

## PS SERIES BEST PRACTICES

# Deploying Microsoft<sup>®</sup> System Center Data Protection Manager 2007 in an iSCSI SAN

### ABSTRACT

This Technical Report describes scenarios for deploying Microsoft System Center Data Protection Manager 2007 (DPM) with PS Series storage, providing a high performance, highly available, and scalable DPM storage pool.



Copyright © 2007 EqualLogic, Inc.

September 2007

EqualLogic is a registered trademark of EqualLogic, Inc.

All trademarks and registered trademarks mentioned herein are the property of their respective owners.

Possession, use, or copying of the documentation or the software described in this publication is authorized only under the license agreement specified herein.

EqualLogic, Inc. will not be held liable for technical or editorial errors or omissions contained herein. The information in this document is subject to change.

PS Series Firmware Version 3.2 or later.

EqualLogic Inc.  
110 Spit Brook Road  
Nashua, NH 03062

Tel: 603.579.9762  
Fax: 603.579.6910

## Table of Contents

---

Revision Information .....	iv
Introduction.....	1
Data Protection Manager 2007 Overview.....	1
Benefits of DPM over Traditional Tape-Only Backup Solutions.....	3
Benefits of Deploying DPM with PS Series Storage.....	4
DPM Server Deployment Options .....	5
DPM Server Local to Protected Servers .....	6
DPM Server Remote from Protected Servers .....	6
iSCSI SAN Replication of DPM Volumes .....	8
Requirements and Recommendations.....	10
PS Series Group Requirements .....	10
SAN Boot Recommendations .....	10
DPM Server Requirements and Recommendations.....	11
Requirements for Protected Servers.....	12
Network Requirements .....	14
Deploying DPM with PS Series Storage .....	14
Using Microsoft DPM to Protect Microsoft Exchange Server .....	15
Installing the DPM Server .....	16
SAN Initialization of the First DPM Replica.....	17
Protecting Exchange Server 2007 .....	18
Recovering Exchange Data.....	24
Using the SAN unique features of DPM to protect SQL 2005.....	25
Steps to follow for SAN recovery:.....	29
Power Shell Script: .....	31
Summary .....	33
Documentation and Customer Support.....	33
Related Links .....	34

## Revision Information

---

The following table describes the revision history of this Technical Report.

Technical Report Revision	Date	Change
1.0	September 27, 2007	First release
1.1	October 26, 2007	Updated release

**Table 1: Revision history**

Table 1.1 reflects the software and hardware revisions used for the preparation of this Technical Report.

Vendor	Product / Model	Software Revision
Microsoft®	Windows Server™ 2003	SP2
Microsoft	Microsoft System Center Data Protection Manager 2007	2.0.5785.0 (Evaluation version) July 2007
Microsoft	iSCSI Initiator Service	V 2.04
QLogic™	QLogic QLA405x iSCSI HBA	BIOS: 1.09 Firmware: 2.0.0.45
QLogic	SANsurfer Manager	4.03.18
EqualLogic	PS Series Firmware	Version 3.2
EqualLogic	Host Integration Tools Kit for Microsoft Windows	V2.2.1

**Table 1.1: Software and hardware Versions**

## Introduction

---

This Technical Report describes the benefits of using EqualLogic PS Series SAN storage with Microsoft System Center Data Protection Manager 2007 (DPM), a server software application that provides:

- Continuous Data Protection for Windows Application and File Servers protects Windows data by continuously capturing data changes with application-aware byte- and block-level agents, providing an easy-to-manage and robust disk/tape data protection solution, and one-click lossless application recovery.
- Rapid and Reliable Recovery enables IT administrators and end-users to easily recover data in minutes from easily accessible disk instead of locating and restoring from less-reliable tapes.

Intelligent PS Series storage arrays provide fast setup, automated management, easy scalability, multipath I/O (MPIO) support, SAN boot support, and remote volume replication. This makes a PS Series group—an iSCSI SAN consisting of one or more arrays connected to an IP network—an excellent choice for the storage pool resources used in DPM configurations. Not only does a PS Series SAN improve storage utilization efficiency and availability, it also delivers flexibility and ease-of-management—regardless of SAN scale.

In addition, data backup and recovery times can be dramatically reduced when PS Series SAN features are used in conjunction with DPM. The data replication features of DPM allow you to store multiple shadow copies of protected server data on disk-based PS Series storage, thus minimizing the need to recover from tape.

**Figure 1: PS Series Storage Array**



---

## Data Protection Manager 2007 Overview

Data Protection Manager (DPM) 2007, part of the Microsoft System Center family of management products, sets a new standard for Windows backup and recovery. With seamless support of disk and tape

backup, DPM delivers effective data protection for Microsoft application and file servers plus rapid and reliable data recovery for enterprises of all sizes.

Focused on the primary Microsoft server workloads, DPM was specifically built to protect and recover key Microsoft applications: Exchange Server, SQL Server™, SharePoint® Portal Server, Virtual Server, and Windows file services. These applications can now rely on a common platform for protection and recovery.

DPM captures the changes made to data in real time, and then synchronizes as often as every 15 minutes. For supported applications, DPM integrates a point-in-time database restore with existing application logs to deliver “zero data loss” recovery of the application data – eliminating the constant replication or synchronization that would otherwise be required. The benefits of DPM include:

**Rapid Recovery** – Backing up data to disk provides the fastest way to recover data that’s been lost due to user error or software and hardware corruption. With DPM, recovering information is as simple as browsing a share and copying directly from the DPM platform to the production server within seconds. By restoring data from disk, DPM enables customers to recover data in minutes, instead of the hours it takes to recover from tape.

**Reliable Recovery** – DPM leverages disk-based backup to provide the highest level of reliability, which traditional—and often unpredictable—tape backup methods cannot offer. All tape backup failure points (including corrupt indexes, broken media, misplaced cartridges, and human error) can be avoided by relying on disk storage as the primary restoration medium, while still leveraging tape for long-term archival storage.

**Seamless Disk and Tape Integration** – DPM transparently leverages both disk and tape mediums to enable fast, multiple points-in-time-per-day restores from disk, while ensuring long term retention and off site portability with disk.

**Unified Protection Policies Across Data Types** – DPM allows protection to be configured across heterogeneous applications and file-sharing platforms with a single policy. This allows you to manage logical groupings of data from a single UI—delivering Exchange, SQL, SharePoint, and file data mixed, within a single policy, to any combination of disk and tape protection.

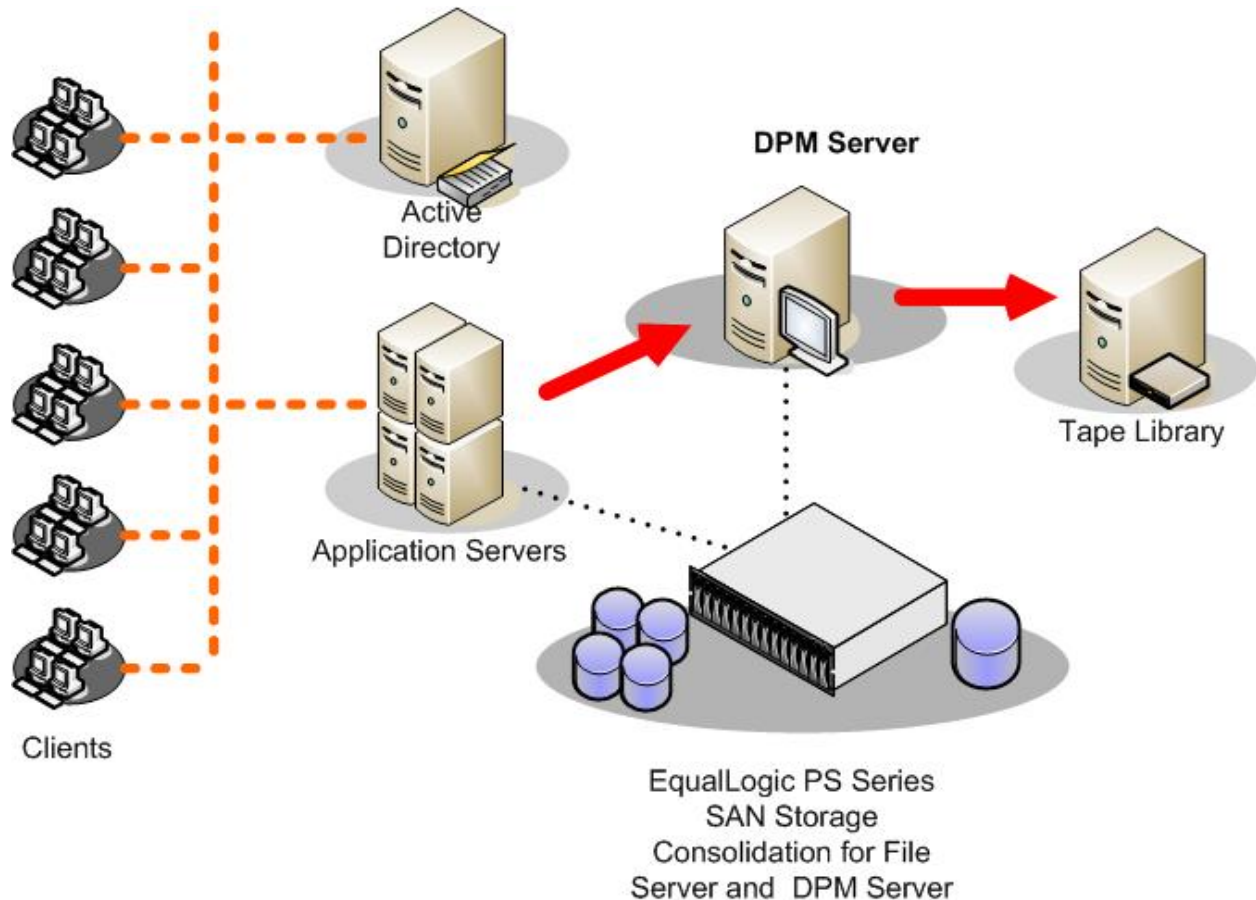
**SLA-driven Backup Process** – Protection policies are based on intent and SLAs, creating a layer of abstraction that insulates the user from the often confusing process of scheduling individual backup jobs in order to meet an overall SLA.

**Block Filter** – With an efficient disk infrastructure and reduced network traffic, DPM’s volume filter changes how backups are achieved and maintained. For instance:

- The volume of full backups can be reduced by as much as 90 percent, saving disk space and reducing backup time from hours to minutes.
- Express full backups and an enhanced network throttling mechanism allow for more granular management of bandwidth.

Figure 2 depicts a basic DPM configuration with a single DPM server, a PS Series group with one array (group member) for the DPM storage pool, and four protected servers supporting multiple clients within an Active Directory Domain.

**Figure 2: DPM in Disk-to-Disk-to-Tape Deployment With iSCSI SAN Storage and 3<sup>rd</sup> Party Tape Software**



Deploying DPM with a PS Series SAN provides multiple benefits to administrators who want complete control of data backups and real-time information on backup status. Benefits include rapid configuration of the DPM environment, simple and immediate storage pool expansion, and flexibility for remote site volume replication. A completely redundant environment can be configured using multipath I/O technology, which improves the reliability of the DPM server.

In addition, with a PS Series SAN, you can boot the DPM server and the protected application servers from the SAN, resulting in a configuration that can support nearly immediate system recovery.

## **Benefits of DPM over Traditional Tape-Only Backup Solutions**

DPM provides a new form of data protection by providing near-continuous disk backups for protected file servers. In DPM configurations, backups are run throughout the day, minimizing the amount of work lost in the event of data loss.

