HITACHI
DATA SYSTEMS

HiCommand® Protection Manager
Console User's Guide

MK-94HC071-05

Trademarks

Sun is a trademark or registered trademark of Sun Microsystems, Inc. in the United States and other countries.

Sun Microsystems is a trademark or registered trademark of Sun Microsystems, Inc. in the United States and other countries.

Symantec is a U.S. registered trademark of Symantec Corporation.

VERITAS is a registered trademark of Symantec Corporation in the U.S. and other countries.

Windows is a registered trademark of Microsoft Corp. in the U.S. and other countries.

Windows Vista is either a registered trademark or trademark of Microsoft Corporation in the United States and/or 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-94HC071-P	August 2004	Preliminary Release
MK-94HC071-00	March 2005	Initial Release
MK-94HC071-01	May 2005	Revision 1, supersedes and replaces MK-94HC071-00
MK-94HC071-02	November 2005	Revision 2, supersedes and replaces MK-94HC071-01
MK-94HC071-03	January 2006	Revision 3, supersedes and replaces MK-94HC071-02
MK-94HC071-04	December 2006	Revision 4, supersedes and replaces MK-94HC071-03
MK-94HC071-05	May 2007	Revision 5, supersedes and replaces MK-94HC071-04

Preface

The *HiCommand Protection Manager Console User's Guide* describes how to install, manage, and operate HiCommand Protection Manager Console.

This manual is intended for system administrators who use Protection Manager Console to manage data on storage subsystems. The readers of this manual should have a basic knowledge of the following functions:

- Management functions of Windows
- Management functions of Hitachi storage subsystems (TagmaStore, Lightning, Thunder Series products)
- Management functions of Hitachi RAID Manager

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

Software Version

This document revision applies to HiCommand Protection Manager version 5.7.

Convention for Storage Capacity Values

Storage capacity values displayed by HiCommand Protection Manager are calculated based on the following values:

1 KB (kilobyte) = 1,024 bytes
1 MB (megabyte) = $1,024^2$ bytes
1 GB (gigabyte) = $1,024^3$ bytes
1 TB (terabyte) = $1,024^4$ bytes

Referenced Documents

- *HiCommand Protection Manager User's Guide*, MK-94HC070
- *HiCommand Protection Manager Command Reference*, MK-94HC072
- *HiCommand Protection Manager Messages*, MK-94HC073
- HiCommand Device Manager Web Client User's Guide, MK-91HC001-21#
- HiCommand Device Manager Server Installation and Configuration Guide MK-91HC002-21#
- HiCommand Device Manager Agent Installation Guide MK-92HC019-15#
- HiCommand Device Manager Error Codes MK-92HC016-15#

#:

These manuals are for HiCommand Device Manager 5.0 or later.

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 Protection Manager Console

Protection Manager Console allows users to perform HiCommand Protection Manager operations, storage subsystem data protection management functions, from a console. This chapter describes the features, system structure, and functions of Protection Manager Console:

- Introducing Protection Manager (see section 1.1)
- Reviewing the Components of HiCommand Protection Manager (see section 1.2)
- Understanding the Features of Protection Manager Console (see section 1.3)
- Implementing Protection Manager Console (see section 1.4)
- Understanding the Protection Manager Console Functions (see section 1.5)

1.1 Introducing Protection Manager

Protection Manager supports data maintenance operations, including operations for backup and restoration, and ensures protection of important data with minimum interruption to other processing jobs. Protection Manager enables you to manage data using simple operations without requiring complex procedures and expertise. For example, Protection Manager internally manages information about the:

- relationships between the object subject to backup and the associated logical unit among the RAID devices,
- relationship between the primary and secondary volumes, and the
- backup history.

This information is contained in a dictionary map file. Protection Manager references the information in the dictionary map file to automatically control the database and RAID devices, which reduces the system administrator's workload and the storage system's total cost of ownership.

Figure 1.1 provides an overview of Protection Manager functions.

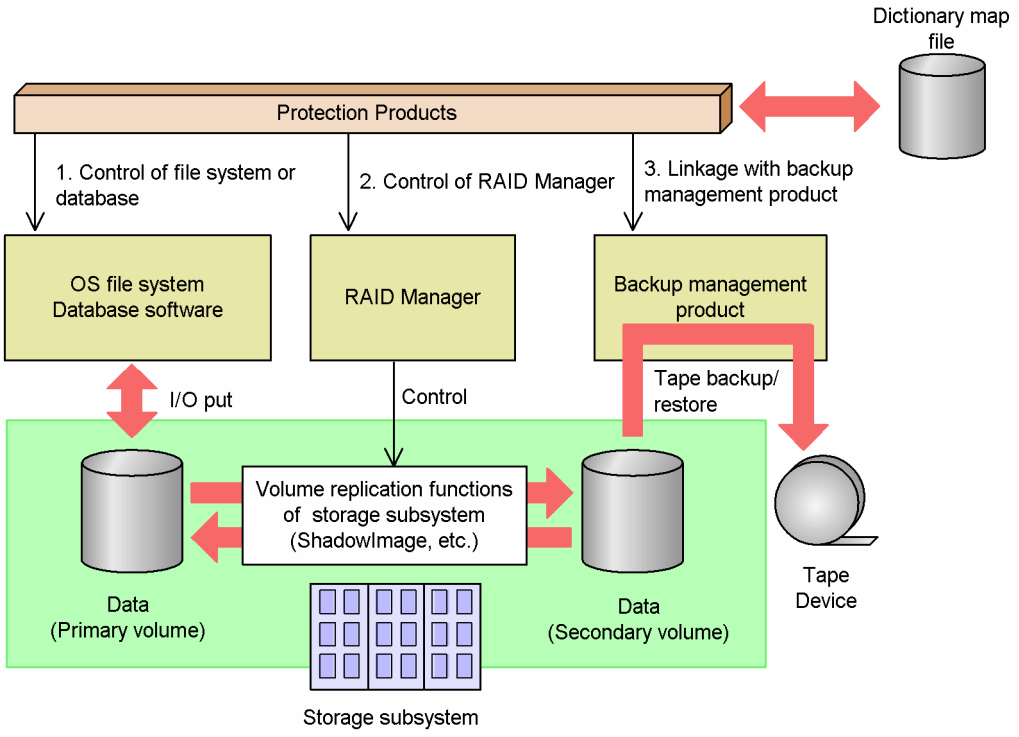


Figure 1.1 Overview of Protection Manager Functions

As illustrated in the figure, Protection Manager does the following:

1. **Ensures reliable backup operations**: Protection Products programs freeze file systems or databases in the storage subsystems.
2. **Controls RAID Manager**: For performing volume backup and restore operations using the volume replication functions of the storage subsystems.
3. **Links with backup management**: Operate (in linkage) with backup management products to control tape backup and restore operations.

Note: Internally, Protection Manager uses the command line interface (CLI) function of RAID Manager and a backup management product. To use Protection Manager, these products must have already been set up and must be ready to use.

Because enterprise information systems must be able to protect important data without interrupting other processing jobs, and restart such processing jobs quickly if an error occurs, the Hitachi storage subsystems (TagmaStore, Lightning, and Thunder Series) provide RAID management (through RAID Manager) and volume replication functions (through ShadowImage). These replication functions can quickly create a replica of a logical volume within a storage subsystem, without using a host. A system administrator who manages backups can use these functions to back up a replica (secondary volume) of a primary volume to tape without disconnecting the primary volume, so that it can continue to be used by the current processing job.

1.2 Reviewing the Components of HiCommand Protection Manager

HiCommand Protection Manager has several components, as listed in Table 1.1. Each listed product is supported on the Windows platform.

Table 1.1 Components of HiCommand Protection Manager

Product Name	Main Components
HiCommand Protection Manager for SQL	▪ HiCommand Protection Manager for SQL ▪ HiCommand Protection Manager Copy Controller ▪ HiCommand Protection Manager Console
HiCommand Protection Manager for Exchange	▪ HiCommand Protection Manager for Exchange ▪ HiCommand Protection Manager Copy Controller ▪ HiCommand Protection Manager Console

1.3 Understanding the Features of Protection Manager Console

Protection Manager Console is a program that allows backup and restore processes to be executed from a console. The following list summarizes the features of Protection Manager Console:

- **Display of backup data**. A list of information necessary for backup can be displayed. This information can also be output to a file (in a tab-delimited list format), so that you can manage your resources using spreadsheet applications.
- **Display of management information**. Information necessary for managing the history and generations of backup can be displayed. This information can also be output to a file (in a tab-delimited list format), so that you can manage the backup history using spreadsheet applications.
- **Display of instance names and mount points**. The instance names and mount points of the file system to be backed up are displayed on the screen, providing confirmation of the objects to be backed up when the backup is executed. Also, since the backup options can be specified on the console, complex operations such as command entries are not needed.
- **Simple data restoration**. Restoration can be performed simply, by selecting the target backup ID to restore, and then specifying restoration. Also, the restore options can be specified on a console, thereby eliminating complex command entry operations.
- **Automatic execution of backup operations**. Backup operations can be executed automatically by registering backup jobs with a specified schedule. Also, you can check the execution status and results of backup jobs in a list.
- **Link capability**. By linking functions of Device Manager, backup and restore operations can be performed from a remote site (through remote startup).
- **Locking capability**. You can lock or unlock a copy group while checking its lock status.
- **Copy group resynchronization**. You can resynchronize a copy group simply by selecting the backup ID associated with the copy group to be resynchronized, and then specifying resynchronization.
- **Setup GUI function**. You can use the Setup GUI function to set up the operating environment required for Protection Manager operations. Setting up items through the GUI eliminates the need to execute commands or edit configuration files. Also, you can set up only the items you need, in the desired order.

1.4 Implementing Protection Manager Console

Before you can begin working with Protection Manager Console, you must configure the system. This section describes the basic system configurations for file systems, databases, and remote startup operations.

1.4.1 System Configuration for File Systems

Backup and restore processes for a file system can be executed from a console, by installing Protection Manager Console on an application server where Protection Manager Copy Controller is installed, as shown in Figure 1.2.

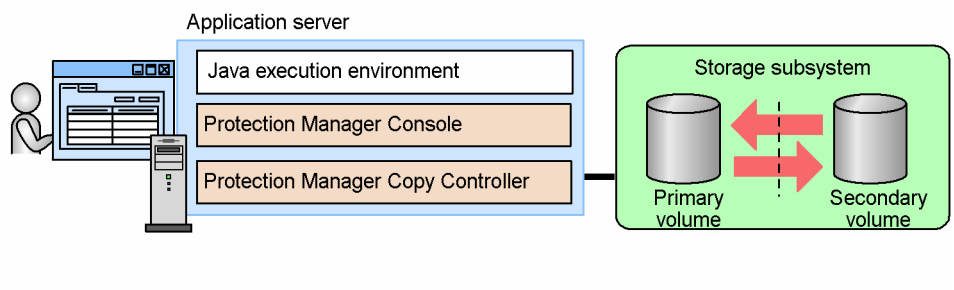


Figure 1.2 System Configuration for a File System

The following programs are required and must be installed on the application server:

- **Protection Manager Copy Controller**

  This product is a prerequisite for Protection Manager Console.

- **Java execution environment**

  Java Runtime Environment (JRE) 32-bit version: version 1.4.2, version 5.0 (1.5.0), or version 6.0

1.4.2 System Configuration for Databases

Backup and restore processes for SQL Server or Exchange databases can be executed from a console, by installing Protection Manager for SQL or Protection Manager for Exchange on the application server where Protection Manager Copy Controller and Protection Manager Console are also installed. Figure 1.3 shows an example of the system configuration for a database.

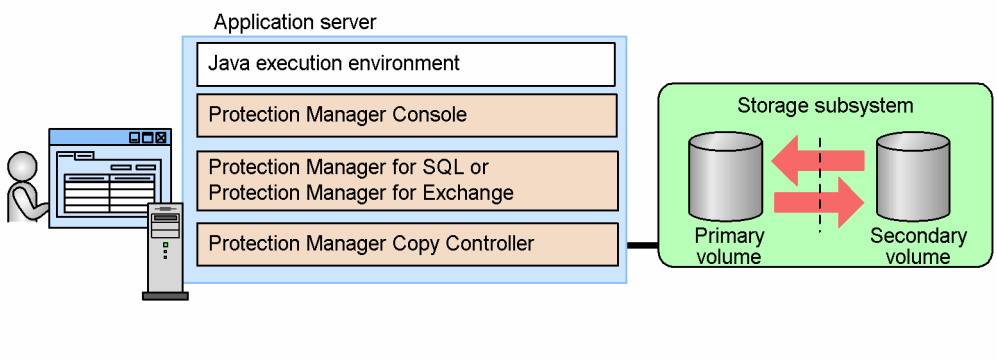


Figure 1.3 System Configuration for a Database

The following programs are required and must be installed on the application server:

- **Protection Manager Copy Controller**

  This product is a prerequisite for Protection Manager Console.

- **Java execution environment**

  Java Runtime Environment (JRE) 32-bit version: version 1.4.2, version 5.0 (1.5.0), or version 6.0

- **Protection Manager for SQL**

  This is used when operating on a SQL Server database. Protection Manager for SQL must be installed on the same application server where Protection Manager Copy Controller is installed.

- **Protection Manager for Exchange**

  This is used when operating on an Exchange database. Protection Manager for Exchange must be installed on the same application server where Protection Manager Copy Controller is installed.

1.4.3 System Configuration with Linkage to Device Manager (Remote Startup)

The system can be configured to enable a management client (Device Manager client) to perform a backup or restore from a console, by starting Protection Manager Console on the target application server. Figure 1.4 shows an example of such a configuration.

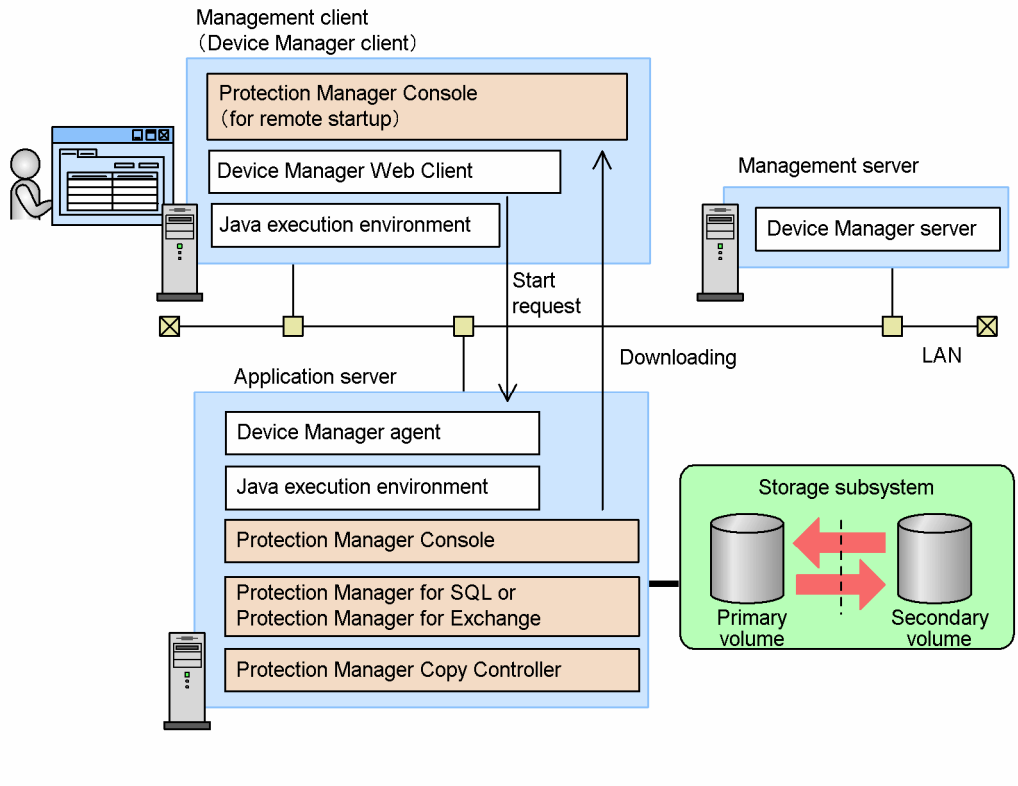


Figure 1.4 System Configuration with Linkage to Device Manager (Remote Startup)

HiCommand Device Manager is required to start Protection Manager Console from Device Manager.

The following programs are required for each host:

- **Application server**

  The application server must have the Device Manager agent and the Java Runtime Environment (JRE) installed, and the Device Manager usage environment must be set up, in order to start Protection Manager Console from Device Manager. For details about the Device Manager agent and Java Runtime Environment required for the application server, see the manual for the Device Manager.

  Protection Manager components that are necessary for linking to Device Manager are the same as when not linking to Device Manager. See section 1.4.1 and 1.4.2.

- **Management server**

  The management server must have the Device Manager server installed, and the Device Manager usage environment must be set up. For details on the Device Manager server, see the manual for Device Manager.

- **Management client (Device Manager client)**

  From the Device Manager Web Client, you can start Protection Manager Console by specifying an application server. When Protection Manager Console is started from the Web Client for the first time, Protection Manager Console for remote startup is downloaded from the application server.

  In order to start Protection Manager Console from Device Manager, the environment must be set up so that the Device Manager Web Client can be used from the client. For information on the Device Manager Web Client, see the manual for Device Manager. Also, the following programs must be installed as the Java execution environment (installing JRE automatically installs JWS):

  - Java Runtime Environment (JRE)
  - Java Web Start (JWS)

  For the version of JRE or JWS required on management clients, see the Device Manager manuals.

  Note: When Protection Manager Console is started from Device Manager remotely and the OS for the management client is Solaris, you must use the CDE (Common Desktop Environment). Because the GNOME desktop is not supported, the Protection Manager Console windows might be displayed incorrectly when using the GNOME desktop.

1.4.4 Prerequisite Operating Systems (OSs) for Each Host

Following are the prerequisite OSs for hosts acting as application servers, management servers (Device Manager server) and management clients (Device Manager client).

- **Application server**
  - Windows 2000 Server
  - Windows Server 2003

  When you want to use Windows Server 2003 (IPF version), you must install the *IA-32 Execution Layer 4.3 software driver*. You can download this driver from the Microsoft homepage. If it is not installed, Protection Manager Console might terminate abnormally.

- **Management server**

  Prerequisite OSs are the same as for the Device Manager server. For details, please see the Device Manager manual.

- **Management client**
  - Windows 2000 Professional
  - Windows 2000 Server
  - Windows XP Professional
  - Windows Server 2003
  - Windows Vista
  - Solaris 8
  - Solaris 9

  When you want to use Windows Server 2003 (IPF version), you must install the *IA-32 Execution Layer 4.3 software driver*.

1.4.5 User Privileges for Executing Protection Manager Console

To execute Protection Manager Console, the following administrator privileges are required:

- Administrator privileges of the OS

  Grant local administrator privileges to the executing user.

- Database access privileges
  - When backing up an SQL Server database

    Access the SQL Server using Windows authentication. The executing user must therefore be registered as a member of the SQL Server sysadmin-fixed server role.
  - When backing up an Exchange database

    Allow the executing user to belong to the domain Enterprise Admins group or the domain Exchange Domain Servers group.

Note: To start Protection Manager Console from Device Manager, note the following:

- The service start account for the Device Manager agent must have database access privileges.
- The Device Manager agent services must have been started by the Administrator account. If a Device Manager agent service has been started by an account other than the Administrator account, problems might occur. For example, if the environment variable `DRM_HOSTNAME` is changed, the change might not be applied to the service.

1.5 Understanding the Protection Manager Console Functions

Backup and restore processing for file systems, SQL Server databases, or Exchange databases can be executed from a console using Protection Manager Console. Protection Manager Console consists of three pages: the Application View, Backup Catalog View, and Backup Job View.

1.5.1 Viewing Application Information

The Application View, shown in Figure 1.5, displays a list of file systems and database instances that can be backed up or restored. In Protection Manager Console, this information is called the application information.

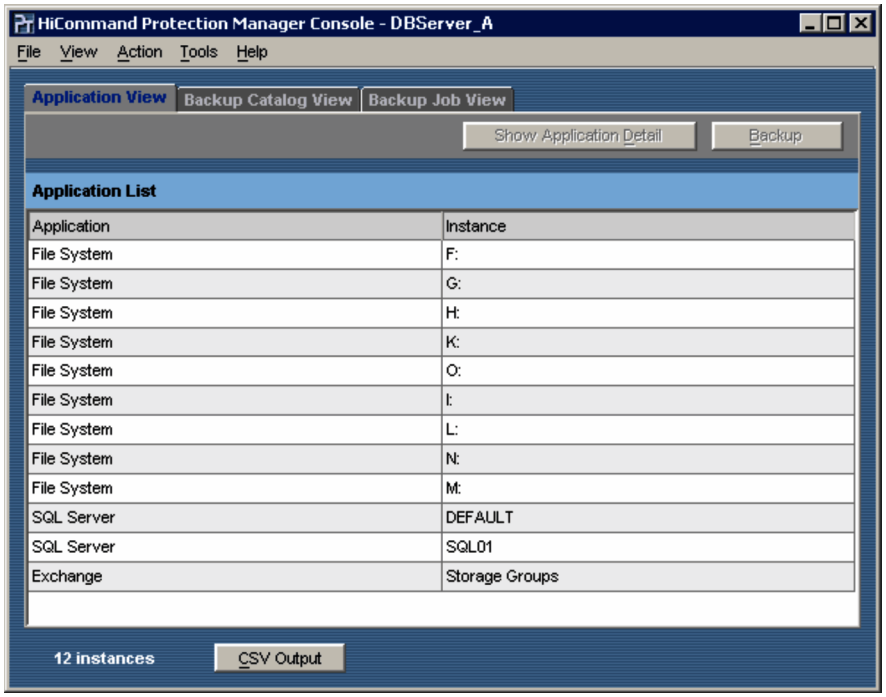


Figure 1.5 Protection Manager Console Application View

In order to back up databases or file systems, resource information is needed, including such information as the mount point directory for database objects and the file system, and the relation to the disk number within the RAID device. In Protection Manager, this information is managed as an application map, core map, and copy group map, in a dictionary map file.

By using Protection Manager Console, you can view the list of information necessary for backup, without having to enter commands or complete other operations.

1.5.2 Viewing Catalog Information

The Backup Catalog View, shown in Figure 1.6, displays a list of file systems and database instances that have been backed up thus far. In Protection Manager Console, this information is called catalog information.

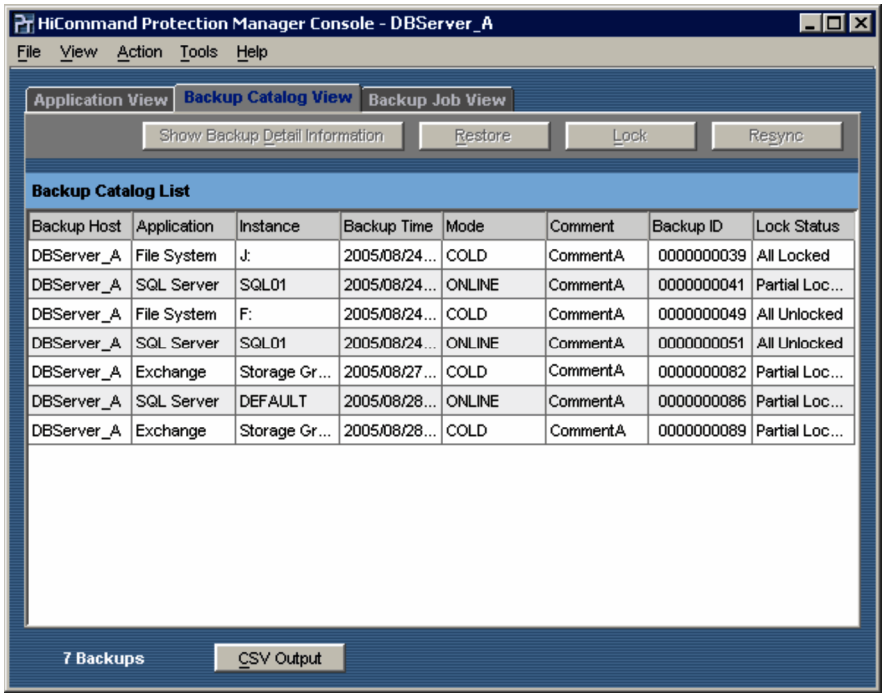


Figure 1.6 Protection Manager Console Backup Catalog View

Restoring from a backup requires the resource information from when the backup was executed. In Protection Manager, the system resource information used at the time of backup is associated with a unique backup ID, and is managed as a backup catalog of a dictionary map file. By using Protection Manager Console, you can view all information necessary for backup operations, such as backup history, as well as information for management of backup generations.

1.5.3 Backing up and Restoring Data

Protection Manager Console supports data backup and restoration on the console so that complex operations such as command entries are not necessary.

By creating the user script, you can perform the set of tasks to back up data from the primary volume, via the secondary volume, to tape, in one command.

- **Backing up Data**. Users can back up from a primary volume to a secondary volume, through either application database (DBMS) instance units or file system units. By selecting an instance name or a mount point for the file system that is displayed in the Application View, and then choosing backup, you can back up data without concern for related information about the applications or file system.
- **Restoring Data**. Users can restore from a secondary volume to a primary volume, using the backup catalog. You can execute a restore by selecting a backup ID from the catalog information displayed on the backup catalog view, and then choosing restore.

1.5.4 Managing Backup Jobs

If periodic backups are required, we recommend using the automatic job scheduler, instead of the manual backup method. You can register one or more backup jobs for each backup target that is displayed in the Application View of Protection Manager Console. By registering backup jobs, backup operations can be executed automatically in accordance with a specified schedule.

The Backup Job View (see Figure 1.7) lists all registered backup jobs, and it lets you perform the following operations:

- Checking the status
- Executing a job immediately
- Changing options
- Deleting jobs
- Displaying the execution result details window

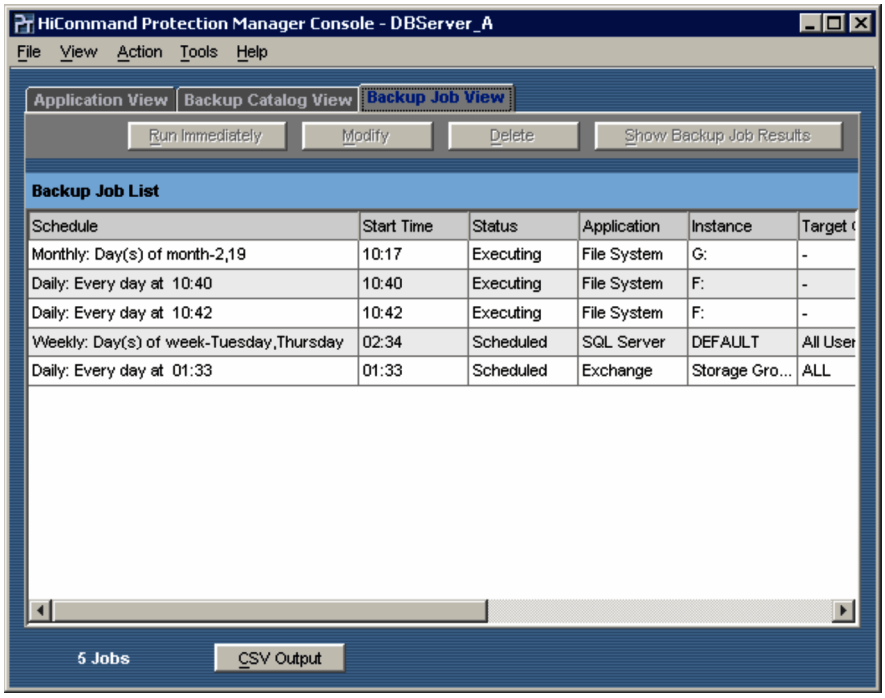


Figure 1.7 Protection Manager Console Backup Job View

1.5.5 Locking a Copy Group

You can lock a copy group by selecting the backup ID associated with the copy group from the catalog information that is displayed in Backup Catalog View, then specifying lock. Similarly, you can unlock a copy group.

Protection Manager automatically selects the backup destination copy group when executing backup. However, if you lock a particular copy group beforehand, Protection Manager can only continue backup using other copy groups.

1.5.6 Resynchronizing a Copy Group

You can resynchronize a copy group by selecting the backup ID associated with the copy group from the catalog information that is displayed in Backup Catalog View, then specifying resynchronization. When you resynchronize a copy group, the primary volume and secondary volume become mirrored.

- When usual operation is in a split state, resynchronize the copy group before backing up data.
- When usual operation is in a pair state, you do not need to resynchronize the copy group before backing up data. After the tape backup ends, resynchronize the copy group to initialize it.

Note: When using the Thunder 9200, the ShadowImage on the Thunder 9500V Series or the TagmaStore AMS/WMS Series, resynchronize the copy group on the database server. You can speed up the backup by resynchronizing the copy group prior to backup.

1.5.7 Outputting Application Information and Catalog Information to Files

Application information that is displayed in the Application View, and catalog information that is displayed in the Backup Catalog View, can be output to a file. Detailed application and catalog information can also be output to a file, using the detail display view. This view can be opened from either the Application View or the Backup Catalog View.

Using Protection Manager Console, application information and catalog information can be output to a file (in a tab-delimited list format), allowing the user to manage resources and backup history with spreadsheet applications.

1.5.8 Mounting and Unmounting a Secondary Volume

To reference backup data stored on a secondary volume, the secondary volume must be mounted. For example, if you want to use backup data on the secondary volume as a source for data mining, you can mount the secondary volume using Protection Manager Console. (Note, however, that once the backup data is used, you can no longer use it as backup data.)

If you want to synchronize the data in the primary and secondary volumes after mounting the secondary volume to reference the data in it, unmount the mounted secondary volume, and then back it up again. You can use Protection Manager Console to unmount the secondary volume that has been mounted.

1.5.9 Updating a Dictionary Map File

Even after starting your operation, you must update the dictionary map file when you modify the database configuration or perform related operations. You can use Protection Manager Console to update the dictionary map file on the desired host from one of the application servers (file server, database server, or backup server) or the management client (Device Manager client).

1.5.10 Linking to Device Manager (Remote Startup)

In addition to starting directly from an application server (a file server, a database server, or a backup server) on which it is installed, Protection Manager Console can also be started from a management client (Device Manager client) by selecting the target host (the application server). By linking with Device Manager, backup and restore processing can be performed as an integrated part of storage hardware management.

1.5.11 Starting the Setup GUI

You can start the Setup GUI from a Protection Manager Console menu. The Setup GUI(Graphial User Interface) function lets you use a GUI to set up the operating environment that is required for Protection Manager operations. Using the Setup GUI has the following advantages:

- Specialized knowledge about the commands and files used for environment setup is not required.
- You only need to set up required items because settings change automatically according to previous settings.
- You can check the current settings for each functional unit.

For details on using Setup GUI and settings, see the *HiCommand Protection Manager User's Guide*.

1.5.12 Configuration Check Function

Protection Manager provides the configuration check function to verify the required system configurations. With the configuration check function, you can check the following:

- Version of the OS
- Version of the DBMS
- Storage location of the database file to be backed up
- Integrity of the configuration definition file used by Protection Manager
- Existence of the programs required to run VSS (volume shadow copy service)
- Integrity of the volume manager and the disk configuration

When you first construct the system with Protection Manager or modify the existing system configuration, it is recommended that you use the configuration check function to verify your system configuration.

For details on how to use the configuration check function, see the *HiCommand Protection Manager User's Guide*.

Chapter 2 System Configuration with Protection Manager Console

This chapter describes the primary configuration patterns used for systems based on Protection Manager:

- Overview (see section 2.1)
- Configuring the System to Back up and Restore Data Between Volumes (see section 2.2)
- Configuring the System to Mount or Unmount a Secondary Volume (see section 2.3)
- Cluster Configuration of Operation Standby Type (Active-Passive)(see section 2.4)
- Cluster Configuration of Mutual Standby Type (Active-Active)(see section 2.5)
- Configuring the System to Execute Remote Copy (see section 2.6)
- Configuring the System when the Backup is Performed Using VSS (see section 2.7)
- Configuring the System when Using a Dynamic Disk Configuration (see section 2.8)

2.1 Overview

Protection Manager Console must be used in an environment in which Protection Manager and all the prerequisite products for Protection Manager Console are already installed and set up. The following sections in this chapter explain the required configuration of the Protection Manager and prerequisite products when using Protection Manager Console.

2.2 Configuring the System to Back up and Restore Data Between Volumes

To backup or restore data between a primary volume and a secondary volume using Protection Manager, connect a file server or database server to the storage subsystem. For such a configuration, install Protection Manager in the file server or database server, and then perform the backup and restoration operations. Figure 2.1 shows an example of a system configured to back up and restore data between volumes. Only primary volumes can be managed from the file server or database server.

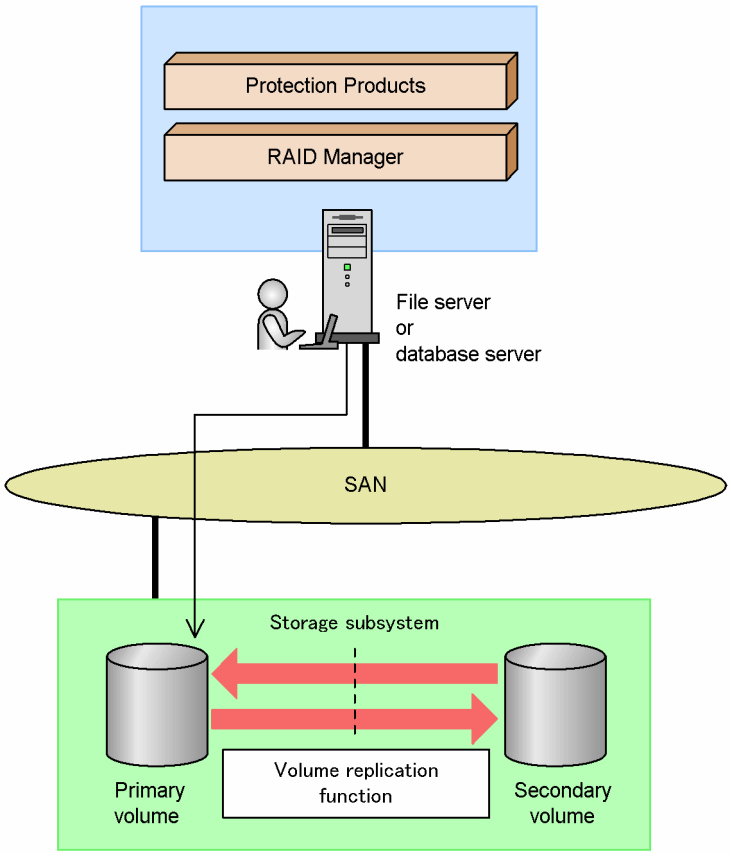


Figure 2.1 A System Configured to Back up and Restore Data Between Volumes

2.3 Configuring the System to Mount or Unmount a Secondary Volume

To store data that was backed up using Protection Manager in tape devices, or to reuse the backed-up data, you must mount a secondary volume. In this case, two servers are required: a file server or database server that manages a primary volume, and a backup server.

In such a configuration, install Protection Manager on the file server or database server, and on the backup server. Operate on the primary volume from the file server or database server, and on the secondary volume from the backup server.

The following is an example of a system configured to mount or unmount a secondary volume. You can mount or unmount a secondary volume by using Protection Manager Console.

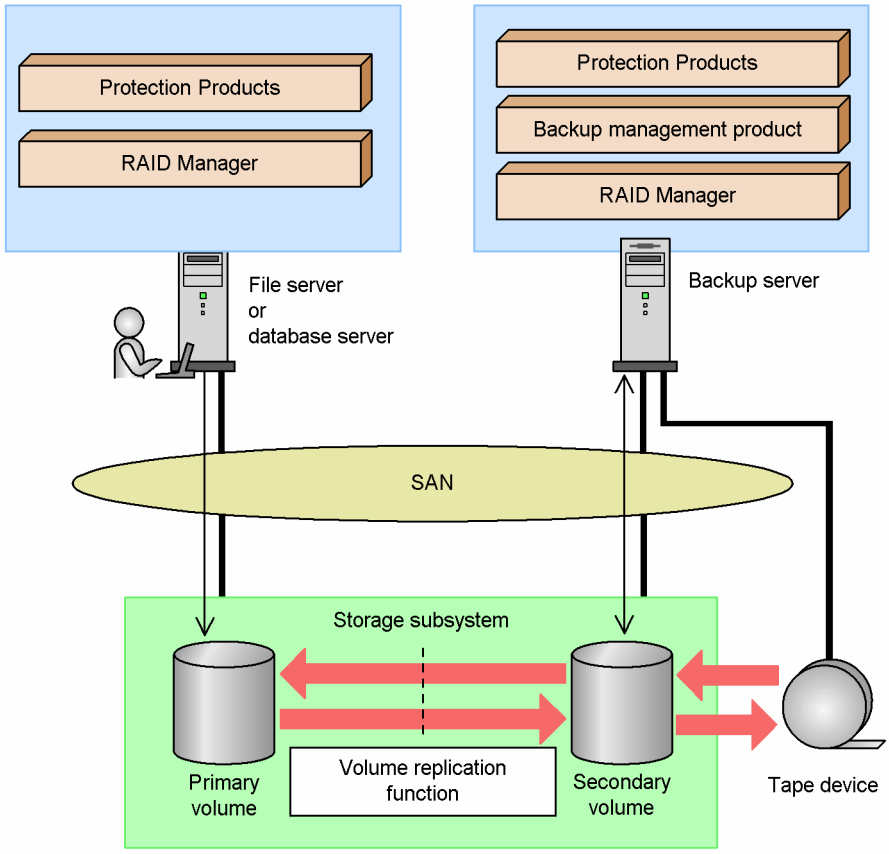


Figure 2.2 A System Configured to Mount or Unmount a Secondary Volume

2.4 Cluster Configuration of Operation Standby Type (Active-Passive)

Protection Manager supports cluster configurations of operation standby type (Active-Passive) in two-node configurations, on the database server and file server.

Figure 2.3 shows an example of a cluster configuration of operation standby type (Active-Passive). You can build a cluster configuration using file servers or database servers.

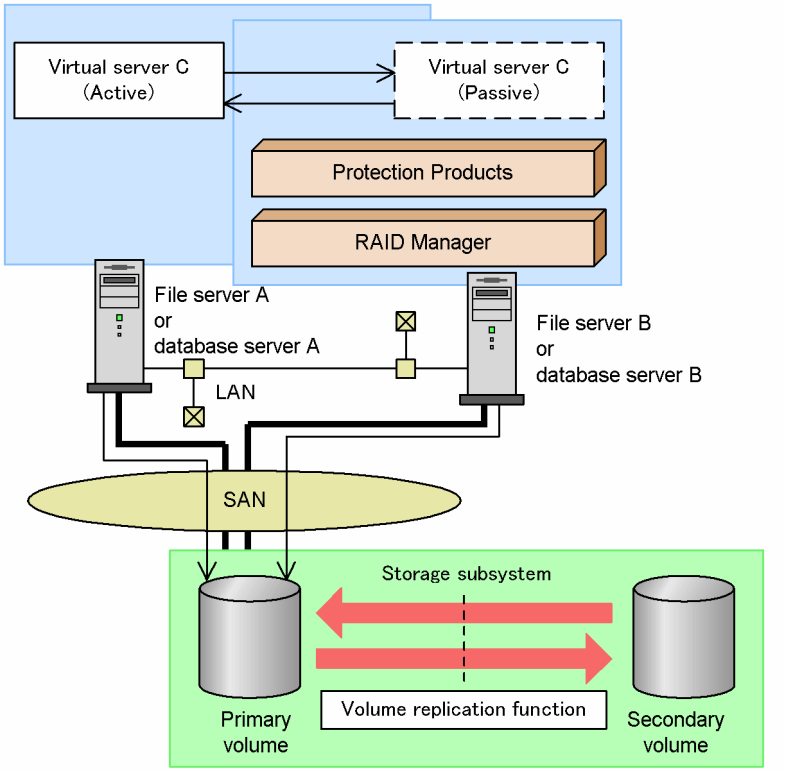


Figure 2.3 A Cluster Configuration of Operation Standby Type (Active-Passive)

To execute Protection Manager commands in a cluster configuration of operation standby type (Active-Passive), you must assign a storage destination for the dictionary map file used by each virtual server. For more information on how to assign the dictionary map file in a cluster configuration, see the *HiCommand Protection Manager User's Guide*.

2.4.1 Using a Backup Job in a . Cluster Configuration

To use a backup job in a cluster configuration of operation standby type (Active-Passive), you must use the cluster software to set up the environment. For details on how to do this, see section 4.4.

In normal operation, you do not need to be aware of internal job-schedule control because one server manages backup jobs regardless of whether the system is in a cluster configuration. However, if a failover occurs in a cluster configuration, you need be aware of the movement of job-schedule control because the server that manages backup jobs is switched.

In Protection Manager Console on a shared disk, a *schedule information file* manages backup job schedule information, and a *job execution result information file* records execution results. During normal operation, the job schedule management function on the active server accesses these files to control the job schedule. During operation after a failover occurs, the same schedule information file and job execution result information file are still used, but control of the job schedule management function is moved from the active server to the standby server.

The job-schedule control moves when a failover occurs because the environment was set up using the cluster software. The following figure shows job-schedule control after a failover.

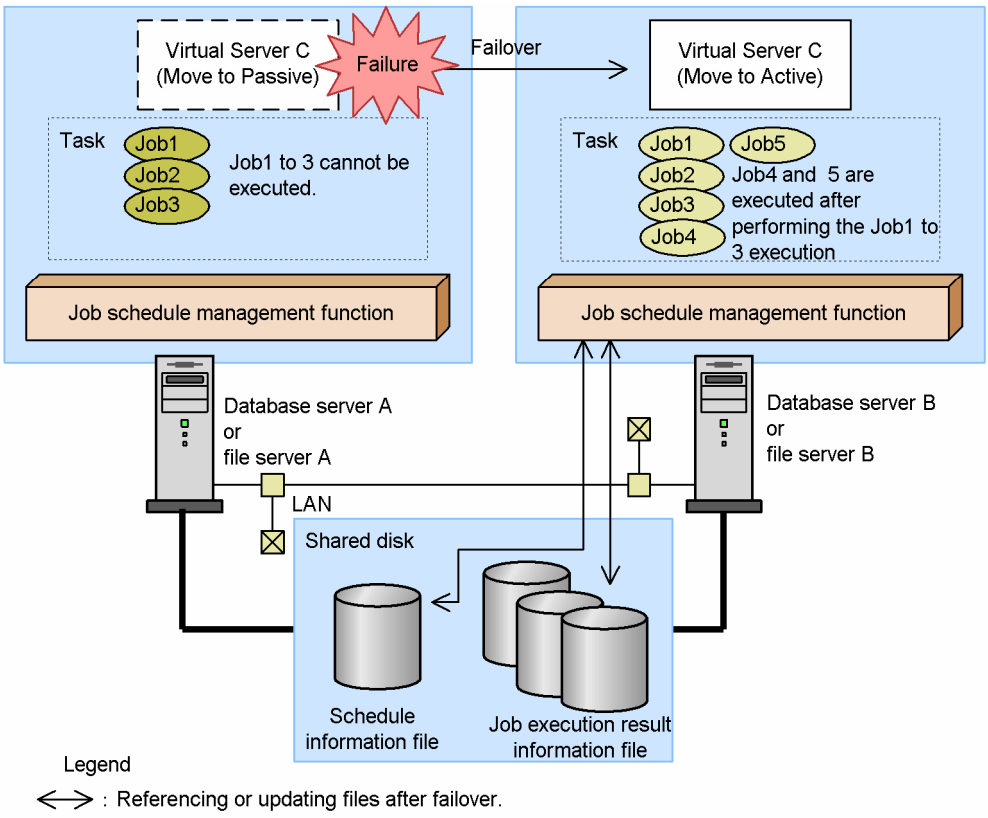


Figure 2.4 Job-Schedule Control after a Failover

2.5 Cluster Configuration of Mutual Standby Type (Active-Active)

Protection Manager supports cluster configurations of mutual standby type (Active-Active). A cluster configuration of mutual standby type is a configuration consisting of multiple operation standby type environments. Figure 2.5 shows an example of a cluster configuration of mutual standby type (Active-Active). You can build a cluster configuration using file servers or database servers.

