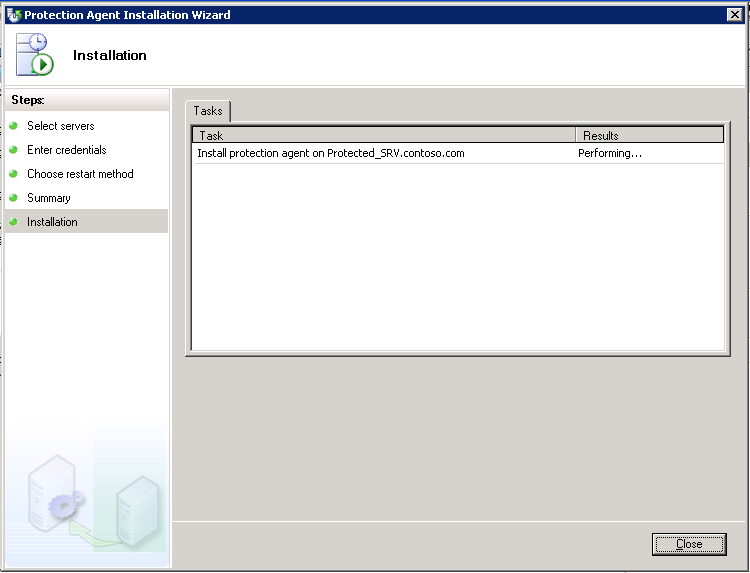


Figure 37 Protection Agent Installation Wizard, Installation page

# Section 3: Back Up Data

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 as members.

Not all data is created equal, even when it is of the same broad category. To efficiently use your storage, and both your and your customers’ bandwidth, you must work with your customers to design a set of recovery goals that takes into account the nature of each protected data source. To define these goals, you must first determine your customers’ desired synchronization frequency, recovery point schedule, and retention range.

The **synchronization frequency** determines how often the DPM agent will capture snapshots of your data and transmit the changes to the DPM server. This value reflects how much data a given customer is willing to lose from this data source if there is an outage or disaster. Think of the synchronization frequency as how often your customer wants incremental backups of their data.

The **recovery point schedule** determines how often DPM creates discrete recovery points for the protected data. The DPM recovery point schedule is conceptually similar to the opportunities that your customers have to recover their data by using a traditional backup application. If you perform a weekly full backup and a daily incremental backup for a customer, that customer will have seven unique points of recovery. In DPM, recovery points are created every time DPM performs a full backup, and also when data is synchronized by the DPM agent. Synchronizing every fifteen minutes throughout the day provides 96 recovery points per day (4 x 24 hours).

The **retention range** determines how long your customer needs DPM to keep the protected data available for recovery. You may define both short-term and long-term protection policies to control recovery from both disk and tape. Short-term policies may use either disk or tape, while long-term policies are intended to provide control over your customers’ extended tape retention.

* Defining a *short term to tape* scenario implies using DPM as a traditional tape backup solution, intending to replace one’s existing backup solution.
* Defining *short term to disk* (only) is often used to provide a robust backup and recovery solution for Microsoft® Exchange Server and other workloads through DPM, and then enable a third-party “enterprise” tape solution to back up the DPM server for long-term compliance.
* Most DPM users, however, will choose *short term to disk* plus *long term to tape*, which provides a complete solution offering rapid and reliable disk-based protection and recovery, with a seamlessly integrated tape component for long-term data retention.

Steps covered in this section:

[Create and configure protection groups 49](#_Toc172722270)

Your protection groups are collections of data sources that share the same protection configuration and schedule. When created and configured, you will manage your customers' data protection through protection groups in DPM.

[Set bandwidth throttling 59](#_Toc172722271)

Bandwidth throttling is a performance optimization in DPM that limits the percentage of network bandwidth that protection and recovery jobs can consume. Particularly as your DPM virtual servers will be operating remotely from the customer computers with which they will interact in this deployment scenario, this is a vital feature of DPM to take advantage of.

[Optimize performance 60](#_Toc172722272)

DPM provides several ways to increase server performance expectations and optimize DPM performance. Among these, you can decrease the size of data being transferred during replica creation and synchronization, stagger the start time of protection jobs, and schedule you consistency checks for off-peak hours.

#### Create and configure protection groups

In this section we will go through the various sections of the **Create New Protection Group Wizard**.

##### Start the Create New Protection Group Wizard

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

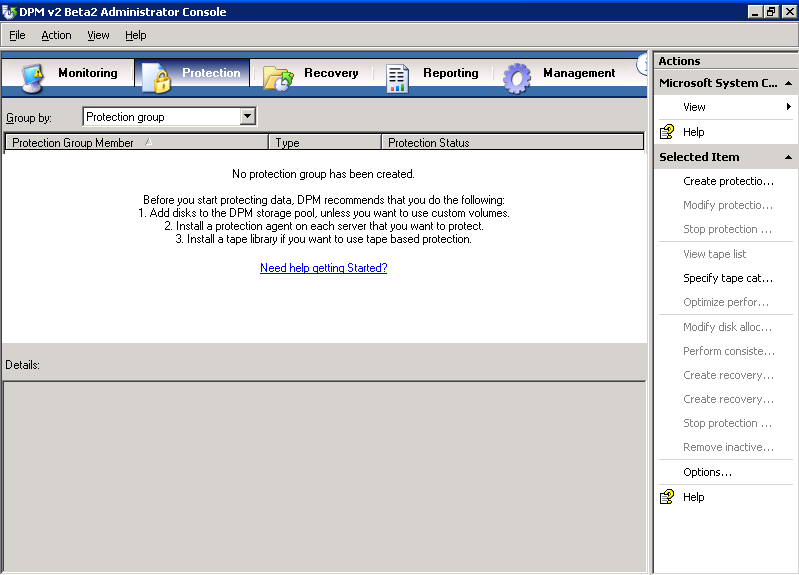


Figure Administrator Console, Protection tab

1. On the **Actions** pane, click **Create protection group**. The **Create New Protection Group Wizard** appears.
2. Review the **Welcome** page, and then click **Next**.

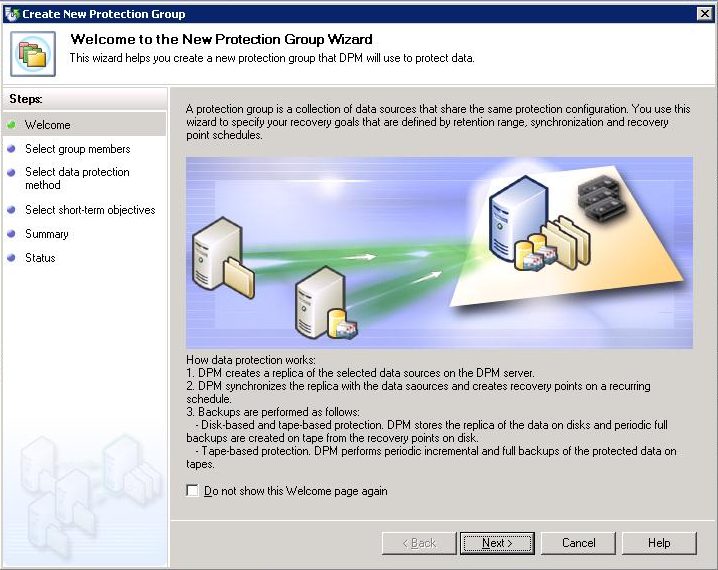


Figure Create New Protection Group Wizard, Welcome page

##### Select members for the protection group

You can protect the following members by using DPM:

* **File servers:** Volumes, shares, and folders
* **Computers running Exchange Server:** Storage groups
* **Computers running SQL Server:** Databases

1. On the **Select Group Members** page, verify that all servers that store data that you want to protect are displayed in the **Available members** box. If servers are missing, click **Add Servers**, and then follow the instructions for adding them.

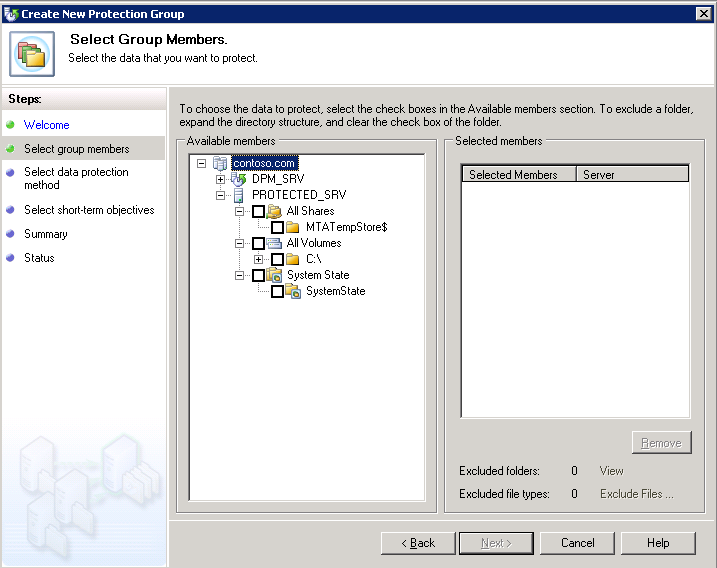


Figure Create New Protection Group Wizard, Select Group Members page

1. In the **Available Members** box, expand the server nodes to display the available data sources on each server. If you have just installed the protection agent, you may experience a delay of several minutes before you can expand the node for the server and display its available data sources.

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.

If you are following this cookbook in your test environment, select all of the data sources in **PROTECTED\_SRV** and click **Next**.

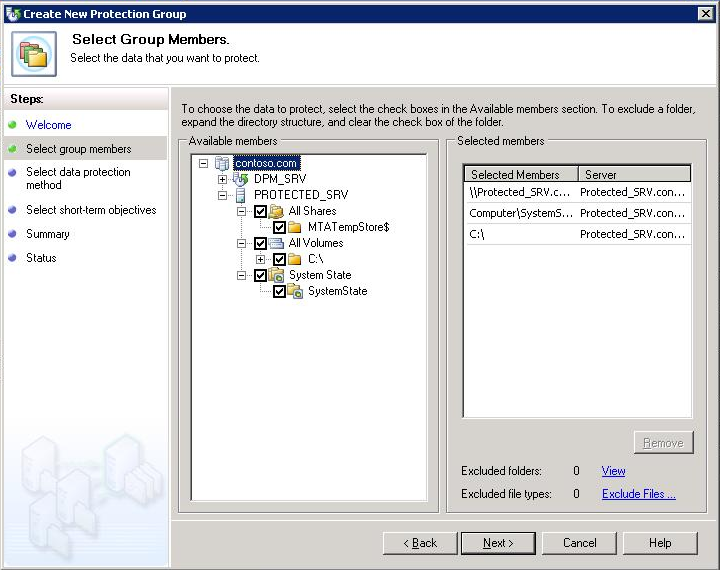


Figure Create New Protection Group Wizard, Selected Members box

Note the following:

* You cannot include data sources from the same volume in different protection groups.
* You can include data sources from more than one volume in a protection group.
* 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.
* If a boot volume contains user data that you want to protect, Microsoft recommends that you protect the relevant folders or shares individually, rather than protecting the whole boot volume.
* To exclude a folder, expand the directory structure, and then click to clear the check box of the folder that you want to exclude.
* To exclude file types, click the **Exclude File Types** link. In the **Exclude File Types** dialog box, type the file types you want to exclude, and then click **OK**.

1. After you have selected the members for the protection group, click **Next**.

##### Select a name and protection method for the protection group

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

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. In this example we will use the default name.

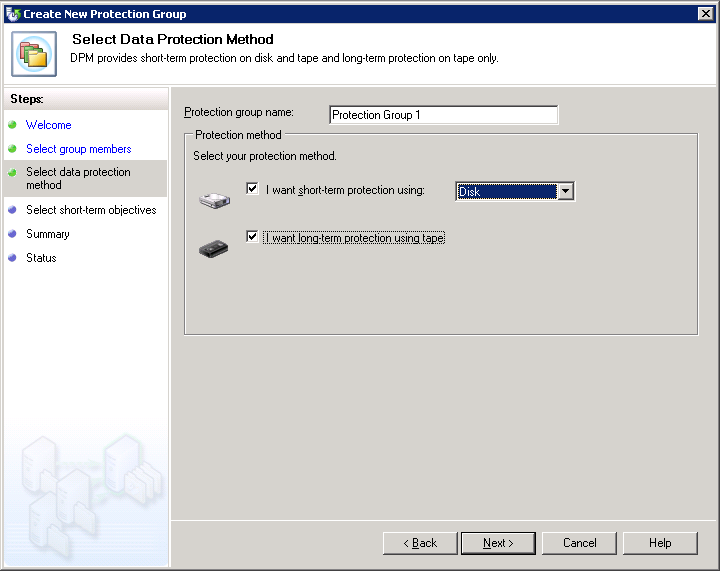


Figure Create New Protection Group Wizard, Select Data Protection Method page

1. In the **Protection policy** section, select the **I want short-term protection using** check box, and then select **Disk** from the drop-down list.

For long-term protection, you can select **I want long-term protection using tape** if you have a tape-based storage device attached to the DPM server. Data Protection Manager 2007 supports tape-based backup and can detect tape backup devices.

1. Click **Next**.

##### Specify your short-term protection policy

You define your short-term protection policy by selecting a retention range for your data, specifying how frequently data should be 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.

1. On the Specify Short-Term Goals page, in the Retention range box, select **5**. In the **Synchronization frequency** section, click **Every** and choose **15 minutes**.

In your production environment, choose one of the options:

* Click **Every**, and then select the days and times for which you want recovery points created for file protection. The synchronization frequency determines the recovery point schedule for application data protection.
* Click **Just before a recovery point** to replicate data just before a scheduled recovery point.

