



**HiCommand Protection Service
for Microsoft® Exchange Server**

**Volume Shadow Copy Service (VSS)
Linkage Function**

© 2004 Hitachi Data Systems Corporation, ALL RIGHTS RESERVED

Notice: No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording, or stored in a database or retrieval system for any purpose without the express written permission of Hitachi Data Systems Corporation.

Hitachi Data Systems reserves the right to make changes to this document at any time without notice and assumes no responsibility for its use. Hitachi Data Systems products and services can only be ordered under the terms and conditions of Hitachi Data Systems' applicable agreements. All of the features described in this document may not be currently available. Refer to the most recent product announcement or contact your local Hitachi Data Systems sales office for information on feature and product availability.

This document contains the most current information available at the time of publication. When new and/or revised information becomes available, this entire document will be updated and distributed to all registered users.

Trademarks

Hitachi Data Systems is a registered trademark and service mark of Hitachi, Ltd., and the Hitachi Data Systems design mark is a trademark and service mark of Hitachi, Ltd.

HiCommand, Hitachi Freedom Storage, Lightning 9900, Thunder 9200, and Thunder 9500 are trademarks of Hitachi Data Systems Corporation in the United States and other countries.

InstallShield is a registered trademark and service mark of InstallShield Software Corporation.

Microsoft, Windows, and Windows Server are registered trademarks or trademarks of Microsoft Corporation in the United States and other countries.

VERITAS is a trademark of VERITAS Software in the United States and other countries.

All other brand or product names are or may be trademarks or service marks of and are used to identify products or services of their respective owners.

Notice of Export Controls

Export of technical data contained in this document may require an export license from the United States government and/or the government of Japan. Please contact the Hitachi Data Systems Legal Department for any export compliance questions.

Document Revision Level

Revision	Date	Description
MK-94HC074-00	May 2004	Initial Release

Source Documents for this Revision

- *HiCommand Protection Service for Microsoft(R) Exchange Server version 01-05, Volume Shadow Copy Service (VSS) Linkage Function*, Operation Manual 031796 (April 2004) (Hitachi SD document)
- *RAID Manager Basic Specifications*, revision 45 (February 2004) (Hitachi RSD document)
- *Enhancements of RAID Manager (Ver. 01-12-03/06)*, ERM011206 (Hitachi RSD document)

Referenced Documents

- *HiCommand Protection Services User and Reference Guide*, MK-93HC039
- *Hitachi Lightning 9900™ V Series and Lightning 9900™ Command Control Interface (CCI) User and Reference Guide*, MK-90RD011
- *Hitachi Thunder 9500™ V Series Command Control Interface (CCI) User and Reference Guide*, MK-92DF609

Preface

This document describes the Volume Shadow Copy Service (VSS) linkage function of the HiCommand™ Protection Service for Microsoft® Exchange Server product, version 1.5.

The following manual is related to this document. Read this manual when necessary:

- *HiCommand Protection Services User and Reference Guide* (MK-93HC039)
(based on *HiCommand Protection Service for Microsoft® Exchange Server User's Guide*, 3020-3-D56-30(E))

Note: The use of HiCommand™ Protection Service and all other Hitachi Data Systems products is governed by the terms of your license agreement(s) with Hitachi Data Systems.

Software Version

This document revision applies to HiCommand™ Protection Service version 1.5 only.

Comments

Please send us your comments on this document. Make sure to include the document title, number, and revision. Please refer to specific section(s) and paragraph(s) whenever possible.

- E-mail: doc.comments@hds.com
- Fax: 858-695-1186
- Mail:
Technical Writing, M/S 35-50
Hitachi Data Systems
10277 Scripps Ranch Blvd.
San Diego, CA 92131

Thank you! (All comments become the property of Hitachi Data Systems Corporation.)

Contents

Chapter 1	Overview and Requirements	
1.1	Functional Overview	1
1.2	Requirements	1
1.3	Environment Setup	2
Chapter 2	Protection Service Operations	
2.1	Backup Operations	3
2.2	Operations on the Backup Results	3
2.3	Notes on Operations	4
2.3.1	Specifications of Backup Targets	4
2.3.2	Status of Exchange Server during Backup	4
2.3.3	Backup Generations	4
2.3.4	Log Files not Recorded in the Backup Catalog	4
2.3.5	Upper Limit of the Disk Configuration	5
2.3.6	Special Attributes of the Secondary Volume for VSS Backup Results	5
2.3.7	Version of Protection Service on the Backup Server	5
2.3.8	Changing the Storage Group or Information Store Name while Mounted	5
2.4	Commands	6
2.4.1	drmexgbackup Command	6
2.4.2	EX_DRM_EXG_BACKUP Command	8
Chapter 3	VSS Hardware Provider Operations	
3.1	Overview	11
3.2	VSS Configuration	11
3.2.1	Single HOST Configuration	12
3.2.2	Coordination of Shadow Copy Creation	12
3.3	Restrictions on VSS Configurations	13
3.4	Relationship Between Requestor and Configurations	15
3.5	Installation Procedures	16
3.5.1	Procedure for New Installation	16
3.5.2	Procedure for Update Installation	17
3.5.3	Version Confirmation after Installation	17
3.6	Uninstallation Procedure	18
3.7	VSS Start-up Procedures on Single Host	19
3.7.1	Setting the System Environment Variables	19
3.7.2	Setting the CCI Environment	20
3.7.3	Executing the Backup	23
3.7.4	Notes on VSS Operation	24
3.8	Troubleshooting VSS Hardware Provider	25
3.9	Checking VSS Hardware Provider Error Messages	26
Chapter 4	Protection Service Messages	29
	Acronyms and Abbreviations	31

List of Figures

Figure 3.1	Single-Host Configuration for VSS Hardware Provider	12
------------	---	----