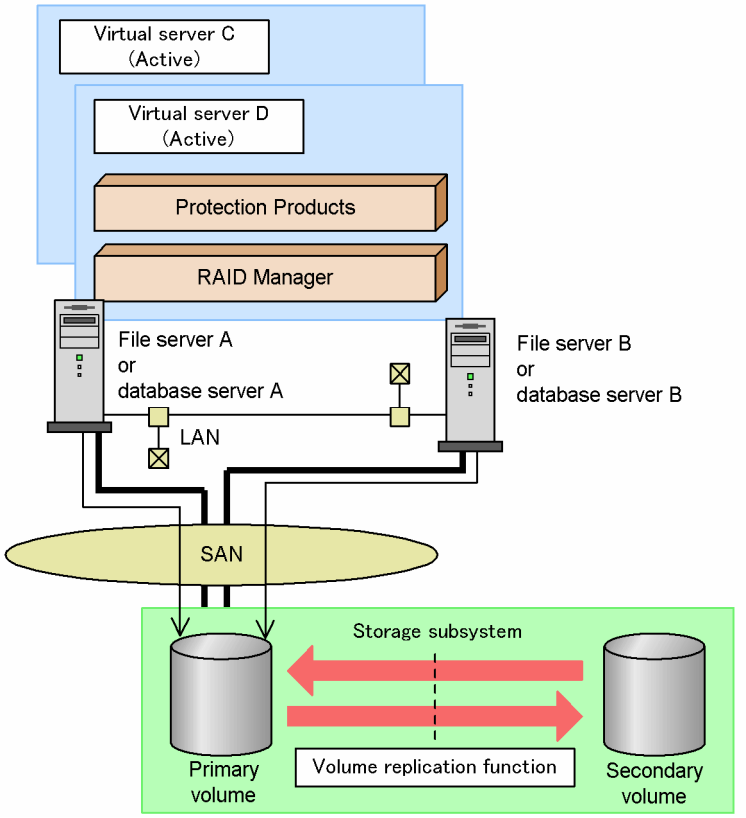


Figure 2.5 A Cluster Configuration of Mutual Standby Type (Active-Active)

To execute Protection Manager commands in a cluster configuration of mutual standby type (Active-Active), you must create a dictionary map file for each virtual server. You must also assign a storage destination for the dictionary map file used by each virtual server. For more information on how to assign the dictionary map file in a cluster configuration, see the *HiCommand Protection Manager User's Guide*.

To use a backup job in a cluster configuration of mutual standby type (Active-Active), it is necessary to use the cluster software to set up the environment. For details on how to do this, see section 4.4.

2.6 Configuring the System to Execute Remote Copy

By using TrueCopy and Universal Replicator (UR), Protection Manager supports backup to a storage subsystem at a remote site, and restoration from that storage subsystem. This support enables recovery from failures in a storage subsystem at the local site. The supported system configurations are as follows:

- TrueCopy or UR configurations
- ShadowImage and TrueCopy multi-target configurations
- ShadowImage and UR multi-target configurations
- ShadowImage (multiple generations), TrueCopy, or UR configurations

For cautionary notes on backing up or restoring between storage subsystems, see the *HiCommand Protection Manager User's Guide*.

2.6.1 TrueCopy or UR Configurations

As the basic configurations for backing up and restoring data between storage subsystems, Protection Manager supports configurations that use TrueCopy or UR functionality. The following figure shows an example of such a configuration.

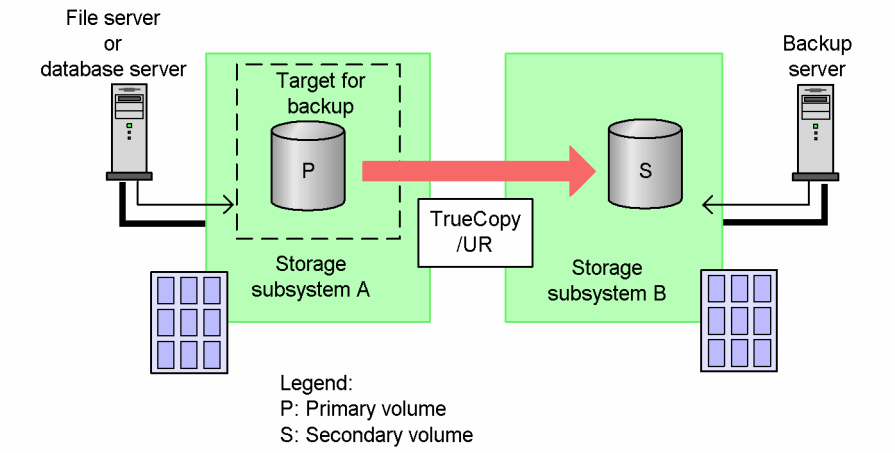


Figure 2.6 Example TrueCopy or UR System Configuration

2.6.2 ShadowImage and TrueCopy Multi-Target Configurations

Protection Manager supports ShadowImage and TrueCopy multi-target configurations. The following figure shows an example of such a configuration.

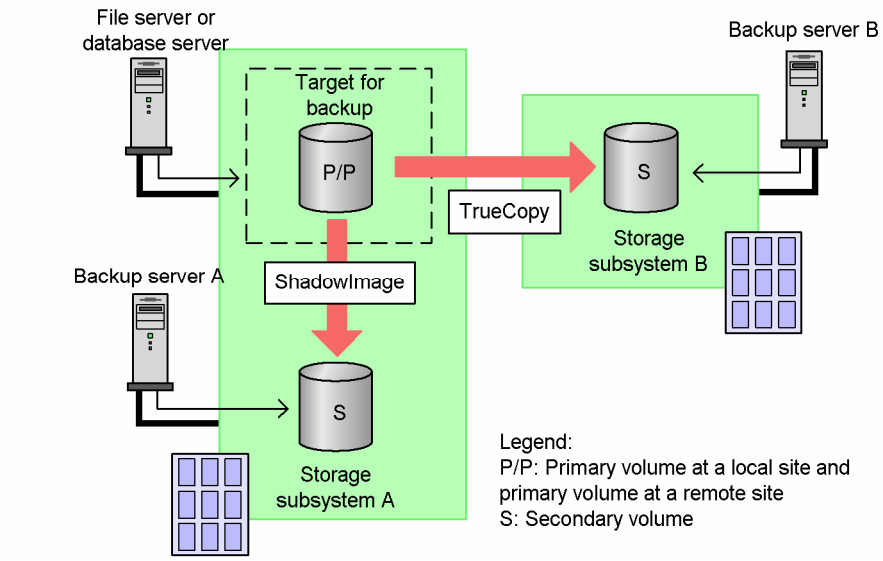


Figure 2.7 Example ShadowImage and TrueCopy Multi-Target Configuration

2.6.3 ShadowImage and UR Multi-Target Configurations

Protection Manager supports ShadowImage and UR multi-target configurations. The following figure shows an example of such a configuration.

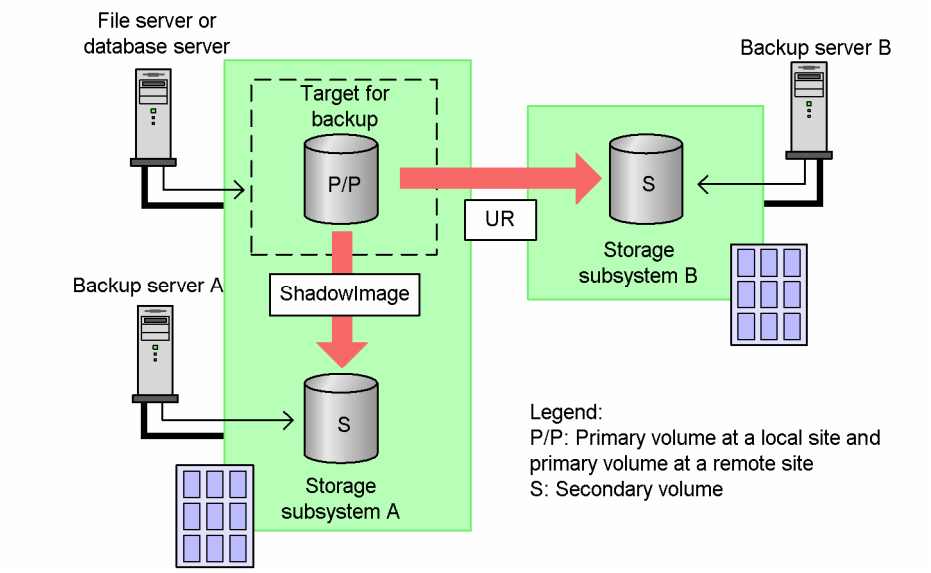


Figure 2.8 Example ShadowImage and UR Multi-Target Configuration

2.6.4 ShadowImage (Multiple Generations), TrueCopy or UR Configurations

Protection Manager supports ShadowImage (multiple generations), TrueCopy, or UR configurations. The following figure shows an example of such a configuration.

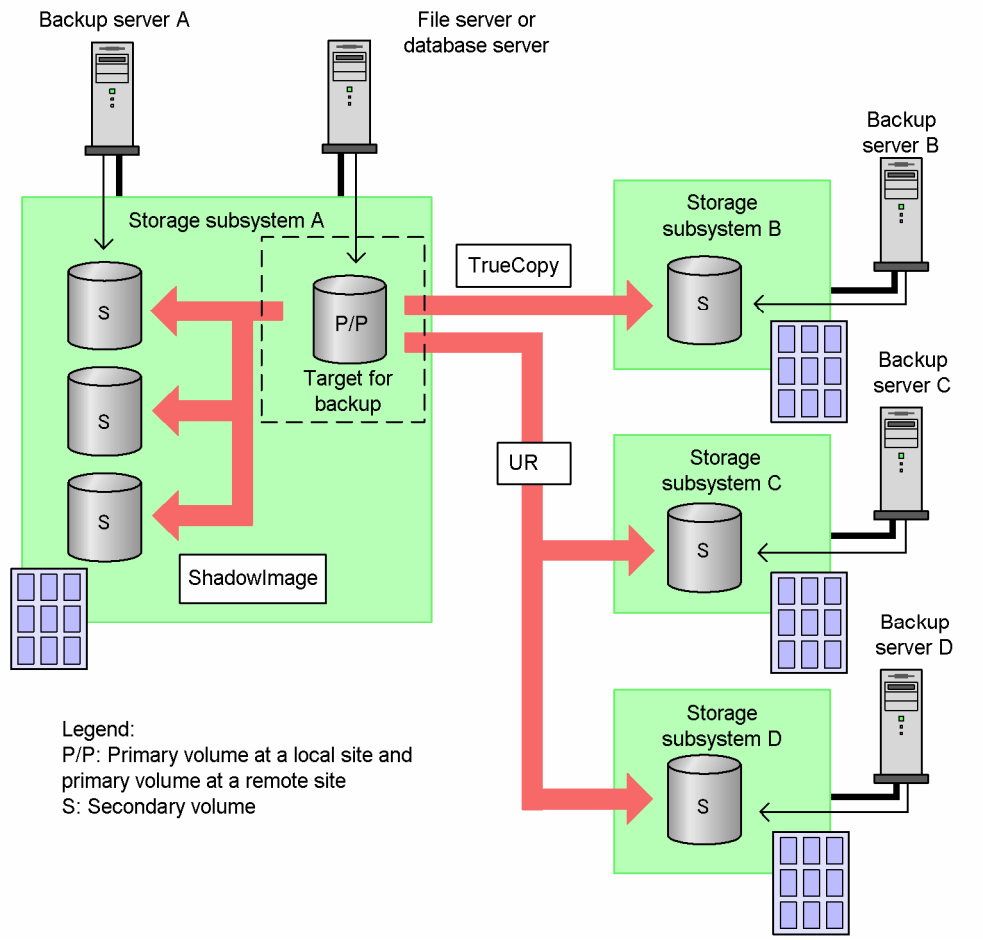


Figure 2.9 Example ShadowImage (Multiple Generations), TrueCopy or UR Configuration

2.7 Configuring the System when the Backup is Performed Using VSS

Protection Manager can use VSS to back up data when the backup is of a file system or an Exchange database. Protection Manager requires two servers (one file server or database server and one backup server) when it uses VSS to back up data. The file server and database server manage primary volumes. The backup server imports VSS snapshots and verifies the file system or Exchange database. The backup server imports VSS snapshots and verifies the Exchange database. The backup server can also store backup results on a tape.

In this configuration, you perform backups and restorations on the file server or database server. In the backup server, the Protection Manager service communicates with the file server or database server to perform the import of the VSS snapshot and the verification of the Exchange database.

The following figure is an example of a system configuration where Protection Manager uses VSS to back up data.

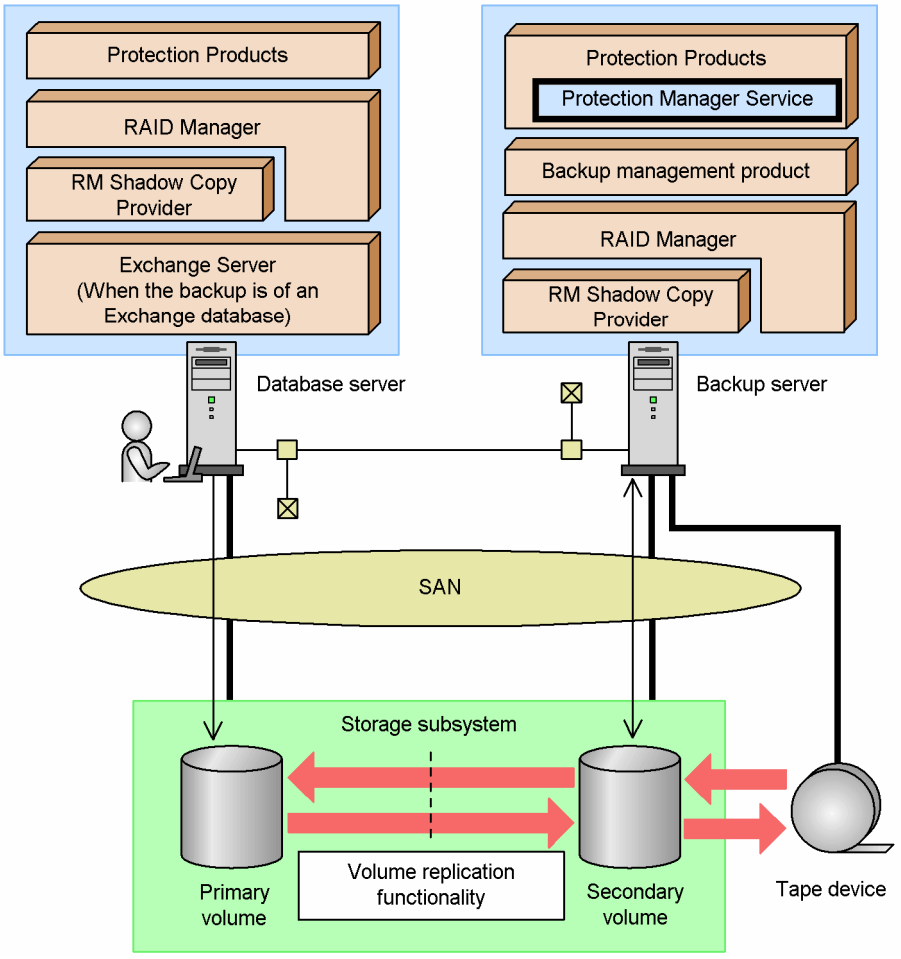


Figure 2.10 A System Configuration Where Protection Manager Uses VSS

2.8 Configuring the System when Using a Dynamic Disk Configuration

Protection Manager supports a system configuration using Windows dynamic disks.

Protection Manager Console allows you to back up and restore a file system only when the file system has a one-to-one relationship with a disk group (disk set).

The following figure shows an example of a system configuration using dynamic disks.

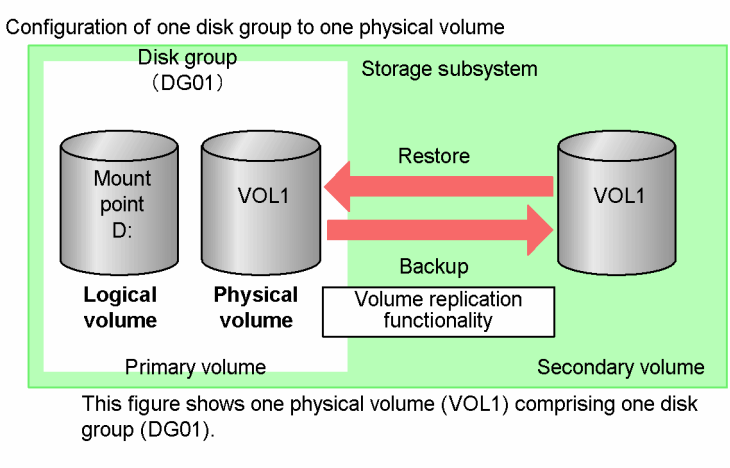


Figure 2.11 Example System Configuration Using Dynamic Disks

Chapter 3 Installing Protection Manager Console

This chapter describes how to install and uninstall Protection Manager Console:

- Preparing to Install Protection Manager Console (see section 3.1)
- Installing Protection Manager Console (see section 3.2)
- Uninstalling Protection Manager Console (see section 3.3)

3.1 Preparing to Install Protection Manager Console

This section describes the preparations required before you install Protection Manager Console.

3.1.1 Confirming Prerequisite Programs

Before installing Protection Manager Console, you must install all prerequisite programs and complete setup of the environment, as listed in the following tables. For information about system conditions for each product, see the manual *HiCommand Protection Manager User's Guide*.

Table 3.1 Prerequisite Products and Their Locations (for Local Startup)

Prerequisite Product		Application Server
Protection Manager Products	Protection Manager Copy Controller (required)	Required
	Protection Manager for SQL (optional)	Required for database operations
	Protection Manager for Exchange (optional)	
Java execution environment (JRE)		Required

Table 3.2 Prerequisite Products and Their Locations (for Remote Startup)

Prerequisite Product		Application Server	Management server (Device Manager server)	Management Client (Device Manager Client)
Protection Manager Products	Protection Manager Copy Controller (required)	Required	—	
	Protection Manager for SQL (optional)	Required for database operations		
	Protection Manager for Exchange (optional)			
Device Manager	Device Manager server	—	Required	—
	Device Manager agent	Required	—	—
Java execution environment	JRE	Required	—	Required
	JWS	—	—	Required

Note: You can install the Java execution environment and Device Manager in any order. When using an English version of Protection Manager Console, use English versions of Protection Manager Copy Controller, Protection Manager for SQL, and Protection Manager for Exchange.

3.1.2 Installing Protection Manager

Use of Protection Manager Console requires Protection Manager Copy Controller. When backing up or restoring a database, either Protection Manager for SQL or Protection Manager for Exchange is required, depending on the database.

For information about how to install Protection Manager Copy Controller, Protection Manager for SQL, and Protection Manager for Exchange, as well as details about environment setup, please see the *HiCommand Protection Manager User's Guide*.

Notes

- During the first-time installation of Protection Manager Copy Controller, a value is added to the system environment variable. To apply the system environment variable to the system, restart the system.
- After installing Protection Manager (prerequisite products), or after changing the system configuration (such as instance increases, decreases and volume changes), update the object map for the dictionary map file. To update the object map, use the following commands:
  - For Protection Manager Copy Controller: `drmfsdisplay`
  - For Protection Manager for SQL: `drmsqldisplay`
  - For Protection Manager for Exchange: `drmexgdisplay`

For details about updating the object map, see the *HiCommand Protection Manager User's Guide*. For details about the `drmfsdisplay`, `drmsqldisplay`, and `drmexgdisplay` commands, see the *HiCommand Protection Manager Command Reference*.

3.1.3 Installing Device Manager

Before starting Protection Manager Console from Device Manager by linking with Device Manager (remote starting), you must install the following Device Manager components, and you must complete the environment setup:

- Application server: Install Device Manager agent
- Management server: Install Device Manager server

Notes on the environment settings for Device Manager:

To complete a remote start, specify the application server from Device Manager Web Client, in order to start Protection Manager Console. Afterward, configure the Device Manager server and the Device Manager agent so that you can view the target host (application server) from the Device Manager Web Client.

For information about Device Manager installation and environment setup, please see the manual for Device Manager.

3.1.4 Installing the Java Execution Environment

To use Protection Manager Console from an application server (local starting), you must install JRE on the application server. To start Protection Manager Console from Device Manager by linking with Device Manager (remote starting), you must install JRE on the application server, and also install JRE and JWS on the Management client (Device Manager client). Download the Java execution environment from the Sun Microsystems, Inc. website. An installation of JRE also installs JWS automatically.

When installing the Java Runtime Environment (JRE), select "Custom install" and install the "Support for Additional Languages" function.

For information about the JRE and JWS versions required on each host, see section 1.4.

Notes on the JRE version

- On the JRE version 1.4.2_07 or earlier, when the OS is Windows Server 2003 SP1 or Windows Server 2003 R2 and the hardware DEP is enabled, sometimes Protection Manager Console does not run. If this happens, install JRE version 1.4.2_08 or later.
- If the management client OS is Windows Vista, install JRE version 6.0.

3.2 Installing Protection Manager Console

You can install Protection Manager Console on application servers such as file servers, database servers, and backup servers.

This section describes the procedures for installing Protection Manager Console. Before you start the installation, make sure that:

- The prerequisite programs for Protection Manager Console are already installed, and the environment setup is complete.
- You are logged in with Administrator privileges.
- All programs are inactive.
- Services of the Device Manager agent in the application server are inactive (when linking with Device Manager).

Note: If you want to reinstall Protection Manager Console, and the version you want to install is the same as the one already installed, make sure that you completely uninstall the program beforehand.

To install Protection Manager Console:

1. Insert the Protection Manager Console installation CD-ROM into a connected CD-ROM drive.
2. From the Windows **Start** menu, choose **Run**.

   The Run dialog box appears.
3. Type **x:\Setup.exe** (the x: drive represents the CD-ROM drive), then click the **OK** button.

   The installer window appears.
4. Click the **Next** button.

   A dialog box appears, prompting you to enter user information.
5. Enter the user name and company name, then click the **Next** button.

   A dialog box prompting you to confirm the installation destination appears.
6. Change the installation destination from the default if required, then click the **Next** button.

   Note: If you change the installation destination directory, do not specify a directory where another product is installed. The usable characters are alphanumeric characters, one-byte spaces, and the following special characters:

   # + - @ _ ( ) .

   If you do not change the installation destination directory, the following folder is assumed to be the installation destination for Protection Manager Console (if the OS is Windows Server 2003, the installation destination directory may vary):

   C:\Program Files\HITACHI\DRM_CONSOLE

   A dialog box appears, prompting you to select the setup type.

7. Select the setup type, then click the **Next** button. You can select any of the following three setup types:
   - **Standard**

     The Protection Manager Console program and the online manual are installed.
   - **Compact**

     Only the Protection Manager Console program is installed.
   - **Customized**

     The user selects the components to be installed.
8. Enter the name of the program folder, then click the **Next** button.

   A dialog box appears, prompting you to enter confirmation before file copying starts.
9. Ensure that the information you specified is correct, then click the **Next** button.

   Installation starts. Wait until a message is displayed, reporting that installation has finished.
10. Click the **Finish** button.

    When the installation finishes, the following directories are added to the PATH environment variable:
    - *Protection-Manager-Console-installation-directory*\lib
    - *Protection-Manager-Console-installation-directory*\bin

    Note: The length of the character string for the system environment variable `PATH` must be no more than 1,023 bytes. If the length exceeds 1,023 bytes, an error occurs.

3.2.1 Linking with Device Manager

When Protection Manager Console is installed, the files relevant to Protection Manager Console are automatically copied to the installation directory of Device Manager agent, so that a link to Device Manager is established. However, if the files copied to the Device Manager agent installation directory are corrupted after the Protection Manager Console installation, they must be *deleted and re-copied*. Execute these commands from the command prompt to delete or copy the files necessary for Device Manager linkage:

- **ptmguiuninst.exe** Deletes the files required for Device Manager linkage to the installation directory of Device Manager agent.
- **ptmguiinst.exe** Copies the files required for Device Manager linkage to the installation directory of Device Manager agent.

Important: Before running either executable, ensure that the following conditions are satisfied:

- Device Manager agent is installed.
- Services for Device Manager agent are stopped.
- Protection Manager Console is installed.

3.2.1.1 Deleting Files Required for Device Manager Linkage

Execute **ptmguiuninst.exe** from the command prompt on the application server where Protection Manager Console and Device Manager agent are installed.

3.2.1.2 Copying Files Required for Device Manager Linkage

Execute **ptmguiinst.exe** from the command prompt on the application server where Protection Manager Console and Device Manager agent are installed.

3.2.1.3 Command Details

Installation destination: *Protection-Manager-Console-installation-directory*`\bin`

Return code:

- `0`: Normal termination
- `1`: Termination with an error

For details about output messages, see the *HiCommand Protection Manager Messages*.

3.3 Uninstalling Protection Manager Console

Uninstalling Protection Manager Console automatically deletes files related to Protection Manager Console from the installation directory of Device Manager agent, and releases linkage of Protection Manager Console with Device Manager. After the uninstallation, please see section 3.2.1 for details about deleting files required for Device Manager linkage.

Important: Before you uninstall the Protection Manager Console, verify the following items:

- You are logged on with Administrator privileges.
- All programs are inactive.
- When linking with Device Manager, the Device Manager agent services (in the application server) are inactive.

To uninstall Protection Manager Console:

1. From the Windows **Start** menu, choose **Settings** and then **Control Panel**.

   The Control Panel opens.

2. Double-click **Add or Remove Programs** in Windows 2003 Server.

   The Add/Remove Programs dialog box appears.

3. In the **Currently installed programs** list, select **HiCommand Protection Manager Console**, then click the **Remove** button.

   The installer window appears.

4. Click the **Remove** button, then click the **Next** button.

   A dialog box appears, confirming whether you want to delete Protection Manager Console.

5. Click the **OK** button.

   Uninstallation starts.

6. After uninstallation finishes, close the dialog box.

7. Delete any user files that were created after installation, such as definition files and/or log files.

8. Delete the following directories from the system environment variable PATH:

   - Protection-Manager-Console-installation-directory\lib
   - Protection-Manager-Console-installation-directory\bin

   Note: For details about how to change environment variables, see the Windows help.

Note: In Windows Server 2003, when an attempt to uninstall Protection Manager Console fails, a dialog box that shows an X symbol might be displayed (this means that processing cannot continue). In this case, you must execute the `Setup.exe` command from the CD-ROM media to uninstall Protection Manager Console.

Chapter 4 Setting up the Protection Manager Console Environment

This chapter describes operating environment settings that are required for Protection Manager Console.

For details on environment setup affecting an entire Protection Manager system, see the *HiCommand Protection Manager User's Guide*.

- Overview (see section 4.1)
- Working with the Environment Setup Files for Protection Manager Console (see section 4.2)
- Working with the Setup Items for the Environment Setup File (see section 4.3)
- Using Backup Jobs in a Cluster Configuration (see section 4.4)

4.1 Overview

The operation environment of Protection Manager Console is configured through environment setup files. The following items can be configured using the files:

- The log function for Protection Manager Console
- Communication with the Device Manager agent
- Backup job management

Default values are set for all items. Alter these as necessary to suit your operations. For details on the environment setup files for Protection Manager Console, see section 4.2 and 4.3.

Note: To use Protection Manager Console, environment setup for Protection Manager Copy Controller must be completed. Similarly, to back up or restore a database, depending on the target DBMS, the environment setup for either Protection Manager for SQL or Protection Manager for Exchange must be completed. For more information on how to setup the environment for these products, see the *HiCommand Protection Manager User's Guide*.

4.2 Working with the Environment Setup Files for Protection Manager Console

Figure 4.1 provides an overview of the environment setup files.

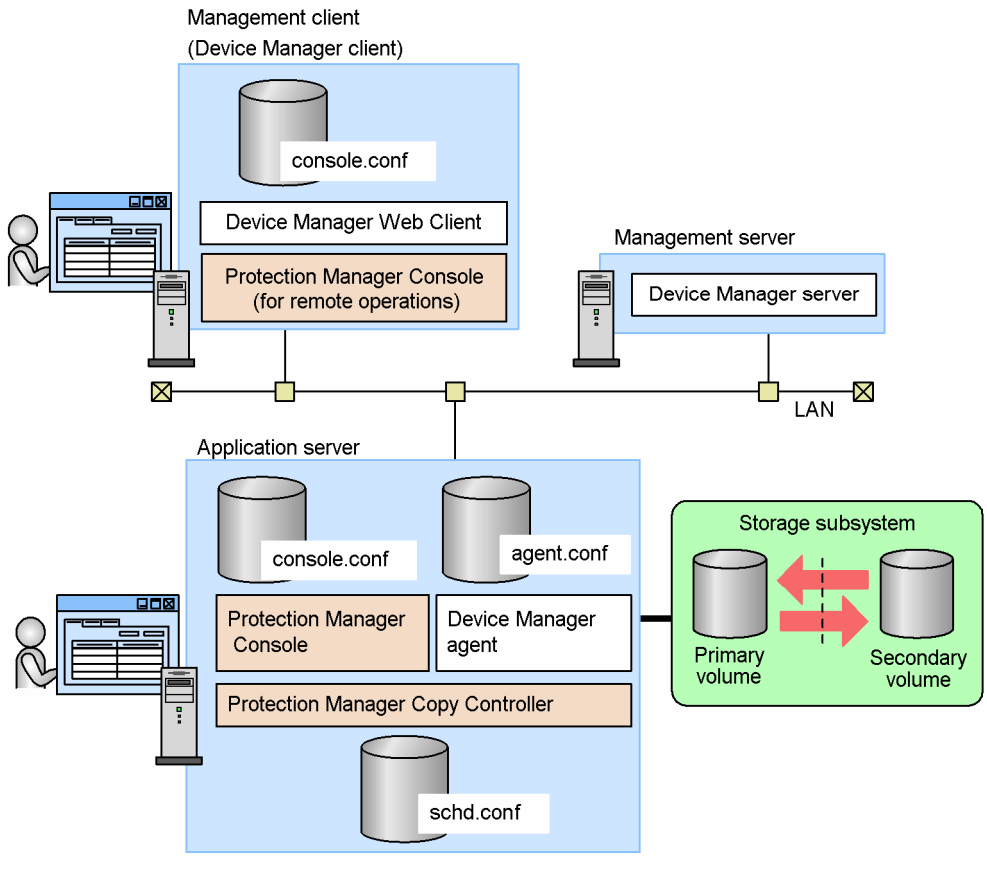


Figure 4.1 Environment Setup Files for Protection Manager Console

Table 4.1 describes the files for local execution (when using Protection Manager Console running on an application server) and remote execution (when using Protection Manager Console running on an application file server, from a management client (Device Manager client).

Table 4.1 Environment Setup Files for Protection Manager Console

Type	File Name	Server	Installed Location
Setup file for local execution	`console.conf`	Application server	*Protection-Manager-Console-installation-directory*`\conf\`
Setup file for remote execution	`agent.conf`	Application server	*Protection-Manager-Console-installation-directory*`\conf\`
	`console.conf`	Management client (Device Manager client)	In Windows: *user-home-directory-for-the-management-client*`\drm_console\conf\` In Solaris: *home-directory-for-the-management-client*`/drm_console/conf/`
Setup file for backup job management	`schd.conf`	Application server	*Protection-Manager-installation-directory*`\conf\`

Files for local execution, console.conf and agent.conf, are created when Protection Manager Console is installed on an application server. In contrast, the file for remote execution, console.conf, is created when Protection Manager Console is started for the first time on the management client (Device Manager client).

The `schd.conf` file is created when Protection Manager is installed. If necessary, edit the settings by using a text editor. For details, see section 4.3.4.

If changes have been made to the settings items in the:

- **agent.conf** file, restart the Device Manager Agent service to validate the changes.
- **console.conf file**, restart Protection Manager Console to validate the changes.
- **schd.conf file**, restart Protection Manager Console to validate the changes.

4.3 Working with the Setup Items for the Environment Setup File

The following table lists the environment setup files for Protection Manager Console, and lists the setup items in each file.

Table 4.2 Environment Setup Files for Protection Manager Console and Setup Items

Environment setup file	Setup Item	Description
console.conf (For local execution)	log.level	Setup items relating to log files, for local execution, that are located on an application server
	log.max_filecount	
	log.max_filesize	
	gui.progress.elapsed_time.interval	
	gui.progress.bar.interval	
agent.conf	log.level	Setup items relating to log files, for remote execution, that are located on an application server
	log.max_filecount	
	log.max_filesize	
console.conf (For remote execution)	log.level	Setup items relating to log files, for remote execution, that are located on a management client (Device Manager client)
	log.max_filecount	
	log.max_filesize	
	gui.progress.elapsed_time.interval	
	gui.progress.bar.interval	
	agent.timeout	Setup items relating to communication with the Device Manager agent
	agent.retry_count	
	agent.retry_time	
schd.conf	SCH_MAP_PATH	Setup items relating to storage destinations for the files used for backup job management.
	EXEC_LOG_OUTPUT	
	MAX_JOB_REGISTRATION_COUNT	Setup items relating to maximum values that can be specified for backup job management.
	MAX_JOB_RESULT_COUNT	

4.3.1 Setup Items for the console.conf File (for Local Execution)

4.3.1.1 log.level

Use this option to set the threshold level for the trace log files output by the log output function. Specify one of the following four values: 0, 10, 20, or 30. Larger values allow more detailed log information to be output.

Regardless of the type of each message (such as error, warning, or information), in Protection Manager Console the log output levels 0, 10, 20 and 30 are set according to the message content. Messages that have output levels less than or equal to the value set in log.level are output to the trace log file (trace$.log). The default value is 10.

The meaning of each output level is as follows:

- **0**: Specify for normal operation. Only high severity level messages are output.
- **10**: Specify for normal operation (including waiting for recovery). Warning level messages are output.
- **20**: Specify for error investigation (for recovery testing). The output messages are at a level that enables the readers to understand the processing flow.
- **30**: Specify for error investigation. All messages are output.

4.3.1.2 log.max_filecount

Use this option to set the maximum number of trace log files (trace$.log) output by the log output function.

When the files become full of log output, each file is backed up in turn until the number of files reaches a number one less than the maximum number specified in log.max_filecount. The most recent log file name has a 0 in place of the $. For the older files, the number can be any number greater than 0 and less than the specified number; the larger the number is, the older the log file. Specify a value between 2 and 10 for log.max_filecount. The default value is 2. Set a value that is appropriate for the operating environment.

4.3.1.3 log.max_filesize

Use this option to set the maximum size of the trace log files output by the log output function. The size should be specified in megabyte (MB) units. Specify a value between 1 and 32 for log.max_filesize. The default value is 1. Set a value that is appropriate for the operating environment.

4.3.1.4 gui.progress.elapsed_time.interval

Use this function to specify (in seconds) the refresh interval for the elapsed time displayed during the running of backup, restoration, lock, unlock, and resynchronization operations. Specify a value from 1 to 60 for gui.progress.elapsed_time.interval. The default value is 1.

4.3.1.5 gui.progress.bar.interval

Use this function to specify (in seconds) the refresh interval for the progress rate displayed during the running of backup, restoration, and resynchronization operations. Setting a small value may cause an increase in inquiries about progress status made to the application server, resulting in a delay in backup and other processes, or an increase in network load. A user familiar with the system should set this value, taking remote execution into consideration. Specify a value from 10 to 60 for gui.progress.bar.interval. The default value is 30.

4.3.2 Setup Items for the agent.conf File

Settings in the agent.conf file are only effective for remote execution of Protection Manager Console. Setting the agent.conf file is not necessary for local execution.

4.3.2.1 log.level

Use this option to set the threshold level for the trace log files output by the log output function. Specify one of the following four values: 0, 10, 20, or 30. Larger values allow more detailed log information to be output.

Regardless of the type of each message (such as error, warning, or information), in Protection Manager Console the log output levels 0, 10, 20 and 30 are set according to the message content. Messages that have output levels less than or equal to the value set in log.level are output to the trace log file (agt_trace.log.$). The default value is 10.

4.3.2.2 log.max_filecount

Use this option to set the maximum number of trace log files (agt_trace.log.$) output by the log output function.

When the files become full of log output, each file is backed up in turn until the number of files reaches a number one less than the maximum number specified in log.max_filecount. The most recent log file has the name agt_trace.log. For the older files, the number assigned to the file in its file name can be any number greater than 1 and less than the specified number; the larger the number is, the older the log file. Specify a value between 2 and 10 for log.max_filecount. The default value is 2.

4.3.2.3 log.max_filesize

Use this option to set the maximum size of the trace log files output by the log output function. The size should be specified in megabyte (MB) units. Specify a value between 1 and 32 for log.max_filesize. The default value is 1.

4.3.3 Setup Items for the console.conf File (for Remote Execution)

4.3.3.1 log.level

Use this option to set the threshold level for the trace log files output by the log output function. Specify one of the following four values: 0, 10, 20, or 30. Larger values allow more detailed log information to be output.

Regardless of the type of each message (such as error, warning, or information), in Protection Manager Console the log output levels 0, 10, 20 and 30 are set according to the message content. Messages that have output levels less than or equal to the value set in log.level are output to the trace log file (ip-address-of-application-server-or-host-name_trace$.log). The default value is 10.

4.3.3.2 log.max_filecount

Use this option to set the maximum number of trace log files (ip-address-of-application-server-or-host-name_trace$.log) output by the log output function.

When the files become full of log output, each file is backed up in turn until the number of files reaches a number one less than the maximum number specified in log.max_filecount. The most recent log file name has a 0 in place of the $. For the older files, the number can be any number greater than 0 and less than the specified number; the larger the number is, the older the log file. Specify a value between 2 and 10 for log.max_filecount. The default value is 2.

4.3.3.3 log.max_filesize

Use this option to set the maximum size of the trace log files output by the log output function. The size should be specified in megabyte (MB) units. Specify a value between 1 and 32 for log.max_filesize. The default value is 1.

4.3.3.4 gui.progress.elapsed_time.interval

Use this function to specify (in seconds) the refresh interval of the elapsed time displayed during the running of backup, restoration, lock, unlock, and resynchronization operations. Specify a value from 1 to 60 for gui.progress.elapsed_time.interval. The default value is 1.

4.3.3.5 gui.progress.bar.interval

Use this function to specify (in seconds) the refresh interval for the progress rate displayed during the running of backup, restoration, and resynchronization operations. Setting a small value may cause an increase in inquiries about progress status made to the application server, resulting in a delay in backup and other processes, or an increase in network load. A user familiar with the system should set this value, taking remote execution into consideration. Specify a value from 10 to 60 for gui.progress.bar.interval. The default value is 30.

4.3.3.6 agent.timeout

Use this option to set the connection timeout value, in milliseconds, for communication with Device Manager agent. You can specify agent.timeout as a value between 0 and the value set in Device Manager as the web server function completion time (server.agent.shutDownTime) for Device Manager agent. If 0 is specified, the timeout period is set as infinite. The default value is 5,000.

4.3.3.7 agent.retry_count

Use this option to set the retry count for when communication problems occur with Device Manager agent. Specify a value between 0 and 2,147,483,647 for agent.retry_count. The default value is 5.

4.3.3.8 agent.retry_time

Use this option to set the retry interval, in seconds, for when communication problems occur with Device Manager agent. You can specify agent.retry_time as a value between 0 and the value set in Device Manager as the web server function completion time (server.agent.shutDownTime) for Device Manager agent. The default value is 10.

4.3.4 Setup Items for the schd.conf File

4.3.4.1 SCH_MAP_PATH

Use this option to set the storage destination for a schedule information file by an absolute path. The settings vary depending on whether the system is in a cluster configuration. If the system is in a cluster configuration, you must specify the storage destination on a shared disk. For details on a schedule information file, see section 2.4.1.

- For a cluster configuration:

  If the virtual server is VS1, and the storage destination for a schedule information file viewed from the server is `M:\PTM\schedule`, the setting is as follows:

```
# Virtual Server (VS1) Storage Mapping
SCH_MAP_PATH=M:\PTM\schedule;VS1
```

  If the virtual servers are VS1 and VS2, and the storage destinations for schedule information files viewed from those servers are `M:\PTM\schedule` and `N:\PTM\schedule` respectively, the settings are as follows:

```
# Virtual Server (VS1) Storage Mapping
SCH_MAP_PATH=M:\PTM\schedule;VS1

# Virtual Server (VS2) Storage Mapping
SCH_MAP_PATH=N:\PTM\schedule;VS2
```

- For a non-cluster configuration:

  If the storage destination for a schedule information file is `C:\Program files\PTM\schedule`, the settings are as follows:

```
# Server Storage Mapping
SCH_MAP_PATH=C:\Program files\PTM\schedule
```

  If you omit this parameter, the following storage destination is assumed by default:

  Protection-Manager-installation-directory `\schedule`

4.3.4.2 EXEC_LOG_OUTPUT

Use this option to set the storage destination for a job execution result information file by an absolute path. The settings vary depending on whether the system is in a cluster configuration. If the system is in a cluster configuration, you must specify the storage destination on a shared disk. For details on a job execution result information file, see section 2.4.1.

- For a cluster configuration:

  If the virtual servers are VS1 and VS2, and the storage destinations for job execution result information files viewed from those servers are `M:\PTM\schedule` and `N:\PTM\schedule` respectively, the settings are as follows:

```
# Virtual Server (VS1) Storage Mapping
EXEC_LOG_OUTPUT=M:\PTM\schedule;VS1

# Virtual Server (VS2) Storage Mapping
EXEC_LOG_OUTPUT=N:\PTM\schedule;VS2
```

- For a non-cluster configuration:

  If the storage destination for a job execution result information file is `C:\Program files\PTM\schedule`, the settings are as follows:

```
# Server Storage Mapping
EXEC_LOG_OUTPUT=C:\Program files\PTM\schedule
```

  If you omit this parameter, the following storage destination is assumed by default:

  Protection-Manager-installation-directory `\schedule`

4.3.4.3 MAX_JOB_REGISTRATION_COUNT

Use this option to set the maximum number of backup jobs that can be registered. Specify a value between `1` and `500` for `MAX_JOB_REGISTRATION_COUNT`. The default value is `500`.

Note: If `MAX_JOB_REGISTRATION_COUNT` is set to a smaller value than the number of backup jobs that have already been registered, the specified value is ignored and the default value is used as the maximum value.

4.3.4.4 MAX_JOB_RESULT_COUNT

Use this option to set the maximum number of execution results that can be displayed for one backup job. Specify a value between `1` and `64` for `MAX_JOB_RESULT_COUNT`. The default value is `64`.

4.4 Using Backup Jobs in a Cluster Configuration

This section describes how to set up an operating environment that enables backup jobs to be used in a cluster configuration.

Protection Manager Console provides a dedicated command (executable file) for switching the target node for which backup jobs are to be executed. Set up this command (`drmjobsch.exe`) in the cluster software so that it runs automatically when a failover occurs.

Verify the following before performing the appropriate procedure for the cluster software you are using:

- Protection Manager and the cluster software have been installed successfully.
- You have logged in as a member of the Administrators group.

When using Microsoft Cluster Service (MSCS)

Perform the following procedure on each server that makes up the virtual server.

To specify the required settings:

1. Create a VBScript file.

   File name: `RecoverJob.vbs`

   File storage location: *Protection-Manager-installation-directory*`\schedule`

   Note: For details on the Protection Manager installation directory, see the *HiCommand Protection Manager User's Guide*.

   You can change the name of a created VBScript file and the file storage location. For maintenance reasons, Hitachi recommends that you use the above file name and file storage location.