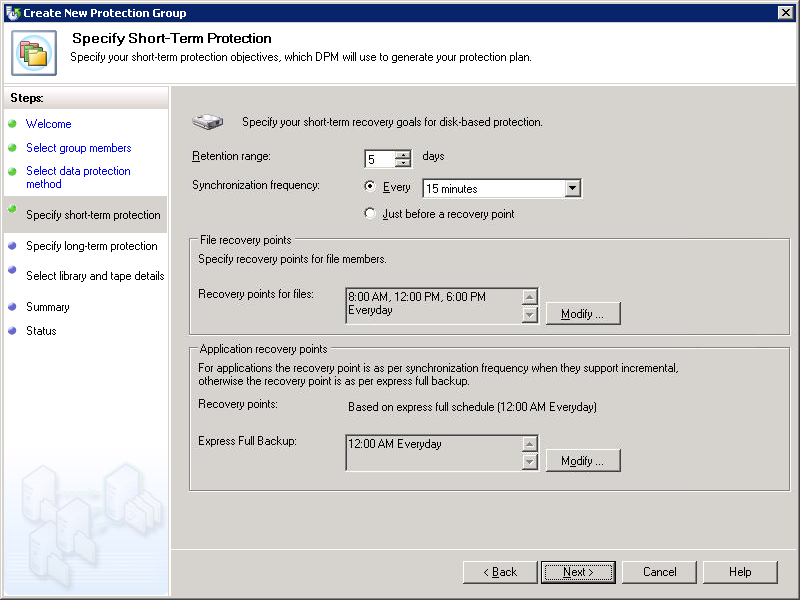


Figure Create New Protection Group Wizard, Specify Short-Term Goals page

1. To modify the recovery points, in the **File recovery points** section, click **Modify** next to the data source for which you want to change the recovery points. At this point, you do not need to modify any of the recovery points. On the **Modify Recovery Points** screen, select the available times and days of the week to the times and days that you want, and then click **OK**.

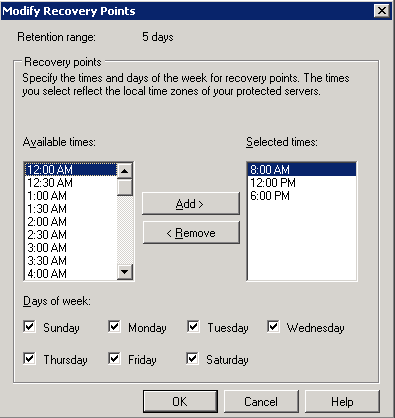


Figure Modify Recovery Points screen

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

##### Allocate space for the protection group

When you create a protection group, 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 that you must follow to increase or decrease the allocated disk space.

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

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

1. On the **Disk Allocation** page, accept the recommended allocations, and then click **Next**.

To change a recommended allocation in your production environment, click **Modify**, and then make the necessary adjustments.

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

##### Specify your long-term protection plan

If you want long-term protection by using tape, you must specify your long-term protection plan. You define your long-term protection plan by selecting a retention range for your data and a long-term backup schedule.

1. On the **Specify Long-Term Protection** page, in the **Retention range** box, select **three weeks**, which is the duration of time for which you might want the data to be available for recovery from the drop-list box. In the **Frequency of backup** box, select a backup frequency of **weekly** from the choices of daily, weekly, or monthly from the drop-down list.

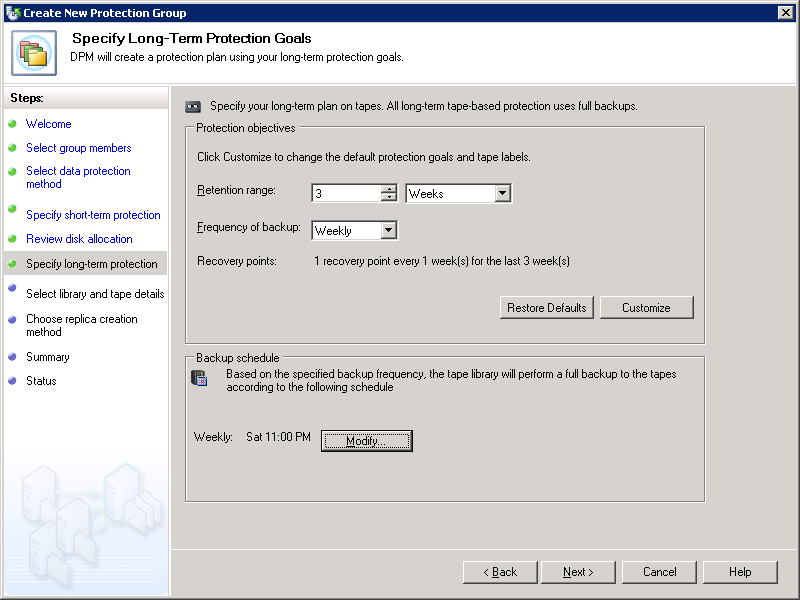


Figure Create New Protection Group Wizard, Specify Long-Term Goals page

1. You will not do this now, but in the future, to change the long-term backup schedule, click **Modify** under **Backup schedule**. In this dialog box, you can select the day of the week, month, or year that you want to back up your data, depending frequency of long-term backups that you select on the **Specify Long-Term Goals** page of the Create New Protection Group Wizard.

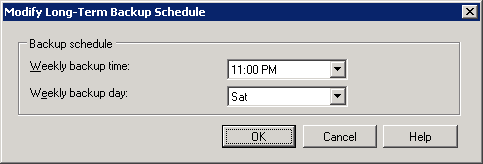


Figure Modify Long-Term Backup Schedule dialog box

1. Click **OK**.
2. On the **Specify Long-term Protection Policy** page, click **Next**.

##### Specify tape and library details

When you are protecting data for the long term, you must specify the number of copies that you need and how many tapes you want to allocate for long-term protection. You also specify whether you want DPM to encrypt and compress the data, and whether you want DPM to check the backup for data integrity.

1. On the **Select Tape and Library Details** page, in the **Library details** section, in the L**ibrary** box, select the backup library that you want from the drop-down list. The libraries listed in the drop-down list will depend on the tape libraries attached to your DPM server.

In the **Drives allocated** box, select how many drives you want to allocate from the drop-down list. This number will depend on the tape libraries attached to your DPM server.

In the **Copy library** box, select the tape copy library that you want from the drop-down list. The libraries listed in the drop-down list will depend on the tape libraries attached to your DPM server.

1. For this example, in the **Tape options for long-term protection** section, leave Compress data selected.

In your production environment, you may choose to either not compress your data or to encrypt your data.

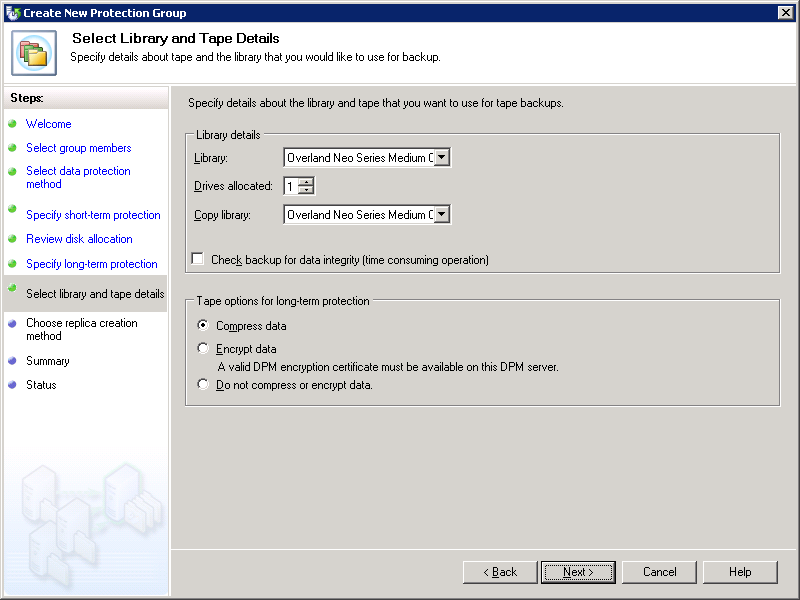


Figure Create New Protection Group Wizard, Select Library and Tape Details page

1. Click **Next**.

##### Choose a replica creation method

When you create a protection group, a replica is created for each protected volume in the protection group. In DPM, a replica is a complete copy of the protected data on a single volume, database, or storage group.

You can automatically perform synchronization at the times specified in your protection schedule, or you can manually synchronize a replica.

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

If, in your production environment, you select **Later** to replicate the data and a specified time, then select the date and time from the drop-down lists.

1. Click **Next**.

##### Create the protection group

Before you create the protection group, you review the tasks that DPM is set to perform. These tasks are based on the options that you specified while performing the steps in the **Create New Protection Group Wizard**.

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.

1. On the **Confirmation** page, click **Close**.

#### Set bandwidth throttling

Bandwidth throttling will allow you to limit the amount of bandwidth used by DPM, set a maximum speed for data transfers from the file servers to the DPM server, compress data on the wire to decrease the size of the data transferred to make replicas, and/or stagger the starting times for protection jobs.

1. In DPM Administrator Console, click **Management** on the navigation bar.
2. Click the **Agents** tab, and select the server you want to throttle. In this example, right-click **PROTECTED\_SRV** and select **Throttle Server**.

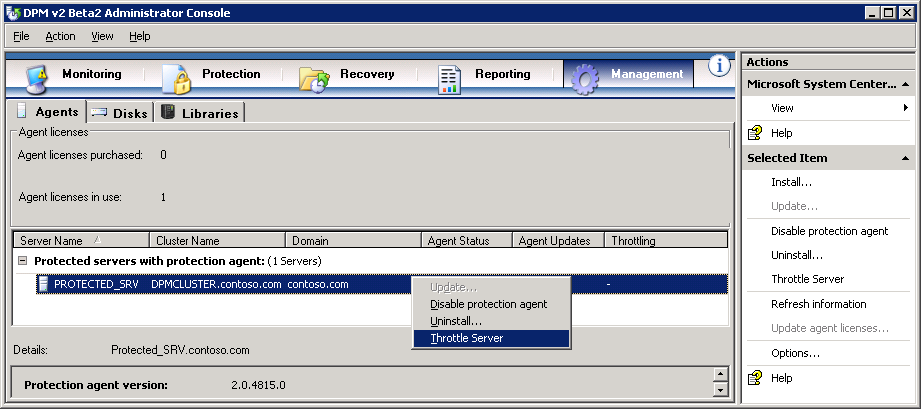


Figure Administrator Console, Management tab

1. In the **Throttle** dialog box, check **Enable network bandwidth usage throttling**. In this example, leave the default settings under **Settings** and **Work Schedule**. In production environment, set these to your desire settings.

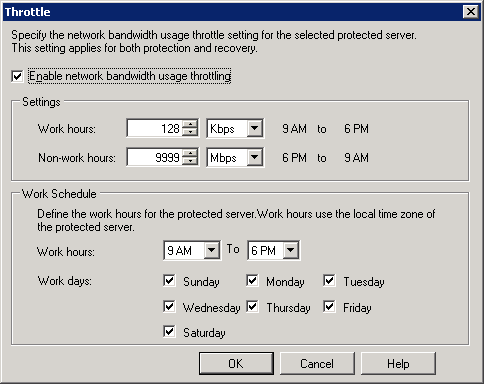


Figure Network bandwidth throttling dialog box

1. Click **OK**.

#### Optimize performance

DPM provides several ways to increase server performance expectations and optimize DPM performance. Among these, you can enable on-the-wire compression to decreases the size of data being transferred during replica creation and synchronization and allows more data throughput with less impact to network performance, stagger the start time of protection jobs to avoid performance degradation from starting too many jobs at once, and schedule you consistency checks for off-peak hours.

**Note:** Network speed, the performance characteristics of the protected server, the size of your protected data, and the rate at which the protected data changes can affect your actual results.

1. In DPM Administrator Console, click **Protection** on the navigation bar.
2. In the **Display** pane, right-click the protection group for which you want to modify performance options. In this example, right-click **Protection Group 1** and select **Optimize performance**.

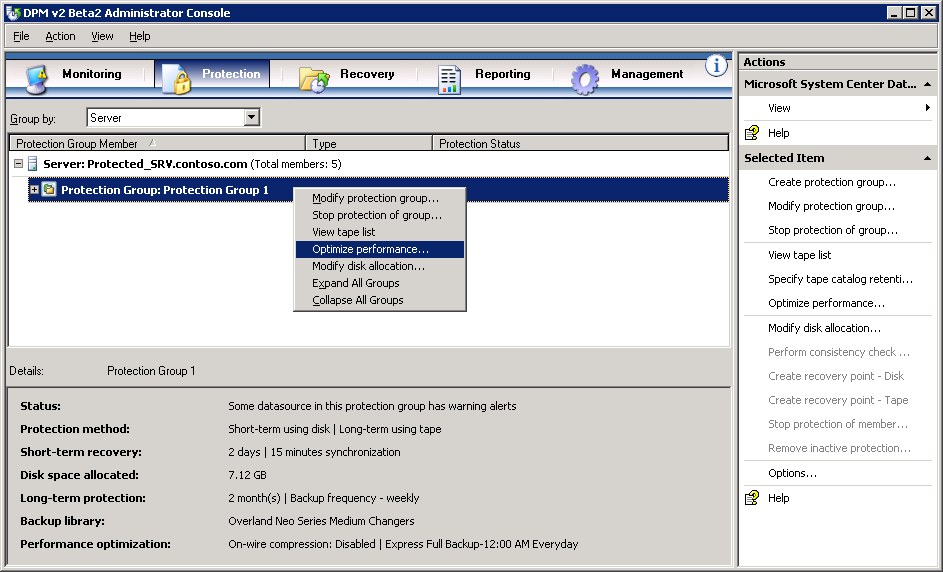


Figure Administrator Console, Protection tab

1. To enable on-the-wire compression, on the **Network** tab, check **Enable on-the-wire compression**.

To stagger the starting times for protection jobs, under **Start protection jobs**, specify the number of minutes after the hour to start synchronization and shadow copy jobs.

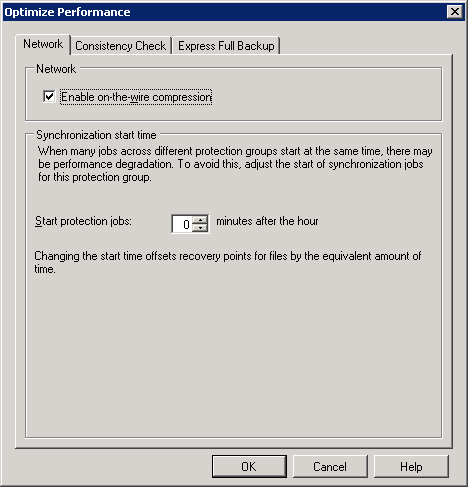


Figure 51 Optimize Performance dialog box, Network tab

1. To ensure that your replica of your protected data does not become inconsistent due to problems on the protected server or the network, you can schedule consistency checks. To do this, check **Schedule daily consistency check** on the **Consistency Check** tab.

