NETAPP TECHNICAL REPORT

# Microsoft System Center Data Protection Manager 2007 with NetApp Fabric-Attached Storage

November 2008 | TR-3726

## EXECUTIVE SUMMARY

This report explains the new features of Microsoft System Center Data Protection Manager 2007 (DPM 2007) and shows an example of an implementation of DPM 2007 with NetApp® fabric-attached storage systems.

# TABLE OF CONTENTS

# 1 OVERVIEW OF MICROSOFT DATA PROTECTION MANAGER 2007

Data Protection Manager 2007 (DPM 2007) is a key member of the Microsoft System Center family of management products, designed to help IT professionals protect their Microsoft® Windows® environment. DPM 2007 is the new standard for Windows backup and recovery, delivering continuous data protection for Microsoft application and file servers by using seamlessly integrated disk and tape media. DPM enables rapid and reliable recovery through advanced technology for enterprises of all sizes.

Today's business climate is more challenging than ever, and businesses are under constant pressure to lower costs while improving overall operational efficiency. In short, businesses are being asked to "do more for less." One way that enterprises of all sizes can reduce costs and improve business agility is by changing the way data protection is managed. DPM provides the following additional benefits:

- Continuous data protection
- Lossless restores for applications
- Superior application integration for Microsoft Exchange Server, SQL Server®, and SharePoint®
- Rapid recovery
- Reliable recovery
- Seamless disk and tape integration
- Unified protection policies across data types
- SLA-driven backup process
- Block filter

For more information on Microsoft System Center Data Protection Manager 2007, see http://www.microsoft.com/systemcenter/dataprotectionmanager/en/us/overview.aspx.

# 2 OVERVIEW OF NETAPP FAS STORAGE AND SOFTWARE

## 2.1 NETAPP FABRIC-ATTACHED STORAGE

NetApp® fabric-attached storage (FAS) systems simplify data management, and enable enterprise customers to reduce costs, complexity, minimize risks, and control change. The FAS product line provides storage solutions for a broad range of needs—from remote office applications to the largest corporate data center applications. The FAS product line features the high-end FAS6000 series for large-scale data consolidation and high-performance applications; the midrange FAS3000 series that provides exceptional price-performance value; and the FAS2000 series for remote offices of large enterprises as well as primary storage for small and medium-size enterprises.

## 2.2 NETAPP SOFTWARE

All NetApp FAS systems run the Data ONTAP® operating system, which simplifies data management and optimizes storage utilization with features that enable flexible storage provisioning, superior scalability, and concurrent block and file access. Data ONTAP integrates seamlessly with the UNIX®, Windows, and Web environments to provide the foundation for enterprise-wide storage and data infrastructures supporting mission-critical business applications.

Table 1 provides an overview of NetApp software.

**Table 1) NetApp software overview.**

| Software Feature | Function | Benefit |
|---|---|---|
| Data ONTAP | NetApp storage operating system providing full-featured and unified data management for both block and file-serving environments | Single architecture and user interface to simplify data management and reduce costs for SAN and NAS deployments |

| Software Feature | Function | Benefit |
|---|---|---|
| Deduplication for FAS | Identifies and eliminates redundant data with minimal performance impact | Reduces the capacity required to store redundant data on primary storage |
| FlexClone® | Instantaneously creates LUN and volume clones without requiring additional storage | Accelerated test and development and storage capacity savings |
| FlexCache™ | Caches NFS volumes for accelerated file access in remote offices and for server compute farms | Improves performance, response times, and data availability |
| FlexShare™ | Prioritizes storage resource allocation to highest-value workloads on a heavily loaded system | Provides best performance to designated high-priority applications |
| FlexVol® | Creates flexibly sized LUNs and volumes across a large pool of disks and one or more RAID groups | Fast, simple, and flexible storage provisioning and high-capacity utilization |
| Snapshot™ | Makes incremental, data-in-place, point-in-time copies of a LUN or volume with minimal performance impact | Enables frequent, nondisruptive, space-efficient, and quickly restorable backups |
| SnapMover® | Enables rapid reassignment of disks between controllers within a system without disruption | Enables fast, nondisruptive load balancing within an active-active controller system |
| SnapRestore® | Rapidly restores single files, directories, or entire LUNs and volumes from any Snapshot backup | Enables near-instantaneous recovery of files, databases, and complete volumes |
| Operations Manager (formerly DataFabric® Manager) | Manages multiple NetApp systems from a single administrative console | Faster deployment and consolidated management of multiple NetApp systems |
| Protection Manager | Backup and replication management software for NetApp disk-to-disk environment | Improves productivity through automation of data protection tasks; delivers higher assurance of data protection than with manual execution of tasks by reducing human errors |
| MultiStore® | Securely partitions a storage system into multiple virtual storage appliances | Enables secure consolidation of multiple domains and file servers |
| RAID-DP® | Integrated with the NetApp Data ONTAP system to provide double-parity RAID protection against data loss with negligible performance overhead | Protects data from double disk failures while providing the performance that even the most demanding applications require |
| SnapDrive® | Provides host-based data management of NetApp storage from Windows, UNIX, and Linux® servers | Simplifies host-consistent Snapshot copy creation and automates error-free restores |
| SnapManager® | Provides host-based data management of NetApp storage for databases and business applications | Simplifies application-consistent Snapshot copies, automates error-free data restores, and enables application-aware disaster recovery |
| SnapMirror® | Enables automatic, incremental data replication between systems: synchronous or asynchronous | Provides flexible, space and network-efficient, site-to-site mirroring for disaster recovery and data distribution |

| Software Feature | Function | Benefit |
|---|---|---|
| SyncMirror® | Maintains two online copies of data with RAID-DP® protection on each side of the mirror | Provides automated, nondisruptive capacity expansion, data replication, and data management across heterogeneous file-server environments |
| Thin Provisioning | Thin provisioning is a mechanism that is being adopted by many enterprise storage administrators to efficiently manage storage provisioning and storage utilization by maintaining a common, unallocated storage space that is readily available to other applications on an as-needed basis | Provides effective utilization of storage on an as-needed basis |

## 2.3 BENEFITS OF USING NETAPP FAS WITH DPM 2007

NetApp FAS systems provides a disk-based target for DPM backups and supports high-performance database applications. NetApp FlexClone and Snapshot technologies can be easily integrated with DPM 2007 and business critical applications such as Microsoft Exchange and SQL Server.
By using NetApp FAS systems to contain the storage pool for DPM, you can leverage many of the features of Data ONTAP. The key features that pertain to DPM are:

- FlexClone for fast initial replica creation and shorter RTOs by enabling SAN-based recovery in DPM
- RAID-DP for superior data protection against double disk failure
- NetApp Multipath HA for high availability
- FlexVol for easy scaling of storage pools
- Thin provisioning for increased storage utilization
- Deduplication for space savings
- SnapMirror for Disaster Recovery

**FlexClone**
NetApp FlexClone enables true cloning—instant replication of data volumes and data sets without requiring additional storage space at the time of creation. Depending on the amount of existing data to protect, using FlexClone volumes to create the initial Replica of the DPM-protected data can drastically reduce the initial sync time by replicating the data at the storage level in the Fabric instead of transferring it over the network.

FlexClone enables SAN-based recovery in DPM. As with the initial sync, when used with SAN-based recovery, FlexClone can drastically reduce the recovery time by having the recovered data replicated at the storage level in the Fabric instead of transferring it over the network. The faster the recovery time, the shorter the down time, and the quicker systems are back in production.

In addition, the NetApp Snapshot copies leveraged by FlexClone provide a second level of protection of the DPM protected data in case it is accidentally deleted or lost.

**RAID-DP**
NetApp RAID-DP, a RAID 6 implementation, provides double-parity RAID protection against data loss with negligible performance overhead and zero cost penalty compared to single-parity RAID. RAID-DP is a standard feature of Data ONTAP and prevents data loss in the event of a second drive failure without excessive redundancy costs. RAID-DP offers significantly more protection than single parity schemes (including RAID 5 and NetApp's RAID 4) with zero to minimal cost and performance impact. Compared to RAID 1 (mirroring), RAID-DP offers superior data protection against double disk failure at a fraction of the cost. See http://technet.microsoft.com/en-us/library/bb738146(EXCHG.80).aspx

**NetApp Multipath HA**
A NetApp FAS Active-Active Controller configuration provides redundancy at every level of the storage configuration to continuously serve data at higher than 99.99% availability and provide a highly available backend storage environment for DPM 2007

**FlexVol**
NetApp FlexVol technology delivers true storage virtualization solutions that can lower overhead and capital expenses, reduce disruption and risk, and provide the flexibility to adapt quickly and easily to the dynamic needs of the enterprise. FlexVol technology pools storage resources automatically and enables creation of multiple flexible volumes on a large pool of disks. This flexibility allows you to focus on managing data, not hardware, and make changes quickly and seamlessly. The result is that you can add storage when and where it's needed without disruption and at the lowest incremental cost.

**Thin Provisioning**
Thin provisioning separates the logical representation of storage from the underlying physical disk arrays, making it possible to allocate more storage capacity to applications than is physically installed. With the ability to do thin provisioning, NetApp storage systems make it possible to oversubscribe free space and adapt rapidly to the changing needs of the enterprise. This is essentially an allocate-on-demand model that allows allocation of storage to be configured based on anticipated application needs, without actually installing all of the provisioned capacity up front. Because you can present more storage space to the hosts or servers connecting to the storage system than is actually available, storage purchases can be deferred until real application capacity thresholds are realized. The resulting increase in storage utilization means less unused storage capacity wasting space, power, and cooling in the data center.

**Deduplication**
NetApp Deduplication for FAS provides block-level deduplication within the entire flexible volume on primary storage. Deduplication stores only unique blocks in the flexible volume and creates a small amount of additional metadata in the process. It is application-transparent and can therefore be used for deduplication of DPM data (backups). We have observed greater than 30% space savings, however actual space savings will vary depending on the dataset that is being deduplicated.

**SnapMirror**
Replicating DPM 2007 protected data to a remote site for disaster recovery can be achieved using NetApp SnapMirror. SnapMirror works in synchronous, asynchronous, and semi-synchronous modes, to replicate only the changed blocks on the file system after creating a file system consistent recovery point. Offloading the replication to the storage layer in a multi site environment reduces the network and performance overhead on the DPM server. The data replicated by SnapMirror can be instantly presented to the DPM Server at the DR site.