DPM delivers the following capabilities:

- **Efficient, near-continuous data protection.** DPM logs and replicates byte-level changes to the data on the protected servers. This allows for near-continuous backups with minimum data movement between protected servers and the DPM server.
- **Flexible backup scheduling.** DPM provides default schedules for hourly and daily backups, but IT administrators can also customize protection schedules for specific server data.
- **Multiple point-in-time backups using frequent shadow copies.** Shadow copies are also known as snapshots or point-in-time, past-time, or cache copies. DPM uses the Windows Server 2003 Volume Shadow Copy Service (VSS) component to create shadow copies of the protected data and store them on the DPM server.
- **Protection from network outages and hardware failures.** The DPM agent logs and backs up the data from each of the protected servers to the server running DPM. If the protected server goes down or is destroyed, a copy of the data is still available on the server running DPM.
- **Network throttling.** You can minimize the impact that backups will have on your network by using the ability of DPM to throttle network traffic by setting limits for maximum network utilization. On-the-wire compression can also be used to minimize the data that is transferred.
- **Integration without disruption.** DPM integrates with existing backup systems to supplement them, not replace them. At any time, IT administrators can backup data to tape using existing tape backup products from the server running DPM, thus off-loading the backup processing from the protected file server and eliminating the backup window problem.

---

## Benefits of Deploying DPM with PS Series Storage

The benefits of deploying DPM with a PS Series SAN are as follows:

- **Rapid configuration of the DPM storage pool** – Whether the PS Series storage is configured as simply an additional volume within the DPM storage pool or as the total storage provider for the DPM server, storage management operations can be completed quickly. A simple setup utility lets you quickly configure an array on the network and create a PS Series group. Automation of complex operations such as RAID configuration, disk sparing, data provisioning, and load balancing means that even novices can effectively manage the SAN.
- **Redundant hardware and hot serviceable configuration** – PS Series storage arrays are fully redundant with dual controllers, power supplies, and fans—all of which can be serviced online and without disrupting applications. In addition, support for multipath I/O enables you to configure multiple paths between servers and storage, providing end-to-end redundancy for primary data as well as for the DPM storage pool. This ensures maximum reliability and online operation.
- **SAN boot capability** – By configuring DPM to boot from the PS Series SAN, server hardware can be quickly replaced in the event of a failure without needing to re-install the server or DPM, thus dramatically increasing disaster tolerance and reducing recovery time. iSCSI HBAs provide increased I/O performance as well as the ability to install and boot the Windows operating system from a SAN.

- **Simple and immediate DPM storage pool expansion** – A PS Series SAN works in harmony with the DPM software to provide online storage pool expansion. Whether you deploy PS Series storage only for the DPM storage pool or as the total storage solution for the DPM server and the protected file servers, you can quickly expand the SAN with no disruption to users.
- **Network path protection and load balancing** – MPIO enhances the reliability and performance of DPM by providing dynamic load balancing of iSCSI SAN traffic across multiple paths between the DPM server and the PS Series SAN.
- **Dramatic time reduction in initial DPM replication operations** – When a PS Series SAN provides storage resources for the DPM storage pool and the protected servers, the DPM server can initialize the first replica of a protected server's data from a SAN Clone. This SAN feature can dramatically reduce the time required for the initial replication operation as well as reducing overhead on the protected server and the network during the initial replication.
- **Remote site PS Series volume replication** – With PS Series volume replication, data can be automatically transferred to remote data centers, protecting it from serious failures ranging from volume destruction to a complete site disaster—with no impact on data availability or performance.
- **SAN recovery** – SAN Recovery allows DPM to recover an application such as Exchange or SQL using hardware snapshots, bypassing the LAN.

## **DPM Server Deployment Options**

---

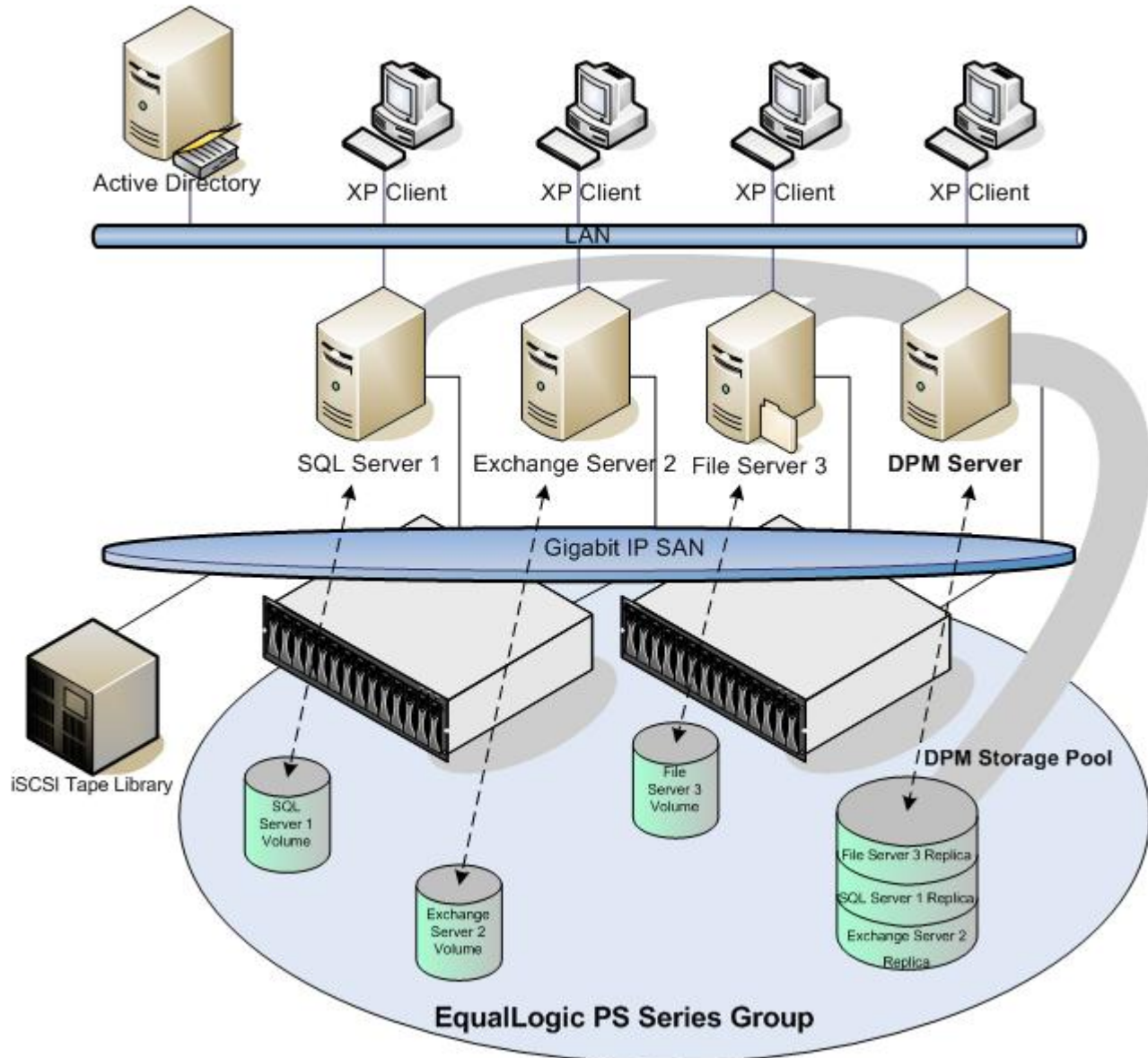
Three common deployment topologies using DPM and a PS Series SAN are presented in the sections that follow.

- The first topology (Figure 3) locates the DPM server in the same LAN as the protected servers and the PS Series SAN.
- In the second topology (Figure 4), the DPM server is located in a LAN that is across a WAN.
- The third topology (Figure 5) demonstrates deployment of the DPM server in the same LAN as the protected servers and the PS Series SAN, but also includes another PS Series SAN that is located remotely, so the DPM storage can be replicated to the remote SAN.

## DPM Server Local to Protected Servers

Typically, DPM is deployed in the same data center as the servers it is protecting. This ensures high-performance operations when protecting data, as well as when recovering data.

**Figure 3: DPM Server Local to the Protected Servers and the PS Series Arrays**



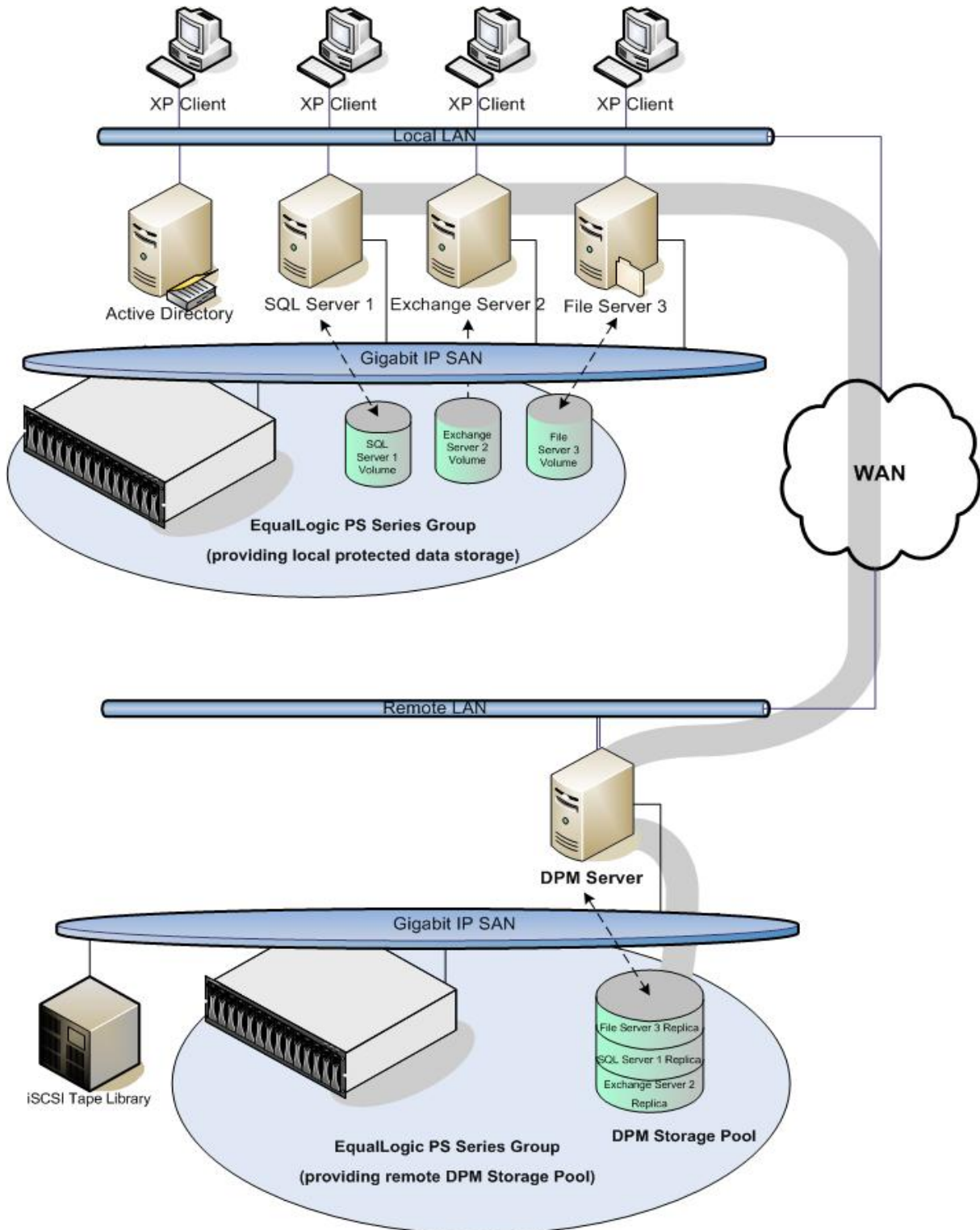
## DPM Server Remote from Protected Servers

It is possible to deploy the DPM server in a different data center than the one in which the servers are being protected. Additional considerations for this deployment include:

- Bandwidth needed for data protection
- Bandwidth needed for recovery operations

In this scenario, the local data center contains the protected servers and the PS Series SAN. The remote data center contains the DPM server and another PS Series SAN. DPM synchronization occurs across the WAN, providing data and disaster protection; however, it does so at a cost of reduced performance across the WAN.

