

Infrastructure Planning
and Design

Microsoft® System Center Data Protection Manager 2007 with Service Pack 1

Version 1.1

Published: January 2009

Updated: July 2010

For the latest information, please see [microsoft.com/technet/SolutionAccelerators](http://www.microsoft.com/technet/solutionaccelerators/default.mspx)

Copyright © 2010 Microsoft Corporation. This documentation is licensed to you under the Creative Commons Attribution License.  To view a copy of this license, visit <http://creativecommons.org/licenses/by/3.0/us/> or send a letter to Creative Commons, 543 Howard Street, 5th Floor, San Francisco, California, 94105, USA.  When using this documentation, provide the following attribution: Infrastructure Planning and Design is provided with permission from Microsoft Corporation.

This documentation is provided to you for informational purposes only, and is provided to you entirely "AS IS". Your use of the documentation cannot be understood as substituting for customized service and information that might be developed by Microsoft Corporation for a particular user based upon that user’s particular environment. To the extent permitted by law, MICROSOFT MAKES NO WARRANTY OF ANY KIND, DISCLAIMS ALL EXPRESS, IMPLIED AND STATUTORY WARRANTIES, AND ASSUMES NO LIABILITY TO YOU FOR ANY DAMAGES OF ANY TYPE IN CONNECTION WITH THESE MATERIALS OR ANY INTELLECTUAL PROPERTY IN THEM.

Microsoft may have patents, patent applications, trademarks, or other intellectual property rights covering subject matter within this documentation. Except as provided in a separate agreement from Microsoft, your use of this document does not give you any license to these patents, trademarks or other intellectual property.

Information in this document, including URL and other Internet website references, is subject to change without notice. Unless otherwise noted, the example companies, organizations, products, domain names, email addresses, logos, people, places and events depicted herein are fictitious.

Microsoft, Active Directory, Hyper-V, SharePoint, Windows, Windows Server, and Windows Vista are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries and regions.

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

You have no obligation to give Microsoft any suggestions, comments or other feedback ("Feedback") relating to the documentation. However, if you do provide any Feedback to Microsoft then you provide to Microsoft, without charge, the right to use, share and commercialize your Feedback in any way and for any purpose. You also give to third parties, without charge, any patent rights needed for their products, technologies and services to use or interface with any specific parts of a Microsoft software or service that includes the Feedback. You will not give Feedback that is subject to a license that requires Microsoft to license its software or documentation to third parties because we include your Feedback in them.

Contents

[The Planning and Design Series Approach 1](#_Toc265427314)

[Overview of Microsoft System Center Data Protection Manager 2007 with SP1 2](#_Toc265427315)

[Introduction to the Microsoft System Center Data Protection Manager 2007 with Service Pack 1 Guide 3](#_Toc265427316)

[Data Protection Manager 2007 with SP1 in Microsoft Infrastructure Optimization 7](#_Toc265427317)

[Data Protection Manager Design Process 8](#_Toc265427318)

[Step 1: Define the Project Scope 10](#_Toc265427319)

[Step 2: Determine What Data Will Be Protected 13](#_Toc265427320)

[Step 3: Create Logical Design for Protection 17](#_Toc265427321)

[Step 4: Design the Storage 21](#_Toc265427322)

[Step 5: Design the DPM Server 26](#_Toc265427323)

[Conclusion 32](#_Toc265427324)

[Appendix A: Protected Environment 33](#_Toc265427325)

[Appendix B: Protection Strategy 34](#_Toc265427326)

[Appendix C: Protection Group Design 37](#_Toc265427327)

[Appendix D: Storage Planning 38](#_Toc265427328)

[Appendix E: DPM Servers Job Aid 43](#_Toc265427329)

[Appendix F: Additional Information on DPM 44](#_Toc265427330)

[Version History 47](#_Toc265427331)

[Acknowledgments 48](#_Toc265427332)

#

# The Planning and Design Series Approach

This guide is one in a series of planning and design guides that clarify and streamline the planning and design process for Microsoft® infrastructure technologies.

Each guide in the series addresses a unique infrastructure technology or scenario. These guides include the following topics:

* Defining the technical decision flow (flow chart) through the planning process.
* Describing the decisions to be made and the commonly available options to consider in making the decisions.
* Relating the decisions and options to the business in terms of cost, complexity, and other characteristics.
* Framing the decision in terms of additional questions to the business to ensure a comprehensive understanding of the appropriate business landscape.

The guides in this series are intended to complement and augment the product documentation.

## Benefits of Using This Guide

Using this guide will help an organization to plan the best architecture for the business and to deliver the most cost-effective data protection manager technology.

Benefits for Business Stakeholders/Decision Makers:

* Most cost-effective design solution for an implementation. Infrastructure Planning and Design (IPD) eliminates over-architecting and overspending by precisely matching the technology solution to the business needs.
* Alignment between the business and IT from the beginning of the design process to the end.

Benefits for Infrastructure Stakeholders/Decision Makers:

* Authoritative guidance. Microsoft is the best source for guidance about the design of Microsoft products.
* Business validation questions to ensure the solution meets the requirements of both business and infrastructure stakeholders.
* High integrity design criteria that includes product limitations.
* Fault-tolerant infrastructure, where necessary.
* Proportionate system and network availability to meet business requirements. Infrastructure that is sized appropriately to meet business requirements.

**Benefits for** Consultants or Partners:

* Rapid readiness for consulting engagements.
* Planning and design template to standardize design and peer reviews.
* A “leave-behind” for pre- and post-sales visits to customer sites.
* General classroom instruction/preparation.

Benefits for the Entire Organization:

Using this guide should result in a design that will be sized, configured, and appropriately placed to deliver a solution for achieving stated business requirements, while considering the performance, capacity, manageability, and fault tolerance of the system.

# Overview of Microsoft System Center Data Protection Manager 2007 with SP1

Data Protection Manager (DPM) 2007 is a member of the Microsoft System Center family of management products, which are designed to help IT pros manage their Windows Server® infrastructures.

First released in September 2007 and now including Service Pack 1 (SP1), DPM 2007 delivers data protection for Microsoft application and file servers to a disk and tape solution attached to the DPM server.

Microsoft designed DPM 2007 to protect and recover Microsoft SQL Server® data management software, Exchange Server, SharePoint® products and technologies, and Windows® Virtualization hosts (Microsoft Virtual Server and Hyper-V™), as well as Windows file services.

DPM 2007 provides protection for the core Windows Server-based workloads by backing up their critical files to a DPM server or appliance, which provides disk-based recovery and tape-based, long-term archival storage as well as disaster recovery from off-site repositories.



Figure 1. Overview of DPM functionality

# Introduction to the Microsoft System Center Data Protection Manager 2007 with Service Pack 1 Guide

This guide describes in detail the process of planning a Microsoft System Center Data Protection Manager (DPM) 2007 with SP1 infrastructure. The guide addresses the following fundamental decisions and tasks:

* Identify the type of data to be protected and the goals for recovering this data.
* Design a protection strategy to meet the recovery goals.
* Design the storage media and DPM server infrastructure.

Business objectives should be prioritized at the start of the project so that they are clearly understood and agreed on by IT and business managers.

Following the instructions in this guide will result in a design that is sized, configured, and appropriately placed to deliver the stated business benefits, while also considering the user experience, security, manageability, performance, capacity, and fault tolerance of the system.

The guide addresses the scenarios most likely to be encountered when designing a DPM infrastructure. Customers should consider having their architecture reviewed by Microsoft Customer Service and Support or by a Microsoft certified partner prior to implementation to ensure supportability of a particular design.

Figure 2 illustrates the relationship between the various components involved in delivering a data protection management solution with DPM.



Figure 2. Data Protection Manager architecture

The components can be designed in many different ways. Figure 2 shows the components in one implementation for illustrative purposes only.

## Key Terms

The following table contains definitions of key terms found in this guide.

Table 1. Key Terms

|  |  |
| --- | --- |
| Term | Definition |
| custom volume | A volume that is not in the DPM storage pool and is configured to store the replica and recovery points for a protection group member. |
| data source | The data that DPM considers as a unit for protection. DPM allocates separate storage for each data source. |
| differential backup | This term is not used with DPM. It refers to a backup in which all of the files that are new, or have changed since the last backup, are backed up. |
| express full backup | A type of backup that only transfers blocks that changed since the previous express full backup. This creates a new recovery point. |
| incremental backup | A type of backup that uses the application’s native form of incremental data protection. For example, for a server running SQL Server, it’s a log file backup; and for a server running Exchange Server, it’s a VSS incremental backup. Each incremental backup creates a new recovery point. With incremental backups, only the data that has changed since the most recent full or incremental backup are backed up, which means that the size of the incremental backup is usually much smaller than a full backup. |
| protection group | One or more data sources that are grouped together, to be protected in the same way, by the same DPM server. |
| recovery point | The point in time view of a previous version of a data source that is available for recovery from media managed by DPM. |
| replica | A full copy of a protected data source that reflects the result of the most recent DPM operation for that data source. |
| replica volume | A volume that holds the current copy of the protected data for a data source. |
| synchronization | The process by which DPM transfers changes to protected data from the protected computer to the DPM server, and applies the changes to the replica of the protected volume. |
| Volume Shadow Copy Service (VSS) | Provides the backup infrastructure for the Windows XP, Windows Vista®, Windows Server 2003, and Windows Server 2008 operating systems, as well as a mechanism for creating consistent point-in-time copies of data known as shadow copies. |

## Assumptions

To limit the scope of material in this guide, the following assumptions have been made:

* The decision to implement DPM 2007 with SP1 has already been made.
* Active Directory® Domain Services (AD DS) has already been designed. The DPM servers will be either in the same domain as the servers they protect, or there will be a two-way cross-domain or cross-forest trust into the domain where the protected servers will be located.
* The server environment that will be protected by DPM is Windows Server 2003 and Windows Server 2008.