# 3 DPM INITIAL REPLICATION AND RECOVERY OVERVIEW

Data Protection Manager helps you protect and recover data on the file and application servers in your network. This section describes how to successfully protect and recover data in the DPM environment. For more information, see: http://www.microsoft.com/systemcenter/dpm.

## 3.1 PROTECTING DATA

As illustrated in Figure 1, the high-level process used to protect data involves the following steps:

1. Select data sources on a server that you want to protect, whether it is an application server or a file server.
2. To start protecting data, DPM creates a full copy (referred to as a *replica*) of the selected data sources on the DPM server.
3. To continue protecting data, DPM synchronizes each replica with the data sources on a recurring schedule.
4. To support data recovery, DPM creates point-in-time views (referred to as recovery points) of the replica on a recurring schedule. DPM maintains up to 64 recovery points for volumes and 512 recovery points for applications for each data source. Each recovery point is maintained on a separate volume.

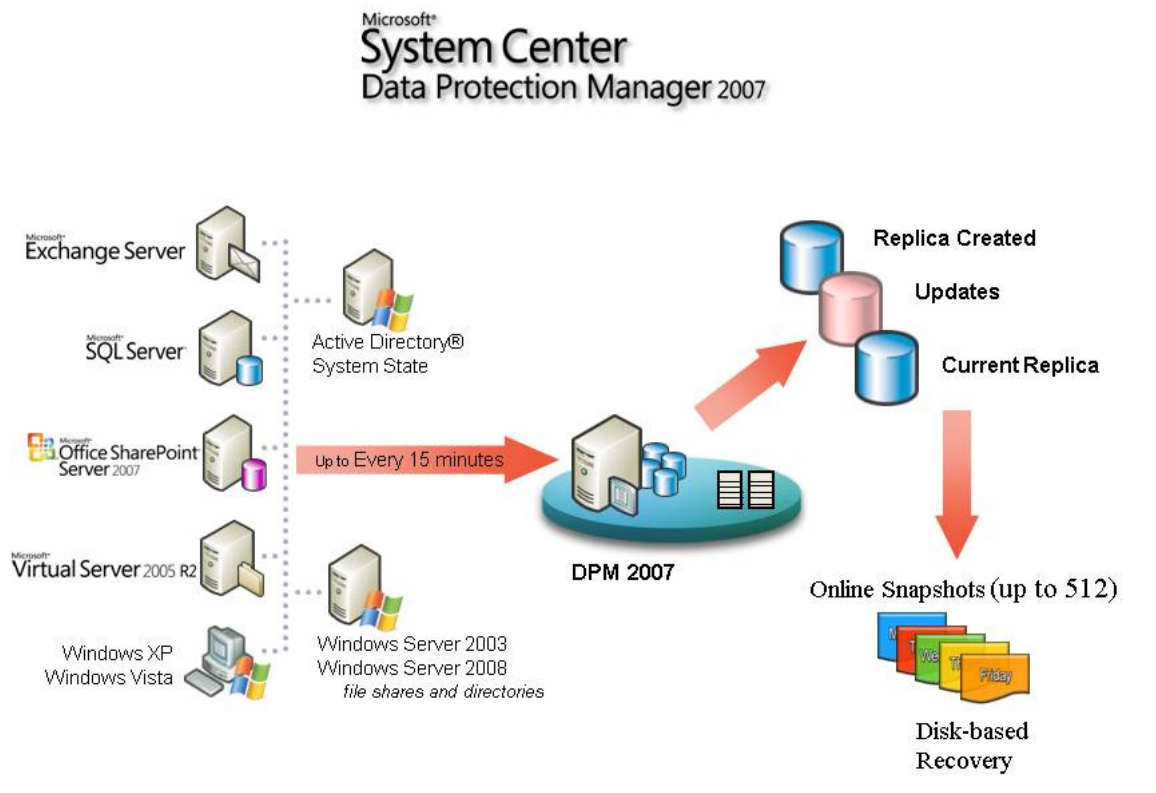



**Figure 1) DPM 2007 data protection.**

## 3.2 RECOVERING DATA

The high-level processes for recovering data is as follows:

1. Selecting the version of the data to be recovered from the recovery points on the DPM server.
2. DPM restores a copy of the selected data to its point of origin on the server or to an alternate destination specified.

# 4 DPM: INITIAL REPLICATION AND RECOVERY PROCESS USING NETAPP FAS SYSTEMS

Designing storage to provide physical boundaries for performance and availability is a well-defined principle that applies to many storage subsystems. Before implementing the procedures outlined on NetApp FAS systems, storage administrators should be familiar with the following:

- Data ONTAP
- SnapDrive for Windows
- FlexClone
- Snapshot

## 4.1 CREATING A DPM PROTECTION GROUP

Data Protection Manager helps you manage the process of protecting and recovering data in the file and application servers in your network. This section describes the high-level steps you need to perform to successfully protect and recover data in the DPM environment. For additional details, see the DPM help files and planning guides.

To protect your data with DPM:

1. Install DPM agents on protected servers.
2. Define the protection group.
3. Select the data to protect.
4. Choose a name and protection method (disk, tape, or both).
5. Select short-term and long-term protection policies.
6. Allocate space for the protection group.
7. Specify tape and library details.
8. Choose a replica creation method.

### 4.1.1 INSTALLING A PROTECTION AGENT

Before protecting data, a protection agent must be installed on each server that contains data to be protected. The agent can be pushed from the DPM server, and installed remotely. The server must be restarted after installing or removing the agent. After the agent is successfully installed, the server is referred to as a protected computer in the Management task screen of the DPM Administrator Console.

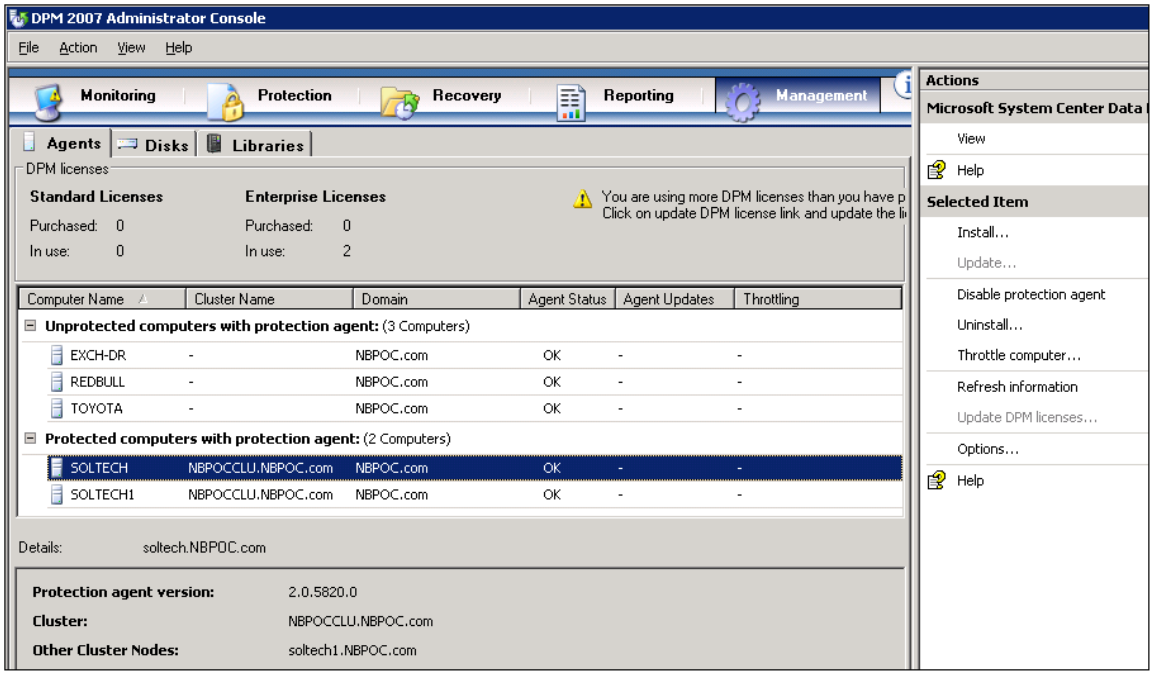



**Figure 2) DPM 2007 data protection.**

### 4.1.2 DEFINING THE PROTECTION GROUP

A protection group is a collection of data sources that share the same protection configuration and schedule. A data source can be a volume, folder, or share. After a data source is added to a protection group, the data source is described as a member of the group.

1. Click the Protection tab from the DPM 2007 Administrator Console and click Create Protection Group.
2. Select the data to protect.

The Create New Protection Group wizard allows selecting unprotected computers with DPM agent installed. Applications such as Microsoft Exchange and SQL must have the database online to appear as an available data source to be protected.

