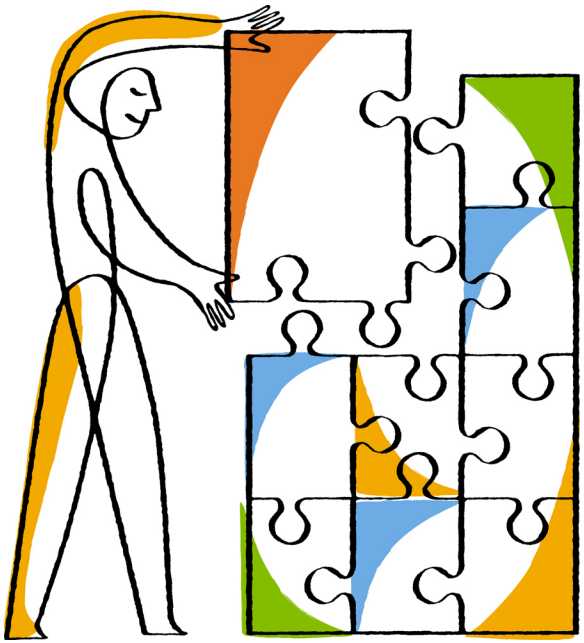
Draft for beta release -- October 2014

SnapManager® 2.1 for Hyper-V®

Installation and Administration Guide



NetApp, Inc.
495 East Java Drive
Sunnyvale, CA 94089
U.S.

Telephone: +1 (408) 822-6000
Fax: +1 (408) 822-4501
Support telephone: +1 (888) 463-8277
Web: www.netapp.com
Feedback: doccomments@netapp.com

Part number: 215-08967_A0
November 2014

Content subject to change

Draft for beta release -- October 2014

Contents

What SnapManager for Hyper-V is 7
What you can do with SnapManager for Hyper-V 7
List of SnapManager for Hyper-V limitations 8
Data management concepts 9
List of requirements for installing SnapManager for Hyper-V 12
SnapManager for Hyper-V licensing for Data ONTAP 13
Hyper-V parent host requirements 13
Hotfix requirements for Windows Server environments 14
License requirements 14
Requirements for using the Remote Host Install wizard 15
Installing SnapManager for Hyper-V 17
Downloading SnapManager for Hyper-V 17
Installation order for SnapDrive for Windows and SnapManager for Hyper-V 18
Installing SnapManager for Hyper-V 18
Remotely installing or uninstalling SnapManager for Hyper-V on nodes or hosts 19
List and description of command line switches for silent installation 19
Uninstalling SnapManager for Hyper-V on Windows 22
Uninstalling SnapManager for Hyper-V 22
Configuring SnapManager for Hyper-V 23
Dashboard settings 23
Configuring hosts 24
Requirements for adding a Hyper-V parent host or host cluster 24
Adding a Hyper-V parent host or host cluster 26
Managing storage connection settings 26
Viewing a Hyper-V parent host or host cluster 27
Viewing a virtual machine 27
Migrating a Hyper-V virtual machine for SnapManager for Hyper-V operations 27
Importing or exporting host and dataset configuration information 31
Removing a Hyper-V parent host or parent host cluster 32
Event notification settings 32

Content subject to change

Draft for beta release -- October 2014

Report path settings 32
Configuring SnapInfo directory settings 33
Setting up a SnapInfo LUN 33
Changing the SnapInfo directory path 34
Configuring datasets 35
Requirements for creating a dataset 35
Creating a dataset 36
Modifying a dataset 37
Viewing a dataset 37
Deleting a dataset 37
Configuring policies 38
Requirements for adding policies to a dataset 38
Adding policies 41
Modifying policies 41
Viewing policies 42
Deleting policies 42
Managing reports 43
Viewing a dataset report 43
Viewing a host report 44
Deleting a report 44
Understanding VSS components 45
CSV 2.0 in Windows Server 2012 45
SMB 3.0 support for Hyper-V VMs in Windows Server 2012 46
How SnapManager for Hyper-V uses VSS 47
Data ONTAP VSS Hardware Provider requirement 47
Viewing installed VSS providers 47
Verifying that the VSS Hardware Provider was used successfully 48
Creating and managing backup jobs in SnapManager for Hyper-V 49
Requirements for manually backing up a dataset 50
How SnapManager for Hyper-V handles saved-state backups 52
Manually backing up a dataset 52
Monitoring backup jobs 53
Deleting a backup 53
Restoring a virtual machine 55
Requirements for restoring a virtual machine 55
Restoring a virtual machine from a backup copy 57

Content subject to change

Draft for beta release -- October 2014

Performing disaster recovery 59
Configuring SnapManager for Hyper-V for failover 59
Recovering and restoring from a disaster recovery failover 60
Reconfiguring storage systems after a disaster recovery failback 63
Restoring the original configuration for standalone hosts 66
Restoring the original configuration for clustered hosts 67
Troubleshooting SnapManager for Hyper-V 68
Warning: Current VHD configuration of the VM is different from that at the time of backup 68
VM could not be realized due to errors in its configuration file which could not be resolved 68
Backup Failed for the following VM(s) since it cannot be backedup online or No VM to be found for backup 69
Unexpected error querying for the IVssWriterCallback interface. hr = 0x80070005, Access is denied. 69
Backup reports use management console time zone information in report name 69
Backup and restore notifications not sent in IPv6-only environments 70
Failover clustering event ID 5121 70
Virtual machine backups made while a restore operation is in progress might be invalid 70
Virtual machine managing itself 71
Connection time is longer with IPv6-only host 71
Volume Shadow Copy Service error: An internal inconsistency was detected 72
Web Service Client channel was unable to connect to the ConfigurationManagementService instance on machine smhv51_81clus 72
MSI custom property used in silent installation 73
SnapManager for Hyper-V is not licensed on the host or in the Storage System 73
Deleting backups after failover 74
Storage performance degrades after failed backup 74
Deleted SnapInfo Snapshot copies 74
High memory consumption caused by antivirus solution 75
Space consumption when making two Snapshot copies for each backup 75
SnapDrive SDDiscoveryFileSystemListInfo response is null while backing up 76
Error: Vss Requestor - Backup components failed 77
Vss Requestor - Backup Components failed. An expected disk did not arrive in the system 77

Content subject to change

Draft for beta release -- October 2014

Vss Requestor - Backup Components failed with partial writer error 78
VSS returns errors against Microsoft iSCSI Target VSS Hardware Provider during NAS backup 80
Vss Requestor - Backup Components failed. Failed to call keep snapshot set. 80
MBR LUNs unsupported in SnapManager for Hyper-V 81
Backup fails after you remove a virtual machine from Hyper-V Manager 81
Some types of backup failures do not result in partial backup failure 82
Restore failure after storage system volume renaming 82
Restoring from a backup after failback 83
Web Service Client channel unable to connect while updating the dataset to the new node 83
Datasets are not automatically replicated to new nodes in a Windows Failover Cluster 84
Error 1935. An error occurred during the installation of assembly component 84
Backup jobs that involve more than 15 CSVs from the same storage system might fail 85
Either the specified VM(s) are not present or they cannot be backed up online 85
Required hotfix KB2263829 cannot be installed on some platforms 86
Backup failure with the error “Shadow copy creation is already in progress” 87

Copyright information 88
Trademark information 89
How to send your comments 90
Index 91

Content subject to change

What SnapManager for Hyper-V is

SnapManager for Hyper-V provides you with a solution for data protection and recovery for Microsoft Hyper-V virtual machines (VMs) residing on storage systems running Data ONTAP.

You can perform application-consistent and crash-consistent dataset backups according to dataset protection policies set by your backup administrator. You can also restore VMs from these backups. Reporting features enable you to monitor the status of the backups and get detailed information about your backup and restore jobs.

What you can do with SnapManager for Hyper-V

SnapManager for Hyper-V enables you to back up and restore multiple virtual machines across multiple hosts. You can create datasets and apply policies to them to automate backup tasks such as scheduling, retention, and replication.

You can perform the following tasks with SnapManager for Hyper-V:

- Group virtual machines into datasets that have the same protection requirements and apply policies to those datasets
- Back up and restore dedicated and clustered virtual machines residing on storage systems running Data ONTAP software
- Back up and restore virtual machines hosted on Cluster Shared Volumes (CSVs)
- Automate dataset backups using scheduling policies
- Perform on-demand backups of datasets
- Retain dataset backups for as long as you need them, using retention policies
- Update the SnapMirror destination location after a backup successfully finishes
- Specify custom scripts to run before or after a backup
- Restore virtual machines from backups
- Monitor the status of all scheduled and running jobs
- Manage hosts remotely from a management console
- Provide consolidated reports for dataset backup, restore, and configuration operations
- Perform a combination of crash-consistent and application-consistent backups
- Perform disaster recovery operations using PowerShell cmdlets

Draft for beta release -- October 2014

List of SnapManager for Hyper-V limitations

It is important that you understand that some features are not supported in SnapManager 2.1 for Hyper-V.

- Canceling, suspending, and resuming backup and restore jobs is not supported.
- Policies cannot be copied across datasets.
- Role-based access control (RBAC) is not supported.
- Excluding virtual hard disks (VHDs) from a SnapManager for Hyper-V Volume Shadow Copy Service (VSS) backup job is not supported.
- Single file restore from a backup copy is not natively supported.
- Cross-version management is not supported; for example, you cannot use Client Console 1.2 to manage SnapManager 2.0 for Hyper-V, and vice versa.
- If you start to restore a Hyper-V virtual machine (VM), and another backup or restoration of the same VM is in process, your attempt fails.
- Restoring a deleted VM from a crash-consistent backup copy is supported only for Windows Server 2012.
- Running different versions of SnapManager for Hyper-V on different nodes of a failover cluster is not supported.
- Reverting from SnapManager 2.0 for Hyper-V is not supported.
- Backup or restore jobs of virtual machines are not supported when users change the cluster ownership node while backing up or restoring.
- Mixed-mode backups (of virtual machines containing files on CSV 2.0 volumes and SMB shares) are not supported.
- After you migrate the storage of a VM to another location using Windows Server 2012, you cannot restore on that VM from backup copies made before the migration.
- For Windows Server 2012, you cannot perform a backup job where the backup set includes both a Cluster Shared Volume (CSV) and a shared disk.
- When configuring Manage Storage Connection Settings, you cannot use Remote Procedure Call (RPC) protocol; you can use only HTTP and HTTPS protocols.
- Making an application-consistent backup of a virtual machine (VM) that is stored on NAS storage is not supported by Microsoft Hyper-V Server 2012.
  This limitation does not apply to crash-consistent backups. It only applies to the free Hyper-V server, which does not include file share shadow copy services.

Content subject to change

Draft for beta release -- October 2014

- The virtual switch name for a VM must be exactly the same for the primary and secondary Windows hosts.
- Backup and restore operations require a FlexClone license when Hyper-V VMs are deployed over SMB 3.0.
- The maximum supported LUN size for restore operations is 14 TB.

Related information

Microsoft Download Center: Window Server 2012 Products and Editions Comparison

Data management concepts

SnapManager for Hyper-V uses datasets and policies, which enables you to group virtual machines and then apply rules to these groups to govern their behavior. This information is useful in scenarios in which you are using SnapManager for Hyper-V to schedule a backup and to specify a retention policy for the backup.

datasets

A dataset is a group of virtual machines (VMs) that enables you to protect data using retention, scheduling, and replication policies. You can use datasets to group virtual machines that have the same protection requirements. A VM can be part of multiple datasets.

Hyper-V parent hosts

Hyper-V parent hosts are physical servers on which the Hyper-V role is enabled. Hosts that contain virtual machines are added to SnapManager for Hyper-V for protection and recovery. SnapManager for Hyper-V must be installed and running on each Hyper-V parent host.

unprotected resources

Unprotected resources are virtual machines that are not part of any dataset. You can protect these resources by adding them to a dataset.

virtual machines

A virtual machine run on a Hyper-V parent host is a representation of a physical machine, with its own operating system, applications, and hardware.

SnapManager for Hyper-V tracks the globally unique identifier, or GUID, of the virtual machine and not the virtual machine name. If you delete a virtual machine that is protected by SnapManager for Hyper-V, and then create a different virtual machine with the same name, the new virtual machine is not protected, because it has a different GUID.

management consoles

Content subject to change

Draft for beta release -- October 2014

Management consoles are computers on which SnapManager for Hyper-V is installed and running as a client. You can use management consoles to remotely manage SnapManager for Hyper-V operations on a remote Hyper-V parent host.

scheduling policies

Scheduling policies assign backup jobs for particular times, enabling you to automate the scheduling process. You can add multiple scheduling policies, which apply to all virtual machines that are dataset members. SnapManager for Hyper-V uses Windows Scheduler to create scheduled tasks.

retention policies

A retention policy is the way you manage dataset backup retention in SnapManager for Hyper-V. Retention policies determine how long to keep a dataset backup, based on either time or number of backup copies.

The limits that you set in a retention policy ensure that your data backup does not compromise future storage capacity.

You can set the following retention periods in SnapManager for Hyper-V:

- One hour
- One day
- One week
- One month
- Unlimited

Note: You can specify a retention period once per dataset.

After choosing how often dataset backups are deleted, you can choose to delete either backups that are older than a specified period of time or backups that exceed a maximum total.

If your system appears to retain old backups, check your retention policies. All objects being backed up that share a Snapshot copy must meet the backup deletion criteria in order for the retention policy to trigger the removal of a Snapshot copy.

replication policies

A replication policy determines whether the SnapMirror destination is updated after a successful backup operation. SnapManager for Hyper-V supports volume-based SnapMirror only. You must configure a SnapMirror relationship on the two storage systems before you attempt to perform a SnapMirror update. This is required for both the source and destination.

Related information

Data ONTAP 8.2 Data Protection Online Backup and Recovery Guide for 7-Mode

Content subject to change

Draft for beta release -- October 2014

NetApp Documentation: SnapDrive for Windows (current releases)

Content subject to change

Draft for beta release -- October 2014

List of requirements for installing SnapManager for Hyper-V

Your environment must meet all hardware, software, Data ONTAP, and licensing requirements before you can install SnapManager for Hyper-V. The installer stops if the requirements for the minimum Windows operating system and .Net 4.5 are not met.

Hyper-V parent host requirements

You must have the Hyper-V parent hosts running Windows Server 2008 R2 or higher. You must have the Hyper-V roles enabled on the parent hosts. You must have SnapDrive 7.1 for Windows or later installed on the Hyper-V parent host.

SnapManager for Hyper-V download

You must have downloaded the SnapManager for Hyper-V software from the NetApp Support Site.

Storage system requirements

The storage system must run the appropriate version of the Data ONTAP software. You can use either host-based or storage system licensing to install SnapManager for Hyper-V.

Licenses

You must have the appropriate licenses to run SnapManager for Hyper-V.

Credentials

You must have the appropriate credentials to install and run SnapManager for Hyper-V.

Service account and authentication requirements

You must have a service account and must meet the authentication requirements. You must be able to log in to the host using the service account, and that account must have administrative rights.

Web service port number

You must have the Web service Net.Tcp port number available. The default port number is 808. When installing SnapManager for Hyper-V on a cluster, you must make sure that the same port number is used across all nodes.

Content subject to change

Draft for beta release -- October 2014

SnapManager for Hyper-V licensing for Data ONTAP

SnapManager for Hyper-V licensing depends on the version of Data ONTAP that you use.

For host-based licensing and storage-based licensing, you must use Data ONTAP 8.0 or later.

You must use Data ONTAP 8.2 or later of MultiStore (vFiler unit) for use with SnapManager for Hyper-V.

If using a version of Data ONTAP prior to 8.2, there are some restrictions on certain operations.

Related information

NetApp Interoperability Matrix Tool
NetApp Documentation: SnapDrive for Windows (current releases)

Hyper-V parent host requirements

Hyper-V parent hosts are physical servers on which the Hyper-V role is enabled. Host servers that contain virtual machines are added to SnapManager for Hyper-V for protection and recovery. To install and run all of the SnapManager for Hyper-V software components, you must ensure that the Hyper-V parent hosts meet minimum operating system and Hyper-V requirements.

Supported operating systems

SnapManager for Hyper-V runs on the following operating systems:

- Windows Server 2008 R2 SP1
- Windows Server 2012 R2
- Windows Server 2012

Supported management console operating systems

Management consoles must be running the following operating systems:

- Windows Server 2008 R2 SP1
- Windows Server 2012 R2
- Windows Server 2012

Hyper-V requirements

For more information, see the Hyper-V getting started information in the Microsoft TechNet library.

Internationalization support

Content subject to change

Draft for beta release -- October 2014

SnapManager for Hyper-V has been tested on German-language and Japanese-language operating systems.

Related information

Microsoft TechNet: Hyper-V
NetApp Interoperability Matrix Tool

Hotfix requirements for Windows Server environments

You must manually install hotfixes to Microsoft Windows Server operating system environments.

For Windows Server 2012, the following hotfixes are required:

- *KB2770917*
- *KB2779768*

For Windows Server 2008 R2, the following hotfixes are required:

- *KB977096*
- *KB974909*
- *KB975354*
- *KB2637197*

For Windows Server 2008 R2 SP1, the following hotfixes are required:

- *KB2263829*
- *KB2494016*
- *KB2637197*

These are the minimum patch levels.

See the *SnapManager 2.1 for Hyper-V Release Notes* for the latest Microsoft-recommended hotfixes.

License requirements

To run SnapManager for Hyper-V, you must select either host-based or storage system licenses during the installation of the licenses.

SnapManager suite license

A SnapManager suite license is required on the Windows host system. You can choose either host-based licensing or storage system licensing.