**Figure 4: DPM Server remote from Protected Servers**



DPM can deploy agents and protect data on a WAN, but this creates the potential for performance problems – network latency when replicating data with DPM over a WAN, and bandwidth limitations that may exist on the WAN. If you are protecting data in this way, consider doing the following:

- Enable on-the-wire compression on the WAN link.
- Enable network throttling.

For information on how to perform these tasks, see *How to modify protection options* at:

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

---

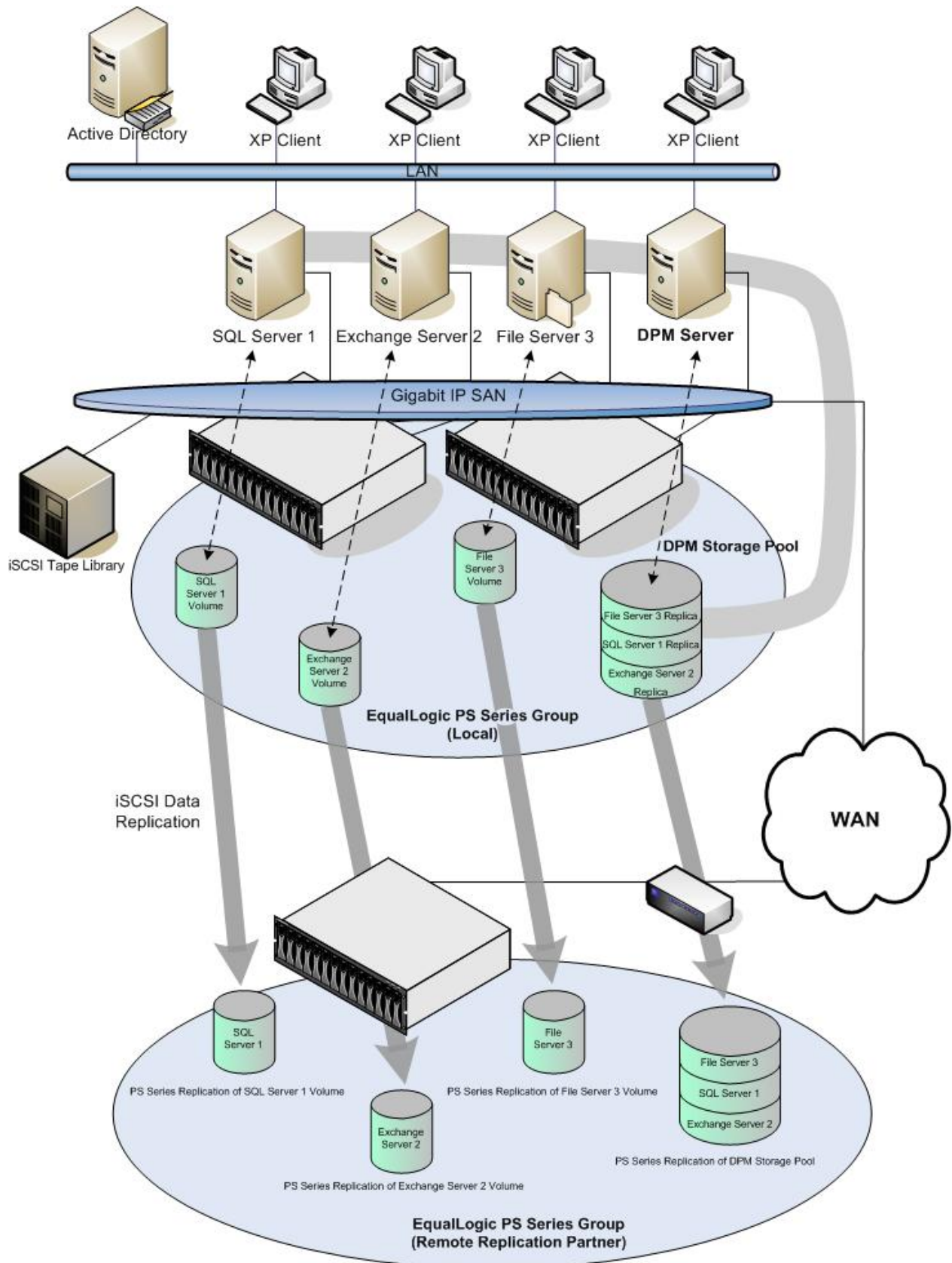
## iSCSI SAN Replication of DPM Volumes

A PS Series SAN provides enhanced data services, including high-end features such as volume snapshots. In addition, PS Series replication functionality enables you to set up a simple, yet robust, disaster recovery configuration. These features can be exploited to dramatically improve the capabilities of DPM.

For example, when using PS Series replication, the local data center contains the DPM server, the protected servers, and a PS Series group. The remote location contains another PS Series group. The DPM synchronization occurs on the local network. For disaster recovery purposes, data can be replicated across the WAN from one group to the other, delivering high-performance for both the protection and recovery of data.

PS Series replication improves disaster recovery capabilities by reducing the time and effort required to reestablish the DPM server and the storage pool. Administrators can recover a DPM server with its protected data in minutes, rather than waiting hours or days. Replication also ensures good DPM performance under normal conditions, because the DPM environment is not affected by WAN performance. The PS Series groups perform replication across the WAN, independent of DPM operations.

**Figure 5: DPM with iSCSI SAN Replication**



## Requirements and Recommendations

---

The following sections describe installation requirements and recommendations that should be met to ensure a successful DPM/PS Series deployment.

### PS Series Group Requirements

---

PS Series group requirements are as follows:

- PS Series Firmware Version 3.2 or higher. See [Group Administration](#) for information about creating a group.
- Volumes for the DPM storage pool: See *DPM Server Requirements and Recommendations* for information about sizing volumes.
  - In addition, for each volume that needs to be connected to the DPM server, set up at least one access control record that will allow the DPM server access.
- Optionally, volumes for the protected servers and access control records are needed to ensure server access to the volumes.
- Optionally, volumes for booting servers from the PS Series SAN and access control records are needed to ensure server access to the volumes. See *SAN Boot Recommendations* for more information.

### SAN Boot Recommendations

---

SAN boot is a capability that allows disk-less server hardware configurations. All storage, including the system disk, is configured in the SAN. EqualLogic recommends that the DPM server and protected servers be configured to boot from a PS Series volume for fast recovery in the event of a server failure and for easy server hardware upgrades without reinstallation.

This provides the following benefits:

- Server hardware can be quickly replaced in the event of a failure, without needing to re-install the server or applications, thus dramatically reducing recovery time.
- This configuration improves redundancy and serviceability of the server system disk. Because a PS Series SAN is deployed fully redundant and hot serviceable, data protection is improved for all the system storage.
- In disaster recovery replication configurations, having the system disks in a PS Series SAN allows all server data to be protected from disasters. In event of a disaster, the server can be quickly recovered at the recovery site, without the need for lengthy system reinstallation.

For more information on SAN boot using PS Series storage, see the QLogic QLA405x iSCSI [Host Bus Adapter: Booting Windows 2003 From a PS Series SAN](#) Technical Report on the EqualLogic Customer Support website.

## **DPM Server Requirements and Recommendations**

DPM installation and configuration documentation can be found on the installation media within the Deployment and Planning help file. Additional product information can be found on Microsoft's website:

<http://www.microsoft.com/windowsserversystem/dpm/default.aspx>

DPM requirements and recommendations are as follows:

- The Microsoft System Center Data Protection Manager 2007 (DPM) server must be a dedicated, single-purpose server, and cannot be either a domain controller or an application server.
- For a complete updated list of the DPM server prerequisite software visit Microsoft's web site: <http://technet.microsoft.com/hi-in/library/bb808832.aspx>

<b><u>Component</u></b>	<b><u>Requirement</u></b>	<b><u>Recommendation</u></b>
<b>Processor</b>	1 GHz or faster	2.33 GHz Quad
<b>Memory</b>	1 gigabyte (GB) RAM	4 gigabyte (GB) RAM
<b><u>Disk 1:</u> Disk space for DPM installation files</b>	Space Requirements: Program files drive: 410 MB Database files drive: 900 MB System drive: 2650 MB  <b>Note</b> The system drive disk space requirement is necessary if you chose to install the instance of SQL Server from the DPM download package. If you are using an existing instance of SQL Server, this disk space requirement is considerably less.	N/A
<b><u>Disk 2:</u> Disk space for storage pool</b>	1.5 times the size of the used space on the protected volume.	The total size of the protected volume.

**Table 2: DPM Server Requirements**

The DPM server must be running Windows Server 2003 (Standard or Enterprise Edition) with Service Pack 1 (SP1) and hotfix 891957 and hotfix 940349 or later installed and must meet the hardware requirements in Table 2.

Additional DPM requirements and recommendations:

- The DPM server must have at least two volumes available for use: one that is the system disk (and will store the DPM installation files) and one or more disks that will be dedicated to the DPM storage pool.
- The DPM server should be persistently connected to the PS Series volume used for the storage pool. This will ensure that the volumes are available each time the server boots. Each PS Series volume appears on the network as an iSCSI target. Follow Microsoft's iSCSI initiator instructions for discovering and connecting to iSCSI targets.
- Always consult the DPM installation and configuration documentation, found on the installation media within the Deployment and Planning help file, and at:

<http://technet.microsoft.com/hi-in/library/bb808832.aspx>

## Requirements for Protected Servers

Each server protected by Microsoft System Center Data Protection Manager (DPM) 2007 must meet the requirements in Table 3. Please also review <http://technet.microsoft.com/hi-in/library/bb808832.aspx> for an updated requirements list.

<u>Protected Servers</u>	<u>Server Requirements</u>
File servers	<ul style="list-style-type: none"> <li>• Windows Server 2003 with Service Pack 1 (SP1)</li> <li>• Windows Server 2003 x64</li> <li>• Windows Server 2003 R2</li> <li>• Windows Server 2003 R2 x64</li> <li>• Windows Storage Server 2003 with Service Pack 1 (SP1)</li> </ul> <p><b>Note</b></p> <p>To obtain SP1 for Windows Storage Server 2003, contact your equipment manufacturer.</p> <ul style="list-style-type: none"> <li>• Windows Storage Server 2003 R2</li> <li>• Windows Storage Server 2003 R2 x64</li> </ul> <p><b>Note</b></p> <p>DPM supports Standard and Enterprise Editions of all the required operating systems.</p>
Computers running SQL Server	<ul style="list-style-type: none"> <li>• Microsoft SQL Server 2000 with Service Pack 4 (SP4)</li> </ul> <p style="text-align: center;">- OR -</p>

	<ul style="list-style-type: none"> <li>• Microsoft SQL Server 2005 with Service Pack 1 (SP1) or Service Pack 2 (SP2)</li> </ul> <p><b>Note</b></p> <p>DPM supports Standard, Enterprise, Workgroup, and Express Editions of SQL Server.</p> <p><b>Important</b></p> <p>You must start the SQL Server VSS Writer Service on the SQL server before you can start protecting SQL Server data. By default, the SQL Server VSS Writer Service is turned off when you install SQL Server 2005.</p> <p style="text-align: center;"><b>To start the SQL Server VSS Writer Service</b></p> <ol style="list-style-type: none"> <li>1. Click Start, point to Administrative Tools, and then click Services.</li> <li>2. On the Services screen, scroll down and right-click SQL Server VSS writer, and then click Start.</li> </ol> <ul style="list-style-type: none"> <li>• Computers running Exchange Server</li> <li>• Exchange Server 2003 with Service Pack 2 (SP2)</li> </ul> <p style="text-align: center;">- OR -</p> <ul style="list-style-type: none"> <li>• Exchange Server 2007</li> </ul> <p><b>Note</b></p> <p>DPM supports Standard and Enterprise Editions of Exchange Server.</p>
Computers running Virtual Server	<ul style="list-style-type: none"> <li>• Microsoft Virtual Server 2005 R2 Service Pack 1 (SP1)</li> </ul>
Windows SharePoint Services	<ul style="list-style-type: none"> <li>• Windows SharePoint Services (WSS) 3.0</li> <li>• Microsoft Office SharePoint Server (MOSS) 2007</li> </ul> <p><b>Important</b></p> <p>Before you can protect SharePoint data you must start the SharePoint Writer service on the SharePoint server. Then provide the protection agent with credentials for the SharePoint Services farm. For more information, see Starting and Configuring the SharePoint Writer Service.</p>
Shared disk clusters	<ul style="list-style-type: none"> <li>• File servers</li> <li>• SQL Server 2000 with Service Pack 4 (SP4)</li> <li>• SQL Server 2005 with Service Pack 1 (SP1)</li> <li>• Exchange Server 2003 with Service Pack 2 (SP2)</li> <li>• Exchange Server 2007 Beta 2</li> </ul> <p><b>Note</b></p>