## Feedback

Please direct questions and comments about this guide to satfdbk@microsoft.com.

We value your feedback on the usefulness of this guide. Please complete the following **Solution Accelerators Satisfaction Survey**, available at [http://go.microsoft.com/fwlink/?LinkID=132579](http://www.microsoft.com/IPD), and help us build better guidance and tools.

## IPD in Microsoft Operations Framework (MOF 4.0)

Microsoft Operations Framework (MOF) offers integrated best practices, principles, and activities to assist an organization in achieving reliable solutions and services. MOF provides guidance to help individuals and organizations create, operate, and support technology services, while helping to ensure the investment in technology delivers expected business value at an acceptable level of risk. MOF’s question-based guidance helps to determine what is needed for an organization now, as well as providing activities that will keep the organization running efficiently and effectively in the future.

Use MOF with IPD guides to ensure that people and process considerations are addressed when changes to an organization’s technology services are being planned.

* Use the Plan Phase to maintain focus on meeting business needs, consider business requirements and constraints, and align business strategy with the technology strategy. IPD helps to define an architecture that delivers the right solution as determined in the Plan Phase.
* Use the Deliver Phase to build solutions and deploy updated technology. In this phase, IPD helps IT pros design their technology infrastructures.
* Use the Operate Phase to plan for operations, service monitoring and control, as well as troubleshooting. The appropriate infrastructure, built with the help of IPD guides, can increase the efficiency and effectiveness of operating activities.
* Use the Manage Layer to work effectively and efficiently to make decisions that are in compliance with management objectives. The full value of sound architectural practices embodied in IPD will help deliver value to the top levels of a business.



Figure 3. The architecture of Microsoft Operations Framework (MOF) 4.0

# Data Protection Manager 2007 with SP1 in Microsoft Infrastructure Optimization

The Infrastructure Optimization (IO) Model at Microsoft groups IT processes and technologies across a continuum of organizational maturity. (For more information, see http://www.microsoft.com/infrastructure.) The model was developed by industry analysts, the Massachusetts Institute of Technology (MIT) Center for Information Systems Research (CISR), and Microsoft's own experiences with its enterprise customers. A key goal for Microsoft in creating the Infrastructure Optimization Model was to develop a simple way to use a maturity framework that is flexible and can easily be applied as the benchmark for technical capability and business value.

IO is structured around three information technology models: Core Infrastructure Optimization, Application Platform Optimization, and Business Productivity Infrastructure Optimization. According to the Core Infrastructure Optimization Model, protecting critical business data and applications will help move an organization to the Rationalized level. System Center Data Protection Manager 2007 provides the ability to protect the state and integrity of servers and workstations, as well as the files and applications that run on them, so in the event of data loss or corruption, the service can be quickly recovered.



Figure 4. Mapping of Data Protection Manager technology into Core Infrastructure Model

# Data Protection Manager Design Process

This guide addresses the following decisions and activities that must occur in planning the design for Data Protection Manager. The five steps that follow represent the most critical design elements in a well-planned Data Protection Manager design:

* Step 1: Define the Project Scope
* Step 2: Determine What Data Will Be Protected
* Step 3: Create Logical Design for Protection
* Step 4: Design the Storage
* Step 5: Design the DPM Server

## Decision Flow

The following figure provides a graphical overview of the steps in designing a Microsoft System Center Data Protection Manager 2007 with SP1 infrastructure.



Figure 5. The Data Protection Manager 2007 with SP1 infrastructure decision flow

## Information Collection

The following information is required in order to design a Data Protection Manager infrastructure:

* The Active Directory domain and forest design. This will be used in Step 5 to determine the number of DPM servers that will be required.
* The network topology design and available bandwidth.

## Applicable Scenarios

This guide addresses the following scenarios when planning and designing the necessary components for a successful implementation of Data Protection Manager:

* DPM is being used to replace an existing data protection solution.
* DPM will be implemented to provide protection for the Windows environment and may be integrated with an existing backup solution for third-party platforms.

## Out of Scope

The following topics are out of scope for this guide:

* Designing synchronization frequency and recovery point schedule. However, these configuration decisions need to be made prior to implementing DPM and will be used as input to the DPM infrastructure design.
* Storage technology recommendations.
* Virtual machine operating systems that are not VSS-aware.
* Using the DPM OEM appliance on Windows Storage Server, in place of DPM on Windows Server 2008 or Windows Server 2003.

# Step 1: Define the Project Scope

The scope of the data protection project will be defined in this step in order to align the goals of the project and the data protection capabilities of DPM with the business requirements for data protection, business continuity, and disaster recovery.

DPM can protect data for the following applications:

* Virtual machines (VMs) that are running on Windows Server 2008 Hyper-V or Virtual Server 2005 R2 SP1. Entire guest VMs can be protected.
* Microsoft Exchange Server 2007 and Exchange Server 2003 SP2. This protection applies to mailbox servers only.
* Microsoft SQL Server 2008, SQL Server 2005, and SQL Server 2000 SP4. Protection is at the database level.
* Windows SharePoint Services. DPM can protect data for servers running Windows SharePoint Services 3.0, Office SharePoint Server 2007, and Office SharePoint Portal Server 2003. This protection applies to the farm configuration database, the content server databases, and the search index on the SharePoint MOSS server.

DPM can also protect:

* Volumes, folders, and shares on:
* File servers running Windows Server 2008 or Windows Server 2003 SP1 or later.
* Workstations running Windows XP Professional SP2 and Windows Vista operating system editions except Home Premium or Home Basic.
* System state, including the system volume and the registry for all computers on which the DPM agent is supported.

Supported virtualization environments, application data, and files are listed at <http://technet.microsoft.com/en-us/dpm/bb808847.aspx>.

DPM is designed to provide data protection for the above files; it is not intended to be used as a general purpose backup tool, and it does not provide bare metal restore for Windows Server 2008.

In this step, the data protection requirements of each of the applications used by the business will be clearly defined so that these requirements can be used in turn to determine what data will be protected in Step 2, and to create the logical design for protection in Step 3.

## Task 1: Determine the Business Requirements for Protecting Data

To plan and design a DPM infrastructure, an organization needs to determine the business motivations for protecting data. First, determine which business applications are in scope for data protection and who owns and manages those applications and their data. Then, for each application, record the following information in Table A-1 in Appendix A: “Protected Environment.”

* **Data loss tolerance.** How much data can the business afford to lose (measured in minutes, hours, or days)? This is equivalent to the recovery point objective (RPO), which is the acceptable amount of data loss that can be tolerated, measured in time. DPM can back up changed data as frequently as every 15 minutes, or as infrequently as once a week. More frequent backups will increase the cost and complexity of the implementation.

The data loss tolerance will be used in Step 3 to determine how frequently backups will be made.

* **Retention range.** How long must protected data be kept available for recovery? This will be used to determine how long the protected data will be stored.

There may be regulatory requirements to protect the data for a minimum length of time, such as Sarbanes–Oxley (SOX), Health Insurance Portability and Accountability Act (HIPAA), or Payment Card Industry Data Security Standards (PCI DSS). Regulatory and compliance requirements may also mandate where the data must be stored. In some cases, the data retention period is years, which will require storing data on media that won’t degrade over a long period of time.

Data may also need to be protected sufficiently long enough to satisfy the requirements of business users who call the help desk to retrieve data they have accidentally deleted.

This retention range will be used in Step 3 to determine the logical design for protection, including the choice of media, and in Step 4 to design and place the storage for backups.

* **Speed of data recovery.** How quickly must the organization’s data be recovered after a problem occurs?This is one of the components of the recovery time objective (RTO), which is the time within which a business process must be restored to a serviceable state after a problem occurs. Restoring a business process to a serviceable state has many other dependencies in addition to the recovery of the application’s data. Indeed, the business service may be restored and made available to users prior to the recovery of protected data, which may occur over time as a background operation.

The requirements for speed of data recovery will be used to determine storage throughput and location in Step 4, and DPM server sizing and placement in Step 5. These requirements may also be used to determine the data protection approach: Data can be protected as a VM, which can enable very rapid recovery of an entire system to a newly provisioned machine. The decision whether to protect data as a VM will be determined in Step 5.

* End-user recovery. Should end users have the ability to recover files that that have become corrupt, deleted from their workstation, or on server file shares that they control, without the assistance of administrators? If this service will be provided to end users, the recovery client must be implemented on their workstations.
* **Disaster recovery.** Is the purpose for data protection part of a business continuity plan (BCP) or disaster recovery plan (DRP)? The BCP/DRP determines how quickly the organization must be operational again after a data loss event. How quickly the organization must be operational again will be used to decide how and where the data is stored in Step 4, and to determine whether DPM itself needs to be protected in Step 5. Ask the business for the assigned BCP/DRP priority of each application’s data based on:
* Scope of the user base that would be affected by an outage.
* Categorization of how an outage of that service would affect work (work stoppage, work impairment, sustainable workaround available, no impact).

The data protection goals must be clearly defined. For each business application requiring protection, record the data protection goals for it in Table A-1 in Appendix A.

## Validating with the Business

To ensure the business motivations for protection are clearly defined and understood, ask business stakeholders the following questions:

* **Are any changes planned for the future that may affect the portfolio of applications requiring data protection? Do any of the following need to be planned for in the data protection design?**
* Business acquisitions or divestitures.
* Applications that require data protection that may be retired or replaced.
* Files that may grow or reduce in size.
* New applications that require protection.
* **Are current business policies up to date with today’s internal and external governance requirements**? If not, they should be updated prior to the DPM data protection project so that the technology design can accurately reflect the business requirements.

