HITACHI
DATA SYSTEMS

HiCommand® Protection Manager VSS Backup of Microsoft® Exchange Server Getting Started Guide

MK-96HC127-02

Trademarks

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-96HC127-P	February 2006	Preliminary release
MK-96HC127-00	June 2006	Initial release, supersedes and replaces version –P
MK-96HC127-01	January 2007	Update release for V5.5, supersedes and replaces version –00
MK-96HC127-02	May 2007	Update release for V5.7, supersedes and replaces version –01

Referenced Documents

- *HiCommand Protection Manager User's Guide* (MK-94HC070)
- *HiCommand Protection Manager Console User's Guide* (MK-94HC071)
- *HiCommand Protection Manager Command Reference* (MK-94HC072)
- *HiCommand Protection Manager Messages* (MK-94HC073)

Related Documents

- *Hitachi RAID Manager Shadow Copy Provider for Microsoft® Volume Shadow Copy Service (VSS) Installation Guide* (MK-94RD166)
- *Hitachi Command Control Interface (CCI) User and Reference Guide* (MK-90RD011)
- *Hitachi TagmaStore Adaptable Modular Storage Command Control Interface (CCI) User and Reference Guide* (MK-95DF701)
- *Hitachi Freedom Storage Thunder 9520 V Series Command Control Interface (CCI) User and Reference Guide* (MK-94DF687)
- *Hitachi Freedom Storage Thunder 9500 V Series Command Control Interface (CCI) User and Reference Guide* (MK-92DF609)
- *Hitachi Freedom Storage Thunder 9200 Command Control Interface (CCI) for ShadowImage User and Reference Guide* (MK-91DF557)

Readme and Release Notes Contents

These files can be found on the installation CD. They contain requirements and notes for use of HiCommand Protection Manager that may not be fully described in the manual. Be sure to review these files before installing HiCommand Protection Manager.

Preface

The *HiCommand Protection Manager Getting Started Guide for VSS Backup of Microsoft Exchange Server* describes how to install and setup HiCommand Protection Manager for Microsoft Exchange, using a Volume Shadow Copy Service (VSS) integration scenario. It also contains information about the prerequisite components, which include CCI, RM Shadow Copy Provider, and PVOL/SVOL setup.

This document is not intended to replace product manuals; rather, it is a concise reference for those who need to implement Protection Manager and must quickly grasp the implementation procedures. Therefore, this document should be used as a supplemental reference to the complete product manuals and release notes. Please consult those documents for detailed instructions and background information.

Software Version

This document revision applies to HiCommand Protection Manager software version 5.7

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 35-10
  Hitachi Data Systems
  10277 Scripps Ranch Blvd.
  San Diego, CA 92131

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

Contents

List of Figures

List of Tables

Chapter 1 Overview of the VSS Backup

This chapter provides an overview of the VSS Backup process.

- Understanding the VSS Backup Procedure (see section 1.1)

1.1 Understanding the VSS Backup Procedure

Figure 1-1 provides a visual representation of the VSS backup process. The Protection Manager main program is designed to be installed on the production Exchange server, but it requires a separate physical server called the *Import server*. The Import server can work as a "Backup server" to backup data from SVOL to TAPE (you cannot assign a server within an Exchange cluster). The two main requirements for an Import server are that Protection Manager:

- Hides the INQUIRY attribute of the target SVOL from the Import server
- Unmounts the target SVOL from the Import server

These are part of the Microsoft guidelines for VSS compliance.

The processes running on both servers work together to perform VSS backup.

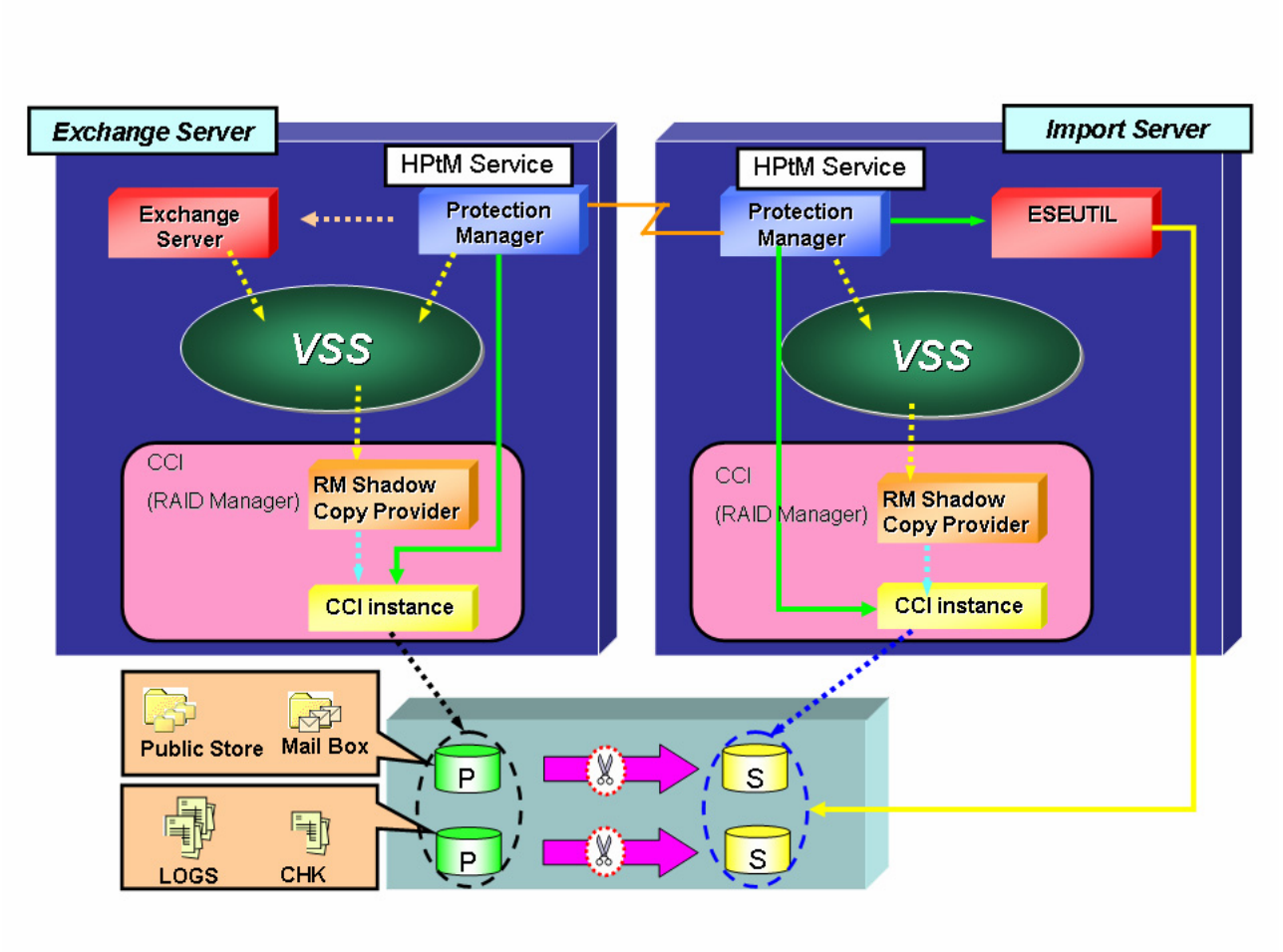

Figure 1-1 VSS Backup Process

1.1.1 Reviewing the Process Flow

Table 1.1 lists the order of the processes for the VSS Backup procedure. Please note that the Protection Manager Service on the Exchange server and Import server are started prior to running the Protection Manager backup command. Afterward, Protection Manager is ready to execute the `drmexgbackup` command, while the `-mode vss` option on the Exchange server invokes the entire backup process.

Regarding the Exchange database states:

- **Online** indicates that the read and write access is available.
- **Online (Freeze)** indicates that the read access is available, but the write access is pending.

Table 1.1 VSS Backup Process Flow

Step	Server	Procedure	CCI Pair Status	Exchange Database
1	Exchange	Protection Manager checks the cluster resources related to the target Exchange server, if cluster environment	PSUS/SSUS or PAIR	Online
2	Exchange	Protection Manager gets the information of the Exchange information store		
3	Exchange	Protection Manager communicates to the Import server by using Protection Manager Service		
4	Exchange	Protection Manager gets the physical object mapping information (mount point, Harddisk#, CCI copy pair name, SERIAL#, LDEV# and so on) from its internal repository		
5	Exchange	Protection Manager selects the target SVOL for this VSS backup		
6	Exchange	Protection Manager starts-up the CCI instance, if not started		
7	Exchange	Protection Manager sets the CCI environment variables (HORCMINST, HORCC_MRCF) for the pair operations		
8	Exchange	Protection Manager checks the target CCI copy pair status		
9	Exchange	Protection Manager resyncs (pairresync) the target CCI copy pair, if not PAIR status	PAIR or COPY	Online
10	Exchange	Protection Manager deletes the old backup catalog information in its internal repository		
11	Import	Protection Manager hides the INQUIRY attribute of the target SVOL from the Import server		
12	Exchange	Protection Manager checks whether the target CCI copy pair status is PAIR	PAIR	

Step	Server	Procedure	CCI Pair Status	Exchange Database
13	Exchange	Protection Manager requests VSS to keep consistent image as “Shadow Copy” and then VSS asks the VSS writer (Exchange Server) to freeze I/O operations	PAIR	Online (Freeze)
14	Exchange	VSS asks the VSS provider (RM Shadow Copy Provider) to split the target CCI copy pair	PSUS/SSUS	
15	Exchange	VSS asks the VSS writer (Exchange Server) to thaw I/O operations		Online
16	Exchange	Protection Manager checks whether the CCI copy pair status is PSUS/SSUS		
17	Import	Protection Manager requests VSS to import (mount) the target SVOL to the Import server		
18	Import	Protection Manager verifies the backed up Exchange data by using `ESEUTIL` command		
19	Import	Protection Manager unmounts the target SVOL from the Import server		
20	Exchange	Protection Manager resisters the backup catalog information to its internal repository		

Chapter 2 Reviewing Prerequisite Tasks for VSS Backup

This chapter describes all components that are required for VSS Backup.

- Reviewing and Gathering Requirements (see section 2.1)
- Reviewing the Support Matrices (see section 2.2)

2.1 Reviewing and Gathering Requirements

The Import server (Backup server) is required even if backed up data (SVOL) is not intended to be backed up to tape. This is because the Backup server imports VSS snapshots and verifies the Exchange database, as illustrated in the following example.

