1
Online Articles

Data Protection Manager overview and what's new in DPM's latest release

DPM provides Workload-Aware backups for top Microsoft workloads, namely Exchange Server, SharePoint Server, Hyper-V, and SQL Server. This includes working closely with the workload team to jointly validate backup methodology in all configurations and ensuring that they are fully supported both from the backup and workload perspectives.

DPM is recognized in the industry as a best-in-class enterprise backup, and together with the Azure Backup service, it provides a compelling hybrid cloud backup solution for four key classes of data:

- Enterprise client protection (PCs and desktops).
- Host-level VM backups for Microsoft Hyper-V, more popularly known in the backup domain as *agentless virtual machine backups*.
- Workload-aware backup for Microsoft SQL Server, Microsoft SharePoint Server, and Microsoft Exchange Server. These workloads typically run on a physical server, but they could also be running on a guest operating system in a Hyper-V VM, or an Azure IaaS VM as well.
- Agentless backup for VMware virtual machines. Microsoft also added support for VMware platform by using VMware's VADP API to protect VMware VMs remotely without installing agents on vCenter or ESXi servers. Please read `Chapter 11`, *Protecting VMware VMs*, for more details.

On the client protection side, support was added in Azure Backup to directly protect Windows clients (desktops and clients) in Azure. There has been wide acceptance of this feature since customers like the fact that they can reduce their on-premises storage infrastructure and leverage Azure for it, but still take advantage of enterprise scale management for client machines, such as central management, enforcement of compliance policies, auto-provisioning for new machines, and so on. The goal is to diversify and become a truly heterogeneous enterprise backup solution.

In System Center 2016 and in System Center 2019 DPM, Microsoft added improvements in three key areas: **Storage efficiency**, **Performance**, and **Security**.

The following features were introduced in DPM:

- **Modern Backup Storage (MBS)**: MBS uses **Resilient File System** (**ReFS**) block-cloning technology, which was introduced in Windows Server 2016, to store incremental backups. DPM takes advantage of this improvement by creating storage space savings of up to 30-40%. In addition to space savings, you can create storage based on performance efficiency by configuring **Workload-Aware Storage** so that you back up designated workloads to specific volumes. This will improve DPM performance and reduce I/O requirements by up to 70%, which results in much faster backups. Please read `Chapter 2`, *DPM Post-Installation and Management Tasks*, for more information.
- **Resilient Change Tracking (RCT)**: DPM uses RCT (the native change tracking in Windows Server 2016 Hyper-V), which removes the need to go through a **Consistency Check** (**CC**) in the case of sudden power loss or VM storage migration. DPM can keep tracking of when you move a VM between different storage by using RCT technology. Please read `Chapter 3`, *Protecting Hyper-V VMs*, for more information.
- **Cluster OS Rolling Upgrade**: DPM continues to protect VMs during the cluster OS rolling upgrade from Windows Server 2012 R2 to Windows Server 2016, or from Windows Server 2016 to Windows Server 2019, without bringing it down. Please read `Chapter 3`, *Protecting Hyper-V VMs*, for more information.
- **Shielded Virtual Machine Protection**: Shielded VMs are a set of technologies that have the same goal: protect tenant secrets from tampering and data theft by malware and malicious administrators that got elevated rights inside a virtualized environment. DPM protects and retains the protection provided by shielded VMs to ensure that they can be recovered seamlessly and securely. Please read `Chapter 3`, *Protecting Hyper-V VMs*, for more information.

