TECHNICAL PAPER

HITACHI
Inspire the Next

Protecting Microsoft® Hyper-V® Environments with IntelliSnap in Hitachi Data Protection Suite, Powered by CommVault

Tech Note

By Steven Burns

October 14, 2014

Windows Server 2012 Certified

Hitachi Data Systems

Feedback

Hitachi Data Systems welcomes your feedback. Please share your thoughts by sending an email message to SolutionLab@hds.com. To assist the routing of this message, use the paper number in the subject and the title of this white paper in the text.

Table of Contents

Protecting Microsoft® Hyper-V® Environments with IntelliSnap in Hitachi Data Protection Suite, Powered by CommVault

Tech Note

This paper documents how to configure IntelliSnap backup in Hitachi Data Protection Suite, powered by CommVault, to protect virtual machines in a Microsoft® Hyper-V® environment. It describes two methods for protecting virtual machines.

- Protection at the virtual machine level using operating system and application iDataAgents installed on the virtual machine
- Protection at the Hyper-V host level using the virtual server agent (VSA) iDataAgent

For this tech note, the following scenarios were tested.

Table 1. Test Scenarios

Backups performed on	*Hyper-V Host Configuration*	*VHD Location*
Guest (virtual machine)	Standalone Hyper-V host	Host volume
		Pass-through disk
	Hyper-V hosts in Failover Cluster	Host volume
		Cluster shared volume (CSV)
		Pass-through disk
Hyper-V host	Standalone Hyper-V host	Host volume
		Pass-through disk
	Hyper-V hosts in Failover Cluster	Host volume
		Cluster shared volume (CSV)
		Pass-through disk

In a production environment, the method you choose for a specific virtual machine depends on many variables. For example, for a database server that has a small database and a low transaction rate, protecting it at the host level using the virtual server agent may be the best choice. For a large database server with multiple databases and high transaction rate using pass through disks, protecting it at the virtual machine level may be the best choice.

Note — Testing of this configuration was in a lab environment. Many things affect production environments beyond prediction or duplication in a lab environment. Follow the recommended practice of conducting proof-of-concept testing for acceptable results in a non-production, isolated test environment that otherwise matches your production environment before your production implementation of this solution.

Hitachi Data Protection Suite IntelliSnap Overview

IntelliSnap backup enables you to create a point-in-time snapshot of the data used for backups. An effective way to back up live data is to quiesce it temporarily, take a snapshot, and then resume live operations. IntelliSnap backup works in conjunction with Hitachi storage systems to provide snapshot functionality for backup.

You can use the IntelliSnap backup to perform any level of backups: full, incremental, or differential. When you switch from a snap to a traditional backup or vice-versa, the next job is converted to a full backup. When you perform an IntelliSnap backup or any subsequent operation, you can use a proxy server to reduce the load on the production server. The backup copy operation uses the proxy to move the snap to backup media.

IntelliSnap can be used to create snapshots at the Microsoft Hyper-V host level or at the virtual machine level. When used at the Hyper-V host level using the virtual server agent, large number of virtual machines can be backed up quickly. The virtual server agent allows you to filter the virtual machines backed up by a specific job by multiple criteria.

IntelliSnap uses the VSS Hardware Provider for Microsoft Windows Server® 2012 clients that is installed as part of the Hitachi Data Protection Suite where it is required.

Hitachi Data Protection Suite Configuration Requirements

There are specific configuration requirements when using IntelliSnap to perform backups and restores in a Hitachi Data Protection Suite environment.

Hitachi Data Protection Suite version 10 with service pack 7 or later is required. Installations of version 10 with earlier service pack levels patched to service pack 7 will work, but see Recommended Practices for possible issues when installing software from the CommCell console in Hitachi Data Protection Suite to clients. Additional hot fixes may be required, depending on the Microsoft Windows Server updates installed on the client servers. Make sure that hot fix level is consistent across the Hitachi Data Protection Suite environment.

If backups are to be performed at the virtual machine (guest operating system) level, the following requirements exist:

- These Hitachi Data Protection Suite packages must be installed on the virtual machine:
  - MediaAgent
  - File System iDataAgent
  - Application iDataAgents as needed
  - VSS Provider (for Windows 2008 R2)
  - VSS Hardware Provider (for Windows 2012)

Note — Hitachi Data Protection Suite only supports the VSS Hardware Provider that is included with the product. Use of any other VSS Hardware Provider is not supported for IntelliSnap operation.