You do not need to do this in this example. If you do this in a production environment, optimize network performance and run the consistency check during off-peak hours.

1. Express full backups allow DPM to provide quick recoveries to application data. In this example, leave the default settings on the **Express Full Backup** tab.

In you production environment, choose the settings the meet your customers’ data recovery time goals.

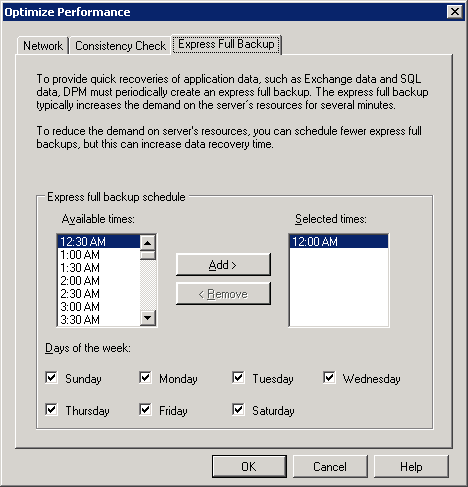


Figure Optimize Performance dialog box, Network tab

1. To apply your changes, click **OK**.

# Section 4: Monitor and Report

After you set up data protection, you should monitor DPM activity to verify that everything is working correctly and to troubleshoot any problems that occur. Monitoring is essential to give you an overview of what has already happened, what is currently happening, and what is scheduled to happen. By monitoring DPM, you will know that data protection activities are working as expected, and you can have confidence that errors and warnings will be brought to your attention when they occur.

DPM reporting provides both new and historical reports. In addition, you can subscribe to DPM reports. A new report is created dynamically, based on the options that you select when you set up the report. A historical report is created and saved for future reference only when you schedule a report. You choose the options that you want at the time that you schedule the report.

Steps covered in this section:

[Monitor DPM alerts 64](#_Toc171320791)

DPM alerts enable you to monitor DPM activity, job status, and error conditions. Alerts form your first avenue of troubleshooting.

[Monitor DPM jobs 65](#_Toc171320792)

You can directly monitor the status of all completed, scheduled, and running protection jobs, as well as all associated tasks.

[Display a new DPM report 66](#_Toc171320793)

A report selected through DPM Administrator Console always opens as a Web page in Internet Explorer

[Schedule DPM reports 67](#_Toc171320794)

Schedule DPM reports to run one time, weekly, or monthly, and customize the way that data is organized within reports.

[Subscribe to DPM reports 67](#_Toc171320795)

You can choose to send scheduled reports to subscribers through e-mail.

#### Monitor DPM alerts

By monitoring alerts, you can monitor data protection activity, job status, and error conditions in Data Protection Manager (DPM) and take action, when necessary, to resolve issues. In DPM, alerts are displayed in the **Monitoring** task area on the **Alerts** tab.

As a general rule, you should start troubleshooting an issue in DPM by reviewing the relevant alert details. For detailed information about a specific job related to the issue, review the job details.

##### Display details for an alert

1. In the DPM Administrator Console, click **Monitoring** on the navigation bar, and then click the **Alerts** tab.
2. Select the alert for which you want more details. The alert information is displayed in the **Details** pane.

When an alert is resolved, or when the conditions that generated the alert no longer apply, the alert becomes inactive. Inactive alerts are displayed for 30 days in the **Alerts** view of the **Monitoring** task area by default. After an alert has been inactive for 30 days, it is removed from the inactive alerts history and it can no longer be displayed. If you want to hide inactive alerts, you can disable the **Show inactive alerts** option.

##### Disable inactive alerts

1. In DPM Administrator Console, click **Monitoring** on the navigation bar, and then select the **Alerts** tab.
2. Clear the **Show inactive alerts** check box. This check box is located below the navigation bar and above the **Display** pane.

#### Monitor DPM jobs

Jobs are displayed in the **Monitoring** task area on the **Jobs** tab. On the **Jobs** tab, you can monitor the status of all completed, scheduled, and running jobs, and all associated tasks. Use the **Group by** drop-down list box to group the list of jobs by protection group, server, status, or type. Use the **Time period** drop-down list box to filter the list of jobs according to a selected time period. Select or clear the **Show synchronization** check box to include or exclude synchronization jobs in the list of jobs.

DPM provides both an Alerts view and a Jobs view so that you can easily access both summary and detailed information about data protection activity. The **Alerts** tab aggregates alerts, error conditions, and jobs to provide a summary view of what is happening across the entire system. The **Jobs** tab provides the operational details for each scheduled, completed, running, canceled, or failed job. For example, in response to multiple shadow copy job failures of the same replica, the Alerts view displays a single “shadow copy failure” alert; in contrast, the Jobs view displays an entry for each shadow copy job failure. In the Jobs view, you can also display completed shadow copy jobs for the past 30 days and scheduled shadow copy jobs for the next seven days.

As a general rule, you should start troubleshooting an issue in DPM by reviewing the relevant alert details. For detailed information about a specific job related to the issue, review the job details.

##### Check job status

1. In DPM Administrator Console, click **Monitoring** on the navigation bar, and then click the **Jobs** tab.
2. In the **Group by** list box, select **Status**.
3. In the **Time Period** list box, select the time period that you want to review. The jobs for the selected time period are displayed, grouped by status.
4. To review details for a specific job, select the job and refer to the information in the **Details** pane.

##### Display job details

1. In DPM Administrator Console, click **Monitoring** on the navigation bar, and then click the **Jobs** tab.
2. Select the job for which you want more details. The information for the job is displayed in the **Details** pane, in the lower part of the console.

#### Display a new DPM report

A report selected through DPM Administrator Console always opens as a Web page in Internet Explorer. New reports are not saved for future reference; they are deleted when closed.

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

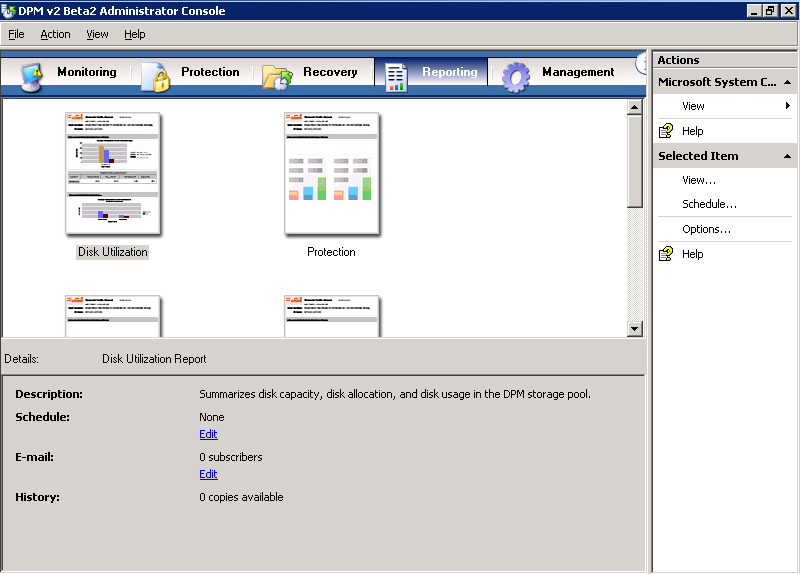


Figure Administrator Console, Reporting tab

1. Select a report, and then, on the **Actions** pane, click **View**. Alternatively, you can double-click or right-click a report in the **Display** pane, and then click **View**.
2. Select display options for the report, and then click **OK**.

#### Schedule DPM reports

No reports are scheduled in DPM by default. To prompt DPM to start creating and saving historical reports, you must specify report creation schedules. Each of the standard reports operates on an independent schedule. You can schedule DPM reports to run one time, weekly, or monthly, and you can customize the way that data is organized within the report. When you schedule reports, you can also choose to send reports to specified recipients through e-mail.

1. In DPM Administrator Console, click **Reporting** on the navigation bar.
2. On the **Display** pane, select the report that you want to schedule.
3. On the **Actions** pane, click **Schedule**. Alternatively, you can right-click the report icon, and then click **Schedule**.
4. In the **Schedule** dialog box, click **Enable Schedule**.
5. On the **Schedule** tab, select the **Run the Disk Utilization report according to the schedule options** check box, fill in the appropriate values, and then click **OK**.

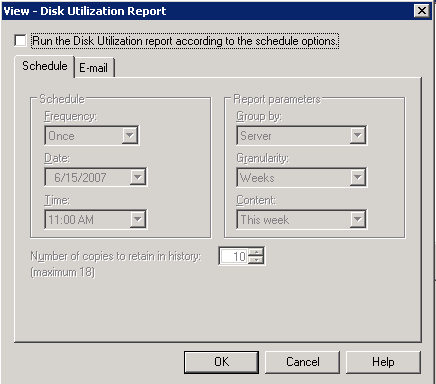


Figure Reporting, schedule options

1. Repeat steps 2 through 5 for each report that you want to schedule.

#### Subscribe to DPM reports

When you schedule reports, you can enable the option to send reports to subscribers through e-mail. Before you enable this option, you must specify the SMTP server that DPM will use to send reports.

##### Configure the SMTP server

1. In DPM Administrator Console, click the **Action** menu, and then click **Options**.
2. The **Options** dialog box appears.
3. On the **SMTP Server** tab, type the SMTP server name, the SMTP server port, and the e-mail address that you want to appear in the **From** box of the e-mail messages that DPM will send.

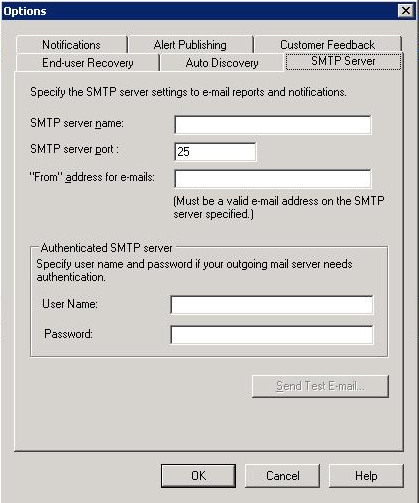


Figure Options, SMTP Server tab

1. To test the SMTP server settings, click **Send Test E-mail**, and type the e-mail address to which you want DPM to send the test message.
2. Click **OK**.

##### Subscribe to reports

1. In DPM Administrator Console, click **Reporting** on the navigation bar.
2. On the **Display** pane, right-click the report to which you want to subscribe. On the **Actions** pane, click **Schedule**. Alternatively, you can right-click a report in the **Display** pane, and then click **Schedule**.
3. On the **E-mail** tab, in the **Recipients** box, type the e-mail addresses of all the people or groups to whom DPM should send reports, and then click **OK**.

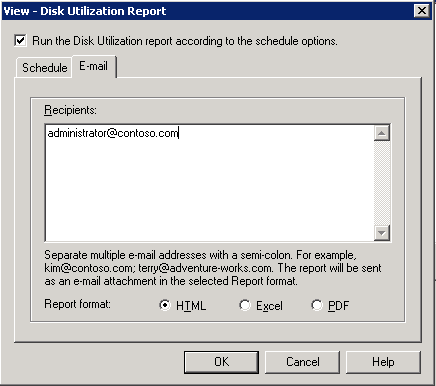


Figure Reporting, E-mail tab

1. Select the report format—HTML, Excel, or PDF—and then click **OK**.
2. Repeat steps 2 through 4 for each type of report that you want to distribute through e-mail.

##### Add a subscriber to an existing subscription

1. In DPM Administrator Console, click **Reporting** on the navigation bar.
2. In the **Display** pane, right-click the report for which you want to add e-mail recipients, and then click **Schedule**.
3. On the **E-mail** tab, in the **Recipients** box, add the subscriber to the list of recipients, separating it from the last entry by a semicolon, and then click **OK**.

##### Modify the report format for an existing subscription

1. In DPM Administrator Console, click **Reporting** on the navigation bar.
2. On the **Display** pane, right-click the report for which you want to modify the report format, and then click **Schedule**.
3. On the **E-mail** tab, in the **Report format** box, select the report format for this report—HTML, Excel, or PDF—and then click **OK**.

# Section 5: Restore Data

After Microsoft System Center Data Protection Manager (DPM) is deployed in your environment, you will use DPM and its disk-based recovery functionality to handle most of your short-term data recovery needs. You can also continue to use tape for long-term data archiving and disaster recovery. DPM fits seamlessly into existing archiving solutions.

Archiving file server data from the replicas on the DPM server rather than from the file servers eliminates the problem of scheduling backups around file server availability. When you archive DPM to tape, you can, in case of disaster, restore archived data to file servers and rebuild the DPM server.

Note that if you would like to backup and restore a running virtual machine, you can find those steps in [Appendix A](#_Appendix_A:_).

Steps covered in this section:

[Recover data on the file server 70](#_Toc171320800)

Recovery in DPM is the process by which you restore previous versions of shares, volumes, folders, or files from the shadow copies to customer computers from copies kept on the DPM server.

[Support end-user restores 76](#_Toc171320801)

This feature of DPM enables end users to independently recover data by retrieving a shadow copy of their data.

[Restore data from tape 80](#_Toc171320802)

The process of restoring data from long-term storage on tape is very similar in DPM to restoring data from disk.

#### Recover data on the file server

You can easily and quickly recover data by using the DPM Recovery Wizard. Recover your data by selecting a previous version of the data from a recovery point stored on the DPM server.

A recovery point, also referred to as a *snapshot*, is a point-in-time copy of the files and folders that are protected by the DPM server.

##### Create a recovery point

1. Switch to the DPM server, **DPM\_SVR**.
2. In DPM Administrator Console, on the **Protection** tab, expand **Protection Group: Protection Group 1**, and then select the folder that you want to protect. In this example, that folder is **Computer\SystemState**. In the **Actions** pane, click **Create recovery point**.