- **Hyper-V with Storage Spaces Direct (S2D)**: S2D is the first true **Software-Defined Storage** (**SDS**) from Microsoft. DPM will recognize and protect Hyper-V VMs that are deployed on the Storage Spaces Direct cluster. Please read `Chapter 3`, *Protecting Hyper-V VMs*, for more information.
- **Hyper-V with ReFS Scale-Out File Server** (**SOFS) Cluster**: SOFS is a clustered file server feature that was introduced in Windows Server 2012/R2, which lets you store server application data such as Hyper-V virtual machine files and SQL Server databases on SMB file shares. DPM protects Hyper-V VMs that are deployed on ReFS-based SOFS clusters. Backup and recovery can be done with RCT VMs and non-RCT VMs as well.
- **Upgrading DPM does not require a reboot**: In earlier releases of DPM, when you install or upgrade the DPM agent on the production server, you are required to reboot. However, starting with DPM 2016 onward, you are not required to reboot when you deploy the agent. Backups continue to work.

In June 2017, Microsoft introduced a new servicing model called **Semi-Annual Channel** (**SAC**), with a faster release cadence. With this new servicing model, you will see two System Center releases per year. The SAC releases will be available for customers with active Software Assurance. The SAC release is not for every business; if your workloads require longer term stability and predictability, you can still use the **Long-Term Servicing Channel** (**LTSC**) for System Center, which will remain identical to older versions of System Center such as System Center 2012, System Center 2016, and System Center 2019. You can find more information about the System Center release options in the following article: `https://docs.microsoft.com/en-us/system-center/ltsc-and-sac-overview`.

> Please note that if you are using the SAC version, you will receive new features and bug fixes every 6 months. However, if you are using the **Long-Term Servicing Channel** (**LTSC**), Microsoft will continue to release **Update Rollups** (**UR**), but those will only have bug fixes and no new features. With the new SAC release cadence of DPM software, Microsoft is meeting new challenges that companies are struggling with by releasing new features twice a year.

Understanding the prerequisites and considerations for Hyper-V protection

In this recipe, we will cover the prerequisites and considerations for Hyper-V protection. Before you are able to provide a restore plan for your virtual machines to recover the services that you are providing in your modern datacenter, you need to understand the backup prerequisites for protecting Hyper-V virtual machines with DPM.

Prerequisites

The following are the prerequisites for backing up Hyper-V virtual machines with DPM:

- If your recovery plan is to recover files and folders using the **Item-Level Recovery** (**ILR**) feature for virtual machines, then you'll need to make sure that you have installed the Hyper-V role on the DPM server, whether it be physical or virtual. If you only want to recover the virtual machine itself, then the Hyper-V role isn't required.
- You can protect up to a maximum of 800 virtual machines that are 100 GB each with one DPM server, which allows for multiple DPM servers that support larger clusters. When protecting a Hyper-V cluster with multiple DPM servers, you cannot add secondary protection for the protected Hyper-V workloads.
- You can back up a Hyper-V server or cluster in the same domain as the DPM server, or in a child or trusted domain. If you want to backup Hyper-V in a work group or an untrusted domain, you'll need to set up authentication. For a standalone Hyper-V server, you can use NTLM or certificate authentication. For a cluster, you can use certificate authentication only. Please refer to `Chapter 8`, *Protecting Workgroups and Untrusted Domains*, for more information.
- You cannot back up virtual machine data on passthrough disks. In this scenario, Microsoft recommends that you use the host-level to backup VHDX files and guest-level to back up the data within the guest that isn't visible on the Hyper-V host.
- You can back up Hyper-V replica virtual machines starting with DPM 2012 R2 or later when the Hyper-V host is running Windows Server 2012 R2 or later.
- You can back up deduplicated volumes and mount points.

Please note that DPM will not *traverse* mount points located on a volume by itself; you need to explicitly select the mount point at the time of protection. For example, if you protect just the D: volume, DPM will not protect any data under the `mountpointdir` directory on the `D` drive. You need to navigate to the `mountpointdir` directory and protect it; only then will DPM recognize it as a separate volume and protect the data under the mount point.

