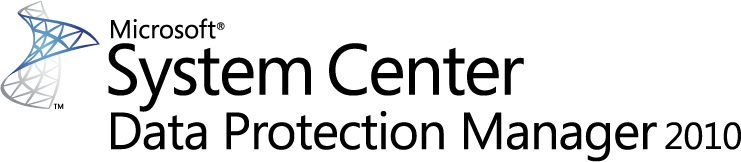


****

Protecting Virtual Environments with System Center Data Protection Manager 2010

Published: February 2010

For the latest information, please see <www.microsoft.com/DPM/virtualization>

Executive Summary:

Microsoft System Center Data Protection Manager 2010 (DPM) provides continuous data protection for virtual machines hosted on servers running Microsoft’s Hyper-V. This protection includes online backup of supported guest virtual machines hosted on clustered or standalone systems; protection of virtual machines during the live migration process; and, item level recovery from host-level backup. DPM 2010 offers disk-to-disk, disk-to-tape, and disk-to-disk-to-tape technologies; all of which maintain the business value of a virtualized infrastructure by ensuring that it is better protected and always available.

Contents

[Protecting Critical Business Data 1](#_Toc253378937)

[Business Imperatives 1](#_Toc253378938)

[Improving Protection with Data Protection Manager 2](#_Toc253378939)

[Microsoft and Windows-Specific Design 2](#_Toc253378940)

[Unified Protection for Disk, Tape, and Cloud 3](#_Toc253378941)

[Ease of Use and Management 4](#_Toc253378942)

[Using Microsoft DPM 2010 to Protect Hyper-V 5](#_Toc253378943)

[Typical protection for virtual machines 5](#_Toc253378944)

[Better protection for virtual machines with DPM 6](#_Toc253378945)

[How DPM uses VSS in Hyper-V 6](#_Toc253378946)

[What’s New in DPM 2010 for Hyper-V 8](#_Toc253378947)

[Cluster Shared Volumes 8](#_Toc253378948)

[Live Migration 8](#_Toc253378949)

[Item Level Recovery 8](#_Toc253378950)

[How to Protect Hyper-V with DPM 2010 10](#_Toc253378951)

[Installing the DPM Server 10](#_Toc253378952)

[Configuring Disk/Tape Media for the DPM Server 11](#_Toc253378953)

[Figure 2. Configuring disk media for a DPM server. 12](#_Toc253378954)

[Installing the DPM Agent and Preparing Hyper-V hosts 12](#_Toc253378955)

[Configuring Protection Groups 13](#_Toc253378956)

[Additional Considerations 14](#_Toc253378957)

[How to Recover Virtual Machines with DPM 2010 15](#_Toc253378958)

[Recovering a Virtual Machine to its Original Host 15](#_Toc253378959)

[Recovering a Virtual Machine to an Alternate Host 15](#_Toc253378960)

[Restore Virtual Machine Files to a Network Folder 17](#_Toc253378961)

[Recovering Individual File Items from VM Backups 17](#_Toc253378962)

[Best Practices 18](#_Toc253378963)

[Storage Calculator 18](#_Toc253378964)

[Conclusion 19](#_Toc253378965)

# Protecting Critical Business Data

Protecting business data is about protecting an organization’s memory. For example, when a business loses data stored in a database, it will forget its customer orders. When a business loses the data hosted on a mailbox server, it forgets its internal and external conversations. When a business loses the data hosted on its SharePoint sites, it forgets the plans it has made for the future.

When you are determining the best way of protecting that organizational memory, you need to find the right balance between factors such as legal requirements, auditing capabilities, data security, and cost. Finding this balance involves understanding the underlying business cases for data protection and addressing technical challenges that may restrict you from meeting your organization’s data protection goals.

This paper outlines benefits of using Microsoft System Center Data Protection Manager 2010 (DPM) for your data protection needs. These include:

* DPM is built specifically to protect Windows environments and products, with an emphasis on Hyper-V and virtualization.
* DPM 2010 offers enhanced and improved methods of backing up to tape, disk, or hosted servers.
* DPM 2010 offers a streamlined interface administrators need in order to work through complex tasks.

## Business Imperatives

When deciding on a specific data protection solution and strategy it is necessary to first understand your organization’s common data management scenarios. For example:

* **Managing system downtime.** Organizations are dependent on their information systems in order to stay productive, and can be crippled without access to their systems and data. There is a direct relationship between the amount of time it takes for an organization to recover its failed infrastructure and the cost of that loss to the organization.
* **Allocating sufficient backup time.** Traditional IT operations have a limited, defined window of time during which they can perform backups, yet the amount of data organizations need to protect continues to grow each year. Deciding on a data protection solution requires a thorough understanding of how long your backups take and whether backups can occur at the same time as normal IT operations.
* **Gauging backup solution reliability.** When selecting a data protection solution, you must assess the reliability of the backup medium along with the cost of the solution relative to that reliability. For example, backing up data to a RAID 1+0 storage device is going to produce a more reliable data recovery solution than backing up to a single tape drive, but is also going to cost a lot more money.
* **Protecting branch and remote offices.** In the current IT landscape, many organizations are moving towards consolidating their IT infrastructure. As part of this move, it is necessary to ensure that data hosted at branch office and remote locations is as protected as data hosted at the head office.

