SEAGATE

VSS Hardware Provider Installation Guide

Abstract

This document provides installation and usage instructions for the VSS Hardware Provider that works with Microsoft Windows Server and Seagate storage systems. It also includes installation instructions for the CAPI Proxy, which must be installed to enable support for the VSS Hardware Provider.

Firmware Version: G265

P/N 83-00007206-10-01
Revision A
December 2017

Contents

About this guide

This document provides installation and usage instructions for the VSS Hardware Provider that works with Microsoft Windows Server and Seagate storage systems. It also includes installation instructions for the CAPI Proxy that must be installed to enable support for the VSS Hardware Provider.

Intended audience

This guide is intended for system administrators and storage administrators.

Prerequisites

Prerequisites for using this product include knowledge of:

- Server system administration
- Microsoft Windows servers
- Storage system configuration
- Storage area network (SAN) management
- Fibre Channel (FC) protocol
- Serial Attached SCSI (SAS) protocol
- Internet SCSI (iSCSI) protocol

Before you begin to follow procedures in this guide, you must have already installed enclosures and learned of any late-breaking information related to system operation, as described in the Hardware Installation and Maintenance Guide and in Release Notes.

Document conventions and symbols

Table 1 Document conventions

Convention	Element
Colored text	Cross-reference links
Black, underlined text	Email addresses
Colored, underlined text	Website addresses
Bold text	• Keys that are pressed • Text typed into a GUI element, such as a box • GUI elements that are clicked or selected, such as menu and list items, buttons, and check boxes
Italic text	Text emphasis
`Monospace` text	• File and directory names • System output • Code • Commands, their arguments, and argument values
`Monospace, italic` text	• Code variables • Command variables
`Monospace, bold` text	Emphasis of file and directory names, system output, code, and text typed at the command line

CAUTION: Indicates that failure to follow directions could result in damage to equipment or data.

IMPORTANT: Provides clarifying information or specific instructions.

NOTE: Provides additional information.

TIP: Provides helpful hints and shortcuts.

1 The VSS Hardware Provider and the CAPI Proxy

The VSS Hardware Provider and CAPI Proxy described in this document are used with Seagate 5005/4005 Series storage systems in Microsoft Windows Server environments. They are available for download as separate installation files:

- A VSS Hardware Provider for FC, iSCSI, and SAS storage systems.
- A CAPI Proxy that enables in-band management from host-based applications. The CAPI Proxy is necessary to enable the VSS Hardware Provider. It must be installed on all hosts that will run the VSS Hardware Provider.

Version 3.8 of the VSS Hardware Provider and CAPI Proxy are to be used with Seagate 5005/4005 Series and newer storage systems.

If any of the providers on a host are upgraded to 3.8, all other Hardware Providers and the CAPI Proxy installed on the host must be upgraded to the same version.

IMPORTANT: In environments with Seagate 5005/4005 Series systems using FC and iSCSI host interface ports in combination, do not connect both iSCSI and FC ports from the same controller to the same host.

Table 2 Compatible versions of software

VSS and CAPI Proxy versions:	Applies to product family:
Seagate v.3.8	Seagate 5005 Series
	Seagate 4005 Series

Installation requirements

Each of the software components described in this document can be downloaded from the support website seagate.com/support-home.

All VSS/CAPI packages are typically included in a single archive file, such as `seagate-vss-3.8.x.xx.zip`, which in turn contains `.zip` files for each individual component. Several server-specific files might be available on the support website. If multiple versions are available, they will be identified by a filename suffix such as `x64` or `x86`. Be sure to download the appropriate `.zip` file for the server on which you will be installing the VSS Hardware Provider.

The VSS Hardware Provider requires the following software:

- A supported operating system:
  - Microsoft Windows Server 2012 x64 Edition
  - Microsoft Windows Server 2012 R2 x64 Edition
  - Microsoft Windows Server 2016
- CAPI Proxy 3.8 or later

About VSS

Microsoft Windows Server operating systems provide enhanced services for managing storage area networks, including Volume Shadow Copy Service (VSS). VSS, with its standard set of extensible APIs, provides the backup infrastructure for Windows Server, as well as a mechanism for creating consistent point-in-time copies of data known as shadow copies. VSS provides interfaces to ensure that volume shadow copies are in a consistent state.