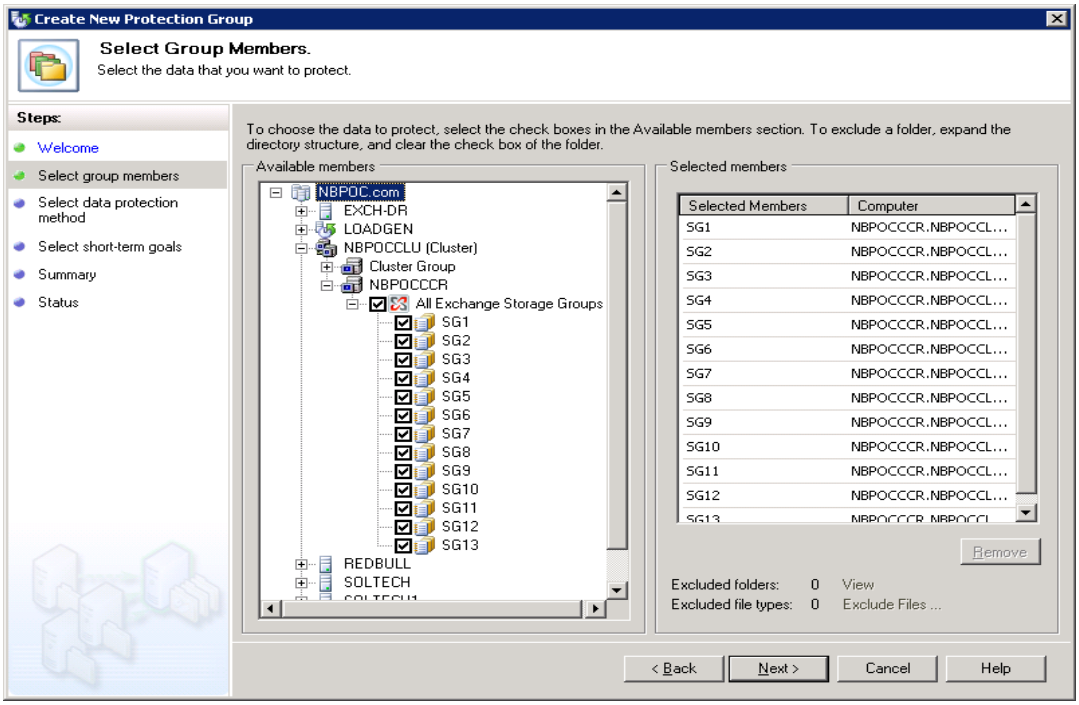
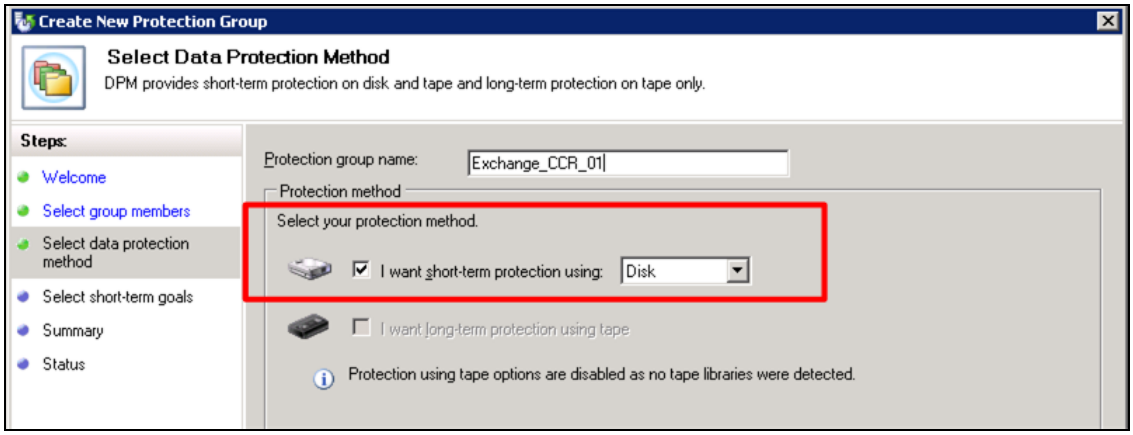



**Figure 3) Create New Protection Group wizard.**

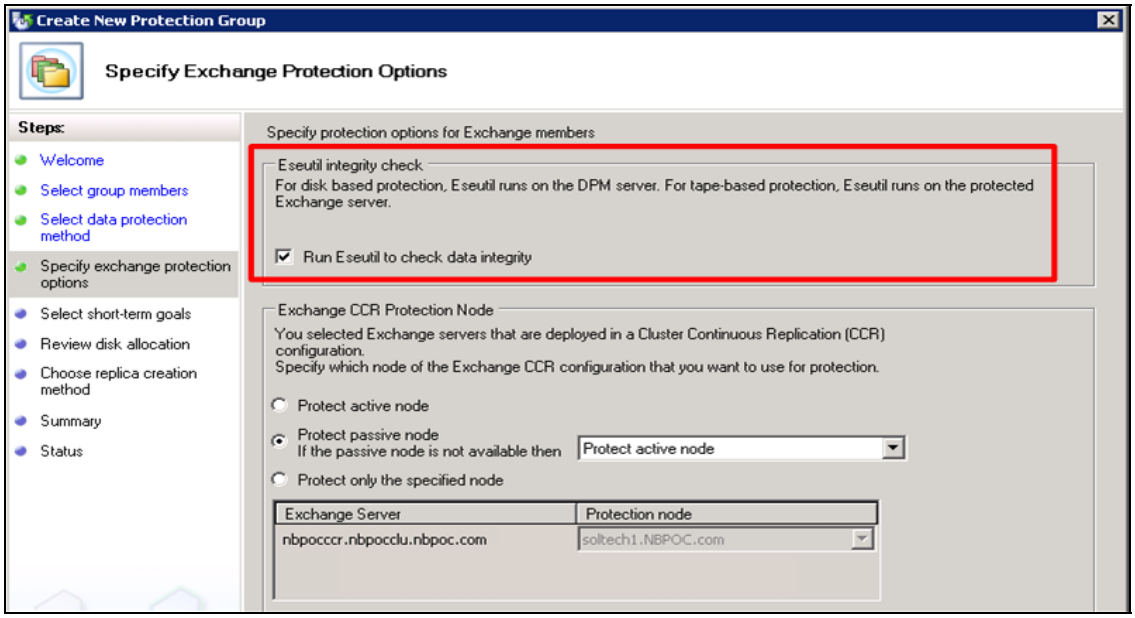
### 4.1.3 CHOOSING A PROTECTION METHOD

DPM supports both disk and tape backups that can be integrated in a disk-to-disk-to-tape rotation (D2D2T). This paper describes the back up procedure to a disk-based target (NetApp FAS) and does not describe the procedure for tape backup.

During initial creation of the DPM Protection Group, the Data Protection Method defaults to disk when there are no tape devices installed on the DPM server. Using DPM 2007 to back up to disk enables SAN administrators to use the SAN infrastructure for backup and recovery of highly available applications such as Microsoft Exchange and SQL Server.




Specify protection options for applications such as running Eseutil checksum. Using disk-based backup allows offloading the Eseutil checksum process to the DPM server. This minimizes the backup load on the Exchange server. In addition, Eseutil checksum can be run at any time on the DPM server with no impact on the Exchange mailbox server.




### 4.1.4 SELECTING PROTECTION POLICIES

The retention range determines how long DPM keeps the protected data available for recovery. You can define both short-term and long-term protection policies to control recovery from both disk and tape. Short-term policies can use either disk or tape, while long-term policies provide control over your extended tape retention.

Recovery point synchronization frequency can be scheduled every 15 minutes. Applications that support incremental recovery points allow frequent backups. Otherwise, DPM synchronizes the recovery point with an express full backup. For additional information on this topic in the DPM 2007 planning guide documentation, see the Microsoft DPM Web site at http://www.microsoft.com/dpm.

### 4.1.5 ALLOCATING DISK (CUSTOM VOLUME)

SAN volumes are presented to DPM as custom volumes. The integration of SAN volumes in DPM is configured in the Disk Allocation Review step in the Create New Protection Group wizard. Before this step can be completed, a clone replica of the data volume that is to be protected must be created.

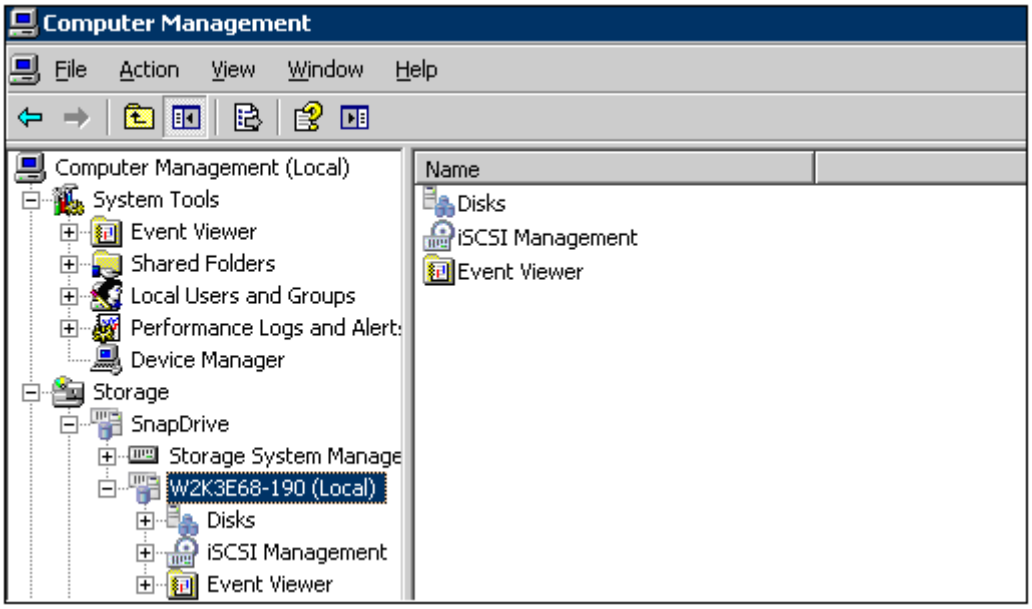
## 4.2 CREATING A SAN REPLICA

This section describes in detail the procedures for creating a clone using SnapDrive.

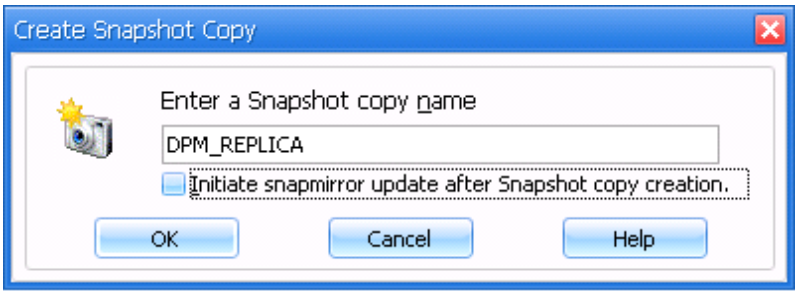
The custom volume should be created using the FlexClone feature in Data ONTAP using SnapDrive for Windows, and the cloned volume should be mounted on the DPM server. This section describes in detail the procedures for creating a clone using SnapDrive.