Hyper-V Host prerequisites

The following versions of Windows Server Hyper-V are supported by DPM 2016 or later, and can protect and restore:

- **Windows Server 2019**: Datacenter and Standard (Server with Desktop Experience and Core)
- **Windows Server 2016**: Datacenter and Standard (Server with Desktop Experience and Core)
- **Windows Server 2012 R2**: Datacenter and Standard (Server with Desktop Experience and Core)
- **Windows Server 2012**: Datacenter and Standard (Server with Desktop Experience and Core)
- **Windows Server 2008 R2 SP1**: Enterprise and Standard (Server with Desktop Experience and Core)
- **Windows Server 2008 SP2**

Hyper-V VM prerequisites

Please look at the following points for the prerequisites for Hyper-V VM:

- The version of integration components that is installed inside the virtual machine should be running the latest version. In Windows Server 2016 Hyper-V, Microsoft changed the update process by updating the Hyper-V integration components in the guest OS via Windows Update. The guest OS in your virtual machines must have access to Windows Update in some way, such as direct access, **Windows Server Update Services** (**WSUS**), or **System Center Configuration Manager** (**SCCM**).

- For each virtual machine you plan to protect, you need free space on the volume hosting the **virtual hard disk** (**VHDX**) files to allow Hyper-V to create differentiating disks (AVHDX's) during backup.The free space must be at least equal to the initial virtual disk size, multiplied by the expected churn rate (data changes), multiplied by the window backup time.
- If you want to protect generation 1 virtual machines running on Windows Server 2012 R2 Hyper-V host, then you should have at least one SCSI virtual controller attached, even if it's not connected to anything. This is due to the online backup enhancement introduced in Windows Server 2012 R2, because during backup, the Hyper-V host will mount a new VHDX in the VM and then dismount it when the backup is completed. Generation 2 virtual machines have SCSI controllers attached by default.
- The virtual machine must have its own **Volume Shadow Copy** (**VSS**) in a stable state. This is because the Hyper-V backup integration service inside of the virtual machine asks the guest instance of VSS to create a data-consistent VSS snapshot of the virtual machine. If the guest operating system is facing an internal VSS error, SCDPM will not able to provide a consistent data snapshot and will therefore throw an error.

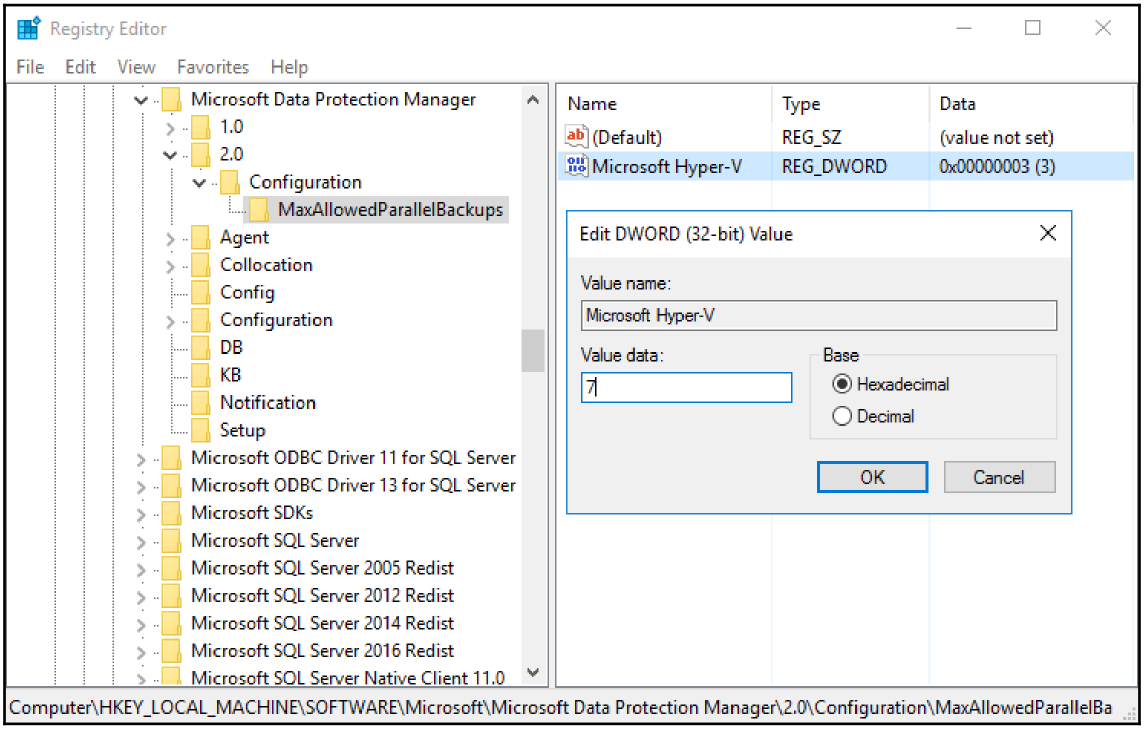
System Center Data Protection Manager 2016 or later can also protect Linux running as a virtual machine. Hyper-V must be running on Windows Server 2012 R2 or later. Please note that only file-consistent snapshots are supported for Linux workloads.