2. Edit the VBScript file, and specify the recovery processing to be performed by `drmjobsch.exe`.

   At the entry point `Function Online( )`, specify that the following command is to be executed, where *virtual-server-name* is the name of a virtual sever to be put online:

```
"Protection-Manager-installation-directory\bin\drmjobsch.exe" -recover -hostname
virtual-server-name
```

   The following shows an example of specifying a VBScript file. In the example, *Protection-Manager-installation-directory* is `C:\Program Files\HITACHI\DRM`.

```
'Script-Level Global Variables
Resource.LogInformation("Script-wide code begins execution")
Dim WshShell, oExec
Set WshShell = CreateObject("WScript.Shell")

Function Online( )
    Online = 0
    Resource.LogInformation "Entering Online"

    Set oExec = WshShell.Exec (CHR(34) & "C:\Program Files\Hitachi\drm\
       bin\drmjobsch.exe" & CHR(34) & " -recover -hostname virtual-server-name")
    Do While oExec.Status = 0
      Set oWait = WshShell.Exec("timeout /t 1")
    Loop
```

```
    Resource.LogInformation "Exiting Online"
End Function

Function Offline( )
    Offline = 0
End Function

Function LooksAlive( )
    LooksAlive = 0
End Function

Function IsAlive( )
    IsAlive = 0
End Function

Function Open( )
    Open = 0
End Function

Function Close( )
    Close = 0
End Function

Function Terminate( )
    Terminate = 0
End Function
```

Note: `CHR(34)` indicates a double quotation mark ("). When *Protection-Manager-installation-directory* does not contain any spaces, you do not need to specify `CHR(34)`. The following is the specification when there are no spaces:

`"C:\drm\bin\drmjobsch.exe" & " -recover -hostname` *virtual-server-name*`"`

For details on the specification method, see the VBScript documentation.

3. Use the Cluster Administrator wizard to add the new resource to the cluster resource group with the name *virtual-server-name* (such as a cluster resource group for SQL Server or Exchange Server).

   Resource type: `Generic Script`

   Script file path: Path name of the created VBScript file

   If the VBScript file is stored on a shared disk for nodes, register this shared disk as a Physical Disk resource in the **Resource dependencies** field in the Dependencies dialog box.

When using VERITAS Cluster Server (VCS)

As with MSCS, create a script that specifies recovery performed by `drmjobsch.exe` and then set the script as a `PostOnline` event trigger of VCS.

For details on how to specify the script and how to set up the event trigger, see the VCS documentation.

Chapter 5 Using Setup GUI to Set Up an Environment

Setup GUI is one of the Protection Manager Console functions. By using Setup GUI, you can set up an operating environment for Protection Manager from GUI windows.

This chapter describes how to set up an environment for Protection Manager by using Setup GUI.

This chapter also explains how to use the configuration check function to check the environment after setting it up with the Setup GUI.

- What is Setup GUI? (see section 5.1)
- Setup GUI Windows (see section 5.2)
- Configuration Check Function (see section 5.3)

5.1 What is Setup GUI?

Setup GUI is a function that allows you to use GUI windows to set up an operating environment for Protection Manager.

In the Setup GUI window, the operating environment settings required for Protection Manager operation are grouped into, and displayed as tabbed pages, each corresponding to a particular processing target, functionality, or operating method. You can use Setup GUI to navigate to the tab where the desired setting can be specified (called *tab navigation*). To set up an environment for Protection Manager, follow the tab navigation instructions to assign item values as necessary for each tab, and then click the **Save** button.

5.1.1 What Can You Do with Setup GUI?

Of the operating environment settings that are required for Protection Manager operation, you can use Setup GUI to specify the items listed in the table below. For further information on these items and the corresponding configuration files, see the sections indicated in the *Reference* column.

Table 5.1 Protection Manager Operating Environment Settings Specifiable in Setup GUI

Item	Tab	Configuration files	Command	Server
Configuration settings for Protection Manager operation	**Configuration Settings** tab	None	None	FS, DB, BK
Protection Manager operation settings	**Operation Setup** tab	Protection Products configuration definition file (`init.conf`)	None	FS, DB, BK
Creation of a dictionary map file	**Operation Setup** tab	None	`drmdbsetup -i`	FS, DB, BK
Settings for linkage with RAID Manager	**RAID Manager Linkage** tab, **RAID Manager Operation** tab	RAID Manager-linkage definition file (`DEFAULT.dat`[1])	None	FS, DB, BK
Creation of a cluster information configuration definition file	**Cluster Configuration** tab (the Instance Details dialog box is also used)	For VCS: Cluster information configuration definition file (`VCS.dat`) `DEFAULT.dat`[1]	`drmclusinit`	FS, DB
		For MSCS: Protection Products configuration definition file (`init.conf`)	None	
Creation of a database	**Database Configuration** tab	Database configuration definition file (*instance-*	`drmsqlinit`	FS, DB

Item	Tab	Configuration files	Command	Server
configuration definition file (required when the backup is of an SQL Server database)		*name*.dat)		
		Protection Products configuration definition file (init.conf)	None	
Settings required to use VSS (required if the backup is of a file system or an Exchange database)	**VSS Definition** tab	VSS definition file (vsscom.conf),	None	FS, DB, BK
	VSS Environment tab	Environment variables	None	
Specification of the port number to be used by the Protection Manager service	**Protection Manager Service tab**	Windows services file	None	FS, DB, BK
Updating of the dictionary map file	**Update Dictionary Map** tab	None	drmfsdisplay -refresh or drmsqldisplay -refresh or drmexgdisplay -refresh	FS, DB, BK[2]
Settings for linkage with the backup management product	**Backup Linkage** tab	Configuration definition file for linkage with the backup management product (DEFAULT.dat[1])	drmtapeinit	BK
	Tape Backup tab	Tape backup configuration definition file (NBU.dat, BEWS.dat)	None	
Settings for Linkage with RAID Manager particular to the operation style	**Copy Definition** tab	Copy parameter definition file[3] (*any-file-name*)	None	FS, DB, BK
Creation of target definition files (except the transaction log list file)	**List File** tab	List file (*any-file-name*)	None	FS, DB, BK
Preparation for extended command execution	**Extended Commands Definition** tab	Operation definition file (_*operation-ID*.dat)	None	FS, DB, BK
		Host environment settings file (host.dat)	None	
Creating a user script	**Pre/Post Job Template** tab	User script file (any file name)	None	FS,DB
Mail send settings	**Email Notification** tab	Mail send definition file	None	FS,DB

Item	Tab	Configuration files	Command	Server
		(mail.conf)		

Legend:

- FS: This item is required on a file server.
- DB: This item is required on a database server.
- BK: This item is required on a backup server.

[1]Although these files are of the same name DEFAULT.dat, they are different files stored at different locations.

[2]This is not usually required for a backup server. When a primary volume does not exist in the backup server, updating of the dictionary map file is not necessary. It is only necessary to update the file when a primary volume exists in the backup server.

[3]When Protection Manager is verifying pair status at the time of backup, restore, or resynchronization, use this file if you want to specify the number of verification times or specify interval lengths separately for particular processing purposes or load conditions.

Notes:

You cannot use Setup GUI to specify or perform the following items or tasks.

- Specification of the PAIR_CREATE parameter in the RAID Manager-linkage definition file (DEFAULT.dat)

  For details on how to specify this parameter, see "Specifying Volume Pair Creation" in the *HiCommand Protection Manager User's Guide*.

- Creation of a transaction log list file

  For details on how to create this file, see section see "Creating a Transaction Log List File" in the *HiCommand Protection Manager User's Guide*.

- Specification of the SQL Server login timeout option (SQL_LOGIN_TIMEOUT parameter) or SQL Server automatic recovery time (SQL_AUTORECOVERY_TIME parameter) in the configuration file sqlinit_*instance-name*.conf is required when the backup is of a SQL Server database

  For details on how to specify these parameters, see section see "Specifying Settings Related to Linkage with an SQL Server" in the *HiCommand Protection Manager User's Guide*.

You cannot use Setup GUI to specify the environment settings shown in

Table 5.2 required for prerequisite products. For details on these items, see the documentation and sections indicated in the *Reference* column.

Table 5.2 Environment Settings for Prerequisite Products

Environment setting	Configuration file	Server type	Reference
Configuration of the storage subsystem volume replication function	None	Not applicable	Storage subsystem documentation
Configuration of RAID Manager	RAID Manager configuration definition file (`horcmn.conf` where *n* is the instance number)	FS, DB, BK	Section 5.2.4
Configuration of the backup management product	None	BK	Documentation of the backup management product

Legend:

- FS: This item is required on a file server.
- DB: This item is required on a database server.
- BK: This item is required on a backup server.

5.1.2 Setup GUI Startup Method and Window Components

This section describes the Setup GUI startup method and Setup GUI window components.

5.1.2.1 Setup GUI Startup Method

To start Setup GUI, select **Tools** and then **Setup** from the menu in the Protection Manager Console Main window. For further information on how to start Protection Manager Console and about the Protection Manager Console Main window, see the *HiCommand Protection Manager Console User's Guide*.

Notes:

Before you can use Setup GUI, Protection Manager Console must be installed.

Note that you can use Setup GUI only when Protection Manager Console has been locally started from an application server. You cannot use Setup GUI if Protection Manager Console has been remotely started from Device Manager.

5.1.2.2 Setup GUI Window Components

A Setup GUI window consists of a title bar, a tab view bar, and an information view. When you select a tab on the tab view bar, the information view displays the tabbed page containing detailed information, allowing you to specify main Protection Manager operating environment settings in the window.

An information view that appears when the corresponding tab is clicked on the tab view bar is hereafter called a *window*. For example, the window displayed when the **Configuration Settings** tab is selected is called the Configuration Settings window.

Figure 5.1 shows the Setup GUI window components:

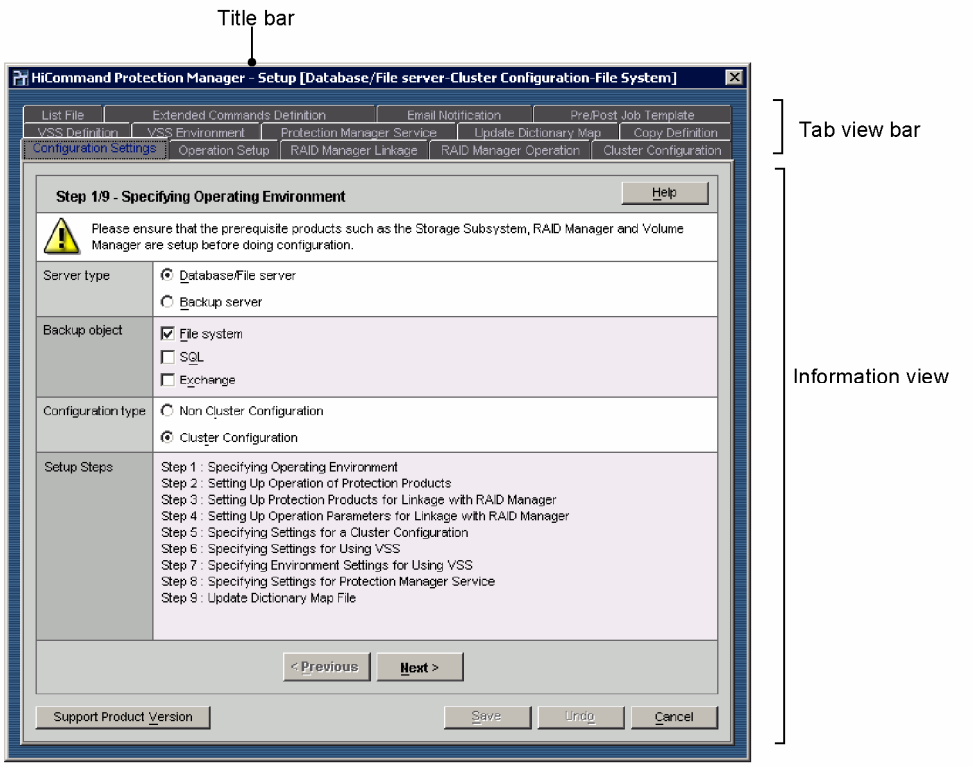


Figure 5.1 Setup GUI Window Components

Title bar

Displays the title of the window you specified in the Configuration Settings window, in the following format:

```
HiCommand Protection Manager - Setup [Server type - Configuration type - Backup object]
```

Information displayed in the title area is explained below:

```
HiCommand Protection Manager - Setup
```

Indicates that the window is a Setup GUI window.

Server type

Displays the *server type* (**Database/File server** or **Backup server**) selected in the Configuration Settings window.

Configuration type

Displays the *Configuration type* (**Non Cluster Configuration** or **Cluster Configuration**) selected in the Configuration Settings window.

Backup object

Displays the *backup object* (**File system**, **SQL**, and/or **Exchange**) selected in the Configuration Settings window.

If you selected two or more backup objects, the selected backup objects are displayed in a list, with each object separated by a comma (,).

For example, if you selected **File system** and **SQL**, the backup objects are displayed as follows: `File system, SQL`

Tab view bar

Parameters required for Protection Manager operation are grouped according to the processing target, functionality, and manipulation style, and these groups are displayed as tabs. When you click a tab, the corresponding information view appears.

Note: You can use Setup GUI to navigate to other tabs where you can specify the remaining settings, based on the settings that you specified in the Configuration Settings window. Depending on the specified settings, the number of displayed tabs varies.

Information view

Displays a list of the settings that are required for Protection Manager operation.

On each information view, the left area displays the title of the setting (the main category of the setting) and the right area displays the setup parameter names (more detailed subcategories of the setting) and input/output fields for these parameter values.

Shared Setup GUI operation buttons are also displayed. For further information on these buttons, see section 5.1.2.3.

Notes:

- Placing the mouse cursor near a setting on an information view will display a brief text description (tool tips) of the item.
- The top line of an information view indicates what you can specify on the current tab in the following format:

  `Step` *number-of-the-step-being-executed/total-number-of-steps – overview-of-setup-item-to-be-specified-on-the-window*

  This shows how far you have progressed within the entire setup flow.

  For the following setup windows, which can only be displayed by direct selection, only an *overview-of-setup-item-to-be-specified-on-the-window* is displayed:

  - Copy Definition window
  - List File window
  - Extended Commands Definition window
- Depending on the settings specified in the Configuration Settings window, the number and types of items that are displayed in an information view other than the Configuration Settings window vary.
- On some windows, settings are displayed as check boxes. You can specify a value for such a setting by selecting the check box.

5.1.2.3 Shared Setup GUI Operation Buttons

Shared Setup GUI operation buttons displayed on information views are outlined below. To learn the functionality of a button on a specific tab, see the Setup GUI help that appears when the **Help** button is clicked.

Help

Displays help information about the current window in a default browser window. Click this button when you want to learn or confirm details about an item in the window.

< Previous

If you have not modified a parameter value in the current window, and then click this button, the previous window is displayed.

If you have modified one or more parameter values in the current window and click this button, a dialog box appears, asking you whether you want to save the modified parameter values.

If you click the **Yes** button:

The modified parameter values are saved in the corresponding configuration files, and then the previous window is displayed.

If you click the **No** button:

The previous window is displayed, without saving the changes to the parameter values.

If you click the **Cancel** button:

The current window will remain.

Next >

If you have not modified a parameter value in the current window, and then click this button, the next required window will be displayed.

If you have modified one or more parameter values in the current window, and then click this button, a dialog box appears, asking whether you want to save the modified parameter values.

If you click the **Yes** button:

The modified parameter values are saved in the corresponding configuration files, and then the next required window is displayed.

If you click the **No** button:

The next required window is displayed, without saving the changes to the parameter values.

If you click the **Cancel** button:

The current window will remain.

Support Product Version

Displays environment information, including the storage subsystem in use, RAID Manager information, and VSS information (such as the serial number, micro code, and version information) in the Version Information window.

Save

The modified parameter values are reflected in the settings.

If you have modified one or more parameter values in the window, and then click this button, Setup GUI checks whether the command corresponding to each modified parameter needs to be executed.

If command execution is necessary:

The command is executed and a corresponding configuration definition file is created or updated.

If the corresponding command is `drmclusinit`, `drmsqlinit`, or `drmtapeinit`, Setup GUI checks whether a corresponding configuration definition file exists, and what values are assigned to the parameters.

If a corresponding configuration definition file exists, the existing file is backed up in the following format (where the file name is followed by the date and time when you clicked the **Save** button):
file-name-yyyy-mm-dd-hh-mm-ss.extension

If a parameter value is invalid, Setup GUI prompts you to reenter the value.

If command execution is not necessary:

Setup GUI checks whether a corresponding configuration definition file exists.

If a configuration definition file corresponding to the parameter exists, the existing file is backed up in the following format (where the file name is followed by the date and time when you clicked the **Save** button). Then, the existing configuration definition file is updated with the modified parameter value:
file-name-yyyy-mm-dd-hh-mm-ss.extension

If a configuration definition file corresponding to the parameter does not exist, a new configuration definition file is created. If a directory for the configuration definition file does not exist, a new directory is also created.

If the configuration definition file corresponding to the parameter is not assigned a standard file name (or can be assigned any file name), a file selection dialog box is displayed, for you to specify a new file name.

If you have not modified any parameters in the window, this button is disabled.

Note: The backup destination directory for the existing configuration definition file is the `setup_bk` directory in the directory containing that file.

Undo

The modified parameter values are restored to their previous values.

If you have modified one or more parameter values in the window, and then click this button, a dialog box appears, asking whether you want to undo the modifications.

If you click the **Yes** button:

Setup GUI displays the previous parameter value, or the parameter value that was last saved by using the Save button or other means.

If you click the **No** button:

Nothing will be performed. The window display does not change.

If you have not modified a parameter value in the window, and then click this button, nothing is performed, and the window display does not change.

Cancel

If you have not modified a parameter value in the window, and then click this button, Setup GUI terminates.

If you have modified one or more parameter values in the window, and then click this button, a dialog box appears, asking whether you want to save the modified parameter values.

If you click the **Yes** button:

The modified parameter values are saved in the corresponding configuration files, and then Setup GUI terminates.

If you click the **No** button:

Setup GUI terminates, without saving the modified parameter values.

If you click the **Cancel** button:

Nothing will be performed. The window display does not change.

5.1.3 Prerequisite Conditions and Notes on Using Setup GUI

This section describes prerequisite conditions and notes on using Setup GUI.

5.1.3.1 Prerequisite Conditions

Before you can use Setup GUI, RAID Manager and the backup management product must be set up.

For details on how to do this, see the RAID Manager documentation. For details on how to set up the backup management product, see the documentation for the backup management product.

5.1.3.2 Notes

You must check that the current environment settings displayed in the Version Information window are supported by Protection Manager. The environment information displayed in the Version Information window includes the storage subsystem in use, RAID Manager, and VSS information (including the serial number, micro code, and version information).

If the correct RAID Manager installation path is not assigned to the `INSTALLPATH` parameter in the RAID Manager-linkage definition file (`DEFAULT.dat`), Setup GUI cannot display the storage subsystem information or the RAID Manager information. In the RAID Manager Linkage window, specify the correct RAID Manager installation path.

When you click the **Support Product Version** button in the Setup GUI window, the Version Information window is displayed.

In the Version Information window used to display the storage subsystem information, the microcode version of DKC is displayed as "*aa-bb-cc/ee*" instead of as "*aa-bb-cc-dd/ee*".

5.1.4 Setting up an Operating Environment for HPtM Using Setup GUI

When you use Setup GUI, we recommend the following window transition sequence. First, in the current Setup GUI window, set up the environment by specifying the setting for each displayed item, then click the **Save** button, and then click the **Next** or **Previous** button. This will move you to the next appropriate Setup GUI window in the environment setup flow. Alternatively, you can specify an item setting by directly selecting the relevant tab.

To follow Setup GUI window transition, first select the **Configuration Settings** tab, and then, in the Configuration Settings window, specify items to be backed up. When you click the **Next** button, the next window that you need to set up is displayed, depending on the settings that you have made in the Configuration Settings window. In the displayed tab window, specify the settings for the items in the window and then click the **Next** button. The next required window will be displayed.

In this way, you can specify almost all the settings that are required for Protection Manager operation simply by clicking the **Next** button repeatedly, until you reach a window with an inactive **Next** button. To confirm or modify the settings that you have made in the previous window, click the **Previous** button.

Note: When you click the **Save** button in a tab window, the command corresponding to the parameter that you have specified in the window is executed, and the settings are written into the corresponding configuration file. If you click the **Next** or **Previous** button, or select another tab without clicking the **Save** button in the current window, a confirmation dialog box appears, asking whether you want to save any changes to settings you have made in the current window. If you click the **Yes** button, your settings are saved, and then the next or previous window is displayed. If you click the **No** button, the next or previous window is displayed, without saving changes you have made to item settings. If you click the **Cancel** button, the current window will remain.

Depending on the type of the server that manages the backup target, the objects to be backed up, and whether the system is in a cluster configuration, the environment setup flow navigated by using Setup GUI varies.

With Setup GUI, there are two main types of environment setup flow:

- Environment setup flow for a file server or database server
- Environment setup flow for a backup server

These two types of environment setup flow are explained below.

5.1.4.1 Environment Setup Flow for a File Server or Database Server

Figure 5.2 shows the environment setup flow for a file server or database server.

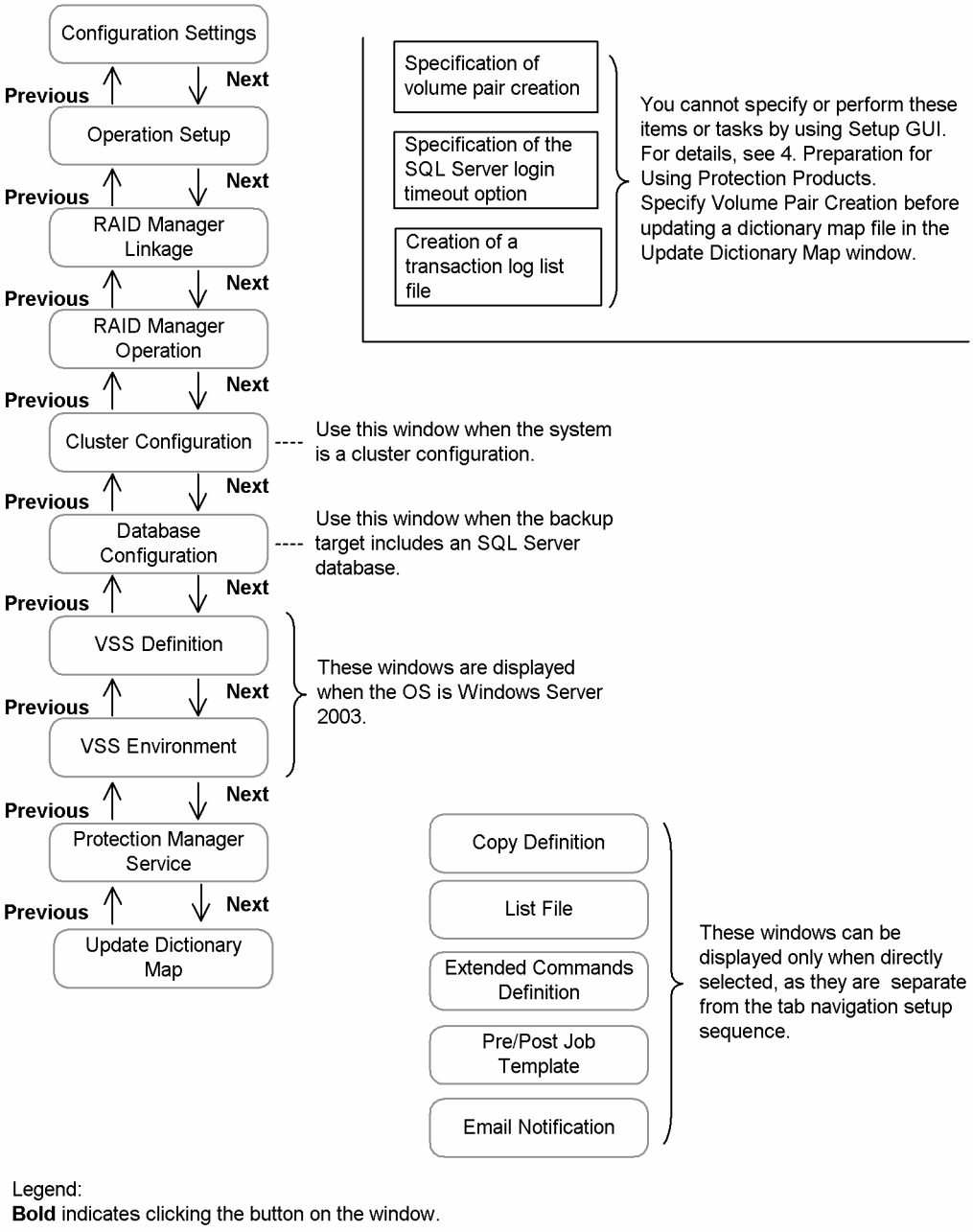


Figure 5.2 Environment Setup Flow for a File Server or Database Server

5.1.4.2 Environment Setup Flow for a Backup Server

Figure 5.3 shows the environment setup flow for a backup server.

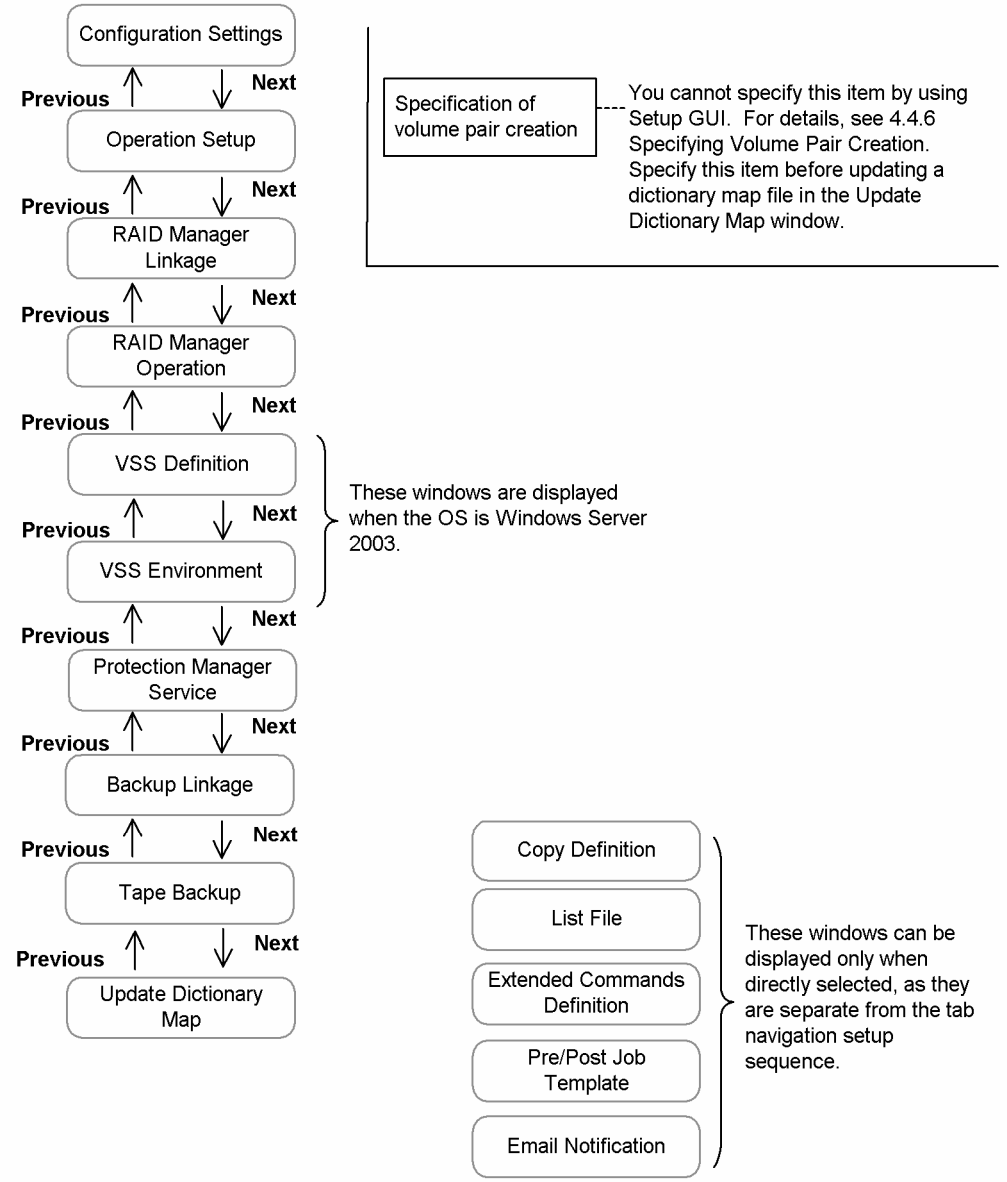


Figure 5.3 Environment Setup Flow for a Backup Server

5.2 Setup GUI Windows

There are two types of setup GUI windows:

- Windows that are displayed in the setup sequence as navigated by Setup GUI. These Setup GUI windows include the **Next** and **Previous** buttons. Based on the settings you specified in the Configuration Settings window, click these buttons to navigate from window to window in the setup sequence determined by Setup GUI.
- Windows that are displayed through direct tab selection. These Setup GUI windows are displayed when you directly select a tab. The windows are separate from those displayed in a tab navigation setup sequence.

The remaining sections of this manual describe each window in detail, focusing on the relationship between the settings specified in the window and the Protection Manager environment setup parameters. For further information on the settings specified in each window, see the *Reference* column in the table that lists the items displayed in the window.

If a configuration file already exists for a window that is displayed, and a parameter value in the file can be used for Protection Manager, that parameter value is displayed as a setting value in the window. If no such configuration file exists, the field for the setting in the window displays the default value or is blank.

5.2.1 Configuration Settings Window

The Configuration Settings window is the window that is used first in the Setup GUI navigated environment setup flow (tab navigation). Use this window to specify configuration settings required for Protection Manager operation. Figure 5.4Configuration Settings Window.

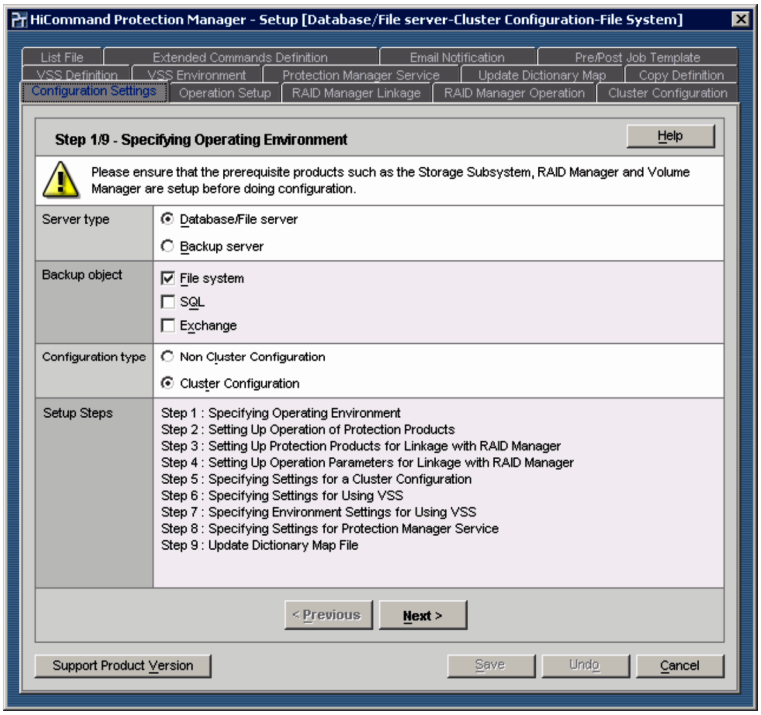


Figure 5.4 Configuration Settings Window

Table 5.3 lists items in the Configuration Settings Window.

Table 5.3 Configuration Settings Window Items

Item	Environment setup parameter or description	Default value	Reference
Server type	Specifies the server type (required).	`Database/File server`	Not applicable
Backup object	Specifies the backup target object(s) (required).	`File system`	
Configuration type	Specifies whether the system is in a cluster configuration (required).	`Non Cluster Configuration`	
Setup Steps	Displays the setup steps in Setup GUI.	Depending on the combination of the selected settings, the steps displayed and their sequence vary.	

The items specified in this window are not associated with any Protection Manager environment setup parameter. Note that the settings you specify in this window determine the number of tabs that will be displayed on the tab view bar, the setup procedure, and the items that will be displayed in each setup window.

5.2.2 Operation Setup Window

Use the Operation Setup window to specify settings related to Protection Manager operation and specify a directory where a dictionary map file is to be created. The settings you specify here will be reflected in the Protection Products configuration definition file (`init.conf`). A dictionary map file will be created at the specified location.

Settings are needed for file servers, database servers, and backup servers.

Although a dictionary map file is automatically created during installation, you must create a separate dictionary map file if:

- The system is in a cluster configuration, or
- You want to create a dictionary map file in a user-specified directory and use it there.

Depending on the value you have specified for **Configuration type** in the Configuration Settings window, the information displayed in the Operation Setup window varies.

5.2.2.1 If You Selected Non Cluster Configuration as the Configuration Type

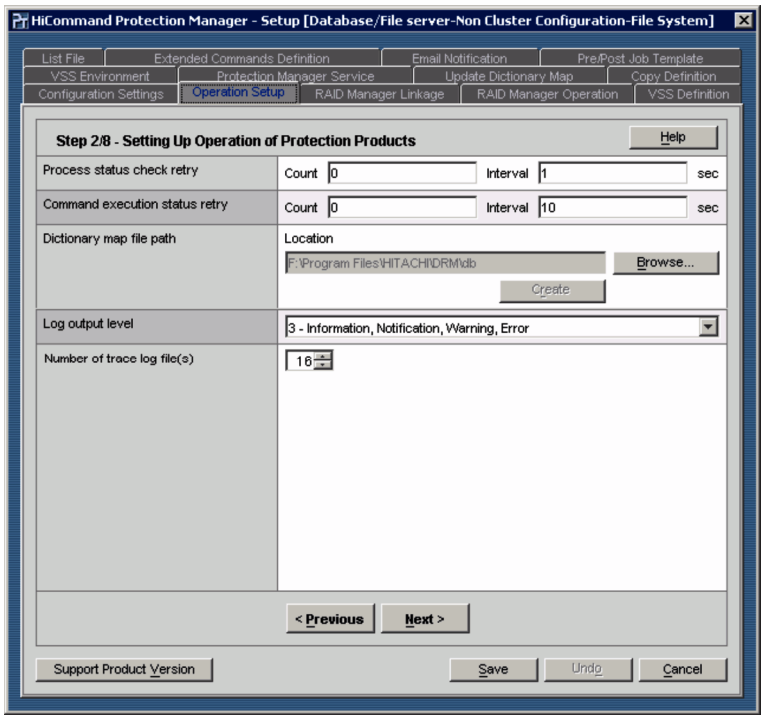


Figure 5.5 Operation Setup Window (for Non Cluster Configuration)

Table 5.4 Operation Setup Window Items (for Non Cluster Configuration)

Item		Environment setup parameter or description
Process status check retry	Count	SVC_RETRY_TIME
	Interval	SVC_RETRY_WAIT
Command execution status retry	Count	COM_RETRY_TIME
	Interval	COM_RETRY_WAIT
Dictionary map file path	Location	DRM_DB_PATH
Log output level		LOGLEVEL
Number of trace log file(s)		PP_LOGFILE_NUM

5.2.2.2 If You Selected Cluster Configuration as the Configuration Type

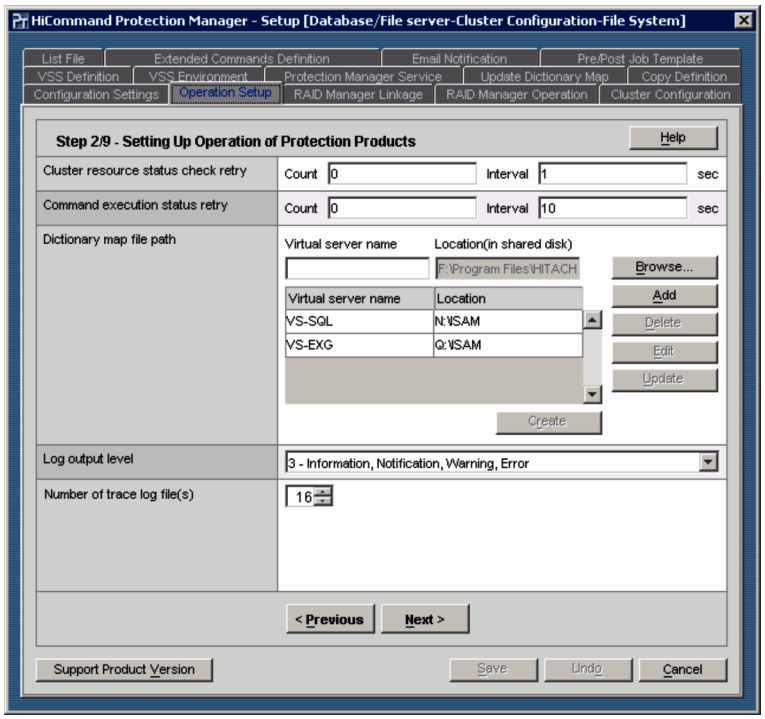


Figure 5.6 Operation Setup Window (for Cluster Configuration)

Table 5.5 Operation Setup Window Items (for Cluster Configuration)

Item		Environment setup parameter or description	HPtM User's Guide Reference
Cluster resource status check retry	**Count**	CLU_RETRY_TIME	Section 4.3
	Interval	CLU_RETRY_WAIT	
Command execution status retry	**Count**	COM_RETRY_TIME	Section 4.3
	Interval	COM_RETRY_WAIT	
Dictionary map file path	**Virtual server name**	DRM_DB_PATH	Section 4.5
	Location(in shared disk)		
Log output level		LOGLEVEL	Section 10.5
Number of trace log file(s)		PP_LOGFILE_NUM	Section 10.5

5.2.3 RAID Manager Linkage Window

Use the RAID Manager Linkage window to specify or update the following items that are required for linkage with RAID Manager. The settings that you specify here will be reflected in the RAID Manager-linkage definition file (DEFAULT.dat).

- RAID Manager instance number
- Data copy track size
- Setting for dynamic secondary volume recognition
- Setting of the operation mode assumed for automatic copy group selection
- RAID Manager installation path
- Whether the pair status is to be changed to PSUS if an error occurs during backup processing

Settings are needed for file servers, database servers, and backup servers.

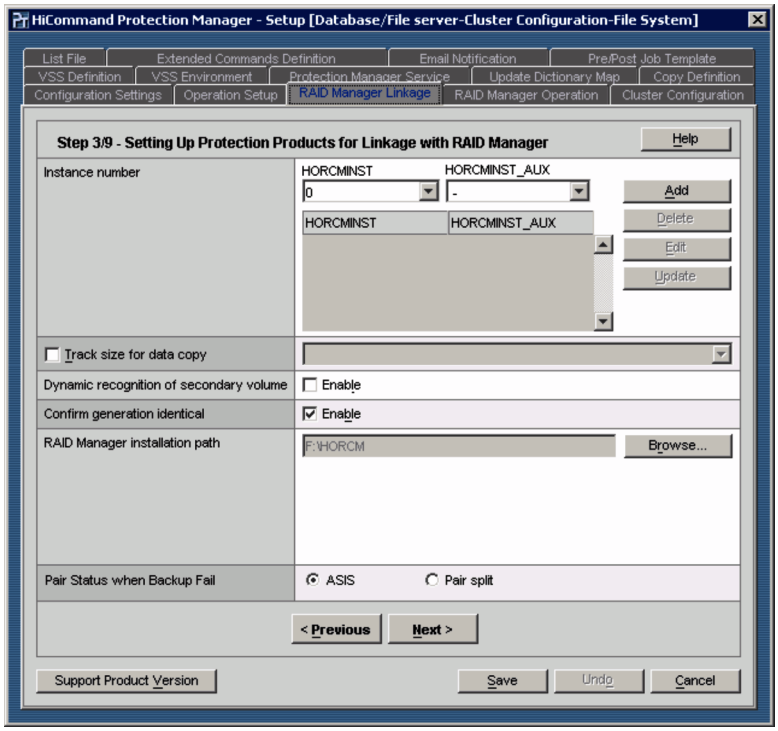


Figure 5.7 RAID Manager Linkage Window

Table 5.6 RAID Manager Linkage Window Items

Item		Environment setup parameter or description	HPtM User's Guide Reference
Instance number	**HORCMINST**	HORCMINST	Section 4.4
	HORCMINST_AUX	HORCMINST_AUX	
Track size for data copy		COPY_SIZE	Section 4.4
Dynamic recognition of secondary volume		DEVICE_DETACH	Section 4.4
Confirm generation identical		CONFIRM_GENERATION_IDENTICAL	Section 4.4
RAID Manager installation path		INSTALLPATH	Section 4.4
Pair Status when Backup Fail		RECOVERY_MODE_ON_BACKUP_ABORTING	Section 4.4

5.2.4 RAID Manager Operation Window

Use the RAID Manager Operation window to specify or update the following items that are required for linkage with RAID Manager. The settings that you specify here will be reflected in the RAID Manager-linkage definition file (`DEFAULT.dat`).

- The retry count and the retry interval for checking Protection Manager's volume pair status
- The retry count and the retry interval for checking Protection Manager's pair status, according to the purpose (`Resync` (pair resynchronization), `Split` (pair split), or `Restore` (resynchronization during restoration)

- The retry count and the retry interval for checking Protection Manager's RAID Manager command busy status

Settings are needed for file servers, database servers, and backup servers.

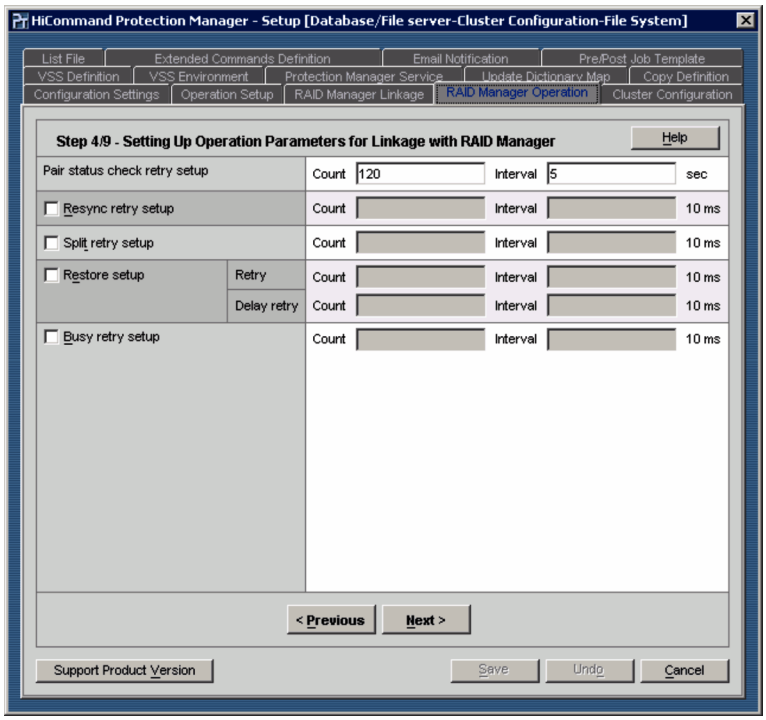


Figure 5.8 RAID Manager Operation Window

Table 5.7 RAID Manager Operation Window Items

Item			Environment setup parameter or description	HPtM User's Guide Reference
Pair status check retry setup		**Count**	RETRY_TIME	Section 4.4
		Interval	RETRY_WAIT	
Resync retry setup		**Count**	RESYNC_RETRY_TIME	
		Interval	RESYNC_RETRY_WAIT	
Split retry setup		**Count**	SPLIT_RETRY_TIME	
		Interval	SPLIT_RETRY_WAIT	
Restore setup	**Retry**	**Count**	RESTORE_RETRY_TIME	
		Interval	RESTORE_RETRY_WAIT	
	Delay retry	**Count**	RESTORE_DELAY_RETRY_TIME	
		Interval	RESTORE_DELAY_RETRY_WAIT	
Busy retry setup		**Count**	BUSY_RETRY_TIME	Section 4.4

Item		Environment setup parameter or description	HPtM User's Guide Reference
	Interval	BUSY_RETRY_WAIT	

5.2.5 Cluster ConfigurationWindow

Use the Cluster Configuration window to specify the settings that are required in a cluster environment. The settings you specify here will be reflected in a way that depends on the cluster product in use, as explained below.