FlexClone can be created using SnapDrive Snapshot copies as follows:

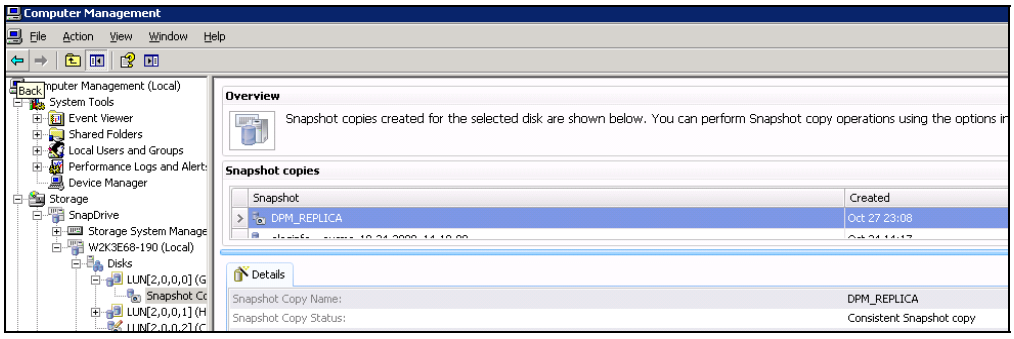
1. Open Computer Management and expand the SnapDrive entry in the left pane.




2. Expand Disks, select a disk, right-click it, and click Create Snapshot. Eter a name for the Snapshot copy and click OK.



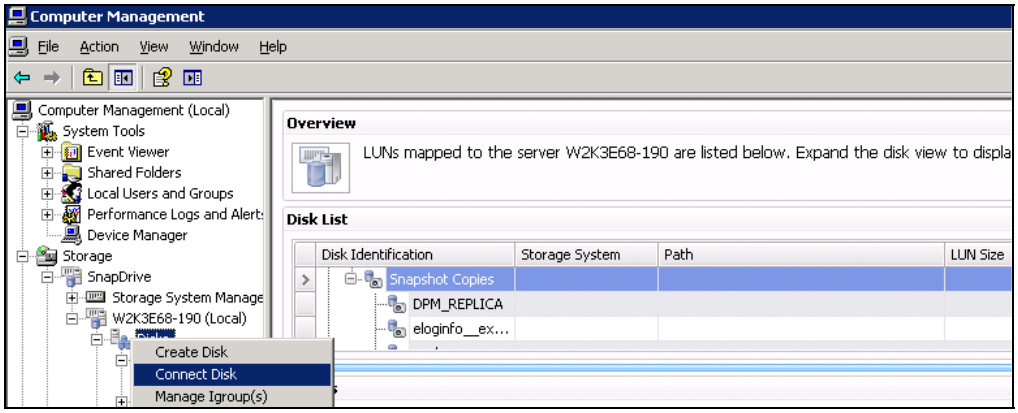

3. After the Snapshot creation is completed, expand the disk, select Snapshot copies in the left pane, and check that the Snapshot copy exists.



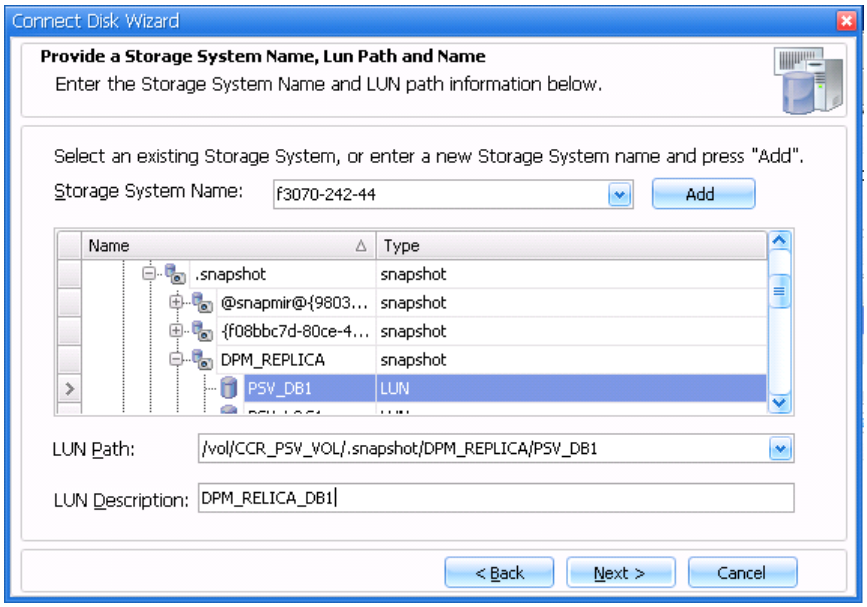
4. Perform the same steps for all the disks provisioned to the protected server.

### 4.2.1 CREATING A CLONE

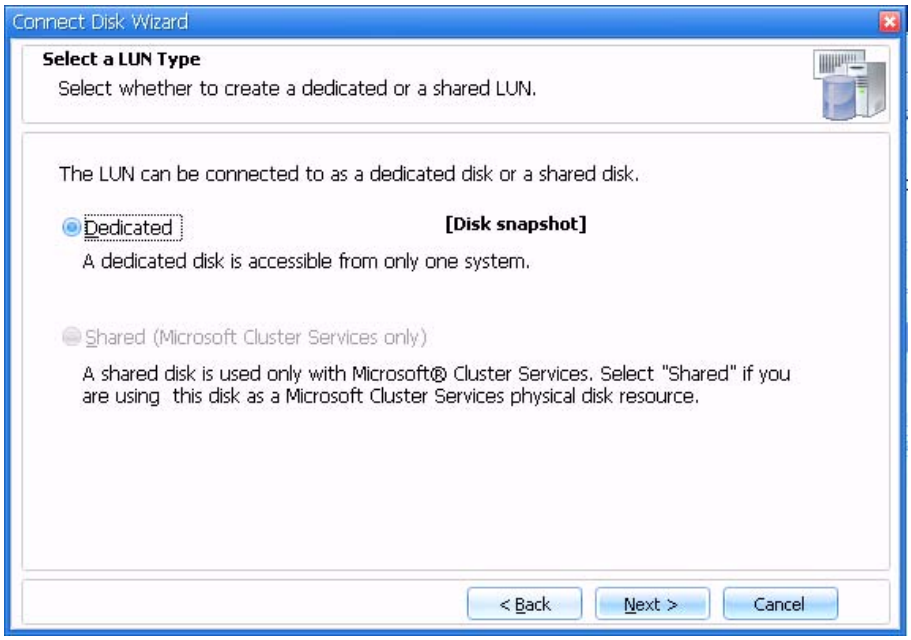
1. From the SnapDrive Management Console, right-click Disks and click Connect Disk to start the Connect Disk wizard.



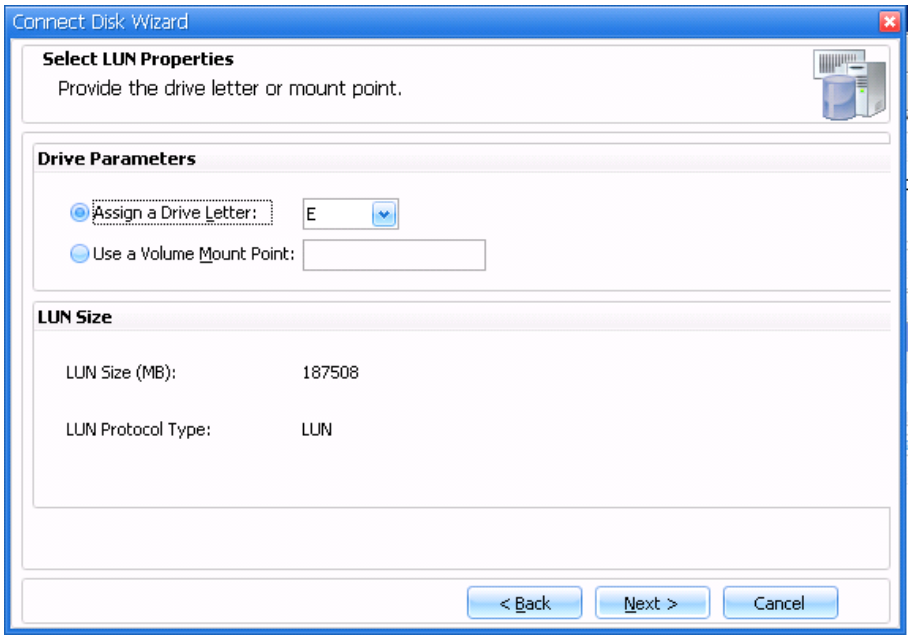

2. In the Storage System Name field, enter the name of the storage system that hosts the application data. Expand the volume and expand Snapshot copy name. Select the LUN (virtual disk) to which you want to connect and click Next.




3. Select the LUN Type. In this case, the drive type can only be Dedicated. Click Next.

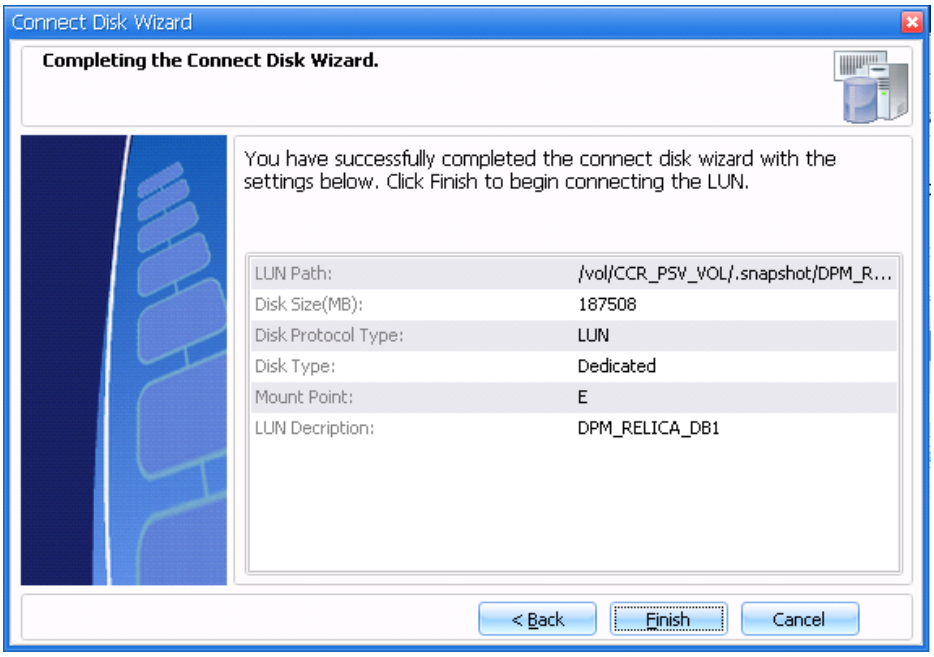



4. Select a drive letter or mount point to be assigned to the drive, and click Next.




5. Select the initiator group through which you want to connect this drive on the storage controller. Click Next and select Automatic to enable SnapDrive to manage the iGroup management, then click Next.