Content subject to change

Draft for beta release -- October 2014

Per server license

This is also known as *host-based licensing*. If you select host-based licensing, you must provide a SnapManager suite license key during installation, which you can change later if you need to. You can change the license key after installation by clicking **License settings** in the SnapManager for Hyper-V Welcome window. Each parent host requires a SnapManager suite license.

Per storage system license

This is also known as *storage system licensing*. If you select storage system licensing, you must add the SnapManager suite license to all storage systems to run the SnapManager for Hyper-V operations.

Per client system license

You should use this licensing option when you are installing the management console.

Requirements for using the Remote Host Install wizard

Before using the Remote Host Install wizard to remotely install SnapManager for Hyper-V on a host or node, you must gather some required host details.

You can access the Remote Host Install wizard from the Actions pane in the Protection window. It enables you to remotely install or uninstall SnapManager for Hyper-V on standalone and cluster nodes or hosts.

If you add a host that does not have SnapManager for Hyper-V, the Add Host wizard prompts you to install it on the host.

Install or Uninstall

You must choose whether to use the wizard to remotely install or uninstall SnapManager for Hyper-V on hosts or nodes.

Per Server or Per Storage

You must choose whether to install SnapManager for Hyper-V on a per-server or a per-storage basis.

Host Name/IP

You must provide the name or IP address of the host on which you want to install SnapManager for Hyper-V. You can select **Browse...** to browse for the host or node.

Port

You must provide the port number to connect to the host or node.

SMHV License Key

You must provide the SnapManager for Hyper-V license key.

SDW License Key

Content subject to change

Draft for beta release -- October 2014

You must provide the SnapDrive for Windows license key.

User Name

You must provide the host or node administrator-level user name using the format *domain* *username*.

Password

You must enter the host or node password.

Confirm Password

You must reenter the host or node password for confirmation.

Content subject to change

Installing SnapManager for Hyper-V

Before you install SnapManager for Hyper-V, it is a good practice to decide how you want to configure your environment, which includes the installation of SnapDrive for Windows on all Hyper-V hosts prior to the installation of SnapManager for Hyper-V.

Downloading SnapManager for Hyper-V

Before installing SnapManager for Hyper-V, you must download the software package from the NetApp Support Site.

Before you begin

You must have login credentials for the NetApp Support Site.

Steps

1. Log in to the NetApp Support Site.
2. Go to the Download Software page.
3. From the drop-down list, select the operating system on which you are installing SnapManager for Hyper-V and click **Go!**.
4. Click **View & Download** for the software version you want to install.
5. On the Description page, click **Continue**.
6. Review and accept the license agreement.
7. On the Download page, click the link for the installation file.
8. Save the SnapManager for Hyper-V file to a local or network directory.
9. Click **Save File**.
10. Verify the checksum to ensure that the software downloaded correctly.

Related information

NetApp Support

Draft for beta release -- October 2014

Installation order for SnapDrive for Windows and SnapManager for Hyper-V

You must install SnapDrive for Windows on all hosts before installing SnapManager for Hyper-V. If the hosts are members of a cluster, all nodes in the cluster require the installation of SnapDrive for Windows.

When SnapManager for Hyper-V starts, it communicates with SnapDrive for Windows to get the list of all virtual machines running on a host. If SnapDrive for Windows is not installed on the host, this API fails and the SnapManager for Hyper-V internal cache does not update with the virtual machine information.

You might receive the following message: `Error :SnapManager for Hyper-V is not licensed on the host or in the Storage System, backup is aborted:.`

Installing SnapManager for Hyper-V

You can install SnapManager for Hyper-V so that you are able to back up and restore your data. You should install SnapDrive for Windows before installing SnapManager for Hyper-V.

Before you begin

Your existing data must be backed up, and you must have the following information ready:

- License key
- Login credentials
- Port number (default: 808; must match the SnapDrive for Windows installation port number)

Steps

1. Double-click the SnapManager for Hyper-V executable file to launch the SnapManager for Hyper-V installer.
2. Select the installation location and click **Next**.
3. Complete the steps in the SnapManager for Hyper-V **InstallShield** wizard.
4. Click **Install** on the **Ready to Install** page.
5. Review the summary of your selections and click **Finish**.

Related references

Hotfix requirements for Windows Server environments on page 14

Content subject to change

Draft for beta release -- October 2014

Remotely installing or uninstalling SnapManager for Hyper-V on nodes or hosts

The Remote Host Install wizard enables you to remotely install or uninstall SnapManager for Hyper-V on standalone and cluster hosts or nodes. You can remotely install SnapManager for Hyper-V if you want to install the software on all nodes of a cluster at one time instead of installing it on each individual node.

Before you begin

You must already have SnapManager for Hyper-V installed on a host node to use the Remote Host Install wizard.

Steps

1. From the navigation pane, click **Protection**.
2. From the **Actions** pane, click **Remote Host Install**.
3. Run the **Remote Host Install** wizard.

Result

When you run the Remote Host Install wizard, the host node pushes SnapManager for Hyper-V installation or uninstallation to other nodes or hosts in the cluster.

List and description of command line switches for silent installation

You can use command line switches to perform a silent installation, which enables you to use an installation script to install SnapManager for Hyper-V.

The following table provides a list of values and describes each of the available command-line installation switches.

Switch	Value	Description
SILENT_MODE=	1	Enables SnapManager for Hyper-V to properly execute the unattended install feature. This switch is required for first-time installations, upgrades, and complete uninstallations.

Content subject to change

Draft for beta release -- October 2014

Switch	Value	Description
REINSTALLMODE=		Specifies the reinstall mode to be used.
REINSTALLMODE=	v	Indicates that the installation is run from the source package and that the local package is cached. Do not use this option for first-time installations of SnapManager for Hyper-V. Reinstalls all files regardless of version, date, or checksum value.
REINSTALLMODE=	a	Reinstalls SnapManager for Hyper-V files if older versions are present or if files are missing.
REINSTALLMODE=	o	Indicates that all SnapManager for Hyper-V required registry entries from HKEY_LOCAL_MACHINE and HKEY_CLASSES_ROOT should be rewritten.
REINSTALLMODE=	m	Indicates that all SnapManager for Hyper-V required registry entries from HKEY_CURRENT_USER and HKEY_USERS should be rewritten.
REINSTALLMODE=	u	Reinstalls all shortcuts and recaches all icons, overwriting any existing shortcuts and icons.
REINSTALL=	ALL	Reinstalls all SnapManager for Hyper-V features.
/Li	filename	Specifies that a SnapDrive installation log should be generated.
SMHV_LICENSE=	license	Specifies the appropriate and valid SnapManager for Hyper-V license.
INSTALLDIR=	target installation directory	Specifies the target installation directory to which SnapManager for Hyper-V is installed. This switch is required only when installing SnapManager for Hyper-V for the first time.
SVCUSERNAME=	DOMAIN \username	Specifies the domain and user name that SnapManager for Hyper-V uses during the unattended installation.

Content subject to change

Draft for beta release -- October 2014

Switch	Value	Description
SMHVSRV_PASSWORD=	password	Specifies the password for the SMHVSRV_PASSWORD user.
SMHVSRV_CONFIRMUSERPASSWORD=	password	Confirms the password for the SMHVSRV_CONFIRMUSERPASSWORD user.
SMHV_WEBSRV_TCP_PORT	port number	Specifies which port the SnapManager for Hyper-V web service uses for Net.Tcp. The default port is 808.

The following syntax shows a fresh installation:

```
setup.exe /s /v"/qn SILENT_MODE=1 /L*v SMHVInstall.log
SVCUSERNAME=Domain\User Name SMHVSRV_PASSWORD=password
SMHVSRV_CONFIRMUSERPASSWORD=password"
```

The following syntax shows an upgrade:

```
setup.exe /s /v"/qn REINSTALLMODE=vamus REINSTALL=ALL
SILENT_MODE=1 /L*v SMHVUpgrade.log SVCUSERNAME=Domain\User Name
SMHVSRV_PASSWORD=password SMHVSRV_CONFIRMUSERPASSWORD=password"
```

The following syntax shows an uninstallation:

```
Setup.exe /s /x /v"/qn SILENT_MODE=1 /L*v SMHVuninstall.log"
```

Content subject to change

Draft for beta release -- October 2014

Uninstalling SnapManager for Hyper-V on Windows

You can uninstall SnapManager for Hyper-V from the Windows host when you no longer need the software. You must run the uninstallation program interactively.

Uninstalling SnapManager for Hyper-V

You can uninstall SnapManager for Hyper-V from the Windows server using the Control Panel uninstall application for your operating system. You can remotely uninstall SnapManager for Hyper-V on standalone and cluster nodes or hosts using the Remote Host Install wizard from the Actions pane in the Protection window.

About this task

Uninstalling SnapManager for Hyper-V deletes all datasets and policies. You cannot recover that information after the uninstallation is complete. If you want to save your datasets and host configuration information, you can export them before you uninstall.

Steps

1. On the Windows server where you installed SnapManager for Hyper-V, navigate to the Control Panel and select **Control Panel > Programs > Programs and Features**.
2. Scroll through the list of installed programs to find SnapManager for Hyper-V.
3. Click the name of the program and then click **Uninstall**.
4. When prompted to confirm uninstallation, click **Yes**.

Related tasks

Importing or exporting host and dataset configuration information on page 31

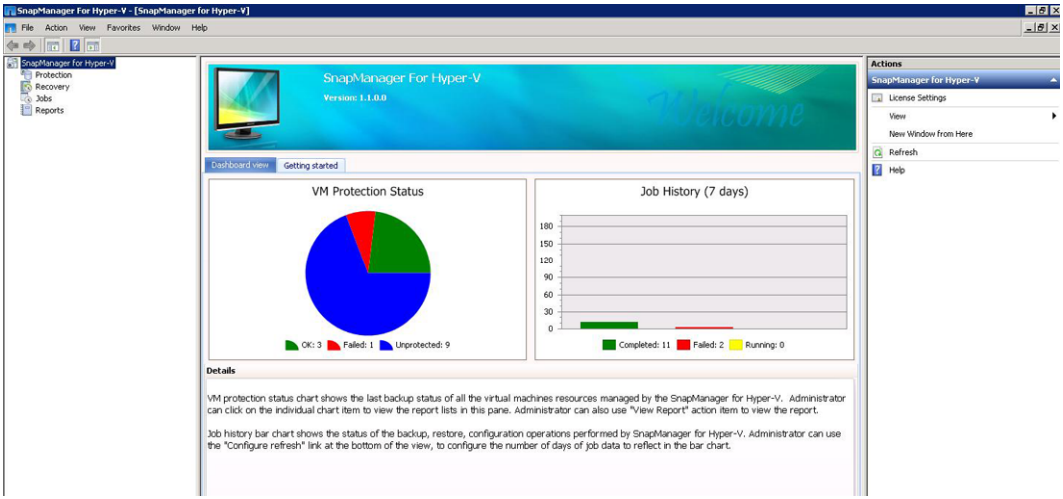
Content subject to change

Configuring SnapManager for Hyper-V

After you install SnapManager for Hyper-V, you can configure and manage your hosts and virtual machines by adding policies to protect and restore your data.

Dashboard settings

The SnapManager for Hyper-V dashboard displays an overview of resources that are currently being protected, as well as those that are not protected. You can select different segments of either the VM Protection Status pie chart or the Job History bar graph to view general information about the status of your jobs, resources, and history.



VM protection status

When you select a segment in the VM Protection Status pie chart, you can view information about the protection status of the virtual machines in the Details pane. The descriptions for valid values are as follows:

OK

Displays the most recent successful backup of all virtual machines.

Failed

Displays the most recent failed backup of each virtual machine.

Unprotected

Displays the virtual machines that do not belong to any datasets and are therefore unprotected.

Job history

Draft for beta release -- October 2014

When you select a segment in the Job History bar graph, you can view, in the Details pane, the history of completed, failed, and running jobs over a specified period of time. You can change the length of time that job details are displayed in the Job History bar graph. The default value is seven days.

Configure refresh

You can change how often the dashboard refreshes the displayed information by using the **Configure refresh** button. The default value is 10 minutes.

Configuring hosts

You can add, view, and remove Hyper-V parent hosts or clusters by using SnapManager for Hyper-V.

Requirements for adding a Hyper-V parent host or host cluster

You must have all necessary configuration information available before adding a parent host or host cluster to SnapManager for Hyper-V.

SnapManager for Hyper-V installation

SnapManager for Hyper-V must be installed on the Hyper-V host that you want to add.

If you do not have SnapManager for Hyper-V installed, you are prompted to run the Remote Host Install wizard. The same SnapManager for Hyper-V version must be installed on each cluster node.

Configuration settings

The Hyper-V parent host that you want to add must be configured for SnapManager for Hyper-V.

If the SnapInfo settings, report directory settings, and notification settings are not configured for SnapManager for Hyper-V, you can configure them after you add the host, using the Configuration wizard.

You must configure the backup repository and report directory settings to add and manage virtual machines by using SnapManager for Hyper-V. Notification settings are optional.

Virtual machines and Data ONTAP LUNs

All of the files associated with the virtual machines, including configuration files, Snapshot copy file location, and VHDs, must reside on Data ONTAP LUNs.

This is necessary to perform a successful backup.

Note: If you change a virtual machine Snapshot file location to a different Data ONTAP LUN after creating the virtual machine, you should create at least one virtual machine Snapshot copy using Hyper-V Manager before making a backup by using SnapManager for Hyper-V. If you

Content subject to change

Draft for beta release -- October 2014

change the Snapshot copy file location and do not make a virtual machine Snapshot copy before making a backup, the backup operation could fail.

Dedicated and clustered virtual machines

Your virtual machines can be dedicated or part of a cluster.

If you add a single host, SnapManager for Hyper-V manages the dedicated virtual machines on that host. If you add a host cluster, SnapManager for Hyper-V manages the shared virtual machines on the host cluster. Virtual machines residing on SAN and NAS that belong to the same host cluster should not exist in the same dataset. Adding these types of resources to a single dataset can cause the dataset backup to fail.

For application-consistent backups, dataset backups of clustered virtual machines take longer to complete when the virtual machines run on different nodes of the cluster. When virtual machines run on different nodes, separate backup operations are required for each node in the cluster. If all virtual machines run on the same node, only one backup operation is required, resulting in a faster backup.

Number of virtual machines

If your Hyper-V host or host cluster has more than 1000 virtual machines, you must increase the value of the `maximumElementsInCacheBeforeScavenging` property in SnapMgrServiceHost.exe.config file for Hyper-V Cache Manager. This value should be greater than or equal to the number of Hyper-V hosts running on a standalone host or cluster. The value should be changed on each node of the cluster. Restart SnapManager for Hyper-V service after changing this value. You must manually edit the SnapMgrServiceHost.exe.config file using a text editor.

```
<cacheManagers>
…
      <add name="HyperV Cache Manager"

type="Microsoft.Practices.EnterpriseLibrary.Caching.CacheManager,
                           Microsoft.Practices.EnterpriseLibrary.Caching"
                        expirationPollFrequencyInSeconds="60"
                        maximumElementsInCacheBeforeScavenging="1200"
                        numberToRemoveWhenScavenging="10"
                        backingStoreName="inMemory" />
…
</cacheManagers>
```

SnapManager for Hyper-V service account requirements

When using SnapManager for Hyper-V to manage a Hyper-V host cluster, the SnapManager for Hyper-V and SnapDrive for Windows service accounts must be domain user accounts with local administrator rights on the server.

SnapManager for Hyper-V application-consistent backups run on the cluster node where the virtual machine is running. If Cluster Shared Volumes (CSVs) used by the virtual machine are not owned by the same node, virtual machine backups can fail when the SnapManager for Hyper-V service is using

Content subject to change

Draft for beta release -- October 2014

a local system account (even though the account has administrator privileges). In this case, SnapManager for Hyper-V cannot detect that the virtual machine files are residing on a CSV, causing the backup to fail.

Note: To ensure that remote Volume Shadow Copy Service (VSS) operations with virtual machines stored on clustered Data ONTAP SMB 3.0 continuous availability (CA) shares work properly, you must grant full control rights to the share for the SnapDrive for Windows service accounts and a minimum read-level access to the SnapManager for Hyper-V web service account.

Related information

Microsoft TechNet: Hyper-V

Adding a Hyper-V parent host or host cluster

You can add a Hyper-V parent host or host cluster to back up and restore your virtual machines.

Steps

1. From the navigation pane, click **Protection**.
2. From the **Actions** pane, click **Add host**.
3. Run the **Add host** wizard.

After you finish

When you add a host to a cluster, the information about the new host is not automatically displayed in the GUI. Manually add the host information to the xml file in the installation directory.

SnapManager for Hyper-V must be installed on each cluster node. If you do not have SnapManager for Hyper-V installed, you are prompted to run the Remote Host Install wizard.

Managing storage connection settings

After adding a host, you can enter all the storage connections (SnapDrive for Windows and SnapManager for Hyper-V) using Manage Storage Connection Settings in **Protection** > **Dataset Management**.

Before you begin

You must have at least one host added to SnapManager for Hyper-V before you can manage your storage connection settings.

Step

1. From **Protection** > **Dataset Management**, select **Manage Storage Connection Settings**.

   This displays the list of storage server credentials currently saved.

Content subject to change

Draft for beta release -- October 2014

Viewing a Hyper-V parent host or host cluster

You can view configuration information about a specific Hyper-V parent host or host cluster so that you can monitor its status.

Steps

1. From the navigation pane, click **Protection** > **Hosts**.
2. Select the host or host cluster that you want to view.

   The Details pane displays the host or host cluster name, domain, cluster members (if applicable), and configuration messages. If you select a host that is not configured, the Details pane displays information about what is not configured.

Viewing a virtual machine

From the Virtual Machine tab and VHD tab of the Details pane for a virtual machine, you can view information about and monitor the status of that machine.