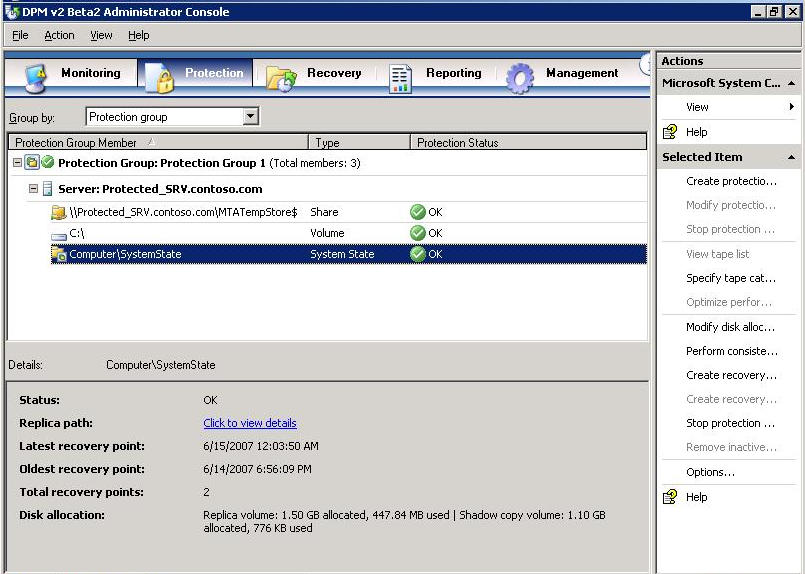


Figure Administrator Console, Protection tab

1. In the **Create recovery point** dialog box, click **OK**. The new recovery point appears in the recovery point list.

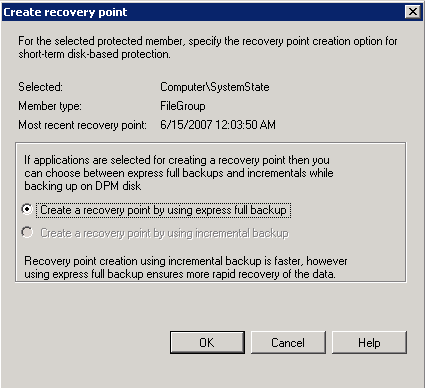


Figure Create recovery point dialog box

##### Recover the data

1. Switch to the DPM Server.
2. In DPM Administrator Console, on the navigation bar, click the **Recovery** tab. In the **Protected data** pane, navigate to the **PROTECTED\_SRV**, expand **All Protected Volumes**, and then select the drive **C:\**. In the right pane, in the **Recoverable Item** list, choose a file that is in the root of **C:\** . In this example, we have picked a file called **additions.log**. On the calendar, select the latest recovery point for the folder. Available recovery points are indicated in bold.

**Note:** Additions.log is a file created when you install Virtual Machine Additions on **PROTECTED\_SRV**. If you did not install Virtual Machine Additions on **PROTECTED\_SRV**, select another file, such as boot.ini.

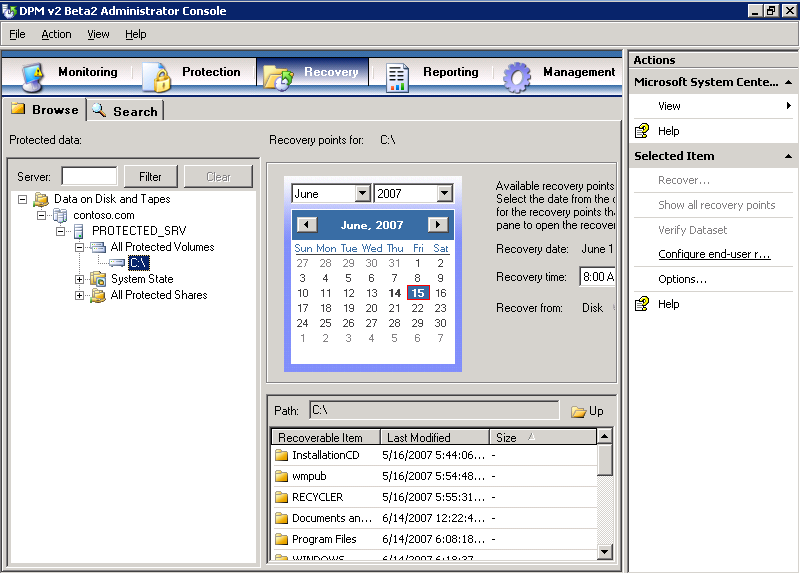


Figure Administrator Console, Recovery tab

1. In the **Actions** pane, click **Recover**. The **Recovery Wizard** appears.
2. On the **Review Recovery Selection** page, verify that the file that you want to recover appears in the **Recovery items** list. Here we have chosen additions.log, but your choice may be different. Then click **Next**.

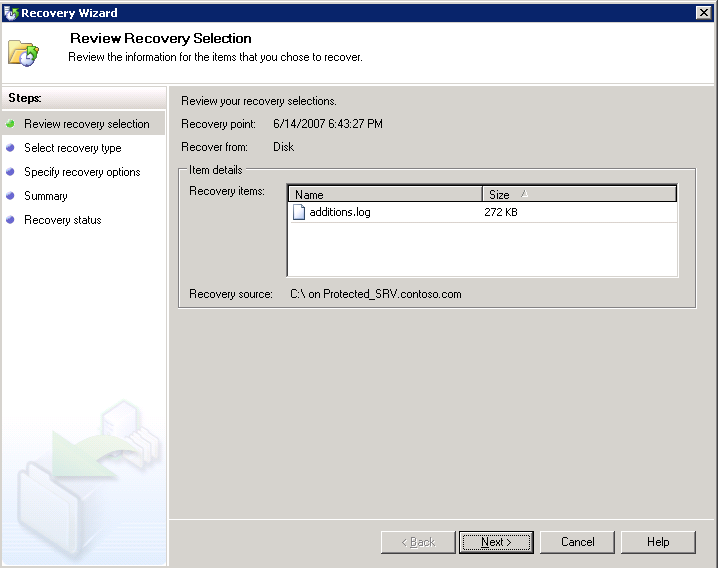


Figure Recovery Wizard, Review Recovery Selection page

1. On the **Select Recovery Type** page, select **Recovery to the original location**, and then click **Next**.

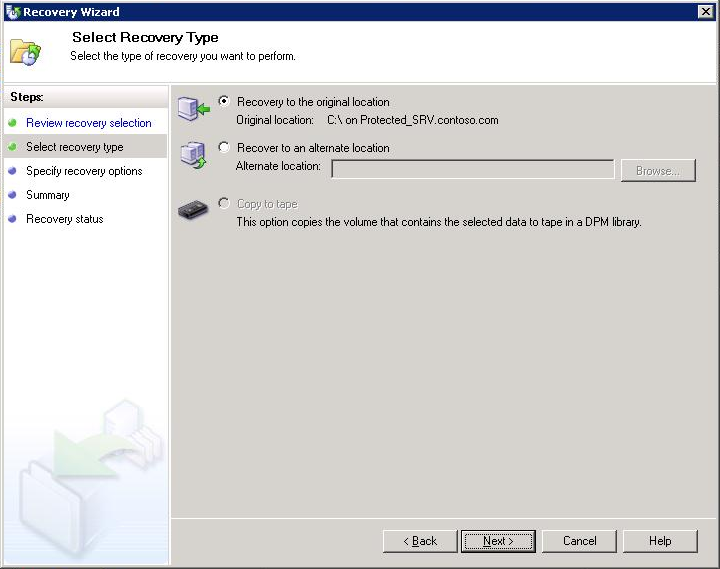


Figure Recovery Wizard, Select Recovery Type page

1. On the **Specify Recovery Options** page, in the **Existing version recovery behavior** section, click **Create copy**. This will create another copy of the file you are recovering in the event that DPM finds an existing version of that file.

If you choose **Skip**, DPM will do nothing to the existing version of the file. If you choose **Overwrite**, DPM will overwrite any existing versions of that file.

In the **Restore security** section, select **Use security setting of the destination server** and then click **Next**. This will cause the file being restored to inherit the current security settings of the server you are restoring it to.

**Apply the security settings of the recovery point version** will cause the file to be restored with the security attributes of the recovery point from which you are restoring the file.

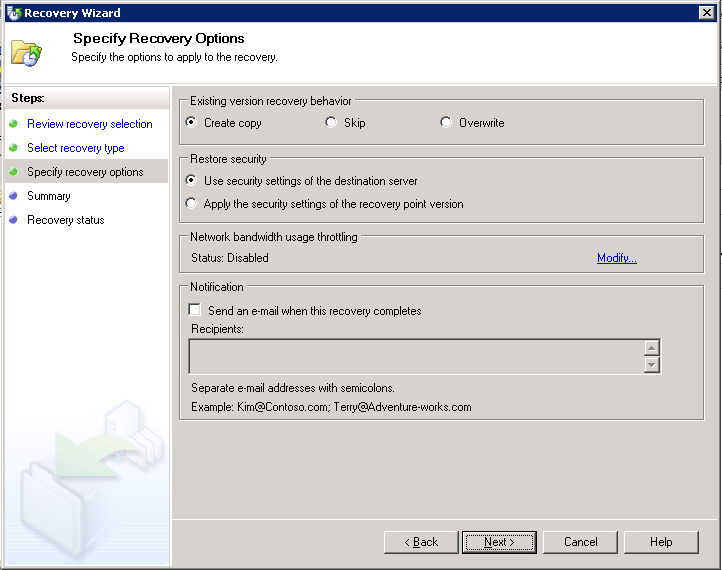


Figure Recovery Wizard, Specify Recovery Options page

1. On the **Summary** page, verify that **additions.log** appears in the **Recovery Items** list, and then click **Recover**.

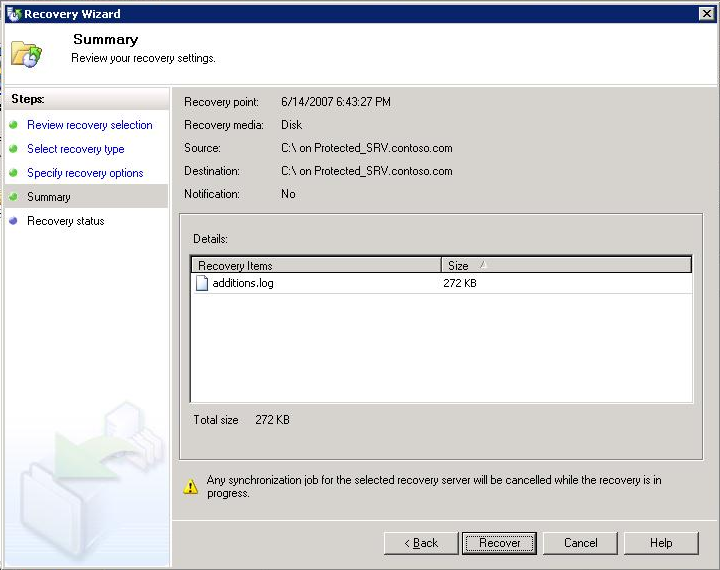


Figure Recovery Wizard, Summary page

1. On the **Recovery Status** page, after the recovery is complete, click **Close**.

#### Support end-user restores

End-user recovery enables your end users to independently recover data by retrieving the most recent copies of their files. End-user recovery is supported in Active Directory domains.

##### Enable end-user recovery

1. Switch to the DPM server (**DPM\_SRV** in your test environment).
2. In DPM Administrator Console, from the **Action** menu, select **Options**. The **Options** dialog box appears. On the **End-user Recovery** tab, click **Configure Active Directory.**

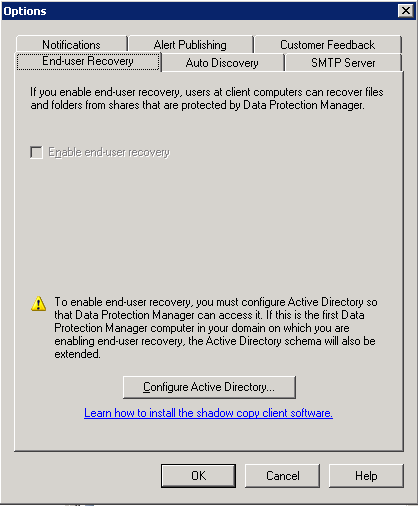


Figure End-user Recovery Options

1. In the **Configure Active Directory** dialog box, select the **Enter credentials** option. Fill in the **User name** and **Password** box with the user name and password of a user who has permission to make changes to the Active Directory. Typically this user is a member of the Domain Admins Security Group. Then click **OK.**



Figure Configure Active Directory dialogue box

1. On the **Active Directory Configuration for Data Protection Manager** dialog box, click **Yes**, and then click **OK**.

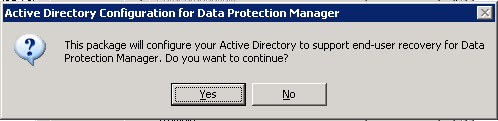


Figure Active Directory Configuration dialogue box

1. After configuration of Active Directory is complete, select the check box for **Enable end-user recovery**, and then click **OK**.

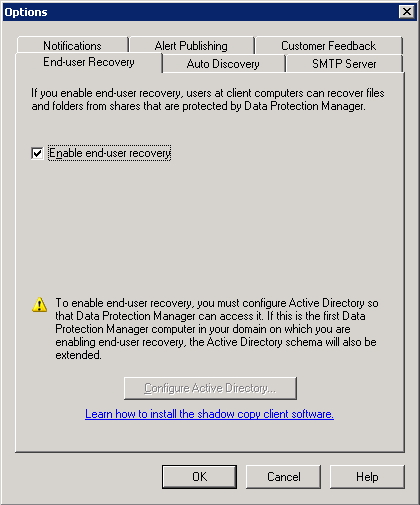


Figure End-user recovery options

1. In the **Options** dialog box, click **OK**.

Before your users can begin independently recovering previous versions of their files, the DPM shadow copy client software must be installed on their computers.

##### Install the shadow copy client software

1. Install the client software which is located at <http://go.microsoft.com/fwlink/?LinkId=46064> on the computers of your customers on which you want to enable end-user recovery. In your test environment, install this on **PROTECTED\_SRV**.

In your production environment, you can deploy this software package to your users using Group Policy, or another method.