If VERITAS Cluster Server (VCS) is used, your settings will be reflected in the cluster information configuration definition files (`VCS.dat` and `DEFAULT.dat`).

If Microsoft Cluster Service (MSCS) is used, your settings will be reflected in the Protection Products configuration definition file (`init.conf`) as the settings that specify whether restoration is to be performed while the cluster resources that monitor the DBMS remain in the online state or after they are placed in the offline state.

Settings are needed for file servers, database servers. Depending on the cluster product that you select in the window, the information displayed in the Cluster Configuration window varies.

5.2.5.1 If You Selected VERITAS Cluster Server (VCS)

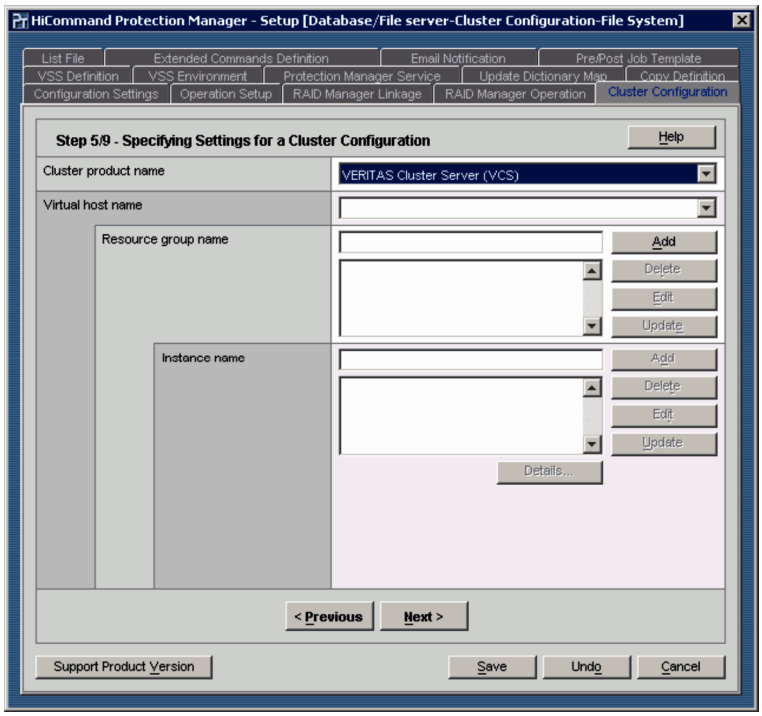


Figure 5.9 Cluster Configuration Window (for VERITAS Cluster Server (VCS))

Table 5.8 Cluster Configuration Window Items (for VERITAS Cluster Server (VCS))

Item	Environment setup parameter or description	HPtM User's Guide Reference
Cluster product name	Cluster product name	Section 4.6
Virtual host name	Virtual server name	
Resource group name	Resource group name	
Instance name	Name of the backup target instance or application	

When you select one of the instance or application names displayed in the **Instance name** area and then click the **Details** button, the Instance Details dialog box appears. The Instance Details dialog box is explained below.

Instance Details dialog box

If the cluster product is VERITAS Cluster Server, use the Instance Details dialog box allows you to specify details of the backup target (instance or application) that you have specified in the Cluster Configuration window.

The settings you specify here will be reflected in the cluster information configuration definition file (`VCS.dat`).

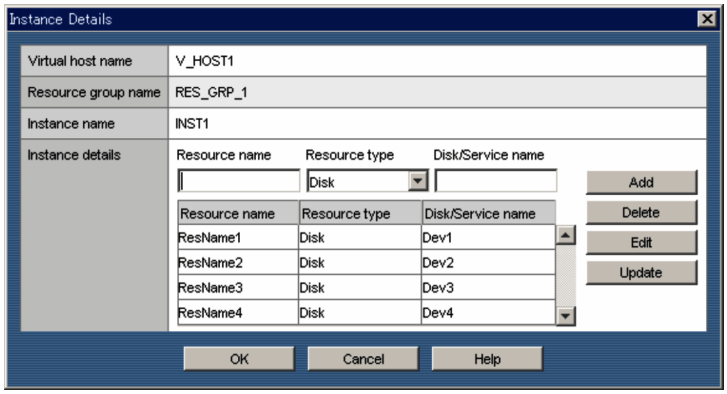


Figure 5.10 Instance Details Dialog Box

Table 5.9 Instance Details Dialog Box Items

Item		Environment setup parameter or description	HPtM User's Guide Reference
Virtual host name		Virtual server name specified in the Cluster Configuration window	Section 4.6
Resource group name		Resource group name specified in the Cluster Configuration window	
Instance name		Backup target instance name or application name specified in the Cluster Configuration window	
Instance details	**Resource name**	Disk resource name	
	Resource type	Resource type	
	Disk/Service name	Information associated with the disk resource	

5.2.5.2 If You Selected Microsoft Cluster Service (MSCS)

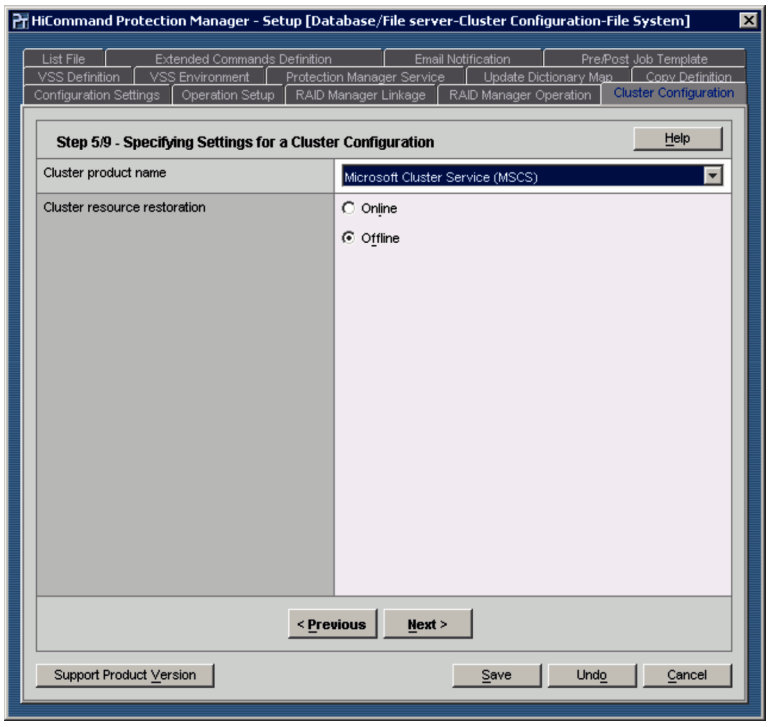


Figure 5.11 Cluster Configuration Window (for Microsoft Cluster Service (MSCS))

Table 5.10 Cluster Configuration Window Items (for Microsoft Cluster Service (MSCS))

Item	Environment setup parameter or description	HPtM User's Guide Reference
Cluster product name	Cluster product name	Not applicable
Cluster resource restoration*	CLU_MSCS_RESTORE	Section 4.3
*This item is displayed only when the OS is Windows Server 2003 SP1.		

5.2.6 Database Configuration Window

When the backup is of a SQL Server database, use the Database Configuration window to register the following required information into the database configuration definition file (*instance-name*.dat). In the window you can also specify the options for the backup, dictionary map synchronization, and recovery.

- VDI (Virtual Device Interface) metafile storage directory
- VDI generation timeout
- UNDO log file storage directory
- Transaction log backup file storage directory

The settings for backup, dictionary map synchronization, and recovery are reflected in the Protection Products configuration definition file (init.conf).

Settings are needed for file servers, database servers.

Note: When the backup is of a SQL Server database, the command may terminate with an error due to a SQL Server login request timeout (error message: KAVX1008-E, detailed message DRM-11013, Code: 0), or with an error because the automatic recovery processing at SQL Server startup is not complete (error message: KAVX1008-E, detailed message DRM-11011, Code: 5180). In this case, specify the SQL Server login timeout option, or the SQL Server automatic recovery time. Note that you cannot use Setup GUI to specify these options. For details on how to do this, see the *HPtM User's Guide*.

The information displayed in the Database Configuration window varies depending on the value you have specified for **Configuration type** in the Configuration Settings window.

5.2.6.1 If You Selected Non Cluster Configuration as the Configuration Type

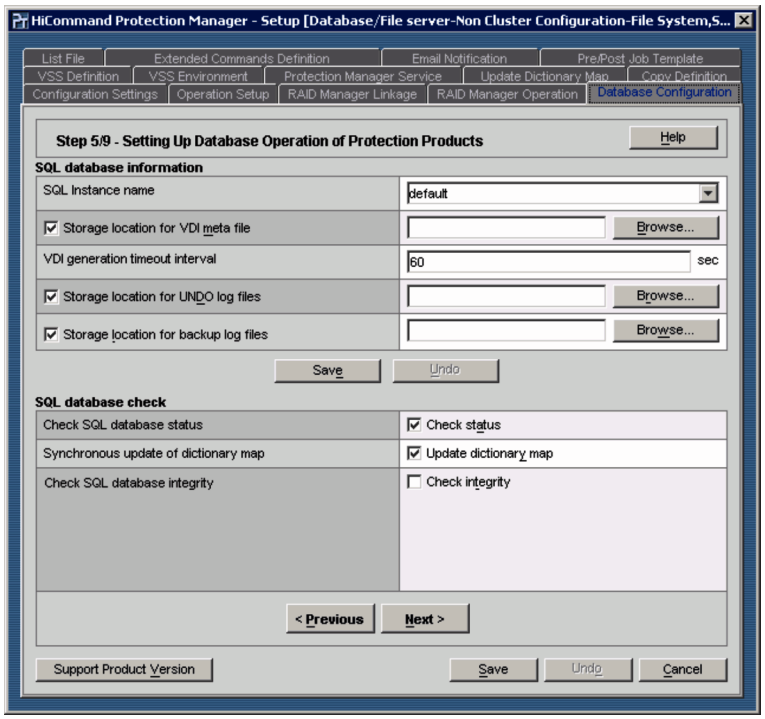


Figure 5.12 Database Configuration Window (for Non Cluster Configuration)

Table 5.11 Database Configuration Window Items (for Non Cluster Configuration)

Item	Environment setup parameter or description	HPtM User's Guide Reference
SQL Instance name	SQL Server instance name	Section 4.7
Storage location for VDI meta file*	VDI (Virtual Device Interface) metafile storage directory	
VDI generation timeout interval	VDI generation timeout	
Storage location for UNDO log files*	UNDO log file storage directory	
Storage location for backup log files*	Transaction log backup file storage directory	
Check SQL database status	`SQL_QUICK_BACKUP`	Section 4.3
Synchronous update of dictionary map	`DRM_DB_SYNC`	Section 4.3
Check SQL database integrity	`SQL_CHECKDB`	Section 4.3
*In a cluster environment, a character string `(in shareddisk)` is appended.		

5.2.6.2 If You Selected Cluster Configuration as the Configuration Type

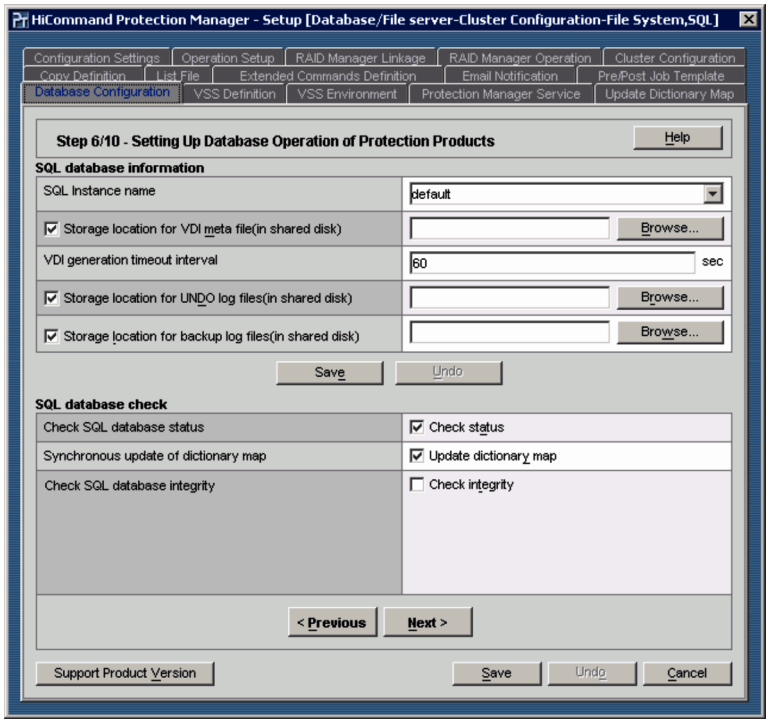


Figure 5.13 Database Configuration Window (for Cluster Configuration)

For information about the relationship between the items in this window and the environment setup parameters, see Table 5.11. In a cluster environment, you must assign a shared disk directory that can be read from both the active and standby servers to **Storage location for VDI meta file (in shared disk)**, **Storage location for UNDO log files (in shared disk)**, and **Storage location for backup log files (in shared disk)**.

5.2.7 VSS Definition Window

Use the VSS Definition window to specify VSS definition file information, as this is part of the information that is required for VSS-based online backup when the backup is of a file system or an Exchange database. The settings that you specify in the window will be reflected in the following file:

VSS definition file (`vsscom.conf`).

You can also create or update your own VSS definition file. Your own VSS definition file is stored in the following location: *Protection-Manager-installation-directory*`\conf\vss`.

Settings are needed for file servers and database servers.

For details on other settings required for VSS-based online backup, see the *HPtM User's Guide*.

Note: This window is supported for Windows Server 2003 only.

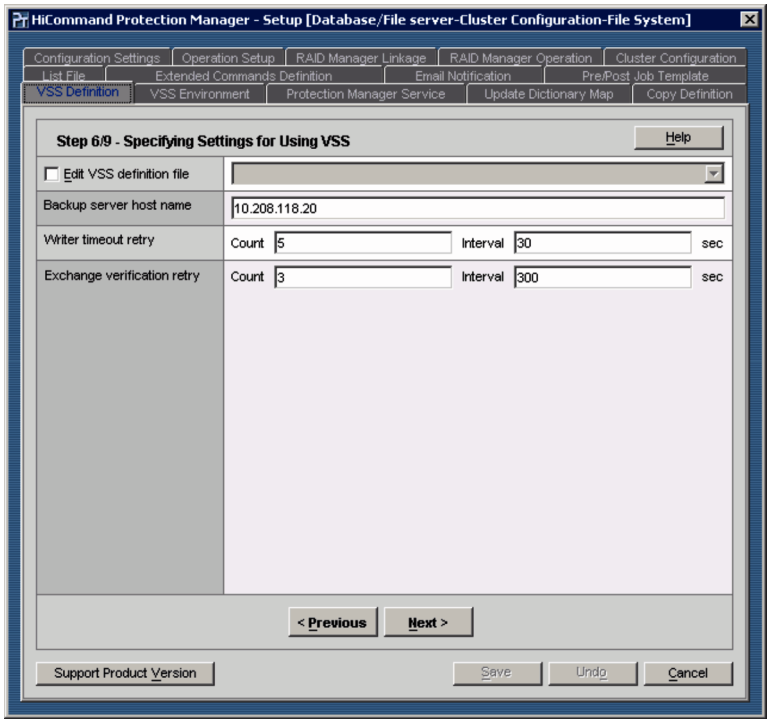


Figure 5.14 VSS Definition Window

Table 5.12 VSS Definition Window Items

Item		Environment setup parameter or description	HPtM User's Guide Reference
Edit VSS definition file		Editing of your own VSS definition file	Not applicable
Backup server host name		BACKUP_SERVER	Section 4.9
Writer timeout retry	**Count**	WRITER_TIMEOUT_RETRY_COUNT	
	Interval	WRITER_TIMEOUT_RETRY_INTERVAL	
Exchange verification retry	**Count**	EXG_VERIFY_RETRY_COUNT	
	Interval	EXG_VERIFY_RETRY_INTERVAL	

5.2.8 VSS Environment Window

The VSS Environment window allows you to specify system environment variables required for the use of VSS. Settings are needed for file servers, database servers, and backup servers. Depending on the value you have specified for **Server type** in the Configuration Settings window, the information displayed in the VSS Environment window varies.

Notes: If you have specified a system environment variable, after Setup GUI is closed, always restart the OS.

Note: This window is supported for Windows Server 2003 only.

5.2.8.1 If You Selected Database/File Server as the Server Type

Specify system environment variables for the file server or database server.

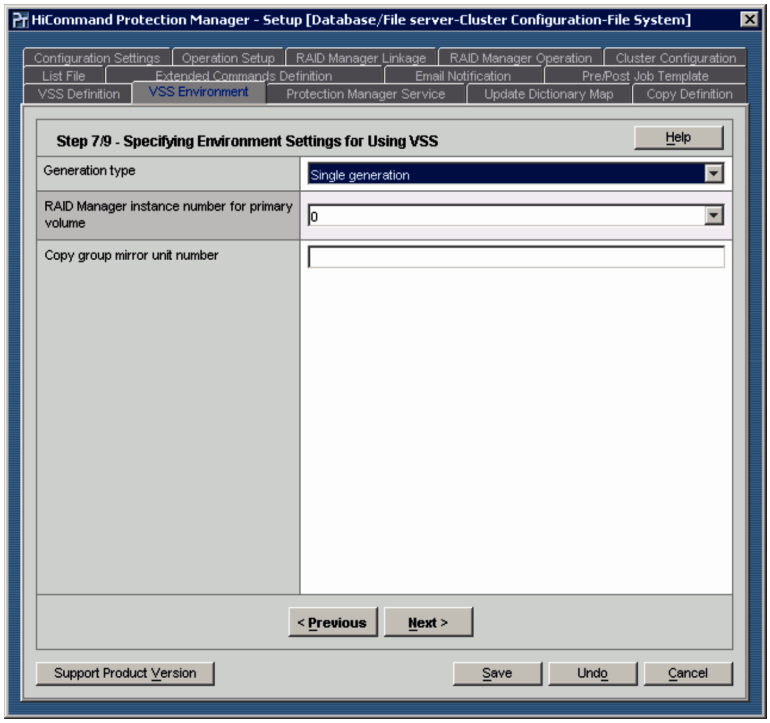


Figure 5.15 VSS Environment Window (for Database/File Server)

Table 5.13 VSS Environment Window Items (for Database/File Server)

Item	Environment variable or description
Generation type	Backup generation type (**Multiple Generation** or **Single Generation**)
RAID Manager instance number for primary volume*	VSHTCHORCMINST_LOCAL
Copy group mirror unit number*	VSHTCHOMRCF_MUN

*This item will not be displayed if you have selected **Multiple Generation** as the **Generation type**.

5.2.8.2 If You Selected Backup Server as the Server Type

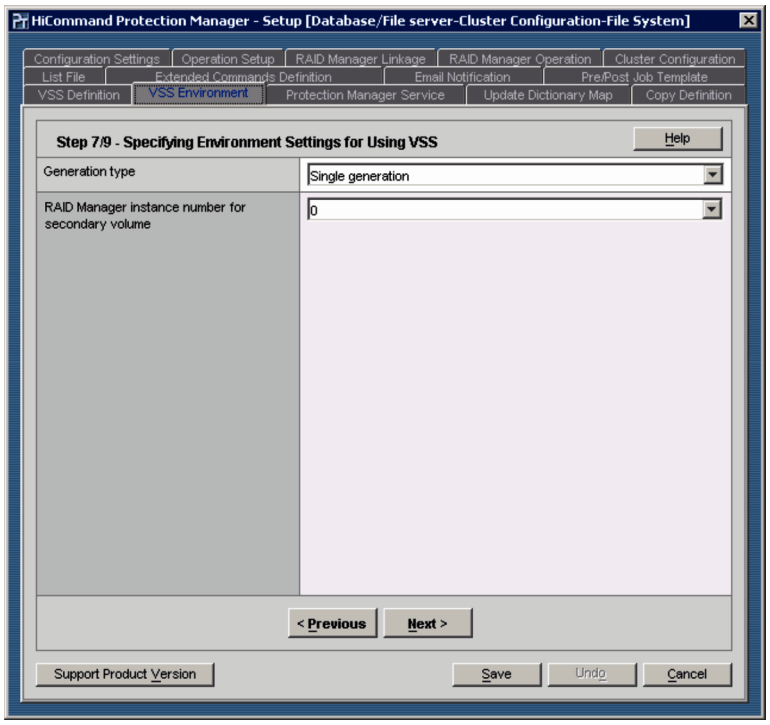


Figure 5.16 VSS Environment Window (for Backup Server)

Table 5.14 VSS Environment Window Items (for Backup Server)

Item	Environment variable or description
Generation type	Backup generation type (**Multiple Generation** or **Single Generation**)
RAID Manager instance number for secondary volume	VSHTCHORCMINST_REMOTE

5.2.9 Protection Manager Service Window

Use the Protection Manager Service window to specify the TCP port number used by the Protection Manager service. The settings you specify here will be reflected in the Windows services file. The TCP port number setting on the file server or database server must be the same as that on the backup server.

Figure 5.17 Protection Manager Service Window

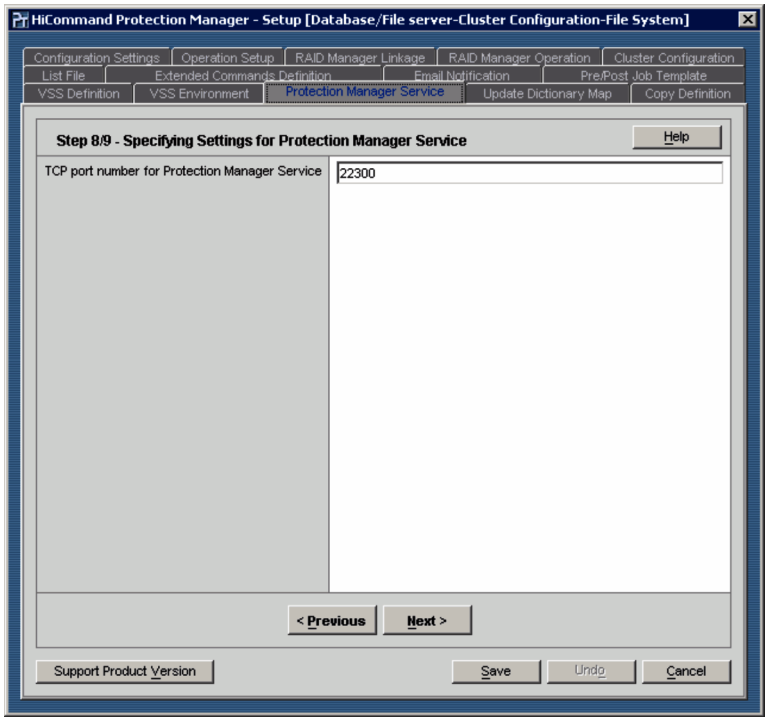


Table 5.15 Protection Manager Service Window Items

Item	Environment variable or description	HPtM User's Guide Reference
TCP port number for Protection Manager Service	`TCP port number to be used by the Protection Manager service (Default value: 22300)`	Section 4.9

5.2.10 Update Dictionary Map Window

The Update Dictionary Map window allows you to update the dictionary map file if:

- You want to check that the environment has been correctly set up.
- You need to update the dictionary map file after operation has started.

Settings are needed for file servers, database servers, and backup servers.

If you are in a cluster environment, you must update the dictionary map file only on the active server. You do not need to update the file on the standby server by switching the cluster to update on the both servers.

Usually, you do not need to update the dictionary map file on the backup server. However, if a primary volume exists in the backup server, the dictionary map file must be updated.

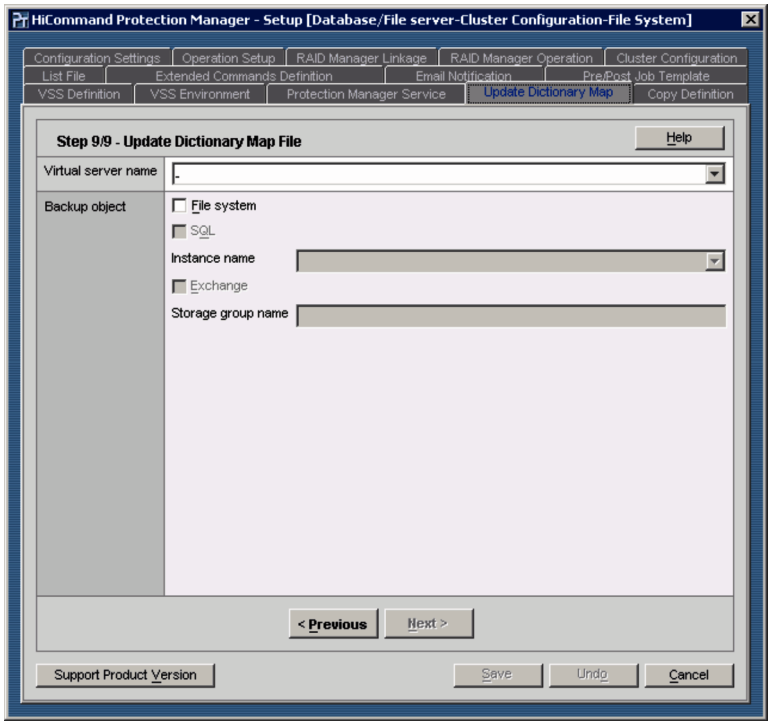


Figure 5.18 Update Dictionary Map Window

Table 5.16 Update Dictionary Map Window Items

Item			Environment setup parameter or description
Virtual server name[1]			Virtual server name
Backup object	**File system**[2]		File system
	SQL[2]		SQL Server database
		Instance name	Registered SQL instance name. If this item is specified, only the information about the specified instance will be updated.
	Exchange[2]		Exchange database
		Storage group name	Storage group name. If this item is specified, only the information on the specified storage group will be updated.

[1]This item is only available when you have selected **Cluster Configuration** as the **Configuration type** in the Configuration Settings window.

[2]When you update the dictionary map file, only the information on the backup object that you specified in the Configuration Settings window is updated.

Depending on the specified backup object, one of the following commands is executed. After command execution is complete, check the file date or other information to make sure that the dictionary map file has been updated.

- When the backup is of a file system:

```
drmfsdisplay -refresh
```

- When the backup is of a SQL Server database:

```
drmsqldisplay -refresh or
drmsqldisplay instance-name -refresh -coremap
```

- When the backup is of an Exchange database:

```
drmsqldisplay -refresh or
drmexgdisplay storage-group-name -refresh -coremap
```

5.2.11 Backup Linkage Window

The Backup Linkage window allows you to specify the information that is required for linkage with the backup management product. The settings that you specify here will be reflected in the configuration definition file for linkage with the backup management product (`DEFAULT.dat`). Settings are needed for backup servers.

Before specifying settings in this window, you must specify the medium protection period with the backup management product.

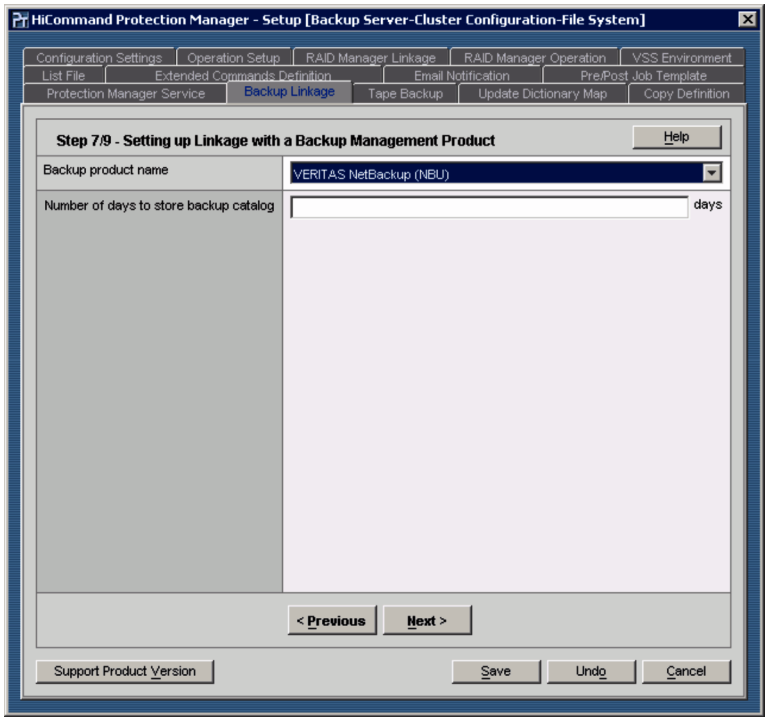


Figure 5.19 Backup Linkage Window

Table 5.17 Backup Linkage Window Items

Item	Environment setup parameter or description	HPtM User's Guide Reference
Backup product name	Backup management product name	Section 4.10
Number of days to store backup catalog	Number of days to store the backup catalog for tape backup	

5.2.12 Tape Backup Window

The Tape Backup window allows you to specify the information required for linkage with the backup management product. The settings you specify here will be reflected in the tape backup configuration definition file (`NBU.dat` or `BEWS.dat`). Settings are needed for backup servers.

Before specifying settings in this window, you must perform the following tasks for the backup management product that is in use:

If the backup management product is VERITAS NetBackup:

- Create as many CLASS or POLICY definitions as the number of backup operations that are to be performed concurrently.
- Specify a SCHEDULE value for each of the POLICY (CLASS) definitions that you have created.

If the backup management product is VERITAS Backup Exec:

Specify the media, device, and logon information.

Note that, depending on the backup management product that you select in this window, the information displayed in the Tape Backup window varies.

5.2.12.1 If You Selected VERITAS NetBackup (NBU)

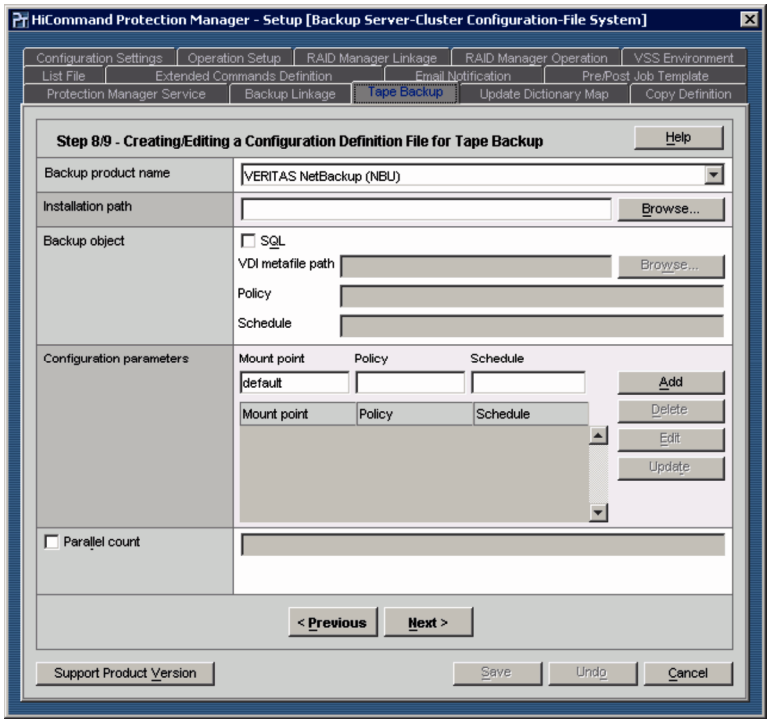


Figure 5.20 Tape Backup Window (for VERITAS NetBackup (NBU))

Table 5.18 Tape Backup Window Items (for VERITAS NetBackup (NBU))

Item		Environment setup parameter or description	HPtM User's Guide Reference
Backup product name		Backup management product name	Not applicable
Installation path		INST_PATH	Section 4.10
Backup object	**SQL**	SQL Server database	
	VDI meta file path	VDI metafile storage directory	
	Policy	POLICY	
	Schedule	SCHEDULE	
Configuration parameters	**Mount point**	MOUNT_POINT	
	Policy	POLICY	
	Schedule	SCHEDULE	
Parallel count		PARALLEL_COUNT	

5.2.12.2 If You Selected VERITAS Backup Exec (BEWS)

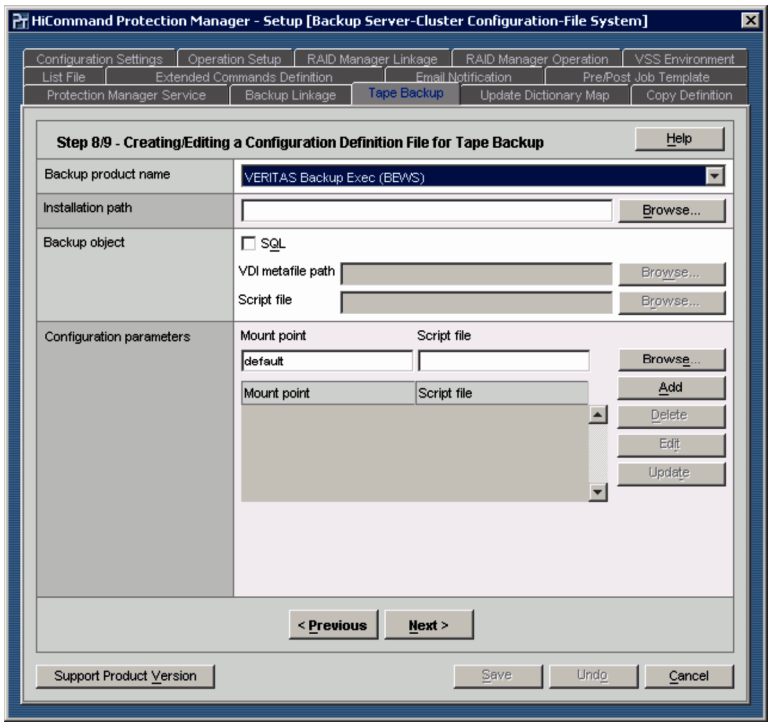


Figure 5.21 Tape Backup Window (for VERITAS Backup Exec (BEWS))

Table 5.19 Tape Backup Window Items (for VERITAS Backup Exec (BEWS))

Item		Environment setup parameter or description	HPtM User's Guide Reference
Backup product name		Backup management product name	Not applicable
Installation path		`INST_PATH`	Section 4.10
Backup object	**SQL**	SQL Server database	
	VDI meta file path	VDI metafile storage directory	
	Script file	`SCRIPT_FILE`	
Configuration parameters	**Mount point**	`MOUNT_POINT`	
	Script file	`SCRIPT_FILE`	

5.2.13 Copy Definition Window

The Copy Definition window is used to create or update the copy parameter definition file (which can be assigned any file name).

You can specify the parameters corresponding to the following items in the copy parameter definition file.

- The retry count and the retry interval for checking Protection Manager's volume pair status
- The retry count and the retry interval for checking Protection Manager's pair status, depending on the purpose `Resync` (pair resynchronization), `Split` (pair split), or `Restore` (resynchronization during restoration).

When executing a backup, restore, or resynchronization command, you can use parameter values that are appropriate for your purpose and CPU load status by specifying the copy parameter definition file as an argument. During command execution, the values in the copy parameter definition file take precedence over the values in the RAID Manager-linkage definition file (`DEFAULT.dat`).

The settings in this window are required on the file server, database server, and backup server for which you want to change the retry count and retry interval to check the pair status, depending on the purpose and CPU load status.

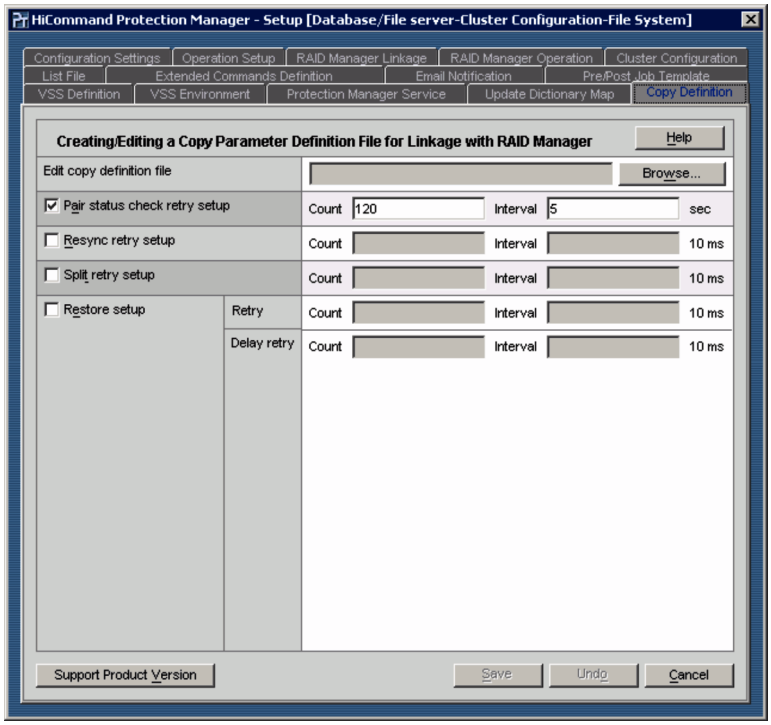


Figure 5.22 Copy Definition Window

Table 5.20 Copy Definition Window Items

Item			Environment setup parameter or description	HPtM User's Guide Reference
Edit copy definition file			Editing of your own existing copy parameter definition file	Section 4.4
Pair status check retry setup		**Count**	RETRY_TIME	
		Interval	RETRY_WAIT	
Resync retry setup		**Count**	RESYNC_RETRY_TIME	
		Interval	RESYNC_RETRY_WAIT	
Split retry setup		**Count**	SPLIT_RETRY_TIME	
		Interval	SPLIT_RETRY_WAIT	
Restore setup	**Retry**	**Count**	RESTORE_RETRY_TIME	
		Interval	RESTORE_RETRY_WAIT	
	Delay retry	**Count**	RESTORE_DELAY_RETRY_TIME	
		Interval	RESTORE_DELAY_RETRY_WAIT	

5.2.14 List File Window

The List File window allows you to create or update the following target definition files (which can be assigned any file name):

- Copy-group list file
- Database or mount point directory list file

You can specify these target definition files as command arguments when you want to back up or restore multiple files, databases, or copy groups in a batch.

The settings in this window are required on the file server, database server, and backup server for multiple files, databases, copy groups, or other entities in which you want to back up or restore in a batch.

Notes: You cannot use Setup GUI to create or update the transaction log list file. For details on how to create a transaction log list file, see the *HPtM User's Guide*.

Depending on the target definition file type that you select in this window, the information displayed in the List File window varies.

5.2.14.1 If You Selected Copy-Group List

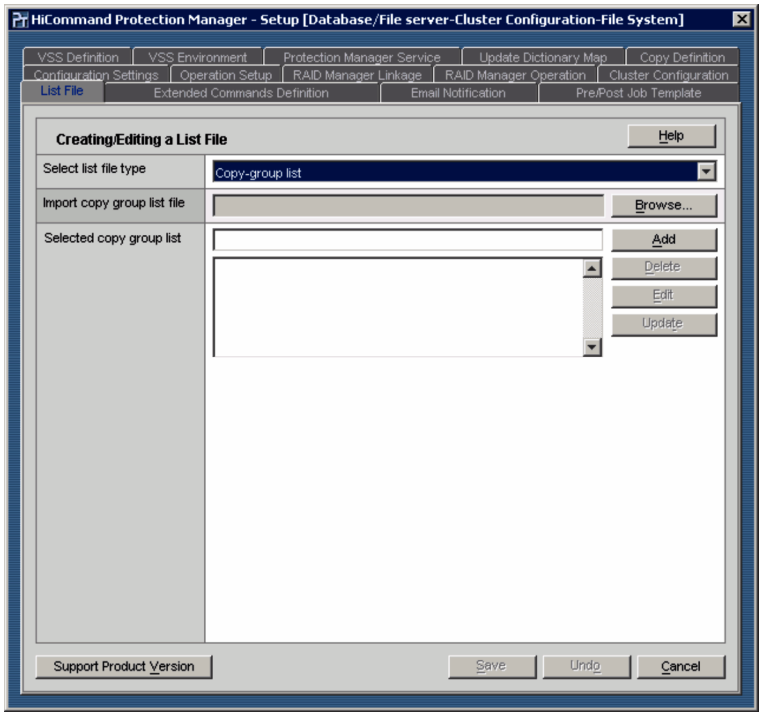


Figure 5.23 List File Window (for Copy-Group List)

Table 5.21 List File Window Items (for Copy-Group List)

Item	Environment setup parameter or description	HPtM User's Guide Reference
Select list file type	Target definition file type	Section 4.11
Import copy group list file	Path to the existing copy-group list file	
Selected copy group list	A list of the defined copy groups	

5.2.14.2 If You Selected Database or Mount Point Directory List

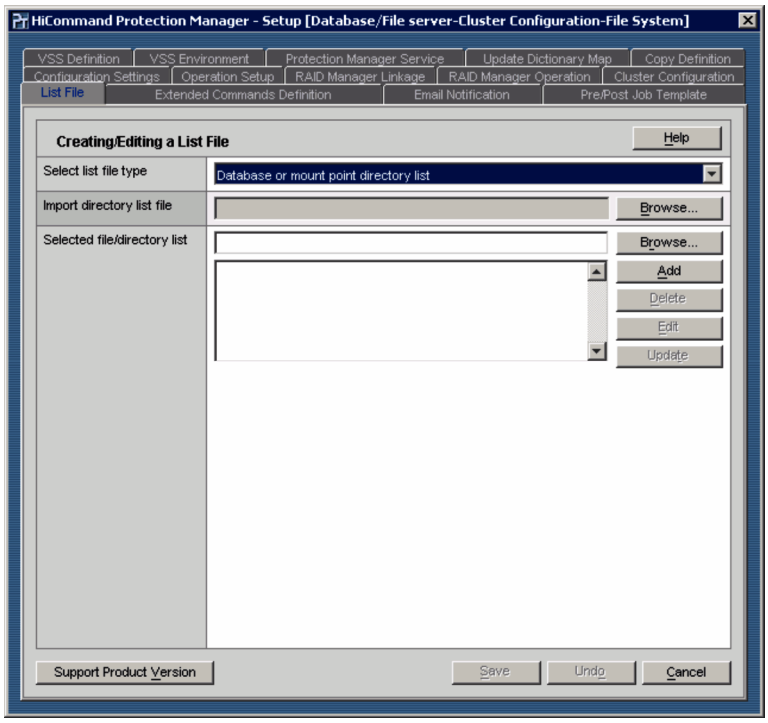


Figure 5.24 List File Window (for Database or Mount Point Directory List)

Table 5.22 List File Window Items (for Database or Mount Point Directory List)

Item	Environment setup parameter or description	HPtM User's Guide Reference
Select list file type	Target definition file type	Section 4.11
Import directory list file	Path to the existing database or mount point directory list file	
Selected file/directory list	A list of the defined file names, directory names, SQL Server database names, storage group names, and other items	

5.2.15 Extended Commands Definition Window

Use the Extended Commands Definition window to create or update the operation definition file (*_operation-ID*`.dat`) and the host environment settings file (`host.dat`) as they are required to execute Protection Manager extended commands.

When you want to execute Protection Manager extended commands, the settings in this window are required on the file server, database server, and backup server. Note that, depending on the backup target and on whether you are in a cluster environment, the server on which the operation definition file is to be located varies. For further information, see the explanation about the location of the operation definition file provided in chapter 4 of the *HPtM User's Guide*.

You must also perform other preparatory steps before executing extended commands, such as creation of the operation IDs to be used as the operation definition file names. ***Note***: After each file is created, either of the following check tools is automatically executed, depending on the backup target and server type.