Steps

1. From the navigation pane, click **Protection** > **Hosts** or **Protection** > **Datasets**.
2. Select the dataset or host to which the virtual machine belongs.
3. Select the appropriate virtual machine.

Result

The Virtual Machine tab displays the name, GUID, and state of the selected virtual machine.

The VHD tab displays system disk, mountpoint, VHD full path, LUN path, storage system name, serial number, and volume name associated with the selected virtual machine.

Migrating a Hyper-V virtual machine for SnapManager for Hyper-V operations

SnapManager for Hyper-V does not contain a migration wizard to help you migrate virtual machines (VMs) from non-Data ONTAP storage to Data ONTAP storage, so that you can use them with SnapManager for Hyper-V. You must manually export and import the VM by using Server Manager.

Steps

1. Export the VM from a non-Data ONTAP host on page 28
   You must export the virtual machine (VM) from the non-Data ONTAP host in order to import the VM later.

Content subject to change

Draft for beta release -- October 2014

2. Import the VM to a Data ONTAP host on page 29
   After you have exported the virtual machine (VM), you can import it on the Data ONTAP host.
3. Delete the previously exported VM from the non-Data ONTAP host on page 31
   After you have imported the virtual machine (VM) successfully, you can delete the VM from the non-Data ONTAP host.

Exporting the VM from a non-Data ONTAP host

You must first export a virtual machine (VM) from a non-Data ONTAP host before you can import it to a Data ONTAP host.

Before you begin

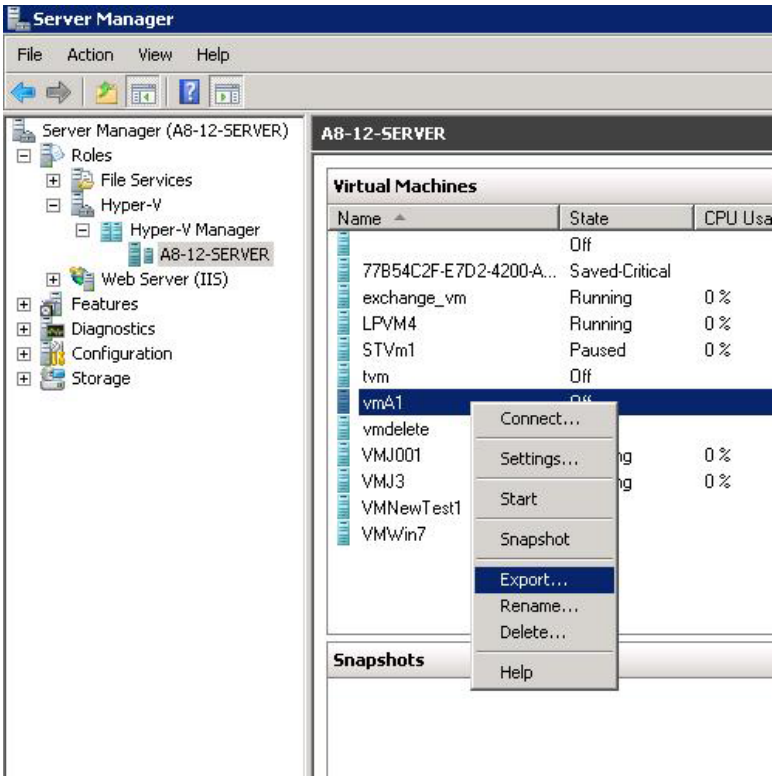
The VM that you want to migrate must be powered off.

Steps

1. Open the application Server Manager.
2. In the left pane, click **Roles** > **Hyper-V** > **Hyper-V Manager**.
3. Select the name of the non-Data ONTAP host on which the VM that you want to migrate currently resides.
4. From the **Virtual Machines** pane, right-click the name of the VM that you want to migrate.
5. Click **Export**.

Content subject to change

Draft for beta release -- October 2014



The Export Virtual Machine window opens.

6. Click **Browse**.

   A window displaying available hard disk drives opens.

7. Click the Data ONTAP host destination for the VM.

8. Click **Select Folder**.

   The VM is exported to the Data ONTAP destination that you chose in Step 7.

After you finish

Next, import the VM to the Data ONTAP host that you chose in Step 7.

Importing a VM to a Data ONTAP host

After you have exported a virtual machine (VM), you can import it to a Data ONTAP host.

Before you begin

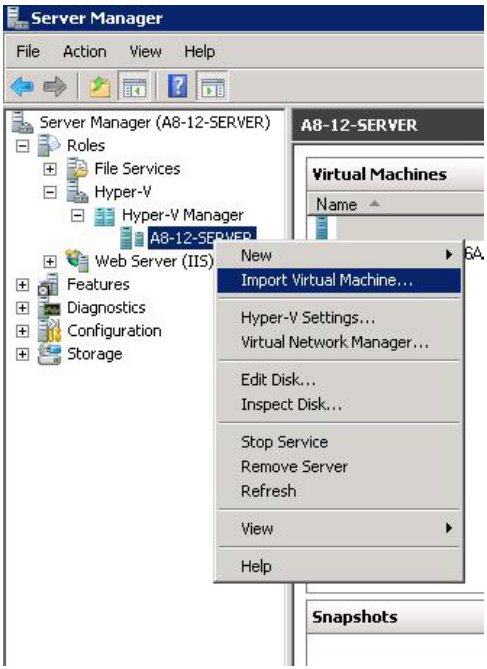
The VM has been exported from the non-Data ONTAP host.

Content subject to change

Draft for beta release -- October 2014

Steps

1. From the left pane, right-click the name of the Data ONTAP host to which you want to import the VM.
2. Select **Import virtual machine**.



The Import Virtual Machine window opens.

3. Click **Browse**.
4. Click the name of the host to which you exported the VM earlier and click **Select Folder**.
5. Under **Import Settings**, select **Copy the virtual machine [create a new unique ID]**.
6. Click **Import**.

After you finish

Next, you must verify that the VM is imported successfully and delete the VM from the non-Data ONTAP host.

Content subject to change

Draft for beta release -- October 2014

Deleting the previously exported VM from the non-Data ONTAP host

After you have imported the virtual machine (VM) successfully, you can delete the VM from the non-Data ONTAP host.

Before you begin

The VM must have been imported successfully.

Steps

1. Select the non-Data ONTAP host on which the VM was originally hosted.
2. From the **Virtual Machines** pane, right-click the name of the VM that you exported previously.
3. Click **Delete**.

   A window opens, asking that you confirm that you want to delete the VM.
4. Click **Delete**.

   The VM is removed from its original host.

Importing or exporting host and dataset configuration information

Although you should manage a host from only one management console, if you need to do so from multiple consoles, you can import and export host and dataset configuration information from one remote management console to another to ensure data consistency.

About this task

You should not import or export configuration information to the directory on which SnapManager for Hyper-V is installed. If you uninstall SnapManager for Hyper-V, this file is lost.

Note: You can use the Import and Export wizard to change host and dataset configuration settings to a previously exported setting. If you perform this operation in a clustered environment, you must import the settings on all nodes in the cluster so that all host and dataset configurations are the same.

Steps

1. From the navigation pane, click **Protection**.
2. From the **Actions** pane, click **Import and export**.

   The Import and Export wizard appears.
3. Complete the steps in the wizard to export host and dataset configuration information from one management console to another.

Content subject to change

Draft for beta release -- October 2014

Note: The export file is static and current only at the time that export file was executed.

4. Complete the steps in the wizard to import host and dataset configuration information to the destination management console.

Removing a Hyper-V parent host or parent host cluster

You can remove a Hyper-V parent host or parent host cluster when you no longer want to manage it using SnapManager for Hyper-V.

Steps

1. From the navigation pane, click **Protection** > **Hosts**.
2. Select the host or host cluster you want to remove.
3. In the **Actions** pane, click **Remove**.

   You can select **Delete all VM backups** to delete any virtual machine backups associated with the host.

   The Hyper-V parent host or host cluster is removed from SnapManager for Hyper-V management but is not deleted permanently. The virtual machines belonging to that host or host cluster are also removed from any datasets to which they belonged.

Event notification settings

You can configure event notification settings to send e-mail, Syslog, and AutoSupport messages if an event occurs.

If event notification settings are not configured when a Hyper-V parent host is added to SnapManager for Hyper-V, you can configure those settings later, using the Configuration wizard.

You can change the event notification settings by using the Configuration wizard even after the host has been added to SnapManager for Hyper-V.

You can configure the event notification settings before you can add virtual machine resources to a dataset.

Report path settings

You can configure report path settings so that you can store reports for SnapManager for Hyper-V operations. You must configure the report path settings before you can add virtual machine resources to a dataset.

If the report settings are not configured when a Hyper-V parent host is added to SnapManager for Hyper-V, you can configure (and even change) those settings later, using the Configuration wizard.

If you configure the report path settings for a parent host cluster, you must manually create the report directory on each cluster node. The report path should not reside on a cluster shared volume (CSV) or a shared LUN.

Content subject to change

Draft for beta release -- October 2014

Related information

Microsoft TechNet: Use Cluster Shared Volumes in a Failover Cluster

Configuring SnapInfo directory settings

You must configure the SnapInfo settings for a host before you can add the virtual machine resources within that host to a dataset. If the SnapInfo settings are not configured when a Hyper-V host is added to SnapManager for Hyper-V, you can configure those settings later, using the Configuration wizard or the **SnapInfo settings** action.

You can also change the SnapInfo settings after the host has been added to SnapManager for Hyper-V. However, if you change the SnapInfo settings, you must manually move all files to the new location; SnapManager for Hyper-V does not update them automatically. If you do not move the files, you cannot restore from or manage the backup copy, and SnapManager for Hyper-V does not list the backup copy.

Starting with SnapManager for Hyper-V, the SnapInfo path can reside on Cluster Shared Volumes (CSV) and it can also reside on SMB shares for Windows Server 2012.

Related information

Microsoft TechNet: Use Cluster Shared Volumes in a Failover Cluster

Setting up a SnapInfo LUN

You must add a SnapInfo LUN in SnapManager for Hyper-V to store the dataset backup metadata. The SnapInfo path must reside on a Data ONTAP LUN, because SnapManager for Hyper-V makes a backup of the SnapInfo copy after a regular backup occurs.

Before you begin

The SnapInfo path can reside on a Cluster Shared Volume (CSV) if you are running a Windows Server 2012 cluster. If you manage dedicated virtual machines, the SnapInfo location must be to a dedicated Data ONTAP LUN. If you manage shared virtual machines, the SnapInfo location must be to a shared Data ONTAP LUN.

Steps

1. Create a new shared disk by using SnapDrive for Windows.
   a. When given the option to choose a Microsoft Cluster Services Group, select the option **Create a new cluster group.**
   b. Name the group **`smhv_snapinfo`** and complete the process.
2. Open Windows Failover Clustering (WFC) and verify that the new group is online.

Content subject to change

Draft for beta release -- October 2014

3. Install SnapManager for Hyper-V on each node in the cluster.
4. Run the **Configuration** wizard and apply the SnapInfo configuration settings to all nodes in the cluster.
   a. Select one of the hosts.
   b. From the **Navigation** pane, click **Protection** > **Hosts**.
   c. From the **Actions** pane, run the **Configuration** wizard.
   d. Apply the SnapInfo settings to the newly created LUN.

Result

When the Configuration wizard is run, the SnapInfo configuration settings are replicated to all nodes in the cluster.

Related references

Error: Snapdrive SDDiscoveryFileSystemListInfo response is null on page 76

Changing the SnapInfo directory path

You can control SnapInfo directory path settings by using the Configuration wizard or the **SnapInfo settings** action.

About this task

SnapInfo directory settings are specified on the host level in SnapManager for Hyper-V. SnapManager for Hyper-V supports NAS (SMB) hosts and SAN hosts. For SAN hosts, the SnapInfo settings are applied on the volume level; for NAS hosts, the SnapInfo settings are applied on the SMB share level.

If you have added the IP address of the storage system to SnapDrive for Windows TPS, the storage settings from SnapDrive for Windows are automatically populated when you run the configuration wizard in SnapManager for Hyper-V. If you do not have SnapDrive for Windows TPS configured, you must specify the IP address of the storage system in the Manage Storage Connections tab in SnapManager for Hyper-V.

Steps

1. From the navigation pane, click **Protection** > **Hosts**.
2. Select the host for which you want to change the SnapInfo directory path.
3. From the **Actions** pane, select **SnapInfo settings**.

   The SnapInfo Settings dialog box opens.

Content subject to change

Draft for beta release -- October 2014

4. Select the storage type from the options shown:

Option	Description
SAN	This is the default storage type.
NAS	Use this option for SMB shares.

5. Click **Browse**.

   The Browse for Folder window opens.

6. Select your SnapInfo storage system (SAN) or volume (NAS) and click **OK**.

   The hosts that display are NAS shares corresponding to the storage systems that have been registered using the `Manage Storage Connections` option at the host level. If you do not see the shares you are looking for, ensure that `Manage Storage Connections` has been configured correctly.

7. From the **SnapInfo Settings** window, click **OK**.

Configuring datasets

You can create, modify, view, and delete datasets based on your protection needs.

Requirements for creating a dataset

You must meet specific requirements when you want to create datasets to protect your data. You must first add the host or host cluster to SnapManager for Hyper-V and then add virtual machines to the host or host cluster.

Dataset name and description

When naming the dataset, you should use a naming convention at your site to help administrators locate and identify datasets, limited to these characters:

- a to z
- A to Z
- 0 to 9
- _ (underscore)
- hyphen

Dataset resources

You must add the host or host cluster to SnapManager for Hyper-V before adding resources such as virtual machines to the dataset.

Content subject to change

Draft for beta release -- October 2014

You can add hosts, dedicated virtual machines, or shared virtual machines to a dataset. If you add a host, you add all of the virtual machines that belong to the host. You can also add virtual machines belonging to different hosts to the dataset. Virtual machines can belong to multiple datasets.

Note: Dedicated and shared virtual machines that belong to the same host cluster should not exist in the same dataset. Adding these types of resources to a single dataset can cause the dataset backup to fail.

Virtual machines and Data ONTAP LUNs

All of the files associated with the virtual machines, including configuration files, Snapshot copies, and VHDs, must reside on Data ONTAP LUNs.

Dataset resource consumption

Only one application-consistent backup operation can occur on a host at any given time. If the same virtual machines belong to different datasets, you should not schedule an application-consistent backup of the datasets at the same time. If this occurs, one of the backup operations fails.

When creating a dataset, you should select all virtual machines that reside on a particular Data ONTAP LUN. This enables you to get all backups in one Snapshot copy and to reduce the space consumption on the storage system.

Creating a dataset

You can create datasets for virtual machine resources that share the same protection requirements. You can add virtual machines to multiple datasets, as necessary.

Before you begin

You must have the following information available:

- Dataset name and description
- Virtual machine resources you plan to add to the dataset

About this task

Dedicated and shared disks that belong to the same host cluster should not be placed in the same dataset. Adding these types of resources to a single dataset can cause the dataset backup to fail. You can have only one type of VM per dataset: NAS or SAN. You cannot have mixed-mode datasets.

The Validate Dataset check box is selected by default. SnapManager for Hyper-V checks for any configuration errors in all VMs during the creation or modification of a dataset. You must ensure that the check box is not selected if you do not want to enable validation of the dataset.

Steps

1. From the navigation pane, click **Protection** > **Datasets**.

Content subject to change

Draft for beta release -- October 2014

2. From the **Actions** pane, click **Create dataset**.
3. Complete the pages of the wizard.

After you finish

You should next add protection policies to the dataset that you created.

Modifying a dataset

After you have created a dataset, you can modify the dataset description and the resources associated with the dataset.

About this task

The Validate Dataset check box is selected by default. SnapManager for Hyper-V checks for any configuration errors in all VMs during the creation or modification of a dataset. You must ensure that the check box is not selected if you do not want to enable validation of the dataset.

Steps

1. From the navigation pane, click **Protection** > **Datasets**.
2. Select the dataset that you want to modify.
3. From the **Actions** pane, click **Modify dataset**.
4. Complete the steps in the wizard.

Viewing a dataset

You can view the virtual machines associated with a dataset.

Steps

1. From the navigation pane, click **Protection** > **Datasets**.
2. Expand the tree view to look at the virtual machines that belong to the dataset.

Deleting a dataset

You can delete a dataset as your protection needs change.

About this task

Deleting a dataset does not delete the virtual machines that belong to the dataset. After the dataset is deleted, the virtual machines that belonged to it become unprotected if they do not belong to another dataset.

Content subject to change

Draft for beta release -- October 2014

Steps

1. From the navigation pane, click **Protection** > **Datasets.**
2. Select the dataset that you want to delete.
3. From the **Actions** pane, click **Delete** and click **OK** to delete the dataset.

   Deleting the dataset also deletes the scheduled jobs from all hosts that are members of the dataset. SnapManager for Hyper-V no longer manages the retention of backups when you delete the dataset, even if it is re-created with the same name.

Result

SnapManager for Hyper-V no longer protects the resources associated with the deleted dataset unless those resources belong to another dataset.

Configuring policies

You can add, modify, or delete policies associated with datasets so that you can protect your data.

Requirements for adding policies to a dataset

You must meet specific requirements when you want to apply policies to datasets for backup or restore functionality. You can add multiple retention, scheduling, and replication policies to the same dataset.

Policy name and description

A policy name and description, limited to these characters:

- a to z
- A to Z
- 0 to 9
- _ (underscore)
- - (hyphen)

Backup retention limits

You must decide the minimum length of time that you want to keep your hourly, daily, weekly, or monthly backup copies before they are deleted.

Note: Backups with a retention type of “Unlimited” are not deleted.