Backing up VMs with CSV storage

For virtual machines running on CSV storage, you need to take into consideration the following:

- You need to install the VSS hardware provider on the Hyper-V server. Therefore, you need to contact your **Storage Area Network** (**SAN**) vendor and ask for the VSS hardware provider.
- If, for any reason, a single node shuts down unexpectedly in a CSV cluster, DPM will perform a **Consistency Check** (**CC**) against the virtual machines that were running on that node.
- If you need to restart a Hyper-V server that has BitLocker Drive Encryption enabled on the CSV cluster, you must run a Consistency Check (CC) for Hyper-V virtual machines.

- With the introduction of **Cluster Shared Volumes** (**CSVs**) in version 2.0 in Windows Server 2012, System Center 2012 SP1 Data Protection Manager and later will be able to make backups both quicker and, more importantly, without the need to query the actual virtual machine for changes that have been made.
- By default, DPM will trigger three parallel backup jobs at a time on each node within a Hyper-V cluster. However, this per node number can be changed by changing the registry key of **Microsoft Hyper-V** located in the DPM server at `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft Data Protection Manager\2.0\Configuration\MaxAllowedParallelBackups`.


Registry Editor
File
Edit
View
Favorites
Help
Microsoft Data Protection Manager
1.0
2.0
Configuration
MaxAllowedParallelBackups
Agent
Collocation
Config
Configuration
DB
KB
Notification
Setup
Microsoft ODBC Driver 11 for SQL Server
Microsoft ODBC Driver 13 for SQL Server
Microsoft SDKs
Microsoft SQL Server
Microsoft SQL Server 2005 Redist
Microsoft SQL Server 2012 Redist
Microsoft SQL Server 2014 Redist
Microsoft SQL Server 2016 Redist
Microsoft SQL Server Native Client 11.0
Edit DWORD (32-bit) Value
OK
Cancel

Name	Type	Data
(Default)	REG_SZ	(value not set)
Microsoft Hyper-V	REG_DWORD	0x00000003 (3)

Value name: Microsoft Hyper-V

Value data: 7

Base: ● Hexadecimal ○ Decimal

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft Data Protection Manager\2.0\Configuration\MaxAllowedParallelBa

- The maximum number of jobs that DPM schedules at any given moment is dependent on the job type. The following is the maximum number of parallel jobs that DPM can trigger:
  - **Initial Replication (IR)**: 50
  - **Delta Replication (DR)**: 75
  - **Consistency Check (CC)**: 50

Please note that you must reboot your DPM server for the registry entry update to take effect.