# Improving Protection with Data Protection Manager

DPM is a Microsoft product specifically developed to provide a cost-effective and reliable data protection solution to servers running Microsoft workloads. Microsoft System Center Data Protection Manager (DPM) addresses two specific data protection challenges: The need for more effective backup and restore functionality with disk rather than tape, and the need to better centralize remote and branch office backup.

DPM 2006 was the first version of DPM.–It focused specifically on the protection of file servers and servers running file-based applications. DPM 2006 wasn’t intended for protecting virtual machines because of the sort of complexities and interdependencies discussed earlier. DPM 2007 was built with a high degree of awareness of how specific Microsoft applications, such as Virtual Server 2005 R2 with SP1, Exchange Server, SQL Server, Microsoft Office SharePoint Server and Hyper-V (DPM 2007 SP1) store data on volumes. Hence, DPM 2007 could provide tailored, application-aware protection for these services. It was later extended to support Hyper-V with DPM 2007 Service Pack 1.

DPM 2010 increases the support provided to virtual machines hosted on Microsoft’s Hyper-V, ensuring that these VMs are protected at all stages of the virtual machine life cycle. This includes full and consistent protection for the Hyper-V live migration process. DPM 2010 also provides an improved user interface, increased PowerShell support, and a robust replication and checkpoint system. This allows systems administrators and IT generalists to develop their own recovery infrastructure, perform their own virtual machine backup, and perform recovery operations without relying on backup or storage specialists.

## Microsoft and Windows-Specific Design

As one of the largest IT companies in the world, Microsoft has significant internal data protection requirements. Given that the company uses its own products for its IT infrastructure, it also has one of the biggest deployments of Microsoft products in the world. Several years ago, Microsoft performed an internal investigation to analyze how the third-party data protection tools met the organization’s backup and recovery needs. The investigation found that there were gaps between the protection that Microsoft needed and the protection those products could provide. With this disparity in mind, Microsoft began development of System Center Data Protection Manager.

DPM is an integrated part of the now mature, robust Microsoft System Center platform. This integration means that organizations can realize synergies by combining DPM with other System Center components. For example:

* **System Center Operations Manager** can be configured to monitor the DPM servers, Hyper-V hosts, and virtual machines in an environment. This allows administrators to view, at a glance, the health and status of all protected servers in addition to the DPM server that is providing the protection.
* **System Center Configuration Manager** can be used to automatically deploy DPM agents to production servers. It can also be used to manage and deploy updates to DPM servers, Hyper-V hosts, and protected virtual machines.
* **System Center Virtual Machine Manager** can be tightly integrated with DPM 2010. For example, VMM utilizes intelligent placement to ensure that virtual machines are recovered on hosts with appropriate available resources.

Using a Microsoft solution to protect a Microsoft product can reduce confusion and frustration when trying to integrate Windows environments and third-party data protection products. When an administrator needs useful assistance with restoring critical organizational data, he wants to make contact with a single organization to get the help he needs as quickly as possible. Administrators do not want to have to go back and forth between two different organizations to determine which one will be able to assist in returning the data assets to full availability.

Some third-party backup solutions leverage unsupported and undocumented APIs and reverse engineer unsupported processes to back up Microsoft products. This can lead to unexpected outcomes in the restoration and recovery of data. However, when an administrator uses DPM to protect a Microsoft product, he only needs to contact Microsoft in the event that support is required. In short, when an organization uses Microsoft DPM to protect a Microsoft workload, the buck stops with Microsoft.

## Unified Protection for Disk, Tape, and Cloud

DPM 2010 allows organizations to find a comfortable balance between disk-based, tape-based, and cloud-based backup systems. Administrators can use disk-based and tape-based backup to perform rapid recovery of recent data from disk media on a regular basis, and to retrieve and restore much older protected data from archival tape media when required.

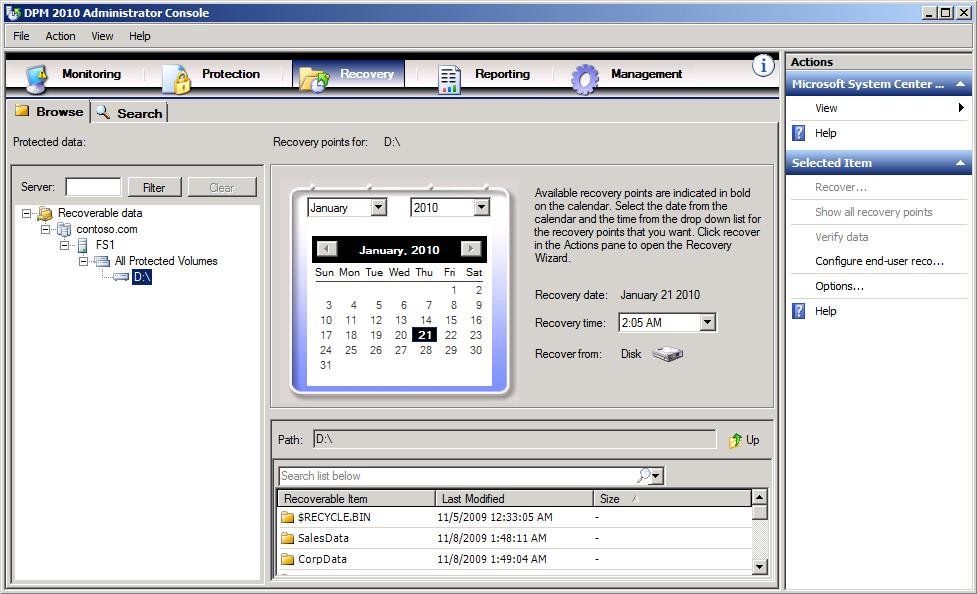
**Disk-Based Backup.** With DPM 2010, disk-based backup is used as the storage location for recent data protection operations. Disk-based protection allows for rapid backup and restore of protected data. This speed is critical in that the vast majority of restore operations occur within a relatively short period after a data backup.