You can keep backups based on either time or a specified number. For example, you can keep the 10 most current backups, or you can delete backups older than 15 days.

Content subject to change

Draft for beta release -- October 2014

If your system appears to retain old backups, you should check your retention policies. All objects being backed up that share a Snapshot copy must meet the backup deletion criteria for the retention policy to trigger the removal of a Snapshot copy.

Scheduled backup job name

You must assign a name to the scheduled backup job.

Permission to schedule backups

You must have appropriate credentials to schedule dataset backups.

Number of possible datasets scheduled for backup simultaneously

If the same virtual machines belong to different datasets, you should not schedule a backup of more than one dataset containing the same VM at the same time. When this occurs, one of the backup operations fails. Only one backup operation can occur on a host at any given time.

Type of scheduled backup

You can perform either an application-consistent or a crash-consistent backup.

Backup options

You must choose if you want to update the SnapMirror destination location after the backup is complete.

The update succeeds only if you already have SnapMirror configured, and if the LUNs containing the virtual machines in the dataset belong to the source SnapMirror volume.

The default behavior of SnapManager for Hyper-V is to fail a backup if one or more virtual machines cannot be backed up online. If a virtual machine is in the saved state or shut down, you cannot perform an online backup. In some cases, virtual machines are in the saved state or shut down for maintenance, but backups still need to proceed, even if an online backup is not possible. To do this, you can move the virtual machines that are in the saved state or shut down to a different dataset with a policy that allows saved state backups.

You can also select the Allow saved state VM backup check box to enable SnapManager for Hyper-V to back up the virtual machine in the saved state. If you select this option, SnapManager for Hyper-V does not fail the backup when the Hyper-V VSS writer backs up the virtual machine in the saved state or performs an offline backup of the virtual machine. Performing a saved-state or offline backup can cause downtime.

The `distributed application-consistent backup` feature enables multiple VMs running on the partner cluster nodes to be consistent in a single hardware Snapshot copy made from the backup node. This feature is supported for all the VMs running on a CSV 2.0 Windows volume across multiple nodes in a Windows Failover Cluster. To use this feature, select the `Application-consistent` backup type and select the **Enable Distributed Backup** check box.

Content subject to change

Draft for beta release -- October 2014

Secondary storage in a SnapMirror backup

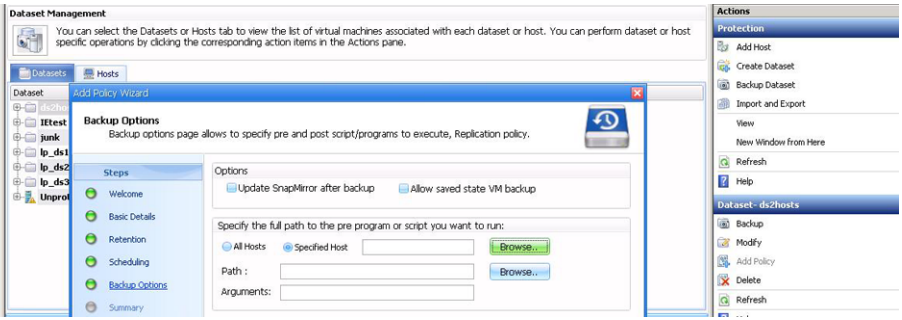
These options enable you to accept options applicable to a secondary storage defined in a SnapMirror relationship. Here, you can select **Update SnapMirror after backup**. Under the Vault label option pane, you can select **Update SnapVault after backup**. If you select **Update SnapVault after backup**, you must a choose a vault label from the drop-down menu or enter a custom label.

Backup scripts

You must decide if you want the optional backup scripts to run either before or after the backup takes place.

These scripts run on all dataset member hosts unless you indicate a specific server.

Backup scripts run on each node in the dataset. You can set the dataset policy to specify the name of the host on which you want to run the scripts. The policy is processed on each node in the cluster where the VM to be backed up is running.



You can use the following environment variables in arguments for backup postscripts:

- **$VMSnapshot**: Specifies the name of the Snapshot copy that is created on the storage system as a result of this backup. When you are performing application-consistent backups in Data ONTAP environments running in 7-Mode, this is the name of the second (backup) Snapshot copy. The first name is same as the second name but without the `_backup` suffix.
- **$SnapInfoName**: Specifies the timestamp used in the SnapInfo directory name.
- **$SnapInfoSnapshot**: Specifies the name of the SnapInfo Snapshot copy created on the storage system. SnapManager for Hyper-V makes a Snapshot copy of the SnapInfo LUN at the end of the dataset backup operation.

  Note: The $SnapInfoSnapshot variable is supported for dedicated virtual machines only.

Related information

Microsoft TechNet: Hyper-V
Clustered Data ONTAP 8.3 Volume Backup Using SnapVault Express Guide

Content subject to change

Draft for beta release -- October 2014

Adding policies

You can add retention, scheduling, and replication policies, as well as scripts, to your datasets so that you can protect your data.

Before you begin

You must have the following information available:

- Policy names and descriptions
- Retention information
- Scheduling information
- Backup options information
- Backup script information

Steps

1. From the navigation pane, click **Protection** > **Datasets**.
2. Select the dataset to which you want to add policies.
3. From the **Actions** pane, click **Add policy**.

   The Create Policy wizard appears.
4. Complete the steps in the wizard to create protection policies for your dataset.

Modifying policies

You can modify the policies that protect your datasets by using the Modify Policy wizard.

Steps

1. From the navigation pane, click **Protection** > **Datasets**.
2. Select the dataset that contains the policies that you want to modify.
3. Select the policy that you want to modify.
4. From the **Actions** pane, click **Modify policy**.

   The Modify Policy wizard appears.
5. Complete the steps in the wizard to modify the protection policy for your dataset.

Content subject to change

Draft for beta release -- October 2014

Viewing policies

You can view policy details associated with a specific dataset.

Steps

1. From the navigation pane, click **Protection** > **Datasets**.
2. Select the dataset that contains the policies that you want to view.
3. From the **Policies** pane, select the specific policy for which you want to view details.

   Information about the policy appears in the Details pane.

Deleting policies

You can delete a policy from a dataset when it is no longer needed.

Steps

1. From the navigation pane, click **Protection** > **Datasets**.
2. Select the dataset that contains the policy that you want to delete.
3. From the **Policies** pane, select the specific policy that you want to delete.
4. From the **Actions** pane, click **Remove** and click **OK** to delete the policy.

   Deleting the policy also deletes the scheduled jobs from all hosts that are members of the dataset.

Content subject to change

Managing reports

You can view and delete backup, restore, and configuration reports in SnapManager for Hyper-V. These reports contain important information about your datasets, virtual machines, and hosts. You can also export reports in several different formats.

Backup reports

Backup reports display all of the backup information for all hosts belonging to a particular dataset. You can view a backup report for either a dataset or a virtual machine. Reports displayed for a virtual machine use the virtual machine name instead of its GUID.

When the backup report is displayed, you can export it into several different formats.

Restore reports

Restore reports display all of the information about the restore operation on a per-VM basis.

When the restore report is displayed, you can export it into several different formats.

Configuration reports

Configuration reports display the notification settings, report path, and SnapInfo path for the selected host.

When the configuration report is displayed, you can export it into several different formats.

Viewing a dataset report

You can view a report about a dataset or virtual machine resource managed in SnapManager for Hyper-V.

Steps

1. From the navigation pane, click **Reports** > **Datasets**.
2. Select the dataset or virtual machine that contains the report you want to view.
3. From the **Reports** pane, click either the **Backup** tab or **Recovery** tab.
4. Select the report that you want to view and click **View report**.

If you want to view a...	Then...
dataset report	You can view a backup report.
virtual machine report	You can view either a backup or recovery report.

Draft for beta release -- October 2014

The report appears in a separate window.

Viewing a host report

You can view a report about a host managed in SnapManager for Hyper-V.

Steps

1. From the navigation pane, click **Reports > Hosts**.
2. Select the host that contains the report you want to view.
3. From the **Reports** pane, select the report that you want to view and click **View report**.

   The configuration report appears in a separate window.

Deleting a report

You can delete one or more reports when they are no longer necessary.

Steps

1. From the navigation pane, click **Reports > Datasets** or **Reports > Hosts**.
2. Select the dataset, virtual machine, or host that contains the report or reports you want to delete.
3. From the **Reports** pane, select the report or reports you want to delete.
4. From the **Actions** pane, click **Delete report** and click **OK** to delete.

Content subject to change

Draft for beta release -- October 2014

Understanding VSS components

You can use Microsoft Windows Server Volume Shadow Copy Service (VSS) coordinate data servers, backup applications, and storage management software to support the creation and management of consistent backups.

VSS coordinates Snapshot copy-based backup and restore operations and includes these components:

VSS requestor

The VSS requestor is a backup application, such as SnapManager for Hyper-V or NTBackup. It initiates VSS backup and restore operations. The requestor also specifies Snapshot copy attributes for backups it initiates.

VSS writer

The VSS writer owns and manages the data to be captured in the Snapshot copy. Microsoft Hyper-V VSS Writer is an example of a VSS writer.

VSS provider

The VSS provider is responsible for creating and managing the Snapshot copy. A provider can be either a hardware provider or a software provider:

- A hardware provider integrates storage array-specific Snapshot copy and cloning functionality into the VSS framework.

  The Data ONTAP VSS Hardware Provider integrates the SnapDrive service and storage systems running Data ONTAP into the VSS framework.

  Note: The Data ONTAP VSS Hardware Provider is installed automatically as part of the SnapDrive software installation.

- A software provider implements Snapshot copy or cloning functionality in software that is running on the Windows system.

  Note: To ensure that the Data ONTAP VSS Hardware Provider works properly, do not use the VSS software provider on Data ONTAP LUNs. If you use the VSS software provider to create Snapshot copies on a Data ONTAP LUN, you cannot delete that LUN by using the VSS Hardware Provider.

CSV 2.0 in Windows Server 2012

The introduction of Windows Server 2012 provides new features for Cluster Shared Volume (CSV) 2.0 that include a new file system, changes to CSV writer, changes to CSV shadow copy, and enhancements to CSV backup.

Windows Server 2012 includes the following changes to CSV 2.0:

Content subject to change

Draft for beta release -- October 2014

- The CSV File System (CSVFS) is available on all nodes in the cluster as a new distributed file system.
- CSV Writer serves volume and component-level metadata from the non-requesting node for CSV volumes and acts as a proxy by including the Hyper-V writers from the remote node for the backup session.
- The CSV shadow copy provider acts as the default software provider for CSV volumes and co-ordinates VSS freeze and VSS thaw across all cluster nodes to provide application and crash consistency.

  The CSV shadow copy provider ensures that a CSV Snapshot volume is writable on the requesting node.
- CSV now supports one application-consistent Snapshot volume across all CSVs for multiple virtual machines.

  The CSV volume from the Snapshot volume is exposed to all the virtual machine owner nodes, to perform autorecovery.

  CSV goes into redirected I/O mode only during Snapshot creation and not during backup.

SnapManager for Hyper-V supports the modified Hyper-V CSV backup architecture. SnapManager for Hyper-V involves the CSV writer in the backup process which creates distributed application consistent backup for all the virtual machines that are running on multiple nodes in a CSV. This removes the current limitation of performance and space utilization issues with CSV Hyper-V backups. SnapManager for Hyper-V also stores in its metadata repository the writer backup metadata and backup components document for all the virtual machines in a CSV, which is used during the restore process.

SMB 3.0 support for Hyper-V VMs in Windows Server 2012

Microsoft enhanced the VSS infrastructure to support application-consistent backups of Hyper-V virtual machines (VMs) running on SMB 3.0 shares using the new Remote VSS Hardware Provider running on the SMB target.

A new provider named SMB File Share Provider is available in Windows 2012 Hypervisor to support and coordinate the Hyper-V VM backups running on SMB 3.0 shares.

When the VSS Requestor (SnapManager for Hyper-V) adds an SMB 3.0 share containing Hyper-V VMs to the VSS Snapshot set, VSS invokes the new SMB File Share Copy Provider to send the MSRPC commands to the SMB target to coordinate the VSS backups.

The new File Share Shadow Copy Agent (Remote VSS Provider) running on the SMB target is responsible for creating the actual hardware Snapshot copy.

Data ONTAP 8.2 implements the file share shadow copy agent (Remote VSS Hardware Provider) to perform the application-consistent backup copy of the SMB shares.

Content subject to change

Draft for beta release -- October 2014

How SnapManager for Hyper-V uses VSS

SnapManager for Hyper-V provides integration with Microsoft Hyper-V Volume Shadow Copy Service (VSS) writer to quiesce a virtual machine (VM) before creating an application-consistent Snapshot copy of the VM.

SnapManager for Hyper-V is a VSS requestor and coordinates the backup operation to create a consistent Snapshot copy, using VSS Hardware Provider for Data ONTAP for Hyper-V VMs running on SAN and Remote VSS provider for Hyper-V VMs running on SMB 3.0 share.

SnapManager for Hyper-V enables you to make application-consistent backups of a VM, if you have Microsoft Exchange, Microsoft SQL, or any other VSS-aware application running on virtual hard disks (VHDs) in the VM. SnapManager for Hyper-V coordinates with the application writers inside the VM to ensure that application data is consistent when the backup occurs.

You can also restore a VM from an application-consistent backup. The applications that exist in the VM restore to the same state as at the time of the backup. SnapManager for Hyper-V restores the VM to its original location.

Note: VSS integration is available only with application-consistent backups. Crash-consistent backups do not use VSS.

Data ONTAP VSS Hardware Provider requirement

You must have the Data ONTAP VSS Hardware Provider installed for SnapManager to function properly. Data ONTAP VSS Hardware Provider integrates the SnapDrive service and storage systems running Data ONTAP into the VSS framework. This is required for VMs running on SAN storage.

The Data ONTAP VSS Hardware Provider, included with SnapDrive, does not need to be installed separately.

For Hyper-V VMs running on SMB 3.0 shares, remote VSS hardware provider running on Data ONTAP 8.2 will be invoked by the Windows Hypervisor.

Viewing installed VSS providers

You can view the VSS providers installed on your host.

Steps

1. Select **Start > Run** and enter the following command to open a Windows command prompt:

   `cmd`

Content subject to change

Draft for beta release -- October 2014

2. At the prompt, enter the following command:

   `vssadmin list providers`

   The output should be similar to the following:

```
Provider name: 'Data ONTAP VSS Hardware Provider'
Provider type: Hardware
Provider ID: {ddd3d232-a96f-4ac5-8f7b-250fd91fd102}
Version: 7.0.0.xxxx
```

Verifying that the VSS Hardware Provider was used successfully

You can verify that the Data ONTAP VSS Hardware Provider was used successfully after a Snapshot copy was made.

Step

1. Navigate to **System Tools** > **Event Viewer** > **Application** in MMC and look for an event with the following values:

Source	Event ID	Description
Navssprv	4089	The VSS provider has successfully completed CommitSnapshots for SnapshotSetId *id* in *n* milliseconds.

Note: VSS requires that the provider commit a Snapshot copy within 10 seconds. If this time limit is exceeded, the Data ONTAP VSS Hardware Provider logs Event ID 4364. This limit could be exceeded due to a transient problem. If this event is logged for a failed backup, retry the backup.

Content subject to change

Draft for beta release -- October 2014

Creating and managing backup jobs in SnapManager for Hyper-V

You can create and monitor on-demand backups or managed scheduled backups in SnapManager for Hyper-V. You can also perform two types of backup jobs with SnapManager for Hyper-V: application consistent and crash consistent.

About SnapManager for Hyper-V backups

You can create on-demand backup jobs and run them when you want or you can create scheduled backup jobs using policies attached to datasets. An on-demand backup job can include retention and replication policies as well as scripts to run before and after the backup takes place. You can create, modify, view, and delete the policies that make up scheduled backup jobs.

Types of backup jobs SnapManager for Hyper-V can perform

You can perform two types of backup jobs with SnapManager for Hyper-V: application consistent and crash consistent.

Application-consistent backup jobs

Application-consistent backup jobs are thorough, reliable, and resource intensive. They are performed in coordination with Microsoft Volume Shadow Copy Service (VSS) to ensure that each application running on the VM is quiesced before creating a Snapshot copy. This backup method guarantees application data consistency. You can use it to restore VMs and the applications running on them. However, application-consistent backup jobs are time consuming and can be complex.

Crash-consistent backup jobs

Crash-consistent backup jobs are quick Snapshot copies of all the LUNs used by VMs involved in a dataset. The resulting backup copies are similar to the data captures of VMs that crash or are otherwise abruptly powered off. Crash-consistent backup jobs provide a quick way to capture data, but the VMs must be present to be restored from a crash-consistent backup. Crash-consistent backup jobs are not intended to replace application-consistent backup jobs.

SnapManager for Hyper-V backup requirements and limitations

You should be aware of the requirements and limitations of a SnapManager for Hyper-V backup:

- Backup and restore operations are not supported if you are performing a switchover or switchback operation on a MetroCluster configuration. If a backup and restore operation and a switchover or switchback operation are running simultaneously, the `.vhd` file format of a VM might change to `.avhdx` in Windows Server 2012 R2 systems. The VM is not affected by this change.