##### Perform an end-user restore

1. On **PROTECTED\_SRV**, create a shared folder called **Docs**. Create a document in this folder called **Important\_Doc.doc**.
2. On the computer on which you have installed the shadow copy client software (**PROTECTED\_SRV**), click **Start, Run,** and type**\\Protected\_SRV\Docs\Important\_Doc.doc**. Open the document and make a change, then close the document.
3. Right-click **Important\_Doc.doc**, and then click **Properties**.
4. In the dialog box, on the **Previous Version** tab, click the previous version of the file, and then click **Restore**. If you don’t see the **Previous Version** tab, go to the DPM Server and manually create a restore point, and then repeat steps 1-4.

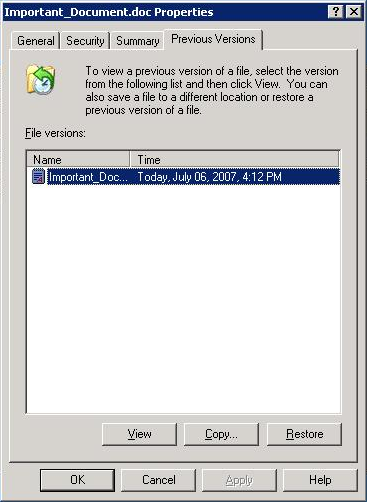


Figure Previous version tab of the file properties dialog box

1. Click **Yes**, and then, after the file has been successfully restored, click **OK**.

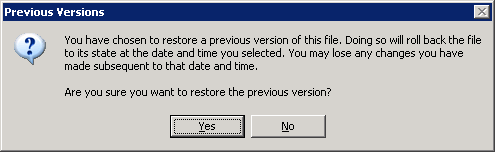


Figure Previous Versions dialog

#### Restore data from tape

Restoring data from tape is very similar to restoring data from disk.

1. On the **Management** page of DPM Administrator Console, select the **Libraries** tab and then select the tape you want to restore from. In Figure 70, for example, Slot 4 houses the tape labeled ‘Protection Group 1-00000001,’ a tape image that can be used to restore from.

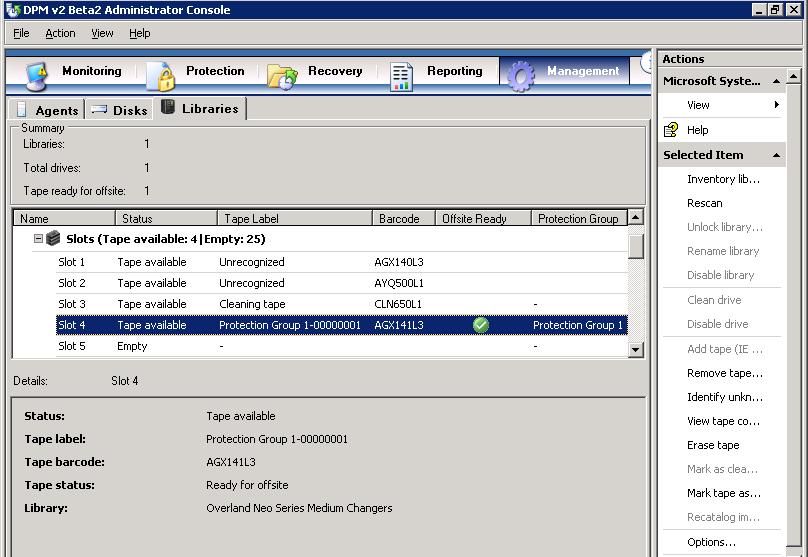


Figure Tape library viewed in DPM Administrator Console

1. On the **Review Recovery Selection** page of the Recovery Wizard, verify that you have selected the correct tape set for recovery in the **Tape set for recovery** drop-down menu. Click **Next**.

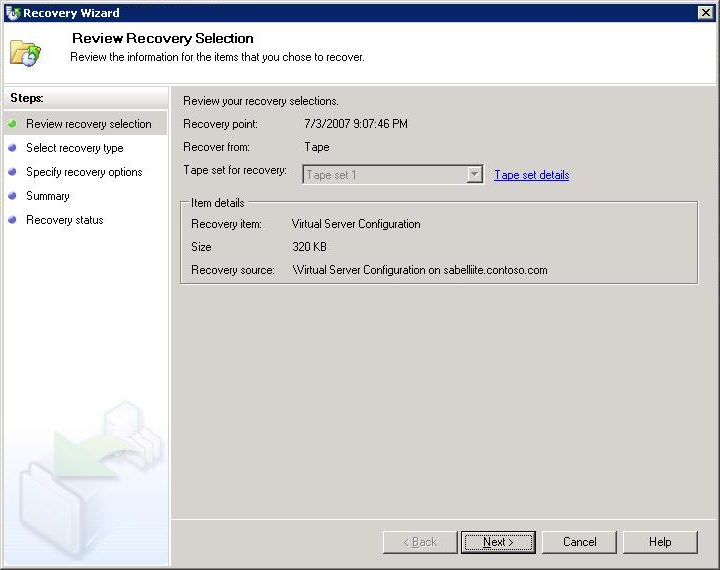


Figure Review Recovery Selection page, Recovery Wizard

1. On the **Select Recovery Type** page, select how you want to recover this data from tape. In Figure 72, **Recover to original instance** is selected. Click **Next**.

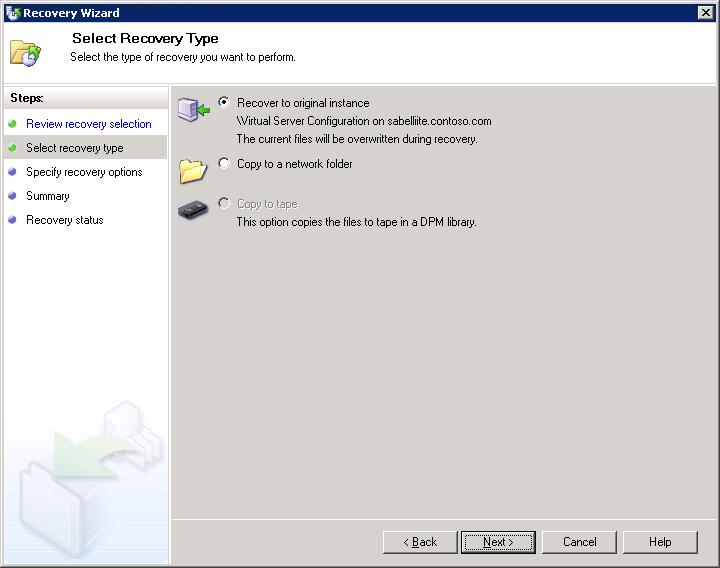


Figure Select Recovery Type page, Recovery Wizard

1. On the **Specify Recovery Options** page, you can set the final parameters for your recovery job, such as the name of the tape library to use, network bandwidth throttling, and recipients for e-mail notifications of the completion of the recovery. In the example in Figure 73, the default library, Overland Neo Series Medium Changers (the name of the specific tape device used in creating this cookbook; your device may be different), is selected. The other parameters are left blank, the default setting for these. Click **Next**.

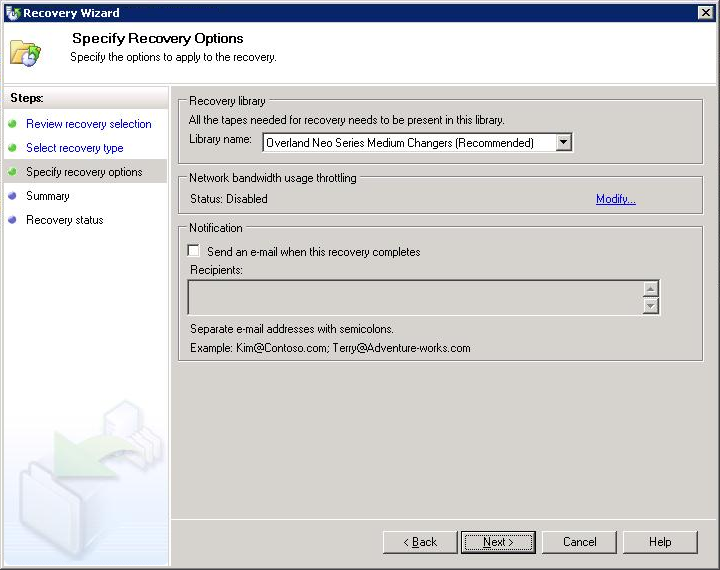


Figure Specify Recovery Options page, Recovery Wizard

1. Review your settings on the **Summary** page, and then click **Next**. This will initiate your recovery.

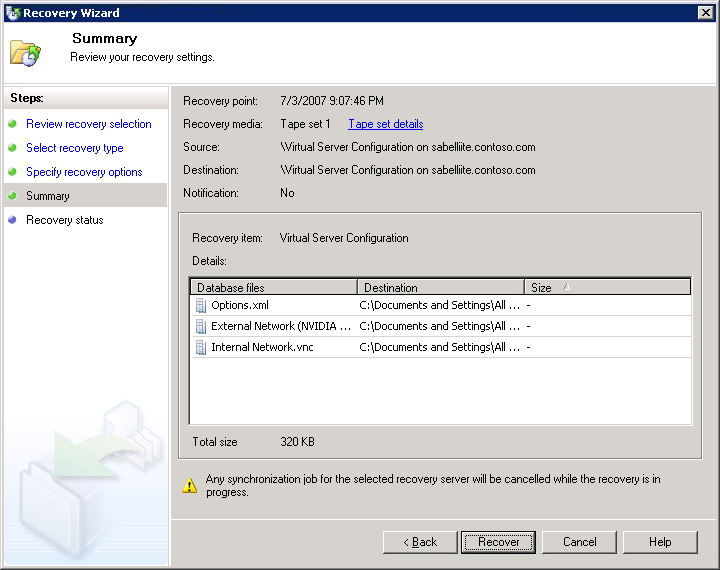


Figure Summary page, Recovery Wizard

1. When the recovery is complete, click **Close** on the **Recovery Status** page.

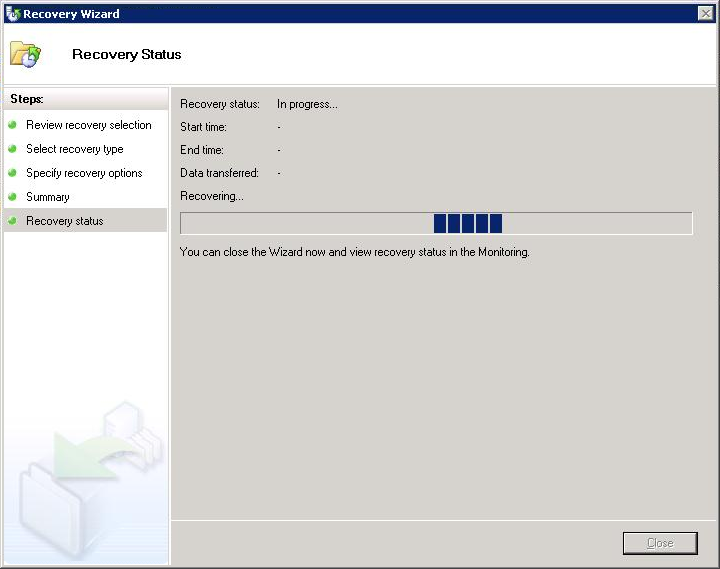


Figure Recovery Status page, Recovery Wizard

1. The files backed up to tape are now restored to their original location and have overwritten any subsequent versions of those files at that location.

# Appendix A: Back Up and Restore Data to a Running VM

Previous to the release of Service Pack 1 for Virtual Server 2005 R2, a Virtual Server-based virtual machine had to be stopped or shut down in order to be fully backed up by the Virtual Shadow Copy Service (VSS). Service Pack 1 provides a VSS writer to Virtual Server 2005 R2, thereby enabling VSS (which DPM uses to back up servers) to back up a running virtual machine. This means that you can provide the same protection for virtual machines running in customer domains that you do for their physical servers, without server downtime for your customers. In this scenario, we are backing up the entire virtual machine, not just files that exist within that virtual machine.

#### Back up a running virtual machine

The following scenario uses these names:

* Physical host: **HOST\_2** (hosts **Protected\_SRV**)
* Virtual machine with DPM: **DPM\_SRV**
* Domain: Contoso.com
* Virtual machine being backed up: **Protected\_SRV**

1. Make sure that the physical machine **HOST\_2**, as well as your other machines, are joined to Contoso.com.
2. Make sure that the DPM Backup Agent is installed on **HOST\_2**.
3. Create a protection group that contains **HOST\_2**. In DPM Administrator Console, select the **Protection** tab.
4. In the **Action** pane on the right side of the screen, click the **Create New Protection Group** link. This will launch the **Create New Protection Group Wizard**.
5. In the Create New Protection Group Wizard, on the **Select Group Members** page, expand **HOST\_2**. Select the check box next to **Protected\_SRV**, and the check box next to **Virtual Machine Configuration**. Click **Next**.

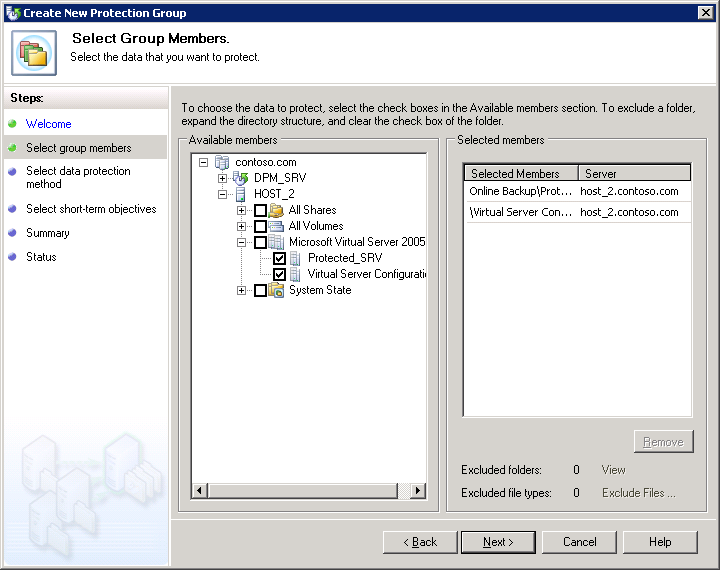


Figure Create New Protection Group Wizard, Select Group Members page

1. On the **Select Data Protection Method** page, give your protection group an appropriate name. Select the check box **I want short-term protection**, and then select **Disk** from the drop-down menu. Click **Next**. In this example we will enter **Protection Group VM** in the **Protection group name** text box.