If backups are to be performed at the Hyper-V host level the following requirements exist.

- The Hitachi Data Protection Suite packages that must be installed on the host are:
  - MediaAgent
  - Virtual Server Agent (VSA)
  - VSS Provider (for Windows 2008 R2)
  - VSS Hardware Provider (for Windows 2012)

Note — If the virtual machines to be protected are hosted on a standalone Microsoft Hyper-V server, the local MediaAgent instance can be used instead of a proxy computer. In a failover cluster environment, the proxy computer should not be a member of the same cluster.

- It is not required to install any Hitachi Data Protection Suite components on the virtual machines if file level recovery is not required. If file level recovery is required, then the File System iDataAgent must be installed on the virtual machine.

Note — File level recovery can be accomplished without the File System iDataAgent installed on the virtual machine. However, the file needs to be recovered by doing a file copy across a UNC connection and all ACLs will be lost.

The virtual server agent has certain limitations on what it can back up.

- This is what gets backed up:
  - Virtual machines
  - VHD/VHDX files
  - Snapshot files
  - Configuration files for the virtual machines
  - Metadata required for granular recovery of files (NTFS and ext3 volumes only)
- This is what does not get backed up:
  - Pass-through disks
  - Windows storage spaces
  - Virtual machines with the following:
    - VHD files residing on SMB Shares or UNC locations
    - UNICODE characters in the virtual machine name or mount path

- Hard links (only for disk-level backup)
- Virtual hard disks with sector size of 4k bytes.
- Virtual machine smart paging files.
- Certain virtual machines in which volume shadow copy service (VSS) fails to create a shadow.
- Devices residing in a guest virtual machine over iSCSI or vHBA.

The configuration and testing for this paper used command control interface and Hitachi Thin Image. There are other configuration options available using Hitachi Device Manager and Hitachi ShadowImage Replication, but these were not tested or covered in this document.

For Hitachi Data Protection Suite, there are three options that will dictate where command control interface will be installed and which servers need command devices configured on the storage.

- **Environment with a proxy and a Remote Snap Media Agent** — Install command control interface on the remote snap media agent server and a command device must be configured for that server. The proxy can be on the same physical server as the remote snap media agent or on a different server. Multiple proxies and remote snap media agents can be configured.
- **Environments with a proxy** — If a remote snap media agent is not configured, install command control interface on all of the servers connected to the storage. Configure a command device for each sever.
- **Environments without a proxy and a Remote Snap Media Agent** — Install command control interface on all of the servers connected to the storage. Configure a command device for each sever.

For most environments, the first option is the best choice to simplify the configuration and operation of the Hitachi Data Protection Suite environment, Depending on the number of virtual machines being protected, multiple proxies and remote snap media agents may be required. In some scenarios the second or third option may need to be used due to requirements related to security.

Prerequisites for the storage array when using command control interface include the following.

- Depending on what software you want to use, licenses for Hitachi ShadowImage, Hitachi Thin Image, and Hitachi Copy-on-Write Snapshot must be installed on the storage array, as applicable. For this document, only Hitachi Thin Image snapshots were used.
- Verify that enough shared memory is configured on the storage array to support the licenses.
- Command devices must be configured.
- Hitachi Thin Image pools must be created.
- vVOLs for Hitachi Thin Image snapshots must be created or you must select the **Create VVOLs for Thin Image** check box in the snap configuration. See Array Management Configuration for more information on this option.

Array Management Configuration

Add and configure the Hitachi storage system information in the **Array Management** section of Hitachi Data Protection Suite. For instructions on adding and configuring Hitachi storage in Hitachi Data Protection Suite see the IntelliSnap User Guide - Hitachi Data Systems User Guide. Note the following.

- Configuration will vary depending on if you use Hitachi Device Manager or command control interface.
- If the **Create vVOLs for Thin Image** check box is checked on the **Snap Configuration** tab of the **Array Properties** window, new vVOLs will be created automatically**.**
- If a remote snap MediaAgent is configured, command control interface does not need to be installed on the client or proxy computers.
- Settings in the **Array Properties** window can be overridden at the storage policy or client level.