The answers to these questions may affect the protection requirements and, therefore, the size or design of the infrastructure.

## Task 2: Review How Data Is Currently Protected

Determine if there is already a data protection infrastructure in place. Record this information in the job aid in Table A-2 in Appendix A. This information will be used in Step 5 if an existing solution is selected to protect the DPM server.

## Step Summary

In this step, the project scope was determined.

The outputs of Step 1 are:

* Completion of Table A-1 to record which business applications require data protection and to record the protection goals for data.
* Completion of Table A-2 to record the data protection infrastructure already in place.

## Additional Reading

* System Center Data Protection Manager 2007 Overview:

[http://technet.microsoft.com/en-us/dpm/bb798076.aspx](http://technet.microsoft.com/en-us/dpm/bb798076.aspx%20)

* Video: Technical Introduction to System Center Data Protection Manager 2007:

<http://www.microsoft.com/emea/spotlight/sessionh.aspx?videoid=987>

# Step 2: Determine What Data Will Be Protected

In Step 1, the business applications in scope for the project and their data protection requirements were determined. In this step, the data that must be protected and its location will be identified in order to design the DPM agent placement.

## Task 1: DPM Agent Placement

For each business application that was determined to be in scope in Step 1, determine where the DPM agent will be placed. Start by mapping the components of the application to data that is supported for protection by DPM, as listed in Step 1. For each business application, record the data that can be protected in Table B-1 in Appendix B: “Protection Strategy.” Next, design the DPM agent placement by following the sequence below.

### Decision 1: Does the Application Run in a Virtual Machine?

DPM can protect data in guest virtual machines (VMs) that are running on Windows Server 2008 Hyper-V or Virtual Server 2005 R2 SP1. If business application data that is in-scope for protection is in a VM, continue with this decision; otherwise, skip to Decision 2: “Are Exchange Server Mailboxes in Use?”

There are two options when backing up virtual machines:

* The entire guest can be protected as a VM, using the VSS Writer in the virtualization host.
* Data within the guest can be separately protected, using each application’s VSS Writer.

The implications of these options are shown in Table 4.

Table 2. Data Protection Options for Workloads in Virtual Machines

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| VM Protection Options | DPM Agent Placement | What Is Protected | What Is Not Protected | Recovery Granularity |
| Protect entire VM | On VM host | Entire system: all applications, files, system state, and OS.Host configuration file. | Pass-through disks that are attached to guest VMs. Deploy a DPM agent into the VM to protect these. | Entire VM must be recovered. |
| Protect data within the VM | On VM host and on each guest with data that requires protection | Data types that DPM supports. | Data types that are not supported by DPM. | Discrete data may be separately recovered. |

For each workload that runs within a VM, determine whether it will be protected as part of the VM using a DPM agent installed on the host machine, or whether its data will be protected separately by a DPM agent on the guest OS within the VM. If the data will be protected as part of a VM, there is no need to also separately protect it.

Record the location of the DPM agents in Table B-2 in Appendix B, and continue to the next decision.

### Decision 2: Are Exchange Server Mailboxes in Use?

If the business application includes Exchange Server mailbox data that must be protected, continue with this decision; otherwise skip to Decision 3: “Are SharePoint Servers in Use?”

The location of the DPM agent depends on the Exchange Server high-availability configuration that may be in place:

* **Exchange Server 2003 and Exchange Server 2007 single copy cluster (SCC).** The DPM agent must be installed on all nodes in the cluster.
* **Exchange Server 2007 local continuous replication (LCR).** Plan to install the DPM agent on both the active and passive node.
* **Exchange Server 2007 cluster continuous replication (CCR).** The DPM agent must be installed on both nodes in the cluster.
* **Exchange Server 2007 SP1 standby continuous replication (SCR).** Plan to install the DPM agent on the active node and the standby nodes.

Record the name of the server running Exchange Server on which the DPM agent will be installed in Table B-3 of Appendix B.

### Decision 3: Are SharePoint Servers in Use?

DPM is able to protect the following components of a Microsoft Office SharePoint Server (MOSS) farm:

* Farm configuration database, which is a SQL Server database
* SQL Server databases for the content servers
* Search index on the Enterprise Search server

DPM also provides this protection for Windows SharePoint Services (WSS) 3.0, except that this environment is not organized as a farm, and there is no farm server to protect.

If the business application includes SharePoint Server data that must be protected, continue with this decision; otherwise, skip to Decision 4: “Are SQL Server Databases in Use?”

Determine which farms should be protected, and plan to install a DPM agent on each farm server. Then, for each farm, determine which SQL Server databases DPM will protect; this determination will be used to design the storage in Step 4. SQL Server databases that are part of the farm do not need to be separately protected using the DPM SQL Server protection, so do not plan for these in the next decision.

Record in Table B-4 in Appendix B, the SharePoint server or MOSS farm server on which the DPM agent will be installed. Record also the SQL Server databases that will be protected as part of any MOSS farm so that they can be excluded from SQL Server database protection in the next decision. Then continue to the next decision.

### Decision 4: Are SQL Server Databases in Use?

If the business application includes SQL Server data that must be protected, and if the agent required for that has not already been designed in the previous decision, continue with this decision; otherwise, skip to Decision 5: “Protect Files?”

Record in Table B-5 in Appendix B which databases will be protected and which servers they run on. Plan to place a DPM agent on each of those servers.

The placement of the DPM agent also depends on the SQL Server high-availability configuration that may be in place:

* **Database mirroring.** Plan to install the DPM agent on both servers running SQL Server.
* **Log shipping.** Plan to install the DPM agent on both the primary and the standby SQL Server-based servers.
* **SQL Server cluster.** Plan to install the DPM agent on the primary server. DPM detects the cluster and installs the agent on other servers.

For databases that are implemented in one of the above high-availability configurations, record that configuration and the server names in Table B-5 in Appendix B. Continue to the next decision.

### Decision 5: Protect Files?

DPM can protect files stored on servers and workstations.

If the business application includes files that must be protected but which are not included in any of the above application-based protection, plan to protect them separately using the DPM file protection.

If necessary, map the files that require protection to the underlying file infrastructure based on the following criteria:

* If a Distributed File Share-Namespace (DFS-N) is used, map to the actual file locations because shares cannot be selected for protection through the DFS hierarchy; they must be selected by their target paths.
* If Distributed File Share-Replication (DFS-R) is used, map to all the replicas and then select one of them for protection. Protecting more than one replica is redundant and, in the case of a failure, DPM will transparently direct the end-user recovery to the protected replica.

Protecting a directory automatically includes all the directories and files underneath it in the protection. Determine whether that is necessary and, if not, exclude files, directories, and file extensions, as appropriate.

If protected files are held on user workstations, determine if the business requires that users be able to recover their file data themselves. If so, plan to install the DPM recovery point client software on the users’ machines.

Record all the files, folders, and shares that must be separately protected in Table B-6 in Appendix B, along with the name of the server or workstation on which they are stored. Then continue to the next decision.

### Decision 6: Protect System State?

DPM can protect critical system components for any computer on which the DPM agent is installed. This enables the machine’s state to be recovered, on similar hardware, if it should become corrupted or even unbootable. The system components that are protected are listed at <http://technet.microsoft.com/en-us/dpm/bb808714.aspx>. Review the list of all systems on which a DPM agent will be installed, and decide whether to also protect the system state.

Record all the systems for which system state will be protected in Table B-7 in Appendix B.

## Validating with the Business

To maximize the opportunity to use standard DPM protection for the application’s components, ask business stakeholders the following questions:

* Will any servers or components of the application be virtualized in the near future? If yes, the systems or applications that require protection could be protected as virtual machines, so it may be most effective to plan to protect them in this way.
* Could servers be moved from another virtualization platform to Windows Server 2008 Hyper-V? These systems could be additional candidates for protection using virtual machines, so they should be included in the planning process.

## Step Summary

In this step, the placement of DPM agents was designed.

The outputs of this step are:

* The placement of DPM agents.
* The systems for which system state will be protected.

## Additional Reading

* “What Do You Want to Protect?”:

<http://technet.microsoft.com/en-us/dpm/bb808876.aspx>

* “Application Data”:

<http://technet.microsoft.com/en-us/dpm/bb808662.aspx>

* “Exchange 2007 Local Continuous Replication”:

<http://technet.microsoft.com/en-us/library/bb125195.aspx>

* “Exchange 2007 Single Copy Clusters”:

<http://technet.microsoft.com/en-us/library/bb125217.aspx>

* “Exchange 2007 Cluster Continuous Replication”:

<http://technet.microsoft.com/en-us/library/bb124521.aspx>

* “Exchange 2007 Standby Continuous Replication”:

<http://technet.microsoft.com/en-us/library/bb676502.aspx>

* “Unsupported Data Types”:

<http://technet.microsoft.com/en-us/dpm/bb808689.aspx>

# Step 3: Create Logical Design for Protection

In Step 2, the placement of DPM agents was designed. In this step, the protection requirements for each data source will be translated into a logical design to deliver those requirements. In DPM, that logical design will be configured as one or more protection groups.

The collective elements of the protection group determine the design of the storage media in Step 4, and the DPM server infrastructure in Step 5.

## Understanding VSS Writer Limits

DPM uses the Volume Shadow Copy Service (VSS) to create backups to disk and is subject to some limitations in the VSS technology. Backups to tape do not use VSS and are not subject to VSS limitations.