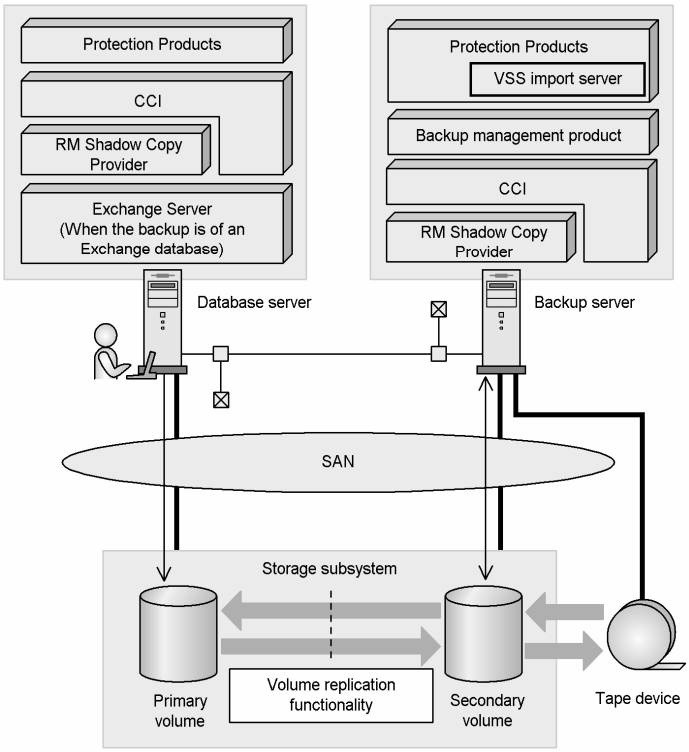

Figure 2-1 Example Hardware and Server Configuration

2.1.1 Hardware and Server Requirements

Table 2.1 lists the hardware and server requirements.

Table 2.1 List of Hardware and Server Requirements

Requirement	Details	Remarks
Operating Systems	Windows Server 2003 Enterprise Edition (no SP) ▪ Hotfix: KB833167 ▪ Protection Manager 4.1 or later	For Exchange Server 2003
	Windows Server 2003 Standard Edition (SP1) Windows Server 2003 Enterprise Edition (SP1) Windows Server 2003 Datacenter Edition (SP1) Windows Server 2003 R2, Standard Edition Windows Server 2003 R2, Enterprise Edition Windows Server 2003 R2, Datacenter Edition ▪ Hotfix: KB891957 ▪ Hotfix: KB903650 (online restore–MSCS extended maintenance mode) ▪ Hotfix: KB912063 ▪ Protection Manager 4.1.1 or later	For Exchange Server 2003
	Windows Server 2003 Standard Edition (SP2) Windows Server 2003 Enterprise Edition (SP2) Windows Server 2003 Datacenter Edition (SP2) Windows Server 2003 R2, Standard Edition (SP2) Windows Server 2003 R2, Enterprise Edition (SP2) Windows Server 2003 R2, Datacenter Edition (SP2) ▪ Hotfix: KB903650 (online restore–MSCS extended maintenance mode) ▪ Protection Manager 5.7.0 or later	For Exchange Server 2003
	Windows Server 2003 Standard x64 Edition (SP1) Windows Server 2003 Enterprise x64 Edition (SP1) Windows Server 2003 Datacenter x64 Edition (SP1) Windows Server 2003 R2, Standard x64 Edition Windows Server 2003 R2, Enterprise x64 Edition Windows Server 2003 R2, Datacenter x64 Edition ▪ Hotfix: KB891957 ▪ Hotfix: KB903081 ▪ Hotfix: KB903650 (online restore–MSCS extended maintenance mode) ▪ Hotfix: KB912063 ▪ Protection Manager 5.7.0 or later	For Exchange Server 2007
	Windows Server 2003 Standard x64 Edition (SP2) Windows Server 2003 Enterprise x64 Edition (SP2) Windows Server 2003 Datacenter x64 Edition (SP2) Windows Server 2003 R2, Standard x64 Edition (SP2) Windows Server 2003 R2, Enterprise x64 Edition (SP2) Windows Server 2003 R2, Datacenter x64 Edition (SP2)	For Exchange Server 2007

Requirement	Details	Remarks
	▪ Hotfix: KB903650 (online restore–MSCS extended maintenance mode) ▪ Protection Manager 5.7.0 or later	
	Use the same OS version across Exchange server and Import server (Backup server) The combination of Windows server2003(x64) on the Exchange server and Windows2003(32 bit) on the Import server is available. Please see the release note for details.	
Windows Server 2003 Enterprise Edition Installation	Uninstall the current version before installing the most recent version. Due to a known issue with the interference with VSS functions, never perform an upgrade installation.	
Host Bus Adapter (HBA) Driver	Use the same HBA driver for Exchange server and Backup server (StorPort is recommended). The HBA driver supports VSS functions.	
Command Device Access	The Exchange server and the Import (Backup) server must have access to the command device of the target storage subsystem.	

2.1.2 CCI Requirements

Table 2.2 lists the CCI requirements.

Table 2.2 List of CCI Requirements

Requirement	Details
Installation	CCI (RAID Manager) must be installed on both the Exchange server and the Import (Backup) server. The installation path should be the Windows system drive (otherwise, VSS does not properly function).
Commands	▪ CCI copy pairs must be created before executing Protection Manager commands. ▪ Protection Manager commands operate the pair volumes for ShadowImage, Copy-On-Write (COW), and True Copy (Sync). ▪ Protection Manager commands do not support operation of True Copy (Async), Universal Replicator, Cross-system Copy or Hitachi Hi-Copy paired volumes.
MU Numbers	▪ When using True Copy, do not enter an MU number in the MU# setting in the CCI definition file (horcm#.conf). If 0 is defined for the MU# setting, volume information for the “True Copy pair will not be stored in the dictionary map. ▪ When using Universal Replicator, define h0 (h and a generation number) for the MU# setting in the CCI definition file (horcm#.conf). If 0 is defined for MU#, the Universal Replicator information will not be stored in the dictionary map. ▪ To backup multiple primary volumes to multiple generations, specify the same dev_group name for all pair volumes that have the same MU#.
Primary and Secondary Volumes	When the CCI instance for the primary volume and the secondary volume are defined on the different servers, make sure that you start the CCI instance for the secondary volume in advance.
Import Server	You cannot use a server within an Exchange cluster as an Import server. Instead, use a backup server that backs up Exchange data from SVOL to TAPE.

2.1.3 VSS Hardware Provider Requirements

- Raid Manager Shadow Copy Provider must be installed on the Exchange server and on the Import (Backup) server. Its installation path should be the Windows system drive.
- When using the VSS backup function, make sure that the storage subsystem model, the CCI version, and the microcode version are appropriate to that function.

2.1.4 Microsoft Exchange Server Requirements

Table 2.3 lists the hardware and server requirements.

Table 2.3 List of Hardware and Server Requirements

Requirement	Details
Microsoft Exchange	▪ Microsoft Exchange Server 2003 Standard Edition (Service Pack 1) ▪ Microsoft Exchange Server 2003 Enterprise Edition (Service Pack 1) ▪ Microsoft Exchange Server 2003 Standard Edition (Service Pack 2) ▪ Microsoft Exchange Server 2003 Enterprise Edition (Service Pack 2) ▪ Microsoft Exchange Server 2007 Standard Edition ▪ Microsoft Exchange Server 2007 Enterprise Edition ***Note***: ▪ For Exchange 2003 Service Pack 1, you need to apply Microsoft hotfix 892514. ▪ For Exchange 2007, you need to apply Microsoft hotfix 898790, 918980, and 922931.
	The following files under the target Exchange Storage Group are backed up by Protection Manager for Exchange Server: ▪ Data files: *.edb, *.stm (Only for Exchange 2003) ▪ Transaction log files: *.log ▪ Checkpoint files: *.chk
Files	▪ The files to be backed up must all be placed on a RAID volume defined and created as a CCI copy pair. ▪ Transaction log files (*.log) and data files (*.edb and *.stm) must be located on a separate volume. ▪ When using VSS backup, data files (*.edb and *.stm) and checkpoint files (*.chk) cannot exist together in a same volume. ▪ When using Information Store (DB) restore granularity with Roll-Forward, the Information Store data files (*.edb and *.stm) must be located on the separate volumes from other data files.
Backup/Restore/Repair	▪ Backup and restore operations using VSS cannot be performed for storage groups that use the circulation log. ▪ The Recovery Storage Group for Exchange Server cannot be backed up. ▪ When performing VSS backup, the Information Store according to target Storage Group must all be in mounted status. However, the Information Store can be restored even if it is in dismounted status. ▪ When repairing Information store or performing defragmentation with ESEUTIL (ESEUTIL /p or ESEUTIL /d), change the name of database and backup images made with Protection Manager. Otherwise, these operations cannot be restored or recovered. Always backup the Exchange database immediately after performing the `ESEUTIL` command.

2.1.5 Other Requirements

- When performing backup or restoration on the Microsoft Exchange server, make sure that the secondary volumes involved are not mounted to any server in advance.
- Protection Manager Service must be started on the Exchange server and Import server prior to running a backup or restore.
- Update the dictionary map file (drmexgdisplay –refresh) before performing backup in any of the following situations concerning Exchange Server objects, File Systems, and/or CCI definition files (horcm#.conf):
  - A new Exchange Storage Group or Information Store was added.
  - A new file system to do with target Exchange Server was mounted.
  - A file system related to the target Exchange Server was unmounted.
  - CCI definition file (horcm#.conf) concerning backup target Exchange Server was changed, such as the adding or deleting of a CCI copy pair.
- If VERITAS Backup Exec Advanced Open File Option is installed on either the Exchange server or the backup server, please apply patch VSP1.04.
- If VSS backup is aborted by system failure etc, the Read-Only and Hidden attributes may be left in the backup target volume. If these attributes are left, the drive name is not assigned and Exchange Server will not correctly operate at the system startup. To correct the issue, clear the attributes according to Microsoft technical Article 840781.
  Note: Microsoft technical article 840781 is also required to apply the hotfix described in Microsoft technical article 831112.
- When using Windows Server 2003 with Service Pack 1 and the firewall function provided by the operating system, note the following points:
  - You must specify firewall settings for the communication ports for CCI.
  - To use VSS, you must execute the following command on the backup server to specify the firewall settings for the VSS import server:
    <Protection-Manager-installation-folder>`\bin\util\drmaddfwlist.bat`
  - To execute the extended commands for FTP transmission (`EX_DRM_FTP_PUT` and `EX_DRM_FTP_PUT`), you must specify firewall settings for the FTP Publishing Service. For details, see *Port requirements for Microsoft Windows server system* (http://support.microsoft.com/default.aspx?scid=kb;en-us;832017).
- If Protection Manager takes multiple generations of backup with VSS, or configured in MSCS, these SVOLs must be hidden from the operating system. Because the SVOLs taken by array-based replication are exact replicas of PVOLs and have the same disk signature, the operating system tends to overwrite when multiple SVOLs are presented. Restoring the SVOL results in MSCS failing to bring the PVOL back online, because MSCS perceives that it is not available. Selecting the **Dynamic recognition of secondary volume** option on Setup GUI prevents this from happening. For details of the procedure, see sections 4.2 and 4.3.