Tested Components

Table 2. Hardware Components

Hardware	*Description*	*Version*	*Quantity*
Hitachi Unified Storage VM	■ Dual controller ■ 16 × 8 Gb/sec Fibre Channel ports ■ 256 GB cache memory ■ 26 GB configured as shared memory ■ 120 × 600 GB 10k RPM SAS drives, 2.5 inch SFF	73-03-07-00/00	1
Hitachi Compute Blade 500 chassis	■ 8 server blade chassis ■ 2 management modules ■ 6 cooling fan modules ■ 4 power supply modules ■ 2 Brocade 5460 8 Gb/sec Fibre Channel switch modules ■ 2 Brocade 10 GbE DCB switch modules	A0165-B-8205	1
520H B1 server blade	■ Half blade ■ 2 x 8-core Intel Xeon E5-2680 processor, 2.70 GHz ■ 96 GB RAM ■ Emulex 10 GbE CNA onboard network adapter ■ Emulex 8 Gb/sec 2-port Fibre Channel mezzanine card	01-81	4

Table 3. Software Components

Software	*Version*
Hitachi Data Protection Suite	10 with SP 7
Hitachi Dynamic Provisioning	Microcode dependent
Hitachi Thin Image	Licensed on Hitachi Unified Storage VM
Hitachi RAID Manager CCI	01-31-03/08
Microsoft Windows Server	2012 R2 Datacenter Edition on physical servers
Microsoft Windows Server	2012 R2 Standard Edition on virtual machines

All four of the physical server blades in the test environment had Microsoft Windows Server 2012 R2, Datacenter edition, installed with the Microsoft Hyper-V role enabled.

Two of the server blades were configured as a failover cluster that hosted multiple virtual machines. The other two server blades were configured as standalone Hyper-V hosts, each hosting multiple virtual machines.

One of the standalone hosts was configured also as the media agent that acted as the proxy for the backups and recovery jobs. This sever was configured also as the remote snap media agent in the **Array Properties** window of the **Array Management** dialog.

The virtual machines on the clustered and standalone host were configured to test the scenarios listed in Table 1 on page 1.

Test Methodology

The steps that were executed to test this Microsoft Hyper-V environment running on Hitachi Unified Storage VM and Hitachi Compute Blade 500 were the following:

1. Install applicable Hitachi Data Protection Suite modules on hosts and virtual machines.
2. Create disk library.
3. Create storage policy with primary and snap primary copies.
4. Configure array management.
5. Create Hyper-V clients for each standalone Hyper-V host and for each Hyper-V cluster.
6. Enable the IntelliSnap option at the Hyper-V client level.
7. Create and configure new subclients.
   (1) Select content using either **Browse** or **Add.**
   (2) Enable IntelliSnap at the subclient level.
   (3) From the list, click **Snap Engine**.
   (4) From the list, click **Proxy.**
   (5) From the list, click **Storage Policy.**
   (6) For **Backup Schedule,** click **Do Not Schedule**.
8. Perform backup.
   (1) For **Backup Type**, click **Full**.
   (2) For **Job Initiation**, click **Immediate**.
   (3) To backup to media after snap backup completes, select **Create Backup Copy immediately**.
   (4) If file level recovery is required, select **Enable Granular Recovery for IntelliSnap**.
9. Verify job results.
10. Perform a recovery.
    (1) Click the **Restore** option.
    (2) Select the content to be recovered.
    (3) Execute the restoration job.
11. Verify the job results.
12. Verify that the recovered virtual machine is healthy or that files have been recovered as expected.

Test Cases

All testing was done using IntelliSnap.

Table 4. Test Cases

Test Case	*Result*
Backup virtual hard drive hosted on physical disk on the Microsoft Hyper-V host. Backup performed at the virtual machine level.	**Failed.** Use standard backup methods or backup from the host using VSA
Backup virtual hard drive on a pass through disk. Backup performed at the virtual machine level.	**Pass**
Backup a single virtual machine on a standalone Hyper-V host with a single virtual machine per volume. Backup performed on a standalone Hyper-V host at the host level using VSA.	**Pass**
Backup a single virtual machine on a standalone Hyper-V host with multiple virtual machines per volume. Backup performed on a standalone Hyper-V host at the host level using VSA.	**Pass**
Backup two virtual machines on a standalone Hyper-V host with both virtual machines on the same volume. Backup performed on a standalone Hyper-V host at the host level using VSA.	**Pass**
Backup three virtual machines on a standalone Hyper-V host with two virtual machines on the one volume and the third on a second volume. Backup performed on a standalone Hyper-V host at the host level using VSA.	**Pass**
Back up a single virtual machine on a failover cluster. With the operating system drive on a cluster shared volume with other virtual machines, backup performed on a Hyper-V failover cluster at the cluster level using VSA.	**Pass**
Back up single virtual machine on a failover cluster. With a pass through data drive, backup performed on a Hyper-V failover cluster at the cluster level using VSA.	**Fail.** Same backup job as test case above. Operating system drive backed up successfully, but data drive was skipped. Back up pass through disks at the virtual machine level.
Back up two virtual machines on a failover cluster. Operating system drives are on same cluster shared volume with other virtual machines, One client had a data drive on a second dedicated cluster shared volume. Backup performed on a Hyper-V failover cluster at the cluster level using VSA.	**Pass**
Recover virtual machine to original location.	**Pass**