**Tape-Based Backup**. Although protected data is not initially written to tape, tape-based backup does have a place in a DPM data protection ecosystem. DPM allows backed-up data to be copied to tape for the purposes of meeting data retention and archiving requirements.

**Cloud-Based Backup**. DPM can be configured to replicate backed-up data across the Internet to a disaster recovery DPM server that is hosted at a separate data center. Microsoft has also partnered with Iron Mountain for a service called CloudRecovery™ that sends the data from an on-site DPM server to an Iron Mountain data center ([www.microsoft.com/DPM/cloud](http://www.microsoft.com/DPM/cloud)). The technologies that make DPM efficient in transporting branch office backup data to a DPM server in a main office also make DPM efficient in transporting backed-up data to other locations on the Internet. Appendix A provides more information on the kind of hosted backup solution that allows organizations to accomplish this data protection objective.

## Ease of Use and Management

DPM 2010 leverages an interface that is familiar across Microsoft’s System Center suite. The DPM interface is engineered to help administrators perform complex tasks with a minimum amount of fuss. In a high-stress data recovery scenario the design of the DPM interface ensures that it is not necessary for administrators to waste time searching through a labyrinth of menus to find a way to launch a specific task or configure a specific option.

**Figure 1. DPM Administrator Console**

DPM 2010 provides structured workflows and wizards to guide administrators through the following series of logical steps:

* Browsing the available host servers and virtual machines
* Specifying recovery goals and retention objectives
* Protecting data

DPM handles the processes of locating the data to protect, managing the disk-based images and logs, and developing a tape rotation policy.

# Using Microsoft DPM 2010 to Protect Hyper-V

Non-Microsoft backup solutions tend to take a generic backup functionality and adapt it to support-specific applications. Microsoft created DPM 2010 to leverage fully supported Microsoft technologies in order to provide continuous data protection, specifically for Windows Server 2008 and Windows Server 2008 R2 hosts running the Hyper-V role.

DPM 2010 protects virtual machines hosted on servers running Hyper-V in a manner fully supported by Microsoft. This support includes:

* Online backup of supported guest virtual machines hosted on clustered or standalone systems.
* Protection of virtual machines during the live migration process.
* Item level recovery from host level backup.

You can recover protected virtual machines to either the original or an alternate Hyper-V host. DPM 2010 also allows recovery of virtual machine hard disks and configuration files to network shares and the restoration of individual files or folders hosted on virtual machine hard disks without requiring the recovery of the virtual machine.

## Typical protection for virtual machines

Backing up and restoring Hyper-V virtual machine files in a consistent fashion is significantly more challenging than backing up closed, static files. A few reasons are:

* Virtual hard drive files host the thousands of files and folders present on a live disk volume. For this reason, it is necessary to ensure that virtual files are in a consistent state before it is possible to process the virtual hard drive files.
* The data stored in virtual machine RAM is in a constantly changing state.
* The virtual machine configuration files may change depending on the state of the virtual machine.
* It is necessary to deal with the state of at least two computers, the virtual machine host and the virtual machine themselves, each of which is in motion independent of the other.

Although Microsoft recommends that backup solutions that protect virtual machines should use the Hyper-V Volume Shadow Copy Services (VSS) writer, not all data protection products leverage this technology. A backup application must capture the state of the virtual machine’s hard drives and configuration in such a way that they are consistent and reflect the state of the virtual machine at the same precise point in time.

Some backup solutions put virtual machines into a state of paused hibernation in which the hard disk drives and memory are frozen. A copy of the frozen virtual machine can then be made before the virtual machine is returned to full operation. Although this approach does ensure that a consistent backup occurs, it also means that the virtual machine is not available to clients during the period when the virtual machine is being frozen and copied. For example, a virtual machine that hosts the back-end database for an e-commerce site would be unavailable to that e-commerce site during the backup process. This would also mean that the administrators of that virtual machine would have to structure their backup routine around the times that it could be offline.

## Better protection for virtual machines with DPM

DPM 2010 is engineered to provide the best possible protection for virtual machines hosted on the Hyper-V platform. The team that built DPM 2010 worked in consultation with the team that built the Windows Server 2008 Hyper-V role to ensure that virtual machine workloads hosted under Hyper-V are protected just as reliably as workloads hosted on traditionally deployed physical servers.