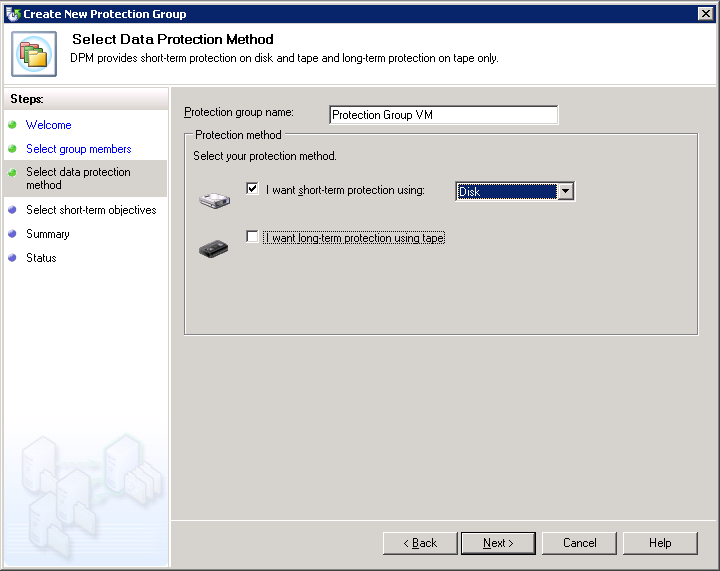


Figure Create New Protection Group Wizard, Select Data Protection Method page

1. On the **Specify Short-Term Goals** page, enter an appropriate number in the **Retention range** field. In this example we will enter **5** days. We will make no changes in the **Recovery points (all members)** section.

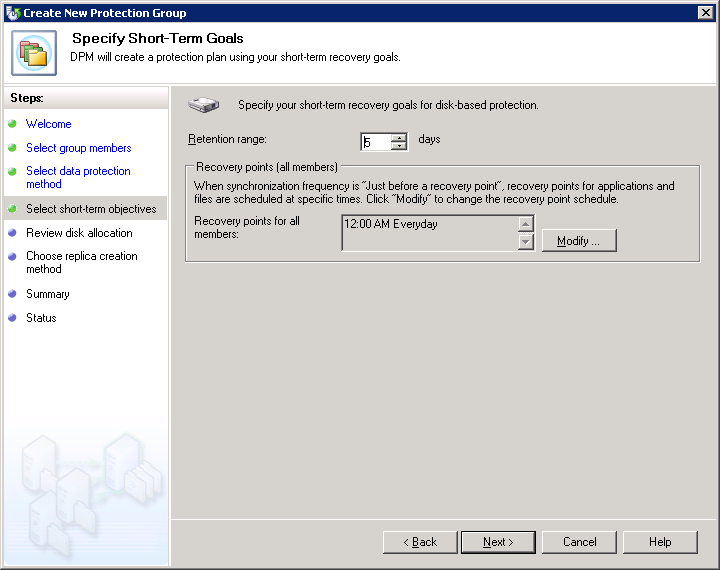


Figure Create New Protection Group Wizard, Define Short-Term Goals page

1. On the **Review Disk Allocation** page, make sure you have sufficient disk space allocated for your backup jobs. Adjust if necessary. Click **Next**.

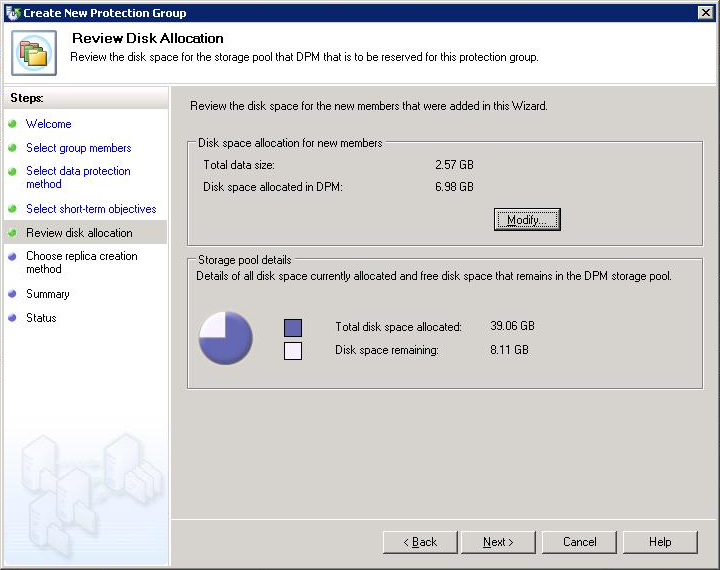


Figure Create New Protection Group Wizard, Review Disk Allocation page

1. On the **Choose Replica Creation Method** page, select the options that best suit your needs. In this example we will select the default option, which is **Automatically** and **Now**. This allows DPM to create a replica to copy the selected data to the DPM server automatically and immediately. Click **Next**.

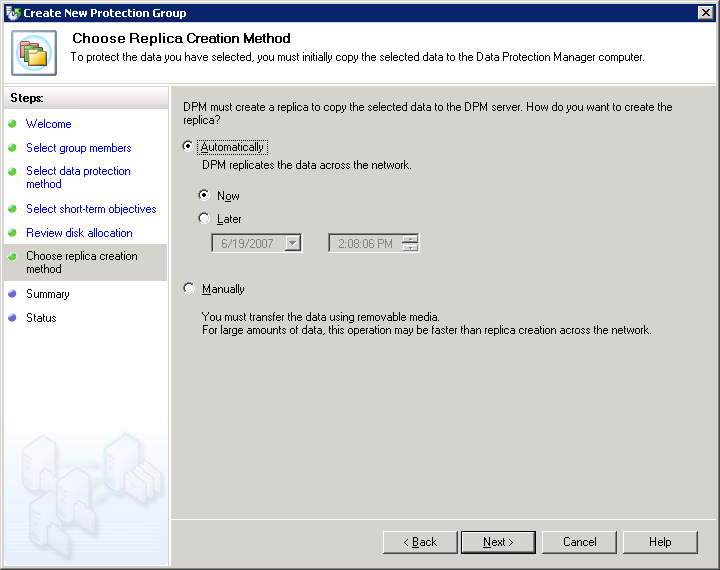


Figure Create New Protection Group Wizard, Choose Replica Creation Method page

1. On the **Summary** page, review the settings and confirm that all the information presented is accurate. Click **Create Group**.

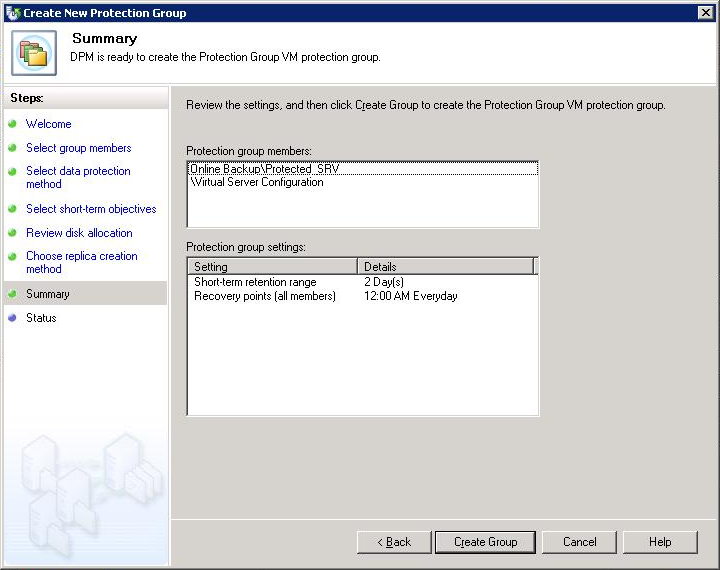


Figure Create New Protection Group Wizard, Summary page

1. Keep an eye on the **Status** page to track progress. When all tasks are finished, click **Close**.

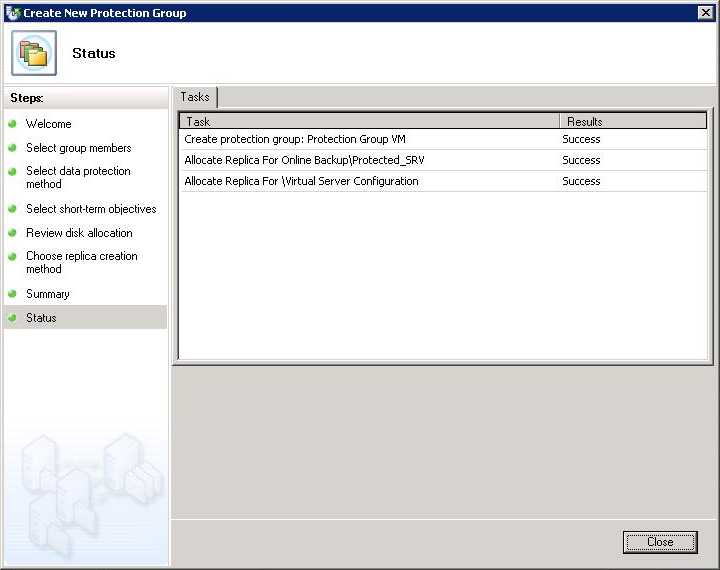


Figure Create New Protection Group Wizard, Status page

1. In DPM Administrator Console, select the **Protection** tab. Confirm that the **Protection Status** for your protection group members is **OK**.

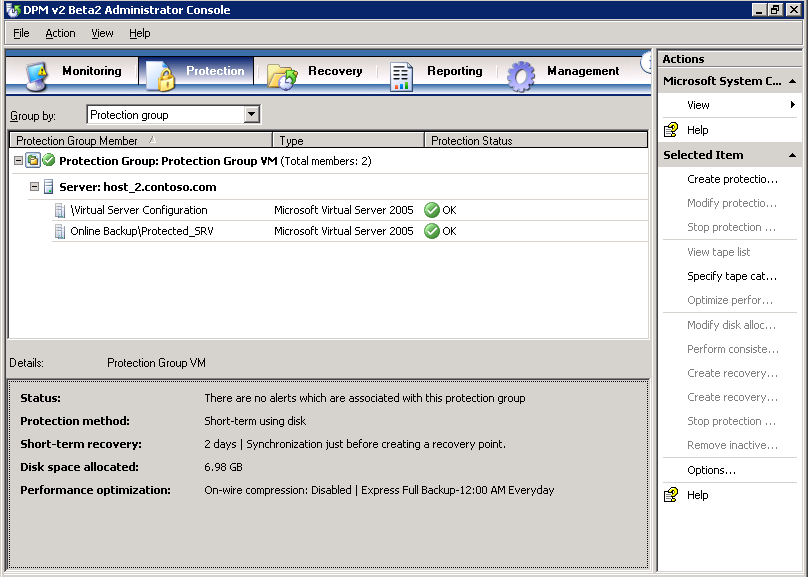


Figure Successfully protected servers in protection group

#### Restore a backed up virtual machine

1. In DPM Administrator Console, click the **Recovery** tab. Expand the tree on the left to navigate to **Protected\_SRV**, and then click it.

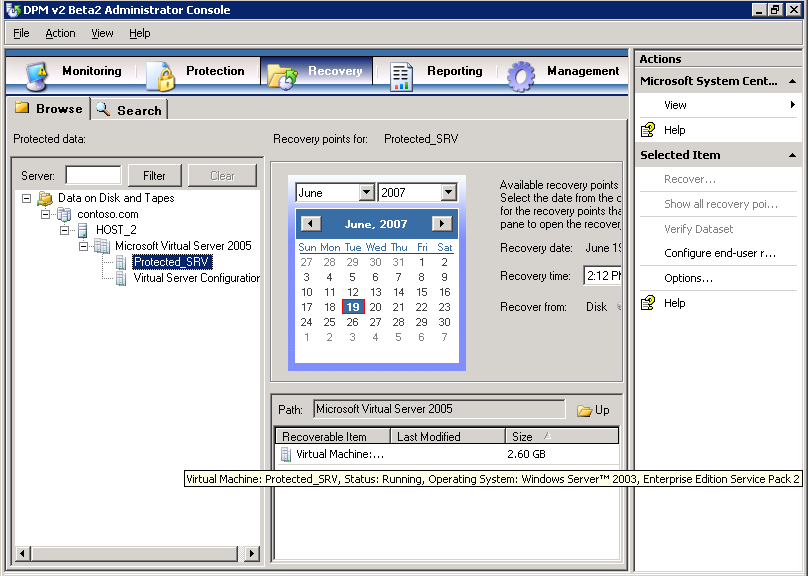


Figure DPM Administrator Console, Recovery tab

1. In the middle pane, right-click **Protected\_SRV**, and then select **Recover**. This will launch the **Recovery Wizard**.
2. On the **Review Recovery Selection** page, review the information presented for accuracy, and then click **Next**.

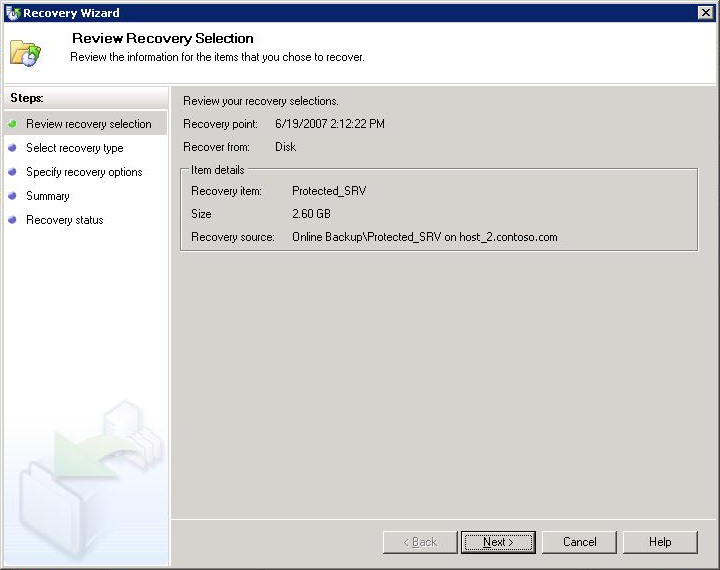


Figure 85 Recovery Wizard, Review Recovery Selection Page

1. On the **Select Recovery Type** page, click **Recover to original instance**, and then click **Next**. This will return the protected machine to its original location. If you would like to choose a new location for the protected machine restore, choose **Copy to a network folder**.