2.2 Reviewing the Support Matrices

2.2.1 VSS versus Subsystem and Copy Functions

The following table lists the supported storage subsystems and copy functions.

Table 2.4 Storage Subsystems and Copy Functions Matrix

	UR	TC (Async)/TCE	TC (Sync)	SI	COW
USP/NSC	Not Supported	Not Supported	Supported	Supported	Supported
AMS	Not Applicable	Not Supported	Supported	Supported	Supported
WMS	Not Applicable	Not Applicable	Supported	Supported	Supported
9900V	Not Applicable	Not Supported	Supported	Supported	Not Applicable
9500V	Not Applicable	Not Applicable	Supported	Supported	Supported

2.2.2 VSS versus Volume Manager and Clusters

The following table lists the supported volume managers and clusters.

Table 2.5 Volume Manager and Cluster Support Matrix

			Shadow Image / Quick Shadow	True Copy (Sync)	Notes
LDM	Basic Disk	No Cluster	Supported	Supported	
		MSCS	Supported	Supported	
		VCS	—	—	Requires volumes to be managed by VxVM
	Dynamic Disk	No Cluster	—	—	Protection Manager does NOT support Dynamic Disk
		MSCS	—	—	MSCS does NOT support Dynamic Disk
		VCS	—	—	Requires volumes to be managed by VxVM
VxVM	Basic Disk	No Cluster	—	—	VxVM (VERITAS Storage Foundation for Windows 4.3 MP1) does NOT support third party VSS hardware providers, including HDS.
		MSCS			
		VCS			
	Dynamic Disk	No Cluster			
		MSCS			
		VCS			

2.2.3 Protection Manager Functions and Prerequisite Versions

The following tables list the supported Protection Manager functions, and the prerequisite versions of RM Shadow Copy Provider, CCI (RAID Manager), and Array microcode.

Table 2.6 Support Matrix for Array Microcode USP / NSC or 9970V / 9980V

Related Version				VSS function of Protection Manager
RM Shadow Copy Provider	CCI (RAID Manager)	Array Microcode		
		9970V / 9980V	USP / NSC	
01-02-03/01	01-15-03/03	21-10-01	50-00-26 for ICS version	Protection Manager 3.51 Exchange single-generation
01-02-03/03	01-16-03/03	Undelivered	50-03-01 for 2's GA	Protection Manager 4.0 Exchange Multiple-generation NTFS Multiple-generation Remote Copy (TC-sync)
01-02-03/05	01-16-03/06	21-13-04-00	Undelivered	Protection Manager 4.3 Windows 2003 SP1
01-02-03/05	01-16-03/06	Undelivered	50-03-89	
01-02-03/06	01-18-03/06	Undelivered	50-05-06-00/00	Protection Manager 4.3.1 Exchange Multiple-generation with Copy-on-write snapshot
01-02-03/07	01-19-03/04	21-14-28	50-08-05	Protection Manager 5.7 Exchange Server 2007

Table 2.7 Support Matrix for Array Microcode AMS / WMS or 9570V (9580V)

Related Version				VSS function of Protection Manager
RM Shadow Copy Provider	CCI (RAID Manager)	Array Microcode		
		9570V (9580V)	AMS / WMS	
01-02-03/01	01-15-03/03	065A(165A)	None	Protection Manager 3.51 Exchange single-generation
01-02-03/02	01-15-03/04	Undelivered	None	
01-02-03/03	01-16-03/03	Undelivered	None	
01-02-03/04	01-16-03/05	None	None	
01-02-03/05	01-16-03/06	065A/R(165A/R)	None	Protection Manager 4.0 Exchange Multiple-generation with QuickShadow NTFS Multiple-generation with QuickShadow Remote Copy (TC-sync) Protection Manager 4.3 Windows 2003 SP1
01-02-03/05	01-16-03/06	Undelivered	0712/A	
01-02-03/07	01-19-03/04	Undelivered	0750/A	Exchange Multiple-generation with ShadowImage NTFS Multiple-generation with ShadowImage Protection Manager 5.5
01-02-03/07	01-19-03/04	0750A	0750A	Protection Manager 5.7 Exchange Server 2007

Chapter 3 Configuring the Microsoft Exchange Database for VSS Backup

This chapter explains the procedures for configuring the Microsoft Exchange database.

- Preparing the Microsoft Exchange Database for VSS Backup (see section 3.1)

3.1 Preparing the Microsoft Exchange Database for VSS Backup

The following table outlines the sequence of volume configuration and installation steps that are required before Protection Manager can be installed and configured.

Table 3.1 Sequence of Volume Configuration and Installation Steps

Configuring the Storage Volume		
Step	**Procedure**	**Server**
1	Create the Logical Units and CMD	—
2	Assign the Logical Units and CMD	—
Configuring the Server Volume		
3	Map LUN to the each server	Exchange Import
4	Format and Mount the volumes	Exchange
Setting up CCI (RAID Manager)		
5	Install the CCI (RAID Manager)	Exchange Import
6	Define the CCI copy pairs	Exchange Import
7	Create the CCI copy pairs	Exchange
Setting up RM Shadow Copy Provider		
8	Install the RM Shadow Copy Provider	Exchange Import

3.1.1 Configuring the Storage Volume

When configuring the storage volume, create the Logical Unit (LU) for the primary volume (PVOL), secondary volume (SVOL), and command device (CMD), then assign to the Exchange and Import (Backup) servers.

For detailed instructions, please refer to the appropriate Storage Navigator Modular or Storage Navigator product manuals.

3.1.2 Configuring the Server Volume

This section describes LUN mapping on both the Exchange server and Import server, using the Emulex Configuration Tool (elxcfg) as an example of an HBA application. The following procedure must be performed on both the Exchange server (PVOL) and Import (Backup) server (SVOL).

To configure the server volume:

1. Map the target LUN to each server:
   a) Start the Emulex Configuration Tool (elxcfg).
   b) Select the target "World Wide Port Name," then click the **Lun Map** button.
   c) When the new dialog displays, click the **Add** button.
   d) Select the target LUN, then click the **OK** button.
   e) Click the **Done** button. From the **File** menu, select **Apply**, then **Exit** to close the application.
   f) Start the Disk Management tool, then select **Rescan Disks** to recognize the new LUN. Verify that Windows recognizes the new LUN.
2. Initialize the volumes:
   a) Right-click the **Not Initialized** disk and select **Initialize Disk**.
   b) Select one or more disks to be initialized, then click the **OK** button.
3. Format and mount the volumes:
   a) Right-click the target disk and select **New Partition**….
   b) Within the Wizard, click the **Next** button.
   c) Select the drive letter to be assigned, then click the **Next** button.
   d) Select any necessary format options, then click the **Next** button.
   e) Confirm the format options, then click the **Finish** button.

3.1.3 Setting up CCI (RAID Manager)

To set up CCI:

1. Install CCI on both the Microsoft Exchange server and the Import (Backup) server:
   a) Run the installation file, **Setup.exe**.
   b) Click the **Next** button in the welcome dialog box.
   c) Click the **Next** button in the **Attention**… dialog box.
   d) Select the installation folder, then click the **Next** button.
   e) Click the **Finish** button.
2. Optional: Check the version of CCI by using "`raidqry`" command.

Note: If you either create the horcm#.conf file by yourself, or if you use "**mkconf.exe**" to create this file, you can skip the following procedure (steps 3-12). For information about using the `mkconf.exe` command, see the CCI (RAID Manager) User and Reference Guide.

```
C:\HORCM\Tool>mkconf
Usage : mkconf
    -g[g] <group> Specify the dev_group for a configuration file.
                  If not specified, 'VG' will be used as default.
   [-m <mu#>  ]   Specify the mirror descriptor for BC(MRCF) volume.
                  Specify the mirror descriptor as '-m h1' for UR volume.
                  CA(HORC) volume dose not specify the mirror descriptor.
   [-i <inst#>]   Specify the instance number for HORCM.
                  No running HORCM instance must be specified.
   [-s <service>] Specify the service name for a configuration file.
                  If not specified, '52323' will be used as default.
   [-c <drive#>]  Specify the drive# in order to discover the CMDDEVs.
                  If not specified, '$PhysicalDrive' will be used as default.
                  If '-a' option is specified, this option is invalid.
   [-a]           Specify an addition of the group for a configuration file.
Example:
type dev_file | mkconf -g dev_group -i 9 [-m 0] [-a]
echo hd10-20  | mkconf -g dev_group -i 9 [-m 0] [-a]
echo $Phys    | mkconf -g dev_group -i 9 [-m 0] [-a]
     $variable specifies as follows.
     $LETALL -> All of the Drive Letter
     $Phys   -> All of the Physical Drives
     $Volume -> All of the LDM Volumes for Windows2000/2003
```

Note: The following procedure (steps 3-12) assumes creation of "horcm0.conf" on the Exchange server, and "horcm1.conf" on the backup server. If you want to create HORCM definition file, replace the number with your preferred in the following procedure.