List of Tables

Table 1.1	Environment Variables for the Database Server	2
Table 2.1	Commands for the Results of a VSS Backup	3
Table 2.2	Guidelines for the VSS-Backup Disk Configuration	5
Table 3.1	Hidden Property of SVOL and Performance Characteristic	13
Table 3.2	Backup Software Confirmed with CCI Shadow Copy Provider	15
Table 3.3	Setting the System Environment Variables	19
Table 3.4	General Troubleshooting for VSS Hardware Provider	25
Table 3.5	Error Messages Generated by CCI Shadow Copy Provider	26-27
Table 4.1	Messages for the VSS Linkage Function	29-30

Chapter 1 Overview and Requirements

1.1 Functional Overview

The Volume Shadow Copy Service (VSS) linkage function uses Volume Copy Service, provided by the Windows Server® 2003 Enterprise Edition product, to back up Exchange databases. The VSS linkage function can back up data during operation of Exchange Server 2003. Compared to online backup that is also available with the previous HiCommand™ Protection Service for Exchange Server, the VSS linkage function has the added ability to ensure successful backup, and to delete the transaction logs.

1.2 Requirements

In addition to the prerequisites for HiCommand™ Protection Service for Exchange Server, the following conditions are required to use the VSS linkage function:

- **Applicable Operating System:** Windows Server® 2003, Enterprise Edition (32-bit only)
- **Prerequisite programs:**
 - Database management system (DBMS):
 - Microsoft® Exchange Server 2003 Standard Edition
 - Microsoft® Exchange Server 2003 Enterprise Edition
 - RAID management software product (server system unit)
 - Command Control Interface (CCI) version 01-12-03/06 or later
- **Cluster environment:** The VSS linkage function cannot be used in a cluster environment.

1.3 Environment Setup

To use the VSS linkage function, you need to set up the environment as follows:

1. **Set up the Protection Service and CCI.** First, set up the environment for HiCommand™ Protection Service and Command Control Interface (CCI) so that Protection Service for Exchange Server can perform a cold backup. For details, see the section on environment setup in the *HiCommand Protection Services User and Reference Guide*.
2. **Install CCI Shadow Copy Provider.** Install the CCI Shadow Copy Provider as described in section 3.5.
3. **Set the environment variables.** Set the system environment variables for the database server as shown in Table 1.1 below.

Note: These settings are not enabled until the database server is restarted. After you finish the settings, you must restart the database server.

Caution: Do not perform the following operations described in the CCI documentation: setting the `VSHTCHORCMINST_REMOTE` environment variable, using the `raidvchkset` command for the secondary volume to hide the inquiries, or using the `paircreate` command with the `noread` attribute.

Table 1.1 Environment Variables for the Database Server

Variable Name	Settings
VSHTCHORCMINST_LOCAL	Specify the instance number of the CCI to be used for the backup by VSS.
VSHTCHOMRCF_MUN	Specify the MU number (pair identifier) of the copy group to be used for the backup by VSS.

Chapter 2 Protection Service Operations

2.1 Backup Operations

To use the VSS linkage function to back up data, specify `vss` as the backup mode for the `drmexgbackup` command or the `EX_DRM_EXG_BACKUP` command. The following shows examples of executing the commands.

In this example, the `drmexgbackup` command performs backup by VSS:

```
C:\>drmexgbackup -mode vss
```

In this example, the `EX_DRM_EXG_BACKUP` command performs backup by VSS:

```
C:\>EX_DRM_EXG_BACKUP operation01 -mode vss
```

The VSS-backup operation examples are the same as the online backup examples provided in the *HiCommand Protection Services User and Reference Guide*, except that:

- The `-mode online` option becomes the `-mode vss` option.

2.2 Operations on the Backup Results

The results of a backup by VSS can be handled in the same way as the results of a cold backup. You can use the commands in Table 2.1 for the results of a backup by VSS.

Table 2.1 Commands for the Results of a VSS Backup

Function	Command
Restore and recover data.	<code>drmexgrestore</code>
Display catalog information.	<code>drmexgcat</code> <code>drmtapecat</code>
Export and import a catalog.	<code>drmdbexport</code> <code>drmdbimport</code>
Mount the secondary volume.	<code>drmmount</code>
Back up data to tape.	<code>drmmediabackup</code>
Restore data from tape.	<code>drmmediarestore</code>
Verify the database.	<code>drmexgverify</code> <code>EX_DRM_EXG_VERIFY</code>

2.3 Notes on Operations

In comparison to the previous online backup, note the following points for backup by VSS (see subsections below):

- Specifications of backup targets
- Status of Exchange Server during backup
- Backup generations
- Log files not recorded in the backup catalog
- Upper limit of the disk configuration

2.3.1 Specifications of Backup Targets

For backup by VSS, you can specify backup targets for each storage group. Files that become backup targets are database files (*.edb and *.stm), transaction log files (*.log), and checkpoint files (*.chk). Database files (*.edb and *.stm) and transaction log files (*.log) cannot be placed in the same volume.

The specifications of the backup targets are the same as for the cold backup.

2.3.2 Status of Exchange Server during Backup

To perform backup by VSS, the Exchange Information Store service must be running. Also, all the information stores in the storage group that will become backup targets must be mounted.

During backup, writing to the database of Exchange Server is stopped for a predefined period (a maximum of 10 seconds). This means that any operation that involves writing to the database, such as sending an email, is suspended (the operation will automatically restart after the backup finishes).

2.3.3 Backup Generations

Since the `VSHTCHOMRCF_MUN` system environment variable determines the backup generation to be used for backup by VSS, only one backup generation can be used. If you changed the `VSHTCHOMRCF_MUN` system environment variable, you must restart the database server. A backup generation acquired in VSS can be overwritten with a backup acquired in another backup mode (cold backup or online backup). Therefore, if you want to save a generation acquired from backup by VSS, use the `drmcgctl` command to protect the backup results.

2.3.4 Log Files not Recorded in the Backup Catalog

The results of the backup by VSS might contain log files that are not recorded in the catalog. This is because the number of log files may increase during the backup by VSS process.