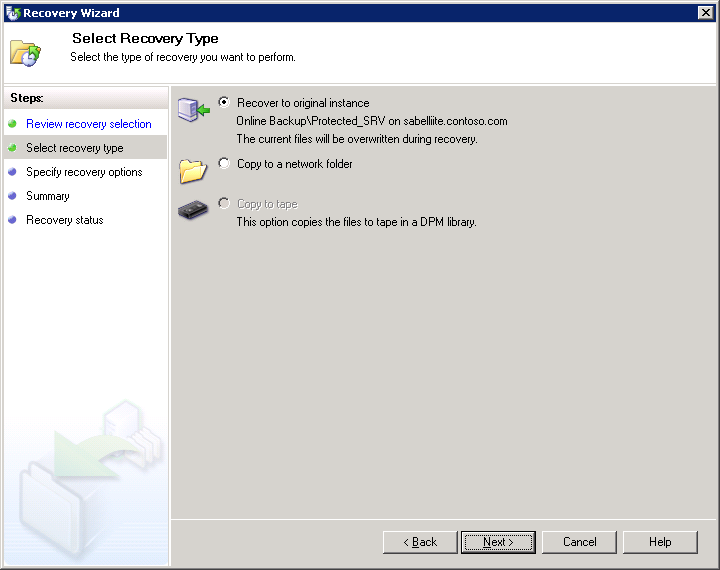


Figure Recovery Wizard, Select Recovery Type page

1. On the **Specify Recovery Options** page, you can choose to have an e-mail notification sent when the recovery completes. (This requires that you have already configured your DPM server for SMTP mail delivery.) In this example we will not send e-mail. Click **Next**.

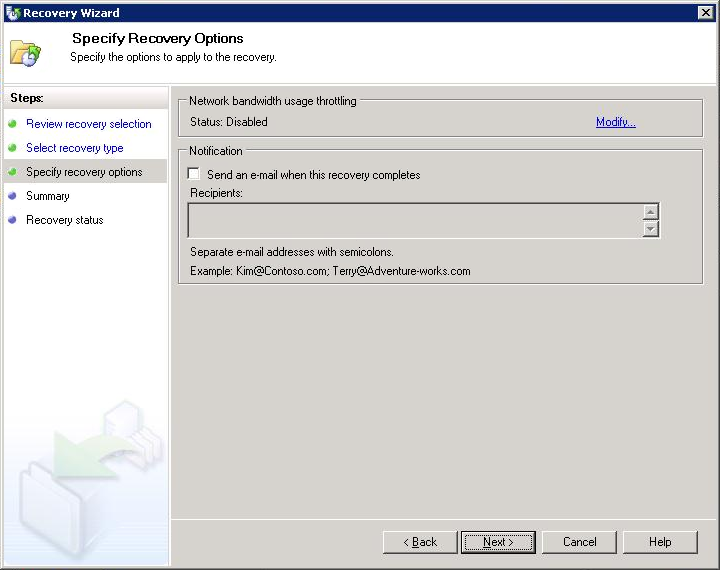


Figure Recovery Wizard, Specify Recovery Options page

1. On the **Summary** page, review the information presented for accuracy. Click **Recover**.

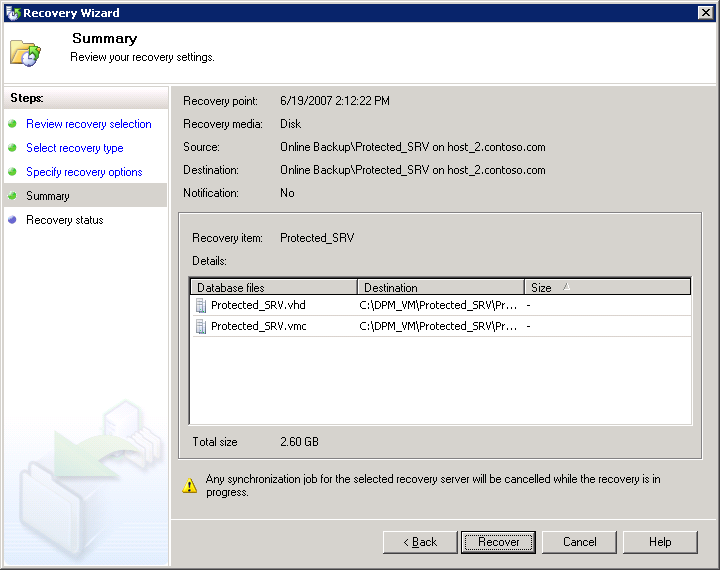


Figure Recovery Wizard, Summary page

1. Click **Close**.

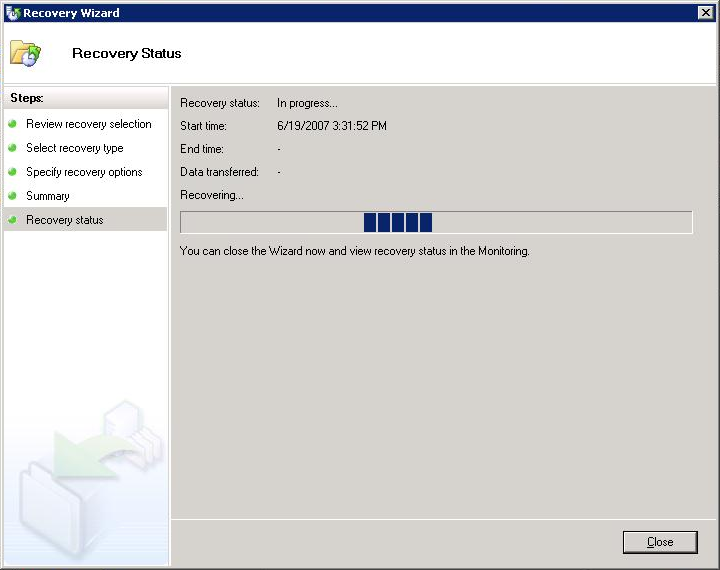


Figure Recovery Wizard, Recovery Status page

1. In DPM Administrator Console, click the **Monitoring** tab, and then click the **Jobs** tab. Keep an eye on your job. When your Restore job completes successfully, a green check ball and a **Completed** status will appear next to it.

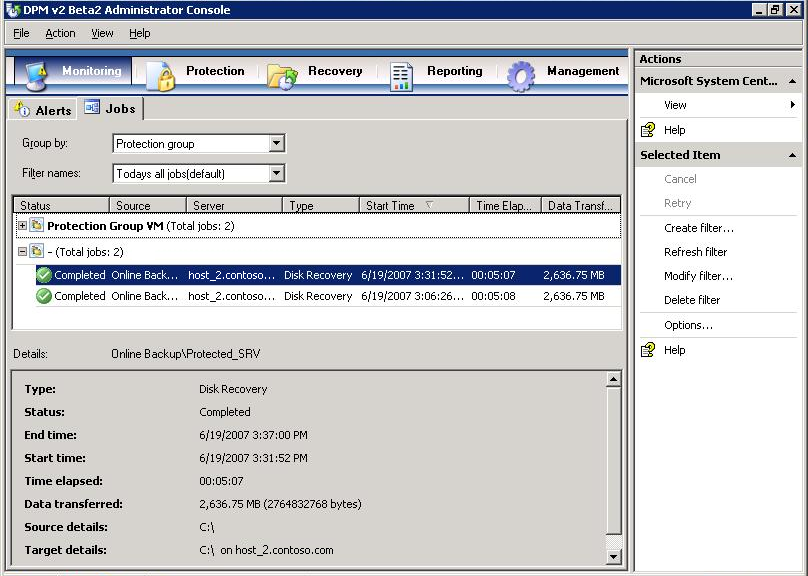


Figure DPM Administrator Console, Monitoring page, Jobs tab

1. Turn on your restored virtual machine. Your restoration is complete.

# Appendix B: DPM Protocols and Ports

If the computers that you want to protect reside behind a firewall, you must configure the firewall to allow communication between the DPM virtual machine, the customer computers that you are protecting, and the customer domain controller (or domain controllers).

Table 4 lists the protocols used by DPM and the ports associated with them. For specific guidance on which ports to open to incoming, outgoing, or bi-directional traffic, consult a network firewall expert.

Table Protocols and ports used by DPM

| **Protocol** | **Port** | **Details** |
| --- | --- | --- |
| DCOM | 135/TCP  Dynamic | The DPM control protocol uses DCOM. DPM issues commands to the file agent by invoking DCOM calls on the agent. The file agent responds by invoking DCOM calls on the DPM server.  TCP port 135 is the Distributed Computing Environment (DCE) endpoint resolution point used by DCOM. |
| TCP | 3148/TCP  3149/TCP | The DPM data channel is based on TCP. Both DPM and the file server initiate connections to enable DPM operations such as synchronization and recovery.  DPM communicates with the agent coordinator on port 3148 and with the file agent on port 3149. |
| DNS | 53/UDP | Used between DPM and the domain controller, and between the file server and the domain controller, for host name resolution. |
| Kerberos | 88/UDP  88/TCP | Used between DPM and the domain controller, and between the file server and the domain controller, for authentication of the connection endpoint. |
| LDAP | 389/TCP  389/UDP | Used between DPM and the domain controller for Active Directory queries. |
| NetBIOS | 137/UDP  138/UDP  139/TCP | Used between DPM and the file server, between DPM and the domain controller, and between the file server and the domain controller, for miscellaneous operations. |

# Appendix C: Install IIS via Control Panel

This alternate method for installing Internet Information Services is for installations of Virtual Server 2005 R2 SP1 on operating systems that do not have the Configure Your Server Wizard—for example, Windows XP Professional. Although Virtual Server 2005 R2 SP1 is supported on operating systems such as Windows XP Professional and Windows Small Business Server 2003, due to maximum supported memory and restrictions connected with operating systems other than the Windows Server family of operating systems, Microsoft does not recommend using such an operating system on the host machine running your DPM virtual machines in a production environment.

#### Install IIS by using Control Panel

You must install the World Wide Web Service component of IIS so that you can use the Administration Website to manage Virtual Server.

1. From the **Start** menu of the physical computer that will run the Virtual Server service, select **Settings** > **Control Panel**.
2. Double-click **Add or Remove Programs**.
3. In the left column, click **Add/Remove Windows Components**.
4. In the **Components** list box, select the check box next to **Application Server**, and then click **Details**.

**Note:** On this page and on subsequent pages of the wizard, leave check boxes that are already selected.

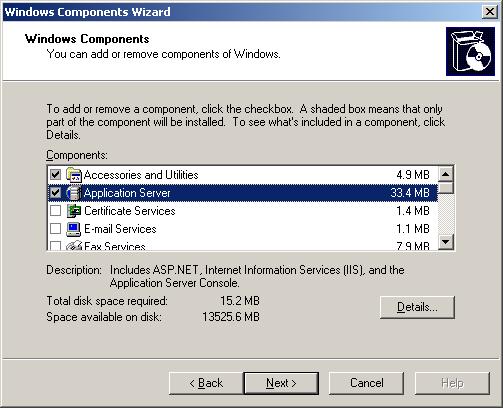


Figure Windows Components page

1. In the **Subcomponents of Application Server** list box, select the check box next to **Internet Information Services Manager**, and then click **Details**.

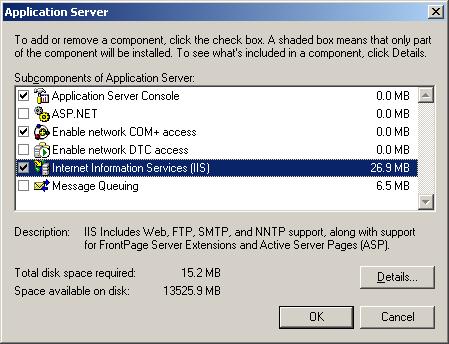


Figure Select IIS on Application Server page

1. In the **Subcomponents of Application Server** list box, select the check box next to **World Wide Web Service**, and then click **Details**.

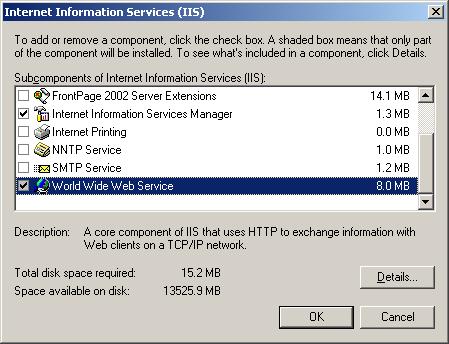


Figure Select World Wide Web Service on IIS page

1. Select the check box next to **World Wide Web Service**, and then click **OK**.

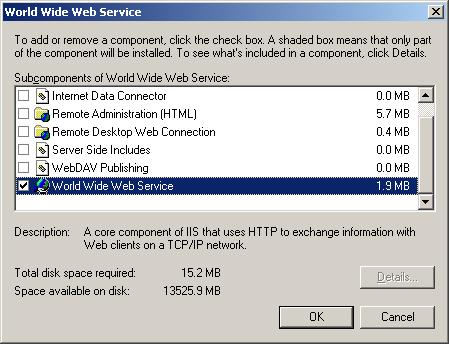


Figure Select World Wide Web Service on World Wide Web Service page

1. On the **Internet Information Services** page, click **OK**.
2. On the **Application Server** page, click **OK**.
3. On the **Windows Components** page, click **Next**. You will need the installation medium (CD or network file) for the operating system of this computer to complete this step.
4. Wait while the Windows Components Wizard configures these settings. Then, on the **Completing the Windows Components Wizard** page, click **Finish**.