3. Define copy pairs using CCI: On the Microsoft Exchange server, find the CMD (Command Device) for the target storage subsystem.

```
C:\HORCM\etc>inqraid $Phys -sort -CM

HORCM_CMD
#dev_name              dev_name               dev_name
#UnitID 0 (Serial# 116)
\\.\PhysicalDrive21
#UnitID 1 (Serial# 5368)
\\.\PhysicalDrive11
```

```
#UnitID 2 (Serial# 55014)
\\.\PhysicalDrive20

C:\HORCM\etc>
```

4. Create the temporary HORCM definition file (in this case, "horcm0.conf"). Only define the CMD and the arbitrary port number.

```
HORCM_MON
#ip_address        service         poll(10ms)     timeout(10ms)
localhost            50000           1000              3000

HORCM_CMD
#dev_name                dev_name                dev_name
\\.\PhysicalDrive11

HORCM_DEV
#dev_group        dev_name        port#          TargetID        LU#       MU#

HORCM_INST
#dev_group        ip_address      service
```

5. Start up the temporary HORCM instance: Run the `horcmstart` command and specify the temporary HORCM instance number.

```
E:\HORCM\etc>horcmstart 0
starting HORCM inst 0
HORCM inst 0 starts successfully.
```

6. Specify the temporary `HORCM` instance number to `HORCMINST` variable, then activate the `HORCC_MRCF` variable.

```
C:\HORCM\etc>set HORCMINST=0

C:\HORCM\etc>set HORCC_MRCF=1
```

7. Check the RAID disks connected to the Microsoft Exchange server: Run the `raidscan` command with the `-find` option.

```
C:\HORCM\etc>raidscan -pi $Phys -find -CLI
DEVICE_FILE      UID  S/F PORT   TARG  LUN    SERIAL  LDEV  PRODUCT_ID
Harddisk20       -     -   CL2-A     -       -        5014        55       OPEN-3-CM
Harddisk21       -     -   CL2-A     -       -         116        88       DF600F-CM
Harddisk4        0     F   CL2-C     1       4        5368        4         DF600F
Harddisk5        0     F   CL2-C     1       5        5368        5         DF600F
Harddisk6        0     F   CL2-C     1       6        5368        6         DF600F
Harddisk7        0     F   CL2-C     1       7        5368        7         DF600F
Harddisk11       0     F   CL2-C     1      20        5368        20       DF600F-CM
Harddisk12       0     F   CL2-C     1      21        5368        21       DF600F
```

8. Define the name of `dev_group` and `dev_name` and select the target disk by specifying the `port#`, `TargetID`, and `LU#` in the `HORCM_DEV` entry.

```
HORCM_MON
#ip_address        service         poll(10ms)     timeout(10ms)
localhost            50000           1000              3000

HORCM_CMD
#dev_name                dev_name                dev_name
\\.\PhysicalDrive11

HORCM_DEV
#dev_group        dev_name        port#          TargetID        LU#       MU#
GR01              vol01           CL2-C          1               4           0
GR01              vol02           CL2-C          1               5           0

HORCM_INST
#dev_group        ip_address      service
GR01              xx.xx.xxx.xx     50000
```

9. Restart the HORCM instance: Run the `horcmshutdown` and `horcmstart` commands by specifying the target HORCM instance.

```
C:\HORCM\etc>horcmshutdown 0
inst 0:
HORCM Shutdown inst 0 !!!

C:\HORCM\etc>horcmstart 0
starting HORCM inst 0
```

10. On the backup server, find the CMD (Command Device), create the temporary HORCM definition file (in this case, “horcm1.conf”), and check the RAID disks connected to the backup server (steps 3-7, above).

```
C:\horcm\etc>raidscan -pi $Phys -find -CLI
DEVICE_FILE         UID  S/F   PORT    TARG     LUN    SERIAL     LDEV    PRODUCT_ID
Harddisk5           0    F     CL2-C     1      11       5368       11        DF600F
Harddisk6           0    F     CL2-C     1      12       5368       12        DF600F
Harddisk7           0    F     CL2-C     1      13       5368       13        DF600F
Harddisk8           0    F     CL2-C     1      14       5368       14        DF600F
Harddisk9           0    F     CL2-C     1      15       5368       15        DF600F
Harddisk10          0    F     CL2-C     1      16       5368       16        DF600F
Harddisk11          0    F     CL2-C     1      17       5368       17        DF600F
Harddisk12          0    F     CL2-C     1      32       5368       32        DF600F-CM
```

11. Define the name of `dev_group` and `dev_name` and set the target disk by specifying the `port#`, `TargetID`, and the `LU#` in the `HORCM_DEV` entry.

```
HORCM_MON
#ip_address        service         poll(10ms)     timeout(10ms)
localhost            50000           1000              3000

HORCM_CMD
#dev_name                dev_name                dev_name
\\.\PhysicalDrive12

HORCM_DEV
#dev_group        dev_name        port#          TargetID        LU#       MU#
GR01              vol01           CL2-C          1               11          0
GR01              vol02           CL2-C          1               12          0

HORCM_INST
```

```
#dev_group        ip_address      service
GR01              xx.xx.xxx.xx     50000
```

12. Restart the HORCM instance: Run the `horcmshutdown` and `horcmstart` commands by specifying the target HORCM instance.

```
C:\HORCM\etc>horcmshutdown 1
inst 1:
HORCM Shutdown inst 1 !!!

C:\HORCM\etc>horcmstart 1
starting HORCM inst 1
```

13. Create copy pairs by using CCI: On the Microsoft Exchange server, specify the temporary `HORCM` instance number to the `HORCMINST` variable, then activate the `HORCC_MRCF` variable.

```
C:\HORCM\etc>set HORCMINST=0

C:\HORCM\etc>set HORCC_MRCF=1
```

14. Create the `HORCM` copy pair: Run the `paircreate` command with the `-vl` and `-m noread` options, and specify the target `HORCM` copy pair name. When creating the pair with TrueCopy, -m noread option is not required.

```
C:\HORCM\etc>paircreate -g GR01 -vl -c 15 -m noread

C:\HORCM\etc>
```

3.1.4 Setting up RM Shadow Copy Provider

To set up Shadow Copy Provider:

1. Install RM Shadow Copy Provider on both Exchange and Backup server:
   a) Run the installation file RMVSSPRV.exe located in the folder `C:\HORCM\tool`.
   b) Click the **Next** button in the welcome dialog box.
   c) Select the installation folder and click the **Next** button.
   d) To verify the correct installation, check the existence of "RM Shadow Copy Provider" by using the service applet of Windows.
   e) Optional: Check the version of RM Shadow Copy Provider by using the `vssadmin` command.

Chapter 4 Installing and Setting up Protection Manager

This chapter describes how to install and set up Protection Manager.

- Gathering and Installing the Required Components (see section 4.1)
- Setting up the Microsoft Exchange Server (see section 4.2)
- Setting up the Import (Backup) Server (see section 4.3)
- Setting up the Exchange Verify Tool (see section 4.4)

4.1 Gathering and Installing the Required Components

Before you set up the Microsoft Exchange server, the Import (Backup) server and the cluster environment, please ensure that you have completed the following tasks:

- **Install**:
  - Exchange server: Install Protection Manager Copy Controller, Protection Manager for Exchange Server module, and the Protection Manager Console module. For instructions, see section 4.2.
  - Import (Backup) server: Install Protection Manager Copy Controller and the Protection Manager Console module. For instructions, see section 4.3.
- **Setup Exchange verification tool**:
  - Exchange or Import (Backup) server: The operation required for the setup is depends on the version of Exchange Server. For instructions, see section 4.4.
    - Exchange Server 2003: Copy ESEUTIL files to the specified folder on Import (Backup) server. These files are required to verify the backed up Exchange data.
    - Exchange Server 2007: Install Exchange Management Console on Import (Backup) server. This component is required to verify the backed up Exchange data.
- **Verify**:
  - Import (Backup) server: Run configuration check function to verify the system configuration

Notes:

- Exchange server recognizes command device (CMD) and primary volumes (PVOL).
- The Import (Backup) server recognizes command device (CMD) and secondary volumes (SVOL).
- Exchange server should not recognize SVOLs and Import server should not recognize PVOLs.
- Before installing HPtM Console module, you need to install Java Runtime Environment (JRE) 1.4.2 or 1.5.

4.2 Setting up the Microsoft Exchange Server

To set up the Exchange server:

1. Install HiCommand Protection Manager Copy Controller:
   a) Run the installation file Setup.exe. The welcome dialog box displays.
   b) Click the **Next** button. The install path selection dialog box displays.
   c) Select the folder where Setup will install the files, then click the **Next** button. After the file copy procedure is finished, a completion dialog displays.
   d) Enter Windows account and password for Protection Manager Service.
2. Install HiCommand Protection Manager for Microsoft Exchange Server:
   a) Run the Setup.exe file. The welcome dialog box displays.
   b) Click the **Next** button. The license registration method dialog box displays.
   c) Specify the registration option you want to use, then click the **Next** button.
   d) Enter the license key, then click the **Next** button. After the file copy procedure is finished, a completion dialog displays.
3. Install HiCommand Protection Manager Console:
   a) Run the Setup.exe file. The welcome dialog box displays.
   b) Click the **Next** button. The install path selection dialog box displays.
   c) Select the folder where Setup will install the files, then click the **Next** button. After the file copy procedure is finished, a completion dialog displays.
4. Setup shared volume for dictionary map files in cluster configuration:

   If you installed Protection Manager on cluster configuration of Exchange server, following procedure is required to setup shared volume:
   a) Map a LUN to the Exchange server, then initialize and format the volume.
   b) Add the volume to the Exchange cluster group as a physical disk cluster resource (see Figure 4-1). This disk is supposed to store the dictionary map files of HiCommand Protection Manager, which allows Protection Manager to share the object mapping information and the backup information on both of the cluster node.
5. Set up HiCommand Protection Manager:
   a) Start the Console: From the **Start** menu, select **HiCommand Protection Manager Console**, then choose **Console**.
   b) Open the GUI Setup window: From the Console, select **Tools**, then choose **Setup**.
   c) Within the **Configuration Settings** tab [Step 1/9], select **Database/File server** for the server type, and **Exchange** for the backup object. Depends on the Exchange server configuration, select **Non Cluster Configuration** or **Cluster Configuration** for the cluster configuration. Afterward, the total procedure that you should specify is displayed in the Setup Steps area. For an example for a cluster configuration, see Figure 4-2. Click the **Next** button.

d) Optional: Within the **Operation Setup** tab [Step 2/9], set the retry parameters, the log output level and the number of trace log files. For more detailed information, refer to Chapter 5, "*Setting Up an Environment for Protection Manager Using Setup GUI"* in the *HiCommand Protection Manager User's Guide*. Click the **Next** button. If the Exchange servers are cluster configuration, enter the virtual server name in the **Dictionary map file path**, then click the **Browse...** button. Select the location on the shared disk in which the dictionary map files are stored, then click the **Add** button. Select the new entry, then click the **Create** button to create the dictionary map files. (see Figure 4-3)

e) Within the **RAID Manager Linkage** tab [Step 3/9], check and set the CCI instance number and its install path for HORCMINST, HORCMINST_AUX, and INSTALLPATH entries (see Figure 4-4). Afterward, click the **Next** button.