6. Review the summary and then click Finish to complete the Disk Connect wizard.




**Note:** You may have to connect manually to all the disks in the Snapshot copy on the DPM server. This process can be automated by creating a batch file using the SDCLI command line. Refer to the *SnapDrive for Windows Installation and Administration Guide* or enter **`SDCLI`** at the command prompt for the syntax.

### 4.2.2 SPLITTING THE CLONE

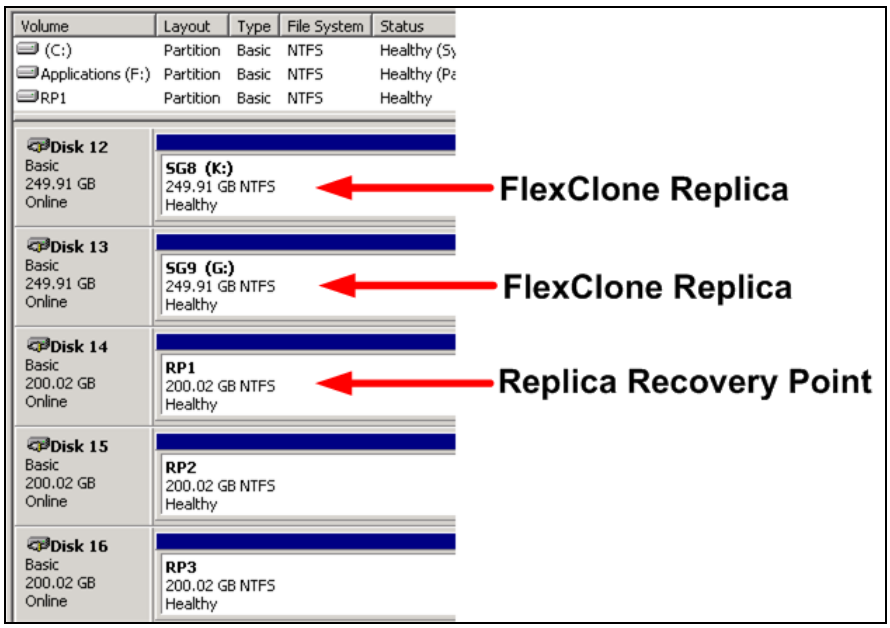
Before a FlexClone volume can be presented to and used by DPM, it must first be made into an independent volume by means of a "clone split". A clone split copies the content of the parent volume to a physically separate volume. The FlexClone volume can be presented to DPM while the split is in progress and this is transparent to the DPM Server.

1. To open the Storage Controller Management GUI, enter `http://<ipaddress>/na_admin`.
2. Expand Volume and FlexClone Volumes and then click Manage.
3. In the right pane, click the FlexClone volume created by SnapDrive and click Rename. Enter a name for the FlexClone volume (This optional step can help ease the administration).
4. In the right pane, check the FlexClone volume created by SnapDrive and click Start Split to split the clone and make this volume an independent copy. A clone split is the process of copying the actual physical blocks of the parent volume. The split times can vary based on the size of the data volume that is being cloned.


5. Create a new volume to be presented to the DPM server recovery point. Typically the recovery point volume should be 1.5 times the data volume.

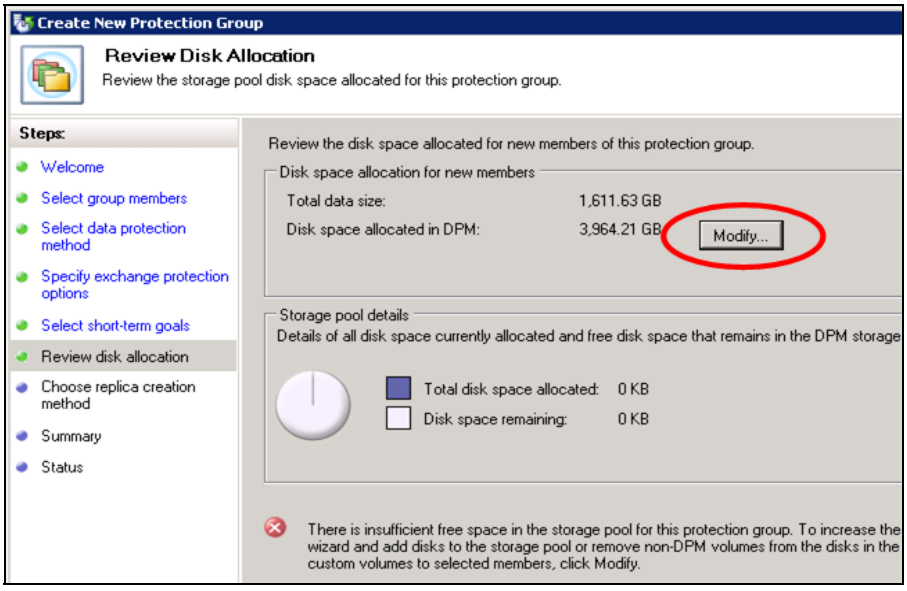
## 4.3 PRESENT THE CLONE REPLICA TO THE DPM 2007 SERVER

A FlexClone can be instantly presented to the DPM server. Drive letters or mount points should be assigned to the replica volume and the replica recovery point. It is helpful to apply meaningful volume names as labels.



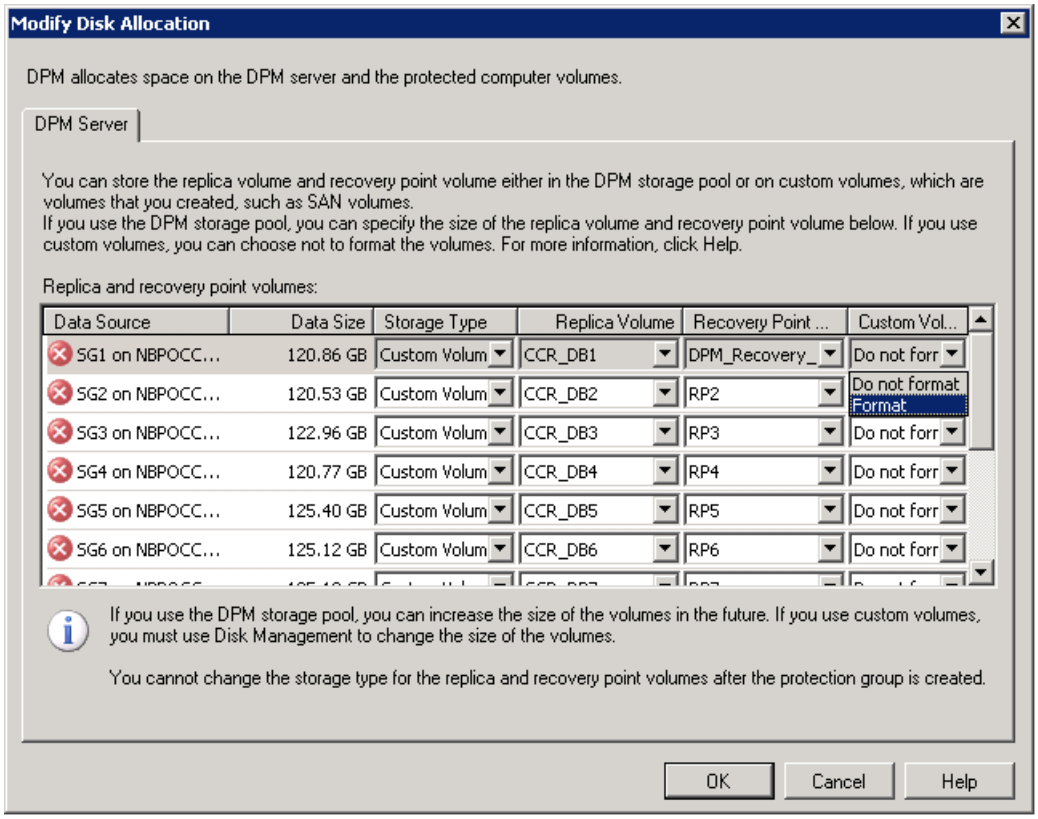

Now the volumes are ready to be allocated as a custom volume for the protection group.

Select Modify from the Review Disk Allocation pane.



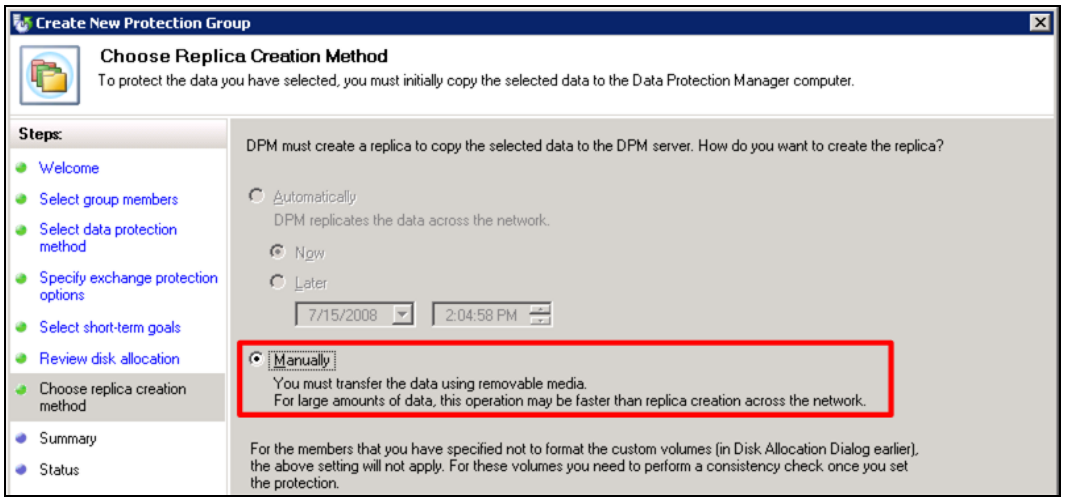
### 4.3.1 SELECTING CUSTOM VOLUMES IN DISK ALLOCATION

Click Modify to open the Modify Disk Allocation window. For SAN-based replicas, select the Custom Volumes option. As shown in the following figure, use the Replica Volume and Recovery Point Volume drop-down menus to select the FlexClone volumes already mounted to the DPM 2007 server.