DPM 2010 seamlessly interacts with the Hyper-V VSS writer so that, depending on the operating system of the virtual machine being captured, consistent versions of a virtual machine can be captured and protected without impacting client access to the virtual machines. For example, if the virtual machine hosting a back-end database was running Windows Server 2008 with SQL Server 2005, a backup could occur without a client interrupting connections to the virtual machine. In order to provide a consistent backup to a guest operating system that has no VSS support, such as some Linux distributions or Windows 2000, DPM has to instruct Hyper-V to hibernate the VM.

## How DPM uses VSS in Hyper-V

The ability to back up open files is critical when it comes to protecting active virtual machines. Volume Shadow Copy Services (VSS) is a technology first introduced in Windows Server 2003 that can be used to create frozen copies of open files. Without VSS a virtual machine would need to be put into hibernation or shut down before a consistent backup of its could be made.

The Hyper-V VSS writer is a special component that ensures that shadow copies can be made of Hyper-V virtual machine files. It is supported on virtual machines running Windows Server 2003, Windows Server 2003 R2, Windows Server 2008 and Windows Server 2008 R2. Virtual machines running these operating systems can be protected by DPM without interrupting the services they provide to clients. VSS, DPM, and Hyper-V interact in the following ways:

* The DPM block-based synchronization engine makes an initial copy of the protected virtual machine and ensures that the copy of the virtual machine is complete and consistent.
* Once the initial copy is made and verified, DPM 2010 captures backups using the Hyper-V VSS writer. The writer provides a data-consistent set of disk-blocks that are synchronized with the DPM server. This approach provides the benefit of a “full backup” with the DPM server while minimizing the amount of backup data that needs to be transferred across the network.
* The DPM agent on a Hyper-V host uses the existing Hyper-V APIs to determine whether a protected virtual machine also supports VSS.
  + If a virtual machine is running Windows Server 2003 or later, and has the Hyper-V integration services component installed, then the Hyper-V VSS writer will recursively forward the VSS request through to all VSS-aware processes on the virtual machine. (This occurs without the DPM 2010 agent being installed on the virtual machine.) This recursive VSS request allows the Hyper-V VSS writer to ensure that disk write operations are synchronized so that a VSS snapshot is captured without the loss of data.
  + The Hyper-V integration services component invokes the VSS writer in VSS-aware applications, such as Exchange Server 2010 and SQL Server 2008, to ensure that their application data is in a consistent state.
  + If the virtual machine does not support VSS, then DPM 2010 will automatically use the Hyper-V APIs to pause the virtual machine before capturing data files.

After the initial baseline copy of the virtual machine synchronizes with the DPM server, all changes made to the virtual machine resources are captured in a new recovery point. The recovery point represents the consistent state of the virtual machine at a specific point in time. Recovery point captures can occur at least once a day. When a new recovery point is created, DPM uses block-level replication in conjunction with the Hyper-V VSS writer to determine which blocks have been altered on the Hyper-V host since the last recovery point was created. These data blocks are then transferred to the DPM server and applied to the replica of the protected data.

The DPM server uses VSS on the volumes that host recovery data so that multiple shadow copies are available. Each of these shadow copies provides a separate recovery point - DPM can maintain up to 448 separate recovery points. VSS recovery points are stored on the DPM server. The temporary copy taken on the host is only stored for the duration of the DPM synchronization.

In addition to protecting individual virtual machines hosted on a Hyper-V server, DPM can also protect workloads running in a virtual machine for an extra level of protection. This is the only method by which you can protect data stored on pass-through disks. Pass-through disks allow the virtual machine direct access to the storage device and do not store virtual volume data within a VHD file.

A big advantage to protecting virtual machines by running the DPM agent on the Hyper-V server and within the guest virtual machines is the ability to restore a protected workload to another protected location. For example, if you configured the DPM agent on a virtual machine that was running SQL Server 2008 as well as its Hyper-V host, not only could you restore the entire virtual machine to another Hyper-V host, but you could also restore a specific SQL Server 2008 database to any protected server running SQL Server 2008. You could then seamlessly restore a database that originated on a virtual machine to a physical computer running SQL Server 2008, or restore a mailbox from a protected physical server running Exchange Server 2010 to a protected virtual server running Exchange Server 2010.

## What’s New in DPM 2010 for Hyper-V

DPM 2010 builds on the functionality of previous versions of DPM for the protection of virtual machines. You can configure DPM 2010 to protect virtual machines running on Windows Server 2008 and Windows Server 2008 R2 hosts that have the Hyper-V role installed.

DPM 2010 can also restore virtual machines to alternate Hyper-V hosts so that they can be brought online, something that was only indirectly possible in DPM 2007 SP1. DPM 2010 can protect Hyper-V hosts during the Live Migration process. Not only are you able to restore virtual machine hard disk files to network locations using DPM 2010, you can also use DPM 2010 to perform item-level recovery.

DPM 2010 can also protect virtual machines deployed in the following scenarios:

* Cluster Shared Volumes (CSV.)
* Highly available virtual machines hosted on a failover cluster.
* Virtual machines deployed on standalone Hyper-V hosts.