   Field definitions:

   - HORCMINST

     Specify the CCI instance number managing the PVOLs. (in this case, "0")

   - HORCMINST_AUX

     Specify the CCI instance number managing the SVOLs. (in this case, "-")

   Selecting **Pair split** on the **Pair Status when Backup Fail** is recommended so that Protection Manager split the pair even if the backup has failed. If you configured multiple generations of SVOL in clustered Exchange server, select the **Dynamic recognition of secondary volume** to make HPtM hide the SVOL from the operating system.

f) If needed, set the retry parameters for turning the performance within the **RAID Manager Operation** tab [Step 4/9]. For details, refer to Chapter 5, "*Setting Up an Environment for Protection Manager Using Setup GUI"* in the *HiCommand Protection Manager User's Guide*. Click the **Next** button.

g) Within the **Cluster Configuration** tab [Step 5/9], select the cluster product name (Microsoft Cluster Service (MSCS) or VERITAS Cluster Server (VCS)). For details, refer to Chapter 5, "*Setting Up an Environment for Protection Manager Using Setup GUI"* in the *HiCommand Protection Manager User's Guide*. Click the **Next** button.

h) Within the **VSS Definition** tab [Step 6/9], set the name of the backup (import) server that verifies the backed up Exchange data after creating a VSS snapshot, then click the **Next** button.

i) Within the **VSS Environment** tab [Step 7/9], select the generation type of the backup environment (**Multiple generation** or **Single generation**. See Figure 4-6). If you select Single generation, specify appropriate number on the **RAID Manager instance number for primary volume**. (in this case, "0"), and on the **Copy group mirror unit number** (in this case, "0"). Then click the **Next** button.

j) Within the **Protection Manager Service** tab [Step 8/9], specify the TCP port number for Protection Manager Service. This number has to be consistent between Exchange server and backup (import) server (see Figure 4-7).

k) Within the **Update Dictionary Map** tab [Step 9/9], check the **Exchange** box on backup object, then click the **Save** button (see Figure 4-8). If you configure cluster of Exchange server, also select the virtual server name specified on **Operation Setup** tab [Step 2/9]. Protection Manager starts to collect the object mapping (including Exchange objects, File System and horcm replication information) by using the "`drmexgdisplay.exe -refresh`" command.

l) Click the **Cancel** button to exit the Setup GUI. If the interface asks you to restart the operating system with the dialog shown on Figure 4-9, do so.