Backing up VMs with SMB storage

For virtual machines running on **Server Message Block** (**SMB**) storage such as **Scale-out File Server** (**SOFS**) or **Storage Spaces Direct** (**S2D**) in disaggregated mode, you need to take into consideration the following:

- You need to turn on auto-mount on the server that is running Hyper-V to enable virtual machine protection. Type the following command from within the `diskpart` Command Prompt to do so:

  ```
  automount enable
  ```

- You need to disable TCP Chimney Offload. Run the following from a Command Prompt to do so:

  ```
  netsh int tcp set global chimney=disabled
  ```

- You need to ensure that all Hyper-V `machine$` accounts have full permissions for the specific remote SMB file shares.
- You'll need to enable the File Server VSS Agent service on each SMB server. To do that, open **Server Manager** and add it in **Add roles and features** | **Select server roles** | **File and Storage Services** | **File Services** | **File Service** | **File Server VSS Agent Service**.

DPM 2016 or later will fully understand and support Hyper-V clusters. When different virtual machines failover from one node in the cluster to another, DPM will seamlessly continue to protect the virtual machines.

Business continuity and disaster recovery (**BC/DR**) planning is an important part of a comprehensive protection strategy. In a large-scale deployment, it is important to provide a backup for the tenants in the most efficient and cost-effective way. Whether your cluster hosts a thousand or just a few hundred tenants, it's still very important to provide a backup solution that is provisioned within the concept of the newly deployed virtual machines or tenants. This also makes a cost-effective backup.

A key takeaway from backing up Hyper-V virtual machines is to exclude the page file that every guest operating system uses. The page file is not of great interest regarding a normal restore scenario. You must move the page file of every virtual machine to a dedicated volume, and after that, you can enable the exclusion of the page file data churn by running the `Set-DPMGlobalProperty PowerShell` cmdlet. It is important that you have a standard naming convention for the page file exclusion disks, since you must work with a standardized concept while hosting the virtual machines. You can use the following command to enable page file exclusion on every DPM server that provides restore capabilities to the Hyper-V environments:

```
Set-DPMGlobalProperty -DPMServerName "DPMServer" -HyperVPagefileExclusions
"*_pagefile.vhdx"
```

The `Set-DPMGlobalProperty` cmdlet will exclude all VHDX files that have `_pagefile.vhdx` in their name.

There's more...

It's advisable that you protect your Hyper-V environment by combining host-level backup of Hyper-V VMs with the existing backup strategy for in-guest applications, such as SQL Server, Exchange Server, and SharePoint. Virtual machines backup is equivalent to protecting a physical server using bare-metal protection. It is recommended that you protect your application data more frequently than your virtual machines. For example, virtual machines can have a schedule that backs up data once per day or once per week, while SQL Server databases could be backed up as frequently as every 15 minutes.

See also

- For more information regarding supported versions of Microsoft Hyper-V, please read the following article: `http://technet.microsoft.com/en-us/library/jj860400.aspx`
- For more information about the history of Hyper-V backup and the new improvements introduced in Windows Server 2016, please read the following article: `https://github.com/MicrosoftDocs/Virtualization-Documentation/blob/master/prospective-docs/Hyper-V-Backup-2016.md`

Understanding Hyper-V management tasks

Understanding how to manage a highly available Hyper-V environment will impact the protection provided by System Center 2016 Data Protection Manager. The most common management tasks for a Hyper-V environment with DPM are as follows:

- Changing the name of a protected virtual machine
- Removing a protected VM from a Hyper-V cluster
- Adding nodes to a Hyper-V cluster
- Removing nodes from a Hyper-V cluster

In the scenario where you need to change a virtual machine's name, you cannot do so without causing interruption to the DPM protection, since System Center Data Protection Manager uses the VM name as a unique identifier. To be able to protect the virtual machine under its new name, you need to first stop the protection and choose to retain the data. Then, you need to enable the protection again by adding the virtual machine under its new name to a protection group.

In a scenario where you need to remove and delete a protected virtual machine from a cluster, DPM raises an alert stating that recovery point creation failed. However, all the existing recovery points will remain intact until the retained data retention range has expired.

When you add a new Hyper-V node to an existing cluster that's protected by DPM, System Center Data Protection Manager raises an alert saying that there is a new node member of a cluster that needs to have the DPM agent installed.

If you remove a Hyper-V cluster node, DPM raises an alert stating that the server is no longer a member of the cluster.