Note: After each file is created, either of the following check tools is automatically executed, depending on the backup target and server type.

- Operation definition file check tool

  `EX_DRM_FS_DEF_CHECK`, `EX_DRM_SQL_DEF_CHECK` or `EX_DRM_EXG_DEF_CHECK`

- Host environment settings file check tool

  `EX_DRM_HOST_DEF_CHECK`

Depending on the value that you have specified for **Configuration type** in the Configuration Settings window, the information displayed in the Extended Commands Definition window varies.

5.2.15.1 If You Selected Non Cluster Configuration as the Configuration type

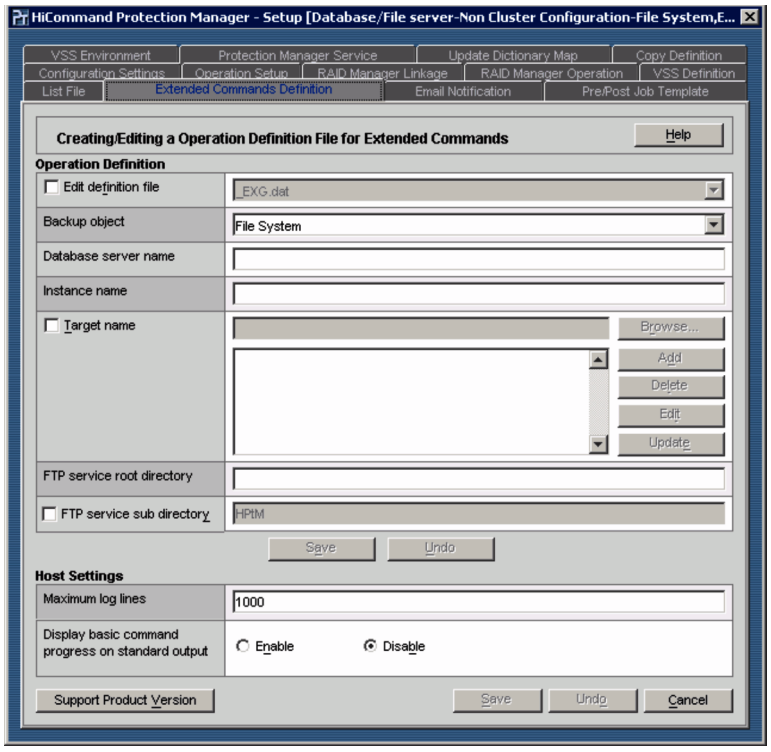


Figure 5.25 Extended Commands Definition Window (for Non Cluster Configuration)

Table 5.23 Extended Commands Definition Window Items (for Non Cluster Configuration)

Item	Environment setup parameter or description	HPtM User's Guide Reference
Edit definition file	Editing of the existing operation definition file	Not applicable
Backup object	BACKUP_OBJECT	Section 4.14
Database server name	DB_SERVER_NAME	
Instance name	INSTANCE_NAME	
Target name	TARGET_NAME	
FTP service root directory	FTP_HOME_DIR	
FTP service sub directory	FTP_SUB_DIR	
Maximum log lines	MAX_LOG_LINES	Section 4.14
Display basic command message on standard output	MSG_OUTPUT	

Based on the value that you have specified for **Server type** in the Configuration Settings window, the HOST_ROLE parameter value in the host environment settings file is automatically determined. Similarly, based on the value that you have specified for **Configuration type** in the Configuration Settings window, the SET_DRM_HOSTNAME parameter value in the operation definition file is automatically determined.

5.2.15.2 If You Selected Cluster Configuration as the Configuration Type

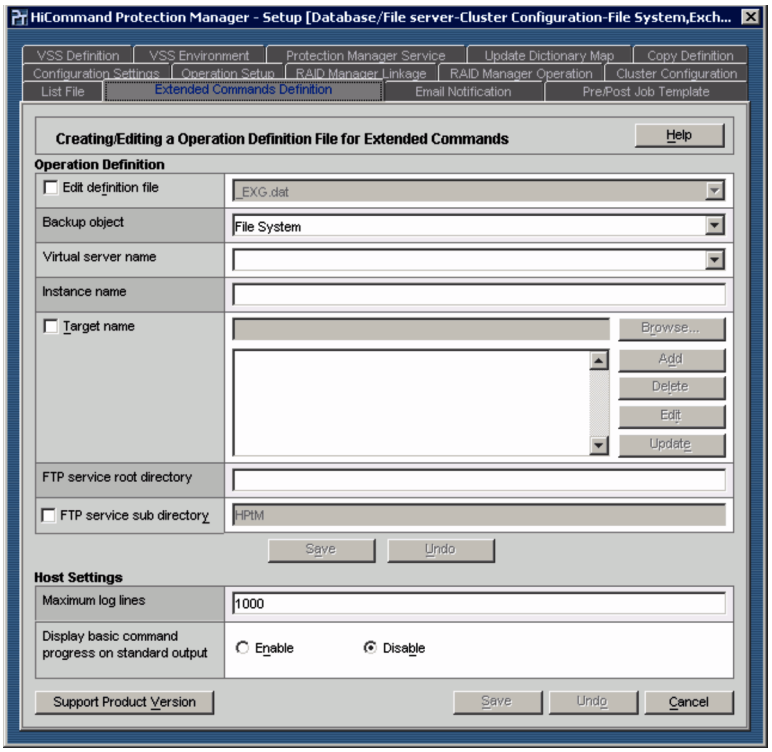


Figure 5.26 Extended Commands Definition Window (for Cluster Configuration)

Table 5.24 Extended Commands Definition Window Items (for Cluster Configuration)

Item	Environment setup parameter or description	HPtM User's Guide Reference
Edit definition file	Editing of the existing operation definition file	Not applicable
Backup object	BACKUP_OBJECT	Section 4.14
Virtual server name	DB_SERVER_NAME	
Instance name	INSTANCE_NAME	
Target name	TARGET_NAME	
FTP service root directory	FTP_HOME_DIR	
FTP service sub directory	FTP_SUB_DIR	
Maximum log lines	MAX_LOG_LINES	Section 4.14
Display basic command message on standard output	MSG_OUTPUT	

Based on the value that you have specified for **Server type** in the Configuration Settings window, the HOST_ROLE parameter value in the host environment settings file is automatically determined. Based on the value that you have specified for **Configuration type** in the Configuration Settings window, the SET_DRM_HOSTNAME parameter value in the operation definition file is automatically determined.

5.2.16 Pre/Post Script Job Window

The Pre/Post Job Template window enables the user to set or update any of the following items related to a user script:

- User script file name
- User pre-processing before the backup command is issued (PRE_PROC)
- User post-processing after the backup command is issued (POST_PROC)

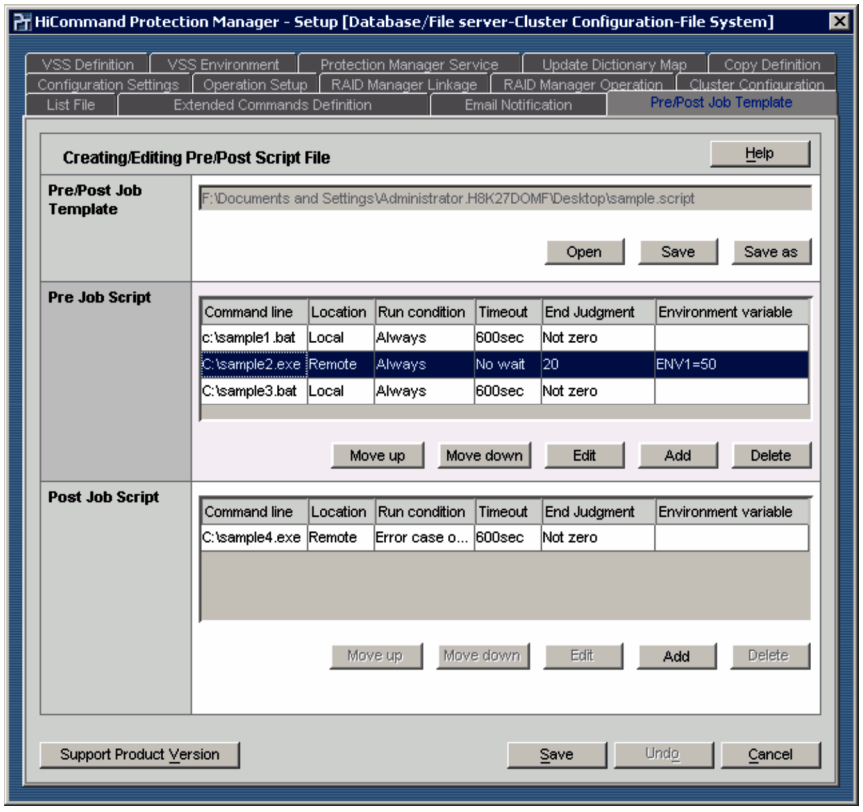


Figure 5.27 Pre/Post Job Template Window

Table 5.25 Pre/Post Job Template Window Items

Item	Explanation
Pre/Post Job Template	User script file
Pre Job Script	Section that defines user pre-processing
Post Job Script	Section that defines user post-processing

The procedures for setting a user script are explained below.

5.2.16.1 Setting User Pre-processing (PRE_PROC)

1. In the Pre/Post Job Template window, click the **Add** button in **Pre Job Script**. The Add Pre script job dialog box appears.

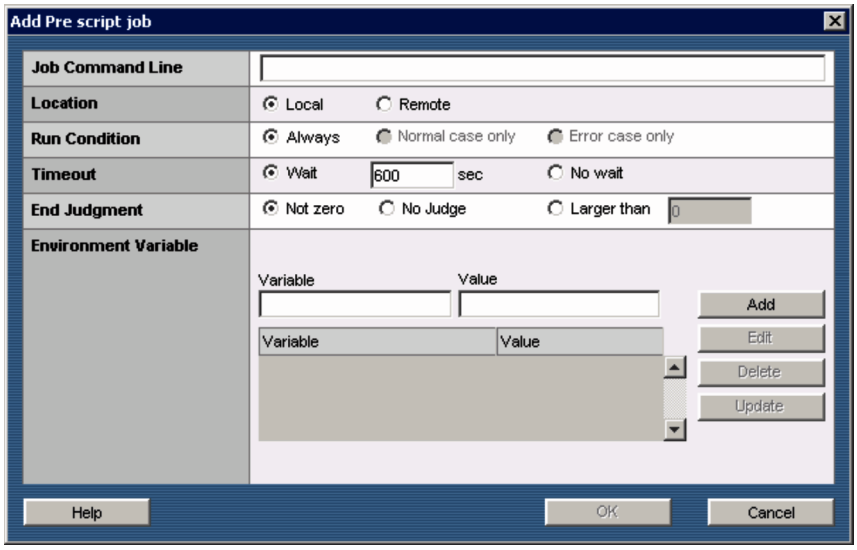


Figure 5.28 Add Pre script job Dialog Box

2. Set the items shown in the

Table 5.26:

Table 5.26 Add Pre script job Dialog Box Items

Item	Description	Value and its meaning	HPtM User's Guide Reference [1]
Job Command Line	Command to be executed	Command line	CMDLINE
Location	Command execution server	▪ Local: Local server ▪ Remote: Backup server	LOCATION
Run Condition	Command execution condition[2]	▪ Always: Always executes the command. ▪ Normal case only: Executes the command only when the parent command is normal. ▪ Error case only: Executes the command only when the parent command is in error.	PARENT_STAT
Timeout	Command timeout value	▪ Wait: Specifies a command timeout value (default: 600). ▪ No wait: Specifies to not wait for termination of the executed command.	TIMEOUT
End Judgment	User script termination condition	▪ Not zero: Terminates the script processing if a non-zero return value is returned. ▪ No Judge: Continues processing regardless of the return value. ▪ Larger than: Specifies an error threshold value as an integer in the range 0 to 255 (default: 0). The script processing terminates if a return value greater than the specified value is returned.	END_CODE
Environment Variable	Environment variable	▪ Variable: Specifies the name of an environment variable. ▪ Value: Specifies the value of an environment variable If you want to delete the environment variable when executing the command, specify, for Variable, the name of the environment variable that you want to delete, and do not specify a value for Value.	ENV

1: The referenced items are shown in Table 4.57 in the *HPtM User's Guide*.

2: Only Always can be selected for user pre-processing.

The following are the rules for environment variables:

- To add an environment variable, enter the name of the environment variable in **Variable** and the value of the environment variable in **Value**, and then click the **Add** button. The environment variable will be added.
- To edit the environment variable, select the applicable line, and then click the **Edit** button to display the values set in **Variable** and **Value**. Edit the values, and then click the **Update** button. The environment variable will be edited.

- To delete an environment variable, select the applicable line, and click the **Delete** button.

3. Click the **OK** button.

   The contents of the settings are displayed in **Pre Job Script** in the Pre/Post Job Template window The commands will be executed in the order of the lines displayed above.

   - To add a line in **Pre Job Script**, repeat steps 1 and 2. A line is added following the last line
   - To edit the line in **Pre Job Script**, select the line to be changed, and then click the **Edit** button to display the Edit Pre script job dialog box. The items that can be set and how to set them are the same as those for the Add Pre script job dialog box, which is displayed by clicking the **Add** button.
   - To delete a line from **Pre Job Script**, select the line to be deleted, and click the **Delete** button.
   - To change the order of lines in **Pre Job Script** (to rearranging the command execution sequence), select the line to be moved and click either the **Move up** or **Move down** button.

5.2.16.2 Setting User Post-Processing

1. In the Pre/Post Job Template window, click the **Add** button in **Post Job Script**.

   The Add Post script job dialog box appears.

2. Set the appropriate items.

   The items that can be set and how to set them are the same as for user pre-processing.

3. Click the **OK** button.

   The contents of the settings are displayed in **Post Job Script** in the Pre/Post Job Template window.

5.2.16.3 Setting a User Script File Name

1. In **Pre/Post Job Template**, click the **Save** or the **Save as** button.

   The Save as dialog box appears.

2. If you have started Protection Manager Console locally, click the **Browse** button to select a file. If you have started Protection Manager Console remotely from Device Manager, directly enter the absolute path of the file name.

   To directly enter the file's absolute path instead of clicking the **Browse** button, specify an appropriate Windows file name by using no more than 255 bytes.

3. Click the **OK** button.

   The user script file name that is set is displayed in **Pre/Post Job Template** in the Pre/Post Job Template window.

Note: The **Save** button in **Pre/Post Job Template** is a **Save And Overwrite** button. The **Save as** button is a **Save under a different name** button. If no file name is specified in **Pre/Post Job Template**, the **Save** button functions as the **Save as** button.

5.2.16.4 Updating a User Script File

The procedure for updating a user script file is explained below.

1. In the Pre/Post Job Template window, in **Pre/Post Job Template** click the **Open** button.

   The Open dialog box appears.

2. If you have started Protection Manager Console locally, click the **Browse** button to select a file. If you have started Protection Manager Console remotely from Device Manager, directly enter the absolute path of the file name.

   To directly enter the file's absolute path instead of clicking the **Browse** button, specify an appropriate Windows file name by using no more than 255 bytes.

3. Click the **OK** button.

   The contents of the selected user script file are displayed in the Pre/Post Job Template window.

4. Update the contents of the **Pre Job Script** or **Post Job Script**.

5. In **Pre/Post Job Template**, click the **Save** button.

   The user script file is updated.

5.2.17 Email Notification Window

You can use the Email Notification window to create or modify the mail send definition file (`mail.conf`) that is necessary to distribute the execution results of Protection Manager's backup command by e-mail.

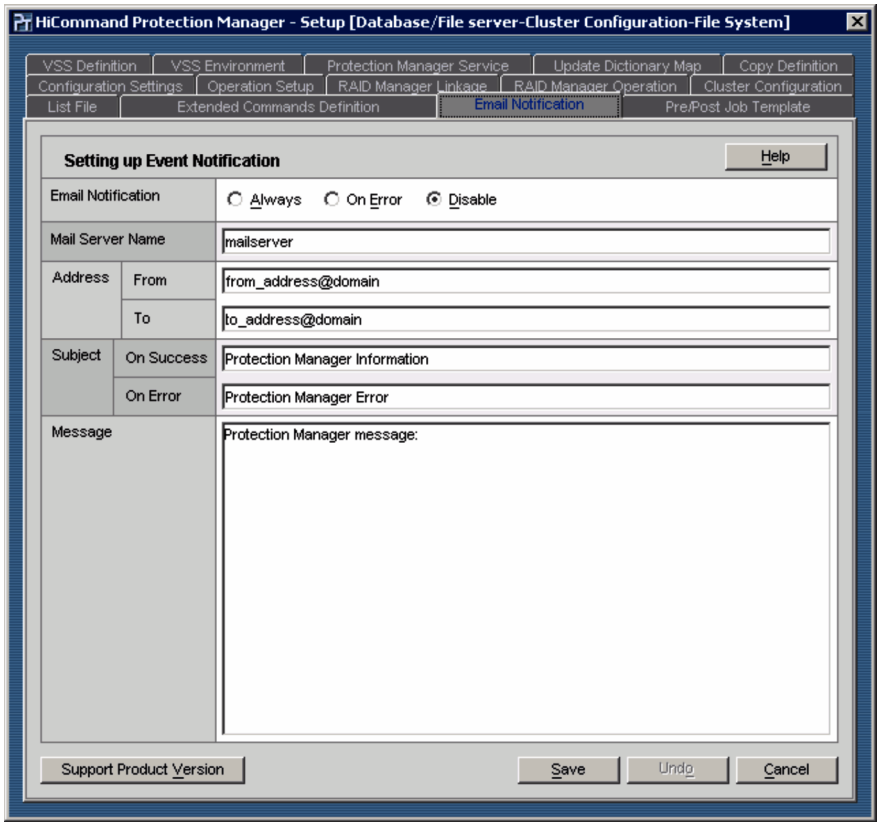


Figure 5.29 Email Notification Window

Table 5.27 Email Notification Window Items

Item		Environment setup parameter or description	HPtM User's Guide Reference
Email Notification		MAIL_SEND	Section 4.16
Mail Server Name		SMTP_SERVER	
Address	**From**	FROM	
	To	TO	
Subject	**On Success**	SUBJECT_NORMAL	
	On Error	SUBJECT_ERROR	
Message		TEXT	

5.3 About the Configuration Check Function

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.

5.3.1 Capabilities of the Configuration Check Function

The configuration check function can check the Protection Manager execution environment items noted in the following table:

Table 5.28 Protection Manager Environment Items Subject to Checking by the Configuration Check Function

No.	Check item	Description	Check object				Check condition
			DB	BK	DB-BK	DB-DB	
1	Windows version	Verifies whether the Windows version installed on the server satisfies Protection Manager's prerequisite conditions.	Y	Y	Y	Y	--
2	Windows version (with VSS used)	Verifies whether the Windows version installed on the server satisfies the prerequisite conditions for using VSS in Protection Manager.	Y	Y	Y	Y	When VSS is being used
3	Versions of the programs used by VSS	Verifies whether the versions of the following programs satisfy prerequisite conditions for using VSS in Protection Manager. ▪ RAID Manager ▪ Hardware provider ▪ Microcode of the storage subsystem	Y	Y	Y	Y	When VSS is being used
4	Existence of Hardware Provider	Verifies whether the hardware provider required for using VSS is installed correctly.	Y	Y	--	--	When VSS is being used
5	Disk configuration	Checks whether a disk configuration not supported by VSS is used (dynamic disk in a Windows LDM environment or in VxVM).	Y	--	--	--	When VSS is being used
6	`vsp.sys` version	Checks the version of the Backup Exec filter driver (`vsp.sys`).	Y	Y	--	--	When VSS is being used
7	Environment variable `HORCMPERM`	Checks whether the environment variable `HORCMPERM` is not set in the system environment variable for	Y	Y	--	--	When VSS is being used

No.	Check item	Description	Check object				Check condition
			DB	BK	DB-BK	DB-DB	
		the OS.					
8	Environment variable HORCMINST	Checks whether the environment variable HORCMINST is not set in the system environment variable for the OS.	Y	Y	--	--	When VSS is being used
9	ESEUTIL command	Verifies whether the ESEUTIL command is installed correctly. Also verifies whether the files for the ESEUTIL command installed on the backup server are the same as those installed on the Exchange server.	Y	Y	Y	--	▪ When VSS is being used ▪ When the backup object is Exchange Server 2003
10	Settings for system environment variables used by VSS	Verifies whether the system environment variables used in VSS have been set up correctly.	Y	Y	--	--	When VSS is being used
11	Path management software version	Verifies whether the version of the path management software is a prerequisite version for Protection Manager.	Y	Y	--	--	--
12	Hotfix required for restoration while the cluster resources are in the online state	Verifies whether Hotfix, which is required for restoration while the cluster resources are in the online state, has been applied to the server. This check item is available when restoration while the cluster resources are in the online state is enabled in init.conf.	Y	Y	--	Y	For cluster configuration
13	Presence/absence of dictionary map file	Verifies that a shared disk is assigned to each virtual server and a dictionary map file is placed on the shared disk.	Y	Y	--	Y	For cluster configuration
14	Exchange Server version	Verifies whether the current version of Exchange Server satisfies Protection Manager's prerequisite conditions. Also verifies whether the required Hotfix has been applied.	Y	--	--	Y	When the backup object is Exchange Server
15	Storage location for the file to be backed up by Exchange Server	Verifies whether Exchange Server data files (*.edb, *.stm), transaction log files (*.log), and checkpoint files (*.chk) are stored in the appropriate locations.	Y	--	--	Y	When the backup object is Exchange Server
16	SQL Server	Verifies whether the current	Y	--	--	Y	When the

No.	Check item	Description	Check object				Check condition
			DB	BK	DB-BK	DB-DB	
	version	version of SQL Server satisfies Protection Manager's prerequisite conditions.					backup object is SQL Server
17	Protection Manager service	Verifies whether the installed Protection Manager Copy Controller supports the Protection Manager service.	Y	Y	--	--	--
18	VSFW (VxVM) version	Checks the compatibility of the current version of VSFW (VxVM) installed on the server and the version of Windows.	Y	Y	Y	Y	When VSFS is being used
19	Protection Manager version	Checks the version of the Protection Manager installed on the server.	Y	Y	Y	Y	--
20	Exchange Management Console	Checks whether Exchange Management Console is correctly installed on the backup server. Also checks whether the Exchange Management Console version matches that of Exchange Server 2007.	--	Y	Y	--	▪ When VSS is being used ▪ When the backup object is Exchange Server 2007

Legend:

/DB: A database server (file server) is checked.

BK: A backup server is checked.

DB-BK: Integrity between a database server (file server) and a backup server is checked.

DB-DB: Integrity among database servers (file servers) is checked.

Y: Checked

N: Not checked, or not applicable

5.3.2 Prerequisites for and Notes on Using the Configuration Check Function

5.3.2.1 Prerequisites

The configuration check function can execute from the file server, database server, or backup server. Before the configuration check function can be used, the following program products must be installed in the execution environment and the appropriate environment settings must be in effect:

- Protection Manager Copy Controller
- Protection Manager Console

For details about how to install Protection Manager Console, see the *HiCommand Protection Manager Console User's Guide*.

In addition, the following environment settings must be complete on all file, database, and backup servers to be checked:

- Protection Manager Copy Controller is installed.
- Protection Manager service is running.

5.3.2.2 Notes

- The Configuration Check Function does not check all the configuration conditions. To verify detailed configuration conditions, see the manual or the Release Notes.
- If the results of the Configuration Check Function show an error, see the information about the relevant configuration in the manual or the Release Notes to correct the flaw before running the Configuration Check Function again.
- The configuration check tool can be used only when Protection Manager Console is directly activated (local starting) from the server on which Protection Manager Console is installed. The configuration check tool cannot be used if Protection Manager Console is activated (remote starting) from Device Manager.

5.3.3 How to Use the Configuration Check Function

This section explains how to use the configuration check function in Protection Manager.

5.3.3.1 Performing Configuration Check

You use the following procedure to execute the configuration check function:

1. Activate Protection Manager Console on the server on which the configuration check is to be executed.

   For details about how to activate Protection Manager Console, see the *HiCommand Protection Manager Console User's Guide*.

2. In the Protection Manager Console main window, choose **Tools**, and then **Check Configuration**

   The Input Servers dialog box appears.

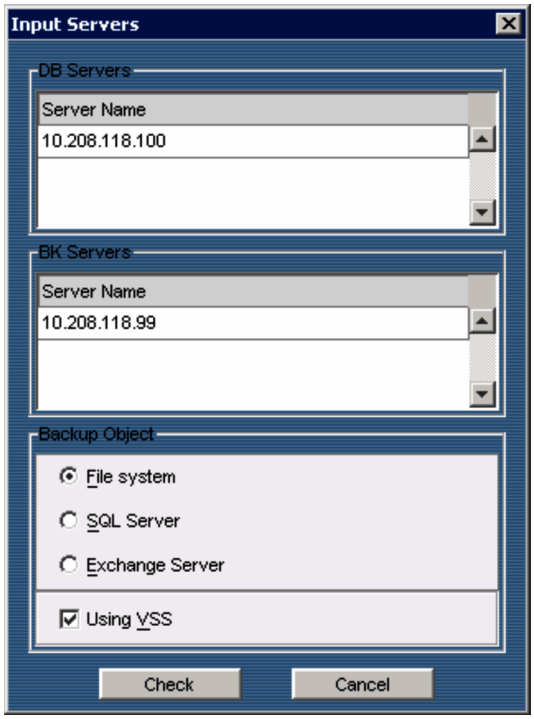


Figure 5.30 Input Servers Dialog Box

3. In the **DB Servers** list box, register either the host name or IP address for the file server or database server to be checked.

   If there is more than one file server or database server, such as in a cluster configuration, all servers must be registered. You can only register physical servers. You cannot register virtual servers. Lines can be added to or deleted from the list box as follows:

   Adding a line

   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.

   Deleting a line

   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.

4. In the **BK Servers** list box, register the host name or IP address for the backup server to be checked.

   See Step 3 for the registration method.

5. In **Backup Object**, select the check box associated with the object to be backed up.

6. If VSS is being used, select the **Using VSS** check box.
7. Click the **Check** button.

   The check starts. The check results are displayed in the Check Results dialog box.

   To cancel the configuration check, click the **Cancel** button.

5.3.3.2 Reviewing the Check Results

You use the following procedure to review the check results that are output by the configuration check function.

1. Review the contents output in the Check Results dialog box.

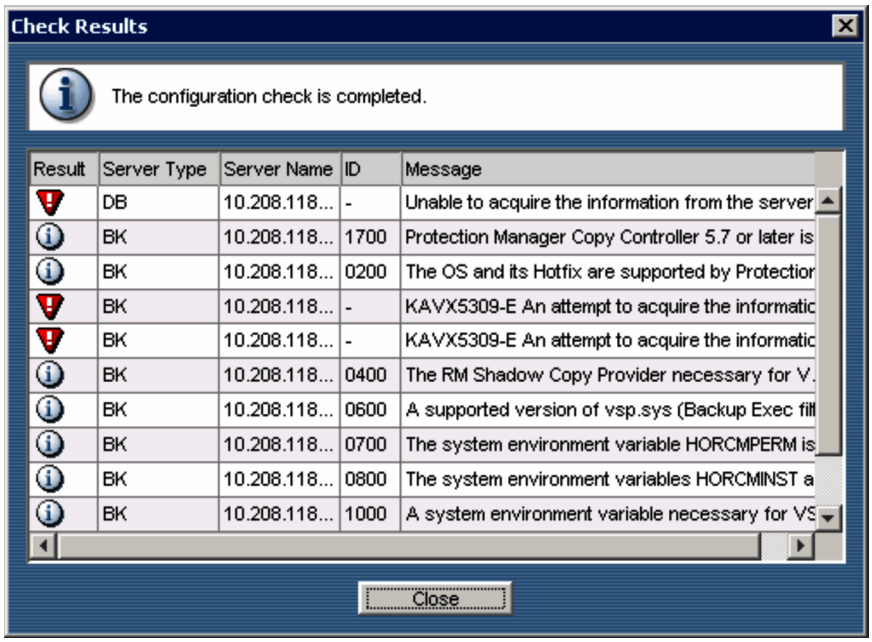


Figure 5.31 Check Results Dialog Box

The following explains the items that are output in the Check Results dialog box:

Result

The check results for each check item are indicated by the following icons:

Icon	Type	Meaning
	Error	The configuration that was checked could produce errors or is an unsupported configuration.
	Warning	The configuration that was checked could produce errors depending on the particular operation performed.
	Normal	The configuration that was checked has no problems.

Server Type

Type of server that was checked:

DB: File or database server

BK: Backup server

Server Name

Name (host name or IP address) of the server that was checked. If the check was between servers, a hyphen (-) is displayed.

ID

Message ID.

Message

Message text for the check results.

2. Detailed information about a checked item can be viewed by double-clicking the item's column.

   Detailed information is output to the Result dialog box.

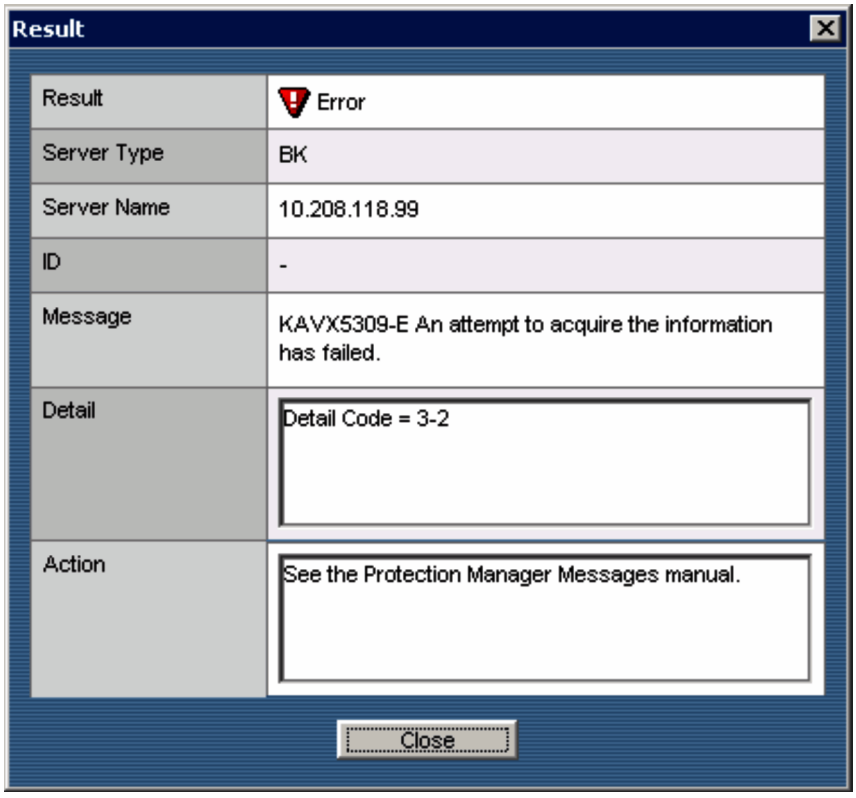


Figure 5.32 Result Dialog Box

If there is a problem in Protection Manager environment settings, the settings should be examined based on the detailed information.

3. Click the **Close** button.

   Closes the Result dialog box.

Repeat Steps 2 to 3 to verify the check results.

4. Click the **Close** button.

   The Check Results dialog box closes, and the configuration check function ends.

Chapter 6 Using Protection Manager Console

This chapter explains how to operate Protection Manager Console. The term *storage group* refers to a database management unit created on Exchange Server. Note that this definition differs from the term storage group used in other HiCommand products.

- Operating the Protection Manager Console (see section 6.1)
- Operations for File Systems (see section 6.2)
- Operations for SQL Server Databases (see section 6.3)
- Operations for Exchange Databases (see section 6.4)
- Operations for Backup Jobs (see section 6.5)
- Locking a Copy Group (see section 6.6)
- Resynchronizing a Copy Group (see section 6.7)
- Mounting and Unmounting the Secondary Volume (see section 6.8)
- Using a User Script (see section 6.9)

6.1 Operating the Protection Manager Console

Before starting Protection Manager Console operations, please see the *HiCommand Protection Manager User's Guide* to complete the environment settings for the prerequisite products.

The following figure provides an example of a system configuration using Protection Manager Console.

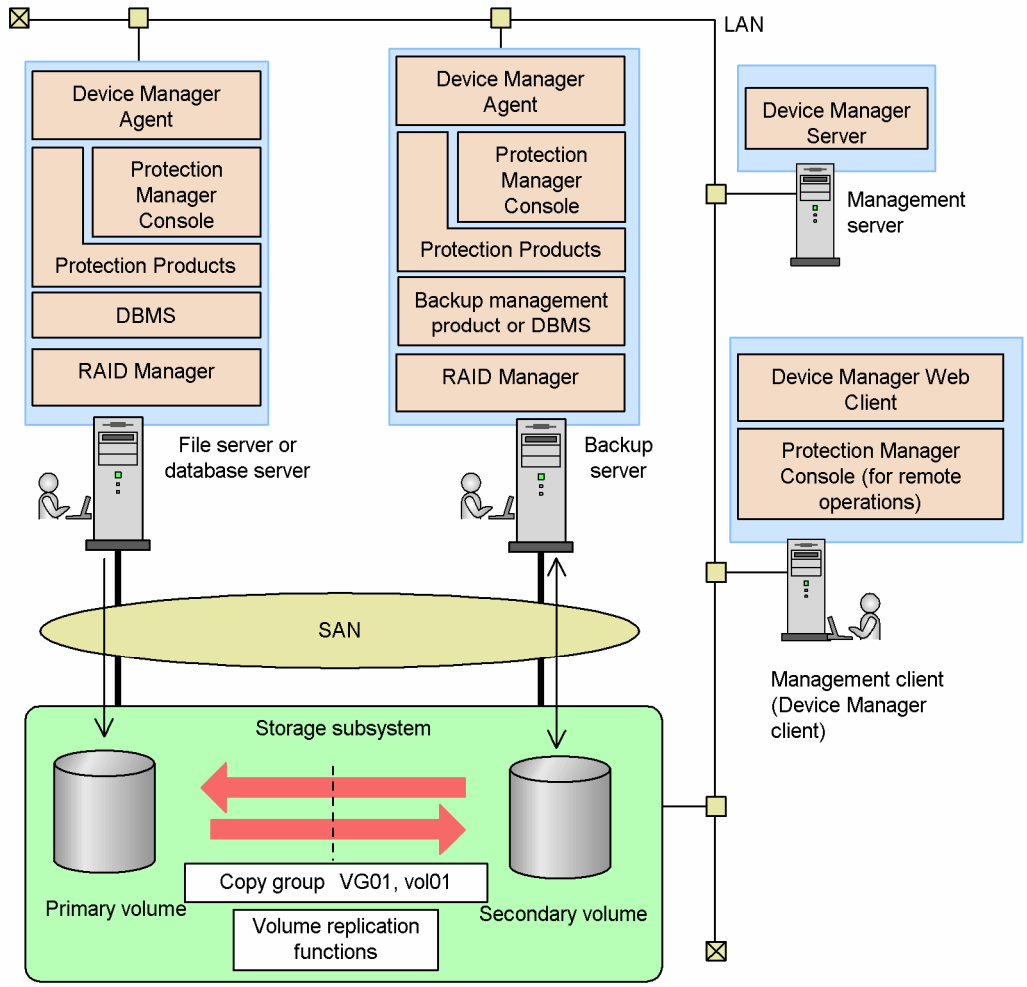


Figure 6.1 Example of a System Configuration Using Protection Manager Console

Notes:

- On the backup server, for the secondary volume, Protection Manager Console can only perform mount and unmount operations. In this manual, a server that mounts and unmounts the secondary volume is called a backup server. For details on operations that Protection Manager Console can perform on the secondary volume, see section 6.8.
- Protection Manager Console treats only ShadowImage, QuickShadow, TrueCopy and UR copy types as backup and restoration targets.

6.1.1 Starting Protection Manager Console

When it is installed on an application server, you can start an instance of Protection Manager Console locally or remotely:

- **Local start**: Start the instance of Protection Manager Console at the application server.
  - To perform backup or restore operations, start the Protection Manager Console that is installed either on the file server or the database server.
  - To perform mount or unmount operations for the secondary volume, start the instance of Protection Manager Console installed on the backup server.
- **Remote start**: From Device Manager, start the instance of Protection Manager Console on the desired application server.

Administrator privileges are required to execute Protection Manager Console. For details on such privileges, see section 1.4.5.

6.1.1.1 Starting Protection Manager Console on an Application Server

You can start Protection Manager Console on an application server such as a file server, database server, or backup server.

To start Protection Manager Console on an application server:

1. Log on as a user with Administrator privileges.
2. From the Windows **Start** menu, choose **Programs**, **HiCommand Protection Manager Console**, and then **Console**.

   Note: If you changed the program folder name during the installation, choose the changed name.

6.1.1.2 Starting Protection Manager Console from Device Manager

Before starting Protection Manager Console from Device Manager, ensure that the services of the Device Manager agent on the application server are active.

Make sure that the Device Manager agent services have been started by the Administrator account, and the service startup account for the Device Manager agent has database access privileges.

Note: If the services of the Device Manager agent are not started by the administrator account, change the user account to the administrator account, and then restart the services. Otherwise, if the services of the Device Manager agent are running under a user account that does not have administrator permissions, problems might occur; for example, the services of the Device Manager agent might not take effect even if the environment variable `DRM_HOSTNAME` is changed.

When the OS on the management client is Windows XP SP2 or Windows Vista, disable the Microsoft Internet Explorer pop-up blocking function. If this function is enabled, you cannot start Protection Manager Console by clicking the **Protection Manager** button in the property window of a host displayed in the Device Manager Web Client.

Disable the Microsoft Internet Explorer pop-up blocking function by using the **Tools** menu of Microsoft Internet Explorer. You can choose one of the following ways:

- disabling only the pop-up blocking function of the Device Manager server
- disabling the pop-up blocking function as a whole.

To start Protection Manager Console from Device Manager:

1. Log in to the Device Manager Web Client.
2. In the hierarchy in the Web Client Navigation frame, choose from **Hosts** the host (file server, database server, or backup server) that you want to access.

   In the Web Client Information frame, the Property window for the selected host appears.
3. Click the **Protection Manager** button.

   Protection Manager Console starts, and the Main window will be displayed.

   Note: When Protection Manager Console is started form the Device Manager Web Client for the first time, Protection Manager Console for remote startup is downloaded from the application server before Protection Manager Console starts.

6.1.1.3 Selecting a Virtual Server

When performing operations for a server in a cluster configuration, you will select the required virtual server from the virtual servers registered in the connection destination host.

To select a virtual server:

1. From the menu bar of the Protection Manager Console main window, choose **Action** and then **Select Virtual Server**.

   The Select Virtual Server dialog box is displayed.

2. Select the required virtual server from the list of virtual servers displayed in the Select Virtual Server dialog box.

3. Click the **OK** button.

   You can now view the dictionary map file that the selected virtual server uses. The Select Virtual Server dialog box closes.

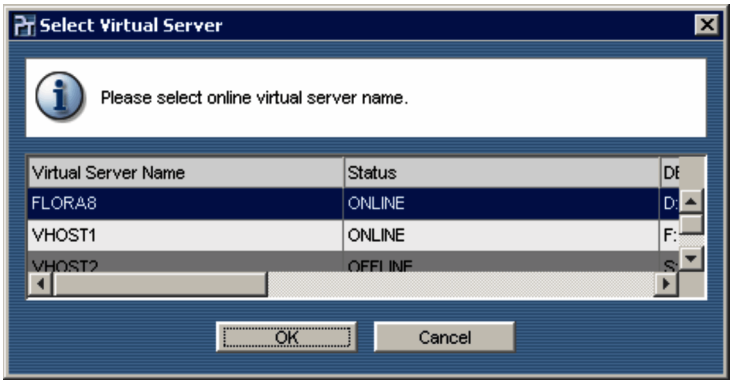


Figure 6.2 Select Virtual Server Dialog Box

6.1.2 Reviewing the Main Window Configuration

The Main window of Protection Manager Console consists of the menu bar and the Information View. You can view specific information by selecting the tabs in the Information View, the Application View, the Backup Catalog View, and the Backup Job View.

Note: The title bar displays `HiCommand Protection Manager Console –` *host-name* - *virtual-server-name*. Note that -*virtual-server-name* is displayed only when the virtual server has been registered in the system environment variable and the setting is enabled.

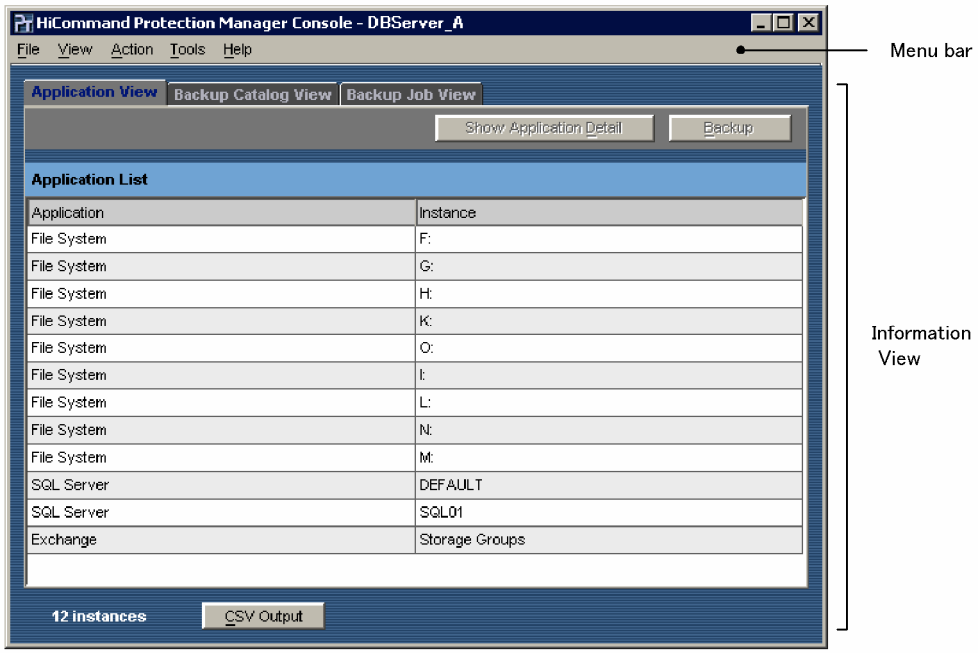


Figure 6.3 Main Window of Protection Manager Console

- **Application View:** Displays application information (a list of file systems and database instances to back up). For details on this view, see section 6.1.3.
- **Backup Catalog View:** Displays catalog information (a list of file systems and database instances that have been backed up). For details on this view, see section 6.1.4.
- **Backup Job View:** Displays backup job information (a list of backup jobs registered thus far). For details on this view, see section 6.1.5.

The following table lists the menu items in the Main window.

Table 6.1 Menu Items in the Main Window

Menu Bar	Menu Item	Description
File	**CSV Output**	Outputs the contents displayed in the Application View or the Backup Catalog View to a file (in a tab-delimited format). This item is only enabled when one or more items are displayed in the list, in the Application View or the Backup Catalog View. You can also perform the same operation by clicking the **CSV Output** button displayed in the Application View and Backup Catalog View.
	Exit	Quits Protection Manager Console.
View	**Application View**	Displays the Application View in the Information View. This item is only enabled when the Backup Catalog View or Backup Job View is displayed in the Main window. You can also perform the same operation by clicking the **Application View** tab in the Main window.
	Backup Catalog View	Displays the Backup Catalog View in the Information view. This item is only enabled when the Application View or Backup Job View is displayed in the Main window. You can also perform the same operation by clicking the **Backup Catalog View** tab in the Main window.
	Backup Job View	Displays the Backup Job View in the Information view. This item is only enabled when the Application View or the Backup Catalog View is displayed in the Main window. You can also perform the same operation by clicking the **Backup Job View** tab in the Main window.
	Application Detail	Displays the Application Detail window. The Application Detail window contains detailed application information. This item is only enabled when a record is selected in the Application View. You can also perform the same operation by clicking the **Show Application Detail** button in the Application View.
	Backup Detail Information	Displays the Backup Detail Information window. The Backup Detail Information window contains detailed catalog information. This item is only enabled when a record is selected in the Backup Catalog View. You can also perform the same operation by clicking the **Show Backup Detail Information** button in the Backup Catalog View.
	Backup Job Results	Displays the Backup Job Result Details window. The Backup Job Result Details window displays details of the backup job execution results. This item is only enabled when a record is selected in the Backup Job View. You can also perform the same operation by clicking the **Show Backup Job Results** button in the Backup Job View.
	Refresh	Updates the information displayed (only in the displayed page) in the Information View.