DPM is a VSS requestor to file and application VSS Writers. The implementation of the VSS Writer is different for each of the data sources; this limits the number of backups that can be stored by a DPM server for each protected volume. The limits are as follows:

* File protection to disk is limited to 64 shadow copies. This limit is forced by the capabilities of the DPM client recovery capability that runs on workstation operating systems. It applies to protection of files on both workstation and server volumes, and it applies equally to administrator-managed recovery and end-user–managed recovery.

Configuration example: For files, DPM can store a maximum of 64 recovery points for each volume included in a protection group, and it can create a maximum of 8 scheduled recovery points (RPs) for each protection group each day.

Result: If there are 8 RPs a day, the retention range cannot be longer than 8 days.

* Application protection to disk is limited to 512 shadow copies, which translates to 512 express full backups. Incremental backups that occur between the express full backups are not counted toward this limit.

## Task 1: Determine the Recovery Goals for Each Data Source

In DPM, recovery goals are defined by synchronization frequency, retention range, and recovery point schedule.

Synchronization frequency is determined by the organization’s tolerance for data loss. Data loss tolerance is the maximum amount of data loss, measured in time, which is acceptable to business requirements. The data loss tolerance will determine how often DPM should synchronize with the protected server by collecting data changes from the protected server. The synchronization frequency can be changed to any interval between 15 minutes and 24 hours. It’s also possible to synchronize just before a recovery point is created, rather than on a specified time schedule.

Retention range is the length of time for which protected data must be kept for recovery, after which it expires and is overwritten.

DPM protects applications by backing up only the data that has changed since the previous backup, so more frequent backups will not result in duplicate data being stored. Likewise, recovery points are aggregated from previous recovery points; no duplicate data is stored, and so a more frequent recovery point schedule does not create greater storage space demand.

Refer to the requirements that were determined in Step 1 to understand what the recovery goals will be for each business application. Then map them to the data that will be protected for the application and record the details of each data source in Table C-1 in Appendix C as follows:

* Protected computer name.
* Whether the computer is a server or a workstation.
* The location of the data.
* The directory and file names of the data.
* Whether it is application data (and if so, which application) or file data.
* Data source size and rate of change.
* The protected volume name.

Next, record the synchronization frequency, retention range, and recovery point schedule in Table C-1 in Appendix C: “Protection Group Design.”

## Task 2: Determine the Protection Media

DPM 2007 offers the following data protection media: disk-based (D2D), tape-based (D2T), or a combination of disk-based and tape-based protection (D2D2T), in which data is backed up from the disk-based replica to tape.

The protection media is configured at the protection-group level. In order to use different media to protect two data sources, the data sources cannot belong to the same protection group.

The selection of disk or tape should be made using the following criteria:

* Whether the media type is suitable for a protection configuration that meets the recovery goals. For example, disk-based protection cannot protect data for longer than 512 days, whereas tape-based protection can retain the data for up to 99 years. And while disk-based protection can synchronize the replica as frequently as every 15 minutes, tape-based protection cannot back up data more frequently than once a day.
* File data can be recovered by end users only if it is on disk. End-user recovery is not available for data that is stored on tape. Refer to the protection business requirements that were determined in Step 1. If end users must be able to recover workstation files themselves, then protection must be to disk.
* How well the media meets the recovery goals. The advantages and disadvantages of each media type are covered in “Selecting a Data Protection Method” at <http://technet.microsoft.com/en-us/library/bb808739.aspx>.

Fill out the Media row in Table C-1 in Appendix C.

## Task 3: Determine How Replicas Will Be Created

If initial replica creation will be done automatically by DPM across the network, this will affect network sizing, especially if new members are added to the protection group on a frequent basis. The initial creation of the replica requires that all the protected data be copied to the replica.

An alternative would be to have the replica and the protected volume on the same storage area network (SAN), in which case the replica creation and the recovery could be SAN-based. However, this would still require sufficient bandwidth on the SAN.

If protection will cross wide area network (WAN) links, it may be better to manually make a local backup, then ship the physical media to the location storage location rather than monopolize the network during replica creation.

The replica creation method is configured at the protection-group level. Fill out the Replica Creation Method row in Table C-1 in Appendix C.

## Task 4: Organize Data Sources into Protection Groups

Now that the data sources that require protection have been identified and the recovery goals, protection media, and replica creation method have been decided, the data sources can be organized into protection groups.

A protection group can include data sources on more than one protected computer, and a protected computer can be a member of more than one protection group, but all the data sources on a protected computer must be protected by the same DPM server.

To organize data sources into protection groups, proceed in the following order:

1. Group all the data sources with retention ranges that are greater than 512 days. These data sources must be protected to tape and must therefore be in a tape-based protection group.
2. Group data sources that are in the same network locations with high bandwidth connections to each other. The bandwidth required between the data sources and the DPM server and its storage can be significant, so if there are a number of data sources together on a local network with available bandwidth, they may be grouped in a single protection group, and a DPM server and storage can be placed locally to protect them.

This applies especially if a dedicated, high-bandwidth backup network can be designed to connect a number of data sources.

1. Determine whether 32-bit or 64-bit hardware will be used for the DPM servers. The DPM product group recommends that DPM be run on a 64-bit server, which will enable it to address twice as much storage and support twice as many data sources than if it were run on a 32-bit server. Group the data sources as follows, according to the hardware form factor that will be used:
* If 32-bit hardware will be used, separate each group of data sources into subgroups of 128 or fewer.
* If 64-bit hardware will be used, separate each group of data sources into subgroups of 256 or fewer.

These limits are imposed by the Logical Disk Manager (LDM) database in Windows Server. Since a protection group cannot be spread across more than one DPM server, no protection group can include more than the above number of data sources.

1. For each group of data sources, compare the size of the data that will be protected against the following limits, which are based on the DPM server architecture that will be used:
* 5 terabytes for 32-bit DPM servers
* 22 terabytes for 64-bit DPM servers

If any group of data sources exceeds these limits, separate the data sources into subgroups that are below the limits. These limits apply because of limitations in storage addressable by the DPM server.

The DPM product group recommends using storage that is two times the size of the data that will be protected; the maximum storage supported on a single DPM server is:

* 10 terabytes for 32-bit DPM servers
* 45 terabytes for 64-bit DPM servers

Organize files, applications, and computers into protection groups, and then fill out the Protection Group Name row in Table C-1 in Appendix C for each protection group. Do not fill out the DPM Server row at this point; that will be done in Step 5.

## Step Summary

In this step, the logical design for protection was created.

The outputs of this step are:

* The recovery goals for each data source were determined.
* The protection media was determined.
* The replica creation method was determined.
* The data sources were organized into protection groups.

## Additional Reading

* “Selecting Protection Group Members”:

[http://technet.microsoft.com/en-us/library/bb795625.aspx](http://technet.microsoft.com/en-us/library/bb795625.aspx%20)

* “How Volume Shadow Copy Service Works”:

<http://technet.microsoft.com/en-us/library/cc785914.aspx>

* “Choosing a Replica Creation Method”:

<http://technet.microsoft.com/en-us/library/bb808709.aspx>.

# Step 4: Design the Storage

Now that the logical design for protection is complete, the storage required for that protection can be designed. If there is not enough storage space available when a DPM protection job runs, the job will fail. Table D-1 in Appendix D: “Storage Planning” provides a reference for the storage requirements of DPM for different protection designs, which can be useful during the storage design in this step.

## Task 1: Calculate the Storage Requirements on the File Protection Data Sources

Determine the storage space that must be allocated on protected file servers or workstations for the change journal. The change journal stores a map of the blocks on the volumes that have been selected for file protection. The DPM product group suggests allocating 300 MB on each protected machine for this purpose. But since each file change on an NTFS volume occupies approximately 100 bytes in this journal (possibly more, depending on the file name size), space should be reserved for that. The NTFS Update Sequence Number (USN) journal for an NTFS volume requires 128 MB per 100,000 files being tracked on that NTFS volume.

For each protected volume, refer to Table C-1 in Appendix C for the size of data that will be protected, and use that to calculate the storage required by the change journal on that protected volume. Then, add another 1 GB to enable the DPM agent to locally store auto release shadow copies while synchronization is in progress.

Record the change journal space requirement in Table D-2 in Appendix D and plan for this space to be available on each protected volume. Refer to “Description of FRS entries in the registry” at <http://support.microsoft.com/kb/221111/EN-US/> for information on how to change the journal space allocation.

## Task 2: Calculate the Storage Requirements for DPM

The DPM product group provides storage calculators that can be used to determine the storage required for each protection group. The calculation of required space can be complex if attempted manually, so it makes sense to use these calculators, not least because they ensure a supported configuration.

For each protection group that was defined in Step 3, use the data size and rate of change from the job aid in Appendix C as input to the disk or tape sizing. Use all of the following sizing tools as are appropriate for the environment:

* The DPM product group suggests designing storage that is two times the size of the data that will be protected in “Calculating Capacity Requirements” at <http://technet.microsoft.com/en-us/library/bb808859.aspx>. The DPM product will automatically use the default values at “Allocating Space for Protection Groups” at <http://technet.microsoft.com/en-us/library/bb795684.aspx> when calculating the required storage. These values are a starting point, which should then be refined by the use of the calculators.
* The product group provides a storage calculator at <http://blogs.technet.com/dpm/archive/2007/10/31/data-protection-manager-2007-storage-calculator.aspx>. This calculator only covers Exchange Server 2003 and Exchange Server 2007. It recommends not only storage sizing, but also the number of DPM servers that will be required.