All management tasks should be planned and well-communicated with various departments in your organization. A lack of communication and providing important information to other stakeholders can have a devastating effect on your business.

Understanding the basics of tape backups

This recipe will cover the basics of tape usage backup with DPM.

System Center Data Protection Manager protects data by making the data source an explicit member of a **protection group**. A protection group can be seen as a backup job that can be configured with specific options that are related to the type of workload that you are protecting.

Tapes are usually used for long-term protection of data, which is protected by DPM, so that data from protected resources is backed up to disk in the short-term and then to tape. You can also select to use tape for short-term protection so that data from protected resources is backed up directly to tape.

Consider the following points on when to use long-term protection and short-term protection:

For long-term protection to tape:

- Any workload can be backed up to tape for long-term protection
- Full backups are always run when using long-term protection to tape
- Long-term protection for tape allocates a tape for each full backup job, so that each long-term backup recovery point is always on a new tape
- If you're using tape for both long-term and short-term protection, DPM creates copies of the latest short-term full backup in order to generate the long-term tape backup
- If you're using disk for short-term backup and tape for long-term, the long-term backup will be taken from the replica disk

> Microsoft recommends that you schedule the short-term protection backup to run a day before the long-term backup. That way, you can be sure that you are using the latest short-term backup in order to create the long-term backup.

For short-term protection to tape:

- DPM doesn't support short-term backup to tape for application data or client computers. Only file data (volumes, shares, and folders) and VMs can be configured for short-term protection to tape.
- You can use a full backup or a full/incremental backup when backups are set to **Daily**.

- If short-term backups are configured to use tape and the full backup option is used, then each full backup job will require a new free tape.
- If you don't have a standalone tape or tape library attached to the DPM server, you will only be able to select **Disk** for short-term protection.

Understanding the concept of the Virtual Tape Library

A **Virtual Tape Library** (**VTL**) simulates a media changer and a number of tape drives. Instead of using physical tapes, the VTL software or hardware writes the backed up data to individual files that represent a tape. Different vendors use different file setups and extensions.

The advantage of using VTL versus an actual tape is that you can gain granularity of the tape while benefiting from the speed of disk-based backup and restore. This also enables you to customize your storage for the VTL software or hardware. You can either choose to have a lot of storage but lack the speed, or the opposite.

A VTL solution is installed and configured the same way as a physical tape library, and from a DPM perspective, you can manage it the same way regarding its short-term and long-term retention policy.

There's more...

There are four vendors that you should consider choosing from if you are implementing a VTL solution with DPM:

- **StarWind Virtual Tape Library**: `https://www.starwindsoftware.com/starwind-virtual-tape-library`
- **Firestreamer Virtual Tape Library**: `https://www.cristalink.com/fs/`
- **DELL EMC Data Domain Virtual Tape Library**: `https://www.emc.com/data-protection/data-domain/data-domain-virtual-tape-library.htm`
- **HPE StoreOnce Data Protection**: `https://www.hpe.com/us/en/storage/storeonce.html`

For the remainder of this chapter, we will leverage StarWind VTL.

See also

For more information about how to integrate StarWind VTL with Microsoft System Center 2016 Data Protection Manager, please check the following article: `https://www.starwindsoftware.com/blog/starwind-virtual-tape-library-vtl-with-microsoft-system-center-data-protection-manager`.

Moving the DPM server to a new domain or renaming a DPM server

When you deploy Microsoft System Center's **Data Protection Manager** (**DPM**), you should take care to ensure that there is not a requirement further down the road to move the DPM server to a new Active Directory domain, or that this isn't a requirement to have to rename the DPM server.

How to do it...

Neither moving nor renaming a DPM server are supported by Microsoft, and there is no workaround for this.

See also

Please check the following link to learn more about the common support information that you might need when deploying and maintaining System Center Data Protection Manager:

- `https://docs.microsoft.com/en-us/system-center/dpm/dpm-support-issues`