Menu Bar	Menu Item		Description
Action	**Backup**		Performs backup. This item is only enabled when a record is selected in the Application View. You can also perform the same operation by clicking the **Backup** button in the Application View.
	Restore		Performs restoration processing. This item is only enabled when a record is selected in the Backup Catalog View. You can also perform the same operation by clicking the **Restore** button in the Backup Catalog View.
	Mount		Mounts the secondary volume on the backup server. For details on mount operations, see section 6.8.1.
	Unmount		Unmounts the secondary volume on the backup server. For details on unmount operations, see section 6.8.2.
	Lock		Locks or unlocks a copy group.
	Resynchronize		Resynchronizes a copy group.
	Job	**Modify**	Changes options relevant to a backup job. This item is only enabled when a record is selected in the Backup Job View. You can also perform the same operation by clicking the **Modify** button in the Backup Job View.
		Delete	Deletes a backup job. This item is only enabled when a record is selected in the Backup Job View. You can also perform the same operation by clicking the **Delete** button in the Backup Job View.
		Run Immediately	Runs a backup job immediately. This item is only enabled when a record is selected in the Backup Job View. You can also perform the same operation by clicking the **Run Immediately** button in the Backup Job View.
	Select Virtual Server		Displays the Select Virtual Server dialog box. When the server is in a cluster configuration, the Select Virtual Server dialog box displays virtual servers registered in the connection destination host. For details on how to select a virtual server, see section 6.1.1.3.
	Update Dictionary Map File		Displays the Update Dictionary Map File dialog box. For details on how to use this dialog box, see section 6.1.6.
Tools	**Setup**		Starts Setup GUI. For details on Setup GUI, see the *HiCommand Protection Manager User's Guide*.
	Check Configuration		Starts the configuration check functionality. For details on the configuration check functionality, see the *HiCommand Protection Manager User's Guide*.
Help	**User's Guide**		Displays the HTML manual. See ***Note***.
	Connected Host Information		Displays the product and version of Protection Products installed on the connection destination host, and the connected virtual server and its database path.
	About Protection Manager		Displays the version information for Protection Manager Console.

Note: When you start Protection Manager Console remotely from Device Manager, if the OS running on the management client is Solaris, the HTML manual might not be displayed after you choose the **Help** menu and then **Users Guide**. In this case, start another browser, and then reselect **Users Guide**.

6.1.3 Viewing Application Information

Application information is comprised of a list of file systems, database instances, and storage configuration information to be backed up. You can display application information in the Application View. Detailed application information can be displayed in the Application Detail window.

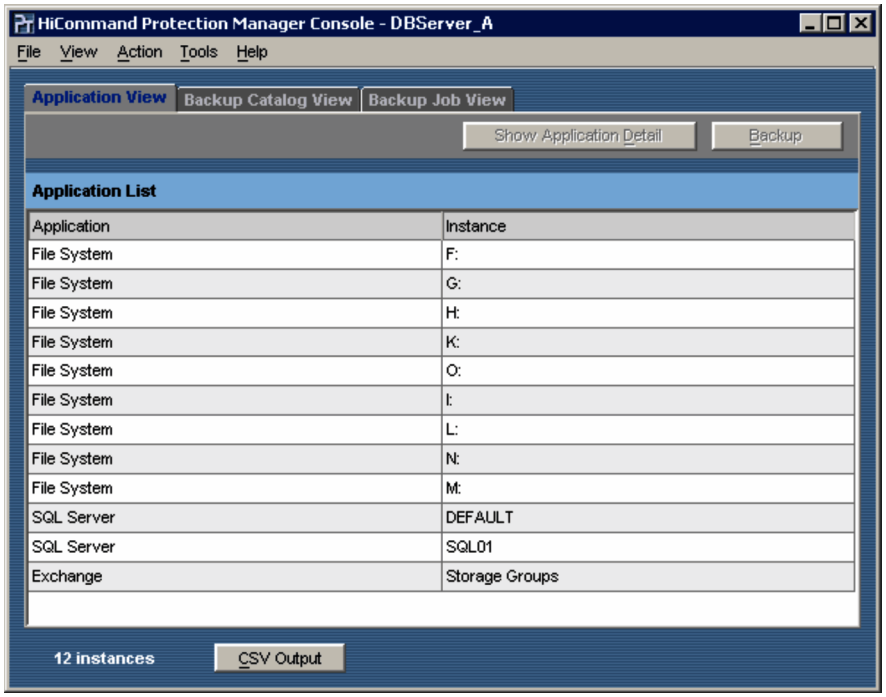


Figure 6.4 Example of the Application View

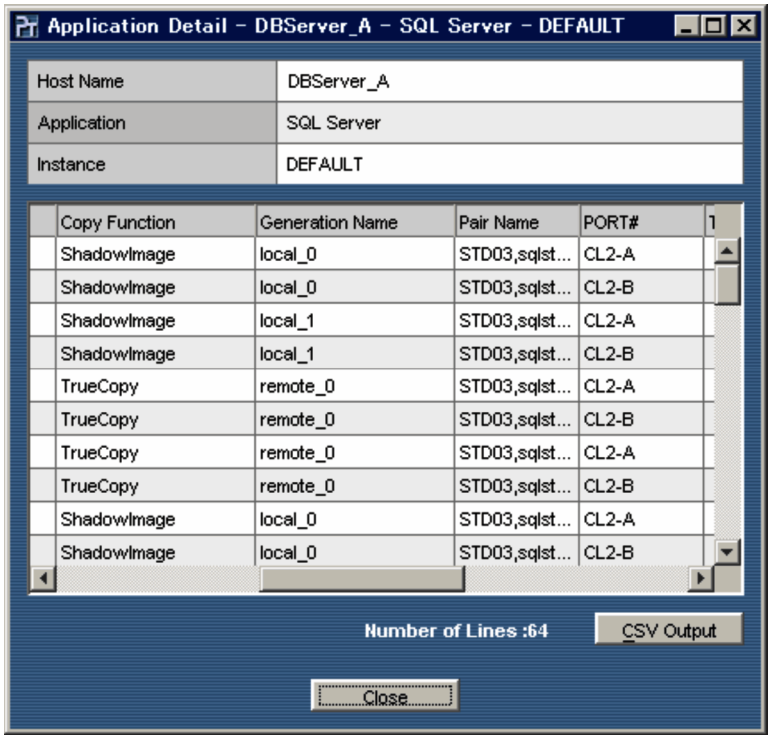


Figure 6.5 Example of the Application Detail Window

A list is displayed in the Application View. You can rearrange the order of the rows to make the list easier to read. You can also click the list headers to sort the contents of that column in ascending or descending order.

The following table lists the items displayed in the Application View.

Table 6.2 Items Displayed in the Application View

Item Name	Contents
Application	The application type `File System`, `SQL Server`, or `Exchange` is displayed.
Instance	Instance-name File System: *mount-point-name* SQL Server: *database-instance-name* Exchange: `Storage Groups`
n **instances**	The number of instances in the list
Show Application Detail button	Displays the Application Detail window. This item is only enabled when a record is selected in the Application View.
Backup button	Performs backup processing. This item is only enabled when a record is selected in the Application View.
CSV Output button	Outputs the contents of the Application View to a file (in a tab-delimited format). When this item is selected, a dialog box for specifying the file name and save location will be displayed.

Table 6.3 Items Displayed in the Application Detail Window

Item Name	Contents
Host Name	Host name
Application	The application type `File System`, `SQL Server`, or `Exchange` is displayed.
Instance	Instance-name File System: *mount-point-name* SQL Server: *database-instance-name* Exchange: `Storage Groups`
Number of Lines	Number of lines in the list.
DB	SQL Server database name This item is displayed only when the backup is of a SQL Server database.
Storage Group	Storage group name This item is displayed only when the backup is of an Exchange database.
File Type	File type This item is displayed only when the backup is of a SQL Server database or of an Exchange database. SQL Server: **DATA/TRAN** Exchange: **MAIL/PBLC/TRAN/CHCK**
Information Store	Name of the information Store. This item is displayed only when the backup is of an Exchange database.
File Name	File name This item is displayed only when the backup is of a SQL Server database or of an Exchange database.
FS	The name of the mount point
Disk Group	Disk group name
Device	Device file name
Copy Function	Copy type Copy type: The name of the copy type varies depending on the DKC software product (storage subsystem unit) and microcode version. –: Indicates the volume where a pair volume has not been configured.(Do not create a program that operates using this display.)
Generation Name	Generation identifier
Pair Name	Copy group name
PORT#	Port name of the server host
TID#	Target ID of the server host
LUN#	Logical unit number of the server host
MU#	Pair identifier
LDEV#	Logical device number in the RAID device

Item Name	Contents
P/S	Indicates whether the volume is the primary volume or the secondary volume. P: Primary volume S: Secondary volume -: SMPL volume
SERIAL#	Serial number of the RAID device (volume)
CSV Output button	Outputs the contents of the Application Detail window to a file (in a tab-delimited format). When this item is selected, a dialog box for specifying the file name and save location will be displayed.

To view application information:

1. Start Protection Manager Console, and click the **Application View** tab.

   The Application View is displayed. For details on the displayed items, see Table 6.2.

2. From the **Application View** list, select the record whose details you want to view, and click the **Show Application Detail** button.

   The Application Detail window is displayed. For details on the displayed items, see Table 6.3. You can also display the Application Detail window by double-clicking a desired record in the list in the Application View.

6.1.4 Viewing Catalog Information

The current list of the file systems and databases that have been backed up is called catalog information. You can view catalog information in the Backup Catalog View, shown in Figure 6.6.

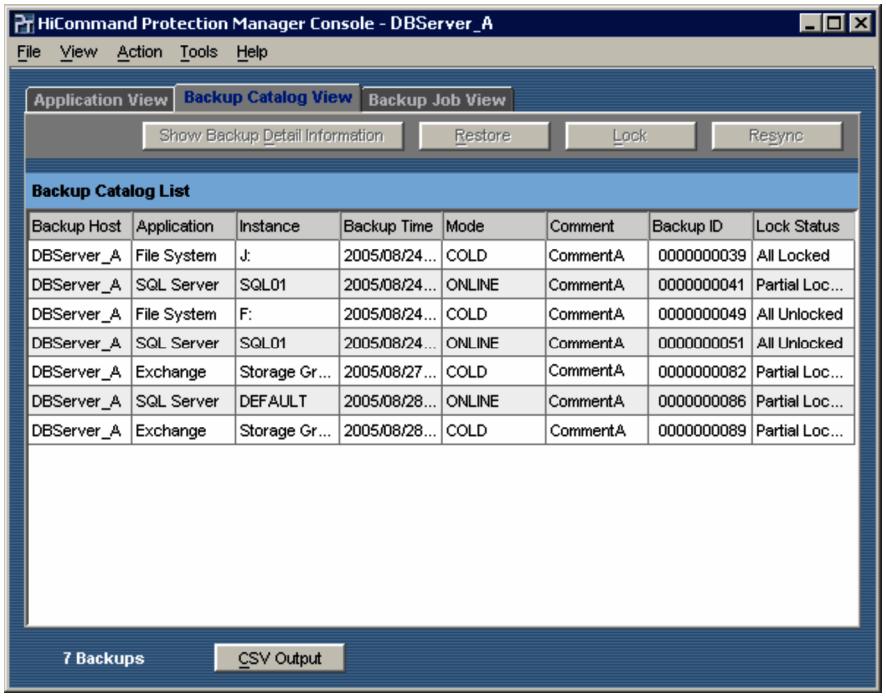


Figure 6.6 Example of the Backup Catalog View

Detailed catalog information can be displayed in the Backup Detail Information window, shown in Figure 6.7.

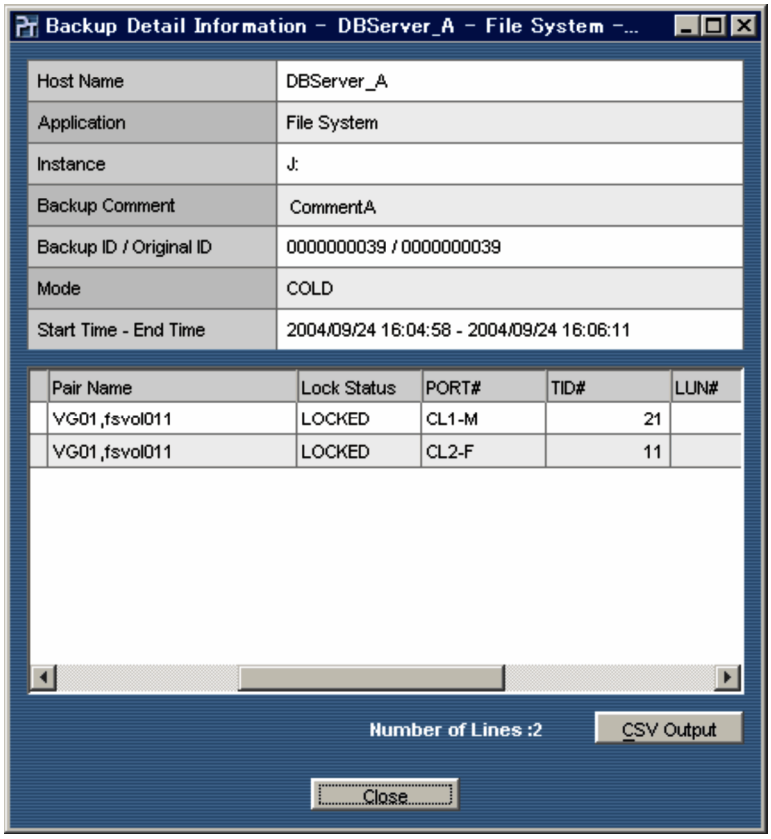


Figure 6.7 Example of the Backup Detail Information Window

A list is displayed in the Backup Catalog View. You can rearrange the order of the rows to make the list easier to read. You can also click the list headers to sort the contents of that column in ascending or descending order.

Table 6.4 lists the items displayed in the Backup Catalog View.

Table 6.4 Items Displayed in the Backup Catalog View

Item Name	Contents
Backup Host	The name of the host for which backup was performed
Application	The application type `File System`, `SQL Server`, or `Exchange` is displayed
Instance	Instance name File System: *mount-point-name* SQL Server: *database-instance-name* Exchange: `Storage Groups`
Backup Time	The time of the backup.
Mode	Backup mode `Cold`, `Online`, or `VSS` is displayed
Comment	Backup comment
Backup ID	Backup ID
n **Backups**	The number of instances backed up
Lock Status	Lock status. The Backup Catalog View displays All Locked when all target copy groups are locked, All Unlocked when all target copy groups are unlocked, and Partial Locked when some target copy groups are locked. If the lock status cannot be obtained, **-** appears.
Show Backup Detail Information button	Backup Detail Information window is displayed. This item is only enabled when a record is selected in the Backup Catalog View.
Restore button	Performs restoration processing. This item is only enabled when a record is selected in the Backup Catalog View.
Lock button	Performs lock processing. This item is only enabled when a record is selected in the Backup Catalog View.
Resync button	Performs resynchronization processing. This item is only enabled when a record is selected in the Backup Catalog View.
CSV Output button	Outputs the contents of the Backup Catalog View window to a file (in a tab-delimited format). When this item is selected, a dialog box for specifying the file name and save location will be displayed.

Table 6.5 lists the items that are displayed in the Backup Detail Information window.

Table 6.5 Items Displayed in the Backup Detail Information Window

Item Name	Contents
Host Name	Host name
Application	The application type `File System`, `SQL Server`, or `Exchange` is displayed
Instance	Instance name File System: *mount-point-name* SQL Server: *database-instance-name* Exchange: `Storage Groups`
Backup Comment	Backup comment
Backup ID / Original ID	Backup ID/Original backup ID The backup ID is overwritten with a new ID during restoration. The original backup ID is the original backup ID obtained during backup.
Mode	Backup mode `Cold`, `Online`, or `VSS` is displayed
Start Time - End Time	Backup start time and end time
Number of Lines	Number of lines in the list
DB	SQL Server database name This item is displayed only when the backup is of a SQL Server database.
Storage Group	Storage group name This item is displayed only when the backup is of an Exchange database.
File Type	File type This item is displayed only when the backup is of a SQL Server database or of an Exchange database. SQL Server: **META/DATA/TRAN** Exchange: **MAIL/PBLC/TRAN/CHCK**
Information Store	Name of the information Store This item is displayed only when the backup is of an Exchange database.
File Name	File name
FS	Name of the mount point directory where the secondary volume is to be mounted.
Disk Group	The disk group name (for environments where logical volume manager is installed) or (–) (for the basic disk configuration) is displayed.
Device	Device file name. `Harddisk`*n* (*n*: integer) is displayed.
Pair Name	Copy group name. A combination of the RAID Manager group name (`dev_group`) and RAID Manager pair logical volume name (`dev_name`).
Lock Status	Lock status The Backup Detail Information window displays (-) when the copy group name is (-), and LOCKED or UNLOCKED when the copy group name is not (-). If the lock status cannot be obtained, **-** appears.

Item Name	Contents
PORT#	Port name of the server host
TID#	Target ID of the server host
LUN#	Logical unit number of the server host
MU#	Pair identifier
LDEV#	Logical device number in the RAID device
P/S	Indicates whether the volume is the primary volume or the secondary volume. P: Primary volume S: Secondary volume -: File in a local disk
SERIAL#	Serial number of the RAID device (volume)
CSV Output button	Outputs the contents of the Backup Detail Information window to a file (in a tab-delimited format). When this item is selected, a dialog box for specifying the file name and save location will be displayed.

To view catalog information:

1. Start Protection Manager Console, and click the **Backup Catalog View** tab.

   The Backup Catalog View is displayed. For details on the displayed items, see Table 6.4.

2. From the **Backup Catalog View** list, select the record whose details you want to view, and click the **Show Backup Detail Information** button.

   The Backup Detail Information window is displayed. For details on the displayed items, see Table 6.5. You can also display the Backup Detail Information window by double-clicking a desired record in the list in the Backup Catalog View.

6.1.5 Viewing Backup Job Information

The list of backup jobs registered thus far is usually referred to as *backup job information*. You can view backup job information in the Backup Job View. You can also view details of the backup job execution results in the Backup Job Result Details window.

To view backup job information:

1. Start Protection Manager Console, and click the **Backup Job View** tab.

   The Backup Job View is displayed (see Figure 6.8). For details on the displayed items, see section 6.1.5.1.

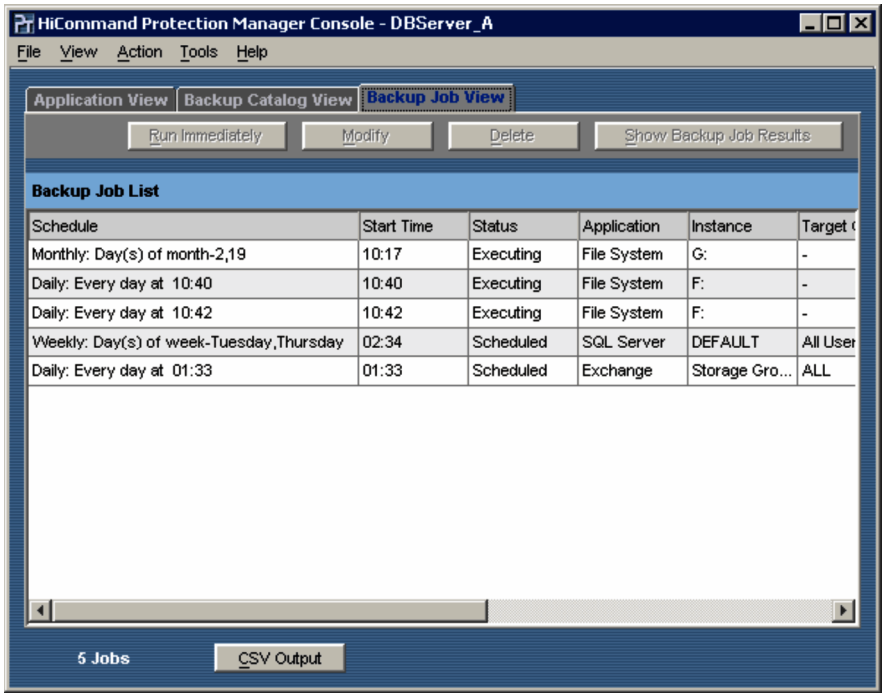


Figure 6.8 Example of the Backup Job View

2. From the Backup Job View list, select the record whose details you want to view, and click the **Show Backup Job Results** button.

   The Backup Job Result Details window is displayed (see Figure 6.9.) For details on the displayed items, see section 6.1.5.2. You can also display this window by double-clicking a record in the list in the Backup Job View.

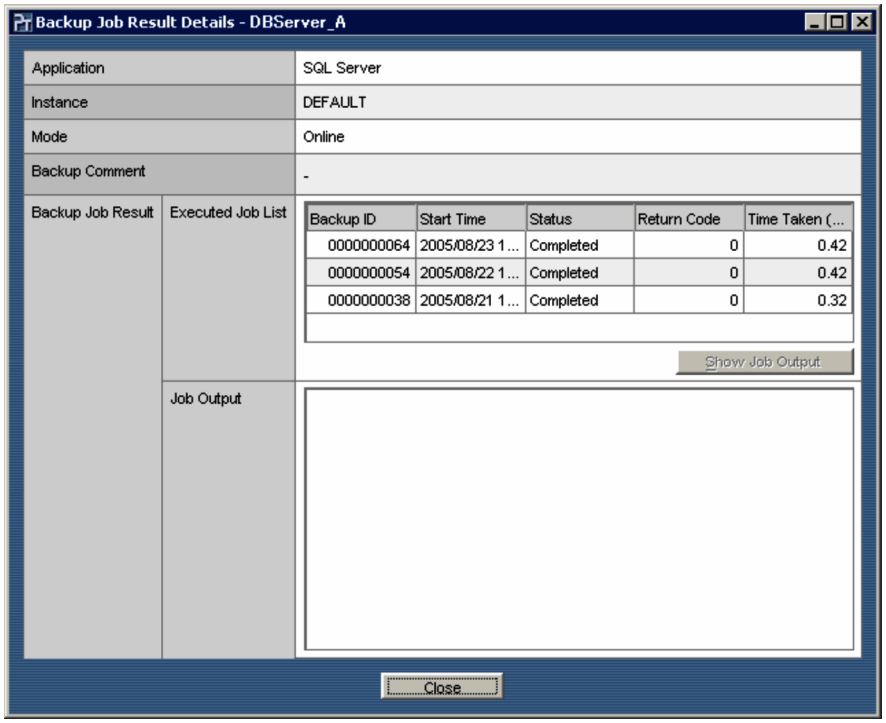


Figure 6.9 Example of the Backup Job Result Details Window

6.1.5.1 Items Displayed in the Backup Job View

The table below lists the items displayed in the Backup Job View.

Note: To make the list displayed in the Backup Job View easier to read, you can rearrange the order of the rows. You can also click the list headers to sort the contents of that column in ascending or descending order.

Table 6.6 Items Displayed in the Backup Job View

Item name	Contents
Schedule	Backup schedule The schedule type is displayed first, followed by the contents specified for the schedule options, such as the date and time. The schedule types are as follows: **Daily**: Run at the specified time each day. **Weekly**: Run at the specified day and time each week. **Monthly**: Run at the specified date and time each month. **Day of week in month**: Run each month at the specified time, day, and week in the specified month. **One time only**: Run one time only at the specified date and time.
Start Time	Backup start time
Status	Backup job status: **Scheduled**: Waiting for schedule execution **Completed**: Backup job has completed **Executing**: During backup job execution **Command Error**: An error occurred at the backup command. **Schedule Execution Error**: An error occurred during schedule execution. ***Note***: If the status becomes **Command Error** or **Schedule Execution Error**, the status remains unchanged until the next time schedule executes normally.
Application	The application type: `File System`, `SQL Server`, or `Exchange` is displayed.
Instance	Instance name File System: *mount-point-name* SQL Server: *database-instance-name* Exchange: **Storage Groups**
Target Object	Backup target name If there are multiple backup targets, they are displayed separated by commas. File System: – SQL Server: *database-name* Exchange: *storage-group-name* and *information-store-name* ***Note***: The name of the information store is displayed only when the backup mode is VSS.
Mode	Backup mode `Cold`, `Online`, or `VSS` is displayed.
Generation Name	Generation identifier

Item name	Contents
Comment	Backup comment
n **Jobs**	Number of backup jobs registered
Run Immediately button	Runs a backup job immediately. This item is only enabled when a record is selected in the Backup Job View.
Modify button	The Backup Job Update dialog box is displayed. You can change backup options in this dialog box. This item is only enabled when a record is selected in the Backup Job View.
Delete button	Deletes a backup job. This item is only enabled when a record is selected in the Backup Job View.
Show Backup Job Results button	Backup Job Result Details window is displayed. This item is only enabled when a record is selected in the Backup Job View.
CSV Output button	Outputs the contents of the Backup Job View window to a file (in a tab-delimited format). When this item is selected, a dialog box for specifying the file name and save location will be displayed.

6.1.5.2 Items Displayed in the Backup Job Result Details Window

The following table lists the items displayed in the Backup Job Result Details window.

Note: To make the list displayed in the Backup Job Result Details window easier to read, you can rearrange the order of the rows. You can also click the list headers to sort the contents of that column in ascending or descending order.

Table 6.7 Items Displayed in the Backup Job Result Details Window

Item name	Contents
Application	The application type `File System`, `SQL Server`, or `Exchange` is displayed.
Instance	Instance name File System: *mount-point-name* SQL Server: *database-instance-name* Exchange: **Storage Groups**
Mode	Backup mode `Cold`, `Online`, or `VSS` is displayed.
Backup Comment	Backup comment
Backup Job Result	Backup job execution results
Executed Job List	List of backup job execution results When the window is opened, job execution results are displayed in descending order of **Start Time**.
Backup ID	Backup ID
Start Time	Backup job execution start time
Status	**Backup** job status **Completed**: Backup job has completed **Command Error**: An error occurred at the backup command. **Schedule Execution Error**: An error occurred during schedule execution.
Time Taken (min)	Time required for the backup job (minutes)
Show Job Output button	Displays the execution result of the specified Backup ID in the **Job Output.** The button is enabled only when you have selected a Backup ID from the **Executed Job List**.
Job Output	Backup job execution results The execution result of the specified Backup ID is displayed. If backup operation terminates with an error, you can use this list to investigate the cause.

6.1.6 Updating the Dictionary Map File

Even after you have started normal operation, you need to update the dictionary map file if you have performed any of the following operations:

- changed the RAID Manager configuration definition file
- changed the pair configuration of the volume
- changed the mount point (or the drive letter in Windows)
- changed the disk configuration by adding or removing a hard disk
- expanded the dynamic volume
- configured or deleted an SQL Server instance
- added or deleted an SQL Server database
- added, deleted, or moved a configuration file for an SQL Server database
- changed the name of an SQL Server database or a database configuration file
- changed the location of the dictionary map file by using the `drmdbsetup` utility.

Note: For a cluster configuration, update the dictionary map file on the active server only: You do not normally need to switch clusters and update the file on both servers. However, if the primary volume resides on the backup server, you must update the dictionary map file on that server.

You can use the Update Dictionary Map File dialog box to update the dictionary map file.

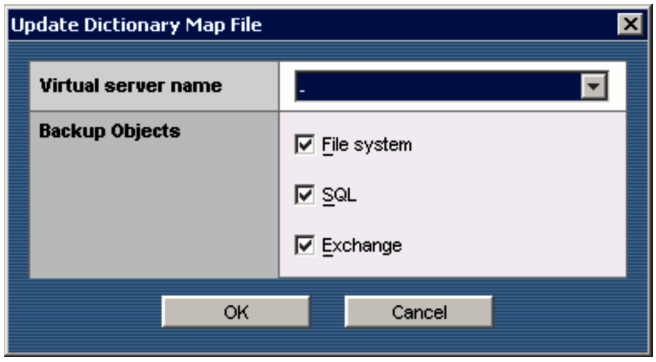


Figure 6.10 Update Dictionary Map File Dialog Box

Table 6.8 Items Displayed in the Update Dictionary Map File Dialog Box

Item name		Parameters or description
Virtual server name		Virtual server name
Backup object	File system	File system
	SQL	SQL Server database
	Exchange	Exchange database

After the update has finished, the Application View displays the latest state.

6.2 Operations for File Systems

You can use Protection Manager Console to perform the following operations for file systems.

Table 6.9 Operations for File Systems

Operation	Details
Backup See ***Notes***	Within a single storage subsystem, you can back up a file system from the primary volume to the secondary volume. Additionally, by registering a backup job, a backup operation can be executed automatically according to a specified schedule. By using a user script, you can back up to a magnetic tape a file system from the primary volume through the secondary volume. File system backups are performed from the instance of Protection Manager Console on the file server. You can specify the following options when backing up a file system: ▪ Backup Comment ▪ Generation Name (Generation identifier) ▪ Backup Mode (Cold, Online, VSS) ▪ Advanced Options (setting a user script) ▪ Job Registration (registering a backup job) For details about the options that can be specified for backup, see section 6.2.2.
Restore See ***Notes***	You can restore a file system from the secondary volume to the primary volume. File system restoration is performed from the instance of Protection Manager Console on the file server. You can specify the following option when restoring a file system. For details about the options that can be specified for restoration, see section 6.2.3.
Operations for backup jobs	You can register backup jobs, and then perform operations such as changing backup options and deleting the backup jobs. For details on backup job operations, see section 6.5.
Locking a copy group	You can lock the contents of a particular copy group. For details, see section 6.6. You can specify the 'Lock Mode' option (Lock, Unlock) when locking a copy group.
Resynchronizing a copy group	You can resynchronize a particular copy group. For details, see section 6.7.
Mounting a secondary volume	You can mount the secondary volume from the instance of Protection Manager Console on the backup server. For details, see section 6.8.1.
Unmounting a secondary volume	You can unmount the secondary volume from the instance of Protection Manager Console on the backup server. For details, see section 6.8.2.
Viewing application information	You can view application information. For details, see section 6.1.3.
Viewing catalog information	You can view catalog information. For details, see section 6.1.4.
Viewing backup job information	You can view backup job information. For details, see section 6.1.5.
Outputting application information, catalog information, or backup job information to a file	You can output the contents of the displayed application information, catalog information, and backup job information to a file (in a tab-delimited format), from the Protection Manager Console on a file server.

Notes:

- Before performing a backup or restoration, you must terminate all applications that are using the file system that is to be backed up or restored. Note that volumes being used by the OS cannot be backed up or restored.
- If the file system consists of several volumes, backup and restoration are performed for all primary volumes and their corresponding secondary volumes.
- For systems consisting of a file server and a backup server, backup operations and restore operations can only be performed from the file server.

6.2.1 Notes on Backing up Mount Points for Databases

In the Application View page, the mount points that a SQL Server or Exchange database uses are also displayed. Normally, you select an instance name to perform backup. However, you can also back up a file system by specifying the mount point name. When the database instance data is stored across multiple mount points, do not perform backup on the mount points for the database. The mount points for the database are displayed in the FS field when you display detailed information about the SQL Server or Exchange database in the Application Detail window.

6.2.2 Backup Options for File Systems

When performing a backup for a file system, you can specify either online backup or cold backup as the backup mode. You can specify the following options when performing a backup for a file system:

- **Generation Name** (name identifying the generation)

  Specify this option to back up the file system to the copy group that has the specified name identifying the generation. The name identifying the generation syntax is local/remote-identifier_generation-number. If the copy type is the volume duplication function in a subsystem (ShadowImage), local is displayed as the identifier. If the copy type is the volume duplication function between subsystems (TrueCopy or UR), remote is displayed as the identifier.

  The generation management MU# that is set for the primary volume is displayed as the generation number.

  For details about the name identifying the generation, see the *HiCommand Protection Manager User's Guide*.

- **Backup Mode**
  - **Cold** (cold backup)

    In a cold backup, the file system is unmounted, and backup is performed while the volume is offline. When backup is complete, the file system is mounted again. If the unmount operation fails, backup processing is cancelled. Backup processing is also cancelled if the volume to be backed up is already unmounted.

    When backup is performed on a server in a cluster configuration, instead of the file system being unmounted, the disk resource to be backed up is taken offline, and the volume is backed up. If the disk resource is already offline, backup processing is cancelled. Backup processing is also cancelled if the command executes, but fails to take the disk resource offline. When backup is complete, the disk resource subject to backup is brought back online.
  - **Online** (online backup)

    In an online backup, backup is performed without unmounting the file system.

    When online backup is specified, only synchronization processing is performed before backup. If you do not prevent applications using the file system from updating data, the integrity of the data that is backed up cannot be guaranteed. When performing an online backup, make sure that the directories on the volume to be backed up are not mounted on another volume.
  - **VSS**

    Specify this option to perform backup by using VSS. By default, this option is selected as the backup mode.

  Note: For both cold and online backups, the file system to be backed up must be mounted before backup.
- **Advanced Options** (setting a user script)

  If you want to use a user script to perform backup operations, click the **Pre/Post Job** button to open the Advanced Options dialog box, and then set backup options.
- **Job Registration** (registering a backup job): You can register a backup job by clicking the **Schedule** button and setting schedule options. In this case, the backup is not run immediately. For details on registering a backup job, see section 6.5.1.

6.2.3 Restoration Options for File Systems

During restoration, data is replicated in a step called resynchronization, in which the contents of the primary volume are made identical to the contents of the secondary volume. In restoration processing, the file system to be restored is unmounted, and then is mounted again once processing is complete. For a cluster configuration, the disk resource to be backed up is taken offline, and the volume is restored. Once restoration is complete, the disk resource is brought back online.

You can specify the following option when performing restoration for a file system: **Force**

Only specify this option when normal restoration cannot be performed, such as when the LDEV number has changed when the volume was switched. When you specify this option, if the name of the copy group on the primary volume, obtained when the file server was backed up, matches the information on the file server, then forced restoration is performed. In such a case, forced restoration is performed even when the LDEV number or SERIAL number does not match that from the backup. Note that if this option is specified for a normal restoration, data might be corrupted.

6.2.4 Example of Backup and Restore Operations for File Systems

The operations described in the following explanations assume a system configuration (consisting of a file server and a backup server), as shown in the following figure.

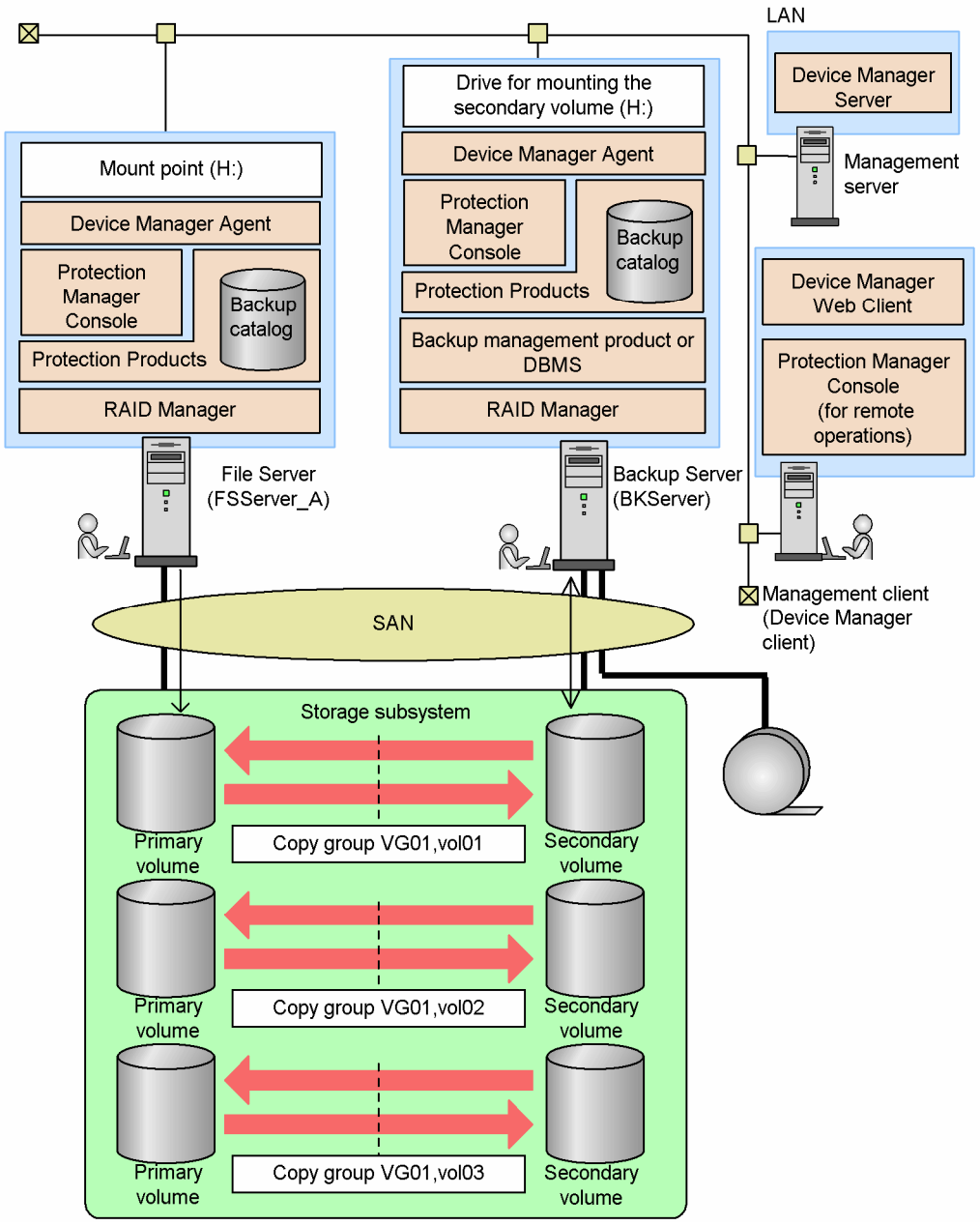


Figure 6.11 System Configuration for Backup and Restore Operations for a File System

The prerequisites for the system shown in Figure 6.11 are:

- A file server (server name: FSServer_A) and a backup server (server name: BKServer) exist.
- Primary volumes on the file server and secondary volumes on the backup server are defined as pairs to constitute a mirror configuration (use the volume replication function and RAID Manager for these settings).
- FSServer_A has the mount point H:.
- The mount point to be backed up is in the NTFS format.
- The mount point to be backed up is permanently under an ordinary split operation.
- During a cold backup, primary volumes are unmounted when the data is backed up to secondary volumes, and are therefore not accessible from the file server.

6.2.5 Backing up a File System to a Secondary Volume

This section provides sample instructions for backing up a file system from a primary volume to a secondary volume. In this example, a file system with mount point H: on FSServer_A is backed up to the secondary volume.

Note: When usual operation is in a split state, you must resynchronize the copy group before backing up data. When usual operation is in a pair state, you do not need to resynchronize the copy group before backing up the data. After the tape backup ends, resynchronize the copy group to initialize it. For details, see section 6.7.

To back up a file system:

1. Start the instance of Protection Manager Console on the file server, and click the **Application View** tab.

   The Application View is displayed. For details on the displayed items, see Table 6.2.

2. Select the file system to be backed up. Select the following rows:
   - Application: File system
   - Instance: H:

   Note: To see detailed information about the file system, in the **Application View**, click the **Show Application Detail** button. The Application Detail window is displayed, allowing you to view detailed information. For details on the displayed items, see Table 6.3.

3. In the **Application View**, click the **Backup** button.

   The Backup File system dialog box, where you can set the backup options, is displayed.

4. Set the backup options:
   - **Backup Comment**

     This registers a backup comment in the backup catalog. The backup-comment value can be a string of up to 64 bytes, consisting of alphanumeric, special, one-byte space, and multi-byte characters. The backup comment is case-sensitive.

     Note: The following special characters cannot be used for backup comments:

     `\ / ` | < > " * ? & ; ( )`

     The first character must not be a hyphen (-).
   - **Generation Name**

     This option backs up the file system to the copy group that has the specified name identifying the generation.
   - **Backup Mode**

     Sets the backup mode. To perform online backup, select the **Online** radio button, or to perform a cold backup, select the **Cold** radio button.
   - **Advanced Options**

     If you want to use a user script to perform backup operations, click the **Job Script** button to open the Advanced Options dialog box, and then set backup options. For more details, see section 6.9.2.

– **Job Registration**

To perform backup immediately without registering a backup job, do not click the **Schedule** button. To register a backup job with the contents specified thus far, see section 6.5.1

5. Click the **OK** button.

   A confirmation dialog box for executing the backup is displayed.

6. Click the **OK** button to start the backup process.

   Backup processing starts. Quitting Protection Manager Console during backup does not terminate the command processing.

   While the backup is in progress, the status is displayed in the **Progress** that shows how much of the volume has been copied. This does not represent the progress of the whole backup process. Copy progress might be displayed as progressing rather slowly near the 0% mark, as well as near the 100% mark. To confirm that all volumes are copied, check Progress.

   If you have started locally, the **Progress Detail** displays messages showing the progress of the backup process.

   When the backup is finished, a dialog box is displayed to indicate the completion of the backup (See Figure 6.12.) This dialog box contains the backup ID.

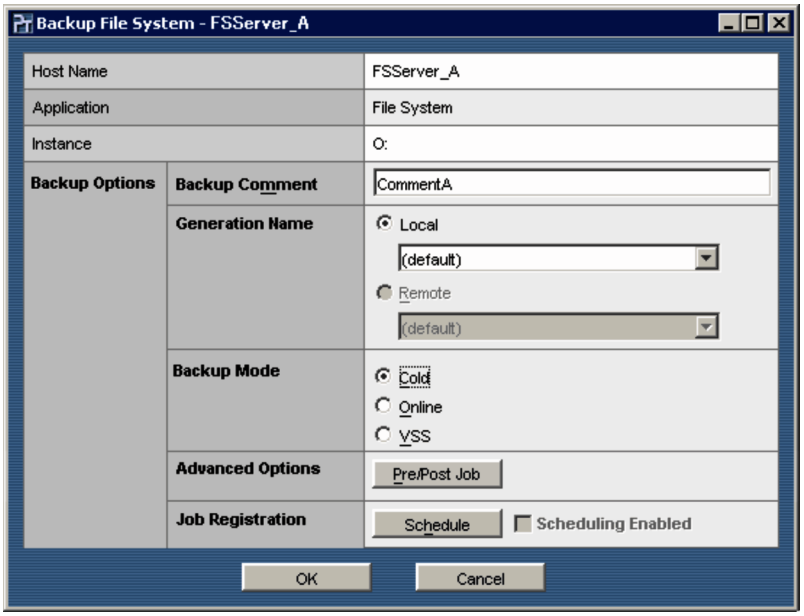


Figure 6.12 Backup File System Dialog Box

6.2.6 Backing up a File System to a Secondary Volume (When VSS is Used)

This section provides sample instructions for backing up a file system from a primary volume to a secondary volume using VSS. In this example, the file system with mount point H: on FSServer_A is backed up to the secondary volume.

Note: When usual operation is in a split state, you must resynchronize the copy group before backing up data. When usual operation is in a pair state, you do not need to resynchronize the copy group before backing up the data. After the tape backup ends, resynchronize the copy group to initialize it. For details, see section 6.7.

To back up a file system by using VSS:

1. Start the instance of Protection Manager Console on the file server, and click the **Application View** tab.

   The Application View is displayed. For details on the displayed items, see Table 6.2.