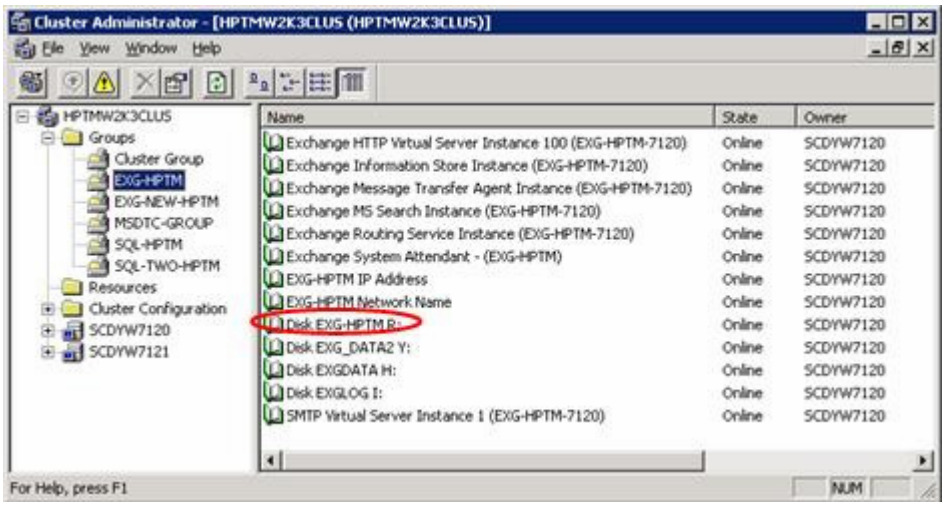

Figure 4-1 Adding a Physical Disk to Exchange Cluster Group

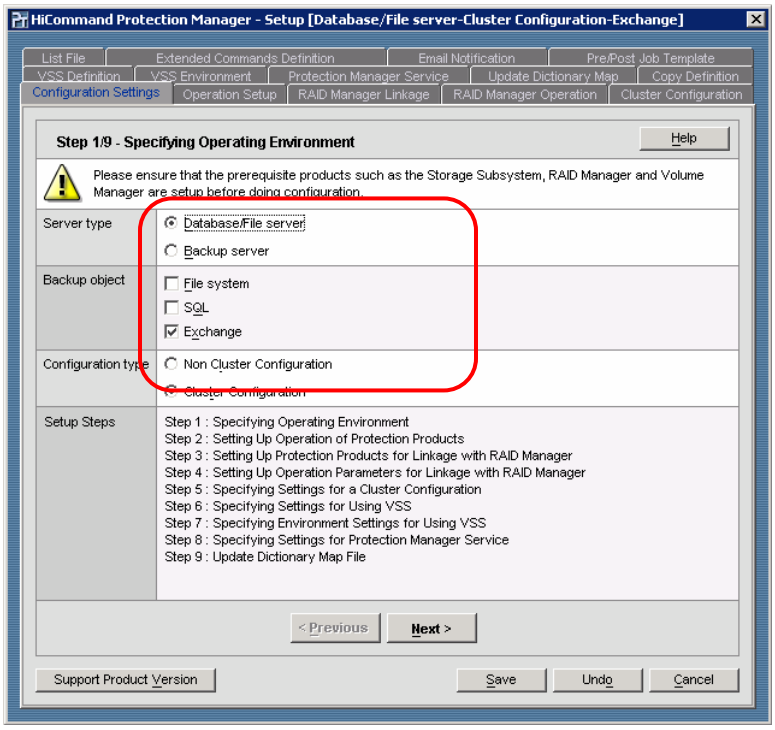

Figure 4-2 Configuration Settings: Step 1/9

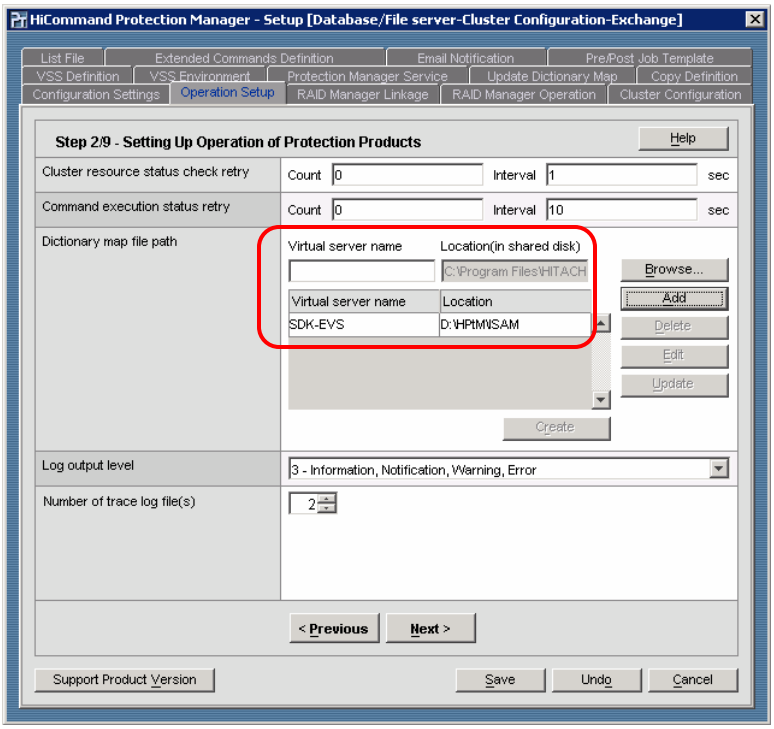

Figure 4-3 Operation Setup: Step 2/9

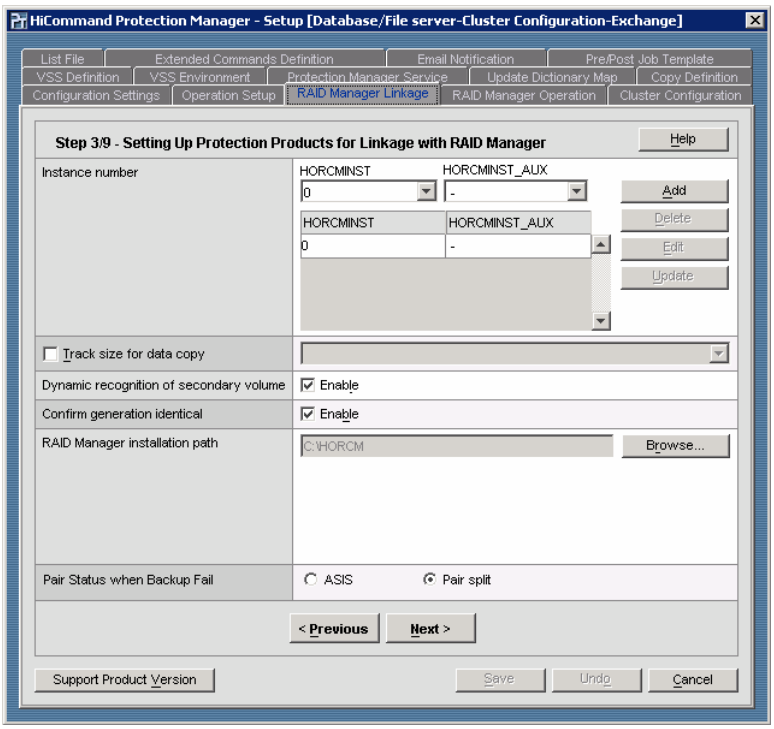

Figure 4-4 RAID Manager Linkage: Step 3/9

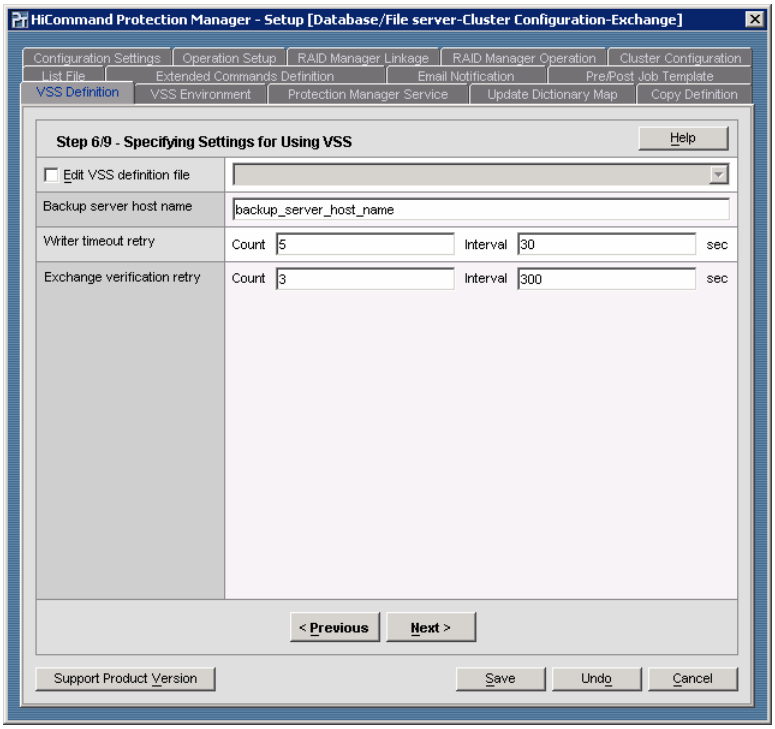

Figure 4-5 VSS Definition: Step 6/9

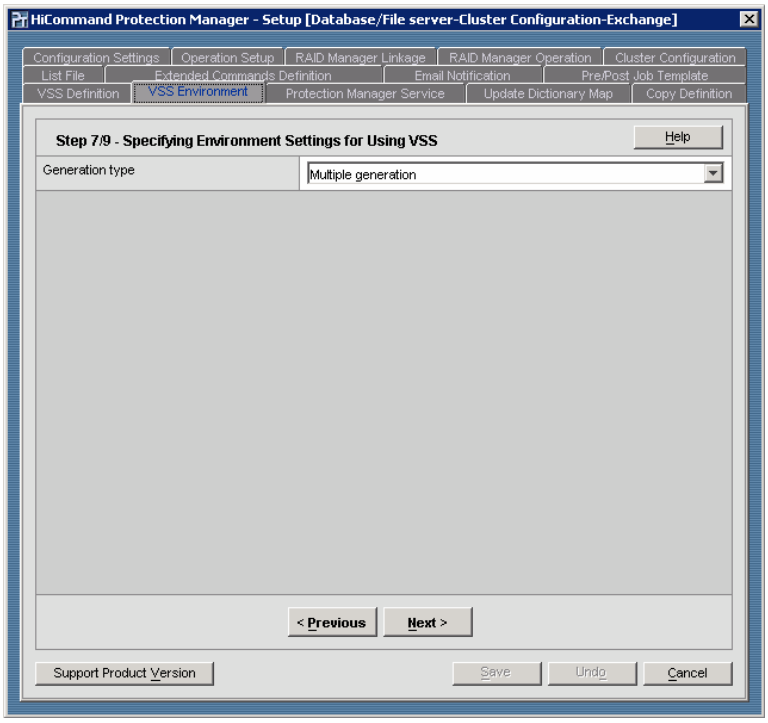

Figure 4-6 VSS Environment: Step 7/9

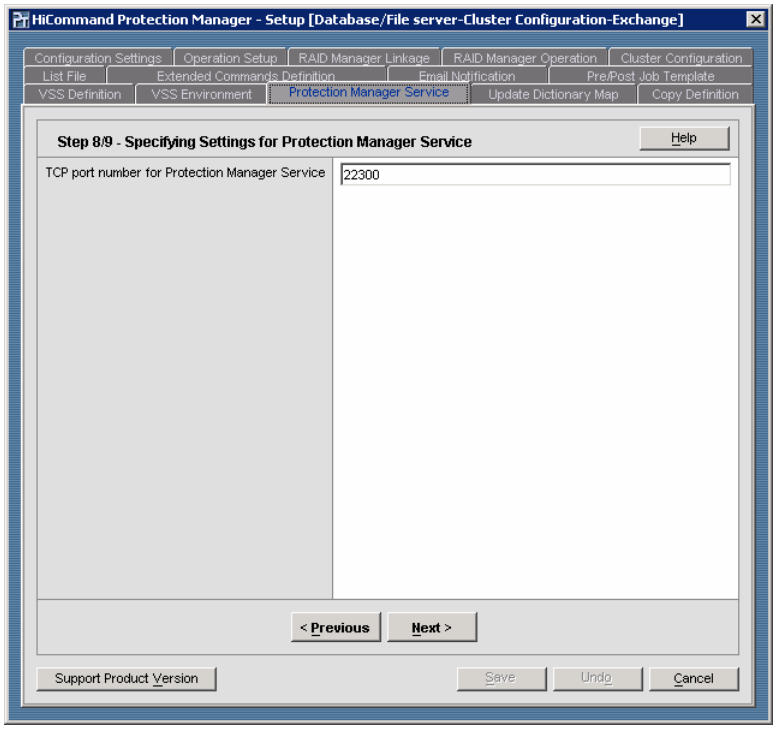

Figure 4-7 Protection Manager Service: Step 8/9

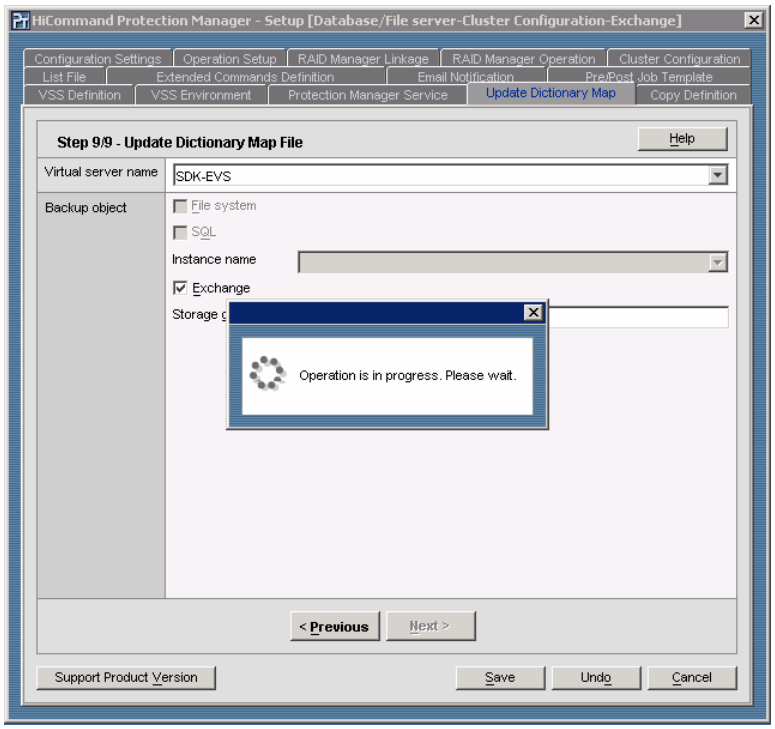

Figure 4-8 Update Dictionary Map: Step 9/9

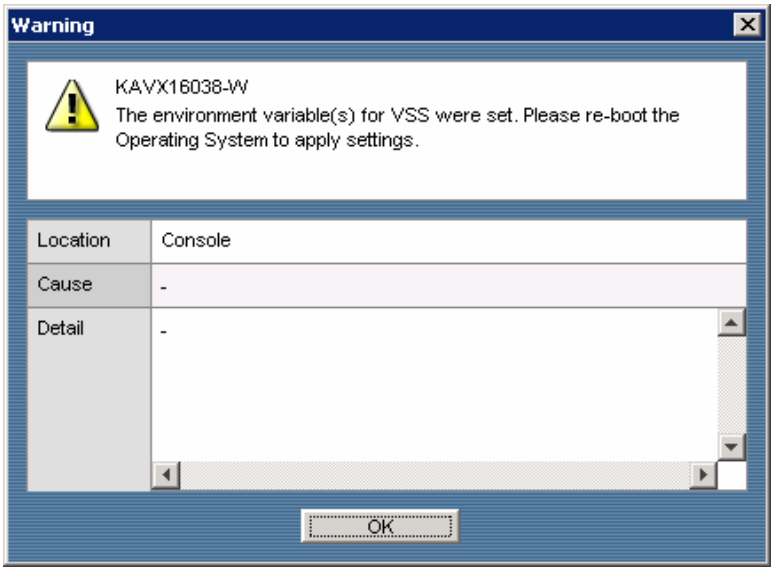

Figure 4-9 KAVX16308-W Warning dialog

4.3 Setting up the Import (Backup) Server

To set up the Import (Backup) server:

1. Install HiCommand Protection Manager Copy Controller:
   a) Run the installation file Setup.exe. The welcome dialog box displays.
   b) Click the **Next** button. The install path selection dialog box displays.
   c) Select the folder where Setup will install files, then click the **Next** button. The setup type selection dialog displays.
   d) Click the **Next** button. After the file copy procedure is finished, a completion dialog displays.
   e) Enter Windows account and password for Protection Manager Service.
2. Install HiCommand Protection Manager Console:
   a) Run the installation file Setup.exe. The welcome dialog box displays.
   b) Click the **Next** button. The install path selection dialog box displays.
   c) Select the folder where Setup will install files, then click the **Next** button. The setup type selection dialog displays.
   d) Click the **Next** button. After the file copy procedure is finished, a completion dialog displays.
3. Set up HiCommand Protection Manager:
   a) Start the Console: From the **Start** menu, select **HiCommand Protection Manager Console**, then choose **Console.**
   b) Open the GUI Setup window: From the Console, select **Tools**, then choose **Setup.**
   c) Within the **Configuration Settings** tab [Step 1/9], select **Backup server** for the server type, and **Non Cluster Configuration** for the cluster configuration. Selecting the backup object is not required on the Import (Backup) server. Afterward, the total procedure that you should specify is displayed in the Setup Steps area. For an example for a cluster configuration, see Figure 4-10. Click the **Next** button.
   d) Optional: Within the **Operation Setup** tab [Step 2/9], set the retry parameters, the log output level and the number of trace log files. For more detailed information, refer to Chapter 5, "*Setting Up an Environment for Protection Manager Using Setup GUI*" in the *HiCommand Protection Manager User's Guide*. Click the **Next** button.
   e) Within the **RAID Manager Linkage** tab [Step 3/9], check and set the CCI instance number and its install path for HORCMINST, HORCMINST_AUX, and INSTALLPATH entries (see Figure 4-11). Afterward, click the **Next** button.