The recommended number of servers is calculated using only the following subset of the criteria that will be use to determine the number of servers in Step 5:

* The DPM storage requirements (maximum of 40 terabytes). Note that as Step 5 states, this limit is currently 10 terabytes for 32-bit DPM servers, and 45 terabytes for 64-bit DPM servers.

So be sure to apply the server count process in Step 5 rather than relying on the server count output from this tool.

* A volume sizing tool is also available for download at <http://www.microsoft.com/downloads/details.aspx?FamilyID=445BC0CD-FC93-480D-98F0-3A5FB05D18D0&displaylang=en>.

Using these, determine the storage required for each protection group and record that in the Space Required column in Table D-2 in Appendix D. If the storage requirement for any protection group is greater than 10 terabytes and 32-bit DPM servers will be used, or if it’s greater than 45 terabytes and 64-bit DPM servers will be used, be prepared to split that protection group across more than one DPM server; this will be done in Step 5.

## Task 3: Determine Whether Custom Volumes Are Required

Custom volumes are disk volumes that are outside the DPM storage pool and are not managed by DPM. Custom volumes can be explicitly selected to store the replica and recovery points for a protection group member data source that requires them, unlike the DPM storage pool, which spreads data across all the volumes in the pool.

A custom volume can be any volume that uses block-level storage and is attached to the DPM server, except the volume that contains the system and program files for the DPM server. Custom volumes can be on basic or dynamic disks.

Select a custom volume for protection, rather than the DPM storage pool, for the following reasons:

* For critical data that must be manually separated onto a high performance Logical Unit Number (LUN). If the data were instead backed into the DPM storage pool, there would be no way to guarantee that it would be stored on that specific LUN, since DPM would make the data placement decisions.
* To meet regulatory requirements for separation. The DPM server treats the storage pool as a pool and will place all the data wherever it chooses within that pool. So a separate DPM server will be required, with another storage pool, if it is necessary to store certain data separately.
* To separate IO-intensive workloads across multiple spindles. DPM protects a data source by applying changes that occur to a single volume in the storage pool where the replica is stored. It also creates many dynamic volumes on the same physical disk for different data sources.

For applications that are highly IO-intensive, such as Exchange Server, and which likely have IO spread across multiple volume spindles, a single disk may not be able to deliver the required I/O operations per second (IOps) throughput. The only way to separate the IO onto different disks is to create custom volumes outside the storage pool.

Review the requirements for each of the disk-based protection groups determined in Step 3, and for each one, determine whether it has any of the above-listed characteristics. If so, plan to assign it a custom volume and record that in the Custom Volume or DPM Storage Pool column in Table D-2 in Appendix D.

## Task 4: Design the Disk Subsystem

Two volumes will be required for each protection group: one to hold the replica and another to hold the recovery points. The replicas and recovery points cannot share a volume.

In this task, the disk configuration must be selected for each protection group. The maximum supported addressable storage for a given DPM server is as follows:

* If 32-bit hardware will be used, separate each group of data sources into subgroups of 128 or fewer.
* If 64-bit hardware will be used, separate each group of data sources into subgroups of 256 or fewer.

The selection must be made in units that are within these limits.

### Disk Configuration

DPM can use any of the following non-removable disks for the storage pool and custom volumes:

* Direct attached storage (DAS)
* Fibre Channel storage area network (SAN)
* iSCSI storage device or SAN

USB or Firewire (IEEE 1394) disks cannot be used.

Any hardware-based configuration of redundant array of independent disks (RAID) or “just a bunch of disks” (JBOD) configuration can also be used.

To decide on the configuration for the disks, balance the relative importance of capacity, cost, reliability, and performance in the environment.

The disk configuration must deliver sufficient performance to support the required number of I/O operations per second (IOps). Two factors apply for each protection group:

* **Peak IOps during backup.** Since all members of a protection group will send data to the DPM server at the same time, this will create a spike in the write load on the storage. For protection to be effective, the disk subsystem throughput must be sufficient to write all the data to storage before the next timed backup begins.
* **Peak IOps during restore.** The DPM restore technology may require the restoration of an entire volume in order to recover a single Microsoft Exchange mailbox. The read IO performance of the disk subsystem must be sufficient to enable the business to meet the Recovery Time Objective for the business application.

Although it is not possible to calculate the required IOps in advance, benchmarks for backup and restore workloads may be available from SAN and disk vendors that may provide a baseline for estimating the required performance and the disk storage that can deliver it. Additionally, a test lab may be set up to simulate the production scenario using the selected disk subsystem and the IOps demand measured for both backup and restore operations.

Select the disk configuration and record that and the required IOps in Table D-2 in Appendix D.

## Task 5: Design the Tape Storage

DPM provides a list of tape libraries that have been tested and found compliant at <http://technet.microsoft.com/en-us/dpm/cc678583.aspx>. The tape library (or stand-alone tape drive) must be storage network-attached or SCSI-attached to the DPM server.

As with the disk configuration, the tape storage must be designed to deliver sufficient performance to support the required number IOps. Two factors apply to each protection group:

* **Peak IOps during backup.** Since all members of a protection group will send data to the DPM server at the same time, this will create a spike in the write load on the storage. For protection to be effective, the tape subsystem throughput must be sufficient to write all the data to storage before the next timed backup begins.
* **Peak IOps during restore.** The DPM restore technology may require the restoration of an entire volume in order to recover a single Microsoft Exchange mailbox. The read IO performance of the tape subsystem must be sufficient to enable the business to meet the Recovery Time Objective for the business application.

In order to achieve the required IOps, it may be necessary to design additional tape drives in parallel to achieve additional throughput, even if fewer tape drives are required to deliver the backup capacity. Alternatively, a virtual tape library that is actually disk hardware can be used to deliver higher throughput.

The co-location capability of DPM allows multiple protection groups with similar retention ranges to share the same tape drive so that each DPM server does not require its own tape drive. This requires that the tape library is storage network-attached and that the library-sharing update has been applied to DPM. However, in this configuration, if the database of one of the DPM servers fails, the tape library will become unavailable to all the other DPM servers. The SQL Server database cannot be put into an MSCS cluster because DPM does not support clustering the database.

Select tape storage devices for each protection group to deliver the required IOps and capacity and record the selections in Table D-2 in Appendix D.

To use a tape library that is not supported by DPM, it is possible to expose the shadow copies (using dpmbackup.exe) as a share, then back up the share with the tape library.

## Task 6: Place the Disk and Tape Storage

Refer to Step 3 where the design of the protection groups was completed and data sources were grouped into protection groups based on their network location. Plan to place the custom disks, the DPM storage pool, and the tape storage in close network proximity to the data sources in order to optimize the performance of backup and recovery operations. This decision will likely affect the placement of DPM servers in Step 5.

Placement involves a trade-off between performance and fault tolerance. To achieve optimal performance, the storage should be located local to the protected data sources. This is particularly important if business requirements necessitate rapid recovery. Whereas the DPM backup technology transfers only the recently changed blocks, a restore may need to transfer an entire volume. For example, although Microsoft Exchange restore can be at the single mailbox level, behind the scenes the entire storage group, possibly including more than one database, may have to be recovered to restore that one mailbox. However, ideally a backup should be stored remotely from the protected data source to avoid a single point of failure in the case of a location disaster.

Determine where the storage will be located and record it in Table D-2 in Appendix D.

## Step Summary

In this step, the required protection storage was designed.

The outputs for this step are:

* The storage requirements on the data sources were calculated.
* The disk and tape storage requirements for DPM were calculated.
* It was determined whether custom volumes are required.
* The disk subsystem was designed.
* The tape storage was designed.
* The storage location was determined.

## Additional Reading

* “Planning the Storage Pool”:

<http://technet.microsoft.com/en-us/library/bb808906.aspx>

* “Calculating Capacity Requirements”:

<http://technet.microsoft.com/en-us/library/bb808859.aspx>

* “Allocating Space for Protection Groups”:

<http://technet.microsoft.com/en-us/library/bb795684.aspx>

* Data Protection Manager 2007 Storage Calculator:

<http://blogs.technet.com/dpm/archive/2007/10/31/data-protection-manager-2007-storage-calculator.aspx>

and

<http://blogs.technet.com/dpm/attachment/2293158.ashx>

* System Center Data Protection Manager 2007 Tested Hardware:

<http://technet.microsoft.com/en-us/dpm/cc678583.aspx>

* Planning the Disk Configuration page:

<http://technet.microsoft.com/en-us/dpm/bb808694.aspx>

* Hardware Requirements page:

<http://technet.microsoft.com/en-us/library/bb808861.aspx>

* “Setting up Tape Library Sharing”:

<http://technet.microsoft.com/en-us/library/cc766563.aspx>

* “Troubleshooting File Replication Service,” which covers change journal sizing:

<http://technet.microsoft.com/en-us/library/bb727056.aspx>

* “Description of FRS entries in the registry”:

<http://support.microsoft.com/kb/221111/EN-US/>

# Step 5: Design the DPM Server

In Step 4, the data sources that require protection were organized into protection groups and the storage was designed to hold the protected data. In this step, the DPM server will be designed.

The DPM server performs backup and restore IO. It processes the incoming data from replica creation, synchronization, and incremental and express full backups, as well as writing to the storage media. When a restore is required, it must read and assemble the appropriate data from storage, then send it across the network to the protected computer.

The DPM server also administers the environment; it manages and stores the DPM configuration including the protection groups, and it produces reports.