**Note:** Select the Do Not Format option when using custom volumes.

### 4.3.2 CHOOSING REPLICA CREATION METHOD




DPM creates a folder structure and mount point on the clone replica volume. The clone data volume must then be mounted to the new DPM folder path.

1. After closing the Create New Protection Group wizard, notice how DPM created the directory structure for the clone replica volume:
   a. You should see a long path, as shown in the following example. The Full folder appears under it.
   b. The cloned data to be used for initial replication also appears.
2. The administrator must manually move the protected data (folders or the Exchange or SQL files) to the folder structure created by the DPM Data Protection wizard.

**Example:** The following folder structure gets created for:

- **File system:**

  **<Drive:>\DPM-Beta1\DPM\Volumes\Replica\Fileserver.mydomain.corp.myorg.com\File System\D-87a82ad4-f9d2-11d9-b758-000d561ae74f\e55173e1-0b7a-4fa4-b4d1-387ac2b016b8\Full**

  If you are protecting the complete volume, move all the volume contents under …`\Full`.

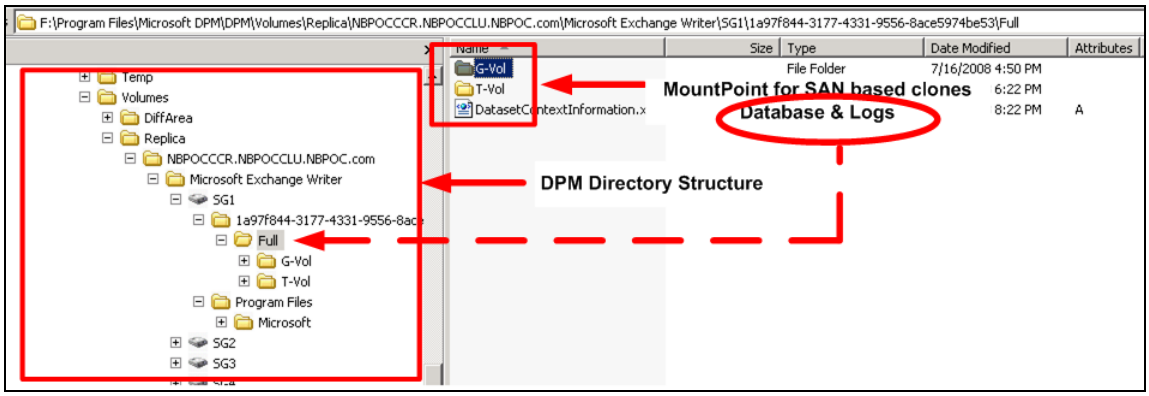
  If you are protecting only `C:\Temp`, move the folder `Temp` and its contents to under …`\Full`.

- **Applications:**

  **<Drive:>\DPM\DPM\Volumes\Replica\Fileserver.mydomain.corp.myorg.com\<Application writer>\<Application Logical Path> \ e55173e1-0b7a-4fa4-b4d1-387ac2b016b8\Full \<Drive Letter-Vol>**

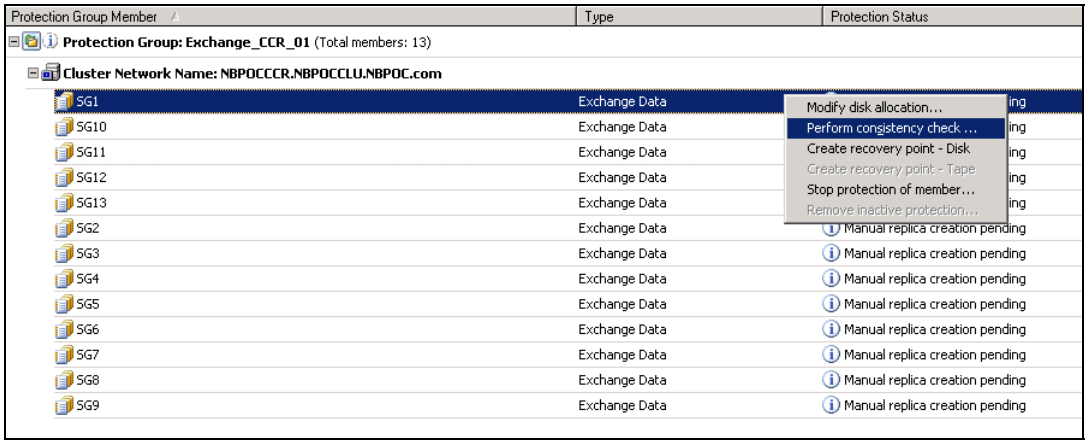
  If you are protecting TestDB in `C:`, move only the database file under …`\C-vol`.

  **<Drive:>\DPM\DPM\Volumes\Replica\Fileserver.mydomain.corp.myorg.com\SQLServerWriter\MS$DPM2007$\TestDB\e55173e1-0b7a-4fa4-b4d1-387ac2b016b8\Full\C-Vol**

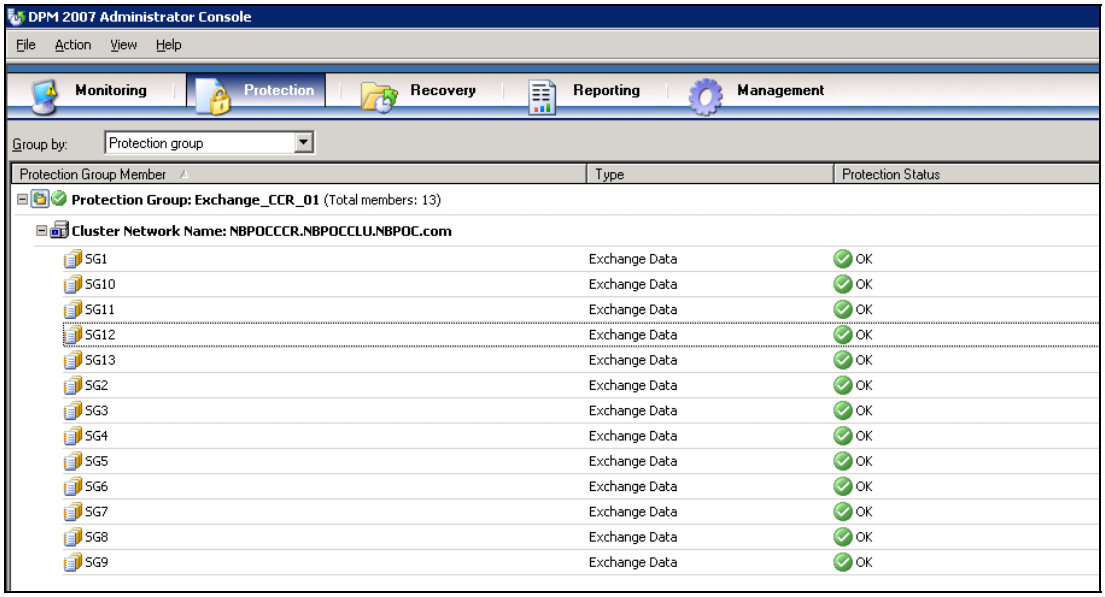



**Note:** Manual replica creation requires mounting the data to the folder path created by DPM on the replica clone volume.

The last step in manual replica creation is a consistency check. Select the newly created Protection Group from the Protection task area of the DPM Administrator Console and select Perform Consistency Check. The consistency check completes quickly with minimal network traffic as the clone replica has very little change from its production data source.

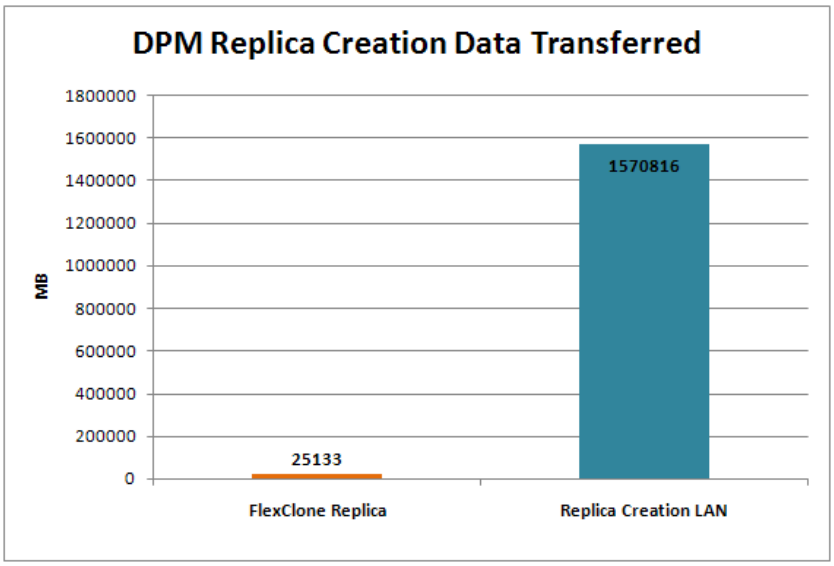



After the consistency check is performed, the initial replica is marked Consistent and the Protection Status turns green.



### 4.3.3 BENEFITS OF MANUAL REPLICA CREATION WITH NETAPP FAS

Using FlexClone to create the initial replica of the protected data on the NetApp FAS system, and manually presenting it to DPM means the protected data is not copied over the network as is the case when using DPM to create the replica. The chart below shows the dramatic difference in network traffic between manual replica creation with FlexClone and automatic replica creation with DPM. Depending on the amount of existing data to protect, the drastically reduced network from manually creating replicas with FlexClone can result in considerable time savings.




## 4.4 REPLICA RECOVERY

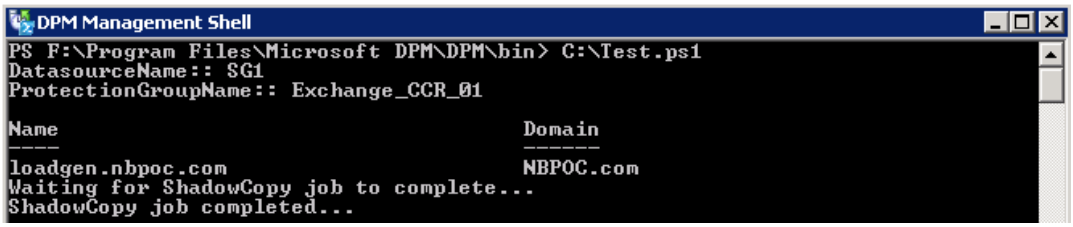
NetApp Snapshot technology enhances recovery options for DPM similar to the way it does for initial replica creation. NetApp Snapshot copies of the replica and the recovery volumes are created from the volumes mounted on the DPM 2007 server. The Snapshot copy is presented to the protected application server. DPM SAN-based recovery can then minimize the LAN network traffic and reduce the time required to recover the data source.