	<p>Only one Network Name resource can exist for the resource group that you are protecting. If there is more than one Network Name resource for a single resource group, DPM can support this configuration only if all dependant resources are associated with the same Network Name resource. For example, if you attempt to protect a SQL shared disk cluster, the physical disk resource that SQL uses must be associated with the same Network Name resource as the computer running SQL Server and the SQL Server Agent.</p>
Non-shared disk clusters	<ul style="list-style-type: none"> <li>Exchange Server 2007</li> </ul>

**Table 3: Protected Server Requirements**

## Network Requirements

Network requirements to support DPM are as follows:

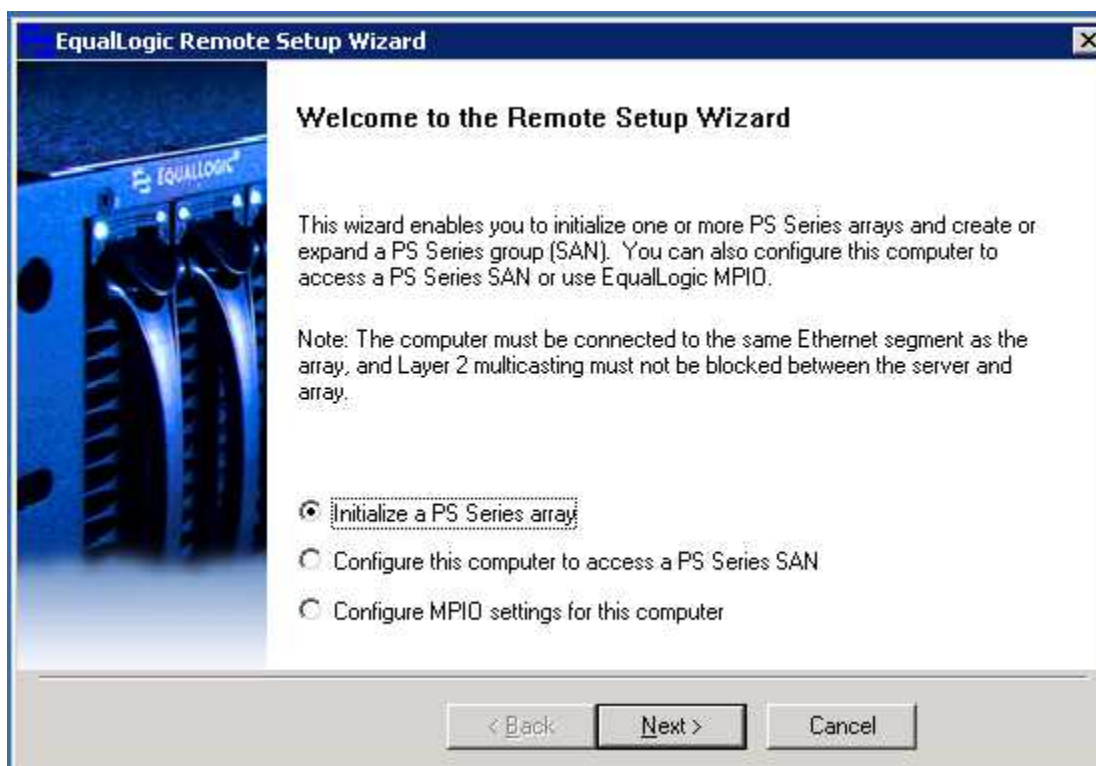
- The DPM server Network Requirements can be found at:  
<http://technet.microsoft.com/hi-in/library/bb808832.aspx>
- In addition, consult the [Network Connection and Performance Guidelines](#) Technical Report on the EqualLogic Customer Support website for information about improving network performance between PS Series storage and servers.

## Deploying DPM with PS Series Storage

The following sections take you through procedures for using PS Series storage for the DPM storage pool. See the EqualLogic PS Series documentation and the DPM documentation for detailed installation and configuration information.

Before you can create a PS Series group, first you must unpack and inspect the PS Series storage array hardware, rack mount the array, and connect the serial cable (only used for the initial setup) and network cables as described in the *QuickStart*.

Once the hardware is connected and the array is powered on, use the EqualLogic Remote Setup Wizard to configure the array and create a group. See the Host Integration Tools for Microsoft Windows *User Guide and Release Notes* for detailed installation and setup information. You will need an IP address for the array, in addition to a group IP address. Also, setup will prompt for the group RAID level, either RAID 10 or RAID 50, an administration password, and a password for adding group members.



**Figure 6: Creating a PS Series Group**

After the group is created, if desired, you can configure additional network interfaces on the new member to increase performance and availability. You can also add more arrays to the group to expand group capacity.

Technical Reports, located on the EqualLogic Customer Support website (<https://www.equallogic.com/support/>), provide detailed information about deploying various applications and configurations with PS Series storage.

Be sure to read [Planning a DPM 2007 Deployment](#) before beginning the deployment. This will help you create a high-availability, high-performance configuration.

## **Using Microsoft DPM to Protect Microsoft Exchange Server**

When used with Microsoft Exchange Server, DPM provides data protection of storage groups and the ability to recover data at the storage group, database, or mailbox level. The DPM protection agent on a computer running Exchange Server takes advantage of the VSS capabilities of Windows Server 2003 to take a snapshot of the entire database at once, ensuring that there is always a consistent view of the data. DPM provides protection for the following versions and editions of Microsoft Exchange Server:

- **Exchange Server 2003** (any edition), with Service Pack 2 or later installed. Shared disk cluster configurations are supported.

- **Exchange Server 2007** (any edition). Local Continuous Replication (LCR), Single Copy Cluster (SCC), and Cluster Continuous Replication (CCR) configurations are supported.

During a planned cluster failover, DPM will automatically continue protection without requiring any administrator action. When a protected cluster node experiences an unplanned failover, DPM will alert the administrator to perform a consistency check of the protected data.

## Installing the DPM Server

---

After you verify that your servers meet the prerequisites for their roles, you can install the DPM software on your intended DPM server. You can install directly from the installation media or copy the setup files to a shared network location. The DPM installer has been optimized to gather all user input at the beginning of the setup process. Once the interactive portion is complete, the installer verifies prerequisites and installs dependent components that may not already be present, such as Internet Information Services. DPM includes Microsoft SQL Server 2005 and Microsoft SQL Server 2005 Reporting Services, allowing it to configure a dedicated SQL Server instance for its internal databases. However, if you already have a suitable SQL Server 2005 installation, you can configure the DPM installer to use your existing deployment.

### Installing the DPM Agent on Exchange Server Computers

After installation, DPM will scan the Microsoft® Active Directory® directory service to find servers that it can protect. Simply choose the servers that you want to protect from the list presented in the Protection Agent Installation Wizard. You will need to deploy the DPM protection agent on the servers to be protected. You can install the DPM protection agent through the DPM Administrator Console, System Center Configuration Manager 2007, Systems Management Server (SMS) 2003, Active Directory group policy, or from the command line on the production server to be protected. See the [Microsoft System Center Data Protection Manager Deployment Guide](#) for instructions on installing protection agents. To install the DPM protection agent on an Exchange Server computer using the DPM Administrator Console, do the following:

1. Open DPM Administrator Console (**Start, All Programs, Microsoft System Center Data Protection Manager**), click **Management** on the navigation bar, and click the **Agents** tab. In the **Actions** pane, click **Install**. The Protection Agent Installation Wizard appears.
2. The first time you use the wizard, DPM assembles a list of potential servers from Active Directory. The daily auto-discovery process creates a stored list of servers that is used for subsequent installations. Select up to 50 servers and click **Add**. You can also specify a server by typing its name in the **Server** name box and clicking **Add**. When you are finished adding servers, click **Next**.
3. Type the user name and password for the domain account to use during the agent installation. This account must be a member of the local administrators group on all selected servers. Click **Next**.
4. Select how you want the selected server to restart when the protection agent is installed and click **Next**.
5. If any of the selected servers are members of a Microsoft Cluster Server (MSCS), you will see an additional screen on which you must select how to restart the clustered servers. DPM will not automatically start servers in an MSCS cluster. Click **Next**.

**Note:** Exchange servers are members of an MSCS cluster if they are Exchange 2003 mailbox servers in a clustered configuration, Exchange 2007 mailbox servers in a SCC configuration, or Exchange 2007 mailbox servers in a CCR configuration.

6. Review the summary and click **Install Agents** to proceed with the installation.
7. The results of the process appear on the **Task** tab of the wizard. You can monitor the installation progress in the **Management** task area on the **Agents** tab in DPM Administrator Console. If the installation is unsuccessful, you can view the alerts in the **Monitoring** task area on the **Alerts** tab.
8. After the installation is complete click **Close**.

## **SAN Initialization of the First DPM Replica**

---

When a PS Series SAN is used to provide storage resources for the DPM storage pool as well as the protected servers, the DPM server can use clone as pre-seeded initial replica. This SAN feature can dramatically reduce the time required for the initial DPM replication operation, in addition to reducing overhead on the protected server and the network during the initial DPM replication.

First create a SAN Clone of the protected server's PS Series volumes. Then, mount the SAN Clone on the DPM server to provide the DPM server with direct access to the data. Requirements include:

- The protected server volumes must be on a PS Series SAN.
- The DPM server must have access to the PS Series SAN containing the protected server's volumes.
- The protected server volumes must be basic partitions.

Follow these steps to initialize the DPM replica using EqualLogic's Volume Clone:

Use the PS Series Group Manager GUI to create a Clone of each protected server volume that will be included in the Protection Group.

**Note:** To allow access by the DPM server, create an access control record for the volume. For example, in the GUI, select the Clone, click the **Access** tab and then click **Add**. Specify the information that gives the DPM server access *only* to the Clone(s).

On the DPM server, use the iSCSI initiator control panel tool to connect to the iSCSI target associated with the Clone. Check the initiator documentation for details. You will need to specify the group IP address as the target portal or discovery address and also the volume's iSCSI target name. Use the Windows Disk Management utility to verify the presence of the clone and to assign a drive letter (in DPM drive letter assignment is not mandatory).

### **Steps to perform initial Replication using SAN Cloned volume.**

1. Prior to following the procedure below, it is assumed that the production volume on which the Exchange database lies is cloned, fractured, and zoned to the DPM Server
2. Ensure that the DPM protection agent is installed on the Exchange server.
3. From the Disk Management snap-in on the DPM server, assign a Drive Letter for the cloned volume, and name it "RepExch07," for example.

4. Create another volume 1.5 times the size of the Exchange database clone (actual size depends on exchange log growth and retention period (consult [Microsoft System Center Data Protection Manager 2007 Planning Guide](#)) for more information about sizing) and zone it to the DPM server.
5. Create partition and format with NTFS. Name it “ExchRecovery” and assign it a Drive Letter. This will be used as the recovery volume.

## Protecting Exchange Server 2007

### Creating the Protection Group

The following steps demonstrate how to start the Create New Protection Group Wizard and begin the process of defining a protection group:

1. Open DPM Administrator Console (**Start, All Programs, Microsoft System Center Data Protection Manager**) and click **Protection** on the navigation bar. In the **Actions** pane, click **Create**.
2. The Create New Protection Group Wizard appears. Click **Next** to continue past the “Welcome page”.