Table 4. Test Cases (Continued)

Test Case	*Result*
Recover virtual machine to a different folder on same host.	**Pass**
Recover virtual machine to a different host.	**Pass**
Perform file level recovery of files that were deleted from virtual machine.	**Pass**

Test Results Summation

Table 5. Test Results

Backups performed on	*Hyper-V Host Configuration*	*Virtual Hard Drive Location*	*Results*
Guest (Virtual Machine)	Standalone Microsoft Hyper-V host	Host volume	Cannot be protected using IntelliSnap. Use standard backup.
		Pass-through disk	Can be protected using IntelliSnap
	Hyper-V hosts in Failover Cluster	Host volume	Cannot be protected using IntelliSnap. Use standard backup.
		Cluster shared volume	Cannot be protected using IntelliSnap. Use standard backup.
		Pass-through disk	Can be protected using IntelliSnap
Hyper-V Host	Standalone Hyper-V host	Host volume	Can be protected using IntelliSnap
		Pass-through disk	Cannot be protected using IntelliSnap using VSA. Use VM level protection.
	Hyper-V hosts in Failover Cluster	Host volume	Can be protected using IntelliSnap
		Cluster Shared Volume	Can be protected using IntelliSnap
		Pass-through disk	Cannot be protected using IntelliSnap using VSA. Use virtual machine level protection

Recommended Practices

The following are recommended practices when using IntelliSnap to protect virtual machines in a Microsoft Hyper-V environment.

- Protect virtual machines hosting high transaction rate applications at the virtual machine level using the applicable application iDataAgents.
- Protect pass through disks at the virtual machine level. Pass through disks cannot be protected using VSA at the Hyper-V host level.
- To enable file level recovery enable granular recovery on the backup job.
- To do file level recovery to a virtual machine the File System iDataAgent must be installed on the target virtual machine.
- Install the Hitachi Data Protection Suite with VSS provider on Microsoft Windows Server 2008 R2 clients and the VSS hardware provider in Hitachi Data Protection Suite on Windows Server 2012 clients.
- When it is required to install the VSS hardware provider in Hitachi Data Protection Suite on clients in an environment that was built using Hitachi Data Protection Suite v10 with a service pack prior to SP7. Do not attempt to install it from the CommCell console. Use either a decoupled installation package or Hitachi Data Protection Suite v10 with SP7 ISO installation image to do a local install on the client. Even though an install from the CommCell console may appear to complete successfully, in some scenarios the VSS hardware provider is not installed.

For More Information

Hitachi Data Systems Global Services offers experienced storage consultants, proven methodologies and a comprehensive services portfolio to assist you in implementing Hitachi products and solutions in your environment. For more information, see the Hitachi Data Systems Global Services website.

Live and recorded product demonstrations are available for many Hitachi products. To schedule a live demonstration, contact a sales representative. To view a recorded demonstration, see the Hitachi Data Systems Corporate Resources website. Click the **Product Demos** tab for a list of available recorded demonstrations.

Hitachi Data Systems Academy provides best-in-class training on Hitachi products, technology, solutions and certifications. Hitachi Data Systems Academy delivers on-demand web-based training (WBT), classroom-based instructor-led training (ILT) and virtual instructor-led training (vILT) courses. For more information, see the Hitachi Data Systems Services Education website.

For more information about Hitachi products and services, contact your sales representative or channel partner or visit the Hitachi Data Systems website.

Hitachi Data Systems Corporation

Corporate Headquarters
2845 Lafayette Street, Santa Clara, California 95050-2627 USA
www.HDS.com

Regional Contact Information
Americas: +1 408 970 1000 or info@HDS.com
Europe, Middle East and Africa: +44 (0) 1753 618000 or info.emea@HDS.com
Asia-Pacific: +852 3189 7900 or hds.marketing.apac@HDS.com

AS-332-00, October 2014