## Task 1: Determine the Number of DPM Servers Required

To determine the number of DPM servers required, use the DPM sizing calculator provided by the product group, available at <http://blogs.technet.com/dpm/archive/2007/10/31/data-protection-manager-2007-storage-calculator.aspx>. It recommends the number of DPM servers needed to support a Microsoft Exchange infrastructure. This value is calculated based on the number of storage groups (maximum 250 per server) and the DPM storage requirements (40 terabytes is used in the calculation, but this limit is currently 10 terabytes for 32-bit DPM servers and 45 terabytes for 64-bit DPM servers). This calculator provides a starting point for Exchange Server, but it does not take into account all of the limits to which the DPM server is subject.

Start the design with one DPM server; then apply the following supported scale limits, in turn, to determine whether additional servers will be required:

* **Maximum 256 data sources per DPM server.** For 256 data sources, 512 volumes will be required because the replicas and recovery points are held on separate volumes. Since a dynamic volume cannot be increased in size more than twice, that would be 1,024 volume growths, which is the Windows Server limit imposed by the Logical Disk Manager (LDM) database when running in 64-bit mode. The limit when running the DPM server in 32-bit mode is 128 data sources.

Perform the calculation:

(# of protected data sources) \* 2 + # of volume resize <1024

and add additional servers until the condition is satisfied.

* **Maximum 8,000 VSS shadow copies.** A DPM server can store up to 9,000 disk-based shadow copies, including those retained when protection of a data source is stopped. This number must be reduced by 1,000 because it must be reserved for as needed activities, including recovery points created through the administrator UI or scripts, in addition to normally scheduled backups.

The shadow copy limit applies only to backups to disk that are based on VSS including:

* File recovery points.
* Express full backups.

Incremental synchronizations of protected applications are not counted toward this limit because those are copies of log files that do not use shadow copy. This limit is imposed by the Windows Server operating system.

Sum the shadow copies for all the data sources in all the protection groups that are instantiated on the DPM server. If the total is greater than 8,000, plan for additional DPM servers.

* **Volume Shadow Copy Service (VSS) addressing limits.** The VSS Writer is unable to address more than 10 terabytes of storage on 32-bit DPM servers. The addressing limit is greater on 64-bit DPM servers, but this has been tested up to 45 terabytes, and that is what is supported.

Because the DPM product group recommends using storage that is two times the size of the data that will be protected, 5 terabytes can be protected by a 32-bit DPM server and 22 terabytes can be protected by a 64-bit DPM server.

This limit applies only to backups to disk that are based on VSS shadow copy including:

* File recovery points.
* Express full backups.

Incremental synchronizations of protected applications are not counted toward this because those are copies of log files that do not leverage shadow copy.

If 32-bit servers will be used, add a server for every 5 terabytes that must be protected.

If 64-bit servers will be used, add a server for every 22 terabytes that must be protected.

* **Number of Exchange Server storage groups.** No more than 250 Exchange Server storage groups can be backed up by a single DPM server.

If more than 250 Exchange Server storage groups must be protected, add a server.

* **Maximum 75 protected servers and 150 protected workstations.** Since all data sources in a protection group will begin to transfer data to the DPM server at the same time, there can be significant competition for resources on the server. Based on testing, the DPM product group recommends that not more than 75 servers and 150 workstations be connected to a single DPM server.

If more than 75 servers and 150 workstations will be protected by a DPM server, add another server.

* **Data sources in an untrusted Active Directory domain.** A DPM server cannot back up a data source that is in another domain unless a domain trust or a forest trust is in place.

If there are data sources in untrusted domains, add DPM servers to the design for each of those domains, and record the name of the domain that necessitates the additional server.

Add a row to in Table E-1 in Appendix E: “Required DPM Servers Job Aid” for each DPM server that will be required.

## Task 2: Map Protection Groups to Servers and Storage

Now that the number of servers has been determined based on the protection group requirements and the architectural limits of the DPM infrastructure, determine which protection groups will be protected by which DPM servers. Refer to the protection group design that was created in Step 3 and recorded in Table C-1 in Appendix C.

No single protection group in that table is beyond the capabilities of a single DPM server, but some of them may be at or near the server limits that are documented in the previous tasks; map each of those protection groups to its own server.

For the remaining protection groups that have requirements that are less than a DPM server can support, attempt to match the protection groups, assembling them into super groups that can be combined while remaining within the limits of a DPM server.

When assembling super groups, apply the following criteria:

* Separate data that cannot coexist on the same server for legal or compliance reasons onto different DPM servers.
* Group protection groups that have different synchronization frequencies. All the data sources within a protection group send data to the DPM server at the same moment, which causes a spike in network traffic and server utilization. Matching protection groups that have different synchronization frequencies spreads that load more evenly.
* Group protection groups with the same media requirements. This can simplify storage configuration on the DPM servers because some of them may only require a single media type.
* Group protection groups that comprise data sources that are within the same high-speed network. That way the server can be placed in the same network location.
* Group protection groups for which doing so may ease administration. For example, group protection groups that will be backed up from or to VMs.

This is a manual process. The goal is to map all the protection groups onto as few physical servers as possible. Once the process is complete, record the assignments in Table C-1 in Appendix C by filling out the blank DPM Server Name row.

## Task 3: Design and Place the Servers

For each DPM server that will be designed, start by referring to the minimum and recommended hardware sizing provided in “Hardware Requirements” at <http://technet.microsoft.com/en-us/library/bb808861.aspx>. Use these as a base configuration; then for each of the components of the form factor listed below, add resources to the configuration as required. Record the form factor for each server in Appendix E.

### 32-Bit or 64-Bit

The DPM product group recommends that DPM be run on a 64-bit server. This will enable it to address twice as much storage and support twice as many data sources as discussed in the previous task. If the design requires a server to support more than 128 data sources or more than 10 terabytes of storage, use 64-bit servers.

### Virtual Memory

The DPM server requires a pagefile size that is 0.2 percent the size of all recovery point volumes combined, in addition to the recommended memory. For example, if the recovery point volumes on a DPM server total 3 terabytes, the pagefile size should be increased by 6 GB. Add this to the memory requirement for each DPM server.

The DPM product group sizing calculator, available at <http://blogs.technet.com/dpm/archive/2007/10/31/data-protection-manager-2007-storage-calculator.aspx>, provides the recommended virtual memory configuration needed to support DPM activities. This value is based on the amount of data being backed up. Calculate the virtual memory required, and add to the base configuration if necessary.

### Virtual Machine

The DPM 2007 with SP1 server can be run in a VM. If this will occur, the storage pool must be connected in one of the following ways:

* Using pass-through disks to enable the guest machine to directly access the disk on the Hyper-V virtualization host.
* Using an iSCSI storage device.

### Limits on Sharing with Other Servers

The product group does not support running the DPM server on the same computer as the following:

* Domain controller
* Exchange Server
* Microsoft Operations Manager 2005 Management Server
* Operations Manager 2007 Root Management Server
* Operations Manager 2007 Management Server
* Operations Manager 2007 Gateway Server

### Network Location

Although the DPM product documentation suggests the use of teamed network adapters on the DPM server to provide increased bandwidth and failover, Microsoft does not provide support for teamed network adapters, which are a third-party solution.

DPM requires a persistent network connection to the protected computers. Place the servers in a network location that will ensure this.

Refer to the protection group design that was created in Step 3 and recorded in
Table C-1 in Appendix C. Data sources were organized into protection groups based in part on their network proximity. Where network proximity was used as a primary criteria in the grouping, place DPM servers in the same location as the data sources.

## Task 4: Design the DPM Database

The DPM database stores the configuration of the DPM environment that is attached to the DPM server, including the protection group definitions.

Each DPM server requires a separate SQL Server instance. The SQL Server instances cannot be shared, but multiple SQL Server instances can be installed on the same machine.

The SQL Server instance can be on the DPM server or on a remote server. If it is on a remote server, it must be within the same forest as the DPM server. The SQL Server database is not supported on the same machine as a domain controller.

If a MOSS data source will be protected, it requires catalog space in the DPM database of 1 GB per 1 million MOSS/WSS farm items. This space is in addition to the minimum required space listed in “Hardware Requirements” at <http://technet.microsoft.com/en-us/library/bb808861.aspx>.

Determine which machine will be the database server, and record that in the Database Server column, and record the form factor of that server in the Form Factor column in the table in Appendix E.

## Task 5: Design the Reporting Components

SQL Server Reporting Services (SSRS) is used to create reports on the DPM environment for delivery to the administrator console in a web browser. SSRS cannot be separated from the DPM server, even if its reporting functionality is not required, so plan to implement SSRS on every DPM server.

DPM uses an instance of IIS to deliver reports to a web browser. If the SQL Server instance is remote from the DPM server, IIS is required on the server running SQL Server.

Determine the IIS server that will be used, and record it in Appendix E.

## Task 6: Determine Whether to Use a Dedicated Backup Network

When DPM backs up a production server, it has to compete for resources with application and user traffic traversing the same network adapter. This can be avoided by dedicating a backup network for workloads with a high rate of change.

Determine whether a dedicated backup network will be used and record it in Appendix E.

## Task 7: Design Fault Tolerance and Protection for DPM

Once DPM has been deployed to protect production data, the DPM server environment may become a critical resource. As such, fault tolerance of the DPM server infrastructure and data protection for DPM itself may be required.

To determine whether the DPM server requires fault tolerance and data protection, refer to the business requirements that were determined in Step 1.

Refer to Step 2, Task 2, to understand the criticality of each business applications’ components and to determine which applications require fault tolerance or data protection for DPM.

Two components can be made fault tolerant: the DPM server and the DPM database. In addition, the DPM server environment can be protected by a secondary DPM server.