To use Snapshot technology for DPM data recovery, do as follows:

1. Cancel all in progress jobs on the data source being recovered.
2. Use the DPM management shell to initialize a shadow script (see Appendix C).

   The script prompts for the DatasourceName and ProtectionGroupName for the protection group that is being recovered. Then it creates a shadow copy with the “without synchronize” option.

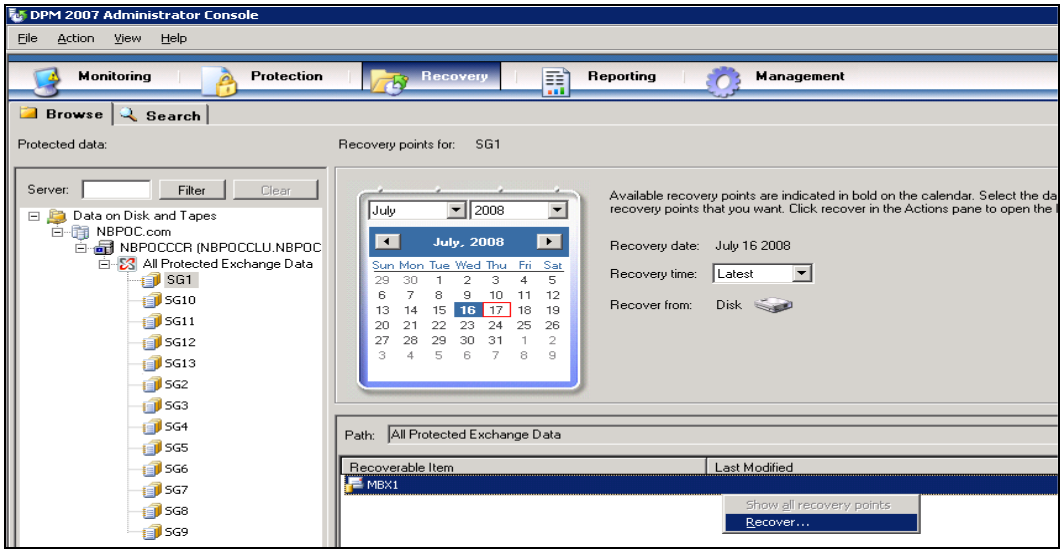
3. From the DPM 2007 server, initiate the DPM management shell.
   a. Copy the ShadowCopy script to the DPM server.
   b. At the DPM management shell prompt, enter the script followed by the parameters for the protection group and the data source.



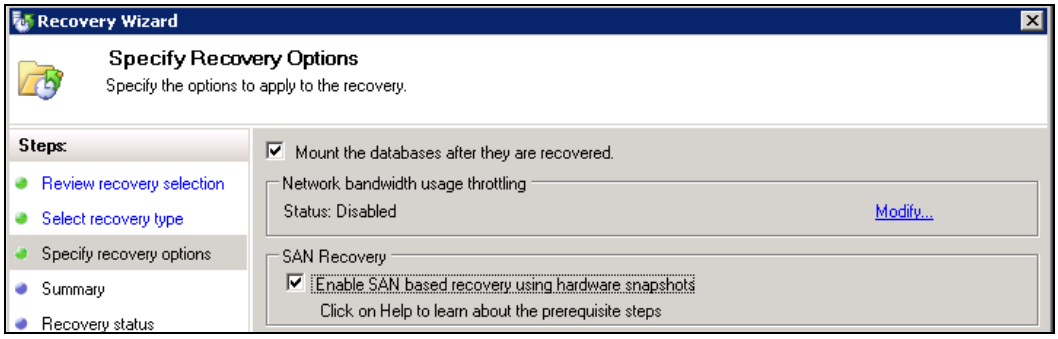

4. Use SnapDrive for Windows to create Snapshot copies of the DPM Replica required for recovery. The Snapshot copy can be mounted to the protected server. The DPM recovery process then copies the data source to the original location.

a. Mount the hardware-Snapshot-based LUNs on the protected server that is being recovered.

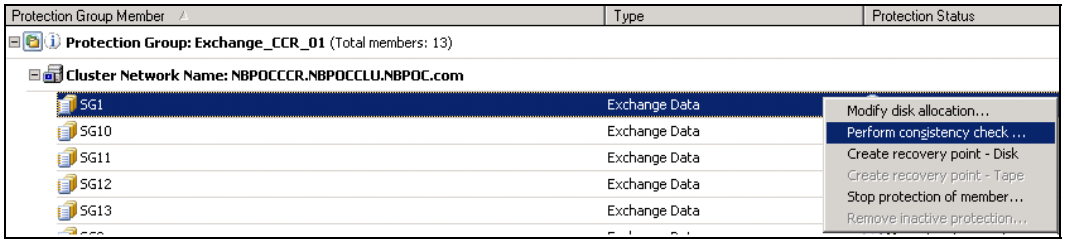
5. Using the DPM Administrator Console, recover from any point in time.




6. Select Enable SAN-based Recovery Using Hardware Snapshots.

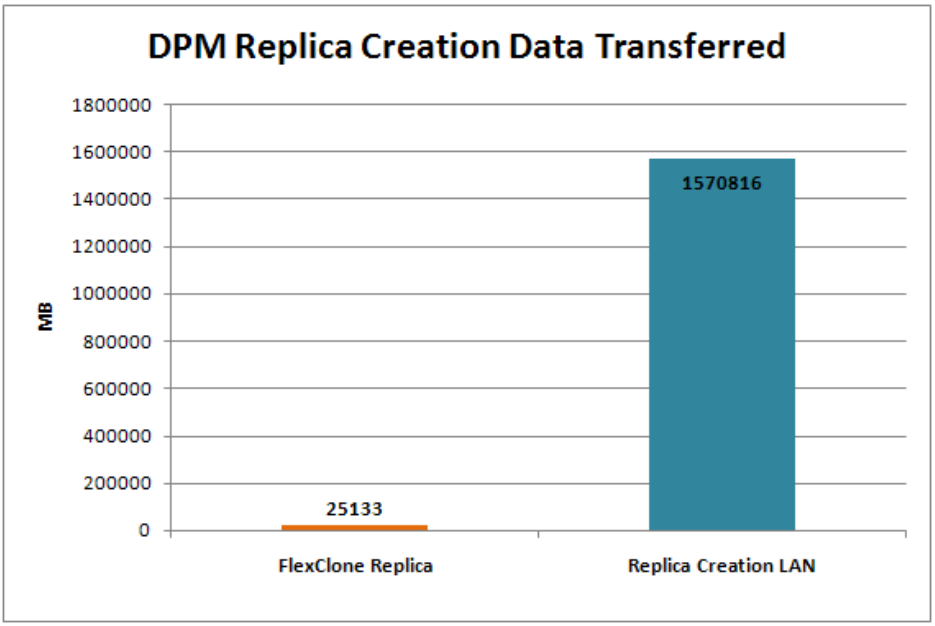



7. After recovery completes, run a consistency check.



# 5 BENEFIT OF INITIAL REPLICATION AND RECOVERY BY INTEGRATING DPM 2007 WITH NETAPP FAS SYSTEMS

DPM SAN-based recovery with NetApp FAS systems involves replicating data in the storage layer within the Fabric. This minimizes network traffic and reduces the time to recover a data source. Depending on the amount of data to recover, SAN-based recovery can considerably reduce downtime for events that require restoring data from backup.




# 6 CONCLUSION

NetApp FAS systems are the ideal storage solution for Data Protection Manager 2007. NetApp FAS systems allow you to configure DPM to protect your application data quickly with faster initial replica creation. NetApp FAS systems enable you to commit to more aggressive RTOs by reducing the time it takes to restore your DPM backups with SAN-based recovery. NetApp FAS systems can store your DPM backups using significantly less physical storage with NetApp FAS systems than you would need with other storage technologies. The robust, flexible, easy to use, and highly available NetApp FAS systems enable DPM to backup your application data without disruption, and to restore it when you need.

# 7 APPENDIX A: REQUIREMENTS AND PREREQUISITES

## 7.1 DPM SERVER

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

To install DPM successfully, you must install the software listed in the following table before installing the DPM application. DPM Setup then installs the additional required software.

If you want to install the required software manually, follow the steps in "Manually Installing Prerequisite Software" in the *Data Protection Manager Help*.

**Table 2) DPM server requirements.**

| Software | Install From |
|---|---|
| Microsoft Management Console 3.0 | http://go.microsoft.com/fwlink/?LinkId=55423 |
| KB 891957<br>**Note:** This hot fix resolves an issue with Windows-based systems that may cause them to deplete their paged pool if the Volume Shadow Copy Service is placed under heavy load. | 32-Bit x86 operating systems:<br>http://go.microsoft.com/fwlink/?LinkId=48584<br>x64-Bit operating systems:<br>http://go.microsoft.com/fwlink/?LinkId=75131 |
| KB 940349<br>**Note:** To apply this update, you must have Windows Server 2003 Service Pack 2 (SP2) installed on the computer. | http://support.microsoft.com/kb/940349/en-us |
| Windows PowerShell 1.0 | 32-Bit x86 operating systems:<br>http://go.microsoft.com/fwlink/?LinkId=658<br>x64-Bit operating systems:<br>http://go.microsoft.com/fwlink/?LinkId=65814 |

## 7.2 PROTECTED SERVER REQUIREMENTS

Each server protected by Microsoft System Center DPM 2007 must meet the requirements listed in Table 3.

