System Center Data Protection Manager 2010 delivers unified data protection for Windows servers and clients as a best-of-breed backup & recovery solution from Microsoft, for Windows environments.

DPM 2010 provides the best protection and most supportable restore scenarios from disk, tape and cloud -- in a scalable, manageable and cost-effective way.

## There Is a Better Way to Back Up Microsoft Virtualization hosts!

www.microsoft.com/DPM

TechNet.microsoft.com/DPM

blogs.technet.com/DPM

DPMINFO@microsoft.com

Twitter @SCDPM

If your company relies on Microsoft® Hyper-V™ virtualization technologies within your server infrastructure, who will you trust to ensure its protection and recovery?

As part of the overall Microsoft Virtualization platform, System Center Data Protection Manager 2010 provides host-based and guest-based backup to disk, to tape and to cloud.

**Maximizing Protection of Microsoft Hyper-V technologies with Microsoft Data Protection Manager**

DPM 2010 is designed for the Virtualization or Server Administrator (or the IT generalist) and uses wizards and workflows to help ensure that you can protect your data – without requiring an advanced degree, training or certification in storage and backup technologies.

DPM presents the VMs for protection with awareness of how the VMs will be backed up – either while the VMs are online (using child snapshots) or temporarily taken offline (hibernation).

**New in DPM 2010 for Hyper-V**

DPM 2010 has been enhanced for virtualization environments, including Hyper-V R2:

* Support for Hyper-V R2 LiveMigration scenarios, including protection for Cluster Shared Volumes (CSV).
* Ability to restore VMs to an alternate VM host then where it was backed up from.
* Able to restore individual files from a host-based VM backup (where the VM did not require an agent).

**How DPM protects Virtual Machines**

DPM protects virtual machines based on the how the Hyper-V VSS\* writer reports the capabilities of the VM:

* If the VM is VSS capable, meaning that the guest is running Windows Server 2003 or better, as well as VSS-capable applications like SQL Server – then the VM can typically be backed up while the VM is online (without interruption).
* If the VM or one of its internal workloads is not VSS capable, then the VM will be momentarily hibernated so that it can be backed up and then resumed.

In either case, DPM utilizes the Hyper-V VSS writer to synchronize block-level differences within the VHDs using a process called an “Express Full”, which identifies which blocks have changed in the entire VHD and then sends just the updated blocks or fragments. This provides a complete and consistent image of the virtual hard disk files on the DPM server or appliance. DPM maintains up to 512 shadow copies of the full VHD set by storing only the block-level differences between any two images.

\* *VSS* – *Volume Shadow copy Services***How VM backups should be done**

By leveraging the internal VSS technologies within the Hyper-V Integration Components (HV-ICs) and the workload’s VSS writers, Hyper-V provides a method of using VSS within a VM which delivers an application-aware backup and a snapshot’ed VHD.

Once the VM is internally snapped, the outside of the VHDs are also snapped using VSS. Then any discrepancies between the two snaps are resolved before the DPM agent identifies any new blocks within the VHDs. The changed blocks are then sent to the DPM server, where they can be applied to the DPM server’s copy of the VHDs.

**What can I restore with DPM?**

**Whole VM** – You can restore the entire VM to either its original host or an alternate virtualization host. Because DPM captures the metadata of the virtual machine configuration, DPM is able to recreate the VM on the original Hyper-V host or new host, with the result being a complete VM restore.

**VHD** – You can restore a single VHD from a virtual machine, so that you can recover an entire data set to a previous point in time.

**Individual File or Directory** – You can select individual file objects from a VHD, if the VM file systems are readable by the DPM server, in which case those individual files can be restored directly to any network location.

Note, this capability is for file-based objects. Application-based data (e.g. database) should be restored from a guest-based application-aware backup, instead of a host-based file backup of a .MDF or .EDB file.

**If you are virtualized, check out the System Center suites.**

Protecting a Hyper-V host requires an “Enterprise” DPM management license (E-DPML), with agents for guest VMs purchased separately.

The E-DPML is also included within the System Center bundle suites, including:

* SC Essentials Plus – midsized orgs
* Enterprise Mgmt. suite (SMSE)
* Datacenter Mgmt. suite (SMSD)

One of the benefits of the System Center suites is use rights for your guests, so that you can buy the appropriate suite for your host (even a non-Hyper-V host) and get use rights for your guest VMs.

If you depend on Microsoft Hyper-V to deliver a virtual infrastructure within your company, take a look at how DPM can protect your virtualized infrastructure. As you deploy new Hyper-V R2 (or continue to manage your existing Hyper-V 2008 or Microsoft Virtual Server hosts), know that DPM 2010 is ready to protect your virtual machines.

To learn more, go to:

[www.microsoft.com/DPM/virtuallization](http://www.microsoft.com/DPM/virtuallization)



For more information about Microsoft System Center Data Protection Manager, visit [**www.microsoft.com/DPM**](http://www.microsoft.com/DPM) **.**

For information on the System Center family of IT management technologies for midsized organizations and enterprises, visit [**www.microsoft.com/SystemCenter**](http://www.microsoft.com/SystemCenter)**.**

This data sheet is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS SUMMARY.

The example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein are fictitious. No association with any real company, organization, product, domain name, e-mail address, logo, person, place, or event is intended or should be inferred. (Use this only if fictitious content appears.)