### Cluster Shared Volumes

A new and important feature of DPM 2010 is its ability to protect Hyper-V virtual machines that are hosted on Cluster Shared Volumes (CSV.) CSV is a Windows Server 2008 R2 failover technology that allows multiple clustered virtual machines using the same LUN (disk) to fail over individually. To learn more about Cluster Shared Volumes and Hyper-V, consult the following web page: <http://technet.microsoft.com/en-us/library/dd630633(WS.10).aspx>

### Live Migration

Live Migration is a process that allows a virtual machine to move from one Windows Server 2008 R2 Hyper-V host to another without clients of that virtual machine experiencing any disruption of service or downtime. For example, server Alpha hosts a virtual machine named Gamma. Virtual machine Gamma functions as a streaming media server. Clients streaming media from Gamma would experience no disruption in that service when an administrator uses the live migration process to migrate the virtual machine to another Hyper-V server named Beta. In contrast, prior to the Windows Server 2008 R2 version of Hyper-V, it was only possible to perform a quick migration. During quick-migration there was a small period of client disruption when the virtual machine was transferred between Hyper-V hosts.

DPM 2010 protects Hyper-V virtual machines before, during, and after the live migration process. In the event that a problem occurs during the handoff from the original host to the destination host, such as both hosts failing, it is possible to recover the VM to the original host or to an alternate host.

### Item Level Recovery

Item Level Recovery (ILR) is a feature of DPM 2010 that allows administrators to restore files hosted on a Hyper-V virtual machine to a network share or to a volume on the Hyper-V host server protected by DPM. ILR does not require the restoration of the virtual machine on which the file or files were originally hosted. For example, a virtualized file server hosted on a Hyper-V host protected by DPM 2010 is decommissioned. A short time after the virtualized file server is decommissioned and deleted from the original Hyper-V host, you realize that a set of important files that were hosted on the virtualized file server have been lost and were not stored elsewhere. Rather than having to restore the entire decommissioned virtualized file server to retrieve the files, DPM 2010 Item Level Recovery can help recover just the files of interest to the host Hyper-V server or to a network share accessible from the DPM 2010 console.

# How to Protect Hyper-V with DPM 2010

In this section you will learn how to perform specific Hyper-V protection tasks using DPM 2010. In this section you will learn how to:

* Install DPM 2010
* Configure disk/tape media for the DPM server
* Install the DPM agent and preparing Hyper-V hosts
* Configure protection groups

### Installing the DPM Server

DPM 2010 requires a server running an x64 version of Windows Server 2008 or Windows Server 2008 R2 with a minimum of 512 MB of RAM, 1 GB free on the system volume, 1.3 GB available on the volume that hosts the DPM files and 900 MB on the volume hosting the database. In a simple deployment, you should devote one disk to hosting the operating system, DPM software and SQL server database and use other disks for hosting protected data. Prior to installing DPM 2010 you should ensure that your computer is running Windows Server 2008 with the following components installed:

* .NET 3.5 Service Pack 1
* Windows Installer 4.5
* Windows Single Instance Store (SIS)
* PowerShell 2.0

These components are already available on servers that use the Windows Server 2008 R2 operating system. DPM 2010 should not be installed on a server under the following circumstances:

* The server functions as a Management Server for SCOM 2007.
* The server functions as an application server.
* The server is part of a Windows Server 2008 or Windows Server 2008 R2 failover cluster.

DPM 2010 also requires access to a private instance of SQL Server 2008 or SQL Server 2008 R2. This instance can be installed locally on the computer that will host DPM 2010 as a part of the DPM installation process, or can be configured separately on a remote server. Both DPM 2010 and SQL Server 2008/2008 R2 can be hosted on an x64 virtual machine running Windows Server 2008 or Windows Server 2008 R2.

To install DPM 2010, perform the following steps:

1. On the Microsoft System Center Data Protection Manager 2010 screen, click the **Install Data Protection Manager** item.
2. Review and then accept the license agreement, then click **OK**. On the Welcome page, click **Next**. The DPM 2010 installer will now perform a prerequisite check. Once the check completes successfully, click **Next**.
3. On the Product Registration page enter registration details.
4. On the Installation Settings page select the folder that will host the DPM program files. Specify whether you want to have an SQL Server instance installed locally or if you are going to use an instance of SQL Server that you created earlier.
5. On the Security Settings page configure passwords for the MICROSOFT$DPM$Acct and DPMR$<computer name> local user accounts and then click **Next**.
6. On the Microsoft Update Opt-In page, specify if you want to sign up for Microsoft Update and then click **Next**. On the Summary of Settings page review the installation choices that you have made and then click **Install.** After installation completes, restart the DPM 2010 host computer.