2.3.5 Upper Limit of the Disk Configuration

If the VSS Hardware Provider cannot complete splitting a volume pair within a predefined time, backup by VSS terminates with an error because Exchange Server restarts writing to the database. The time required for splitting depends on the number of copy groups used by each storage group. Table 2.2 specifies the guidelines for the VSS-backup disk configuration.

Table 2.2 Guidelines for the VSS-Backup Disk Configuration

Condition	Lightning 9900V Series	Thunder 9500V Series (QuickShadow)	Thunder 9500V Series (ShadowImage)*1
The storage groups do not share the same copy group.	Each storage group uses a maximum of 8 copy groups.	Each storage group uses a maximum of 4 copy groups.	Each storage group uses a maximum of 4 copy groups.
The storage groups share the same copy group.	In total, the storage groups use a maximum of 8 copy groups.	In total, the storage groups use a maximum of 4 copy groups.	In total, the storage groups use a maximum of 4 copy groups.

*1 If ShadowImage is used with the Thunder 9500V Series, a backup may fail despite the minimum disk configuration (two disks).

2.3.6 Special Attributes of the Secondary Volume for VSS Backup Results

Special attributes (write inhibit and hidden attributes) are set for the secondary volume that is acquired in a backup by VSS. Therefore, you must cancel these attributes before you reuse the secondary volume acquired in a backup by VSS. To cancel the attributes, do one of the following:

- On Windows Server® 2003, use the drmmount command to mount the secondary volume.
- In a mode other than VSS, retry the backup.
- Delete the partitions on the secondary volume, and then re-create the partitions.

2.3.7 Version of Protection Service on the Backup Server

To use the VSS linkage function, use HiCommand™ Protection Service version 1.5 on the backup server also.

2.3.8 Changing the Storage Group or Information Store Name while Mounted

If the mounted storage group name or the mounted information store name was changed, first unmount all information stores related to the storage group, and then re-mount the information stores.

2.4 Commands

This chapter describes the commands that have been enhanced for the VSS linkage function. This document describes only the options concerning the VSS linkage function. For other functions, see the *HiCommand Protection Services User and Reference Guide*.

2.4.1 drmexgbackup Command

Format:

When performing backup by VSS:

```
drmexgbackup -mode vss  
             [ -target storage-group-names | -f target-list-file-name ]  
             [ -transact_log_del ]
```

Description:

This command backs up the Exchange Server database from the primary volume to the secondary volume.

Before executing this command, you need to clear the system cache for the secondary volume. To clear the system cache, use the backup server to mount the secondary volume and then unmount it.

Arguments:

-target *storage-group-names*

Specify this option to back up database resources that include the specified storage groups. When this option is specified, the command executes a backup on a physical volume basis. If one physical volume contains more than one storage group, specify all the storage groups. If you do not specify all of the storage groups, an error will occur during command execution.

To back up more than one storage group, use a comma to separate each storage group name. If a storage group name includes a space, enclose the storage group name within double quotation marks.

When this option is not specified, the command backs up all the storage groups in the server where the command is executed.

-f *target-list-file-name*

Like the **-target** option, specify this option to back up only the specified storage groups. You must specify either this option or the **-target** option when one physical volume contains the data files of the information stores of multiple storage groups.

Unlike the **-target** option, the **-f** option allows you to specify multiple storage group names collectively by specifying the name of a file that contains a list of storage group names. You need to create the list file in advance. When specifying the list file name, use its absolute path name.

-transact_log_del

Specify this option to delete a committed transaction log file after backup.

When you execute the command with this option specified, the command deletes the transaction log file. Therefore, you cannot restore the database from a backup by specifying the **-recovery** option.

Return values:

0: The command terminated normally.

Other than 0: The command terminated with an error. An error message is sent to the standard output.

Example:

In the following example, the command uses VSS to back up all the databases on Exchange Server:

```
PROMPT> drmexgbackup -mode vss
KAVX0001-I KAVX0001-I The drmexgbackup command will now start.
KAVX1600-I Backup processing will now start.
KAVX0040-I The backup ID has been assigned as follows.
Backup ID = 0000000001
KAVX1601-I Backup processing has finished.
KAVX0002-I The drmexgbackup command will now end.
```

2.4.2 EX_DRM_EXG_BACKUP Command

Format:

When performing backup by VSS:

```
EX_DRM_EXG_BACKUP.wsf operation-ID -mode vss [ -transact_log_del ]
```

Description:

EX_DRM_EXG_BACKUP executes the `drmxgbackup` command, and backs up the Exchange database of the storage group specified with *operation-ID* from the primary volume to the secondary volume. A backup ID is generated at this time.

Prerequisites:

- The operation definition file for the specified operation ID must be created in advance.

Arguments:

operation-ID

Specify a character string that indicates the target resource. The information in the operation definition file for the specified operation ID is used for execution of the extended command.

`-transact_log_del`

Specify this option to delete a committed transaction log file. Deleting a committed transaction log file will increase the amount of free disk space.

When you execute the command with this option specified, the command deletes the transaction log file. Therefore, you cannot restore the database from a backup by specifying the `-recovery` option.

Return values:

- 0: The command terminated normally.
- 2: The command terminated with an error. An error message is sent to the standard output.

Error conditions:

This extended command fails in the following cases:

- When an invalid option was specified.
- When an attempt to acquire information from the definition file for the specified operation ID has failed.
- When the specified Protection Service's command option could not be used for this extended command.
- When an attempt to record the backup ID in the backup ID file has failed.
- When an internally executed command terminated because of an error.