Content subject to change

Draft for beta release -- October 2014

- The `distributed application-consistent backup` option enables multiple VMs running on the partner cluster nodes to be consistent in one single hardware Snapshot copy created from the backup node. This option is supported for all the VMs running on a CSV 2.0 Windows volume across multiple nodes in a Windows Failover Cluster.
- When operating in 7-Mode, application-consistent backup jobs use the VSS Hardware Provider to make two Snapshot copies. The Snapshot copies are called `snapshot_name` and `snapshot_name_backup`. The two Snapshot copies are made to facilitate automatic recovery during the VSS backup.
- In clustered environments, application-consistent backups require only one Snapshot copy for the automatic recovery process. SIS clones are leveraged to perform automatic recovery, and after automatic recovery is complete, the first Snapshot copy (`snapshot_name`) is deleted.
- Each Windows volume in the VM must have at least 300 MB of free disk space. This includes the Windows volumes corresponding to VHDs, iSCSI LUNs, and pass-through disks attached to the VM.
- A crash-consistent backup job always creates only one Snapshot copy. It does not provide VSS integration.
- Multiple crash-consistent backup jobs can execute in parallel. A crash-consistent backup job can run in parallel with an application-consistent backup job.
- `AllowSavedStateBackup` is not applicable to crash-consistent backup jobs.

Requirements for manually backing up a dataset

To backup a dataset manually, you must first name and describe the dataset, choose a backup type and options, and set a retention policy.

Backup name and description

You must assign a name and description to the backup.

The default naming convention for backups is DatasetName_Timestamp. You can change everything in the backup name except the timestamp, which always appears as part of the backup name.

Backup names and descriptions are limited to these characters:

- a to z
- A to Z
- 0 to 9
- _ (underscore)
- hyphen

Content subject to change

Draft for beta release -- October 2014

Policy choice

You must decide which policy you want to use for the on-demand backup.

You can select a specific policy in the Backup wizard. You can override the retention or replication policy, as well as scripts associated with the policy, without changing the policy itself.

You can also choose None, which enables you to make an on-demand backup without creating any policies. This option uses the default values for retention policies, replication policies, and scripts.

Retention value

You can choose to override the retention policy specified in the policy that you selected. If you do this, you must decide what the minimum length of time is that you want to keep your hourly, daily, weekly, monthly, or unlimited backup copies before they are deleted.

You can keep backups based on either time or a specified number of backups. For example, you can keep the 10 most current backups, or you can delete backups older than 15 days.

Type of backup

You can perform an application-consistent or crash-consistent backup.

Backup options

You can allow saved state backups.

The default behavior of SnapManager for Hyper-V is to fail a backup if one or more virtual machines cannot be backed up online. If a virtual machine is in the saved state or shut down, you cannot perform an online backup. In some cases, virtual machines are in the saved state or shut down for maintenance, but backups still must proceed, even if an online backup is not possible. To do this, you can move the virtual machines that are in the saved state or shut down to a different dataset, one with a policy that allows saved state backups.

You can also modify the existing policy by selecting the Allow saved state VM backup check box. This allows SnapManager for Hyper-V to back up the virtual machine in the saved state. If you select this option, SnapManager for Hyper-V does not fail the backup when the Hyper-V VSS writer backs up the virtual machine in the saved state or performs an offline backup of the virtual machine. Performing a saved state or offline backup can cause downtime.

The `distributed application-consistent backup` feature enables multiple VMs running on the partner cluster nodes to be consistent in one single hardware Snapshot copy made from the backup node. This feature is supported for all the VMs running on a CSV 2.0 Windows volume across multiple nodes in a Windows Failover Cluster.

Secondary storage in a SnapMirror backup

These options enable you to accept options applicable to a secondary storage defined in a SnapMirror relationship. You can select **Update SnapMirror after backup**. Under the Vault label option pane,

Content subject to change

Draft for beta release -- October 2014

you can select **Update SnapVault after backup**. If you select **Update SnapVault after backup**, you must a choose a vault label from the drop-down menu or enter a custom label.

Backup scripts

You can override the script options specified in the policy that you selected.

These scripts run on all dataset member hosts, unless you indicate a specific host in the script.

Related information

Microsoft TechNet: Hyper-V

Clustered Data ONTAP 8.3 Volume Backup Using SnapVault Express Guide

How SnapManager for Hyper-V handles saved-state backups

Although the default behavior of SnapManager for Hyper-V is to cause backups containing virtual machines that are in the saved state to shut down or fail, you can perform a saved-state backup by moving the virtual machines to a dataset that has a policy that allows saved-state backups.

You can also create or edit your dataset policy to allow a saved-state virtual machine backup. If you choose this option, SnapManager for Hyper-V does not cause the backup to fail when the Hyper-V VSS writer backs up the virtual machine using the saved state or performs an offline backup of the virtual machine. However, performing a saved-state or offline backup can cause downtime.

Related information

Microsoft TechNet: Hyper-V

Manually backing up a dataset

You can create an on-demand backup of a dataset.

Before you begin

You must have the following information available:

- Backup name and description
- Policy name, if necessary
- Policy override information (if you plan to change any of the previously specified policy options)
- Backup type
- Backup options information

Content subject to change

Draft for beta release -- October 2014

Steps

1. From the navigation pane, click **Protection** > **Datasets**.
2. Select the dataset for which you want to create a manual backup and click **Backup**.

   The Backup wizard appears.
3. Complete the steps in the wizard to create your on-demand backup.

   Closing the wizard does not cancel the on-demand backup.

Result

You can view the status of the on-demand backup in the Jobs Management window.

Monitoring backup jobs

You can view the scheduled backup jobs for a particular dataset by using the Jobs Management window Scheduled tab. You can also view the backup and restore jobs that are currently running by using the Jobs Management window Running tab.

Steps

1. From the navigation pane, click **Jobs**.
2. Click either the **Scheduled** tab or the **Running** tab.
3. Select the scheduled or running backup job, or the restore job, that you want to monitor.

   Information about the job appears in the Details pane.
4. Use the Running Job report in **Reports view**, if you want to view a live report of a running job.

   Note: You can also monitor backup jobs with Microsoft's SCOM console. See the Microsoft web site for more information.

Deleting a backup

You can delete one or more backups associated with either a dataset or a virtual machine.

Steps

1. From the navigation pane, click **Recovery**.
2. Select the virtual machine within the dataset that contains the backup you want to delete.

Content subject to change

Draft for beta release -- October 2014

If you delete a backup associated with a dataset, the backups associated with any virtual machines belonging to that dataset are also deleted. If you delete a backup associated with a virtual machine, only that backup is deleted.

3. In the **Backups** pane, select the backup that you want to delete.
4. Click **Delete**.

   The **Delete Backup** dialog displays. You have the option to delete backups for a selected VM or for an entire dataset.
5. Select the appropriate option, and click **Confirm Delete**.

   You can view the status of the backup delete operation in the status window.

Content subject to change

Restoring a virtual machine

You can use SnapManager for Hyper-V to restore a virtual machine (VM) from a backup copy. You can also restore a VM that is part of a cluster. SnapManager for Hyper-V determines the appropriate node in the cluster to which to restore the VM.

To restore a VM, SnapManager for Hyper-V uses the file-level restore feature in SnapDrive for Windows. You can spread the associated files of a VM, including the configuration file, Snapshot copies, and any VHDs, across multiple Data ONTAP LUNs. A LUN can contain files belonging to multiple VMs.

If a LUN contains only files associated with the VM that you want to restore, SnapManager for Hyper-V restores the LUN by using LCSR (LUN clone split restore). If a LUN contains additional files not associated with the virtual machine that you want to restore, SnapManager for Hyper-V restores the virtual machine by using the file copy restore operation.

Related information

NetApp Documentation: SnapDrive for Windows (current releases)

Requirements for restoring a virtual machine

To restore a virtual machine from a backup copy, you must first determine how you want to restore the backup copy.

VM backup copy name

You must decide which backup copy you want to restore.

All backup copies are listed by name in the Backups pane of the Recovery Management window.

VM backup copy type

Restoring a VM from an application-consistent backup is done in coordination with VSS. Hyper-V VSS writer deletes the VM before restoring and registers the VM to Hyper-V Manager after the restore operation finishes.

Restoring a VM from a crash-consistent backup does not involve VSS. The VM is turned off prior to the restore operation. When you are restoring from a crash-consistent backup, the VM must exist; restoring a deleted VM from a crash-consistent backup fails.

VM backup copy status

You must determine if the virtual machine still exists.

Draft for beta release -- October 2014

If the virtual machine no longer exists, you can still restore it if the LUNs on which the virtual machine was created still exist. The LUNs must have the same drive letters and Windows volume GUIDs as at the time of backup.

If you delete a virtual machine in Windows Server 2008 R2, you can restore the virtual machine from an application-consistent backup, but in Windows Server 2012 and Windows Server 2012 R2, you can restore a deleted virtual machine from both a crash- and application-consistent backup.

If the virtual machine was removed from all datasets before it was deleted, you can still restore it by selecting Unprotected Resources and selecting a backup to which it belonged.

VM backup copy configuration status

You must determine if the virtual machine configuration is the same as it was at the time of the backup.

If the current virtual machine configuration is different than at the time of backup, SnapManager for Hyper-V notifies you that the virtual machine layout has changed, and asks you if you would like to restore the virtual machine configuration and data as it existed in the backup.

> **Note:** Because SnapManager for Hyper-V does not back up the cluster configuration of the virtual machine, it cannot restore the cluster configuration. If the virtual machine and cluster configuration are lost, you can restore the virtual machine from SnapManager for Hyper-V, but you have to manually make it highly available.

If the virtual machine is configured differently than the current configuration of the virtual machine in the backup, you might need to update the cluster configuration to reflect any newly added or removed virtual hard disks (VHDs).

Snapshot copy status

You can verify that the backup Snapshot copies exist on the storage system before attempting the restore operation.

VM restart

You can choose to start the virtual machine after it is restored.

Related information

Microsoft TechNet: Failover Clusters in Windows Server 2008 R2

Content subject to change

Draft for beta release -- October 2014

Restoring a virtual machine from a backup copy

You can use SnapManager for Hyper-V, which restores a single virtual machine (VM) at a time, to recover lost or damaged data from a backup copy.

Before you begin

You must have the following information available:

- Backup name
- Configuration information
- Script information

When restoring to an alternate host, the CPU type on the physical computer on which your original VM resided should be compatible with the physical computer onto which you want to restore the VM. Alternatively, you can use the Hyper-V Manager to specify that the machine is allowed to restore to a machine with a different CPU type.

About this task

After storage live migration, you cannot restore from the latest backup.

If you start a restore operation of a Hyper-V virtual machine, and another backup or restoration of the same virtual machine is in process, it fails.

Steps

1. From the navigation pane, click **Recovery**.
2. Select the virtual machine that you want to restore.
3. In the **Backups** pane, select the name of the backup copy that you want to restore and click **Restore**.

   The Restore wizard appears.
4. Complete the steps in the wizard to restore the virtual machine backup copy.

   Closing the wizard does not cancel the restore operation. SnapManager for Hyper-V validates the virtual machine configuration before beginning the restore operation. If there have been any changes in the virtual machine configuration, a warning appears, enabling you to choose to continue or to cancel the operation.

Content subject to change

Draft for beta release -- October 2014

After you finish

You can view the status of the restore operation in the Jobs Management window or check the operation results by viewing the report in the Reports Management window.

Related references

Restoring from a backup after failback on page 83

Content subject to change

Performing disaster recovery

The disaster recovery feature ensures that if a disaster or other circumstance makes critical protected data at your primary storage sites unavailable, that you can provide access to the backed up copy of that data through your secondary storage sites. Disaster recovery can only be performed using the PowerShell interface.

Configuring SnapManager for Hyper-V for failover

To fully enable your SnapManager for Hyper-V implementation for disaster recovery, you must ensure that the primary and secondary hosts have the same configuration and know that you can perform disaster recovery using only PowerShell.

The following types of setups support disaster recovery:

- Stand-alone primary host and stand-alone secondary Hyper-V host
- Clustered primary and secondary Hyper-V hosts
- Cluster shared volumes (CSV) on the primary and secondary Hyper-V hosts

For example, a cluster virtual machine (VM) on a primary host must be recovered as a cluster VM, a dedicated (stand-alone) VM must be recovered as a dedicated VM, and a CSV VM must be recovered as a CSV VM.

LUNs on a secondary host should be connected in the same way as their counterparts on the primary host. That is, the LUN type (dedicated, shared, or CSV) and the drive letter, mount point, or CSV reparse point should be the same on primary and secondary hosts. With SAN restore operations to an alternate path location, a different drive letter can be specified for the LUN restore operation on a secondary location.

Note: Drive letters or CSVs and volume mount points are supported.

The following example shows a basic disaster recovery setup:

- Site A (primary) contains storage systems and a stand-alone Hyper-V host system or Hyper-V host cluster.
  VMs running on these hosts reside on Data ONTAP storage.
- Site B (secondary) contains storage systems and a Hyper-V host or cluster (same as that of primary).
- SnapDrive for Windows and SnapManager for Hyper-V are installed on both sites A and B.
- The SnapMirror relationship is initialized from site A to site B.

Draft for beta release -- October 2014

- On site A, a Hyper-V host or cluster added to SnapManager for Hyper-V and the VMs is backed up using SnapManager for Hyper-V.
  The policy to update SnapMirror after the backup is checked. After each backup, the secondary site is updated with new Snapshot copies of the VMs and SnapInfo copies.

Recovering and restoring from a disaster recovery failover

To recover from a disaster, SnapManager for Hyper-V must first fail over to a secondary storage system. Failing over involves a series of manual steps in PowerShell.

About this task

Most backups can be restored to an alternate host for both NAS and SAN; however, Windows Server 2008 R2 crash-consistent backups cannot be restored to an alternate host.

Steps

1. If you are running Data ONTAP 8.1.x, on the secondary site, enter the information to the Transport Protocol Setting (TPS) in the SnapDrive for Windows MMC.
2. From the secondary storage system, connect to all of the LUNs.

   If the secondary storage system is clustered, go to the node where the cluster group, which is the available storage group owner node in the destination cluster, is online and then connect to all of the LUNs from that node in the cluster. Refer to the SnapDrive for Windows documentation for information about mapping LUNs.
3. Depending on your configuration, take one of the following actions:

If the primary storage system is...	Then...
A stand-alone host (SAN)	Connect to all of the mount points and LUNs of the same type on the primary storage system.
A clustered host (SAN)	From the node where the cluster group is online, connect to all of the mount points and LUNs in the cluster.
Data ONTAP 8.1.x configured with a single LUN hosting VMs on a source FlexVol volume (SAN)	For SnapMirror updates to succeed, you must create a second, smaller LUN (10 MB to 100 MB) on the source FlexVol volume before initiating a backup. From the node where the cluster group is online, connect to all of the mount points and LUNs in the cluster.
A stand-alone or clustered host (NAS)	Unmount the Data Protection (DP) volume, mount the DP volume as rewriteable, verify that the volume has RWX permissions, and then create CIFS shares for the different volumes.

4. Reconfigure SnapInfo based on your environment:

Content subject to change

Draft for beta release -- October 2014

If your configuration is...	Then...
SAN	Restore the SnapInfo LUN from its last Snapshot copy.
NAS	Mount the SnapInfo directory.

For NAS, if an `access is denied` error occurs, or if you cannot browse to the exposed SMB share location, you might need to reset the access control list on the share.

Note: This is typical when using the System Center Virtual Machine Manager (SCVMM) Console and Data ONTAP SMI-S Agent.

5. Add the secondary storage system or cluster in the SnapManager for Hyper-V MMC, and then configure it with the SnapInfo path.
6. Enter the following cmdlets:
   a. Enter `Get-VMsFromBackup` to retrieve the list of VMs present in the backup metadata.
   b. Enter `Get-Backup` to get the backup copies for each VM.
7. To restore, use `Restore-Backup` with the VM GUID and the backup copy with the following parameters:

To restore from...	Enter this command...
An alternate host	`Restore-Backup` -Server *`Secondary_host_system_or_cluster_name`* -DisableVerifySnapshot -RestoreToAlternateHost
A listed backup	`Restore-Backup` -Server -VirtualMachinePath -SnapShotFilePath @VHD

For `@VHD`, a VM might have multiple VHDs; make sure that you enter both a source and a destination path pair specified for each VHD.

8. If the secondary host system is a cluster, complete the following steps:
   a. Ensure that the LUNs on which the VMs reside are online on the cluster node that owns the cluster group.
   b. Use the failover PowerShell cmdlets to make the VMs highly available.