The VSS Hardware Provider installs on a server running Windows Server and enables VSS to create hardware-resident shadow copies on any storage system attached to the server. With the VSS Hardware Provider and VSS, you can create a shadow copy of the source data volume on one server and then import the shadow copy onto another server, or back to the same server. Before creating the shadow copy, determine whether it will be imported back to the same host, because a snapshot created with the transportable option should not be imported back to the original host.

The VSS Hardware Provider does not include user interfaces or standalone functionality. Instead it enables other applications to manage Seagate storage products. `vshadow.exe` and `diskshadow.exe` are useful command-line tools for creating, deleting, querying, and managing shadow copies in a Microsoft Windows environment. Diskshadow is included in Windows Server, while VShadow is available from Microsoft as part of the Windows SDK.

Supported VSS features

The VSS Hardware Provider supports the following features provided by the Windows VSS subsystem:

- Creating shadow copies/snapshots.

  NOTE: Before you can create shadow copies, a license key must be installed in the storage system to enable snapshot functionality for virtual volumes. Then you must enable shadow copies for a volume by using your configuration management tool. See "Creating shadow copies" (page 8) for more information.

- Exporting shadow copies/snapshots: prepare for use in another Windows Server system.
- Importing snapshots: prepare for local use after export from another Windows Server system.
- Determining when snapshots can be deleted and deleting them.
- Reverting snapshots using the `diskshadow resync` command or `vshadow -resync` option.

Installing the CAPI Proxy

The CAPI Proxy is a prerequisite for the VSS Hardware Provider. Install it before installing the VSS Hardware Provider.

1. Download the single archive file described above.
2. Extract and open the CAPI Proxy setup file to begin the installation.

   NOTE: The CAPI Proxy `setup.exe` can be launched directly from within the archive file without extracting the other files if desired.

3. Follow the on-screen prompts to install the software.

   On 32-bit operating systems, the software program is installed in:

   `C:\Program Files\Seagate\Seagate CAPI Proxy`

   On 64-bit operating systems, the software program is installed in:

   `C:\Program Files(x86)\Seagate\Seagate CAPI Proxy`

   If a previous version of the CAPI Proxy is already installed, a message informs you that the software is installed, but not up to date.
4. Press **Yes** to continue with the installation process, or **No** to exit setup.

2 Installing and using the VSS Hardware Provider

This section describes how to install the VSS Hardware Provider.

NOTE: In a cluster environment the VSS Hardware Provider cannot be installed unless a Microsoft Distributed Transaction Coordinator (MS DTC) cluster resource is configured. If the host part of a cluster and MSDTC is not running, installation will fail. Refer to http://support.microsoft.com/kb/301600 for instructions on configuring MS DTC.

1. Double-click the downloaded Hardware Provider file to launch the installation.
2. Press the **Install** button.
3. Follow the onscreen prompts to install the software.

   The provider is installed in this directory:

   `C:\Program Files\Seagate\Seagate VSS Provider`

   If a previous version of the VSS Hardware Provider is already installed, a message tells you that the software is installed, but not up to date.

   NOTE: Overwriting an existing VSS Hardware Provider will not overwrite previously installed hardware providers used with earlier storage systems.

4. To verify the installation, run the `list providers` command, and make sure that the VSS Hardware Provider is displayed in the list of providers.

```
C:\> vssadmin list providers
vssadmin x.x - Volume Shadow Copy Service administrative command-line tool
(C) Copyright 2001-20xx Microsoft Corp.

Provider name: 'Seagate VSS Hardware Provider'
   Provider type: Hardware
   Provider Id: {9d09666c-5cf8-45ca-9294-127c95562094}
   Version: 3.8.x.xx

Provider name: 'Microsoft Software Shadow Copy provider 1.0'
   Provider type: System
   Provider Id: {b5946137-7b9f-4925-af80-51abd60b20d5}
   Version: 1.0.0.7
```

Creating shadow copies

VSS functionality includes creating, deleting, and managing shadow copies.

To create a shadow copy of a volume in a virtual pool, create the shadow copy using a VSS requester such as Diskshadow (included in Windows Server 2012 and Windows 2016) or VShadow (available as a download from microsoft.com as part of the Windows SDK).