Example:

In the following example, the command backs up the database to the secondary volume by deleting the transaction log file as defined in the "operation01" operation definition file:

```
PROMPT> EX_DRM_EXG_BACKUP.wsf operation01 -mode vss -transact_log_del
```


Chapter 3 VSS Hardware Provider Operations

This chapter describes the Volume Shadow Copy Service (VSS) Hardware Provider and provides instructions for installing and removing the CCI Shadow Copy Provider:

- Overview (see section 3.1)
- VSS Configurations (see section 3.2)
- Restrictions on VSS Configurations (see section 3.3)
- Relationship Between Backup Software and Configurations (see section 3.4)
- Installation Procedures (see section 3.5)
- Uninstallation Procedure (see section 3.6)
- VSS Start-up Procedures on a Single Host (see section 3.7)
- Troubleshooting VSS Hardware Provider (see section 3.8)
- Checking VSS Hardware Provider Error Messages (see section 3.9)

3.1 Overview

The Windows Server® 2003 environment supports the Volume Shadow Copy service (VSS) that provides an infrastructure for creating point-in-time images known as shadow copies. VSS is able to produce high-fidelity shadow copies through its coordination with business applications, backup applications, and RAID storage systems.

VSS is a service that coordinates backup software called “requestors”, “writers” such as database applications, and hardware providers who provide vendor-unique shadow copy functions.

A shadow copy volume is a copy of a volume that is used by an application at a specific time. CCI Shadow Copy Provider is a component that creates a shadow copy volume by controlling RAID via VSS (Volume Shadow Copy Service).

3.2 VSS Configuration

CCI Shadow Copy Provider is a hardware provider for VSS that supports disks that are defined in the CCI configuration files. If any disks for a requestor (backup application) are not defined in CCI configuration files, VSS will select the provider using the following default hierarchy and will create a snapshot volume using the default system software provider:

VSS Hardware Provider → S/W provider → System S/W provider

3.2.1 Single HOST Configuration

Figure 3.1 shows an example of a single-host configuration for VSS Hardware Provider.

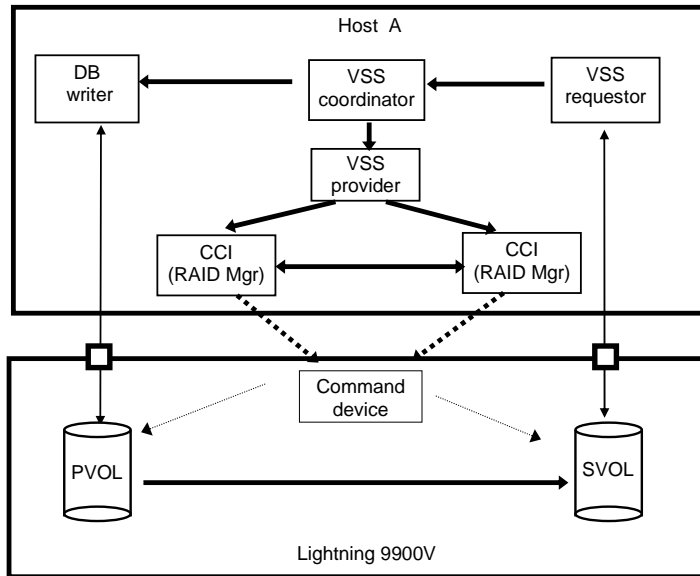


Figure 3.1 Single-Host Configuration for VSS Hardware Provider

3.2.2 Coordination of Shadow Copy Creation

For a description of the roles of the requestor, writer, and provider and the procedure for creating a shadow copy, please refer to the Microsoft® VSS documentation.

3.3 Restrictions on VSS Configurations

VSS and CCI Shadow Copy Provider must be used under the following conditions:

- **Property of the Shadow Copy volume**

The Shadow Copy volume (SVOL) must be created such that it will be detected as “hidden” and “read-only” by the Windows® 2003 OS. Drive letters and/or mount points are not automatically assigned.

VSS requires “INVISIBLE” hidden via SCSI Inquiry as hidden attribute of SVOL. It is possible to support this hidden attribute only for the 9900V and 9500V subsystem, not for 9900. Therefore, the 9900 uses the “NOREAD” attribute to disable SCSI Read command as an alternative for the “INVISIBLE” attribute.

Table 3.1 shows the difference in performance characteristics for the “INVISIBLE” and “NOREAD” attributes of SVOL.

Table 3.1 Hidden Property of SVOL and Performance Characteristic

Subsystem	SVOL Hidden Property	Performance Characteristic		Connectivity with Windows® 2003
		Import Time	Method of Recognition	
9900	NO READ	2-3 minutes	Reboot *	Supported
9900V	INVISIBLE	20-30 seconds	Rescan	Supported
9500V	INVISIBLE	20-30 seconds	Rescan	Supported
9580V, 9585V	INVISIBLE	20-30 seconds	Rescan	Supported

* For 9900, the reboot will be needed only once on SVOL host after pair-creation. Refer to step (8) in section 3.7.2 for details.

- **Snapshots Containing Dynamic Disks**

The native support for dynamic disks cannot accommodate LUNs with duplicate signatures and configuration database contents. The snapshot LUNs must be transported to a different host.

The Logical Disk Manager (LDM) needs to export the copied dynamic disks regardless of VSS. Thus the dynamic disks can only be used on the Export/Import configuration.

When transporting dynamic disk LUNs to a new host, it is best that at least one dynamic disk already exist on the receiving host. This ensures that the disk group identifiers will be unique to both machines.

- **Hardware Snapshots not Supported on MSCS**

MSCS cannot accommodate LUNs with duplicate signatures and partition layout. The snapshot LUNs must be transported to a host outside the cluster.

Thus the Basic disks used for MSCS can only be used on the Export/Import configuration.

- **Using VSS under the Path Manager**

I/O Path Manager must support the Shadow Copy volume as the Plug-and-Play device, and must support all **DeviceIoControl** functions used on the Shadow Copy volume.

In case of HDLM: VSS will not be protected from the path failure, since HDLM does not support all of the **DeviceIoControl** functions that will be in use by VSS.

- **IO during CCI Shadow Copy Provider**

During Commit for Snapshots, VSS (coordinator) is using the “Lovelace” drivers to block any I/O to the source drive snapshot. Therefore if the source drive is specified to the CCI (RAID Mgr) Log directory, the blocked I/O causes the snapshot commit process to deadlock.