      Field definitions:

      - HORCMINST

        Specify the CCI instance number managing the SVOLs. (in this case, "1")

      - HORCMINST_AUX

        Specify the CCI instance number managing the PVOLs. (in this case, "-")

Selecting **Pair split** on the **Pair Status when Backup Fail** is recommended so that Protection Manager splits the pair even if the backup has failed. If you configured multiple generations of SVOL in clustered Exchange server, select the **Dynamic recognition of secondary volume** to make HPtM hide the SVOL from the operating system.

f) If needed, set the retry parameters for turning the performance within the **RAID Manager Operation** tab [Step 4/9]. For details, refer to Chapter 5, "*Setting Up an Environment for Protection Manager Using Setup GUI*" in the *HiCommand Protection Manager User's Guide*. Click the **Next** button.

g) Within the **VSS Environment** tab [Step 5/9], select the generation type of the backup environment (Multiple generation or Single generation). Additionally, specify the **CCI instance number for secondary volume**. (in this case, "1") Click the **Next** button.

h) Within the **Protection Manager Service** tab [Step 6/9], you can change the TCP port of the communication between the Microsoft Exchange server and the backup (import) server by setting the specified port number in the **TCP port number for Protection Manager Service** area. Click the **Next** button.

i) If you do not back up Exchange data from SVOL to TAPE by VERITAS Net Backup or VERITAS Backup Exec, the steps within the **Backup Linkage** tab [Step 7/9] and the **Tape Backup** tab [Step 8/9] are unnecessary. For details, refer to Chapter 5, "*Setting Up an Environment for Protection Manager Using Setup GUI*" in the *HiCommand Protection Manager User's Guide*. Click the **Next** button.

j) Skip **Update Dictionary Map File** [Step/9/9]. Protection Manager doesn't have object mapping on the backup server, so this step is unnecessary.

k) Click the **Cancel** button to exit the Setup GUI. If the interface asks you to restart the operating system with the dialog shown on Figure 4-9, do so.

l) If you configured multiple generations of SVOL in clustered Exchange server, launch a **Command Prompt**, then execute the `drmdevctl` command with "`-detach`" option to conceal the SVOLs on the Backup Server. The command allows Protection Manager to execute the `raidvchkset` command with the "`-vg idb`" option, then rescan the disk and volume with `diskpart` command.

```
C:\HORCM\etc>drmdevctl -detach
KAVX0001-I The drmdevctl command will now start.
KAVX0232-I Hid sqlsia,sqldataa.
KAVX0232-I Hid sqlsia,sqltloga.
KAVX0232-I Hid sqlsib,sqldatab.
KAVX0232-I Hid sqlsib,sqltlogb.
KAVX0232-I Hid sqlsi2,sqlsystem.
KAVX0232-I Hid sqlsi2,sqluser.
KAVX0234-I Rerecognizes the physical volume.
KAVX0235-I Rerecognized the physical volume.
KAVX0002-I The drmdevctl command will now end.
```

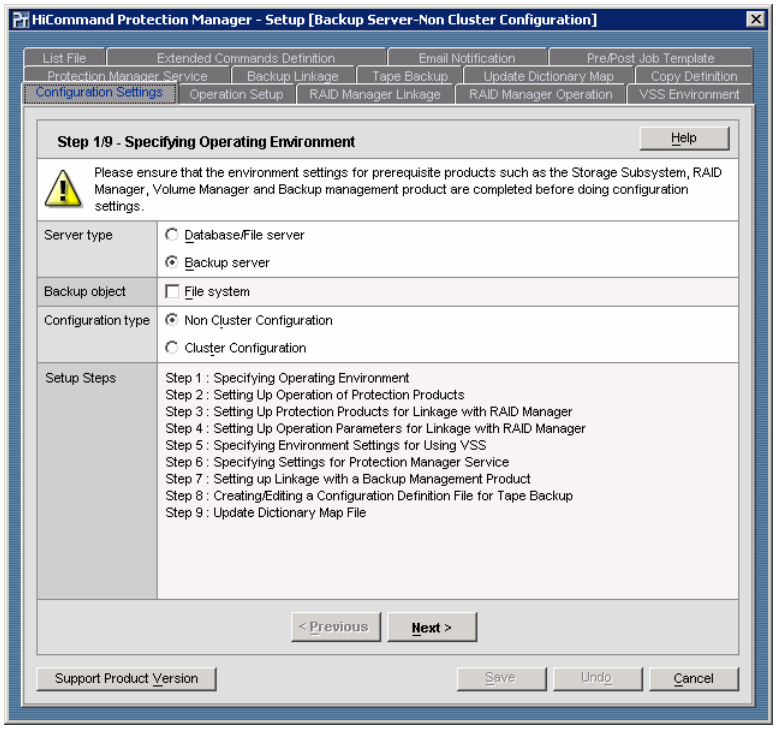

Figure 4-10 Configuration Settings: Step 1/9

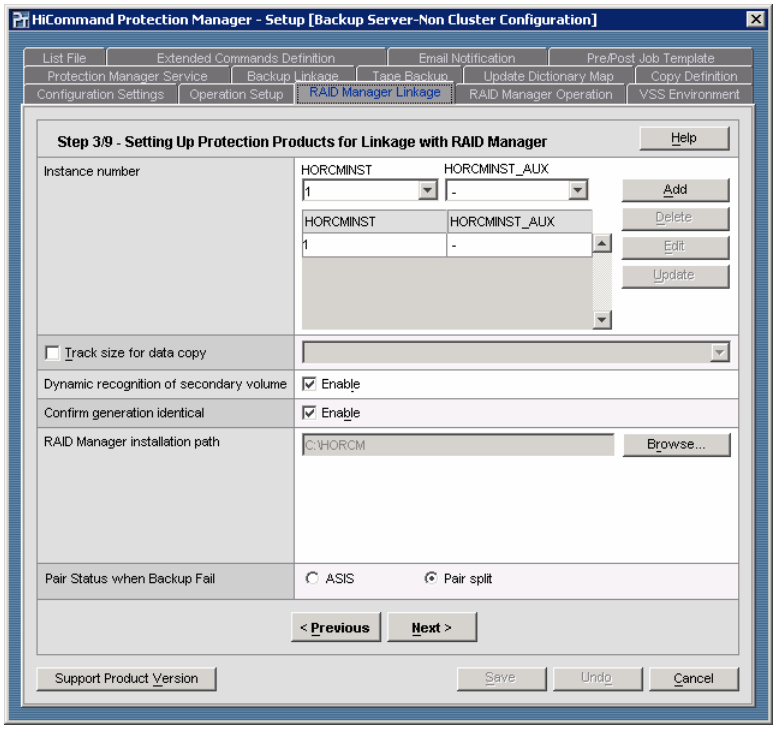

Figure 4-11 RAID Manager Linkage: Step3/9

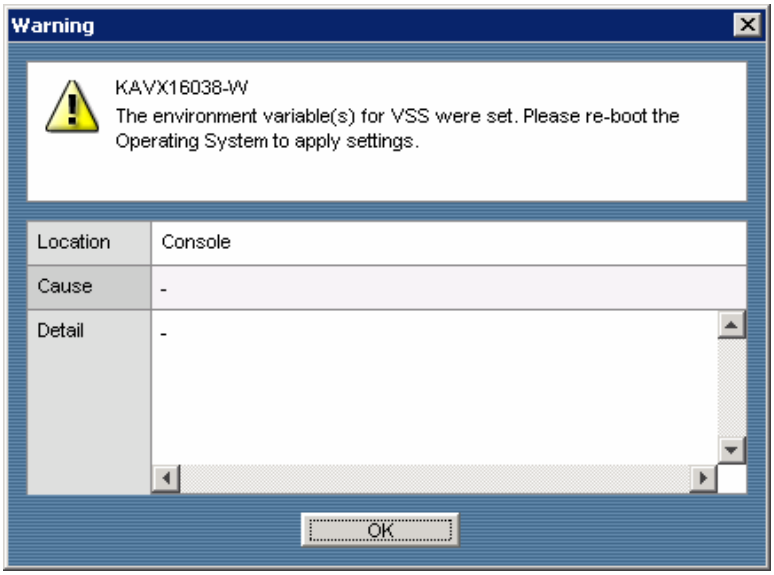

Figure 4-12 KAVX16308-W Warning dialog

4.4 Setting up the Exchange Verify Tool

Verify Tool setup procedure varies depending on the version of Exchange Server.

4.4.1 Setting up for Exchange Server 2003

Copy following files located in the *Exchange-Server-install-path*\bin folder on the Microsoft Exchange server, then paste all four files into the *Protection-Manager-install-path*\bin\util folder on the Import (Backup) server:

- ESEUTIL.exe
- ESE.dll
- EXCHMEM.dll
- EXOSAL.dll

4.4.2 Setting up for Exchange Server 2007

Run the installation file of Exchange Server 2007 on the Import (Backup) server, and select Exchange Management Console for the installation. Once the component is installed on the Import server, Protection Manager uses the API on the component to verify the Exchange data.

4.4.2.1 Running HPtM Configuration Checker on the Import (Backup) Server

Protection Manager provides a configuration check function for verifying the system configuration and ensuring that it is appropriate for proper functioning of Protection Manager. Whenever a new system using Protection Manager is built or an existing system configuration is modified, the configuration check function should be used to verify the system configuration.