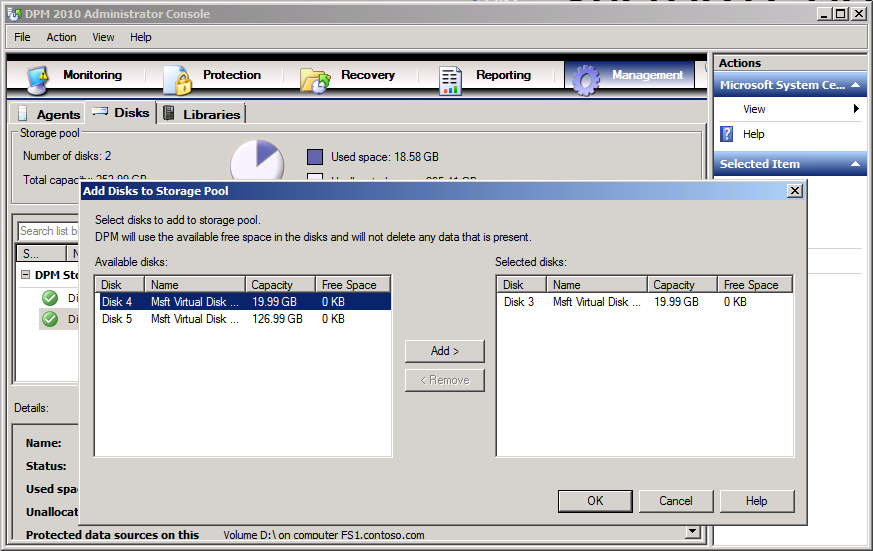
To get the most up-to-date information about installing DPM 2010, consult the following document on Microsoft TechNet: <http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=b880c90b-60cc-4087-b5e5-308e4ac8c78f>

### Configuring Disk/Tape Media for the DPM Server

Windows Server 2008 and 2008 R2 must recognize a storage device as locally attached before DPM can use it for storage. DPM can use direct-attached storage (DAS) or SAN devices attached through iSCSI or Fibre Channel to store protected data. DPM cannot store protected data on removable disk media like USB or IEEE 1394 hard disk drives because these devices are not always attached and do not support VSS. Any volumes that are used must be dedicated to DPM, but it is not necessary to allocate entire disks to DPM. It is possible to add RAID volumes to storage pools, but Microsoft does not recommend the use of RAID 5 due to the technology’s write performance characteristics.

To add disks to the storage pool, perform the following tasks:

1. Open the DPM Administrator Console, click **Management** on the navigation bar and then click the **Disks** tab.
2. To add disks to the DPM storage pool, click **Add** in the Actions pane. This will open the Add Disks To Storage Pool dialog box, shown in the figure below. This dialog box will list all locally attached disks that are available for use by DPM. This list will include all appropriately configured iSCSI and Fibre Channel disks.
3. Select the disks that you wish to add to the storage pool and click **Add**. You can also use this dialog box to remove disks from the DPM 2010 storage pool.



### Figure 2. Configuring disk media for a DPM server.

### Installing the DPM Agent and Preparing Hyper-V hosts

After you have deployed DPM, it will scan the Active Directory service to locate servers that can be protected. You can access this list of servers through the Protection Agent Installation Wizard. You can then install the agent directly using the DPM 2010 console.

Alternatively, you can deploy the agent by using System Center Configuration Manager 2007 R2 or by deploying the installer using software installation policy options of group policy. If you are protecting virtual machines on computers running Hyper-V on Windows Server 2008, you must also ensure that either the hotfix released in January 2009 updating the VSS writer for DPM protection of virtual machines, or Windows Server 2008 service pack 2 is installed. It is not necessary to install the hotfix on computers running Windows Server 2008 R2. A download of the hotfix is available at <http://support.microsoft.com/default.aspx?scid=kb;EN-US;959962>.

To install the DPM protection agent on a Hyper-V host server using the DPM 2010 console, perform the following steps:

1. In the DPM 2010 console, click **Management** and then click on **Agents** tab. In the Actions pane, click **Install.** This launches the Protection Agent Installation Wizard.
2. Select the Hyper-V servers on which you want to install the protection agent from the list of discovered computers, and then click **Add**. When all Hyper-V servers that you want to protect are added to the list, click **Next.**
3. Enter the details of the administrator account to use for the installation of the agent. The domain account must be a member of the local Administrators group on each target Hyper-V server.
4. Specify how you want the target servers to restart in order to complete the installation of the DPM 2010 agent.
5. If any of the selected servers are members of a cluster, you will be presented with an additional screen to choose how to restart the clustered service. You must install the DPM 2010 agent on all nodes in the cluster.
6. Review the summary and click **Install Agents**. Once agent installation is complete, click **Close** to close the Protection Agent Installation Wizard.

### Configuring Protection Groups

Protection Groups in DPM 2010 allow you to group together similar resources so that they can be protected in a similar way. Virtual machines in the same protection group use the same protection method and use the same short- and long-term protection policies.

When you configure a protection group, the wizard recommends allocations for these volumes based on an estimate of the size of the data in the specified protection group. To configure protection groups, perform the following steps:

1. In the DPM Administrator Console, click **Protection** on the navigation bar.
2. In the Actions pane, click **Create Protection Group**. The Create New Protection Group wizard will start. On the Welcome page, click **Next**.
3. On the Select Protection Group Type page, click **Servers** and then click **Next.**
4. Expand the Hyper-V server to see the virtual machines that are hosted on the server. Select the virtual machines that you want to add to the protection group and then click **Next**.
5. Specify a unique name for the protection group or accept the default name.
6. Define protection policies:
   * If you want to define the short-term protection for this protection group, select the **I Want Short-Term Protection Using** checkbox and then select the media where protected data will be stored.
   * If you want to define the long-term protection policy for the protection group, select the **I Want Long-Term Protection Using Tape** checkbox.
7. If you choose short-term protection, select the retention duration for data recovery in the Retention range box.
8. To modify the recovery point schedule for a data source, click **Modify**. Select the desired day and time and then click **OK**.
9. DPM will display recommended disk allocations for the replica volume and the recovery point volume. You can either accept the recommended allocations or adjust the allocations by clicking **Modify**.
10. If you choose long-term protection, select the retention duration for data recovery in the Retention box. In the Frequency Of Backup box, select the desired backup frequency (daily, weekly, or monthly). DPM will recommend a tape rotation scheme based on these selections. It is also possible to create three custom schemes if necessary.
11. Select the default media label in the Backup Tape Label box and provide a new label name.
12. Select the desired library from the list in the Backup Library box.
13. Select how many drives you want to allocate from the list in the Drives Allocated box.
14. Select the **Erase Tape After Recovery Range Period Is Over** option if you want to automatically destroy expired data.
15. Once all protection options are configured you can choose to have DPM replicate data immediately by selecting **Now**, specifying a later time using **Later** or according to a schedule by selecting **Schedule**.
16. Review the summary and then click **Create Group**. Close the confirmation page.

### Additional Considerations

You should take the following into consideration when preparing to use DPM 2010 to protect virtual machines hosted under Hyper-V:

* If the Hyper-V host will use Cluster Shared Volumes (CSV), ensure that the appropriate Volume Shadow Copy Services (VSS) hardware provider is installed. The VSS hardware provider allows you to back up multiple VMs simultaneously. If the VSS hardware provider is not available, the VSS software provider is used and backup jobs are serialized.
* Ensure that the most up-to-date version of Hyper-V integration services is deployed on each guest virtual machine.
* Treat virtual machines that use pass-through and iSCSI disks differently from other virtual machines hosted under Hyper-V. It is only possible to protect the data hosted on the pass-through or iSCSI disk through the DPM agent installed on the virtual machine. Pass-through and iSCSI disks cannot be protected through the DPM agent installed on the Hyper-V server.

# How to Recover Virtual Machines with DPM 2010

DPM 2010 supports the following recovery scenarios:

* Recovery of the virtual machine to the original Hyper-V server
* Recovery of the virtual machine to an alternate Hyper-V server
* Recovery of virtual machine files to a network folder
* Item level recovery of virtual machines backed up at the host level
* Copy to tape

## Recovering a Virtual Machine to its Original Host

When a virtual machine is recovered to its original location, the original VHD file is deleted and DPM restores the VHD and other configuration files to that original location using the Hyper-V VSS writer. A virtual machine that was made highly available will remain highly available after the recovery process is complete as long as the virtual machine is recovered to its original location.

To recover a Hyper-V virtual machine to its original location, perform the following steps:

1. On clusters, ensure that the resource group containing the virtual machine exists. If it does not exist, create it.
2. Open the DPM Administrator Console and click **Recovery** in the navigation bar.
3. Locate the virtual machine to be recovered from the list of Hyper-V hosts that are protected by the DPM server. Select the specific virtual machine to be recovered.
4. Select the bold date and then time from the drop-down list of recovery points of the recovery point to be recovered.
5. In the Recoverable item pane, click to select the item to be recovered.
6. In the Actions pane, click **Recover**. DPM 2010 starts the recovery wizard. Review the recovery selection and then click **Next.**
7. Select **Recover To Original Instance** and then click **OK**.

## Recovering a Virtual Machine to an Alternate Host

DPM 2010 supports seamless recovery of a protected Hyper-V virtual machine to an alternate Hyper-V host. This can occur independently of processor architecture and is possible between Hyper-V hosts running Windows Server 2008 and Windows Server 2008 R2. For example, you may need to recover a virtual machine to an alternate host if the first host fails, or you may need to recover data from a previous version of the virtual machine while the current version remains available to clients.

Hyper-V virtual machines are not automatically made highly available if they are recovered to an alternate location that also acts as a node in a failover cluster. An administrator must manually make the newly recovered virtual machine highly available when the virtual machine is recovered to an alternate failover cluster.

To recover a Hyper-V virtual machine to an alternate location, perform the following steps:

1. Open the DPM Administrator Console and click **Recovery** in the navigation bar.
2. Locate and select the virtual machine to be recovered from the list of Hyper-V hosts that are protected by the DPM server.
3. Select the bold date and time from the dropdown list of recovery points. In the Recoverable item pane, click to select the item to be recovered.
4. In the Actions pane, click **Recover**. DPM 2010 starts the recovery wizard. Review the recovery selection and then click **Next**.
5. Select the **Recover To An Alternate Location** option. Browse to the Hyper-V server that you want the virtual machine to recover to, and then click **OK**.
6. Review your selection and then click **Recover**. Click **Close** when recovery completes.

## Restore Virtual Machine Files to a Network Folder

Recovering a virtual machine to a network folder allows you to recover virtual machine files, such as VHD and configuration files, to network folders accessible to the DPM console. This option can also be used as a part of the manual migration process.