2. Select the file system to be backed up.

   Select the following rows:

   – **Application: File system**

   – **Instance: H:**

   Note: To see more detailed information about the file system, in the Application View, click the Show Application Detail button. The Application Detail window is displayed, allowing you to view detailed information. For details on the displayed items, see Table 6.3.

3. In the Application view, click the **Backup** button.

   The Backup File system dialog box, where (Figure 6.13.) you can set the backup options, is displayed.

4. Set the backup options.

   – **Backup Comment**

     Specify this to register a backup comment in the backup catalog. The backup-comment value can be a string of up to 64 bytes, consisting of alphanumeric, special, one-byte space, and multi-byte characters. The backup comment is case-sensitive.

     The following special characters cannot be used for backup comments:

     \ / ` | < > " * ? & ; ( )

     The first character must not be a hyphen (-).

   – **Generation Name**

     Specify this option to back up the file system to the copy group that has the specified name identifying the generation.

   – **Backup Mode**

     Set the backup mode. In this example, select the **VSS** radio button to perform backup by using VSS.

– **Advanced Options**

  If you want to use a user script to perform backup operations, click the **Job Script** button to open the Advanced Options dialog box, and then set backup options. For more details, see section 6.9.2.

– **Job Registration**

  To perform backup immediately without registering a backup job, do not click the **Schedule** button. To register a backup job with the contents specified thus far, see section 6.5.1.

5. Click the **OK** button.

   A confirmation dialog box for executing the backup is displayed.

6. Click the **OK** button to start the backup processing.

   Backup processing starts. Quitting Protection Manager Console during backup does not terminate the command processing.

   If you have started locally, the **Progress Detail** displays messages showing the progress of the backup processing.

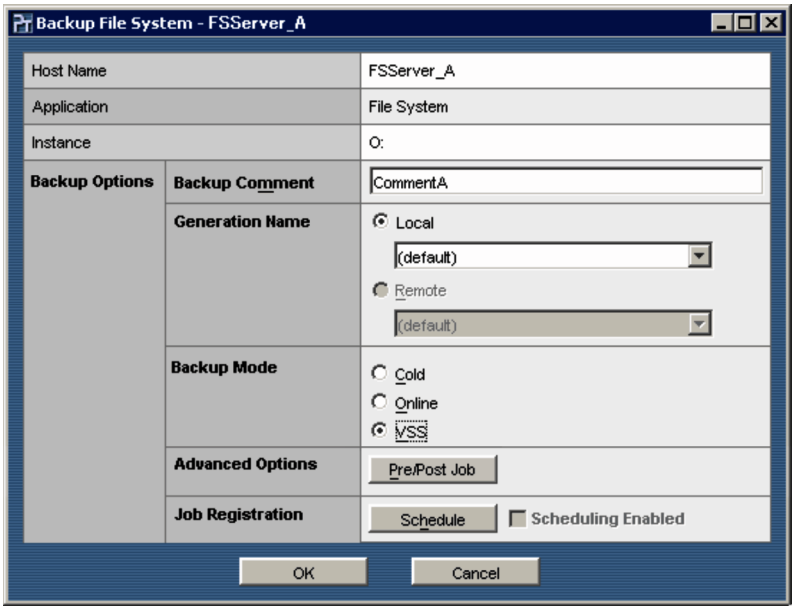


Figure 6.13 Backup File System Dialog Box (When Using VSS to Back up)

6.2.7 Restoring a File System to the Primary Volume

The file system is restored from the secondary volume to the primary volume in a step called resynchronization.

To restore a file system:

1. Start the instance of Protection Manager Console on the file server, and click the **Backup Catalog View** tab.

   The Backup Catalog View is displayed. For details on the displayed items, see Table 6.4.

2. Select the file system to be restored. According to Backup ID, Backup Time, Instance, and Comment, select the row of the file system you want to restore.

   Note: To see more detailed information about the file system, click the **Show Backup Detail Information** button in the Backup Catalog View. The Backup Detail Information window is displayed, allowing you to view detailed information.

3. Click the **Restore** button in the **Backup Catalog View**.

   The Restore File System dialog box, where you can set the restoration options, is displayed (Figure 6.14).

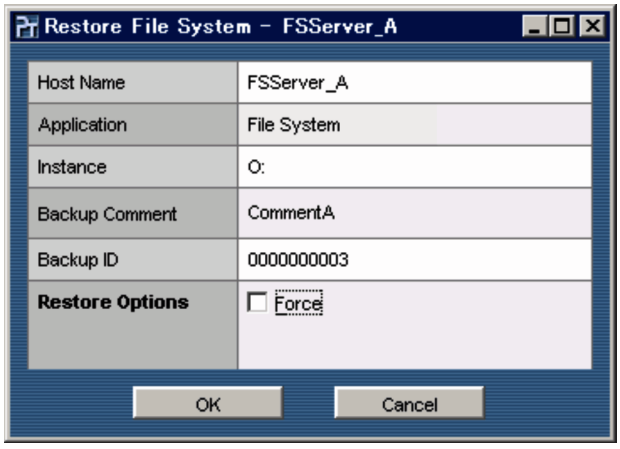


Figure 6.14 Restore File System Dialog Box

4. Set the **Force** restoration option to perform restoration to the primary volume, even if it is not the same volume from which the backup was taken.

   Note: Use this option only when normal restoration cannot be performed, such as when the LDEV number has changed when the volume was switched.

5. Click the **OK** button.

   A dialog box displays, prompting you to confirm the execution of restoration.

6. Click the **OK** button to start restoration processing.

   Restoration processing starts. Quitting Protection Manager Console during restoration does not terminate the command processing.

   While the restoration is in progress, the status is displayed in the **Progress** that shows how much of the volume has been restored. This does not represent the progress of the whole restoration processing. Copy progress might be displayed as moving rather slowly near the 0% mark, as well as near the 100% mark. To confirm that the restoration finishes, check Progress.

   If you have started locally, the **Progress Detail** displays messages showing the progress of the restoration processing.

   When the restoration is finished, a dialog box is displayed to indicate completion of the restoration.

6.3 Operations for SQL Server Databases

You can use Protection Manager Console to perform the following operations for SQL server databases.

Table 6.10 Operations for SQL Server Databases

Operation	Details
Backup See ***Notes***	Within a single storage subsystem, you can back up a SQL Server database from the primary volume to the secondary volume. This backup is performed online and the SQL Server instance must be running when backup is performed. If the specified instance is not running, backup processing will terminate abnormally. When backup is performed, a snapshot of the databases within the instance is created using the SQL Server VDI. The snapshot data (metafile) is kept in the VDI metafile storage directory, under the name backup-ID_database-ID.dmp. Additionally, by registering a backup job, a backup operation can be executed automatically according to a specified schedule. Backup for SQL Server databases is performed from the instance of Protection Manager Console on the database server. You can specify the following options when backing up a SQL Server database: ▪ Backup Comment ▪ Generation name (Generation identifier) ▪ Database (target database): All, Select Source Database (All User Databases, Select) ▪ Job Registration (registering a backup job) For details about the options that can be specified for backup, see section 6.3.1.
Restore See ***Notes***	You can restore a SQL Server database from the secondary volume to the primary volume. Restoration is performed via resynchronization (resync). The data on the primary volume is overwritten by the disk image of the secondary volume when backup operations are performed. Therefore, any data updated or created after backup is invalid. When you restore an SQL Server system database (master, model, msdb, or distribution), to recover the system database, temporarily stop the SQL Server service on which restoration operations are to be performed. For this reason, temporarily, you cannot access the database on which restoration operations are to be performed. Do not connect to the SQL Server during restoration. SQL Server database restoration is performed from the instance of Protection Manager Console on the database server. You can specify the following options when restoring a SQL Server database: ▪ Source Database: All, Select ▪ Target Instance: Recovery to a different instance ▪ Resync Mode: Resync, No Resync ▪ Force ▪ Undo ▪ Check host name For details about the options that can be specified for restoration, see section 6.3.2.
Operations for backup jobs	You can register backup jobs, and then perform operations such as changing backup options and deleting the backup jobs. For details on backup job operations, see section 6.5.

Operation	Details
Locking a copy group	You can lock the contents of a particular copy group. For details, see section 6.6. You can specify the 'Lock Mode' option (Lock, Unlock) when locking a copy group.
Resynchronizing a copy group	You can resynchronize a particular copy group. For details, see section 6.7.
Mounting a secondary volume	You can mount the secondary volume from the instance of Protection Manager Console on the backup server. For details, see section 6.8.1.
Unmounting a secondary volume	You can unmount the secondary volume from the instance of Protection Manager Console on the backup server. For details, see section 6.8.2.
Viewing application information	You can view application information. For details, see section 6.1.3.
Viewing catalog information	You can view catalog information. For details, see section 6.1.4.
Viewing backup job information	You can view backup job information. For details, see section 6.1.5.
Outputting application information, catalog information, or backup job information to a file	You can output the contents displayed for application information, catalog information, and backup job information to a file (in a tab-delimited format), from the instance of Protection Manager Console on the database server.

Notes:

- If the data files, various types of databases, and other objects belonging to the database instance exist across multiple volumes, backup and restoration are performed between all primary volumes and their corresponding secondary volumes.
- For systems consisting of a database server and a backup server, backup operations and restore operations can only be performed from the database server.
- With Protection Manager Console, backup and restoration can only be performed for data files. To back up and restore transaction logs, use the commands instead. For details about using commands to perform backup and restoration, see the *HiCommand Protection Manager User's Guide*. For details about the commands themselves, see the *HiCommand Protection Manager Command Reference*.

6.3.1 Backup Options for SQL Server Databases

You can specify the following options when performing backup for a SQL Server database:

- **Generation Name** (Generation identifier)

  Specify this option to back up the file system to the copy group having the specified name identifying the generation. The name identifying the generation syntax is local/remote-identifier_generation-number. If the copy type is the volume duplication function in a subsystem (ShadowImage), local is displayed as the identifier. If the copy type is the volume duplication function between subsystems (TrueCopy or UR), remote is displayed as the identifier.

  The generation management MU# that is set for the primary volume is displayed as the generation number.

  For details about the name identifying the generation, see the *HiCommand Protection Manager User's Guide*.

- **Database** (target database)

  Specify this to back up a target database. If you back up a system database, the target database will be temporarily inaccessible, because the SQL Server temporarily stops when backup is performed.

  - All (all databases)

    Specify this to back up all databases, including system databases.

  - Select Source Database (select the target database)

    Specify this to select the target database for backup. If you want to back up all user databases, select All User Databases. If you want to back up only specific databases, choose Select and then the target databases. When you choose the target databases, specify all databases stored on the logical volume. If you do not specify all databases, backup will fail.

  - **Advanced Options** (setting a user script)

    If you want to use a user script to perform backup operations, click the **Pre/Post** Job button to open the Advanced Options dialog box, and then set backup options.

- **Job Registration** (registering a backup job)

  You can register a backup job by clicking the **Schedule** button and setting schedule options. In this case, the backup is not run immediately. For details on registering a backup job, see section 6.5.1.

6.3.2 Restoration Options for SQL Server Databases

You can specify the following options when performing a restoration for a SQL Server database:

- **Source Database**

  When restoring only a specific user database from the backed up user databases, select the database to restore from the list.

- **Target Instance** (for a recovery to a different instance)

  If you cannot specify the same SQL Server instance name for the restoration destination database as the one specified as the backup source, you can restore (recover) the data to a SQL Server instance other than the backup source. Select an instance name for the restoration destination from the registered instance names displayed in the combo box. For details on how to recover the data to a different instance, see the *HiCommand Protection Manager User's Guide*.

- **Resync Mode (Resync mode)**
  - Resync

    Performs restoration in a step called resynchronization, from the secondary volume to the primary volume. This makes the contents of the primary volume identical to those of the secondary volume. Restoration is performed with the target database detached. Once restoration is complete, the target database is attached, and then the instance is started.

    For cluster configurations, the resource and disk resource containing the backed up database are taken offline, and the volume is restored. Once restoration is complete, the disk resource is brought back online, and then the cluster resource containing the database is brought back online.

  - No Resync

    Performs restoration of only the metafiles for the data on the primary volume, without performing restoration processing from the secondary volume to the primary volume. Use this option when restoration cannot be performed with the Resync option specified, in cases such as when the disk is corrupted, and restoration cannot be performed directly from tape to the primary volume.

- **Force**

  Only specify this option when normal restoration cannot be performed, such as when the LDEV number has changed when the volume was switched. You can select this option only when Resync is selected for the Resync mode. When you specify this option, if the name of the copy group on the primary volume, obtained when the database server was backed up, matches the information on the database server, then forced restoration is performed. In such a case, forced restoration is performed even when the LDEV number or SERIAL number does not match that from the backup. Note that if this option is specified for a normal restoration, data might be corrupted.

- **Undo**

  Specify this option to restore the database in standby mode. This will allow the database to be used as a read-only database, once restoration is complete. Also, a temporary file for each database will be created in the UNDO file directory.

  If this option is omitted, normal restoration is performed. In this case, once restoration is complete, the database will be placed in loading status, and cannot be used.

- **Check host name**

  Specify this to perform restoration to a host other than the one that was backed up, when either the host name has changed, or when using the log distribution function of Microsoft SQL Server 2000 Enterprise Edition or SQL Server 2005.

  Note: When specifying this option, since the integrity of the host name in the backup catalog is not checked during restoration, be careful not to perform restoration for the wrong host.

6.3.3 Example of Backup and Restore Operations for a SQL Server Database

The operations described in the following explanations are based on a system configuration consisting of a database server and a backup server, as shown in Figure 6.15.

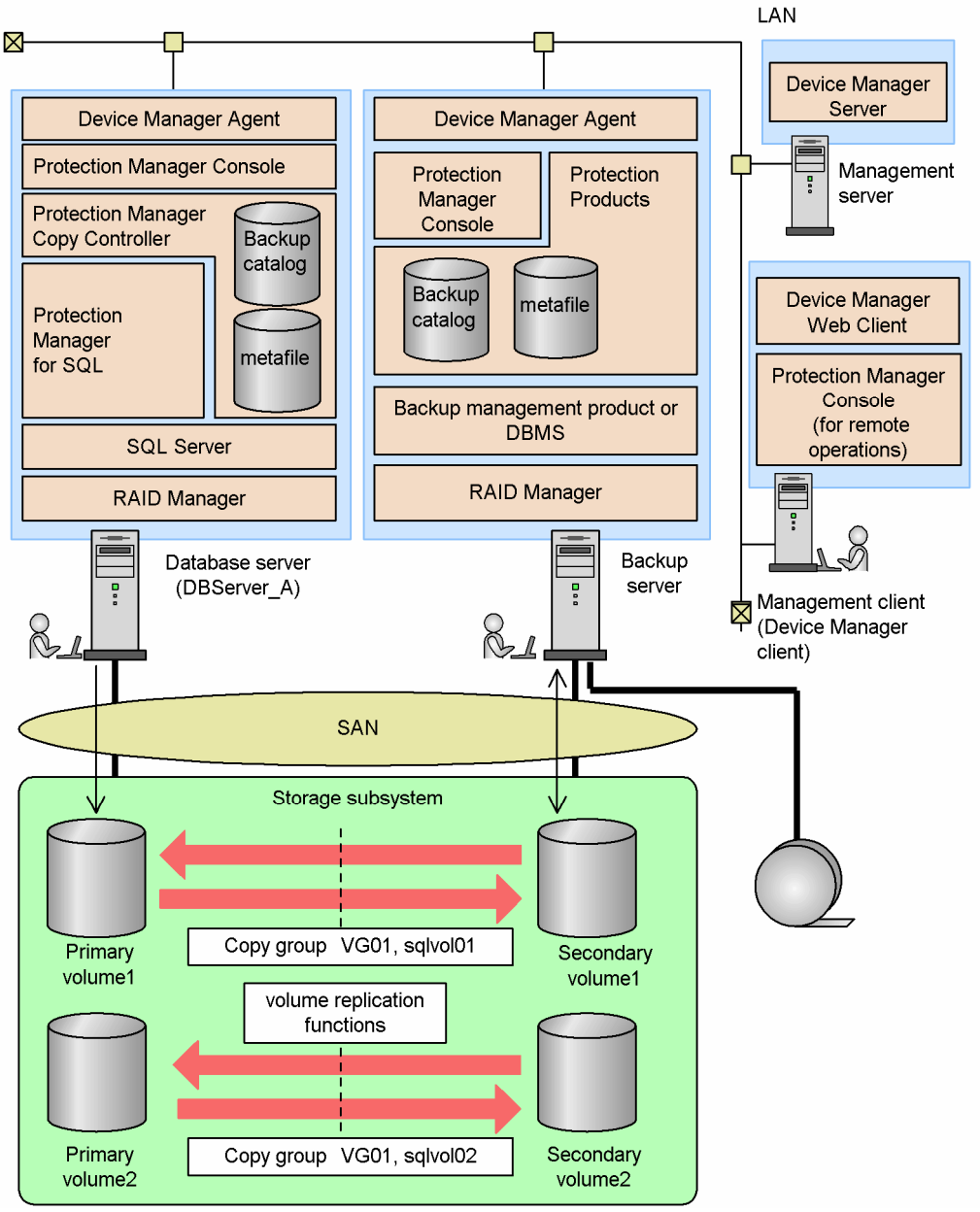


Figure 6.15 System Configuration for Backup and Restore Operations for a SQL Server Database

The prerequisites for the system in the operation example are as follows:

- The primary volume is in NTFS format. Note that volumes for database files being used as databases for SQL Server cannot be shared with the volumes used for logging.
- Primary volumes on the file server and secondary volumes on the backup server are defined as pairs, constituting a mirror configuration (use the volume replication function and RAID Manager for these settings).
- Data for which an online backup was performed from a primary volume to a secondary volume has been backed up to tape.
- A single instance default exists on database server A (server name: DBServer_A), and a service has been started.
- The instance to be backed up is under ordinary split operation.
- The VDI metafile storage directory is created on the database server and backup server.

6.3.4 Backing up a SQL Server Database to a Secondary Volume

This section provides sample instructions for backing up a SQL Server database from a primary volume to a secondary volume. In this example, the database instance default of a database server DBServer_A is backed up to the secondary volume.

Note: When usual operation is in a split state, you must resynchronize the copy group before backing up data. When usual operation is in a pair state, you do not need to resynchronize the copy group before backing up the data. After the tape backup ends, resynchronize the copy group to initialize it. For details on how to do this, see section 6.7.

To back up a SQL Server database:

1. Start Protection Manager Console, and click the **Application View** tab.

   The Application View is displayed. For details on the displayed items, see Table 6.2.

2. Select the SQL Server database instance to be backed up. Select the following rows:
   - Application: SQL Server
   - Instance: default

   Note: To see more information about the file system, in the **Application View**, click the **Show Application Detail** button. The Application Detail window is displayed, allowing you to view detailed information. For details on the displayed items, see Table 6.3.

3. In the Application View, click the **Backup** button.

   The Backup SQL dialog box is displayed. Set the backup options in the Backup SQL dialog box.

4. Set the backup options:
   - **Backup Comment**

     Specify this to register a backup comment in the backup catalog. The backup-comment value can be a string of up to 64 bytes, consisting of alphanumeric, special, one-byte space, and multi-byte characters. The backup comment is case-sensitive.

     Note: The following special characters cannot be used for backup comments:

     \ / ` | < > " * ? & ; ( )

     The first character must not be a hyphen (-).

   - **Database**

     Specify the target database. To back up all databases including the system database, select the **All** radio button. To specify the database to be backed up, select the **Select Source Database** radio button, and then select the database to be backed up. To back up all user databases, select the **All User Databases** radio button. To back up only a specific database, choose the **Select** radio button, and then select the database to be backed up.

   - **Advanced Options**

     If you want to use a user script to perform backup operations, click the **Job Script** button to open the Advanced Options dialog box, and then set backup options. For more details, see section 6.9.2.

– **Job Registration**

To perform backup immediately without registering a backup job, do not click the **Schedule** button. To register a backup job with the contents specified thus far, see section 6.5.1.

5. Click the **OK** button.

   A confirmation dialog box for executing the backup is displayed.

6. Click the **OK** button to start the backup process.

   Backup processing starts. Quitting Protection Manager Console during backup does not terminate the command processing. While the backup is in progress, the status is displayed in the **Progress** that shows how much of the volume has been copied. This does not represent the progress of the whole backup process. Copy progress might be displayed as progressing rather slowly near the 0% mark, as well as near the 100% mark. Use the copy progress status display for reference.

   If you have started locally, the **Progress Detail** displays messages showing the progress of the backup process.

   When the backup is finished, a dialog box is displayed to indicate the completion of the backup. The backup ID is displayed in this dialog box.

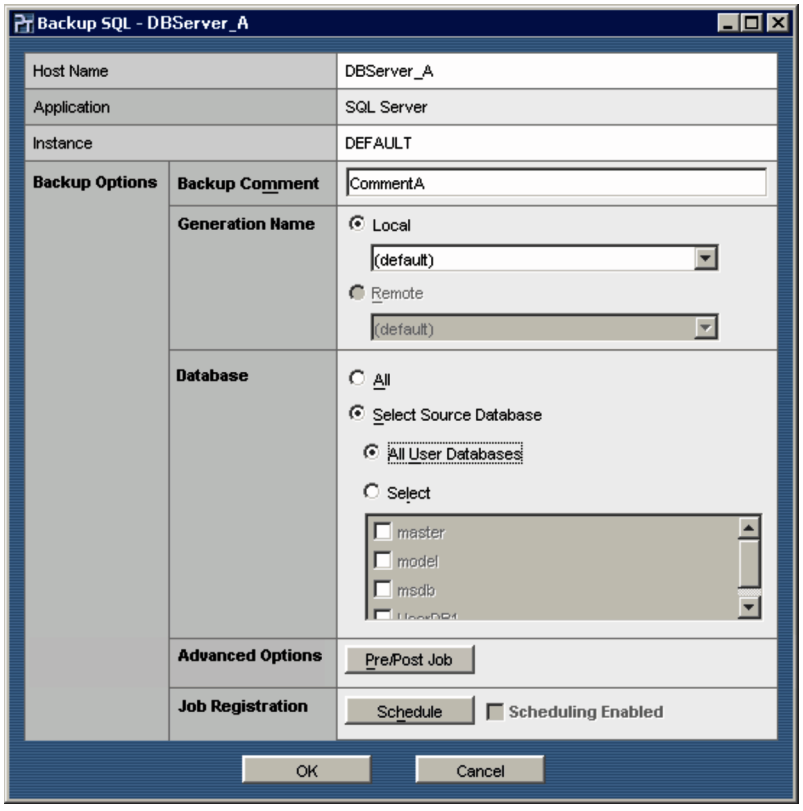


Figure 6.16 Backup SQL Dialog Box

6.3.5 Restoring a SQL Server Database to the Primary Volume

Please review the following notes before performing the restoration procedure:

- If the drive name of the SQL Server database is not the same as the drive name during backup, the command will fail. Before performing restore operations, view the detailed information for the application and check the drive name for the restoration target.
- You cannot perform recovery operations from Protection Manager Console. Use the `drmsqlrecover` command or the `drmsqlrecovertool` command to perform recovery. For details on these commands, see the *HiCommand Protection Manager User's Guide* and the *HiCommand Protection Manager Command Reference*.
- When you restore a SQL Server database whose name has been changed, detach the SQL Server database on which the restore operations are to be performed. If the SQL Server database is not detached and is restored, restore operations will fail and the target SQL Server database might become unusable. If the SQL Server database cannot be used, detach the database and then re-execute the restore operations.

To restore a SQL Server database from the secondary volume to the primary volume:

1. Start Protection Manager Console, and click the **Backup Catalog View** tab.

   The Backup Catalog View is displayed. For details on the displayed items, see Table 6.4.

2. Select the SQL Server database instance to be restored. Based on the Backup ID, Backup Time, Instance, and Comment, select the row of the database you want to restore.

   Note: To see detailed information about the SQL Server database instance, in the Backup Catalog View, click the **Show Backup Detail Information** button. The Backup Detail Information window is displayed, allowing you to view detailed information.

3. Click the **Restore** button in the **Backup Catalog** View.
   The Restore SQL dialog box, where you can set the restoration options, is displayed.

4. Set the restoration options:

   - **Source Database**

     To restore all user databases, select the **All** radio button. To restore only a specific user database, select the **Select** radio button, and then select the user database from the list box. Databases that were specified for backup will be displayed in the list box.
     When you choose the target databases, specify all databases stored on the logical volume. If you do not specify all databases, restore operations will fail.

   - **Target Instance**

     To restore the data to an SQL Server instance that has a different name than the backup source, select the desired instance name from the registered instance names displayed in the combo box.

– **Resync Mode**

To perform restoration in Resync mode, select the **Resync** radio button. To perform restoration in No Resync mode, select the **No Resync** radio button.
When performing restoration in Resync mode, select the **Force** check box to perform restoration to the primary volume, even if it is not the same volume for which the backup was taken.

– **Force**

When you have selected the **Resync** radio button for the **Resync Mode** option, if you want to restore to a primary volume, even if it is not the same volume for which the backup was taken, select the **Force** check box. Use this option only when normal restoration cannot be performed, such as when the LDEV number has changed when the volume was switched.

– **Undo**

Select the Undo check box to restore the database in standby mode. When you restore the database with the Undo option specified, the database is restored in standby mode (read-only mode). This allows you to view the contents of the database. In contrast, when you restore the database without specifying the Undo option, the database is placed in loading status and you cannot view its contents.

When you want to check the contents of the restored database before performing recovery, specify the Undo option.

– **Check host name**

Select the Check host name check box to check the name of the host.

5. Click the **OK** button.

   A dialog box prompting you to confirm the execution of restoration is displayed.

6. Click the **OK** button to start restoration processing.

   Restoration processing starts. Quitting Protection Manager Console during restoration does not terminate the command processing. While the restoration is in progress, the status is displayed in the **Progress** that shows how much of the volume has been restored. This does not represent the progress of the whole restoration processing. Copy progress might be displayed as progressing rather slowly near the 0% mark, as well as near the 100% mark. Use the copy progress status display for reference.

   If you have started locally, the **Progress Detail** displays messages showing the progress of the restoration processing.

   When the restoration is finished, a dialog box is displayed to indicate completion of the restoration.

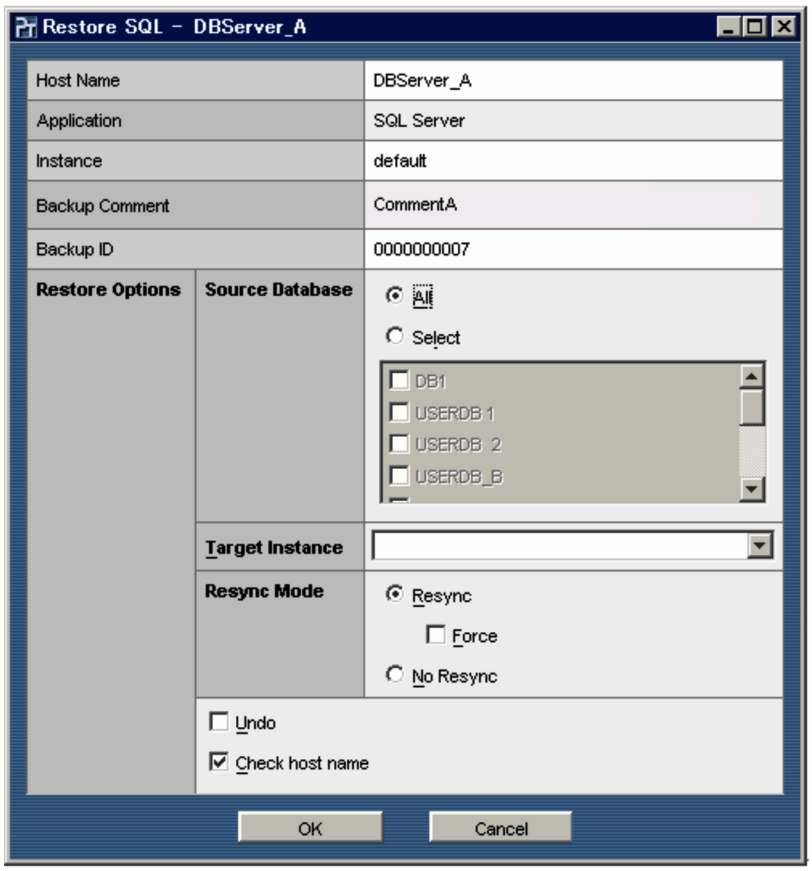


Figure 6.17 Restore SQL Dialog Box

6.4 Operations for Exchange Databases

You can use Protection Manager Console to perform the following operations for Exchange databases.

Table 6.11 Operations for Exchange Databases

Operation	Details
Backup See ***Note***	Within a single storage subsystem, you can back up an Exchange database from the primary volume to the secondary volume. Backup can be performed on either a whole database or on storage group units. Back up the whole database for Exchange 2000 Server and Exchange Server 2003 Standard Edition. For Exchange 2000 Enterprise Server, Exchange Server 2003 Enterprise Edition, and Exchange Server 2007, either back up the whole database, or back it up in storage group units. Additionally, by registering a backup job, a backup operation can be executed automatically according to a specified schedule. Backup for Exchange databases is performed from the instance of Protection Manager Console on the database server. You can specify the following options when backing up an Exchange database: ▪ Backup comment ▪ Generation Name (Generation identifier) ▪ Backup mode: Cold, Online, VSS ▪ Truncate Transaction Log ▪ Cluster Option: Offline, Online ▪ Source Storage Group: All, Select ▪ Eventlog checking before backup (checking event log data) ▪ Advanced Options (setting a user script) ▪ Job Registration (registering a backup job) For details about the options that can be specified for backup, see section 6.4.1.
Restore See ***Note***	You can restore an Exchange database from the primary volume to the secondary volume. Restoration can be performed on a whole database, on storage group units, or on information store units. During restoration, data is replicated in a step called resynchronization, in which the contents of the primary volume are made identical to the contents of the secondary volume. In restoration processing, the file system to be restored is unmounted, and then is mounted again once processing is complete. For a cluster configuration, the disk resource to be backed up is taken offline, and the volume is restored. Once restoration is complete, the disk resource is brought back online. Exchange database restoration is performed from Protection Manager Console on the database server. You can specify the following options when restoring an Exchange database: ▪ **Source Storage Group / Information Store**: All, Select ▪ Roll Forward ▪ Force For details about the options that can be specified for restoration, see section 6.4.2.
Operations for backup jobs	You can register backup jobs, and then perform operations such as changing backup options and deleting the backup jobs. For details on backup job operations, see section 6.5.
Locking a copy group	You can lock the contents of a particular copy group. For details, see section 6.6. You can specify the 'Lock Mode' option (Lock, Unlock) when locking a copy group.

Operation	Details
Resynchronizing a copy group	You can resynchronize a particular copy group. For details, see section 6.7.
Mounting a secondary volume	You can mount the secondary volume from the instance of Protection Manager Console on the backup server. For details, see section 6.8.1.
Unmounting a secondary volume	You can unmount the secondary volume from the instance of Protection Manager Console on the backup server. For details, see section 6.8.2.
Viewing application information	You can view application information. For details, see section 6.1.3.
Viewing catalog information	You can view catalog information. For details, see section 6.1.4.
Viewing backup job information	You can view backup job information. For details, see section 6.1.5.
Outputting application information, catalog information, or backup job information to a file	You can output the contents displayed for application information, catalog information, and backup job information to a file (in a tab-delimited format), from the instance of Protection Manager Console on the database server.

Note: For systems consisting of a database server and a backup server, backup operations and restore operations can only be performed from the database server.

6.4.1 Backup Options for Exchange Databases

You can specify the options shown below when performing a backup for an Exchange database.

Protection Manager Console cannot identify the type of Exchange Server product in use. Because of this, if you specify an option that is not supported by a specific Exchange Server, a command error might occur in Protection Manager Copy Controller.

- **Generation Name** (Generation identifier)

  Specify this option to back up the file system to the copy group that has the specified name identifying the generation. The name identifying the generation syntax is local/remote-identifier_generation-number". If the copy type is the volume duplication function in a subsystem (ShadowImage), local is displayed as the identifier. If the copy type is the volume duplication function between subsystems (TrueCopy or UR), remote is displayed as the identifier.

  The generation management MU# that is set for the primary volume is displayed as the generation number.

  For details about the name identifying the generation, see the *HiCommand Protection Manager User's Guide*.

- **Backup Mode**

  For Exchange 2000 Server or Exchange 2000 Enterprise Server, you can specify **Cold** or **Online**. For Exchange Server 2007, you can specify **VSS** only.

  - Cold

    Specify this option to perform a cold backup by using Protection Manager for Exchange (2000/2003 version). With this option specified, data files in Information Store (`*.edb` and `*.stm`), checkpoint files (`*.chk`), and transaction log files (`*.log`) are backed up. In a cold backup, Information Store and disk drives are unmounted before the backup process, and are mounted again after the process has completed.

    Because Information Store is unmounted, it is not accessible until the cold backup has completed.

  - Online

    Specify this option to perform an online backup by using Protection Manager for Exchange (2000/2003 version). When this option is specified, data files in Information Store (*.edb and *.stm), check point files (*.chk), and transaction log files (*.log) are backed up. In an online backup, backup is performed without unmounting Information Store and disk drives.

    When performing online backup, make sure that no other volume is mounted on the directories of the volume to be backed up.

    In online backup, a backup is obtained by performing forced copying of the primary volume contents to the secondary volume, without unmounting Information Store. If the online backup is obtained while a database is being updated, there is a risk that the backup's integrity might be compromised and its restoration might fail. Thus, if you want to perform online backup, confirm that there is reliable backup data available that was obtained by performing cold backup prior to online backup.

- VSS

  Specify this to perform backup with VSS. The target Exchange database to be backed up is Exchange Server 2003 or Exchange Server 2007. With this option specified, data files in Information Store (*.edb and *.stm#), checkpoint files (*.chk), and transaction log files (*.log) are backed up.

  The differences as compared to the online backup mode are that the VSS is able to use the Truncate Transaction Log option, that VSS can create only one backup generation, and that VSS cannot be used in a cluster environment.

  By default, VSS is selected for **Backup Mode**.

  # In Exchange Server 2007, data files in Information Store (`*.stm`) do not exist.

- **Truncate Transaction Log**

  Select the **Truncate Transaction Log** check box to delete the committed transaction log (the one committed to the database) after completing the backup. Deleting the transaction log file frees disk space. This option cannot be selected for the online backup mode.

  This option can be specified for cold backup or VSS backup. When the backup mode is cold backup and circular logging is in use, this option is ignored. For details on circular logging, see the Exchange Server manual.

  This option cannot be selected when circular logging is in use.

- **Cluster Option**

  Specify whether to take the cluster resources offline, or to keep them online to perform backup in a cluster environment. This option can only be selected for cold backup mode.

  - Offline

    Specify this option to take the cluster resources on physical disks offline for backup.

  - Online

    Specify this option to keep the cluster resources on physical disks online for backup.

- **Source Storage Group**

  When backing up a specific storage group, select it from a list of storage groups. Backup is performed by physical volume (LU) units. When there are multiple storage groups on one physical volume (LU), specify all storage groups. When you choose the target storage groups, specify all storage groups stored on the logical volume. If you do not specify all storage groups, backup will fail. You cannot specify this option if you are using Exchange 2000 Server.

- **Eventlog checking before backup**

  Specify this option to retrieve the event log data of Exchange 2000 Server, Exchange 2000 Enterprise Server, or Exchange Server 2003 to check whether an event indicating that a database is corrupted has been recorded. Specify this option when using Protection Manager for Exchange (2000/2003 version). You cannot specify this option when Protection Manager for Exchange 2007 is being used.

The target event log files to be retrieved are ones that were recorded after the last backup for the Exchange database. If the result of the previous backup does not exist, all the recorded event log data is retrieved. Retrieval of event log data is performed before resynchronizing a pair. If an event indicating a corrupted database is detected, the backup processing terminates with an error.

Protection Products determine that the database is corrupt when the following event is detected:

- Event category: Application
- Type: Error
- Source: ESE
- Event ID: No limitation
- Character string being included: "−1018", "−1019", or "−1022"

- **Advanced Options** (setting a user script)

  If you want to use a user script to perform backup operations, click the **Pre/Post Job** button to open the Advanced Options dialog box, and then set backup options.

- **Job Registration** (registering a backup job)

  You can register a backup job by clicking the **Schedule** button and setting schedule options. In this case, the backup is not run immediately. For details on registering a backup job, see section 6.5.1.

6.4.2 Restoration Options for Exchange Databases

You can specify the options shown below when performing a restoration for an Exchange database.

Protection Manager Console cannot identify the type of Exchange Server product in use. Because of this, if you specify an option that is not supported by a specific Exchange Server, a command error might occur in Protection Manager Copy Controller.

- **Source Storage Group / Information Store** (target storage group or information store)

  When restoring specific storage groups or information stores, specify the objects to be restored from the **Source Storage Group / Information Store** list. If you restore in units of information stores, the following conditions must be met:

  - **VSS** is selected for **Backup Mode** when backup is performed.
  - **Roll Forward** is selected when restoration is performed.

  For details on the procedure when restoration is performed in units of information stores, see the *HiCommand Protection Manager User's Guide*. This option is available for Exchange Server 2003 or Exchange Server 2007 only.

- **Roll Forward (recovery)**

  Specify this option to perform a roll forward recovery. Transaction logs subsequent to the backup are committed during the restoration process, and the database will be restored to the most recent status. However, to perform a roll forward recovery, all the transaction logs, from when the backup was performed through to when Roll Forward is executed, must be stored normally on the Exchange Server.

  The Roll Forward check box is selected by default. If this check box is cleared, the database is restored to the state it was when the backup was obtained.

- **Force**

  Only specify this option when normal restoration cannot be performed, such as when the LDEV number has changed when the volume was switched. When you specify this option, if the name of the copy group on the primary volume, obtained when the database server was backed up, matches the information on the database server, then forced restoration is performed. In such a case, forced restoration is performed even when the LDEV number or SERIAL number does not match that from the backup. Note that if this option is specified for a normal restoration, data might be corrupted.

6.4.3 Example of Backup and Restore Operations for an Exchange Database

The operations described in the following explanations are based on a system configuration consisting of a database server and a backup server, as shown in the following figure.

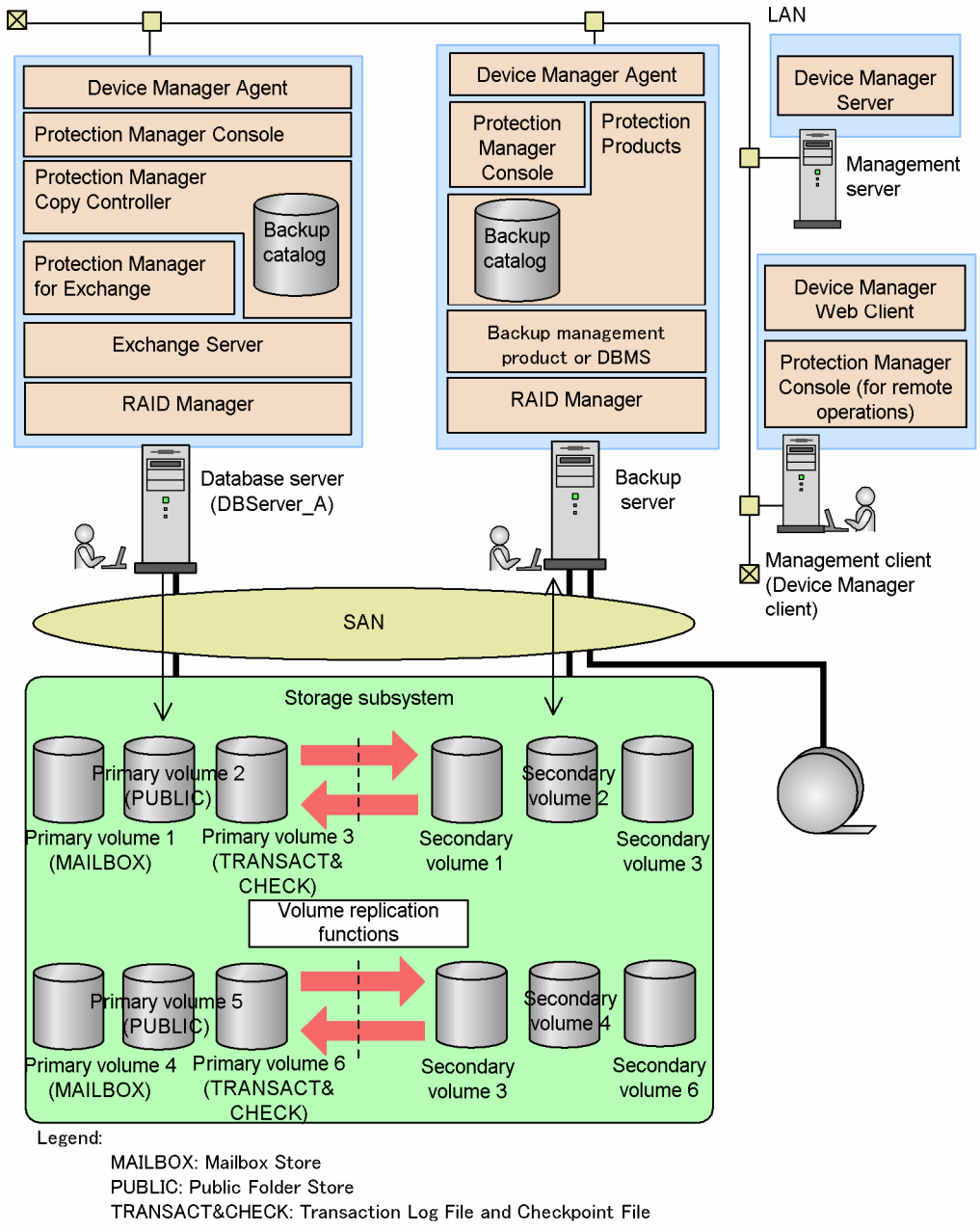


Figure 6.18 System Configuration for Backup and Restore Operations for an Exchange Database

The prerequisites for the system shown in Figure 6.18 are:

- The primary volumes are in NTFS format.
- Primary volumes and secondary volumes are defined as pairs, constituting a mirror configuration on the database server and backup server (use the volume replication function and RAID Manager for these settings).
- The Exchange Server used in the system is Exchange Server 2003 Enterprise Server.
- There are two storage groups STR1 and STR2 on the database server A (server name: DBServer_A), and the service is active.
- Storage groups to be backed up are under ordinary split operation.

The prerequisites for the locations of volumes and files are as follows:

- Information Store and transaction logs are stored in separate volumes.
- The configuration of primary volumes and secondary volumes are noted in Table 6.12.

Table 6.12 Configuration of Primary Volumes and Secondary Volumes

Primary Volume (drive to mount)	Objects to Store	Secondary Volume (drive to mount)
Primary volume 1 (D:)	Mail box store for a storage group STR1.	Secondary volume 1 (U:)
Primary volume 2 (E:)	Public folder store for a storage group STR1.	Secondary volume 2 (V:)
Primary volume 3 (F:)	Transaction log file and check point file for a storage group STR1.	Secondary volume 3 (W:)
Primary volume 4 (G:)	Mail box store for a storage group STR2.	Secondary volume 4 (X:)
Primary volume 5 (H:)	Public folder store for a storage group STR2.	Secondary volume 5 (Y:)
Primary volume 6 (I:)	Transaction log file and check point file for a storage group STR2.	Secondary volume 6 (Z:)

6.4.4 Backing up Storage Groups to a Secondary Volume (for Cold Backup)

This subsection describes an example of using Protection Manager for Exchange (2000/2003 version) to perform, from a primary volume to a secondary volume, a cold backup of storage groups in an Exchange database . In this example, storage groups STR1 and STR2 in a database server DBSServer_A are backed up on the secondary volume.

Note: When usual operation is in a split state, you must resynchronize the copy group before backing up data. When usual operation is in a pair state, you do not need to resynchronize the copy group before backing up the data. After the tape backup ends, resynchronize the copy group to initialize it. For details on how to do this, see section 6.7.