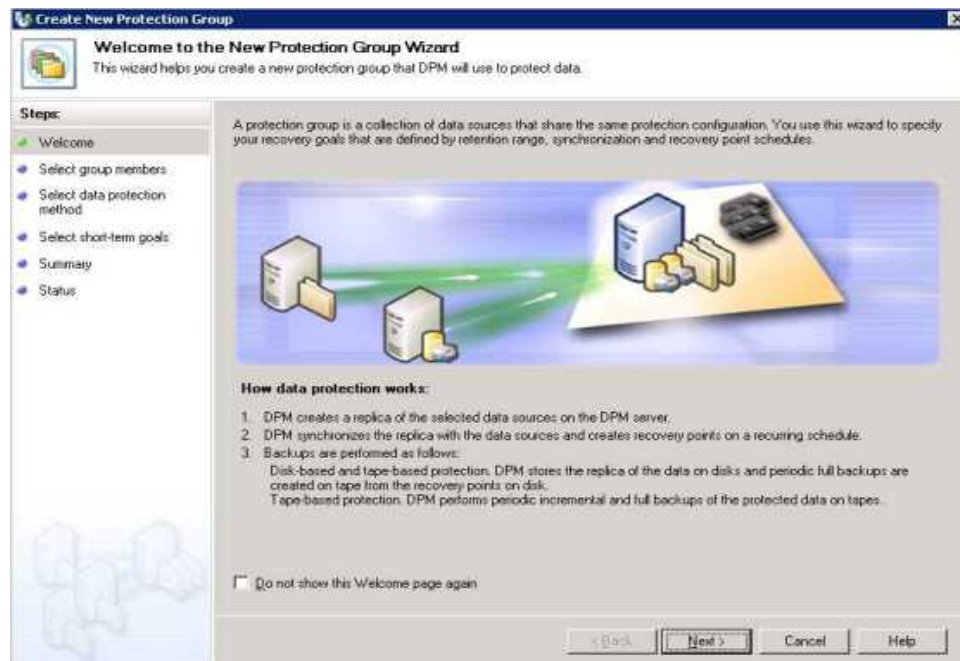
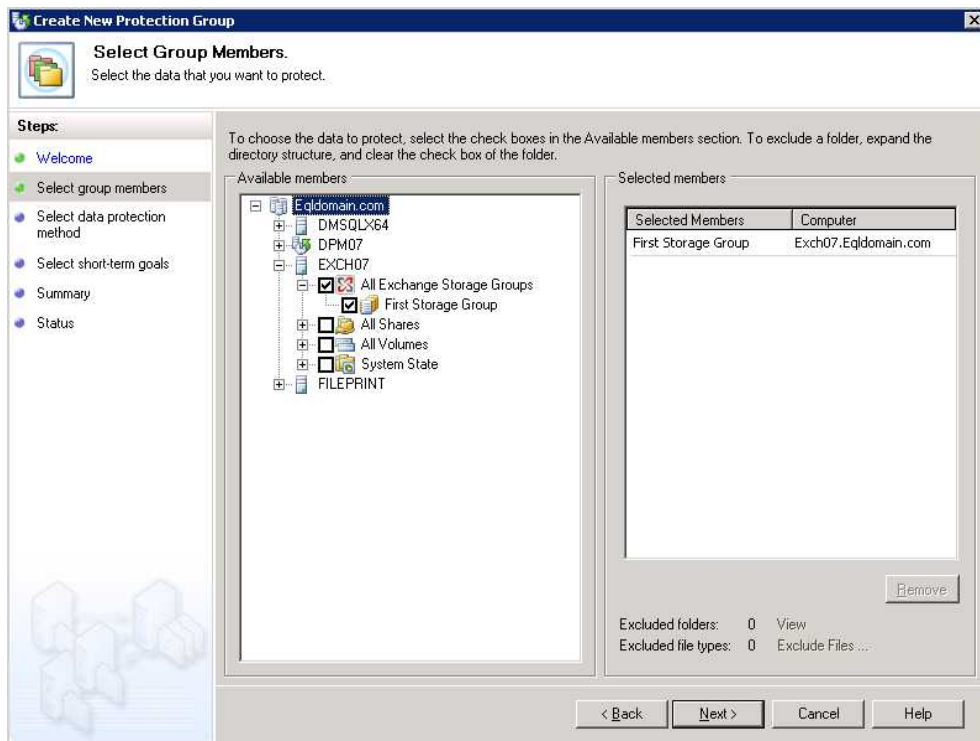


Figure 7: Welcome page

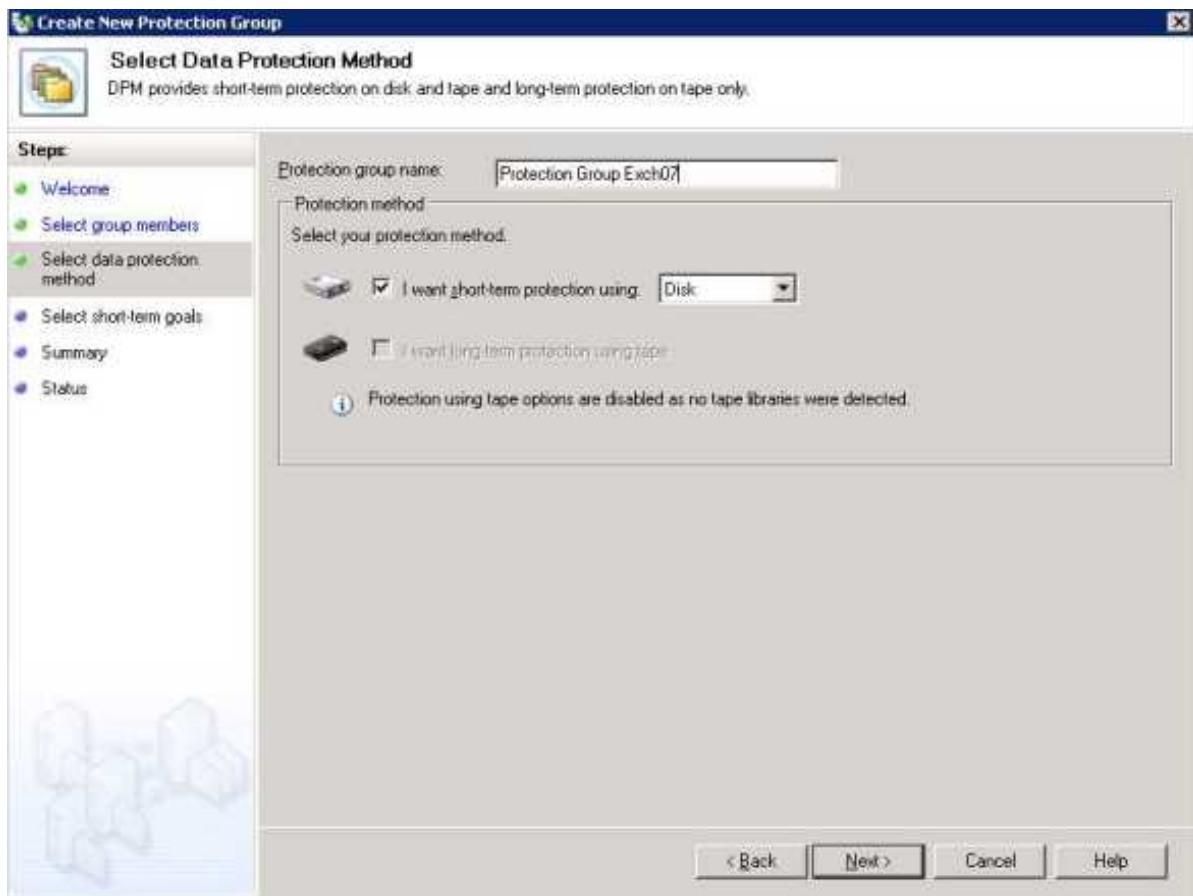
3. Expand the Exchange Server nodes to see each protected Exchange server and their storage groups. Select each storage group you want to include. Confirm that your selections appear in the **Selected Members** box, as shown in Figure 8 and click **Next**.



**Figure 8: Creating the Protection Group**

### Select protection method

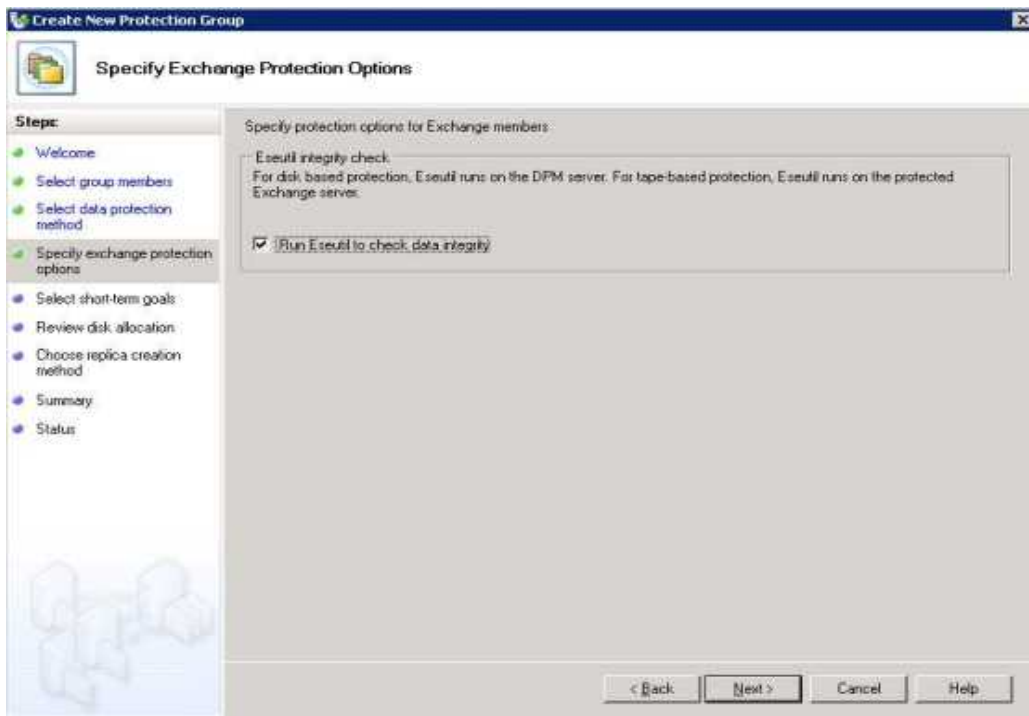
Confirm that “I want short-term protection using disk” is selected in the “Protection method” box as shown in Figure 9 and click **Next**.



**Figure 9: Protection method**

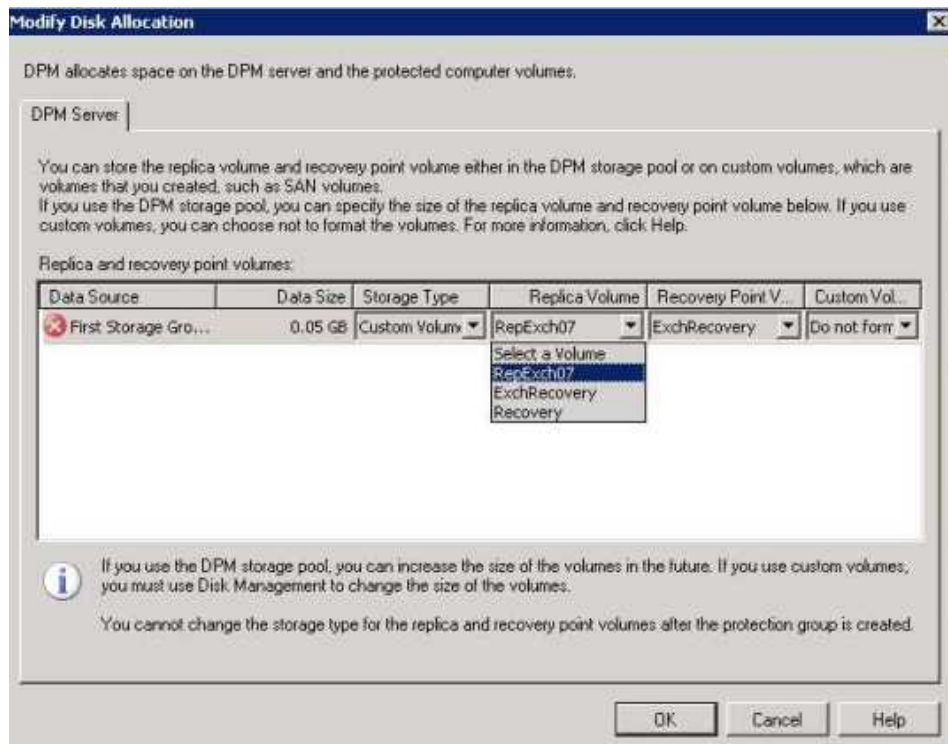
**Specify Exchange Protection option.**

Confirm that “Run Eseutil to check data integrity” is selected in the “Specify Exchange Protection option” box as shown in Figure 10 and click **Next**.