To restore a virtual machine to a network folder, perform the following steps:

1. Open the DPM Administrator Console and click **Recovery** in the navigation bar.
2. Locate and select the virtual machine to be recovered from the list of Hyper-V hosts that are protected by the DPM server.
3. Select the bold date and time from the drop-down list of recovery points.
4. In the Actions pane, click **Recover**. DPM 2010 starts the recovery wizard. Review the recovery selection and then click **Next**.
5. Select **Copy To A Network Folder** and then click **Next**.
6. Select the destination path to recover the storage group files to and then click **Next**. You can choose to have DPM send an email message once the recovery process is complete.
7. Review your selection and then click **Recover**. Click **Close** when enabled or wait for completion as desired.

## Recovering Individual File Items from VM Backups

To perform an item level recovery, you must install the Hyper-V role on the DPM server if the server is running Windows Server 2008. (This step is not necessary if the DPM server is running the Windows Server 2008 R2 operating system.) You can only use a virtualized DPM server to perform item level recovery if that server is running Windows Server 2008 R2. To perform item level recovery, perform the following steps:

1. In the DPM 2010 administration console, click **Recovery** on the Actions pane.
2. Locate the virtual machine that holds the items that you want to recover. Select item (VHD) from the Results pane.
3. Select the recovery point from which you want to perform the recovery.
4. To view the list of files and folders that can be recovered:
   1. Double-click the item (VHD) that you want to recover in the Recoverable Items list.
   2. Double-click the items (volumes in VHD) that you want to recover in the Recoverable Items list.
5. Select the items (files and folders) that you want to recover. It is possible to select and recover multiple files and/or folders.
6. In the Actions pane, click **Recover**. This starts the recovery wizard.
7. Review the recovery selection and then click **Next**.
8. Select **Copy To A Network Folder** and then click **Next**.
9. Review your selection and then click **Recover**. Click **Close** when recovery completes.

# Best Practices

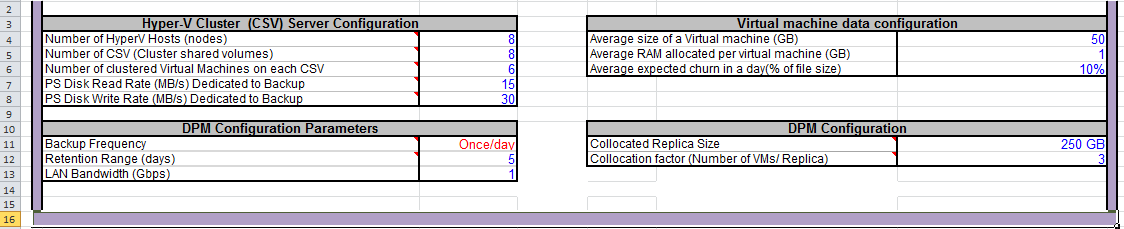
In this section you will find advice on additional aspects of DPM 2010 deployment such as how to calculate the amount of storage space required.

## Storage Calculator

Storage calculator allows you to estimate how much storage you must allocate in DPM 2010 to protect specific resources. DPM 2010 Hyper-V storage calculator is provided to help you plan the protection of your Hyper-V deployment. The storage calculator also provides guidance on three aspects of a DPM 2010 protection for virtual machines running under Hyper-V:

* Estimates how much storage is required to protect a specific Hyper-V environment.
* Outlines the type and class of server, memory requirement, storage requirement and guidance for critical system parameters such as the page file size that are required to create a DPM server.
* Estimates backup window SLAs by providing the time needed for both Initial Replication and Incremental Synchronization.

The input parameters that are required to provide this guidance are as depicted in the screen shot below.



**Figure 3. Storage Calculator example**

Additional tools are available to help you estimate some of the input parameters for your specific implementation such as the amount of change in data from day to day (called “data churn.”) Data “churn” plays a crucial part in estimating the requirement to protect your Hyper-V installation. Another factor that influences the amount of storage you will need is the Retention Range, or the number of days you expect to keep a replica. The Backup Frequency determines how many replica points you will have.

The storage calculator can be used in the initial phase of your DPM 2010 Hyper-V protection to not only estimate the amount of storage you will require but to model your backup policies. You can conduct what-if analysis to see the impact on backup SLAs by changing the storage IOPS and also by varying the network bandwidth available for backup and recovery. You can vary the storage consumption parameters - churn and the Retention Range - to see the effect on the storage requirement over time.

Using the storage calculator to estimate your deployment requirements can result in a deployment configuration that is robust and can function optimally over a period of time.

# Conclusion

Data Protection Manager 2010 provides fully integrated data protection for Hyper-V virtual machines and hosts. DPM was designed in consultation with the virtualization team at Microsoft; therefore, there is a high level of assurance that DPM has a high level of control over recovery time objective and recovery point objective. Deploying DPM 2010 can give an organization confidence that:

* Virtual machines can be quickly and reliably backed up from production Hyper-V servers at frequent intervals throughout the day without a negative impact on performance.
* DPM replicas and recovery points allow organizations to restore virtual machines not only in their most recently backed up configuration, but in any configuration that has existed throughout the defined protection period.
* Flexible recovery options allow virtual machines to be restored not just to the original Hyper-V host, but to other Hyper-V hosts and arbitrary file locations. Features such as Item Level Recovery allow items hosted on virtual machines to be restored separately without requiring the whole virtual machine be restored.

# 

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This white paper is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS   
DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in, or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

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

© 2010 Microsoft Corporation. All rights reserved.

Microsoft is a trademark of the Microsoft group of companies.