### Fault Tolerance for the DPM Server

The DPM server cannot be run as an MSCS clustered application. The DPM server can be run in a VM, and the VM can be run on a host that is in an MSCS cluster.

### Fault Tolerance for the DPM Database

The DPM SQL Server database is not supported in an MSCS cluster.

A DPM server can protect its own databases by backing up the databases to tape. The DPM product group recommends that an additional unique protection group be created for protection of the DPM server databases. This may necessitate adding a DPM server to the design if existing DPM servers are already at any of the design limits that were covered earlier in this step.

### Data Protection for the DPM Server

A secondary DPM server can be designed to protect the DPM server.

Protecting DPM requires protection for the DPM SQL Server database and for the replicas of all the protected data sources.

The secondary DPM server is subject to the scalability limits listed in Task 1. It may be used to provide secondary protection to critical data, a subset of the data that the primary DPM server protects, so a secondary DPM server may be used to back up more than one primary DPM server.

DPM 2007 does not support a primary server and a secondary server protecting each other, so the secondary server must be dedicated to that function. Additionally, DPM does not support protection using chaining (when a third DPM server is used to protect a secondary DPM server).

The secondary DPM server can recover protected data, either to the primary DPM or directly to the protected data sources.

If DPM requires fault tolerance or protection, determine how that will be implemented and record the plan in Appendix E.

## Step Summary

In this step, the DPM servers were designed.

The outputs of this step are:

* The number of DPM servers required was determined.
* Protection groups were mapped to DPM servers and storage.
* The DPM servers were designed and placed.
* The DPM database was designed.
* The reporting components were designed.
* It was determined whether to use a dedicated backup network.
* Fault tolerance and protection was designed for DPM, if necessary.

## Additional Reading

* “Selecting the Number of DPM Servers”:

<http://technet.microsoft.com/en-us/library/bb808681.aspx>

* “Hardware Requirements”:

<http://technet.microsoft.com/en-us/library/bb808861.aspx>

* “Deployment Best Practices”:

<http://technet.microsoft.com/en-us/library/bb808899.aspx>

* “Best practices for using dynamic disks on Windows Server 2003-based computers”:

<http://support.microsoft.com/kb/816307>

* “Using Backup Network Address”:

<http://technet.microsoft.com/en-us/library/cc964298.aspx>

# Conclusion

This guide has summarized the critical design decisions, activities, and tasks required to enable a successful design of Data Protection Manager. It focused on decisions involving:

* What data will be protected.
* The logical design for protection, storage, and the DPM server.

The five steps in the decision flow required to develop a successful design were described in detail. Where appropriate, the decisions and tasks have been illustrated with typical usage scenarios.

When an architecture has been drafted, limited pilot tests should be conducted before a major rollout begins so that lessons learned can be incorporated back into the design.

This guide, when used in conjunction with product documentation, allows organizations to confidently plan the implementation of Data Protection Manager.

## Feedback

Please direct questions and comments about this guide to satfdbk@microsoft.com.

We value your feedback on the usefulness of this guide. Please complete the following **Solution Accelerators Satisfaction Survey**, available at [http://go.microsoft.com/fwlink/?LinkID=132579](http://www.microsoft.com/IPD), and help us build better guidance and tools.

#

# Appendix A: Protected Environment

Use the table below to record the business requirements for data protection for applications from Step 1 that are in scope for the project.

Table A-1. Business Application Data Protection Goals Job Aid

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Business Application | Application Owner | Data Loss Tolerance | Retention Range | Speed of Data Recovery | End-User Recovery | Disaster Recovery |
| <app name> | <app owner’s name> | <X mins/hrs/days> | <X years> | <X minutes> | <Yes or No> | <Offsite> |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

Use the table below to describe the current protection implementation from Step 1.

Table A-2. Current Protection Implementation Job Aid

|  |
| --- |
| Current Protection Implementation |
| <Description of current protection implementation> |

# Appendix B: Protection Strategy

This table is used to record the outputs from Step 2.

Table B-1. Protection Strategy Job Aid

| Business Application | Data That Can Be Protected | Runs in VM | Exchange Server Storage Groups | SQL Server Databases | SharePoint | Files |
| --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

This table is used to record the outputs from Step 2.

Table B-2. Protection Strategy for Virtual Machines Job Aid

| Business Application | VM Host | VM Guest | DPM Agent on Guest (Y or N) | Recovery Host |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |  |
|  |  |  |
|  |  |  |

This table is used to record the outputs from Step 2.

Table B-3. Protection Strategy for Exchange Server Data Job Aid

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Business Application | Exchange Mailboxes | Exchange Server Database | Storage Group to Protect | Exchange Server Name |
|  |  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |
|  |  |  |  |

This table is used to record the outputs from Step 2.

Table B-4. Protection Strategy for SharePoint Services Data Job Aid

|  |  |  |  |
| --- | --- | --- | --- |
| Business Application | MOSS Farm Name | SharePoint Server | SQL Server Databases |
|  |  |  |  |
|  |  |
|  |  |
|  | N/A |  |  |
|  |  |
|  |  |

This table is used to record the outputs from Step 2.

Table B-5. Protection Strategy for SQL Server Databases Job Aid

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Business Application | SQL Server Database | Primary Server | High-Availability Configuration | Secondary Server |
|  |  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |
|  |  |  |  |

This table is used to record the outputs from Step 2.

Table B-6. Protection Strategy for File Data Job Aid

| Business Application | File, Share, or Folder Name | Files and Folders to Exclude | Total Size | Machine | Server or Workstation |
| --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

This table is used to record the outputs from Step 2.

Table B-7. Protection Strategy for System State Job Aid

| Business Application | System Name | System State Protection |
| --- | --- | --- |
|  |  |  |
|  |  |
|  |  |
|  |  |  |
|  |  |
|  |  |
|  |  |  |

# Appendix C: Protection Group Design

Use a table like the one shown below to record the details of the protection groups as they are designed in Step 3.

Table C-1. Protection Group Design Job Aid

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Protected Computer #1** | **Protected Computer #2** | **Protected Computer #3** | **Protected Computer #4** |
| **Server or Workstation** |  |  |  |  |
| **Location** |  |  |  |  |
| **Data to Be Protected** |  |  |  |  |
| **Data Source Type** |  |  |  |  |
| **Data Size** |  |  |  |  |
| **Rate of Change** |  |  |  |  |
| **Protected Volume** |  |  |  |  |
| **Synchronization Frequency** |  |  |  |  |
| **Retention Range** |  |  |  |  |
| **Recovery Point Schedule** |  |  |  |  |
| **Media** |  |  |  |  |
| **Replica Creation Method** |  |  |  |  |
| **Protection Group Name** |  |  |  |  |
| **DPM Server** |  |  |  |  |

# Appendix D: Storage Planning

Use this table as a reference when designing the DPM storage in Step 4.

Table D-1. What Is Stored Where Job Aid

| Protection Type | Backup Type | VSS Writer Used | VSS Writer Limit | Storage Used on Data Source | What Is Sent over the Network | What Is Stored on DPM Server | Protection Media |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Short Term (to Disk) | Workstation files | Synchronization | Workstation file  | 64 shadow copies | Change journal contains pointers | Blocks that changed since previous synchronization | Synch, replica, and recovery points | Disk |
| Server files  | Synchronization | Workstation file  | 64 shadow copies | Change journal contains pointers | Blocks that changed since previous synchronization | Synch, replica, and recovery points | Disk |
| Exchange Server | Incremental backup | Exchange Server  | 96 incrementals per express full backup |  | Transaction logs | Transaction logs, replica, and recovery points | Disk |
| Express full backup | Exchange Server | 512 express full backups | Volume filter contains a bitmask, which includes 1 bit for every block within the protected dataset. | Blocks that have changed since previous snapshot | Replica and recovery points |

| Protection Type | Backup Type | VSS Writer Used | VSS Writer Limit | Storage Used on Data Source | What Is Sent over the Network | What Is Stored on DPM Server | Protection Media |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Short Term (to Disk) | SQL Server (except if read-only, log shipping, or Simple Recovery Model) | Incremental backup | SQL Server | 96 incrementals per express full backup |  | Transaction logs | Transaction logs, replica, and recovery points | Disk |
| Express full backup | SQL Server  | 512 express full backups | Volume filter contains a bitmask, which includes 1 bit for every block within the protected dataset. | Blocks that changed since previous synchronization | Replica and recovery points |
|  |  |  |  |  |  |  |  |
| SQL Server | Express full backup | SQL Server | 512 express full backups | Volume filter contains a bitmask, which includes 1 bit for every block within the protected dataset. | Blocks that changed since previous synchronization | Replica and recovery points | Disk |
| MOSS | Express full backup | MOSS  | 512 express full backups | Volume filter contains a bitmask, which includes 1 bit for every block within the protected dataset. | Blocks that changed since previous synchronization | Replica and recovery points | Disk |