**Table 3) Protected server requirements.**

| Protected Servers | Server Prerequisites |
|---|---|
| File Servers | • Windows Server 2003 with Service Pack 1 (SP1)<br>• Windows Server 2003 x64<br>• Windows Server 2003 R2<br>• Windows Server 2003 R2 x64<br>• Windows Storage Server 2003 with Service Pack 1 (SP1)<br><br>**Note:** To obtain SP1 for Windows Storage Server 2003, contact your original equipment manufacturer.<br><br>• Windows Storage Server 2003 R2<br>• Windows Storage Server 2003 R2 x64<br><br>**Note:** DPM supports both Standard and Enterprise Editions of all the required operating systems. |

| Protected Servers | Server Prerequisites |
|---|---|
| SQL Servers | • Microsoft SQL Server 2000 with Service Pack 4 (SP4)<br>or<br>• Microsoft SQL Server 2005 with Service Pack 1 (SP1) or Service Pack 2 (SP2)<br><br>**Note:** DPM supports Standard, Enterprise, Workgroup, and Express Editions of SQL Server.<br>**Important:** 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.<br><br>To start the SQL Server VSS Writer Service:<br>• Click Start, select Administrative Tools, and then click Services.<br>• On the Services screen, scroll down, right-click SQL Server VSS writer, and then click Start. |
| Exchange Servers | Exchange Server 2003 with Service Pack 2 (SP2)<br>or<br>Exchange Server 2007<br>**Note:** DPM supports Standard and Enterprise Editions of Exchange Server.<br>The eseutil.exe and ese.dll versions that are installed on the most recent edition of Exchange Server must be the same versions that are installed on the DPM server.<br><br>In addition, you must update eseutil.exe and ese.dll on the DPM server if they are updated on a computer running Exchange Server after applying an upgrade or an update. |
| Computers running Virtual Server | Microsoft Virtual Server 2005 R2 SP1 |
| Windows SharePoint Services | • Windows SharePoint Services (WSS) 3.0<br>• Microsoft Office SharePoint Server (MOSS) 2007<br><br>Start the WSS Writer service on the WSS Server and then provide the protection agent with credentials for the WSS farm. For more information about Configuring DPM 2007, see "Starting and Configuring the WSS VSS Writer Service."<br>Update the instance of SQL Server 2005 to SQL Server 2005 SP2. |
| Shared Disk Clusters | File servers:<br>SQL Server 2000 with Service Pack 4 (SP4)<br>SQL Server 2005 with Service Pack 1 (SP1)<br>Exchange Server 2003 with Service Pack 2 (SP2)<br>Exchange Server 2007 SP1<br><br>**Note:** 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. |

| Protected Servers | Server Prerequisites |
|---|---|
| Nonshared disk clusters | Exchange 2007 Cluster Continuous Replication<br><br>Before you can protect Exchange Server 2007 data in a Clustered Continuous Replication (CCR) configuration, you must install hotfix 940006. For details, see Knowledge Base article 940006, "Description of Update Rollup 4 for Exchange 2007." |

## 7.3 NETAPP SNAPDRIVE FOR WINDOWS—SOFTWARE PREREQUISITES

The host must be running either Windows Server 2008 or Windows Server 2003 Standard or Enterprise Edition 32-bit or 64-bit (x64 and IA64) with Service Pack 2 with the following hot fixes.

**Table 4) Software requirements.**

| Operating System and Service Pack Level | Required Hot Fixes |
|---|---|
| Windows Server 2003 SP2 | • 919117<br>• 931300<br>• 932755<br>• 937382 |
| Windows Server 2008 | • 950927<br>• 954475 |

**Note:** For a list of the latest Service Packs and hot fixes required by SnapDrive, see the product description page in the Software Download section of the NOW™ NetApp on the Web) site at http://now.netapp.com/.

# 8 APPENDIX B: GLOSSARY

**Table 5) Glossary.**

| Term | Description |
|---|---|
| custom volume | For certain protected objects, DPM can create custom volumes to hold the replica and recovery point data for those objects, as opposed to creating volumes within the DPM storage pool. By using custom volumes, administrators can leverage SAN capabilities for initial sync and recovery. There is a one-to-one correspondence between custom volumes and the production volumes protected. |
| disk | The disk that is mounted into the Windows file system as a drive letter or mount point. For example, Windows Disk Manager lists all the disks that are mounted to that server. In the case of a SAN, a disk is assigned to a LUN (Fibre Channel) or a volume (iSCSI). DPM also uses the term disk when assigning physical storage to its storage pool. |
| DPM replica volume | A logical volume created by DPM that contains the latest full image of a protected object. |
| DPM recovery point volume | A logical volume created by DPM that contains all valid backup points going back in time. |
| DPM storage pool | A pool of disks that DPM uses as its general repository for replica and recovery point volumes. |
| Volume Shadow Copy Service (VSS) | VSS is a Windows mechanism to ensure that complex applications such as Exchange and SQL Server are consistent when backed up. The three components to VSS are a VSS Requestor (typically a backup product), which “requests” a backup for a particular application; a VSS Writer, which quiesces the application and the database to prepare it for the backup; and a VSS Provider, which performs the backup. Typically, the backup that is performed is a Snapshot copy of the appropriate volumes. |
| Recovery Point Objective (RTO) | The Recovery Point Objective (RPO) is the point in time to which you must recover data as defined by your organization. This is generally a definition of what an organization determines is an "acceptable loss" in a distressed situation. |
| Recovery Time Objective (RTO) | The Recovery Time Objective (RTO) is the duration of time and a service level within which a business process must be restored after a disaster (or disruption) in order to avoid unacceptable consequences associated with a break in business continuity. |

# 9 APPENDIX C: CREATE SHADOWCOPY POWERSHELL SCRIPT

```
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
```

# 10 APPENDIX D: SOFTWARE AND HARDWARE VERSION

**Table 6) Software version.**

| Software Feature | Function | Benefit |
|---|---|---|
| Microsoft | Windows Server | 2003 with SP2 |
| Microsoft | Exchange Server | 2007 with SP1 (CCR) |
| Microsoft | iSCSI initiator | 2.07 |
| Microsoft | System Center Data Protection Manager | 2007 |
| NetApp | FAS 3070 | Data ONTAP 7.2.4 |
| IBM | X 3650 | |

# 11 APPENDIX E: LAB TEST CONFIGURATION

The test environment consists of a single Active Directory (AD) domain that supports the Exchange 2007 infrastructure. The Exchange 2007 infrastructure consists of an Exchange Cluster Continuous Replication (CCR) hosting 10,000 user mailboxes simulated by Microsoft Exchange Server Load Generator 2007. One server is configured for both hub transport and client access server roles.

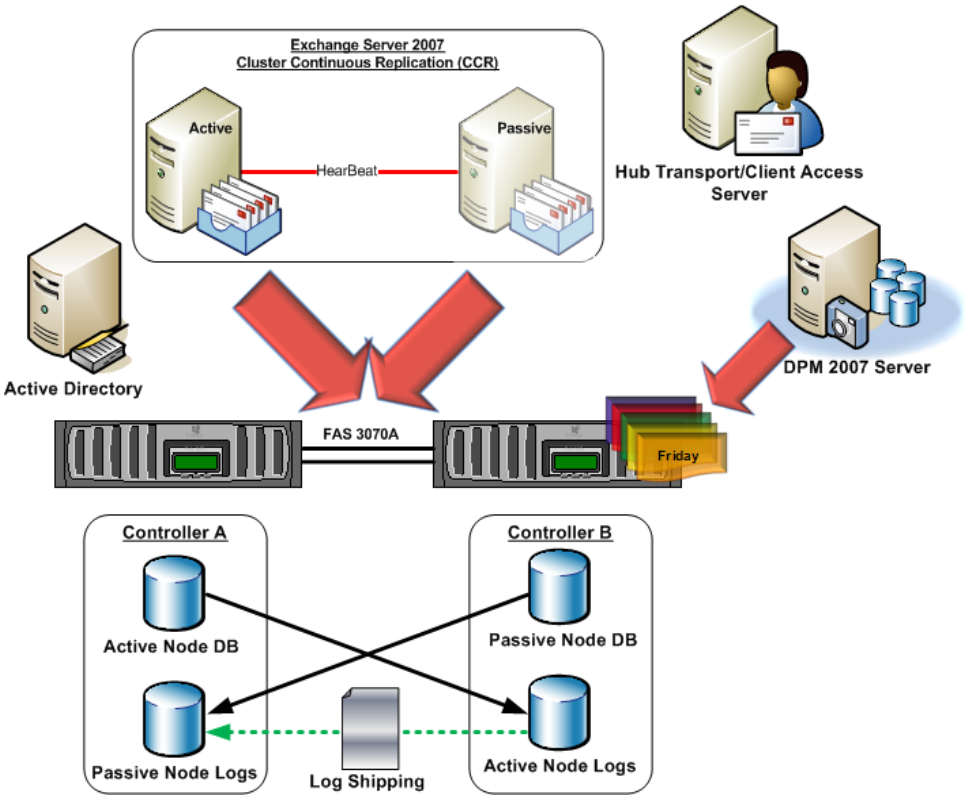



**Figure 4) Lab test configuration.**

# 12 APPENDIX F: RESOURCES

This section lists useful resources to assist you in planning your DPM deployment.

Microsoft System Center Data Protection Manager 2007 Documentation
http://technet.microsoft.com/hi-in/library/bb795539(en-us).aspx

DPM 2007 System Prerequisites
http://technet.microsoft.com/hi-in/library/bb808832(en-us).aspx

DPM 2007 Deployment Planning Guide
http://www.microsoft.com/DOWNLOADS/details.aspx?familyid=50B54355-D497-4E8B-89BC-5C52CF0FB76A&displaylang=en

NetApp Storage Systems
http://www.netapp.com/us/products/storage-systems/

Data ONTAP documentation
http://now.netapp.com/NOW/knowledge/docs/ontap/ontap_index.shtml

NetApp SnapDrive for Windows
http://now.netapp.com/NOW/knowledge/docs/snapdrive/relsnap601/html/index.shtml

www.netapp.com

© 2008 NetApp. All rights reserved. Specifications are subject to change without notice. NetApp, the NetApp logo, Go further, faster, DataFabric, Data ONTAP, FlexCache, FlexClone, FlexShare, FlexVol, MultiStore, NOW, SnapDrive, SnapManager, SnapMirror, SnapMover, SnapRestore, Snapshot, and SyncMirror are trademarks or registered trademarks of NetApp, Inc. in the United States and/or other countries. Linux is registered trademark of Linus Torvalds. Microsoft, Active Directory, SharePoint, SQL Server, Vista, and Windows are registered trademarks of Microsoft Corporation. UNIX is a registered trademark of The Open Group. All other brands or products are trademarks or registered trademarks of their respective holders and should be treated as such.