**Figure 10: Specify Exchange Protection option**

The next screen sets short-term retention range (5 day default) Synchronization and Recovery points both (Every 15 minutes default) click **Next** for Modify Disk allocation screen.



## Figure 11: Modify Disk Allocation

The next screen shows a summary. Click **Next** to **Create Group**.

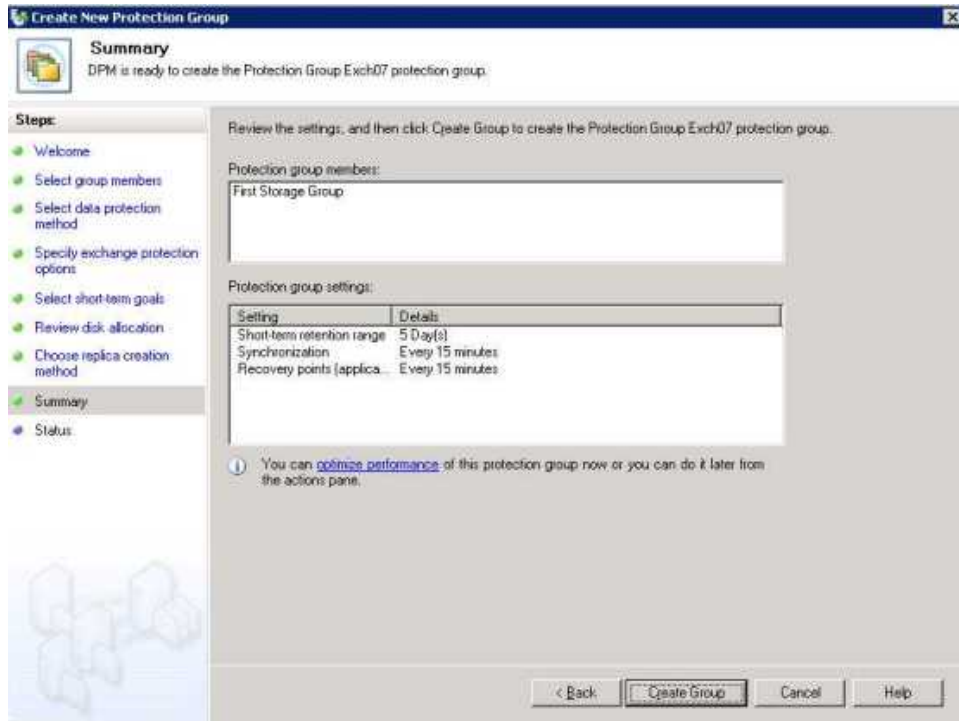


Figure 12: Create Group

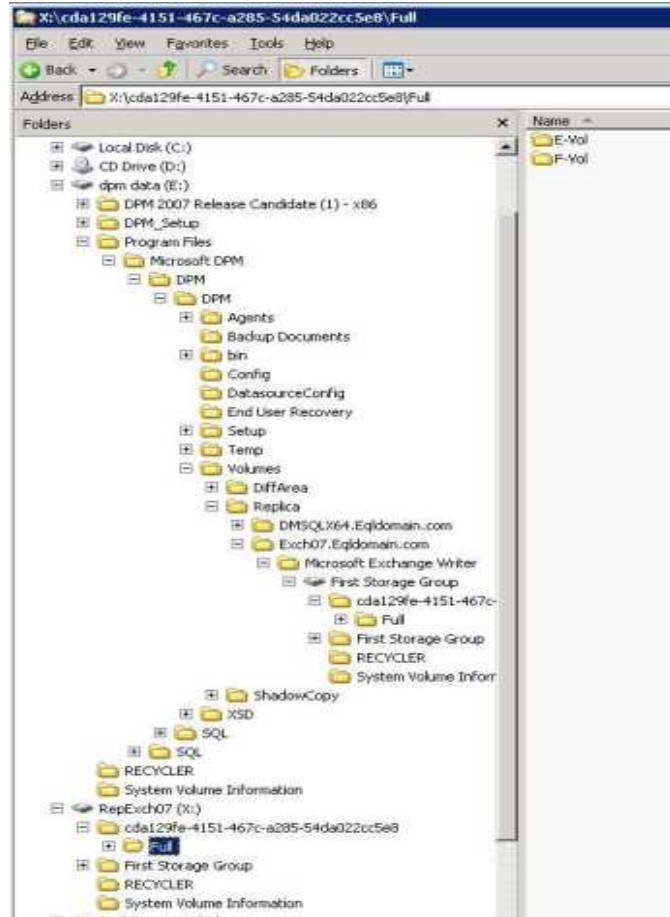
Complete the Protection Group creation process and note the replica folder path. See Figure 13 for an example.

## Figure 13: Replica Path Destination



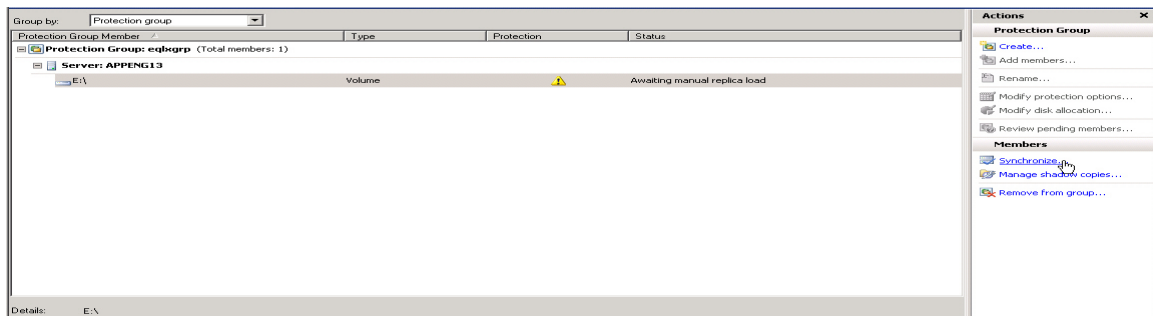
1. The administrator still must manually move the protected data to the folder structure created by the DPM Data Protection Wizard. In this example as shown below, we move X:\cda129fe-4151-

467c-a285-54da022cc5e8\Full to E:\Program Files\Microsoft DPM\DPM\DPM\Volumes\Replica\Exch07.Eqldomain.com\Microsoft Exchange Writer\First Storage Group\cda129fe-4151-467c-a285-54da022cc5e8\Full



When the file move completes, use the DPM Administrator Console to select the replica in the Protection view and initiate Synchronization with Consistency Check. See Figure 14 for an example.

**Figure 14: Synchronization of Replica after File copy**



## Recovering Exchange Data

---

The process of recovering protected Exchange Server data involves several steps and choices. You must first determine which level of recovery you will perform for an entire storage group, a single mailbox database, and a single mailbox.

In the event of recovery of a storage group or mailbox database, you must also determine where you wish to recover the data. In this example we will restore to its original location.

### Recovering a Mailbox Database to its Original Location

1. Open DPM Administrator Console (**Start, All Programs, Microsoft System Center Data Protection Manager**) and click **Recovery** on the navigation bar. Browse to the mailbox database you wish to recover in the “Protected Data” box.
2. Click any bold date in the calendar to see available recovery points. Select the **Latest** recovery point from the Time menu. Click **Recover** in the Actions pane to launch the Recovery Wizard.
3. Review the recovery selection and click **Next**. Select **Recovery to original Exchange Server location** and click **Next**.
4. If there are currently files in the recovery location that have the same names as the files to be recovered, you will be warned that they will be overwritten. Click **Yes** if you agree to have your files overwritten or **No** to cancel the operation.
5. If you want DPM to send an e-mail message when the recovery process is finished, select the **Send a notification when this recovery completes** check box and enter one or more e-mail addresses.

**Note:** When restoring large amounts of Exchange data consider using the SAN unique restore as outlined in: [Steps to Follow for SAN Recovery](#).

## Using the SAN unique features of DPM to protect SQL 2005.

Use the following steps to perform an initial replication using a SAN Cloned volume.

### Steps to perform initial Replication using SAN Cloned volume.

1. Prior to following the procedure below, it is assumed that the production LUN on which the SQL database lies is cloned, fractured, and zoned to the DPM Server
2. Ensure that the DPM protection agent is installed on the SQL server.
3. From the Disk Management snap-in on the DPM server, assign Drive Letter for the cloned LUN, and name it "SqlReplica."
4. Create another LUN 1.5 times the size of the Database clone (actual size differs according to the size of protected data and the number of recovery point setting) and zone it to the DPM server.
5. Create partition and format with NTFS. Name it "SqlRecovery" and assign a Drive Letter. This will be used as the recovery volume.
6. Click on the **Create Protection Group** Hyperlink
7. In the "Select Group Members" page, chose the data source that you want to protect. See Figure 15.

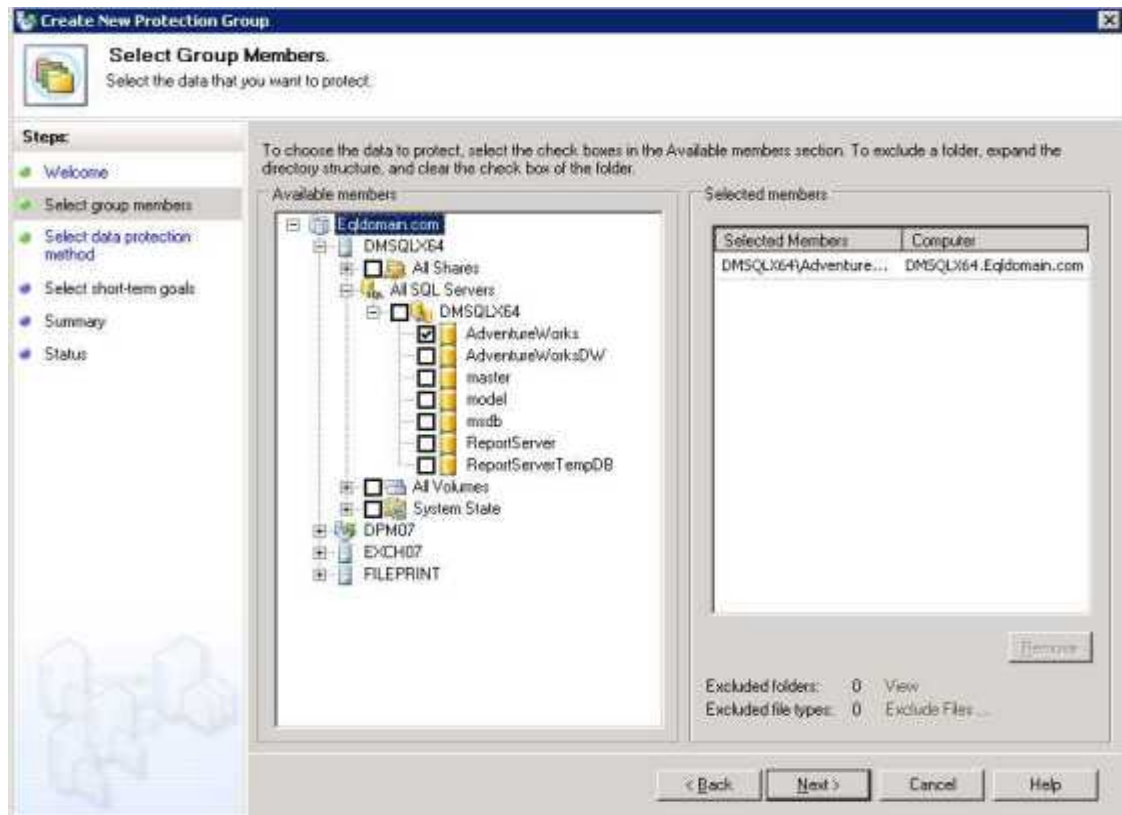


Figure 15

8. In the "Select Data Protection Method" page of the wizard, select short term protection as disk and give a friendly Protection name. See Figure 16.