If the user does this, the user must specify another drive to the CCI Log directory.

3.4 Relationship Between Requestor and Configurations

Table 3.2 shows the related support between the requestor (backup software) and applicable configurations. The CCI Shadow Copy Provider must be used within scope of the following supported backup software. For information on future support for additional backup software applications, please contact your Hitachi Data Systems account team.

Table 3.2 Backup Software Confirmed with CCI Shadow Copy Provider

VSS Component	Component Name	Applicable Configurations		
		Single Host	Export/Import Host	Transportable
Backup software (Requestor)	NT Backup Microsoft	Supported	Unsupported	Unsupported
	Backup Exec (BEWS) VERITAS	Supported	Future support	Under consideration
Provider	CCI Shadow Copy Provider Hitachi	Supported	Supported	Supported
LDM	Basic Disk	Available	Available	Available
	Basic Disk on MSCS	NA	Available	NA
9900V subsystem	Dynamic Disk	NA	Available	NA
	SI (normal)	Available	Available	Available
	SI (quick)	Available	Available	Available
	TC	NA	NA	NA
	Hi-Copy	NA	NA	NA
9500V subsystem	ShadowImage	Available	Available	Available
	QuickSnap	Available	Available	Available
	TrueCopy	NA	NA	NA

3.5 Installation Procedures

This product provides the following file:

No.	Title	Filename	Installation Location
001	CCI Shadow Copy Provider	\\HORCMTool\RMVSSPRV.exe	D:\RHITACHI\VSS Provider\RMVSSPRV.dll <i>DIR</i> = installation directory (default is \Program Files).

3.5.1 Procedure for New Installation

To install to the servers where the CCI Shadow Copy Provider will be used:

1. Stop Microsoft® Volume Shadow Copy Service by using the following command:

```
C:\>net STOP "Volume Shadow Copy"
<In case of running>
    The Volume Shadow Copy service is stopping.
    The Volume Shadow Copy service was stopped successfully.
< In case of stopped>
    The Volume Shadow Copy service is not started.
```

2. Change the current directory to \\HORCMTool\ where CCI is installed.
3. Execute the **RMVSSPRV.exe** setup program.
4. Restart Microsoft® Volume Shadow Copy Service by using the following command if VSS will not be started:

```
C:\>net START "Volume Shadow Copy"
    The Volume Shadow Copy service is starting.
    The Volume Shadow Copy service was started successfully.
```

3.5.2 Procedure for Update Installation

To install to the servers where the CCI Shadow Copy Provider will be used:

1. Stop Microsoft® Volume Shadow Copy Service by using the following command.

```
C:\>net STOP "Volume Shadow Copy"
<In case of running>
    The Volume Shadow Copy service is stopping.
    The Volume Shadow Copy service was stopped successfully.
< In case of stopped>
    The Volume Shadow Copy service is not started.
```

2. Delete the installed CCI Shadow Copy Provider using the **Add or Remove Programs** control panel.
3. Change the current directory to '**HORCM\Tool** where CCI is installed.
4. Execute the **RMVSSPRV.exe** setup program.
5. Restart Microsoft® Volume Shadow Copy Service by using the following command if VSS will not be started.

```
C:\>net START "Volume Shadow Copy"
    The Volume Shadow Copy service is starting.
    The Volume Shadow Copy service was started successfully.
```

3.5.3 Version Confirmation after Installation

After a new installation or update, verify the version information (**Version**) by using the following command:

```
C:\>vssadmin list providers
vssadmin 1.1 - Volume Shadow Copy Service administrative command-line tool
(C) Copyright 2001 Microsoft Corp.

Provider name: 'RM Shadow Copy Provider'
  Provider type: Hardware
  Provider Id: {748babd3-8c62-4b3d-b6b7-430b5f858c74}
  Version: 01-01-03/02

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

3.6 Uninstallation Procedure

To uninstall to the servers where the CCI Shadow Copy Provider was used:

1. Stop Microsoft® Volume Shadow Copy Service by using the following command:

```
C:\>net STOP "Volume Shadow Copy"
```

2. Delete the installed CCI Shadow Copy Provider using the **Add or Remove Programs** control panel.
3. Restart the Microsoft® Volume Shadow Copy Service with the following command if VSS will not be started:

```
C:\>net START "Volume Shadow Copy"
```

3.7 VSS Start-up Procedures on Single Host

3.7.1 Setting the System Environment Variables

To set the system environment variables:

1. Define the system environment variables as shown in Table 3.3.
2. Reboot the Windows® system. VSS will be started as a service automatically.

Table 3.3 Setting the System Environment Variables

Variable	Value
VSHTCHORCMINST_LOCAL	Specifies the CCI Instance number for PVOL side.
VSHTCHORCMINST_REMOTE	Specifies the CCI Instance number for SVOL side.
VSHTCHOMRCF_MUN	Specifies the MUN specified to PVOL in the CCI configuration file.

3.7.2 Setting the CCI Environment

This example assumes the Instance Number and the target volume for backup as follows:

- VSHTCHORCMINST_LOCAL = 50
- VSHTCHORCMINST_REMOTE = 51
- VSHTCHOMRCF_MUN = 2
- The target volume for back-up is mounted as “E: drive” on Harddisk1.
- The requestor (backup software) is ntbackup.exe.

Note: The following procedure must be performed for each change to the `horcm*.conf` file. VSS coordinator will activate the CCI Shadow Copy provider automatically, and then CCI Shadow Copy provider will perform the CCI commands when backup program is executed. Therefore CCI must be started prior to executing the backup program.

To set the CCI environment:

1. Discover and describe the command device for `%windir%\horcm50.conf`. CCI uses the command device, so you need to discover the command device (xxxx-CM).