Failover examples

`The following example shows a two-cluster setup in which smhv-cluster-01 is the primary site and hv-19-cluster is the secondary site:`

```
PS C:\> Get-VMsFromBackup -Server hv-19-cluster

winxp-x64c-135                593ABA72-
B323-4AF7-9AC6-9514F64C0178
csv1-xp-3                     59B85C68-BAFA-4A49-8E85-
```

Content subject to change

Draft for beta release -- October 2014


```
A201045843F7
vm-w2k8r2sp1
5A248757-872B-4FE7-8282-91C8E9D45CF9
um10_11_dr
5AC1B2A8-6603-4F90-98F5-4F2F435AB0C2
winxp-x64c-30                 5B47D3CF-5D96-495D-9BAB-
FB394392CF31
winxp-x64c-126                5B57EED1-B4F1-45A3-
A649-24C6947CB79C
winxp-x64c-118
5B5D417B-70DC-427C-94BB-97FF81C5B92B
winxp-x64c-122                5BEE26B8-BE57-4879-
A28E-9250A6A5EEFC
csv4-w2k3-19                  5D0613E5-B193-4293-8AAD-
F8B94A5D851F

PS C:\> Get-Backup -Server hv-19-cluster -ResourceName um10_11_dr

BackupName    : smhv-ccb-ds_04-10-2012_10.37.58
RetentionType : hourly
DatasetName   : smhv-ccb-ds
BackupId      : smhv-ccb-ds_04-10-2012_10.37.58
BackupTime    : 4/10/2012 10:37:58 AM
BackupType    : Application consistent
BackedupVMs   : {um10_11_dr}

PS C:\> Restore-Backup -Server hv-19-cluster -ResourceName
um10_11_dr -BackupName smhv-ccb-ds_04-10-2012_10.37.58
-DisableVerifySnapshot -RestoreToAlternateHost
```

The following example shows a SAN restore operation to an alternate path for which N:\ is the destination and I:\ is the source LUN path:

```
PS C:\> Restore-Backup -Resourcename dr-san-ded1
-RestoreToAlternateHost -DisableVerifySnapshot -BackupName
san_dr_09-11-2013_10.57.31 -Verbose
-VirtualMachinePath "N:\dr-san-ded1" -SnapshotFilePath "N:\dr-san-
ded1" -VHDs @(@{"SourceFilePath" = "I:\dr-san-ded1\Virtual Hard
Disks\dr-san-ded1.vhdx"; "DestinationFilePath" = "N:\dr-san-
ded1\Virtual Hard Disks\dr-san-ded1"})
```

The following example shows a NAS restore operation to an alternate path for which \\172.17.162.174\ is the source SMB share path and \\172.17.175.82\ is the destination SMB share path:

```
PS C:\> Restore-Backup -Resourcename vm_claba87_cifs1
-RestoreToAlternateHost -DisableVerifySnapshot -BackupName ag-
DR_09-09-2013_16.59.16 -Verbose
-VirtualMachinePath "\\172.17.175.82\vol_new_dest_share\ag-vm1" -
SnapshotFilePath "\\172.17.175.82\vol_new_dest_share\ag-vm1" -VHDs
```

Content subject to change

Draft for beta release -- October 2014


```
@(@{"SourceFilePath" = "\\172.17.162.174\vol_test_src_share\ag-
vm1\Virtual Hard Disks\ag-vm1.vhdx"; "DestinationFilePath" = "\
\172.17.175.82\vol_new_dest_share\ag-vm1\Virtual Hard Disks\ag-
vm1.vhdx"})
```

Related information

Data ONTAP 8.2 Data Protection Online Backup and Recovery Guide for 7-Mode
Clustered Data ONTAP 8.3 Data Protection Guide
NetApp Documentation: SnapDrive for Windows (current releases)
Clustered Data ONTAP 8.3 File Access Management Guide for CIFS

Reconfiguring storage systems after a disaster recovery failback

After failing over to a secondary storage system, SnapManager for Hyper-V completes disaster recovery by failing back to the original primary storage system. Failing back restores primary storage function to the original primary storage site after its storage systems are reenabled or replaced.

Steps

1. Depending on the condition of the primary storage system, take one of the following actions:

If the primary storage system is...	Then...
Recoverable	Move the data from the secondary host back to the primary storage system.
Completely destroyed	Provision a new storage system.

2. Manage the SnapMirror relationship:
   a. Initialize the SnapMirror relationship from the secondary storage system to the primary storage system to recover the data.
   b. Resynchronize the existing SnapMirror relationship from the secondary storage system to the primary storage system.
   c. Using SnapDrive on the secondary storage system, initiate a SnapMirror update for each of the LUNs or SMB shares on the secondary storage system.
3. Depending on your configuration, take one of the following actions:

Content subject to change

Draft for beta release -- October 2014

If the primary storage system is...	Then...
A stand-alone host (SAN)	Connect to all the mount points and LUNs on the primary storage system of the same type.
A clustered host (SAN)	From the node where the cluster group is online, connect to all the mount points and LUNs in the cluster.
Data ONTAP 8.1.x configured with a single LUN hosting VMs on a source FlexVol volume (SAN)	For SnapMirror updates to succeed, you must create a second, smaller LUN (10 MB to 100 MB) on the source FlexVol volume before initiating a backup job. From the node where the cluster group is online, connect to all the mount points and LUNs in the cluster.
A stand-alone or clustered host (NAS)	Unmount the Data Protection (DP) volume, mount the DP volume as rewriteable, verify that the volume has RWX permissions, and then create CIFS shares for the different volumes.

4. Reconfigure SnapInfo based on your environment:

If your configuration is...	Then...
SAN	Restore the SnapInfo LUN from its last Snapshot copy.
NAS	Mount the SnapInfo directory.

For NAS, if an `access is denied` error occurs, or if you cannot browse to the exposed SMB share location, you might need to reset the ACL on the share.

5. Add the primary host or cluster in SnapManager for Hyper-V MMC and configure it with the SnapInfo path.

6. Enter the following cmdlets:

   a. Retrieve the list of VMs present in the backup metadata by using the `Get-VMsFromBackup` cmdlet.

   b. Get the backup copies for each VM by using the `Get-Backup` cmdlet to get the backup copies for each VM.

7. To restore, use `Restore-Backup` with the VM GUID and the backup copy with the following parameters:

To restore from...	Enter this command...
An alternate host	`Restore-Backup -Server` *`Secondary_host_system_or_cluster_name`* `-DisableVerifySnapshot -RestoreToAlternateHost`
A listed backup copy	`Restore-Backup -Server -VirtualMachinePath -SnapShotFilePath @VHD`

Content subject to change

Draft for beta release -- October 2014

For `@VHD`, a VM might have multiple VHDs; you must enter both a source and a destination path pair specified for each VHD.

8. If the secondary host system is a cluster, complete the following steps:

a. Ensure that the LUNs on which the VMs reside are online on the cluster node that owns the cluster group.

b. Use the failover PowerShell cmdlets to make the VMs highly available.

For NAS, after the VMs are exposed as SMB shares from one cluster node, the VMs are accessible to all hosts configured to use the storage system cluster.

Failback examples

The following example shows a two-cluster setup in which smhv-cluster-01 is the primary site and hv-19-cluster is the secondary site:

```
PS C:\> Get-VMsFromBackup -Server smhv-cluster-01

winxp-x64c-135                 593ABA72-
B323-4AF7-9AC6-9514F64C0178
csv1-xp-3                      59B85C68-BAFA-4A49-8E85-
A201045843F7
vm-w2k8r2sp1
5A248757-872B-4FE7-8282-91C8E9D45CF9
um10_11_dr
5AC1B2A8-6603-4F90-98F5-4F2F435AB0C2
winxp-x64c-30                  5B47D3CF-5D96-495D-9BAB-
FB394392CF31
winxp-x64c-126                 5B57EED1-B4F1-45A3-
A649-24C6947CB79C
winxp-x64c-118
5B5D417B-70DC-427C-94BB-97FF81C5B92B
winxp-x64c-122                 5BEE26B8-BE57-4879-
A28E-9250A6A5EEFC
csv4-w2k3-19                   5D0613E5-B193-4293-8AAD-
F8B94A5D851F

PS C:\> Get-Backup -Server smhv-cluster-01 -ResourceName
um10_11_dr

BackupName    : smhv-ccb-ds_04-10-2012_10.37.58
RetentionType : hourly
DatasetName   : smhv-ccb-ds
BackupId      : smhv-ccb-ds_04-10-2012_10.37.58
BackupTime    : 4/10/2012 10:37:58 AM
BackupType    : Application consistent
BackedupVMs   : {um10_11_dr}
```

Content subject to change

Draft for beta release -- October 2014


```
PS C:\> Restore-Backup -Server smhv-cluster-01 -ResourceName
um10_11_dr -BackupName smhv-ccb-ds_04-10-2012_10.37.58
-DisableVerifySnapshot -RestoreToAlternateHost
```

The following example shows a SAN restore operation to an alternate path for which N:\ is the destination and I:\ is the source LUN path:

```
PS C:\> Restore-Backup -Resourcename dr-san-ded1
-RestoreToAlternateHost -DisableVerifySnapshot -BackupName
san_dr_09-11-2013_10.57.31 -Verbose
-VirtualMachinePath "N:\dr-san-ded1" -SnapshotFilePath "N:\dr-san-
ded1" -VHDs @(@{"SourceFilePath" = "I:\dr-san-ded1\Virtual Hard
Disks\dr-san-ded1.vhdx"; "DestinationFilePath" = "N:\dr-san-
ded1\Virtual Hard Disks\dr-san-ded1"})
```

The following example shows a NAS restore operation to an alternate path for which \\172.17.162.174\ is the source SMB share path and \\172.17.175.82\ is the destination SMB share path:

```
PS C:\> Restore-Backup -Resourcename vm_claba87_cifs1
-RestoreToAlternateHost -DisableVerifySnapshot -BackupName ag-
DR_09-09-2013_16.59.16 -Verbose
-VirtualMachinePath "\\172.17.175.82\vol_new_dest_share\ag-vm1" -
SnapshotFilePath "\\172.17.175.82\vol_new_dest_share\ag-vm1" -VHDs
@(@{"SourceFilePath" = "\\172.17.162.174\vol_test_src_share\ag-
vm1\Virtual Hard Disks\ag-vm1.vhdx"; "DestinationFilePath" = "\
\172.17.175.82\vol_new_dest_share\ag-vm1\Virtual Hard Disks\ag-
vm1.vhdx"})
```

Related information

Data ONTAP 8.2 Data Protection Online Backup and Recovery Guide for 7-Mode
Clustered Data ONTAP 8.3 Data Protection Guide
Clustered Data ONTAP 8.3 File Access Management Guide for CIFS

Restoring the original configuration for standalone hosts

After the VMs are backed up on the primary storage system, you can return to the original configuration using a SnapMirror relationship that is established from the primary storage system to the secondary storage system.

Steps

1. Shut down the VMs running on the secondary storage system.

Content subject to change

Draft for beta release -- October 2014

2. Delete the VMs running on the secondary storage system.
3. Disconnect the SnapInfo disk and the disks containing VMs using SnapDrive.
4. Resynchronize the SnapMirror relationship from the primary storage system to the secondary storage system.

Restoring the original configuration for clustered hosts

After the VMs are backed up on the primary storage system, you can return to the original configuration using a SnapMirror relationship which is established from the primary storage system to the secondary storage system.

Steps

1. Offline the virtual machine resource and virtual machine configuration resource for all the VMs.
2. Delete these resources from the cluster.
3. Delete all the VMs from Hyper-V Manager.
4. Disconnect all the disks by using SnapDrive.
5. Resynchronize the SnapMirror relationship from the primary storage system to the secondary storage system.

Content subject to change

Draft for beta release -- October 2014

Troubleshooting SnapManager for Hyper-V

If you encounter unexpected behavior during the installation or configuration of SnapManager for Hyper-V, you can follow specific troubleshooting procedures to identify and resolve the cause of such issues.

Warning: Current VHD configuration of the VM is different from that at the time of backup

Message

```
Warning: Current VHD configuration of the VM is different from that
at the time of backup. Restoring the VM may result in addition of
VHDs to the VM or may result in making some existing VHDs orphan.
```

Description

This message occurs during a restore operation of an application-consistent backup of a virtual machine (VM) with a Hyper-V checkpoint.

Corrective action

You can safely ignore this message by clicking **OK** to proceed with the restore operation.

VM could not be realized due to errors in its configuration file which could not be resolved

Message

```
VM could not be realized due to errors in its configuration file
which could not be resolved
```

Description

This message occurs when a restore operation from a crash-consistent backup to an alternate path location fails. All of the virtual machine (VM) files are successfully restored but the VM registration fails when a VM has more than one checkpoint. This issue is not applicable to application-consistent backups.

Corrective action

Import the VM from Hyper-V Manager using the Import Virtual Machine wizard.

Content subject to change

Draft for beta release -- October 2014

Backup Failed for the following VM(s) since it cannot be backedup online or No VM to be found for backup

Message

`Backup Failed for the following VM(s) since it cannot be backedup online or NO VM to be found for backup`

Description

This message occurs when backing up a Windows 2012 VM in a Windows 2008 R2 SP1 Hyper-V parent without the `Allow saved state VM` backup option enabled fails.

Corrective action

For Windows 2012 backups, run the backup with the `Allow saved state VM` backup option enabled.

Unexpected error querying for the IVssWriterCallback interface. hr = 0x80070005, Access is denied.

Message

`Unexpected error querying for the IVssWriterCallback interface. hr = 0x80070005, Access is denied.`

Description

If a CSV is owned by the cluster group owner and the VM is owned by the partner node, backup of the VM completes successfully with the VSS error in the application event log. This is often caused by incorrect security settings in either the writer or requestor process.

Corrective action

None: this error message can be ignored.

Backup reports use management console time zone information in report name

Issue

When you generate a backup report using a client host that resides in a different time zone than the parent host, the report name uses the client host time zone information and the report contents use the parent host time zone.

Cause

Content subject to change

Draft for beta release -- October 2014

The timestamp in the backup report name appears with the client host time zone information.

Corrective action

No corrective action is necessary.

Backup and restore notifications not sent in IPv6-only environments

Issue

When you run an IPv6-only host, you do not receive any backup or restore operation notifications.

Cause

Your SMTP server does not support IPv6, or it does not have IPv6 enabled on it.

Corrective action

Enable IPv6 on your SMTP server.

Failover clustering event ID 5121

Message

`Failover clustering event ID 5121` from the application event logs, or the host message `NO_DIRECT_IO_DUE_TO_FAILURE`.

Description

This error message occurs when the cluster shared volume (CSV) is no longer directly accessible from the cluster node, and I/O access redirects to the storage device that owns the volume. This occurs because only the coordination node can perform actions using VSS backups. During backup operations, the coordination node locks the CSV and requires all non-coordination nodes to redirect I/O.

Corrective action

After the operation has been completed, the coordination node releases the lock on the CSV and I/O is no longer be redirected. If the error message occurs only during VSS backups, there is no failure and this is expected behavior.

Virtual machine backups made while a restore operation is in progress might be invalid

Issue

Content subject to change

Draft for beta release -- October 2014

An application-consistent backup created while a restore operation is in progress might be invalid. Restoring a virtual machine from this incomplete backup results in data loss and the virtual machine is deleted.

Cause

The SnapManager for Hyper-V configuration information is missing in the backup copy. The backup operation is successful, but the backup copy is invalid because the virtual machine configuration information is not included. The SnapManager for Hyper-V restore operations delete the virtual machine configuration information from the Hyper-V host before performing a restore operation. This behavior is by design in the Microsoft Hyper-V Writer.

Corrective action

Ensure that the backup schedule does not coincide with the restore operation, or that the on-demand backup you want to perform does not overlap with a restore operation on the same data.

Virtual machine managing itself

Issue

If a virtual machine (VM) belongs to a host that has SnapManager for Hyper-V installed, and you install SnapManager for Hyper-V on that VM to use as a management console, you should not use SnapManager for Hyper-V to manage the host to which the VM belongs.

Cause

SnapManager for Hyper-V on a virtual machine cannot manage itself.

Corrective action

No corrective action necessary.

Example

If VM1 belongs to Host1 (with SnapManager for Hyper-V installed), and you install SnapManager for Hyper-V on VM1, you should not use SnapManager for Hyper-V to manage Host1 from VM1.

If you do this, and try to restore the VM from itself, the VM will be deleted or restarted from Hyper-V Manager.

Connection time is longer with IPv6-only host

Issue

If you are working in a mixed IPv4 and IPv6 environment and you add an IPv6-only host to SnapManager for Hyper-V, the connection might take longer than normal.

Cause

Content subject to change

Draft for beta release -- October 2014

This delay occurs because SnapManager for Hyper-V tries IPv4 protocol first.

Corrective action

To work around this delay, add the host in the `\windows\system32\drivers\etc\hosts` file.

Volume Shadow Copy Service error: An internal inconsistency was detected

Message

```
Volume Shadow Copy Service error: An internal inconsistency was
detected in trying to contact shadow copy service writers. Please
check to see that the Event Service and Volume Shadow Copy Service
are operating properly.
```

Description

When you perform a backup of a virtual machine that uses Windows Server 2003, it repeatedly fails due to a retry error.

Corrective action

Check the Windows Application event log inside the virtual machine for any VSS errors.

Related information

Microsoft Support Article 940184: Error message when you run the "vssadmin list writers" command on a Windows Server 2003-based computer: "Error: 0x8000FFFF"

Web Service Client channel was unable to connect to the ConfigurationManagementService instance on machine smhv51_81clus

Message

```
Web Service Client channel was unable to connect to the
ConfigurationManagementService instance on machine smhv51_81clus.

There was no endpoint listening at net.tcp://smhv51_81clus/
SnapManager/HyperV/ConfigMgmtService/v_10 that could accept the
message. This is often caused by an incorrect address or SOAP
action. See InnerException, if present, for more details.
```

Description

If you export configuration information, the local Web service port settings of the managed hosts are stored in the exported configuration file. If you later have to reinstall

Content subject to change

Draft for beta release -- October 2014

SnapManager for Hyper-V using a different Web service port, and import the former configuration information, you experience connection issues.

Corrective action

To prevent this issue, use the same Web service port settings contained in the exported configuration file when reinstalling SnapManager for Hyper-V.

MSI custom property used in silent installation

Issue

Systems running Windows Server 2008 or Vista with Windows Installer version 4.5 do not recognize the built-in properties of SnapManager for Hyper-V installation.

Corrective action

Use the MSIRESTARTMANAGERCONTROL=Disable command switch parameter with installation.

Related information

Microsoft Developer Network (MSDN) Library

SnapManager for Hyper-V is not licensed on the host or in the Storage System

Message

```
SnapManager for Hyper-V is not licensed on the host or in the
Storage System, backup is aborted
```

Description

This message occurs either when your system is not licensed or when there are issues with enumeration, virtual machine caching, or master boot record (MBR) disk use.

Corrective action

1. Ensure that your system is licensed.
2. Migrate any MBR disks, which SnapManager for Hyper-V does not support, to GUID Partition Table (GPT) disks.
3. Restart SnapManager for Hyper-V.

If this does not resolve the issue, you most likely have an enumeration problem and should contact technical support.