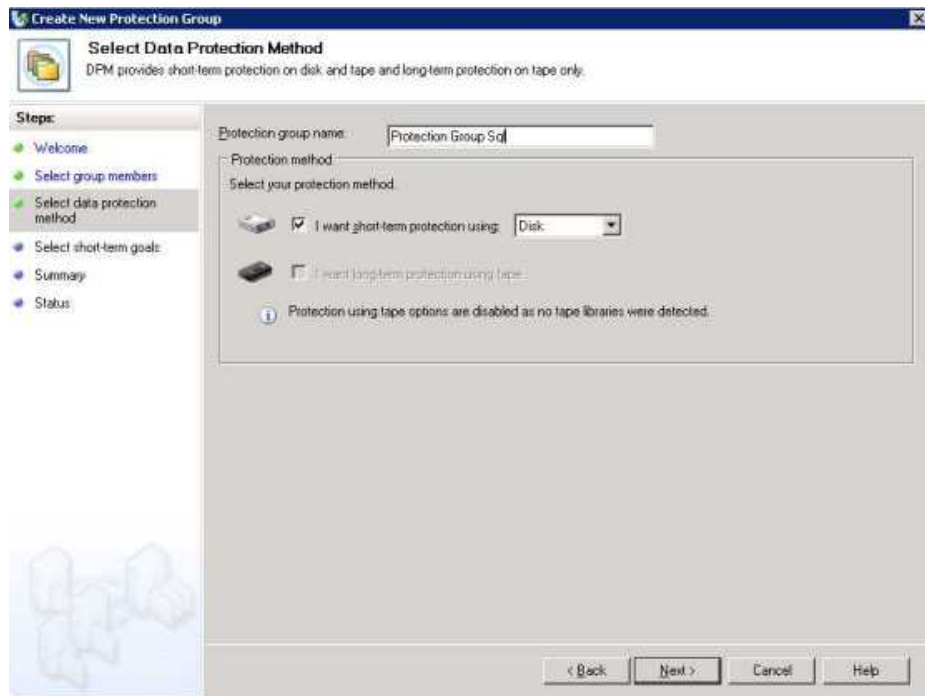


Figure 16

9. Specify your short term protection goals in the next page, as in Figure 17.

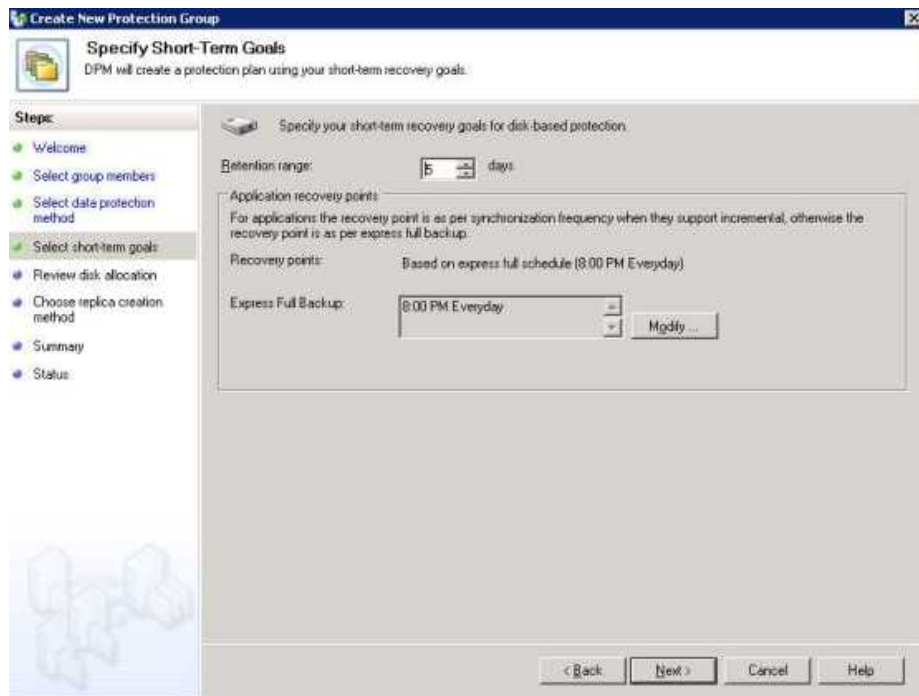


Figure 17

10. On the Review Disk Allocation page, click **Modify** and select **custom volume** and then chose the "Replica Volume" and the "Recovery point" volumes. Also make sure to select the **Do not Format** option from the drop down menu as shown in Figure 18

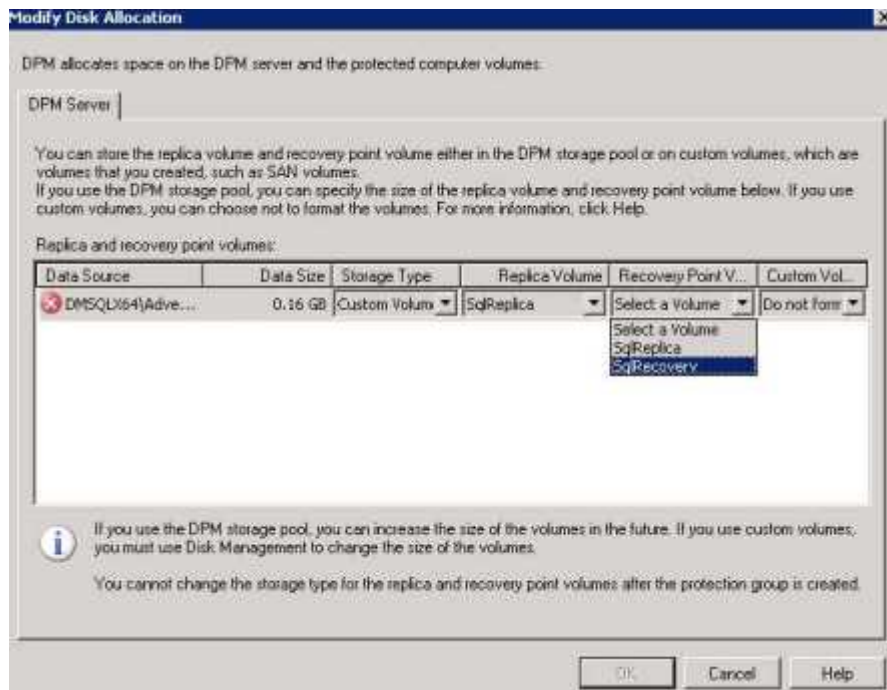


Figure 18

11. Select **Manually** in the "Replica Creation Method" page as shown in Figure 19.

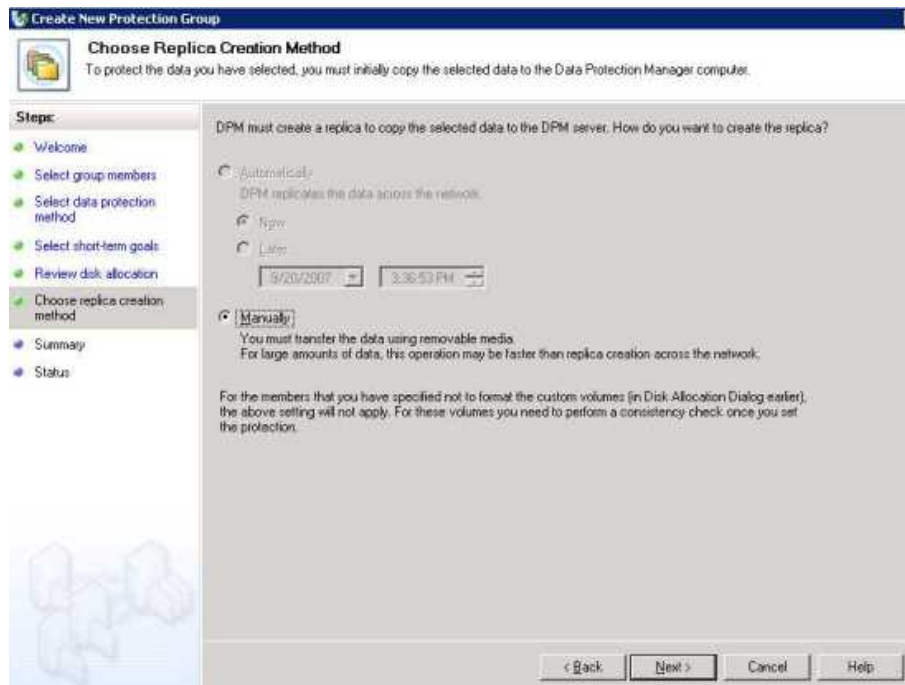


Figure 19

12. Close the wizard.
13. The administrator still must manually move the protected data (SQL files) to the folder structure created by the DPM Data Protection Wizard. This SQL example is shown in Figure 20.

#### 14. SQL:

In this instance you would move z:full to e:full.

Z:\94243ba2-abe3-45af-a715-62e2e99afa0b\Full

To

E:\ProgramFiles\MicrosoftDPM\DPM\DPM\Volumes\Replica\DMSQLX64.Eqldomain.com\SqlServerWriter\AdventureWorks\94243ba2-abe3-45af-a715-62e2e99afa0b\Full

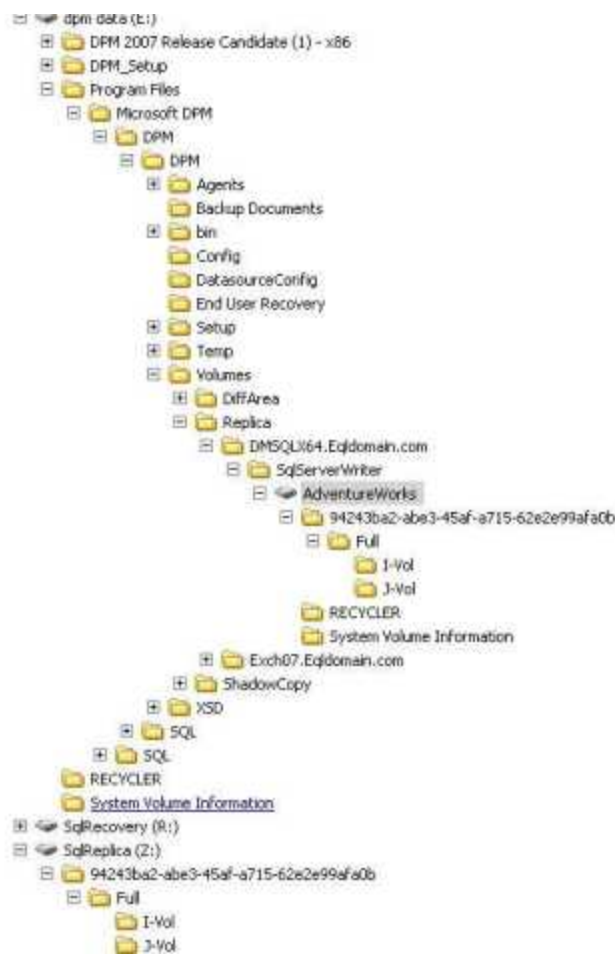


Figure 20

15. Go to the Protection Tab.

16. Select the Protection Group that you just created and run a consistency check. This will take a lot less time and network traffic to synchronize since the manual load that we've presented to this Protection Group is a recent clone of the Production data with very small differences if any at all.