| Protection Type | Backup Type | VSS Writer Used | VSS Writer Limit | Storage Used on Data Source | What Is Sent over the Network | What Is Stored on DPM Server | Protection Media |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Short Term (to Disk) | VMs | Express full backup | Hyper-V or Virtual Server | 512 express full backups | Volume filter contains a bitmask, which includes 1 bit for every block within the protected dataset. | Blocks that changed since previous synchronization | Replica and recovery points | Disk |
|  |  |  |  |  |  |  |  |  |
| Long Term (to Tape) | Workstation files | Synchronization | Workstation file  | No limit | Change journal contains pointers | Blocks that changed since previous synchronization | Synch, replica, and recovery points | Tape |
| Server files  | Synchronization | Workstation file  | No limit | Change journal contains pointers | Blocks that changed since previous synchronization | Synch, replica ,and recovery points | Tape |
| Exchange | Incremental backup | Exchange Server | Long-term express full backups only – not possible to protect incremental data on tape |  | Transaction logs | Transaction logs, replica and recovery points | Tape |
| Express full backup | Exchange Server  | No limit | Volume filter contains a bitmask, which includes 1 bit for every block within the protected dataset. | Blocks that have changed since previous snapshot | Replica and recovery points |
| SQL Server (except if read-only, log shipping or Simple Recovery Model) | Incremental backup | SQL Server  | Long-term express full backups only – not possible to protect incremental data on tape |  | Transaction logs | Transaction logs, replica, and recovery points | Tape |
| Express full backup | SQL Server  | No limit | Volume filter contains a bitmask, which includes 1 bit for every block within the protected dataset. | Blocks that changed since previous synchronization | Replica and recovery points |
| Long Term (to Tape) |  |  |  |  |  |  |  |  |
| SQL Server | Express Full backup | SQL Server | No limit | Volume filter contains a bitmask, which includes 1 bit for every block within the protected dataset. | Blocks that changed since previous synchronization | Replica and recovery points | Tape |

| Protection Type | Backup Type | VSS Writer Used | VSS Writer Limit | Storage Used on Data Source | What Is Sent over the Network | What Is Stored on DPM Server | Protection Media |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Long Term (to Tape) | MOSS | Express full backup | MOSS  | No limit | Volume filter contains a bitmask, which includes 1 bit for every block within the protected dataset. | Blocks that changed since previous synchronization | Replica and recovery points | Tape |
| VMs | Express full backup | Virtual Server/Hyper-V | No limit | Volume filter contains a bitmask, which includes 1 bit for every block within the protected dataset. | Blocks that changed since previous synchronization | Replica and recovery points | Tape |

Record the storage planning decisions in this table.

Table D-2. Storage Plan for DPM Protection Groups Job Aid

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Protection Group Name | Protected Volume | Change Journal Space Required | Space Required | Custom Volume or DPM Storage Pool | Disk or Tape Storage Configuration | IOps | Disk and Tape Storage Location |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

# Appendix E: DPM Servers Job Aid

Use the table below to record the number of DPM servers that will be designed.

Table E-1. Required DPM Servers Job Aid

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| DPM Server | Form Factor | Domain | Database Server | Form Factor | IIS Server | Dedicated Backup Network | DPM Fault Tolerance or Protection |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

# Appendix F: Additional Information on DPM

Background information provided here may be useful in planning for DPM.

## How DPM Protects Applications and Files

Protection works in different ways for each of the applications that DPM can protect.

### Exchange Server Protection

DPM protection for Microsoft Exchange Server applies to mailbox servers only.

On the mailbox server, DPM protects the database files, transaction logs, and indexes. It uses the Microsoft Exchange Server VSS Writer and operates at the storage-group level. In order to recover a single mailbox, DPM recovers the entire storage group. Therefore, DPM recovery is at its most granular when there is one database per storage group.

### MOSS and SharePoint Server Protection

The configuration of the MOSS farm, including all of its component databases, is discovered automatically from the farm server. Backup of all the components is coordinated centrally by the VSS Writer on the farm server, and all the backups flow through the farm server.

Individual items or sites that are protected by DPM for a MOSS farm cannot be recovered directly to that farm. If item-level recovery is required, DPM needs a recovery farm in place to bring up the protected database in an interim state before recovering the protected data to the production farm. So a separate recovery farm must be designed with sufficient disk capacity to hold the largest content database in the MOSS farm. The business requirement for speed of data recovery will determine the design of that recovery farm, as well as its placement within the DPM infrastructure. The recovery farm cannot be installed on:

* Any of the production SharePoint farms’ servers.
* Domain controller.
* DPM server machine, except as a recovery farm in a separate virtual machine.

### SQL Server Protection

DPM protection for SQL Server is at the database level, and each SQL Server database must be protected separately.

SQL Server can be configured in the following ways:

* **The primary database in a log shipping pair.** The transaction log is truncated every time it is shipped.
* **Simple Recovery Mode.** In this mode, the transaction log is truncated every time the log data is written to disk.
* **Read-only.** Since there are no updates, the database contents do not change and there is no transaction log.

If any of these configurations is used, the SQL Server database logs will not be available to DPM and so DPM’s incremental backup option will not be available, which may influence the design of the express full backup frequency.

To provide high availability, SQL Server can be implemented in the following ways (the implementation selected affects the way that DPM backs up the environment):

* **Database mirroring.** The primary server running SQL Server is made fault tolerant by the addition of a secondary redundant SQL Server-based server, and the database logs are replicated. DPM is used to protect the primary database. If that fails, SQL Server rolls to the mirror database, which DPM automatically recognizes, and protection is continued on the secondary server.
* **Log shipping.** A single SQL Server-based server writes into one database and the logs are shipped to a second database, which is updated.
* SQL Server cluster. Two servers in a cluster address a single database. If DPM protects that database and if the active server fails over to the passive server, DPM protection can continue automatically.

### File Server Protection

Folder shares and their permissions are not protected since these are server-specific and may not make sense if the files are recovered onto a different server. Shares must be recreated locally after recovery is completed.

Unsupported file types, such as reparse points and page files, are listed at <http://technet.microsoft.com/en-us/dpm/bb808689.aspx>. Note that when DPM backs up files that are encrypted by the Encrypting File System (EFS), it does not back up keys or certificates that will be required to decrypt those files.

## Protection Using Virtualized Environments

Applications that are not protected by DPM 2007 with SP1 may be protected if the systems they run on are virtualized and then protected as VMs running on Windows Server 2008 Hyper-V.

In addition, the protection provided by DPM can be used to provide additional protection options in a server virtualization environment together with Microsoft System Center Virtual Machine Manager (VMM) 2008. This can provide a very rapid restore capability from bare metal. Restoring a VM from scratch is far quicker than reinstalling the OS, restoring the system state, and then recovering the disk content (minutes versus hours).

The VMM physical to virtual machine migration (P2V) can be used to make a backup of a complete machine, perhaps once a week. If the system state, files, and application are then protected using a DPM server, in the event of a disaster, the system can quickly be recovered on another machine by using the VMM virtual machine to physical machine (V2P) to effect a bare metal restore, and then recovering and superimposing the updated system state, applications, and files from DPM. Alternatively, the backup VM can be simply moved to a production host, brought online, and the changed data restored to it from DPM.

This optimization involves additional planning that is beyond the scope of this guide. Refer to the IPD Guide for Windows Server Virtualization at <http://www.microsoft.com/ipd> for further information.

## Protection Groups

A protection group is a collection of one or more data sources that share the same protection configuration, which includes:

* For file protection, the synchronization schedule, which is the frequency at which DPM transfers change from protected systems to the DPM server. This applies to file protection to disk only.
* For application protection:
* Incremental backup schedule, which is the frequency at which DPM transfers changes from protected systems to the DPM server. This applies only to application protection to disk for Exchange Server and for SQL Server databases that are not in one of the following configurations:
* Primary database in a log shipping pair
* Simple Recovery Mode
* Read-only
* Express full backup schedule, which is the frequency at which DPM transfers changes to the protected application data since the previous express full backup.
* Retention range, which is the duration of time during which data is kept available for recovery.
* Replica creation method, which is the method used to transfer a complete point in time copy of the protected data to the DPM server. The replica must be created before protection can begin.
* Media, which is how the replica and recovery points will be stored: on disk or tape, or both (D2D, D2T, or D2D2T).

## Protection Schedule

For the following data types, DPM backups cannot occur more frequently than once every 15 minutes:

* Files
* VMs
* SharePoint-based servers, including MOSS
* SQL Server instances in one of the following configurations:
* Primary database in a log shipping pair
* Simple Recovery Mode
* Read-only

The most recent data, up to 14 minutes and 59 seconds, cannot be protected for these applications.

For servers running Exchange Server and SQL Server that are not in one of the above configurations, DPM can combine its protection with native capabilities of the application to deliver data protection to within the last minute.

## Additional Reading

* “Microsoft Support Policies and Recommendations for Exchange Servers in Hardware Virtualization Environments”:

<http://technet.microsoft.com/en-us/library/cc794548.aspx>

# Version History

|  |  |  |
| --- | --- | --- |
| **Version** | **Description** | **Date** |
| 1.1 | Minor updates to this guide to reflect current IPD template. | July 2010 |
| 1.0 | Original release. | January 2009 |

# Acknowledgments

The Solution Accelerators–Management and Infrastructure (SA-MI) team acknowledges and thanks the people who produced the *Infrastructure Planning and Design Guide for* Microsoft System Center Data Protection Manager 2007 with Service Pack 1. The following people were either directly responsible for or made a substantial contribution to the writing, development, and testing of this guide.

**Contributors:**

* Ruud Baars – *Microsoft*
* Jude Chosnyk – *GrandMasters*
* Sergio De Chiara – *Microsoft*
* David Muhich *– GrandMasters*
* Fergus Stewart – Microsoft

**Reviewers:**

* Karandeep Anand *–* Microsoft
* Jason Buffington *–* Microsoft
* Michael Kaczmar*ek* – Microsoft
* Calvin Keaton – Microsoft
* Jesper Krakhede – Capgemini
* Joshua Maher – Denali Advanced Integration
* Robin Maher – *Microsoft*
* René Scholten – Capgemini
* Melissa Stowe – *Microsoft*
* Ron Thomas *– GrandMasters*

**Editors:**

* Laurie Dunham – *Microsoft*
* Pat Rytkonen – *Volt Technical Services*