Content subject to change

Draft for beta release -- October 2014

Deleting backups after failover

Message

`The specified backup does not exist for some of the objects in the dataset.`

Description

After failover to a secondary site (site B), you may be unable to delete backups created at the primary site (site A). If you are at a disaster recovery site (site B), and attempt to delete backups made at the primary site (site A), you will be deleting backups from the primary (site A) rather than the disaster recovery site (site B).

Corrective action

After performing disaster recovery operations, only delete backups that were made at your current site of operation.

Storage performance degrades after failed backup

Issue

Storage performance may degrade following a failed backup job.

Cause

If the Microsoft Hyper-V VSS components experience an exception during a backup, the cluster shared volumes (CSVs) might remain in redirected I/O mode, causing I/O overhead and potential bottlenecks within the Windows Failover Cluster. This can lead to overall performance degradation, with the greatest impact to VMs residing on the CSV in redirected I/O mode.

Corrective action

Contact Microsoft Support for assistance with this issue.

Deleted SnapInfo Snapshot copies

Issue

SnapManager for Hyper-V is not maintaining or deleting SnapInfo Snapshot copies.

Cause

After creating a dataset backup, SnapManager for Hyper-V creates a Snapshot copy of the SnapInfo LUN. SnapInfo Snapshot copies are not deleted if the backup is deleted. By default, SnapManager for Hyper-V retains 30 SnapInfo LUN Snapshot copies, replacing the oldest copy with the newest copy each time the newest copy exceeds the 30-copy threshold.

Content subject to change

Draft for beta release -- October 2014

Corrective action

You can configure the number of SnapInfo Snapshot copies you want to retain for each Hyper-V host by using one of the following registry keys:

For stand-alone Hyper-V hosts:
```
key: HKLM\SOFTWARE\NetApp\SnapManager for Hyper-V\Server\<hostname>
DWORD value: snapinfo_snaps_count (number of SnapInfo Snapshot
copies to be retained)
```

For clustered Hyper-V hosts (to be configured on each node in the cluster):
```
key: HKLM\Cluster\SOFTWARE\NetApp\SnapManager for Hyper-V\Server
\<clustername> DWORD value: snapinfo_snaps_count (number of
SnapInfo Snapshot copies to be retained)
```

High memory consumption caused by antivirus solution

Issue

File-level antivirus solutions can cause high memory consumption, which might appear to be a memory leak.

Cause

Under certain conditions, SnapManager for Hyper-V might consume large and steadily increasing amounts of memory due to an incorrectly configured antivirus solution that scans the VM configuration files. When an antivirus solution scans the VM configuration files, an `_InstanceModificationEvent` event displays, which describes the changes. When SnapManager for Hyper-V receives this notification, it triggers an enumeration of storage and VMs with SnapDrive for Windows. In some cases, these events might occur with such rapidity that SnapDrive for Windows is unable to process them, causing SnapManager for Hyper-V to queue them.

Corrective action

Exclude the SnapManager for Hyper-V VM files from being scanned by the antivirus solution.

Space consumption when making two Snapshot copies for each backup

Issue

For every backup containing Hyper-V objects, two Snapshot copies are created, which can lead to concerns over space consumption.

Note: This only applies to application-consistent backups.

Content subject to change

Draft for beta release -- October 2014

Cause

Microsoft Hyper-V VSS Writer creates both VM and application-consistent backup copies within the VMs, with the applications residing on VHDs. To create both software-consistent and VM-consistent backup copies, VSS employs the native autorecovery process, which sets the VM to a state consistent with the software Snapshot copy. Hyper-V VSS writer contacts each VM in the backup, and creates a software-consistent Snapshot copy.

After the Snapshot copies are created, the parent partition creates a VSS Snapshot copy of the entire disk (LUN) that houses these VMs. After the parent partition Snapshot copy is created, VSS requires mounting of the previously created parent partition, to roll each of the VMs back to the software-consistent state and to remove any changes that were made to the VMs after the software Snapshot copy was created. These modifications to the VHDs must be made persistent. Because these Snapshot copies are read-only by default, a new Snapshot copy must be made to retain the updated copies of the VHDs. For this reason, a second Snapshot copy of the volume is created. This Snapshot copy is labeled with the suffix **_backup** and is the backup copy used in restore operations.

Corrective action

The two Snapshot copies are considered a pair. When the retention period ends for the backup, both of the Snapshot copies are deleted. You should not manually delete the first Snapshot copy, because it is necessary for restore operations.

Microsoft VSS supports backing up VMs only on the host that owns the Cluster Shared Volume (CSV), so CSV ownership moves between the nodes to create backups of the VMs on each host in the cluster.

When backing up a CSV, SnapManager for Hyper-V creates two Snapshot copies per host in the cluster that runs a VM from that CSV. This means that if you back up 15 VMs on a single CSV, and those VMs are evenly split across three Hyper-V Servers, there is a total of six Snapshot copies per backup.

SnapDrive SDDiscoveryFileSystemListInfo response is null while backing up

Issue

You receive the error `SnapDrive SDDiscoveryFileSystemListInfo response is null while backing up`.

Cause

This message occurs when the SnapInfo location to which you are backing up is not available.

Corrective action

Verify that the SnapInfo location exists and is available. If it has changed, re-run the configuration manager to specify the new location. Attempt the backup again.

Content subject to change

Draft for beta release -- October 2014

Related tasks

Setting up a SnapInfo LUN on page 33

Error: Vss Requestor - Backup components failed

Message

The following error message is displayed in the SnapManager for Hyper-V report and the Windows Event log: `Error: Vss Requestor - Backup Components failed. Writer Microsoft Hyper-V VSS Writer involved in backup or restore encountered a retryable error. Writer returned failure code 0x800423f3. Writer state is XXX. For more information, see the Hyper-V-VMMS event log in the Windows Event Viewer.`

Description

If you receive a VSS retry error that causes your application-consistent backup to fail, SnapManager for Hyper-V retries the backup three times with a wait of one minute between each attempt.

Corrective action

You can configure the number of retries (retry count) and the duration of wait time between the retries (retry interval) using the following registry keys:

`Key: HKLM\System\CurrentControlSet\Services\OnCommandHyperV \Parameters DWORD value in seconds: vss_retry_sleep (The time duration to wait between retries) DWORD value: vss_retry (Number of retries)`

These settings are at the Hyper-V host level and the keys and values should be set on the Hyper-V host for each virtual machine. If the virtual machine is clustered, the keys should be set on each node in the cluster.

You must restart SnapManager for Hyper-V after making changes to or adding these registry keys.

Vss Requestor - Backup Components failed. An expected disk did not arrive in the system

Cause

This message occurs when you back up a dataset using SnapManager for Hyper-V and the following error appears in the Windows Application event log on the Hyper-V host.

Content subject to change

Draft for beta release -- October 2014


```
A Shadow Copy LUN was not detected in the system and did not
arrive.

     LUN ID     guid

     Version      0x0000000000000001
     Device Type    0x0000000000000000
     Device TypeModifier  0x0000000000000000
     Command Queueing 0x0000000000000001
     Bus Type   0x0000000000000006
     Vendor Id    vendor
     Product Id   LUN
     Product Revision   number
     Serial Number    serial_number

     Storage Identifiers
     Version    0
     Identifier Count 0



    Operation:
       Exposing Disks
       Locating shadow-copy LUNs
       PostSnapshot Event
       Executing Asynchronous Operation

    Context:
       Execution Context: Provider
       Provider Name: Data ONTAP VSS Hardware Provider
       Provider Version: 6. 1. 0. 4289
       Provider ID: {ddd3d232-a96f-4ac5-8f7b-250fd91fd102}
   Current State: DoSnapshotSet
```

Corrective action

Retry the dataset backup.

Vss Requestor - Backup Components failed with partial writer error

Message

```
Error: Vss Requestor - Backup Components failed with partial
writer error.
Writer Microsoft Hyper-V VSS Writer involved in backup or
restore
operation reported partial failure. Writer returned failure code
0x80042336. Writer state is 5.
Application specific error information:
Application error code: 0x1
Application error message: -
```

Content subject to change

Draft for beta release -- October 2014


```
Failed component information:
Failed component: VM GUID XXX
    Writer error code: 0x800423f3
    Application error code: 0x8004230f
    Application error message: Failed to revert to VSS snapshot
on the
    virtual hard disk 'volume_guid' of the virtual machine
'vm_name'.
   (Virtual machine ID XXX)
```

The following errors appear in the Windows Application event log on the Hyper-V host:

```
Volume Shadow Copy Service error: Unexpected error calling
routine
GetOverlappedResult.  hr = 0x80070057, The parameter is
incorrect.

Operation:
   Revert a Shadow Copy

Context:
   Execution Context: System Provider

Volume Shadow Copy Service error: Error calling a routine on a
Shadow
Copy Provider
{b5946137-7b9f-4925-af80-51abd60b20d5}. Routine details
RevertToSnapshot
[hr = 0x80042302, A Volume Shadow Copy Service component
encountered
an unexpected
error.
Check the Application event log for more information.].

Operation:
   Revert a Shadow Copy

Context:
   Execution Context: Coordinator
```

Description

This message appears when performing an application-consistent backup of a dataset. This error causes the backup to fail for some of the virtual machines in the dataset.

Corrective action

- Retry the dataset backup.
- If the retry attempt fails again, split the dataset into two datasets so that all the VMs whose backup failed will be placed into a single dataset and all other VMs will be put into another dataset. Then run the backup again.

Content subject to change

Draft for beta release -- October 2014

VSS returns errors against Microsoft iSCSI Target VSS Hardware Provider during NAS backup

Issue

While performing a NAS backup, the following errors might occur:

```
Vss Requestor - Backup Components failed. Failed to add volume
[example] to snapshot set. The shadow copy provider had an
unexpected error while trying to process the specified operation.
```

```
Volume Shadow Copy Service error: Error creating the Shadow Copy
Provider COM class with CLSID [example]. Access is denied.
```

Cause

These errors occur during a NAS application-consistent backup. NAS backup does not fail, but VSS logs some errors related to Microsoft iSCSI Target VSS Hardware Provider.

Corrective action

The backup has not failed; you can safely ignore these errors.

Vss Requestor - Backup Components failed. Failed to call keep snapshot set.

Error

```
Vss Requestor - Backup Components failed. Failed to call keep
snapshot set. Reason Index and count must refer to a location
within the string.
```

Description

This error occurs when VMs in a backup job reside on a Storage Virtual Machine and CIFS server with the same name.

Corrective action

None available for this release.

Failure example

1. Create a Storage Virtual Machine and CIFS server with the same name: for example, “test1”.
2. Add the test1 name to the DNS with both IP addresses.
3. On a Windows Server 2012 host, install SnapManager for Hyper-V and create some VMs using the CIFS shares from test1.

Content subject to change

Draft for beta release -- October 2014

4. Create a backup copy that includes those VMs.
5. Note that the backup job fails with the error `Backup Components failed. Failed to call keep snapshot set. Reason Index and count must refer to a location within the string.`

MBR LUNs unsupported in SnapManager for Hyper-V

Issue

SnapManager for Hyper-V does not support MBR LUNs for virtual machines running on shared volumes or cluster shared volumes.

Cause

A Microsoft API issue returns different volume GUIDs when the cluster shared volume disk ownership changes. The volume GUID is not the same as the GUID in the cluster disk resource property. This issue also applies to virtual machines made highly available using Microsoft Failover clustering.

Corrective action

See the Microsoft Knowledge Base.

Related information

Microsoft Support Article 2006163: On Microsoft Server 2008 R2 Volume GUID changes for shared MBR disks with drive letters using GetVolumeNameForVolumeMountPoint, ClusterGetVolumeNameForVolumeMountPoint and ClusterPrepareSharedVolumeForBackup APIs

Backup fails after you remove a virtual machine from Hyper-V Manager

Issue

After you remove a Hyper-V virtual machine (VM) from Hyper-V Manager, backup operations fail if you do not update the dataset associated with the VM.

Cause

This issue occurs when you remove a Hyper-V VM from Hyper-V Manager and attempt a backup without modifying the dataset. Additionally, if you re-created a VM, you must modify the dataset. SnapManager for Hyper-V creates datasets based on the VM ID (GUID). The backup fails when a VM is deleted, removed, or re-created, which creates a new GUID. Although this does not trigger the failure of the entire backup process, if a VM is deleted, and then re-created with the same name, it is not automatically protected by SnapManager for Hyper-V.

Content subject to change

Draft for beta release -- October 2014

Corrective action

Remove the VM from the dataset list of VMs, and add any re-created VMs to the dataset.

Related concepts

Configuring datasets on page 35

Related tasks

Modifying a dataset on page 37

Some types of backup failures do not result in partial backup failure

Issue

If one virtual machine in a dataset has an error, SnapManager for Hyper-V does not successfully complete the dataset backup, and in some scenarios, does not generate a partial failure. In these situations, the entire dataset backup fails.

Example

In a scenario where one storage system volume exceeds the 255 Snapshot copy limit, SnapManager for Hyper-V generates a partial failure even though the problem is associated with a subset of virtual machines in the dataset.

Corrective action

To successfully complete the backup operation, you need to fix the virtual machine that has the issue. If that is not possible, you can temporarily move the virtual machine out of the dataset, or create a dataset that only contains virtual machines known not to have a problem.

Restore failure after storage system volume renaming

Message

```
Some of the storage system snapshots required to restore the VM are
missing or inconsistent.
```

Description

If storage system volumes are renamed, you cannot restore a virtual machine (VM) from its backup that was created prior to renaming volumes.

Corrective Action

If storage system volumes are renamed and you need to restore a VM from a backup created prior to renaming volumes, then complete the following:

Content subject to change

Draft for beta release -- October 2014

- While restoring a VM from MMC, make sure that "Enable Snapshot Verification" option is unchecked in the **Restore Options** page of the Restore wizard.
- While restoring a VM by using PowerShell, make sure that `-DisableVerifySnapshot` parameter is specified.

Restoring from a backup after failback

Issue

If you perform a failover and failback, you may not be able to restore VMs on your primary site from a backup created on the same primary site, before the failover.

Cause

Snapshot copy verification uses volume GUIDs. GUIDs changes after disaster recovery.

Corrective Action

You can disable the `Verify Snapshots` option through the PowerShell or the Restore wizard:

- Uncheck the "Enable Snapshot Verification" option in the **Restore Options** page of the Restore wizard.
- Using PowerShell, make sure that `-DisableVerifySnapshot` parameter is specified.

Related tasks

Restoring a virtual machine from a backup copy on page 57

Web Service Client channel unable to connect while updating the dataset to the new node

Issue

If a Web Services Client is not explicitly started, it will fail to connect to SnapManager for Hyper-V.

Cause

SnapManager for Hyper-V no longer automatically starts a Web Services Client channel. If the Web Service Client channel is unable to connect while updating a dataset to a new node, it may be for one of the following reasons:

- Web Services has not been started.
- SnapManager for Hyper-V is not installed.

Content subject to change

Draft for beta release -- October 2014

- The Web Services host is down.

Corrective action

To correct this behavior, be sure you have performed the following tasks:

- Start Web Services.
- Install SnapManager for Hyper-V.
- Restart the Web Services host.

Datasets are not automatically replicated to new nodes in a Windows Failover Cluster

Issue

After adding new nodes to a Windows Failover Cluster, datasets are not automatically transferred to the new node.

Cause

When adding new nodes to a Windows Failover Cluster, SnapManager for Hyper-V does not automatically replicate the existing datasets to the new nodes in the cluster.

Corrective action

Run the Modify Dataset wizard and click **Update Schedule Policies to all the Dataset member nodes** on the Basic Details page.

This wizard must be run for each dataset that has virtual machines.

Related tasks

Modifying a dataset on page 37

Error 1935. An error occurred during the installation of assembly component

Message

```
Error 1935. An error occurred during the installation of assembly
component {2A030FEB-29B5-314B-97B5-ED38673CC885}. HRESULT:
0x80070BC9.
```

Description

This message occurs when the SnapManager for Hyper-V installer fails as a result of the Hyper-V system not being restarted after you install or uninstall Microsoft hotfixes.

Corrective action

Content subject to change

Draft for beta release -- October 2014

Restart your computer and run the SnapManager for Hyper-V installer again.

Backup jobs that involve more than 15 CSVs from the same storage system might fail

Issue

SnapManager for Hyper-V backup jobs that involve more than 15 Cluster Shared Volumes (CSVs) from the same storage system fail with the following error:

```
Failed to rename the Snapshot copy of the LUN to the new
Snapshot copy name.
Error code: The attempt to get the named attribute for the LUN
on the storage system failed.
Error code: 13057.
Error description: An error occurred in the reception and
processing of the API reply from the appliance.
```

Cause

This is a limitation caused by Data ONTAP to prevent a hold of system resources. The limitation of 15 LUNs is applicable only when all of the LUNs belong to the same storage system. If a backup dataset is created so that no more than 15 CSVs are involved from one storage system, then this issue does not occur.

Corrective action

If you want to make a backup that includes more than 15 LUNs from the same storage system, create multiple datasets to avoid this failure.

Either the specified VM(s) are not present or they cannot be backed up online

Message

`Either the specified VM(s) are not present or they cannot be backed up online`

Description

One reason this message occurs is when application-consistent backups fail if the pass-through disk size on the VM is less than 300 MB. Your error log will resemble the following example:

```
Log Name:      Application
Source:        SnapMgrServiceHost
Date:          11/12/2012 12:24:28 PM
Event ID:      106
Task Category: Backup Event
```

Content subject to change

Draft for beta release -- October 2014


```
Level:         Error
Keywords:      Classic
User:          N/A
Computer:      defiant16.wak-qa.com
Description:
SnapManager for Hyper-V backup failed to complete

Backup Failed for the following VM(s) since it cannot be
backedup online or No VM to be found for backup
               VM Name: demovm-0
```

There are no other application or system error messages to indicate the failure.