1. Executing the Configuration Check Function

To execute the configuration check function:

a) Launch Protection Manager Console on the Import (Backup) server.

b) Select **Tools**, and then **Check Configuration** to launch the Input Servers dialog box (see Figure 4-13).

c) In the **DB Servers** list box, register either the host name or IP address for the Exchange server to be verified. If the Exchange servers are in cluster configuration, register all the nodes of Exchange servers. The host name or IP address for virtual server can not be registered.

- To add a server, perform one of the following operations:
  - Right-click the position in the list box where a line is to be added, and choose **Insert Row** from the pop-up menu.
  - Select a position in the list box where a line is to be added, and press the **Insert** key.

- Select the last line in the list box, and press the **Tab** key.

– To delete a server, perform one of the following operations:

- In the list box, right-click the line to be deleted, and select **Delete Row**(s) from the pop-up menu.
- In the list box, select the line to be deleted, and press the **Delete** key.

d) In the **BK Servers** list box, register the host name or IP address for the backup server to be verified. See Step 3 for the registration method.

e) In **Backup Object**, select the **Exchange server** and **Using VSS** check box.

f) Click the **Check** button to start verification. The check results are displayed in the Check Results dialog box.

2. Reviewing the Check Results

To review the check results of the configuration check function:

a) Review the contents output in the Check Results dialog box (see Figure 4-14).

b) Identify items with error or warning result, and check the messages.

c) Double click the item and review the information with the Result dialog box (see Figure 4-15), then fix the problem according to the information displayed on **Action** field.

d) Click the **Close** button to closes the Result dialog box.

e) Repeat Steps from b) to d) for all the items with error or warning.

f) Click the **Close** button to close the Check Results dialog box. Then execute the configuration check function again to ensure the error has fixed.

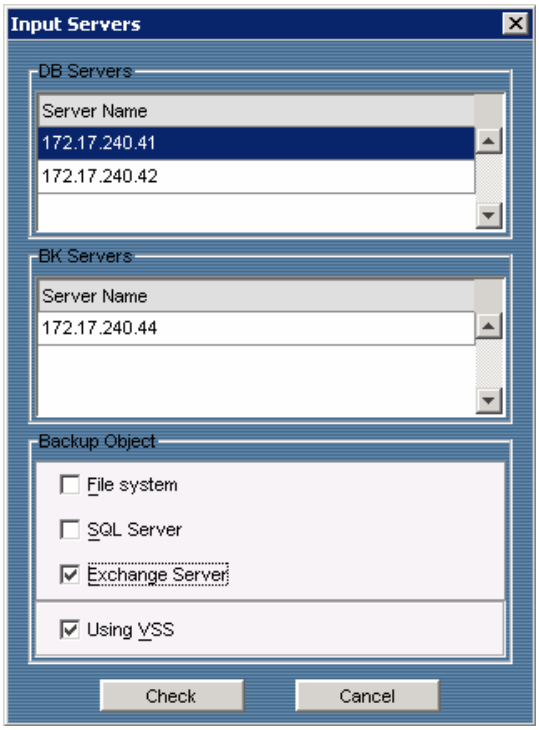

Figure 4-13 Input Servers Dialog Box

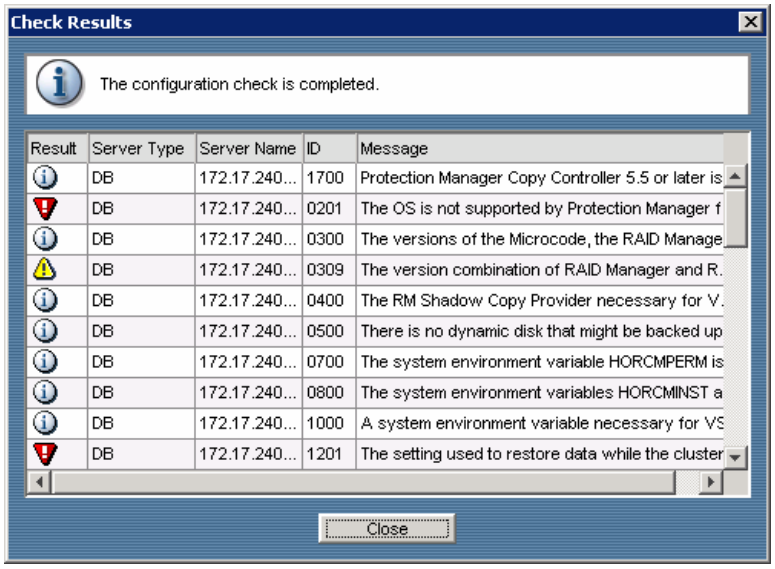

Figure 4-14 Check Results Dialog Box

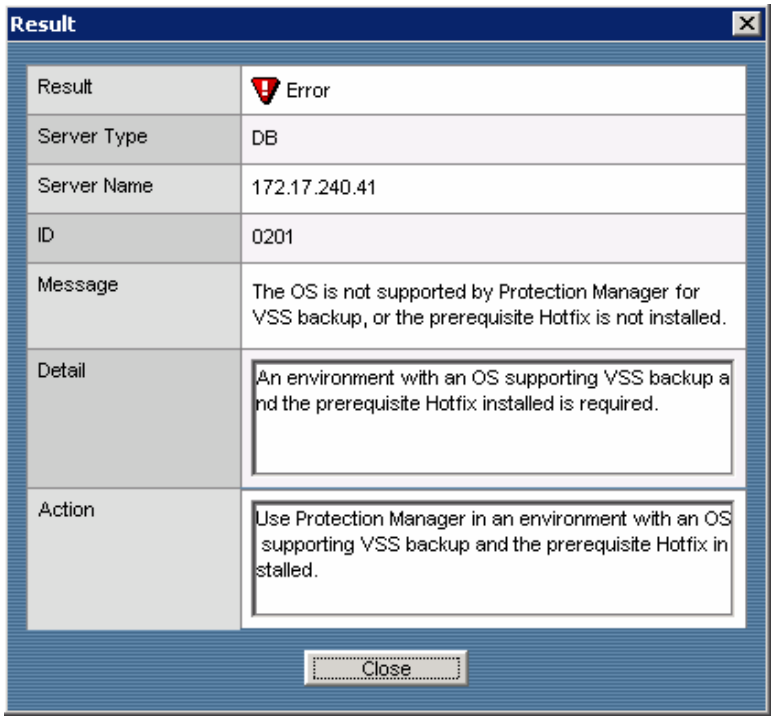

Figure 4-15 Result Dialog Box

Chapter 5 Troubleshooting

This chapter explains how to handle any problems that may occur while you are working with VSS Backup.

- Troubleshooting VSS Backup Errors (see section 5.1)
- Calling the Hitachi Data Systems Support Center (see section 5.2)

5.1 Troubleshooting VSS Backup Errors

The following table lists the common errors you may encounter during VSS backup, and it describes the steps to troubleshoot those issues. For any troubleshooting case that is not listed in this table, please refer to the actual product manuals. For errors that cannot be resolved, please see section 5.2 for information about contacting the Hitachi Data Systems Support Center.

Table 5.1 Error Causes and Troubleshooting Steps

Issue	Cause	Verify	Troubleshooting Steps
`drmexgbackup` command failed with "KAVX5003-E"	The system environment variables related to RM shadow copy provider or HORCM definition file on the Microsoft Exchange server may be invalid,	The Application Event Log of Windows on the Microsoft Exchange server output "Warning" or "Error" logs for "RMVSSPRV" source.	Refer to the content of Application Event Log.
	If this Windows 2003 server was upgraded from Windows 2000 server, VSS function may be unable to work correctly.	The Application Event Log of Windows on the Microsoft Exchange server output "Error" logs for "COM+" source.	Install Windows 2003 Enterprise Edition (do not perform an upgrade installation).
	The DLL registration information of VSS may be corrupt.	The Application Event Log of Windows on the Microsoft Exchange server output "Error" logs for "VSS" source.	Execute the following command line to re-register information, C:\> regsvr32 VSS_PS.DLL and then re-install RM shadow copy provider.
`drmexgbackup` command failed with "KAVX5033-E"	The system environment variables related to RM shadow copy provider or HORCM definition file on the Backup server may be invalid,	The Application Event Log of Windows on the Backup server output "Warning" or "Error" logs for "RMVSSPRV" source.	Refer to the content of Application Event Log.
	If this Windows 2003 server was upgraded from Windows 2000 server, VSS function may be unable to work correctly.	The Application Event Log of Windows on the Backup server output "Error" logs for "COM+" source.	Install Windows 2003 Enterprise Edition newly.
	The DLL registration information of VSS may be corrupt.	The Application Event Log of Windows on the Backup server output "Error" logs for "VSS" source.	Execute the following command line to re-register information, C:\> regsvr32 VSS_PS.DLL , and then re-install RM shadow copy provider.
	The CCI instance number isn't described in "HORCMINST" of "DEFAULT.dat" file on the Backup server as same as the system environment variable VSHTCHORCMINST_REMOTE.	Other than those above	Set the CCI instance number that manages SVOLs (as same as VSHTCHORCM_REMOTE) to "HORCMINST" of "DEFAULT.dat" file.

Issue	Cause	Verify	Troubleshooting Steps
	The following system environment variables may be set on the Backup server: HORCMINST HORCC_MRCF HORCMPERM		Unset these system environment variables on the Backup server, and then restart OS.
`drmexgbackup` command failed with "KAVX5023-E" and "DRM-10434"	The HBA driver may not support VSS function.	The Application Event Log of Windows output the following error log. Source: "VSS" Event ID: 12289	Update the HBA driver that supports VSS function.

5.2 Calling the Hitachi Data Systems Support Center

The Hitachi Data Systems customer support staff is available 24 hours a day, seven days a week. If you need technical support, please call:

- United States: (800) 446-0744
- Outside the United States: (858) 547-4526

Acronyms and Abbreviations

API	application programming interface
BMP	bitmap
CCI	command control interface
CMD	command device
DAMP	disk array management program
DLL	dynamic linking library
DNS	domain name system
FQDN	fully qualified domain name
GUI	graphical user interface
HBA	Host bus adapter
I/O	input/output
JRE	Java Runtime Environment
LAN	local area network
LDEV	logical device
LDM	logical disk manager
LU	logical unit
LUN	logical unit number
MB	megabytes
MU	mirror unit
OS	operating system
PVOL	primary volume
RAID	redundant array of independent disks
SAN	storage area network
SVOL	secondary volume
TC	TrueCopy
UDP	user datagram protocol
VSS	volume shadow copy service

Index