```
C:\HORCM\etc>ingraid -CLI $Phy
DEVICE_FILE      PORT      SERIAL    LDEV CTG   H/M/12  SSID R:Group  PRODUCT_ID
Harddisk0      CL2-C    62496    16  -     -       -       - OPEN-3-CM
Harddisk1        CL2-C     62496     18   -     s/s/ss  0004 5:01-04 OPEN-3
Harddisk2        CL2-C     62496     19   -     s/s/ss  0004 5:01-04 OPEN-3
Harddisk3        -         -         -    -     -       -       - L040L2

C:\HORCM\etc>ingraid -CLI $LETALL
DEVICE_FILE      PORT      SERIAL    LDEV CTG   H/M/12  SSID R:Group  PRODUCT_ID
E:\Vol12\Dsk1  CL2-C    62496    18  -     s/s/ss  0004 5:01-04 OPEN-3
D:\Vol1\Dsk3     -         -         -    -     -       -       - L040L2
```

`%windir%\horcm50.conf`

```
HORCM_MON
#ip_address      service      poll(10ms)  timeout(10ms)
127.0.0.1        52050        1000        3000

HORCM_CMD
#dev_name        dev_name     dev_name
\\.\PhysicalDrive0
```

You will have to start HORCM without a description for `HORCM_DEV` and `HORCM_INST` because **target ID and LUN are Unknown**. You can find out about a mapping of a physical device with a logical name easily by using the `raidscan -find` command option.

2. Execute `horcmstart 50` as background.

```
C:\HORCM\etc>horcmstart 50
starting HORCM inst 50
HORCM inst 50 starts successfully.
```

3. Verify a physical mapping.

```
C:\HORCM\etc>set HORCMINST=50
b C:\HORCM\etc>raidscan -pi $Phys -find
DEVICE_FILE      UID  S/F  PORT  TARG  LUN  SERIAL  LDEV  PRODUCT_ID
Harddisk0        0   F   CL2-C  25   0    62496   16   OPEN-3-CM
Harddisk1        0   F   CL2-C  25   1    62496   18   OPEN-3
Harddisk2        0   F   CL2-C  25   2    62496   19   OPEN-3
```

4. Shut down horcmstart 50.

```
C:\HORCM\etc>horcmshutdown 50
inst 50:
HORCM Shutdown inst 50 !!!
```

5. Describe the known HORCM_DEV on %windir%\horcm50.conf.

%windir%\horcm50.conf for PVOL

```
HORCM_MON
#ip_address      service          poll(10ms)      timeout(10ms)
127.0.0.1        52050           1000            3000

HORCM_CMD
#dev_name        dev_name        dev_name
\\.\PhysicalDrive0

HORCM_DEV
#dev_group      dev_name        port#           TargetID        LU#           MU#
snap            snapdev1        CL2-C          25              1             2

HORCM_INST
#dev_group      ip_address      service
snap            127.0.0.1      52051
```

%windir%\horcm51.conf for SVOL

```
HORCM_MON
#ip_address      service          poll(10ms)      timeout(10ms)
127.0.0.1        52051           1000            3000

HORCM_CMD
#dev_name        dev_name        dev_name
\\.\PhysicalDrive0

HORCM_DEV
#dev_group      dev_name        port#           TargetID        LU#           MU#
snap            snapdev1        CL2-C          25              2             0

HORCM_INST
#dev_group      ip_address      service
snap            127.0.0.1      52050
```

6. Start horcmstart 50 51.

```
C:\HORCM\etc>horcmstart 50 51
starting HORCM inst 50
HORCM inst 50 starts successfully.
starting HORCM inst 51
HORCM inst 51 starts successfully.

C:\HORCM\etc>set HORCMINST=51
C:\HORCM\etc>set HORCC_MRCF=1

C:\HORCM\etc>pairdisplay -g snap -fdc
Group   PairVol(L/R) Device_File      ,Seq#,LDEV#.P/S,Status,   % ,P-LDEV# M
snap    snapdev1(L)  Harddisk2      62496  19..SMPL  ----,-----  ---- -
snap    snapdev1(R)  Harddisk1      62496  18..SMPL  ----,-----  ---- -
```

7. In case of "INVISIBLE" SVOL:

- a) Create and hide an Invisible SVOL (-vg idb option hides a LUN from SCSI Inquiry).

```
C:\HORCM\etc>raidvchkset -g snap -vg idb (only valid for 9900V, 9580V, 9585V)
C:\HORCM\etc>paircreate -g snap -vr -m noread

C:\HORCM\etc>pairdisplay -g snap
Group   PairVol(L/R) (Port#,TID,LU-M),Seq#,LDEV#.P/S,Status, Seq#,P-LDEV# M
snap    snapdev1(L) (CL2-C ,25, 2-0)62496 19..S-VOL PAIR,----- 18 -
snap    snapdev1(R) (CL2-C ,25, 1-2)62496 18..P-VOL PAIR,62496 19 N
```

- b) Perform Rescan disk. VSS needs to make the hidden volumes for SVOL, so you must execute the Rescan disk by using the diskpart command.

```
C:\HORCM\etc>diskpart
:
DISKPART> rescan
Please wait while DiskPart scans your configuration...
DiskPart has finished scanning your configuration.
```

8. In case of "NO READ" SVOL:

- a) Create and hide SVOL with NO READ.

```
C:\HORCM\etc>paircreate -g snap -vr -m noread
C:\HORCM\etc>pairdisplay -g snap
Group   PairVol(L/R) (Port#,TID,LU-M),Seq#,LDEV#.P/S,Status, Seq#,P-LDEV# M
snap    snapdev1(L) (CL2-C ,25, 2-0)62496 19..S-VOL PAIR,----- 18 -
snap    snapdev1(R) (CL2-C ,25, 1-2)62496 18..P-VOL PAIR,62496 19 N
```

- b) Perform REBOOT of the system. VSS needs to make the hidden volumes for SVOL, so you must reboot the system. You only need to reboot the SVOL host (back-up server), and only once after "paircreate -m noread" on SVOL host.

- c) Start horcmstart 50 51.