# Appendix D: Virtual Server Security Considerations

Virtual Server has the following default configuration:

* The Virtual Machine Remote Control (VMRC) server is disabled.
* The VMRC server uses port 5900.
* Virtual Server uses Integrated Windows authentication.
* Only local administrators can access the Administration Website, configure Virtual Server, and create and configure virtual machines and virtual networks; other users must be granted the appropriate permissions manually. The Administration Website is a browser-based tool for configuring and managing Virtual Server and its associated virtual machines and virtual networks.
* Firewall and antivirus software running on the host operating system will not protect guest operating systems. To obtain this protection, you must install firewall and antivirus software directly on the guest operating systems.
* The two Virtual Server services run under security accounts that have low privileges: The Virtual Server service (Vssrvc.exe) runs under the Network Service account, which has limited access to the local computer and authenticated access (as the computer account) to network resources. The Virtual Machine Helper service (Vmh.exe) runs under the Local Service account. This account has limited access to the local computer and anonymous access to network resources.
* Only local administrators can configure Virtual Server or create and configure virtual machines. You can give other users the ability to create and configure virtual machines by changing file system security settings. Use care in giving such permissions to other users.
* Virtual machines run under the account of the user who started the virtual machine, unless you specify a different user account under which to run virtual machines and assign the user account to each virtual machine. Make sure that you specify a user account that has a low level of privileges.

**Note:** To provide a more secure file system, use NT File System (NTFS) on the server that will run the Virtual Server service.

# Appendix E: Install the iSCSI Initiator

1. Download the Microsoft iSCSI Software Initiator version 2.04 software from <http://www.microsoft.com/downloads/details.aspx?FamilyID=12cb3c1a-15d6-4585-b385-befd1319f825&DisplayLang=en>. Save it to a location on your hard disk drive.

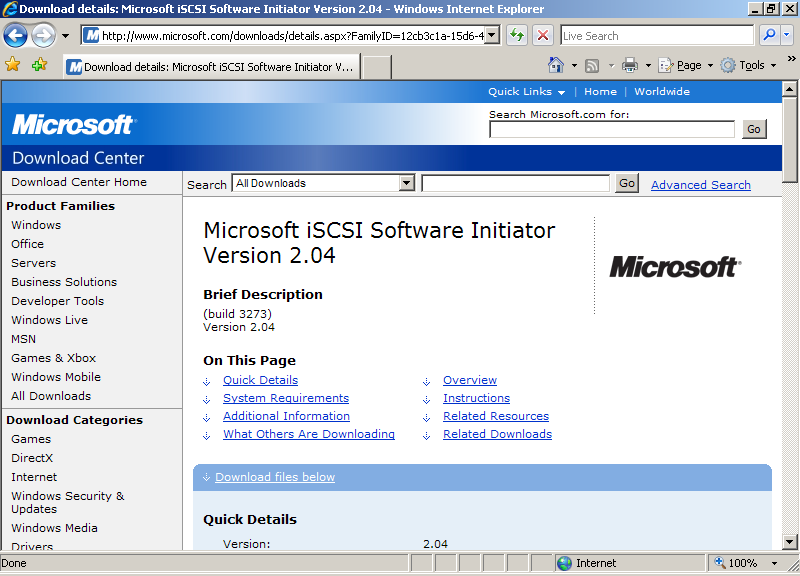


Figure Download Center

1. Double-click **Initiator-2.04-build3273-x86fre.exe**.

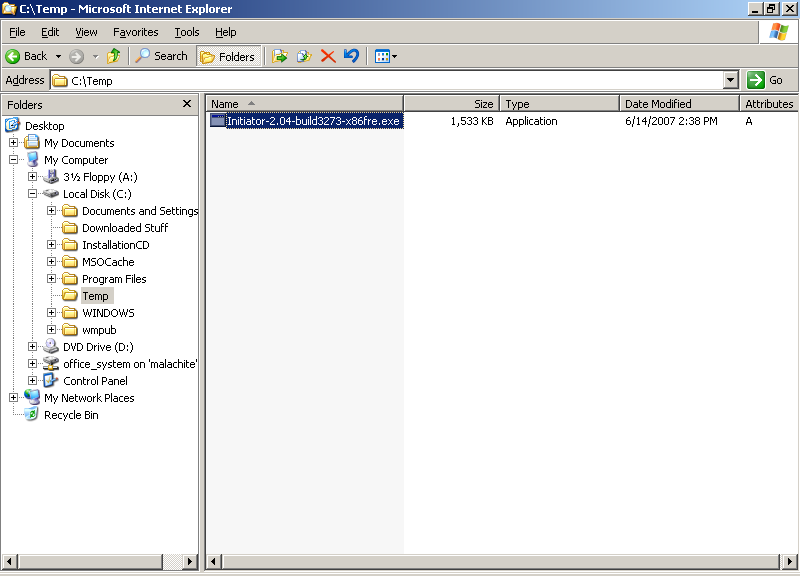


Figure Download initiator

1. When the **Software Installation Update Wizard** appears, click **Next**.



Figure Microsoft iSCSI Initiator page

1. Leave the default settings checked, and click **Next**.

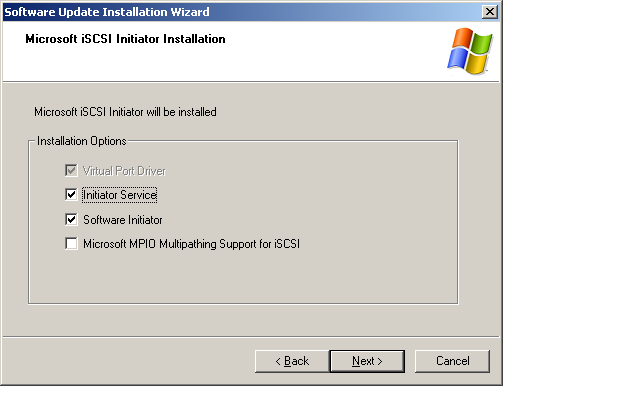


Figure Microsoft iSCSI Initiator Installation page

1. On the **License Agreement** page, read the license agreement, select **I Agree**, and then click **Next**.

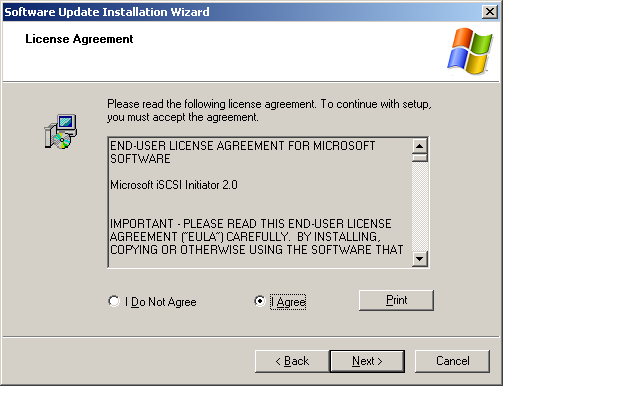


Figure License Agreement page

1. Wait while your system is updated.

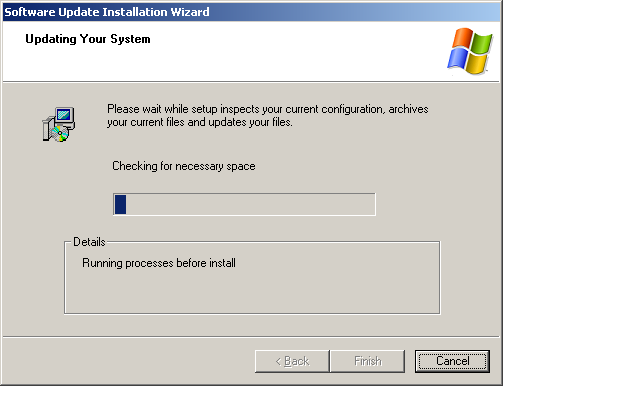


Figure Updating Your System page

1. When the installation process is complete, click **Finish**.

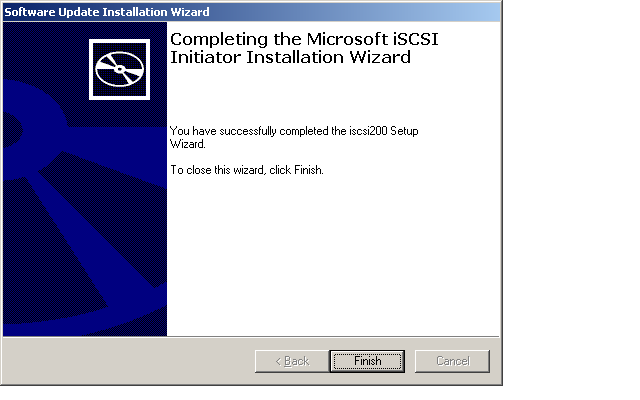


Figure Completing the Microsoft iSCSI Initiator Installation Wizard

1. Click **Start** > **Control Panel**, and double-click the **iSCSI Initiator** icon. The properties box will appear.

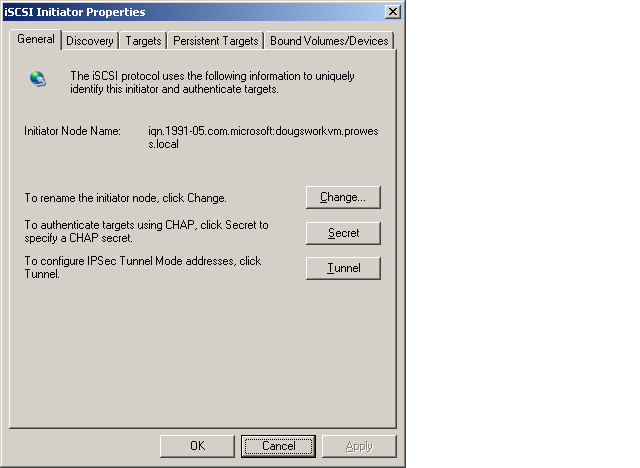


Figure iSCSI Initiator Properties

1. On the **General** tab, make note of your **Initiator Node Name**. This name is important, as it will be used by an iSCSI target device (SAN, tape device, or another type of storage device) to identify your computer.
2. Click the **Discovery** tab.

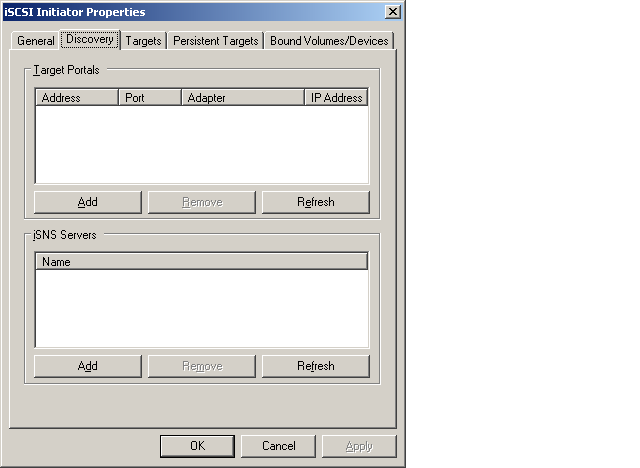


Figure iSCSI Initiator Properties page, Discovery tab

1. Under **Target Portals**, click **Add**.
2. Type the name or IP address of the iSCSI target that you want to use. Click **OK**.

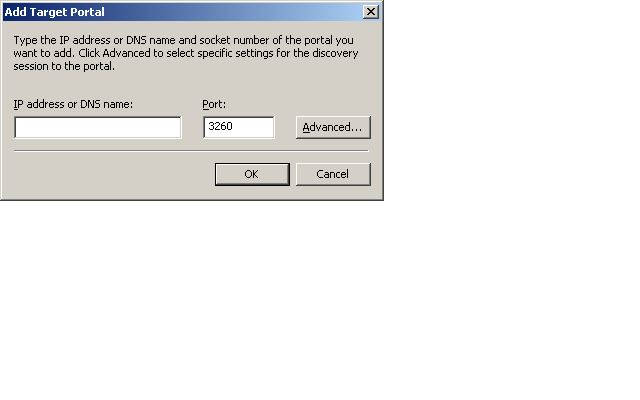


Figure Add Target Portal

1. You will now need to configure your iSCSI target device. See the documentation that came with your iSCSI target device for information.

# Related Links

For more information about Microsoft System Center Data Protection Manager, visit the Data Protection Manager home page at: [www.microsoft.com/systemcenter/dpm/default.mspx](http://www.microsoft.com/systemcenter/dpm/default.mspx)

For more information about Data Protection Manager 2007, visit: [www.microsoft.com/systemcenter/dpm/beta/overview.mspx](http://www.microsoft.com/systemcenter/dpm/beta/overview.mspx)

For more information about Virtual Server 2005 R2 SP1, visit the Virtual Server 2005 R2 home page at:  [www.microsoft.com/windowsserversystem/virtualserver/default.aspx](http://www.microsoft.com/windowsserversystem/virtualserver/default.aspx)

For more information about Intel Xeon processor-based servers, visit: [www.intel.com/products/server/processors/index.htm](http://www.intel.com/products/server/processors/index.htm)

For more information on Intel® Virtualization Technology, visit: [www.intel.com/technology/platform-technology/virtualization/](http://www.intel.com/technology/platform-technology/virtualization/)

To download Virtual Server 2005 R2 or Service Pack 1, visit the Microsoft Virtual Server TechCenter page at:   
[www.microsoft.com/technet/virtualserver/default.mspx](http://www.microsoft.com/technet/virtualserver/default.mspx)

Information in this document, including URL and other Internet Web site references, is subject to change without notice. Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, e-mail address, logo, person, place, or event is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

The names of manufacturers, products, or URLs are provided for informational purposes only and Microsoft makes no representations and warranties, either expressed, implied, or statutory, regarding these manufacturers or the use of the products with any Microsoft technologies. The inclusion of a manufacturer or product does not imply endorsement of Microsoft of the manufacturer or product. Links are provided to third-party sites. Such sites are not under the control of Microsoft and Microsoft is not responsible for the contents of any linked site or any link contained in a linked site, or any changes or updates to such sites. Microsoft is not responsible for webcasting or any other form of transmission received from any linked site. Microsoft is providing these links to you only as a convenience, and the inclusion of any link does not imply endorsement of Microsoft of the site or the products contained therein.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

Copyright © 2007 Microsoft Corporation. All rights reserved.

Microsoft are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

<The publications specialist inserts mention of specific, contractually obligated to, third-party trademarks, provided by the copy editor>

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.