Corrective action

You can either resize the pass-through disk to be larger than 300 MB or run the backup with the `Allow saved state VM backup` option enabled.

Note: This corrective action is applicable in both SAN and NAS environments.

Message

`Either the specified VM(s) are not present or they cannot be backed up online`

Description

A second reason this message occurs is because Windows cannot perform an online backup of this system because the `scoped snapshots` option for Hyper-V VMs is enabled. Scoped snapshots are mainly used by Windows critical updates.

Corrective action

You must disable the `scoped snapshots` option by creating a DWORD ScopeSnapshots parameter with value 0 in:

`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\SystemRestore\`

Note: This corrective action is applicable in both SAN and NAS environments.

Required hotfix KB2263829 cannot be installed on some platforms

Issue

While installing SnapManager for Hyper-V, attempting to install hotfix KB2263829 might fail for Windows Server 2008 R2 SP1. The installer states that the hotfix is not applicable for this server.

Cause

The hotfix is not supported for your platform.

Content subject to change

Draft for beta release -- October 2014

Corrective action

Open a support case with Microsoft and resolve the issue with Microsoft.

Backup failure with the error “Shadow copy creation is already in progress”

Message

```
SnapManager for Hyper-V backup failed to complete
Backup of the Dataset Name: example
Backup id: c1bb4b28-c76c-4001-85fd-ffdfdb5737c9 failed to execute
Error: Vss Requestor - Backup Components failed. Failed to add
volume \\CIFS_USER_SER\USER_SHARE2\ to snapshot set. Another
shadow copy creation is already in progress. Wait a few moments
and try again.
```

Description

This issue occurs because a previous backup is not aborted and is still active. Use the following command to check for any entries listed:

`cifs share show -shadowcopy`

Corrective action

Abort the previous backup job and retry the operation.

Content subject to change

Draft for beta release -- October 2014

Copyright information

Copyright © 1994–2014 NetApp, Inc. All rights reserved. Printed in the U.S.

No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

Content subject to change

Trademark information

NetApp, the NetApp logo, Go Further, Faster, ASUP, AutoSupport, Campaign Express, Cloud ONTAP, clustered Data ONTAP, Customer Fitness, Data ONTAP, DataMotion, Fitness, Flash Accel, Flash Cache, Flash Pool, FlashRay, FlexArray, FlexCache, FlexClone, FlexPod, FlexScale, FlexShare, FlexVol, FPolicy, GetSuccessful, LockVault, Manage ONTAP, Mars, MetroCluster, MultiStore, NetApp Insight, OnCommand, ONTAP, ONTAPI, RAID DP, SANtricity, SecureShare, Simplicity, Simulate ONTAP, Snap Creator, SnapCopy, SnapDrive, SnapIntegrator, SnapLock, SnapManager, SnapMirror, SnapMover, SnapProtect, SnapRestore, Snapshot, SnapValidator, SnapVault, StorageGRID, Tech OnTap, Unbound Cloud, and WAFL are trademarks or registered trademarks of NetApp, Inc., in the United States, and/or other countries. A current list of NetApp trademarks is available on the web at *http://www.netapp.com/us/legal/netapptmlist.aspx*.

Cisco and the Cisco logo are trademarks of Cisco in the U.S. and other countries. All other brands or products are trademarks or registered trademarks of their respective holders and should be treated as such.

Draft for beta release -- October 2014

How to send your comments

You can help us to improve the quality of our documentation by sending us your feedback.

Your feedback is important in helping us to provide the most accurate and high-quality information. If you have suggestions for improving this document, send us your comments by email to *doccomments@netapp.com*. To help us direct your comments to the correct division, include in the subject line the product name, version, and operating system.

You can also contact us in the following ways:

- NetApp, Inc., 495 East Java Drive, Sunnyvale, CA 94089 U.S.
- Telephone: +1 (408) 822-6000
- Fax: +1 (408) 822-4501
- Support telephone: +1 (888) 463-8277

Content subject to change

Draft for beta release -- October 2014

Index

A

add
  policies *41*
adding
  a Hyper-V parent host *26*
  a Hyper-V parent host cluster *26*
  host clusters *24*
  hosts *24*
Antivirus *75*
application event log
  VSS error messages *69*
application-consistent backups
  failure troubleshooting *85*

B

backup
  defined *49*
  manually *52*
  NAS, VSS errors during *80*
  on-demand *49*
  scheduled *49*
backup applications
  using VSS with *45*
backup copies
  restoring virtual machines from *55*
backup error
  Windows 2012 *69*
  Windows 2012 R2 *69*
backup jobs
  aborted due to licensing issue *73*
  failing due to CSVs on the same storage system *85*
  managing on-demand *49*
  managing scheduled *49*
  monitoring *53*
  saved-state *52*
  troubleshooting failure *85*
  types of *49*
  VSS requestor error *80*
backup operation notifications
  issue of not being sent in IPv6-only environments *70*
backup report names
  issue with including misleading time zone *69*
backup reports
  issue with misleading time zone in report name *69*
backup retention
  and space consumption issues *75*
Backup wizard
  prerequisites to using *50*
backups
  deleting *74*
  failure *69*
Backups
  deleting *53*, *83*
  failed *74*
  failure after removing VM *81*
backups, invalid
  made during restore operation *70*
backups, Snapshot copies
  retention and space consumption issues *75*

C

Cluster Shared Volume
  See CSV
Cluster Shared Volume File System (CSVFS) *45*
clustered environment
  restoring virtual machines within *55*
command line switches
  list of used for silent installation *19*
comments
  how to send feedback about documentation *90*
configuration
  exporting *31*
  host, using SnapManager for Hyper-V *24*
  importing *31*
  SnapManager for Hyper-V *23*
Configuration wizard
  using to control SnapInfo directory path settings *34*
configure
  datasets *35*
  policies *38*
configuring
  for failover *59*
connection failure
  Web Services *83*
create
  datasets for virtual machine resources *36*
Create Dataset wizard
  prerequisites to using *35*
Create Policy wizard

Content subject to change

Draft for beta release -- October 2014

preparing to use *38*
CSV 2.0
changes to architecture *45*

D

dashboard
described *23*
settings *23*
data backup
installing SnapManager for Hyper-V *18*
data management
concepts *9*
datasets *9*
Hyper-V hosts *9*
management consoles *9*
replication policies *9*
retention policies *9*
scheduling policies *9*
unprotected resources *9*
using virtual machines *9*
Data ONTAP requirements
for host-based licensing *13*
for storage system licensing *13*
for storage system licensing with a vFiler unit *13*
data restoration
installing SnapManager for Hyper-V *18*
data servers
using VSS with *45*
dataset
viewing *37*
dataset backup
failure *77*
prerequisites to performing *50*
dataset configuration information
exporting *31*
dataset information
importing *31*
datasets
acceptable characters *35*
configure *35*
creating for virtual machine resources *36*
defined *9*
delete *37*
modifying *37*
name and description *35*
on-demand backup *52*
updating *83*
Datasets
not replicated to WFC nodes *84*
delete
datasets *37*
VMs from a non-Data ONTAP host *31*
deleting
policies *42*
reports *44*
Deleting
backups *53*
Deleting backups *74*, *83*
directory path, SnapInfo
setting *34*
directory settings, SnapInfo
path *34*
disaster recovery
configuring SnapManager for Hyper-V for *59*
failing back to the original primary storage system *63*
failing over to a secondary storage system *60*
requirements for *59*
restoring the original configuration *66*
Disaster recovery
deleting backups after *74*, *83*
restoring configuration *67*
documentation
how to send feedback about *90*

E

email notifications
issue of not being sent in IPv6-only environments *70*
Error 1935
description and action *84*
Error 5121 *70*
error messages
backup fails *69*
Either the specified VM(s) are not present or they cannot be backed up online *85*
Failover clustering event ID 5121
no_direct_IO_due_to_failure *70*
Operation failed. Exiting progress message processing. *68*
Vss Requestor - Backup Components failed *80*
Error messages
SnapDrive *76*
SnapInfo *76*
errors
Error 1935 *84*
event ID 5121 *70*
Snapdrive SDDiscoveryFileSystemListInfo response is null *33*

Content subject to change

Draft for beta release -- October 2014

SnapInfo *33*
VSS *69*
Web Service Client channel was unable to connect *72*
errors, licensing
causing backup jobs to fail *73*
event logs *77*
event notification settings *32*
export from non-Data ONTAP hosts
VMs *28*

F

failback *59*
Failback
deleting backups after *83*
failing back
to the original primary storage system for disaster recovery *63*
failing over
to a secondary storage system for disaster recovery *60*
failover
configuring SnapManager for Hyper-V for *59*
Failover
deleting backups after *74*
Failover cluster
new datasets *84*
failure
dataset backup *77*
failures
solutions to *68*
feedback
how to send comments about documentation *90*

H

host
adding a Hyper-V *26*
IPv6-only connection time issues *71*
host cluster
adding a Hyper-V *26*
host clusters
requirements for adding *24*
host configuration
event notification settings *32*
report path settings *32*
when to configure SnapInfo settings *33*
host configuration information
exporting *31*
importing *31*
host information *31*
host licensing errors
causing backup jobs to fail *73*
hosts
configuration using SnapManager for Hyper-V *24*
requirements for adding *24*
hotfix
not applicable *86*
hotfix installation
troubleshooting *86*
hotfix KB2263829
not applicable *86*
hotfixes
Windows Server 2008 R2 *14*
Windows Server 2008 R2 SP1 *14*
Windows Server 2012 *14*
Hyper-V parent host
removing *32*
Hyper-V parent host cluster
removing *32*
Hyper-V parent hosts
defined *9*
described *13*
installation requirements *13*

I

I/O
redirected *70*
I18N
See internationalization
import to Data ONTAP hosts
VMs *29*
information
how to send feedback about improving documentation *90*
installation
Error 1935 *84*
licenses required *14*
list of command line switches used for silent *19*
of remote hosts *15*
order for SnapManager for Hyper-V and SnapDrive for Windows *18*
SnapManager for Hyper-V is not licensed on the host *18*
installation package
downloading *17*
installation requirements
for Hyper-V parent hosts *13*

Content subject to change

Draft for beta release -- October 2014

licensing *14*
SnapManager for Hyper-V *18*
Installation wizard
list of requirements *12*
installation, remote
performing *19*
installation, silent
list of CLI switches used for *19*
installation, system
troubleshooting *73*
using MSI custom property *73*
installing
hotfix installation failure *86*
internationalization
languages supported *13*
IPv6-only environments
issue with preventing notification emails *70*
IPv6-only host
connection time *71*
issues
backing up a VM fails *69*
backup and restore notifications not sent *70*
backup report name contains misleading time zone *69*
Error 1935 *84*
registering a VM fails *68*
space consumption with two Snapshot copies per backup *75*
Web service connection *72*

L

license requirements
Data ONTAP version *13*
licenses
host-based *14*
installing *14*
required Data ONTAP versions *13*
storage system *14*
types *13*
licensing errors
causing backup jobs to fail *73*
limitations
SnapManager 2.1 for Hyper-V *8*
LUNs
SnapInfo settings *33*

M

manage
reports *43*
managing
storage connection settings *26*
manual backups
decisions to make before performing *50*
manually back up
datasets *52*
MBR LUNs
unsupported *81*
Memory
leak *75*
messages
SnapManager for Hyper-V is not licensed *73*
Web Service Client channel was unable to connect *72*
Microsoft hotfixes
Windows Server 2008 R2 *14*
Windows Server 2012 *14*
Windows Server R2 SP1 *14*
migration
VM *27*
modify
datasets *37*
monitor
backup jobs *53*
monitoring
dashboard settings *23*
multiple management consoles
exporting *31*
importing *31*

N

NAS backup
VSS Hardware Provider errors during *80*
notifications
issue with not being sent in an IPv6-only environment *70*

O

on-demand backup
acceptable characters *50*
naming *50*
on-demand backup jobs
defined *49*
original primary storage systems
failing back to, for disaster recovery *63*

Content subject to change

Draft for beta release -- October 2014

P

parent host
removing Hyper-V *32*
parent host cluster
removing Hyper-V *32*
Partial backup failure
issues *82*
partial writer error
VSS requestor *77*
Partial writer error
VSS requestor *78*
Performance *74*, *75*
plug-in uninstallation
using a wizard *22*
policies
add *41*
configure *38*
deleting *42*
requirements to meet before adding *38*
viewing *42*
policy naming
acceptable characters *38*
primary storage systems
failing back to original, for disaster recovery *63*

R

redirected I/O *70*
registration failure, VM host
troubleshooting *68*
Remote Host Install wizard
requirements for using *15*
using for remote installation or uninstallation *19*
remote hosts
installing *15*
remote installation
performing *19*
remote uninstallation
performing *19*
removal
of Hyper-V parent host *32*
of Hyper-V parent host cluster *32*
replication policies
defined *9*
requirements to meet before adding *38*
report path settings
configuration *32*
reports
deleting *44*
manage *43*
view *43*
viewing configuration *44*
viewing database backup *43*
viewing host *44*
viewing recovery *43*
required hotfixes
Windows Server 2008 R2 *14*
Windows Server 2008 R2 SP1 *14*
Windows Server 2012 *14*
requirements
to use Data ONTAP with SnapManager for Hyper-V *13*
Restore failure *82*
restore operation
affect on backups made during *70*
virtual machines *57*
warning message *68*
restore operation error
registering VM on host failed *68*
restore operation notifications
issue of not being sent in IPv6-only environments *70*
restore operations
on virtual machines *55*
restoring virtual machines
decisions to make *55*
retention policies
defined *9*
requirements to meet before adding *38*
retention, Snapshot copies
and space consumption issues *75*

S

saved-state backup
how SnapManager for Hyper-V handles *52*
schedule policies
defined *9*
scheduled backup jobs
defined *49*
scheduling policies
requirements to meet before adding *38*
secondary storage systems
failing over to *60*
settings
SnapInfo *33*
silent installation
list of command line switches used for *19*
SMB 3.0
remote VSS *46*

Content subject to change

Draft for beta release -- October 2014

SnapDrive
error messages *76*
SnapInfo
error messages *76*
LUN setup *33*
settings *33*
Snapdrive SDDiscoveryFileSystemListInfo response is null error *33*
Snapshot copies *74*
SnapInfo directory configuration settings
when to set *33*
SnapInfo directory path
setting *34*
SnapInfo settings action
using to control SnapInfo directory path settings *34*
SnapManager 2.1 for Hyper-V
limitations *8*
SnapManager for Hyper-V
common tasks and goals *7*
configuration *23*
defined *7*
downloading *17*
installation considerations *17*
installing *18*
list of requirements before installing *12*
troubleshooting *68*
uninstalling *22*
uninstalling by using the Windows Control Panel *22*
Snapshot copies
deleted *74*
lost *74*
missing *74*
not retained *74*
retention and space consumption issues *75*
Snapshot verification *83*
software
downloading *17*
space consumption
issue with two Snapshot copies per backup *75*
storage connection settings
managing *26*
storage management
using VSS with *45*
Storage system volume
renaming *82*
storage systems
failing back to original primary, for disaster recovery *63*
suggestions
how to send feedback about documentation *90*
system installation
troubleshooting *73*
using MSI custom property *73*

T

time zones
issue with misleading in backup report name *69*
troubleshooting
application-consistent backup failures *85*
backup failure *87*
backup job failures *85*
deleted SnapInfo Snapshot copies *74*
Error 1935 *84*
Failover clustering event ID 5121 *70*
failure to back up a VM *69*
failure to register a VM *68*
invalid backups made during restore operations *70*
no_direct_IO_due_to_failure *70*
restore operation warning message *68*
shadow copy creation *87*
Windows scoped snapshots *85*
Troubleshooting
restore *82*

U

uninstallation
of SnapManager for Hyper-V by using the Windows Control Panel *22*
using a wizard *22*
uninstallation, remote
performing *19*
unprotected resources
defined *9*
unsupported
MBR LUNs *81*

V

view
reports *43*
virtual machines *27*
VMs *27*
viewing
dataset *37*
dataset backup report *43*
host report *44*
Hyper-V parent host
Hyper-V parent host cluster *27*

Content subject to change

Draft for beta release -- October 2014

policies *42*
schedule policies
backup and restore jobs *53*
virtual machine backup report *43*
virtual machine recovery report *43*
virtual machines, belonging to a dataset *37*
virtual machines
decisions before restoring *55*
defined *9*
invalid backups *70*
restore operations affecting backups *70*
restoring *57*
view *27*
VM
managing itself *71*
VM host registration failure
troubleshooting *68*
VMs
configuration files *75*
exporting from non-Data ONTAP hosts *28*
importing to Data ONTAP hosts *29*
invalid backups made during restore operation *70*
migrating *27*
view *27*
VSS
access is denied *69*
backup components failed *80*
backup job error *80*
error messages *69*
hardware provider *47*
hardware requirement *47*
how SnapManager for Hyper-V uses *47*
requestor error *77*, *78*
retry error *72*
using to prepare for application-consistent backups *47*
verifying provider used *48*
viewing installed providers *47*
VSS components
described *45*

W

warning message
Current VHD configuration of the VM is different from that at the time of backup *68*
Warning: Current VHD configuration... message
troubleshooting *68*
Web service connection
issues with reinstalling *72*
Web Services *83*
Windows 2012
backing up a VM fails *69*
Windows 2012 R2
backing up a VM fails *69*
Windows Application event logs *77*
Windows Control Panel
using to uninstall SnapManager for Hyper-V *22*
Windows scoped snapshots
troubleshooting *85*
Windows Server 2008 R2
hotfixes required *14*
Windows Server 2008 R2 SP1
hotfixes required *14*
Windows Server 2012
CSV changes *45*
hotfixes required *14*
wizards
Remote Host Install *15*

Content subject to change