```
C:\HORCM\etc>horcmstart 50 51
starting HORCM inst 50
HORCM inst 50 starts successfully.
starting HORCM inst 51
HORCM inst 51 starts successfully.
```

Note: In case of the export and import host configuration, VSHTCHORCMINST_LOCAL variable must be set on PVOL side (export) host, and VSHTCHORCMINST_REMOTE variable must be set on SVOL side(import) host. You need to change the configuration definition file for the export and import host configuration. Refer to sections 2.9 and 3.4 of the *Hitachi Lightning 9900V and 9900 CCI User and Reference Guide* for more details.

- PVOL side host must be started by “horcmstart 50”, and HORCMINST=50 variable must be set.
- Also SVOL side host similarly must be started by “horcmstart 51”, and HORCMINST=51 variable must be set.
- PVOL side host must be connected only PVOLs, and SVOL side host must be connected only SVOLs.

3.7.3 Executing the Backup

You are able to execute the backup program by specifying the target volume for backup after setting the CCI environment.

To execute the backup program:

1. Execute the NT backup file (%SystemRoot%\system32\ntbackup.exe) by specifying “E: drive” on the PVOL.
2. If needed, verify that CCI Shadow Copy Provider is working by checking the **Status** field of the CCI command (**pairdisplay -g snap**):
 - When NT backup has been running, the pairdisplay state is “PVOL_PSUS and SVOL_COPY” or “PVOL_PSUS and SVOL_SSUS”.
 - When NT backup has been deleting the snap (**OnLunEmpty()** in H/W provider is called by VSS), the pairdisplay state is “PVOL_COPY and SVOL_COPY” or “PVOL_PAIR and SVOL_PAIR”.

3.7.4 Notes on VSS Operation

- **Command Control Interface (CCI)**

CCI must be started with the administrator privilege, when the user will start the CCI as a service.

If CCI will be started with the system privilege, then CCI commands via DOS prompt will be unable to attach to the CCI.

- **Independent VDS**

The CCI Shadow Copy Provider and CCI do not use the VDS interface.

CCI Shadow Copy Provider and CCI can support two server configurations for the "OFF HOST Backup" (one is export server, another is import server), but these configurations must be supported via the back-up requestor by transporting the XML file between the export and import servers.

- **Required LUN**

VSS inquires about whether or not the VSS provider is supporting the LUN using the SCSI Inquiry Standard Page, Page0x80, and Page0x83. Also, VSS checks all hardware properties of a LUN of SVOL which the provider reported. Therefore, the following is required as SCSI Inquiries of a LUN.

- SCSI Inquiry Standard Page

The Vendor Identification must be "HITACHI".

The Product Identification must be set as the effective character strings (NOT all space strings).

The Product Revision Level must be set as the effective character string (NOT all space strings), and the Product Revision Level must be identical between PVOL and SVOL.

- SCSI Inquiry Page0x80

The Product Serial Number must be set as the effective character strings (NOT all space strings), and the Product Serial Number must be identical between PVOL and SVOL.

- SCSI Inquiry Page0x83

The Device Identification must include the serial number and LDEV number.

3.8 Troubleshooting VSS Hardware Provider

If you are having trouble installing or running VSS Hardware Provider, please refer to Table 3.4 for general troubleshooting information.

Table 3.4 General Troubleshooting for VSS Hardware Provider

Problem	Description
VSS does not work with the Disk Manager tool (LDM).	Because VSS depends on Plug-and-Play, we recommend that you do not use the LDM tool while VSS is running.
Event log increases at every backup.	A warning message is recorded to the event log at time every backup, because VSS uses Plug-and-Play for mounting the copied SVOL that has the same signature to PVOL. Therefore, we recommend that the administrator regularly clear the Event log.
LUN#0 cannot use as SVOL.	Some HBA drivers do not scan all LUNs on a port when LUN#0 is hidden as SVOL. Therefore, we recommend that the user does not LUN#0 as SVOL for all HBA driver.

3.9 Checking VSS Hardware Provider Error Messages

The VSS Hardware Provider generates an error message when an error condition occurs. The error message includes the error code. All VSS Provider error messages are output to the Windows® Event Log.

Table 3.5 Error Messages Generated by CCI Shadow Copy Provider (continues on the next page)

Error Message	Error Cause	Correction
[EV_ERPERM] Permission denied with the VSS hardware provider	CCI Shadow Copy Provider is activated except for the Local System account.	Confirm the CCI Shadow Copy Provider start up account.
[EV_ENOMEM] The memory is insufficient	The memory for executing a CCI Shadow Copy Provider could not be retained.	Increase the virtual memory capacity of the whole system, or terminate unnecessary programs or daemon processes that are running simultaneously.
[EV_INVSTP] Invalid pair status	The pair status of a target volume is not appropriate.	Use the pairdisplay command to confirm volume status.
[EV_ATTHOR] Can't attach to a HORCM daemon	The HORCM daemon is not working.	Verify whether the HORCM daemon is working.
[EV_CMDIOE] Control command I/O error	Control command I/O error, or rejected	Remove a cause of an error after confirming with system error code.
[EV_EGETEV] An error occurred in GetEnvironmentVariable()	The system environment variable could not be obtained from GetEnvironmentVariable() system call.	Verify whether the system environment variable is defined.
[EV_ENOSUP] No supported device	The specified device is a command device or unsupported disk.	Verify whether a target disk is the supported disk.
[EV_ENOINQ] No such inquiry	An Error occurred in the inquiry to the specified device.	Check the connection to the device.
[EV_ENOOBJ] Not found object	The SnapshotSetID that is specified by the Provider is invalid.	Check the Event log for any errors pertaining to Shadow Copy.
[EV_ENOSER] No such serial number	A Serial number could not be acquired from the specified device information.	Check the Event log for any errors pertaining to Shadow Copy.
[EV_ENRMCM] A RAID Manager command binary file is not found	The file of CCI command was removed by an operation miss.	Reinstall CCI.
[EV_ENRMPH] RAID Manager was not found in the "HORCM\ETC" directory in C-Z drives	The directory "HORCM\ETC" was removed by an operation miss.	Reinstall CCI.