## Steps to follow for SAN recovery:

1. First cancel any running job on data source that you are recovering.
2. Run the included Power Shell script on the DPM Server that will prompt for the datasource and the protection group name that is being recovered and create the shadow copy with “without synchronize” option, as in Figure 21.

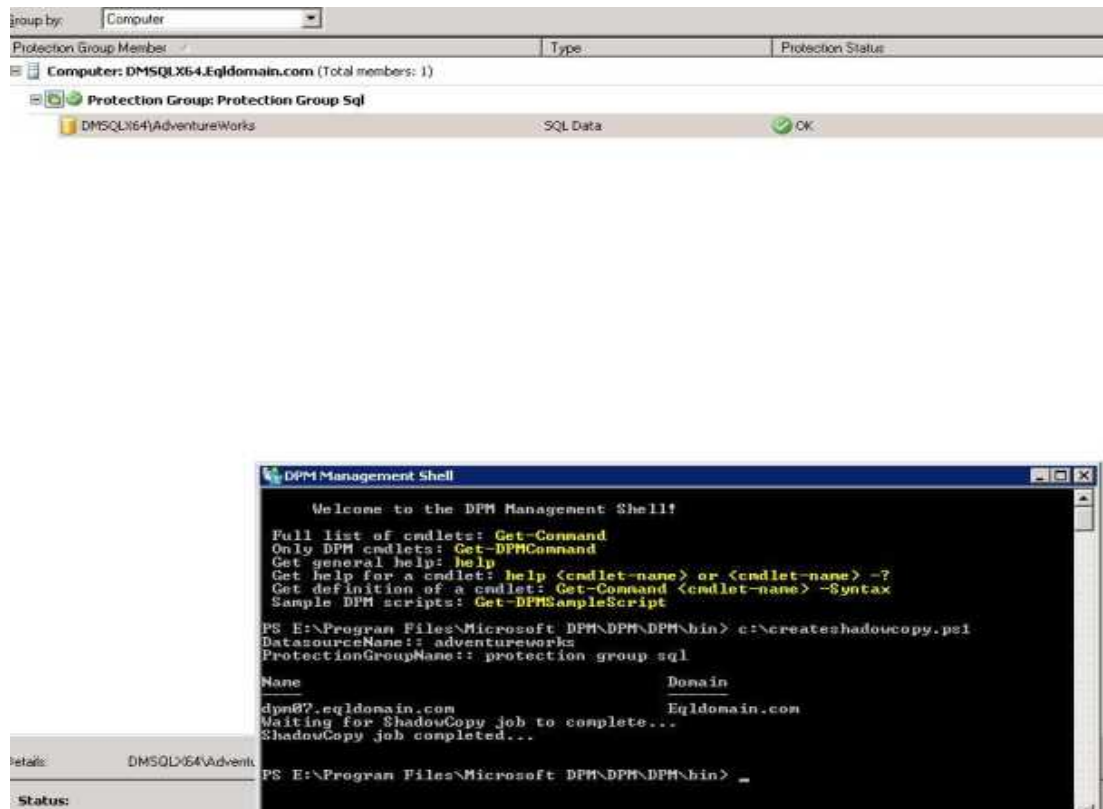


Figure 21

3. Create the hardware snapshot of the DPM Replica and the Recovery volumes of the data source that is being recovered, using EqualLogic’s snapshot creation tool. Do not use Vshadow.exe for this step.
4. Mount the hardware snapshot volumes on the protected server (SQL).
5. Select Recovery Point in Time. In the DPM Recovery wizard, remember to check the checkbox ([X] Use SAN-based hardware snapshots for quicker recovery) as shown in Figure 22.

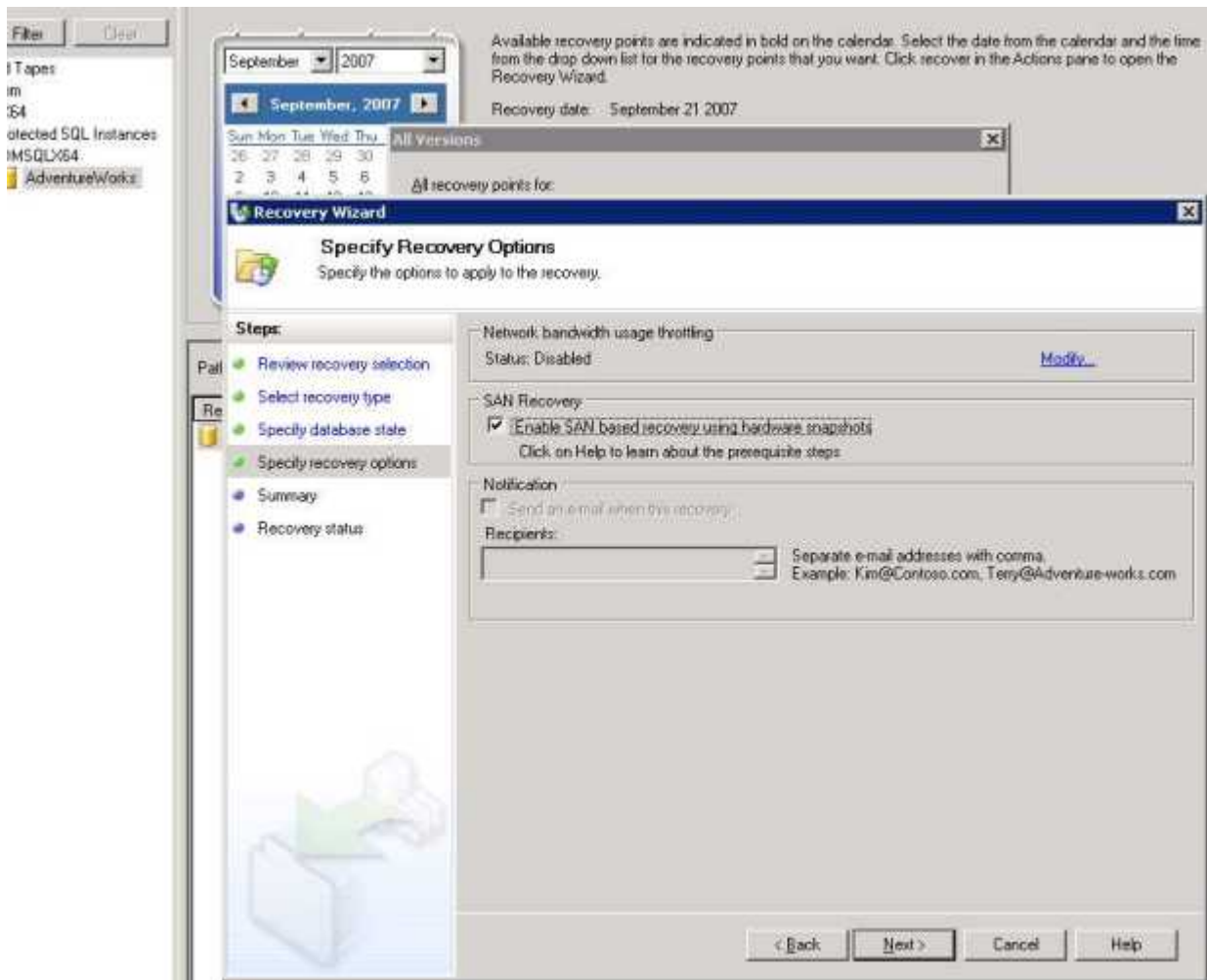


Figure 22

## Power Shell Script:

---

Save the following as: CreateShadowCopy.ps1

```
param([string] $DSName, [string] $PGName)

if(!$args[0])
{
    if(!$DSName)
    {
        $DSName = read-host "DatasourceName:"
    }
}
else
{
    if(("-"?"", "-help") -contains $args[0])
    {
        write-host Usage::
        write-host CreateShadowCopy.ps1 DatasourceName ProtectionGroupName
        write-host Help::
        write-host Creates a shadow copy for the given Datasource
        write-host
        exit 0
    }
    else
    {
        write-host "Usage -? for Help"
        exit 1
    }
}

if(!$PGName)
{
    $PGName = read-host "ProtectionGroupName:"
}

$dpmname = &"hostname"
connect-dpmserver $dpmname

$pg = get-protectiongroup -dpmservername $dpmname
if (!$pg)
{
    write-error "Cannot get the protectionGroup"
    disconnect-dpmserver $dpmname
    exit 1
}

$mypg = $pg | where {$_.FriendlyName -eq $PGName}
```

```

if (!$mypg)
{
    write-error "Cannot get the requested protectionGroup"
    disconnect-dpmserver $dpmname
    exit 1
}

$ds = get-datasource -protectiongroup $mypg
if (!$ds)
{
    write-error "Cannot get the datasources for the PG"
    disconnect-dpmserver $dpmname
    exit 1
}

$myds = $ds | where {$_.Name -eq $DSName}
if (!$myds)
{
    write-error "Cannot get the required Datasource"
    disconnect-dpmserver $dpmname
    exit 1
}

$j = new-recoverypoint -datasource $myds -DiskRecoveryPointOption WithoutSynchronize -Disk

if (!$j)
{
    write-error "Cannot get the required Datasource"
    disconnect-dpmserver $dpmname
    exit 1
}

$jobtype = $j.jobtype

while (! $j.hascompleted )
{
    write-host "Waiting for $jobtype job to complete..."; start-sleep 5
}

if($j.Status -ne "Succeeded")
{
    write-error "Job $jobtype failed..."
}

Write-host "$jobtype job completed..."
disconnect-dpmserver $dpmname
exit

```

## Summary

---

Microsoft System Center Data Protection Manager 2007 and EqualLogic PS Series storage arrays combine to deliver a high-performance, highly available, easily scalable storage solution that dramatically improves data availability by enabling you to quickly recover data when necessary. The data replication features of DPM allow you to store online copies of protected server data on disk-based PS Series storage, thus minimizing the need to recover from tape.

PS Series storage arrays enable you to create an iSCSI SAN that is easy to set up and manage and provides flexible scaling for both protected server and DPM storage pool resources. SAN boot capabilities also facilitate the fast recovery of file servers and the DPM server in the event of server hardware failure or corruption.

In addition, PS Series storage arrays can improve disaster protection by combining PS Series group replication functionality with DPM data protection features.

## Documentation and Customer Support

---

For more information on Data Protection Manager please visit:

<http://www.microsoft.com/windowsserversystem/dpm/default.aspx>

Visit the EqualLogic Customer Support website, where you can download the latest documentation and firmware. You can also view FAQs, the Knowledge Base, and Technical Reports and submit a service request.

EqualLogic PS Series storage array documentation includes the following:

- *Release Notes*. Provides the latest information about PS Series storage arrays.
- *QuickStart*. Describes how to set up the hardware and start using a PS Series storage array.
- *Group Administration*. Describes how to use the Group Manager GUI to manage a PS Series group. This manual provides comprehensive information about product concepts and procedures.
- *CLI Reference*. Describes how to use the Group Manager command line interface to manage a group and individual arrays.
- *Hardware Maintenance*. Provides information on maintaining the PS Series storage array hardware.

To access the Customer Support website, from the EqualLogic website ([www.equallogic.com](http://www.equallogic.com)), click Support and log in to a support account. If you do not have an account, create one by clicking the link under the login prompt.

To contact customer support, send e-mail to mailto: [supportnp@equallogic.com](mailto:supportnp@equallogic.com). If the issue is urgent, call 1-877-887-7337 to speak with a member of the customer support team.

## Related Links

---

Microsoft System Center Data Protection Manager (DPM) website

<http://www.microsoft.com/DPM>

“How to Protect Exchange Server with DPM” on-demand webcast from Microsoft TechNet

<http://msevents.microsoft.com/CUI/WebCastEventDetails.aspx?EventID=1032322917>

Protecting Exchange Server with DPM 2007 White Paper

<http://go.microsoft.com/fwlink/?LinkId=92497>

Protecting SQL Server with DPM 2007 White Paper

<http://go.microsoft.com/fwlink/?LinkId=92498>