NOTE: After the VSS Hardware Provider is installed, your backup software may take advantage of it to create temporary hardware snapshots on the system when your backups are run.

NOTE: The VSS Hardware Provider takes shadow copies quickly (less than 5 seconds), but the Microsoft VSS subsystem can take a long time to recognize and import the new shadow copies. It may take up to 90 seconds to create and import a shadow copy. It takes longer if multiple RAID partitions are included in the same shadow copy set.

LUN 0 mapping

For best performance, avoid mapping any storage system volumes to the host using LUN number 0, which is used by the VSS Hardware Provider to monitor and manage the system. The VSS Hardware Provider automatically assigns LUN numbers starting at LUN 1, but if you have manually mapped LUNs to the host using LUN number 0, the providers have to compete with I/O traffic and this may cause commands to run more slowly or time out.

64-bit VSS clients

When creating snapshots on a 64-bit OS, you must use a 64-bit VSS client application. Microsoft's VSS framework does not support 32-bit requestors on 64-bit operating systems.

Ensuring read-write access of VSS shadow copies

When VSS creates a shadow copy, it maps the LUN with the shadow copy data back to the host. Because this is generally used for backup, the volumes on the LUN are read-only. The LUN is mapped read-write; only the volumes are read-only. You can restore read-write access of the volumes on the server, as shown below.

NOTE: Multiple terms for the same or similar storage elements can include disks, volumes, snapshots and LUNs, depending on whether the storage element is being referenced by an operating system, a storage device, or an application.

The read-only or read-write attribute may also be influenced by the SAN policy of Windows Server systems. The SAN policy in place on the server affects the access level for newly discovered disks, but volumes on the disks for VSS shadow copy snapshots are always initially discovered as read-only, regardless of the SAN policy or version of Windows operating system.

See "LUN 0 mapping" (page 9) for more information.

Restoring read-write access

On the server, clear the read-only status of the imported snapshots' disks and volumes using the commands below. Select the disk that corresponds to the LUN with the snapshot data. After selecting the disk and clearing the disk's read-only status, select the volume and clear the volume's read-only status.

Relative to the tables below, invoke the Microsoft DiskPart utility by typing `diskpart` at the command line. Once invoked, `DISKPART>` appears as a prompt for entering the commands listed in the tables below. Type `exit` to quit the Microsoft DiskPart utility.

Table 3 DiskPart utility - disk commands

Command/sequence		Description
1	`list disk`	Allows you to determine which disk number to use in the following command.
2	`select disk x`	Selects a disk where *x* refers to the disk number from the `list disk` command.
3	`detail disk`	Use command to verify the disk is in an offline and/or read-only state.
4	`online disk`	Use command to bring the selected disk online.

Table 3 DiskPart utility - disk commands (continued)

Command/sequence		Description
5	`attributes disk clear readonly`	Clears the `readonly` attribute, allowing this host to write to the disk.
6	`list volume`	Allows you to get a list of volumes residing on disk, if any. The volume number displayed will be used in the `select volume` command.

The commands in the following table are repeated for each volume on the LUN; typically, there will be only one volume—or none—for a newly-provisioned LUN.

Table 4 DiskPart utility - volume on LUN commands

Command/sequence		Description
1	`select volume y`	Selects a volume, where *y* refers to the volume shown in the `list volume` command.
2	`detail volume`	Use command to verify the volume is read-only.
3	`attributes volume clear readonly`	Clears the `readonly` attribute for the volume.

Troubleshooting

This section contains troubleshooting information for the VSS Hardware Provider.

Table 5 Troubleshooting the VSS Hardware Provider

Issue	Description
The VSS Hardware Provider cannot create a snapshot.	• The maximum number of snapshots allowed by the snapshot license has already been created.
The following error is reported: `VSS_E_PROVIDER_VETO`	• The storage system has failed to execute the commands from the VSS Hardware Provider, or the communication between the VSS Hardware Provider and the system is broken, due to any of the following conditions: o The serial number cannot be obtained for the controller owning the volume. o The snapshot cannot be found in the VSS Hardware Provider's snapshot list. o The partition is not a snapshot. o The LUN assignment to the newly created snapshot failed. o The snapshot that will be deleted is not a Seagate snapshot. o A firmware upgrade operation may temporarily prevent VSS from managing the system.
The shadow copy does not exist on the controller.	• The backup utility automatically deletes the shadow copy when the backup is complete.
	• You might have used the Windows Explorer shadow copy shell extension context menu to create a shadow copy, which is to be used for creating a Windows software shadow copy, not hardware shadow copies.
	• Make sure you have created the shadow copy using the persistent (`-p`) attribute.