[EV_ESETEV] The system environment variable could not be set	The system environment variable could not be set on SetEnvironmentVariable() system call.	Please remove a cause of an error after confirming it with event log if system is unstable with event log.
[EV_EXCEPT] An exception occurred	An Exception occurred during a process of CCI Shadow Copy Provider.	Please remove a cause of an error after confirming it with event log if system is unstable with event log.
[EV_INVARG] Invalid argument	The argument which a coordinator specified is invalid.	Please remove a cause of an error after confirming it with event log if an error about Shadow Copy Service is written in it.

Table 3.5 Error Messages Generated by CCI Shadow Copy Provider (continued)

Error Message	Error Cause	Correction
[EV_INVSEQ] Invalid sequence	The order specified from a coordinator is invalid.	Please remove a cause of an error after confirming it with event log if an error about Shadow Copy Service is written in it
[EV_EOPDEV] Cannot open a device	The specified device special file failed to open.	Please remove a cause of an error after confirming it with system error code.

Chapter 4 Protection Service Messages

This chapter describes the messages added for the VSS linkage function. For the other messages, see the *HiCommand Protection Services User and Reference Guide*.

Table 4.1 Messages for the VSS Linkage Function (continues on the next page)

Message ID	Message Text	Description and Recommended Action
KAVX5000-E	Backup by VSS cannot be performed in this OS.	Backup by VSS was specified in an operating system not supported by the VSS linkage function. This function can be used in Windows Server® 2003, Enterprise Edition.
KAVX5001-E	Backup by VSS cannot be performed in the cluster environment.	Backup by VSS was specified in a cluster environment. The VSS linkage function cannot be used in a cluster environment.
KAVX5002-E	The system environment variable VSHTCHOMRCF_MUN is not set, or an illegal value is set. Make sure that VSS has been set up correctly.	The backup generation used for backup by VSS is invalid. Possible causes are as follows: <ol style="list-style-type: none"> 1. The system environment variable VSHTCHOMRCF_MUN has not been set. 2. The system was not restarted after the system environment variable VSHTCHOMRCF_MUN was set. 3. The MU number set in the system environment variable VSHTCHOMRCF_MUN contains an error. Check the system environment variable VSHTCHOMRCF_MUN settings and the CCI settings.
KAVX5003-E	CCI Shadow Copy Provider could not be used. Make sure that VSS has been set up correctly.	The VSS hardware provider (CCI Shadow Copy Provider) did not operate. Possible causes are as follows: <ol style="list-style-type: none"> 1. CCI Shadow Copy Provider has not been installed. 2. The system environment variable VSHTCHORCMINST_LOCAL has not been set correctly. 3. The system was not restarted after the system environment variable VSHTCHORCMINST_LOCAL was set. Make sure the environment settings for backup by VSS have been set correctly.
KAVX5004-E	A timeout error occurred in the writer. writer name = <i>writer-name</i>	An attempt to acquire a backup failed because a frozen-state timeout occurred in the writer. Possible causes are as follows: <ol style="list-style-type: none"> 1. It took a long time to split a volume pair because the storage group uses many disks. 2. It took a long time to split a volume pair because the system was heavily loaded. Check the disk configuration by referring to the notes about backup by VSS.
DRM-10434	An error occurred in VSS.	An unexpected error occurred in the API of VSS. Collect the information indicated in the Troubleshooting chapter of the <i>HiCommand Protection Services User and Reference Guide</i> , and then contact the Support Center.
DRM-10435	An error occurred in Virtual Disk Service.	An unexpected error occurred in the API of Virtual Disk Service. Collect the information indicated in 6. Troubleshooting in the Troubleshooting chapter of the <i>HiCommand Protection Services User and Reference Guide</i> , and then contact the Support Center.

Table 4.1 Messages for the VSS Linkage Function (continued)

Message ID	Message Text	Description and Recommended Action
KAVX1608-E	Information stores that have not been mounted exist. For a storage group to be backed up using VSS, all information stores must be mounted.	The system stops processing if the Exchange Information Store service is inactive during backup by VSS, or if there is an information store that was not mounted during backup by VSS. Mount all the information stores under the storage group you want to back up, and then perform a backup.
KAVX1609-E	The system stops processing if information from Active Directory and VSS do not match.	The system stops processing if the information acquired from VSS differs from that acquired from Active Directory. Possible causes are as follows: <ol style="list-style-type: none"> 1. The Exchange Server configuration was changed during execution of a backup command. 2. An information store was mounted or unmounted during execution of a backup command. 3. The mounted storage group name or the mounted information store name was changed. Do not perform the above operations during execution of a backup command. If the mounted storage group or the mounted information store name was changed, unmount all information stores related to the storage group once, and then re-mount the information stores.

Acronyms and Abbreviations

API	application program interface
ASCII	American Standard Code for Information Interchange
CCI	Command Control Interface (also called RAID Manager)
CPU	central processing unit
DBMS	database management system
DKC	disk controller
FS	file system
FTP	file transfer protocol
GUID	global unique identifier
ID	identifier, identification
IIS	Internet Information Services
LDEV	logical device
LDM	Logical Disk Manager
LUN	logical unit number
LVM	Logical Volume Manager, logical volume manager
MB	megabyte
MU	mirror unit
OCI	Oracle call interface
ODBC	open database connectivity
OS	operating system
PnP	plug-n-play
P-VOL	primary volume
RAID	redundant array of inexpensive disks
RM	RAID Manager (another name for CCI)
SMPL	simplex
SQL	structured query language
S-VOL	secondary volume
TCO	total cost of ownership
TID	target ID
VDI	Virtual Device Interface
VDS	Virtual Disk Service
VSS	Volume Shadow Copy Service
VxVM	VERITAS Volume Manager VERITAS Volume Manager