Table 5 Troubleshooting the VSS Hardware Provider (continued)

Issue	Description
	• If you use the `Vssadmin` tool from Microsoft to create shadow copies, it is not designed to work with the VSS Hardware Provider. `Vssadmin create shadow` only works with the Microsoft software shadow copy provider built into Windows.
An application error in the Windows event log states: `ssproxy requires that the HBA can handle 256-Kbyte transfers. You might need to set the MaximumSGList to a value of 65 or higher if using a SCSIPort driver.`	The CAPI Proxy requires the maximum data for the CAPI command to be 256 Kbyte. This does not apply to Storport HBA drivers. • For SCSIport HBA drivers, create a `MaximumSGList` registry entry if it does not already exist and set it to a value of 65 or higher, if it has not already been set.[1] **Note:** The SCSIport host-bus adapter driver has been removed in Windows Server 2012. Instead, use either a Storport driver or a different host-bus adapter.
	• To set the registry for Qlogic cards using the SCSIport driver, double-click `qla2300.reg` in the following directory: `C:\Program Files\Seagate\Seagate VSS Provider\qla2300.reg`
It is taking a long time to create the shadow copy.	The VSS Hardware Provider takes shadow copies quickly (less than 5 seconds), but the Microsoft VSS subsystem can take a long time to recognize and import the new shadow copies. It may take up to 90 seconds to create and import a shadow copy. It takes longer if more RAID partitions are included in the same shadow copy set.
`Not Implemented` or 0x80004001 error when `revert` command used in `VShadow` or `Diskshadow`.	The `revert` option is meant for host-based snapshots and is not supported for storage system-based snapshots. Use the `resync` command instead.
`VSS_E_MISSING_DISK` error when using the `RESYNC` command	This error can occur if the target volume is in use when the `RESYNC` command is issued. The target volume may be left in an offline state; use Disk Management or `DISKPART` to bring the target volume back online. To minimize the likelihood of this error occurring, stop the VSS subsystem with the command `NET STOP VSS` prior to performing the `RESYNC` operation; the VSS subsystem will automatically restart when you launch a VSS client. If necessary, use `MOUNTVOL` to unmount the volume prior to issuing the `RESYNC` command to ensure that other applications are not accessing the volume.
`VSS_E_PROVIDER_VETO` error when using the `RESYNC` command	This error can occur if a previous operation in the system is still in progress and the `resync` operation cannot proceed. The target volume may be left in an offline state; use Disk Management or `DISKPART` to bring the target volume back online. Review the event log in the system and wait for any operation in progress to complete before retrying the operation.
A “0mb” volume may appear in the Disk Management applet after creating a hardware snapshot of a GPT-formatted volume.	The Disk Management Control Panel applet may display an unnamed volume with a capacity of 0mb after a snapshot is created on a GPT disk. These are associated with special metadata partitions that Windows creates as part of the snapshot process and may safely be ignored. If they are bothersome, they can be deleted using the `DISKPART` command, by looking for a 256KB partition with an “Unknown” partition type. Volumes formatted with a traditional MBR partition table are not affected.

1. For more information see: http://msdn.microsoft.com/en-us/library/windows/hardware/ff563970(v=vs.85).aspx

Uninstalling the VSS Hardware Provider

To uninstall the VSS Hardware Provider, perform the following steps.

1. Choose **Start > Control Panel > Add/Remove Programs** or **Start > Control Panel > Programs and Features**.
2. Choose **VSS Hardware Provider** and click **Change/Remove**.
3. Respond appropriately to the prompts.
4. You can also select the CAPI Proxy from the Add/Remove Programs list if you do not need it to enable the VSS Hardware Provider for which it is a prerequisite, and uninstall it now.