To back up storage groups:

1. Start the instance of Protection Manager Console on the database server, and click the **Application View** tab.

   The Application View is displayed. For details on the displayed items, see Table 6.2.

2. Select the Exchange database instance to be backed up. Select the following rows:
   - Application: Exchange
   - Instance: Storage Groups

   Note: To see detailed information about the Exchange database instance, in the **Application View**, click the **Show Application Detail** button. The Application Detail window is displayed, allowing you to view detailed information. For details on the displayed items, see Table 6.3.

3. In the **Application View**, click the **Backup** button.

   The Backup Exchange dialog box, where you can set the backup options, is displayed.

4. Set the backup options:
   - **Backup Comment**

     Specify this to register a backup comment in the backup catalog. The backup-comment value can be a string of up to 64 bytes, consisting of alphanumeric, special, one-byte space, and multi-byte characters. The backup comment is case-sensitive.

     The following special characters cannot be used for backup comments:

     \ / ` | < > " * ? & ; ( )

     The first character must not be a hyphen (-).
   - **Generation Name**

     Specify this option to back up the file system to the copy group that has the specified name identifying the generation.
   - **Backup Mode**

     Set the backup mode. For this example, select the **Cold** radio button to perform cold backup.

- **Truncate Transaction Log**

  Select the check box to delete committed transaction logs (committed to the database) at the completion of backup.

- **Cluster Option**

  Set the cluster option. Select the **Offline** radio button to take the cluster resources on a physical disk offline for backup; select the **Online** radio button to keep the cluster resources on a physical disk online for backup.

- **Source Storage Group**

  Select storage groups to back up. Select the **All** radio button to backup all storage groups of the Exchange database instance. Select the **Select** radio button to backup specific storage groups only, and then select the storage groups to back up from the list box.

  Specified storage groups are to be backed up in this example, so select the **Select** radio button, and select the storage groups **STR1** and **STR2** from the list box.

- **Eventlog checking before backup**

  Select the check box for this option to retrieve the event log data of Exchange 2000 Server, Exchange 2000 Enterprise Server, or Exchange Server 2003 to check whether an event indicating that a database is corrupted has been recorded.

- **Advanced Options**

  If you want to use a user script to perform backup operations, click the **Job Script** button to open the Advanced Options dialog box, and then set backup options. For more details, see section 6.9.2.

- **Job Registration**

  To perform backup immediately without registering a backup job, do not click the **Schedule** button. To register a backup job with the contents specified thus far, see section 6.5.1.

5. Click the **OK** button.

   A confirmation dialog box for executing the backup is displayed.

6. Click the **OK** button to start the backup process.

   Backup processing starts. Quitting Protection Manager Console during backup does not terminate the command processing.

   While the backup is in progress, the status is displayed in the **Progress** that shows how much of the volume has been copied. This does not represent the progress of the whole backup process. Copy progress might be displayed as progressing rather slowly near the 0% mark, as well as near the 100% mark. Use the copy progress status display for reference.

   If you have started locally, the **Progress Detail** displays messages showing the progress of the backup process.

   When the backup is finished, a dialog box is displayed to indicate completion of the backup. The backup ID is displayed in this dialog box.

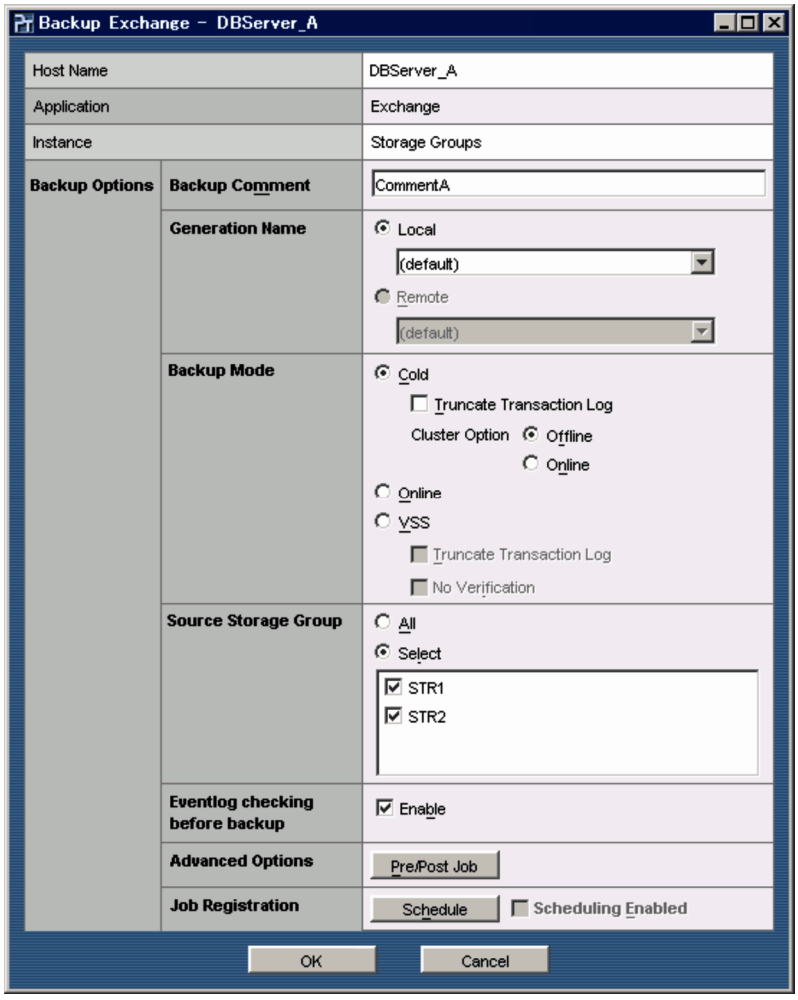


Figure 6.19 Backup Exchange Dialog Box (for Cold Backup)

6.4.5 Backing up a Storage Group to a Secondary Volume (for Online Backup)

This subsection describes an example of using Protection Manager for Exchange (2000/2003 version) to perform, from a primary volume to a secondary volume, an online backup on storage groups on an Exchange database. In this example, storage groups STR1 and STR2 in a database server DBServer_A are backed up on the secondary volume.

Note: When usual operation is in a split state, you must resynchronize the copy group before backing up data. When usual operation is in a pair state, you do not need to resynchronize the copy group before backing up the data. After the tape backup ends, resynchronize the copy group to initialize it. For details on how to do this, see section 6.7.

To back up storage groups:

1. Start the instance of Protection Manager Console on the database server, and click the **Application View** tab.

   The Application View is displayed. For details on the displayed items, see Table 6.2.

2. Select the Exchange database instance to be backed up. Select the following rows:
   - Application: Exchange
   - Instance: Storage Groups

   Note: To see more detailed information about the Exchange database instance, in the **Application View**, click the **Show Application Detail** button. The Application Detail window is displayed, allowing you to view detailed information. For details on the displayed items, see Table 6.3.

3. In the **Application View**, click the **Backup** button.

   The Backup Exchange dialog box, where you can set the backup options, is displayed.

4. Set the backup options:
   - **Backup Comment**

     Specify this to register a backup comment in the backup catalog. The backup-comment value can be a string of up to 64 bytes, consisting of alphanumeric, special, one-byte space, and multi-byte characters. The backup comment is case-sensitive.

     The following special characters cannot be used for backup comments:

     \ / ` | < > " * ? & ; ( )

     The first character must not be a hyphen (-).
   - **Generation Name**

     Specify this option to back up the file system to the copy group that has the specified name identifying the generation.
   - **Backup Mode**

     Set the backup mode. For this example, select the **Online** radio button to perform online backup.

– **Source Storage Group**

  Select storage groups to back up. Select the **All** radio button to backup all storage groups of the Exchange database instance. Select the **Select** radio button to backup specific storage groups only, and then select the storage groups from the list box.

  Specific storage groups are to be backed up in this example, so select the **Select** radio button, and then select the storage groups **STR1** and **STR2** from the list box.

– **Eventlog checking before backup**

  Select the check box for this option to retrieve the event log data of Exchange 2000 Server, Exchange 2000 Enterprise Server, or Exchange Server 2003 to check whether an event indicating that a database is corrupted has been recorded.

– **Advanced Options**

  If you want to use a user script to perform backup operations, click the **Job Script** button to open the Advanced Options dialog box, and then set backup options. For more details, see section 6.9.2.

– **Job Registration**

  To perform backup immediately without registering a backup job, do not click the **Schedule** button. To register a backup job with the contents specified thus far, see section 6.5.1.

5. Click the **OK** button.

   A confirmation dialog box for executing the backup is displayed.

6. Click the **OK** button to start the backup process.

   Backup processing starts. Quitting Protection Manager Console during backup does not terminate the command processing.

   While the backup is in progress, the status is displayed in the **Progress** that shows how much of the volume has been copied. This does not represent the progress of the whole backup process. Copy progress might be displayed as progressing rather slowly near the 0% mark, as well as near the 100% mark. To confirm that all volumes are copied, check the Progress.

   If you have started locally, the **Progress Detail** displays messages showing the progress of the backup process.

   When the backup is finished, a dialog box is displayed to indicate completion of the backup. The backup ID is displayed in this dialog box.

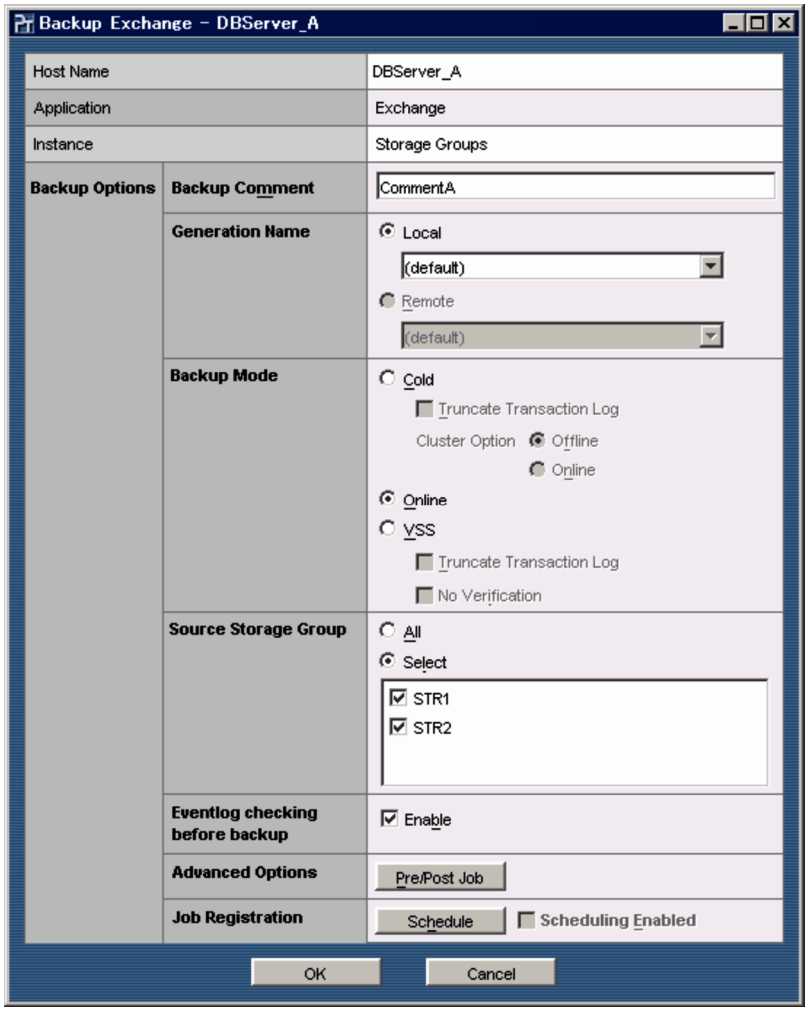


Figure 6.20 Backup Exchange Dialog Box (for Online Backup)

6.4.6 Backing up a Storage Group to a Secondary Volume (for VSS Backup)

This subsection describes an example of using VSS to back up, from a primary volume to a secondary volume, a storage group of Exchange Server 2003 or Exchange Server 2007. In this example, storage groups STR1 and STR2 in a database server DBServer_A are backed up on the secondary volume.

Note: When usual operation is in a split state, you must resynchronize the copy group before backing up data. When usual operation is in a pair state, you do not need to resynchronize the copy group before backing up the data. After the tape backup ends, resynchronize the copy group to initialize it. For details on how to do this, see section 6.7.

To back up a storage group:

1. Start the instance of Protection Manager Console on the database server, and click the **Application View** tab.

   The Application View is displayed. For details on the displayed items, see Table 6.2.

2. Select the Exchange database instance to be backed up. Select the following rows:

- Application: Exchange
- Instance: Storage Groups

Note: To see detailed information about the Exchange database instance, in the **Application View**, click the **Show Application Detail** button. The Application Detail window is displayed, allowing you to view detailed information. For details on the displayed items, see Table 6.3.

3. In the **Application View**, click the **Backup** button.

   The Backup Exchange dialog box, where you can set the backup options, is displayed.

4. Set the backup options:

   - **Backup Comment**

     Specify this to register a backup comment in the backup catalog. The backup-comment value can be a string of up to 64 bytes, consisting of alphanumeric, special, one-byte space, and multi-byte characters. The backup comment is case-sensitive.

     The following special characters cannot be used for backup comments:

     \ / ` | < > " * ? & ; ( )

     The first character must not be a hyphen (-).

   - **Generation Name**

     Specify this option to back up the file system to the copy group that has the specified name identifying the generation.

   - **Backup Mode**

     Set the backup mode. For this example, select the **VSS** radio button to perform VSS backup.

   - **Truncate Transaction Log**

     Select the **Delete Transaction Log** check box to delete the committed transaction log (committed to the database) after completing the backup.

- **Source Storage Group**

  Select storage groups to back up. Select the **All** radio button to backup all storage groups of the Exchange database instance. Select the **Select** radio button to backup specific storage groups only, and then select the storage groups from the list box. Specific storage groups are to be backed up in this example, so select the **Select** radio button, and then select the storage groups **STR1** and **STR2** from the list box.

- **Eventlog checking before backup**

  Select the check box for this option to retrieve the event log data of Exchange Server 2003 to check whether an event indicating that a database is corrupted has been recorded. Specify this option when using Protection Manager for Exchange (2000/2003 version). You cannot specify this option when Protection Manager for Exchange 2007 is being used.

- **Advanced Options**

  If you want to use a user script to perform backup operations, click the **Job Script** button to open the Advanced Options dialog box, and then set backup options. For more details, see section 6.9.2.

- **Job Registration**

  To perform backup immediately without registering a backup job, do not click the **Schedule** button. To register a backup job with the contents specified thus far, see section 6.5.1.

5. Click the **OK** button.

   A confirmation dialog box for executing the backup is displayed.

6. Click the **OK** button to start the backup process.

   Backup processing starts. Quitting Protection Manager Console during backup does not terminate the command processing.

   If you have started locally, the **Progress Detail** displays messages showing the progress of the backup process.

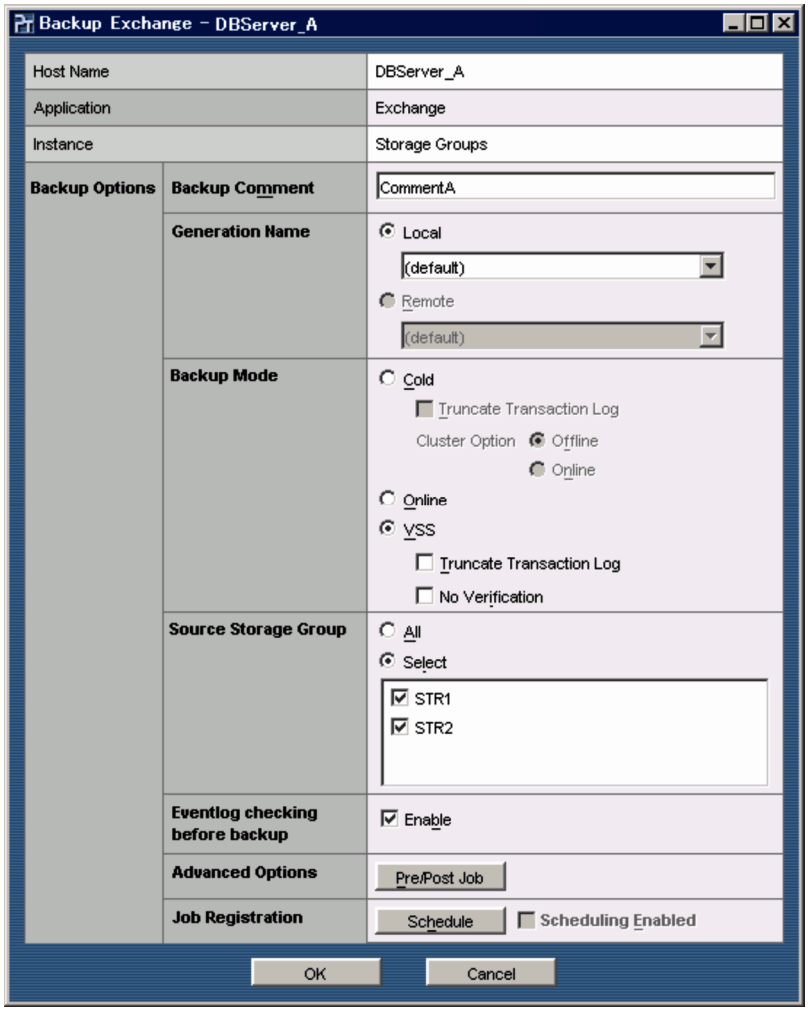


Figure 6.21 Backup Exchange Dialog Box (for VSS Backup)

The above figure shows an example of Protection Manager for Exchange (2000/2003 version).

6.4.7 Restoring Storage Groups to a Primary Volume

This section provides sample instructions for restoring Exchange database storage groups from a secondary volume to a primary volume in a step called resynchronization. This example restores a backup for storage group STR1.

To restore storage groups:

1. Start Protection Manager Console on the database server, and click the **Backup Catalog View** tab.

   The Backup Catalog View is displayed. For details on the displayed items, see Table 6.4.

2. Select the Exchange database instances to restore. Based on the Backup ID, Backup Time, Instance, and Comment, select the row of the database you want to restore.

   Note: To see detailed information about the Exchange database instance, in the Backup Catalog View, click the **Show Backup Detail Information** button. The Backup Detail Information window is displayed, allowing you to view detailed information.

3. In the **Backup Catalog** View, click the **Restore** button.

   The Restore Exchange dialog box is displayed. Specify the restore options in the Restore Exchange dialog box.

4. Set the restoration options:

   – **Source Storage Group / Information Store**

     Select storage groups and information stores to restore. Select the **All** radio button to restore all storage groups of the Exchange database instance. Select the **Select** radio button to restore specific storage groups and information stores, and then select the storage groups and information stores from the list box.

     Specific storage groups are to be restored in this example, so select the **Select** radio button, and then select the storage group **STR1** from the list box.

   Note: When you select the storage group check box, all the subordinate information store check boxes are also selected. If you restore the data in units of information stores, clear the check boxes for the information stores that do not need to be restored.

   – **Roll Forward**

     Select this check box to perform a roll forward recovery. Make sure that you select the check box when restoring the data in units of information stores.

   – **Force**

     Select this check box when restoring to a primary volume even if the volume is not the same volume as the backup source primary volume. Use this option only when normal restoration cannot be performed, such as when the LDEV number has changed when the volume was switched.

5. Click the **OK** button.

   A dialog box prompting you to confirm the execution of restoration is displayed.

6. Click the **OK** button to start the restoration process.

   Restoration processing starts. Quitting Protection Manager Console during restoration does not terminate the command processing.

   While the restoration is in progress, the status is displayed in the **Progress** that shows how much of the volume has been restored. This does not represent the progress of the whole restoration process. Copy progress might be displayed as progressing rather slowly near the 0% mark, as well as near the 100% mark. To confirm that the restoration finishes, check the Progress.

   If you have started locally, the **Progress Detail** displays messages showing the progress of the restoration process.

   When the restoration is finished, a dialog box is displayed to indicate completion of the restoration.

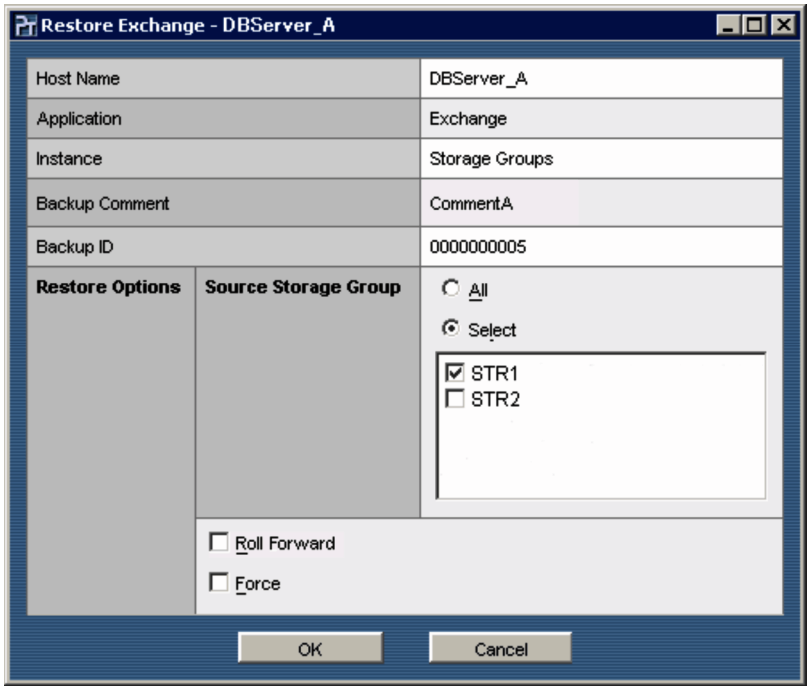


Figure 6.22 Restore Exchange Dialog Box

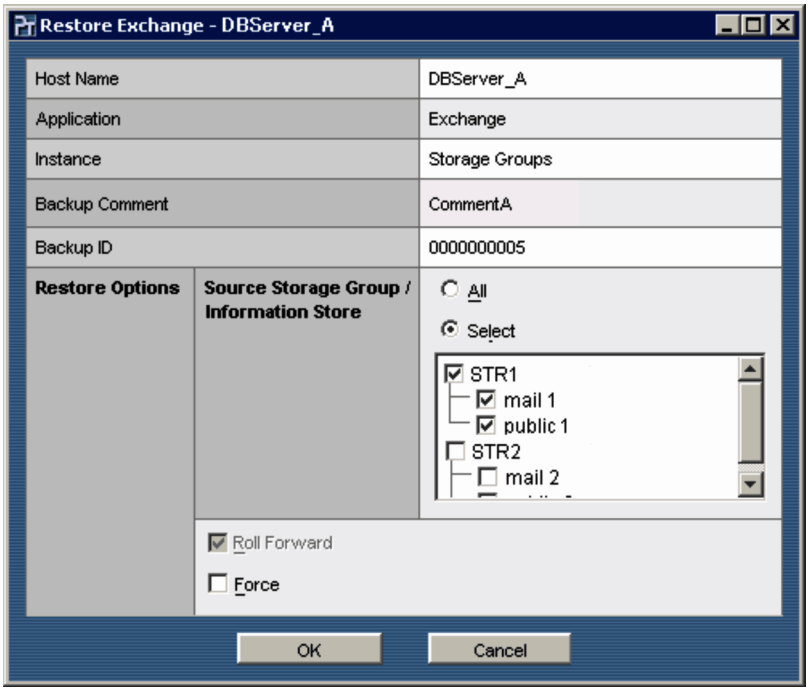


Figure 6.23 Restore Exchange Dialog Box (When Backup Mode is VSS)

6.5 Operations for Backup Jobs

If you want a backup to be executed automatically according to a specified schedule, register a backup job using Protection Manager Console. After registering backup jobs, you can run them immediately, change relevant options (backup options and schedule options), delete the backup jobs, or view their execution results.

6.5.1 Registering a Backup Job

After you register a backup job, the backup is executed automatically according to the specified schedule. The maximum number of backup jobs that can be registered is 500, or the number specified in `MAX_JOB_REGISTRATION_COUNT` of the `schd.conf` file. For details on `MAX_JOB_REGISTRATION_COUNT`, see section 4.3.4.3.

Note: The dialog box for setting up backup options differs depending on the application (file system, SQL Server database, or Exchange database) in use. In the procedures below, these backup option setup dialog boxes are generically called backup dialog boxes.

6.5.1.1 Setting up Backup Options

To set up backup options in the backup dialog box:

1. Start Protection Manager Console on the file server or database server and click the **Application View** tab.

   The Application View is displayed. For details on the displayed items, see Table 6.2.

2. From the list in the Application View, select a record you want to back up, and click the **Backup** button.

   The Backup dialog box is displayed. Set the backup options in the Backup dialog box.

   Note: The backup options to be set up differ depending on the application. For details on which backup options to set, see the backup procedure for the relevant application.

3. Click the **Schedule** button of the Job Registration option.

   The Schedule Option dialog box is displayed.

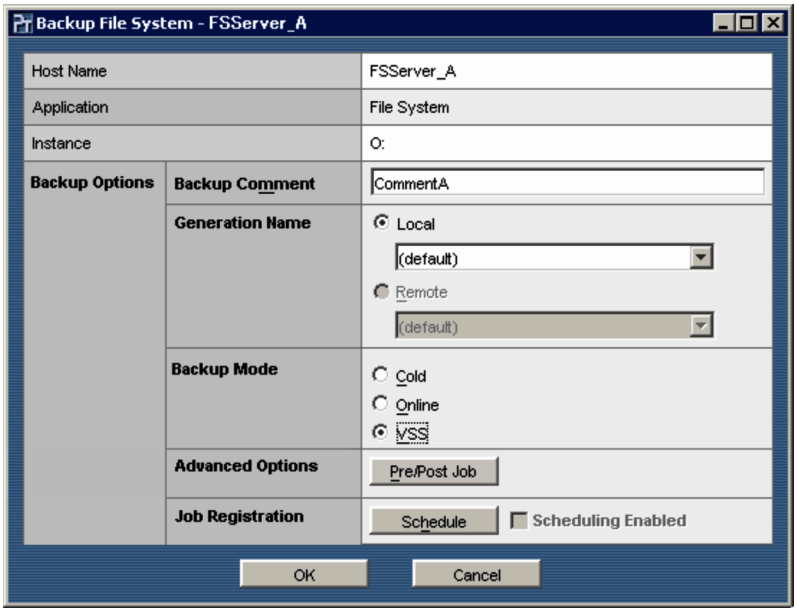


Figure 6.24 Backup Dialog Box (File System)

6.5.1.2 Setting up Schedule Options

To set up schedule options in the Schedule Option dialog box:

1. Set up common schedule options.

   The following common schedule options must be set up for all types:

   - **Schedule Type**

     Select one of the following schedule types:

     Daily: Run at the specified time each day.

     Weekly: Run at the specified day and time each week.

     Monthly: Run at the specified date/time each month. If you specify the date as the 29th, 30th, or 31st, and that date does not exist in the month where the schedule is executed, the specified backup job is not executed.

     Day of week in month: Run every time at the specified time, day, and week in the specified month.

     One time only: Run one time only at the specified date/time. Once a schedule is executed for a backup job for which **One time only** is specified, the backup job cannot be reused.

   - **Start Time**

     Specify the backup start time. Use the system time of the file server or database server to specify the backup start time.

     If backup jobs have been registered in a time zone in which the system time is adjusted for daylight saving time, the system operates as follows:

     - Backup jobs scheduled in a time zone in which the time jumps forward at the beginning of daylight saving time (for example, from 2:00 a.m. to 3:00 a.m.) are not executed.
     - Backup jobs scheduled in a time zone in which the time is repeated at the end of daylight saving time (for example, from 1:00 a.m. to 2:00 a.m.) are executed twice.

     Therefore, to ensure that normal periodic backup is performed by using Protection Manager Console, specify a backup start time that does not fall in a time period in which the system time is adjusted.

2. Set up individual schedule options.

   The schedule options for each schedule type are shown in the table below. The settings differ depending on the setting of the **Schedule Type** option.

Table 6.13 Schedule Option for Each Schedule Type

Schedule type	Schedule option	Contents
Daily	None	Not applicable
Weekly	Day(s) of week	Select a day of week (every week) when you want the backup to run. Multiple days of week can be selected.
Monthly	Day(s) of month	Select a day of month (every month) when you want the backup to run. Multiple days of month can be selected.
Day of week in month	Select Month	Select the month when you want the backup to run. Selecting a month causes backup to run only in the selected month. Selecting **All** causes the backup to run in all months.
	Select Week	Select the week when you want the backup to run.
	Select Day	Select the day of week when you want the backup to run. Multiple days of week can be selected.
One time only	Start Date	Specify the day when you want the backup to run.

3. Click the **OK** button.

   You return to the backup dialog box.

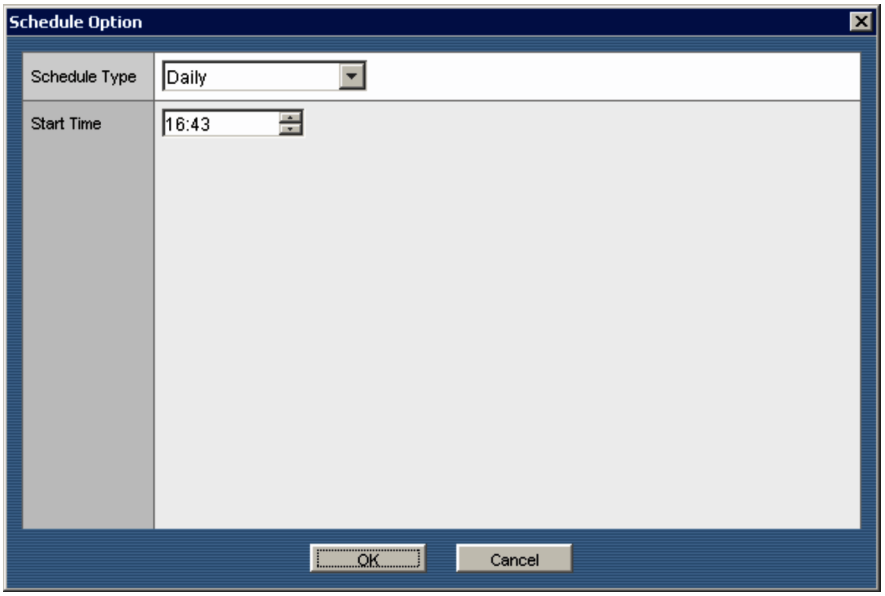


Figure 6.25 Schedule Option Dialog Box (Daily)

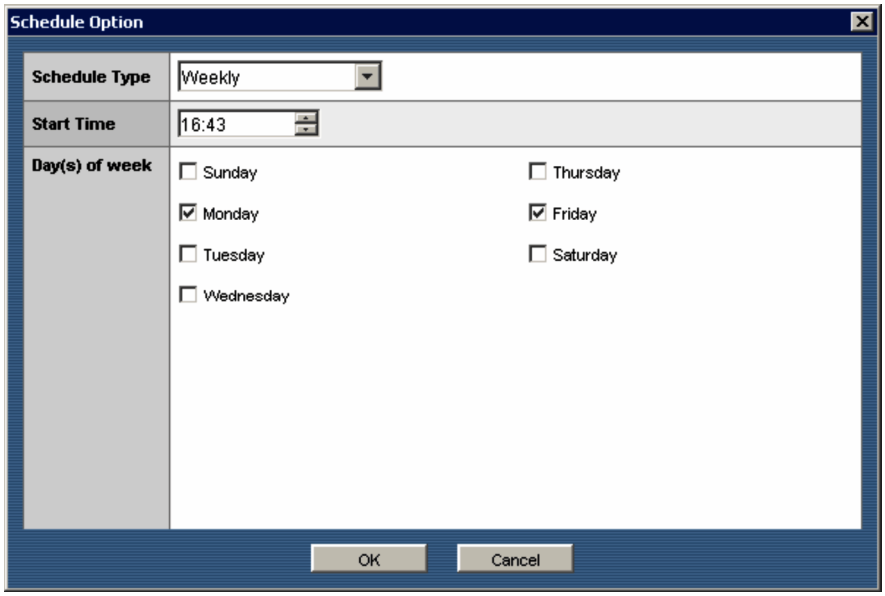


Figure 6.26 Schedule Option Dialog Box (Weekly)

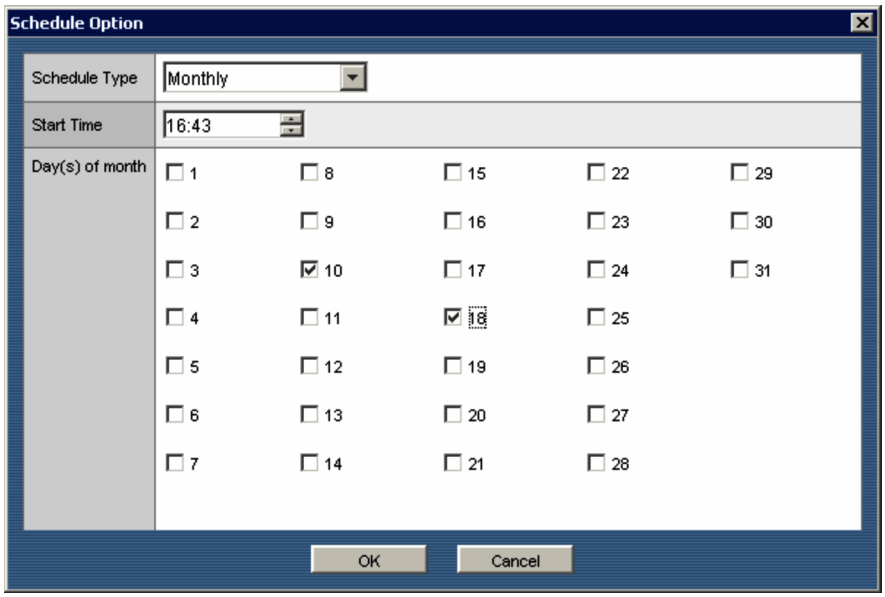


Figure 6.27 Schedule Option Dialog Box (Monthly)

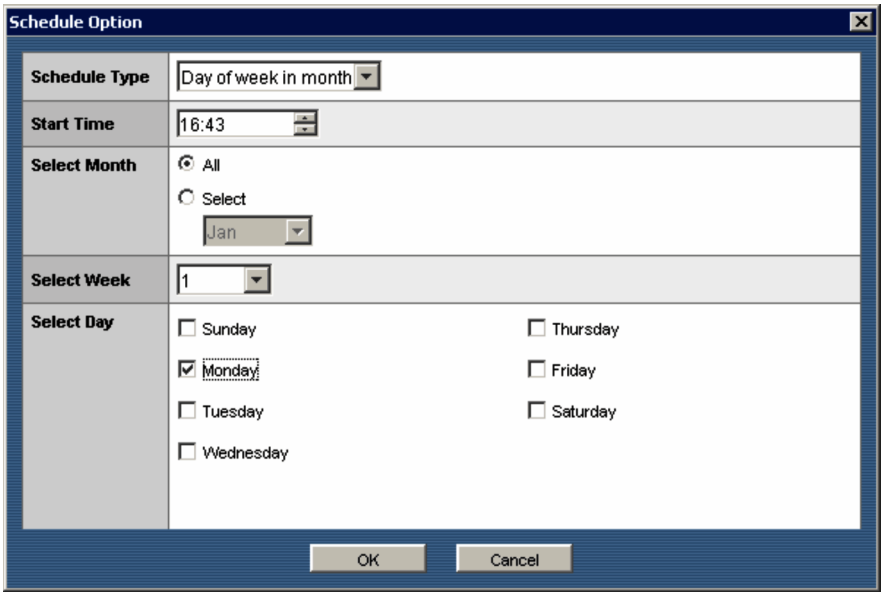


Figure 6.28 Schedule Option Dialog Box (Day of Week in Month)

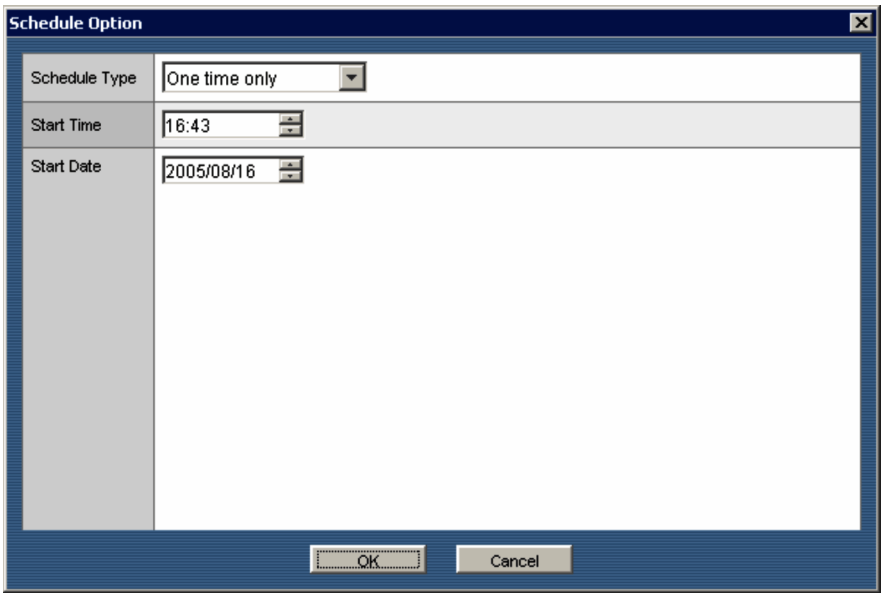


Figure 6.29 Schedule Option Dialog Box (One Time Only)

6.5.1.3 Registering a Backup Job

To register a backup job in the Backup dialog box:

1. Confirm that the **Enable Registration** checkbox of the **Job Registration** option is selected.

   Note: If the **Enable Registration** check box is cleared, backup jobs are not registered.

2. Click the **OK** button.

   The backup job is registered. The registered backup job can be checked in the Backup Job View.

6.5.2 Running a Backup Job Immediately

The following describes how to run a backup job immediately rather than at the scheduled time.

Note: If a schedule is executed for a backup job whose schedule type was specified as **One time only**, an immediate execution cannot be performed for that job whether the job is being executed or has been completed.

For a backup job whose schedule type was specified as a type other than **One time only**, an immediate execution of the job cannot be performed when the job is being executed. Wait until the job finishes, and then retry the operation.

To run a backup job immediately (rather than at a later, scheduled time):

1. Start Protection Manager Console and click the **Backup Job View** tab.

   The Backup Job View is displayed. For details on the displayed items, see section 6.1.5.1.

2. From the list in the Backup Job View, select a schedule you want to run immediately, and click the **Run Immediately** button.

   A confirmation dialog box for executing the backup is displayed.

3. Click the **OK** button to start the backup processing.

   Backup processing starts. Quitting Protection Manager Console during backup does not terminate the command processing.

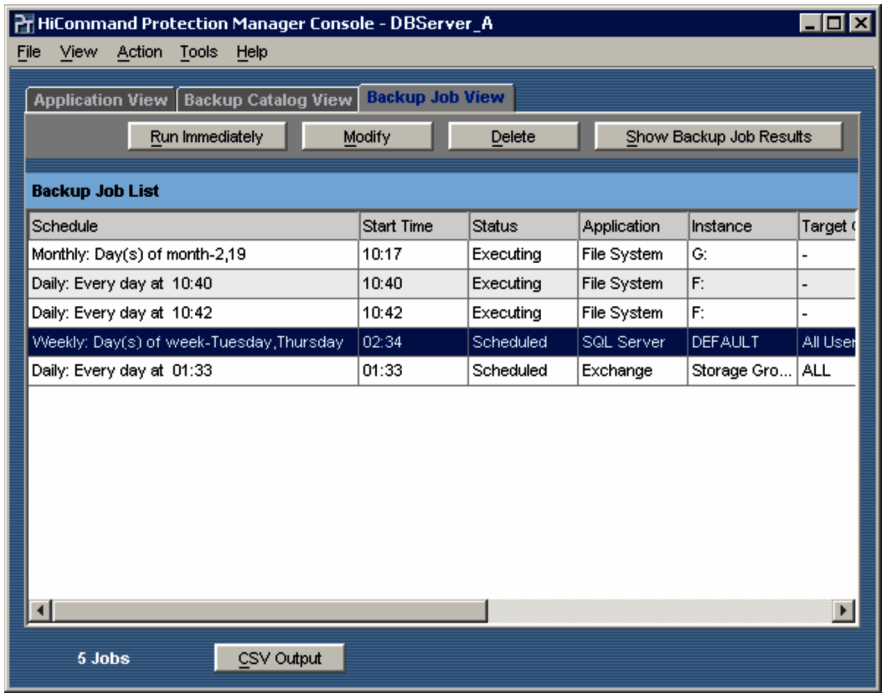


Figure 6.30 Example of the Backup Job View

6.5.3 Changing Options for a Backup Job

The following describes how to change the backup and schedule options after registering backup jobs.

For a backup job whose schedule type has been set to a type other than **One time only**, its options cannot be changed while the job is running. Wait until the job finishes, and then retry the operation.

Notes:

- If a schedule is executed for a backup job whose schedule type was specified as **One time only**, its options cannot be changed regardless of whether the job is running or it has already finished.
- The dialog box for changing backup options differs depending on the application (file system, SQL Server database, or Exchange database) in use. In the procedures below, these dialog boxes are generically called the *Backup Job Update* dialog box.

To change backup and schedule options after registering backup jobs:

1. Start Protection Manager Console and click the **Backup Job View** tab.

   The Backup Job View is displayed. For details on the displayed items, see section 6.1.5.1.

2. From the list in the Backup Job View, select a backup job whose options you want to change, and then click the **Modify** button.

   The Backup Job Update dialog box is displayed. In this dialog box, you can change backup options.

   Note: The backup options to be set up differ depending on the application. For details on the backup options to be set up in the Backup dialog box, see the backup procedures for the relevant application.

3. Click the **Schedule** button of the **Modify Schedule** option.

   The Schedule Option dialog box is displayed.

4. Set up schedule options.

   For details on how to set up schedule options, see section 6.5.1.2.

5. After changing schedule options, click the **OK** button in the Schedule Option dialog box.

   You return to the Backup Job Update dialog box.

6. Click the **OK** button.

   The options relevant to the backup job are changed. You can check the changed backup job options in the Backup Job View.

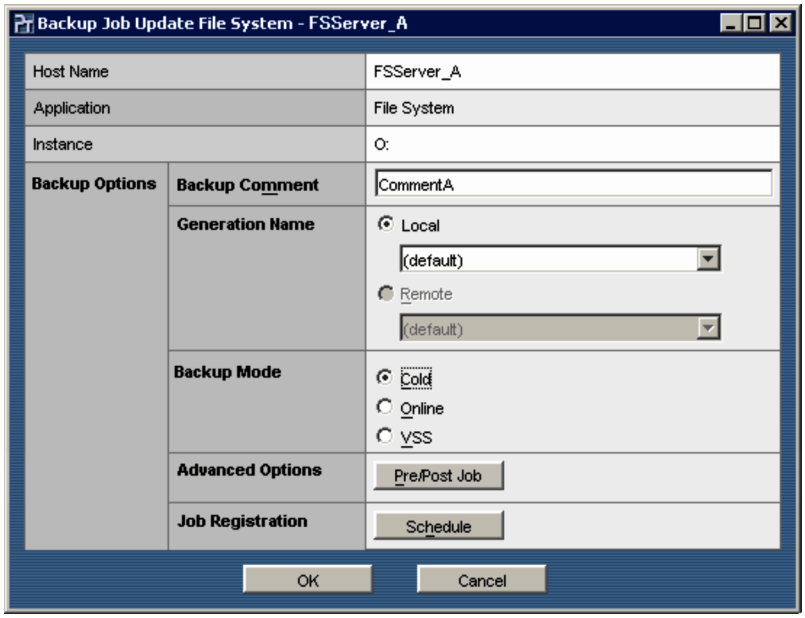


Figure 6.31 Backup Job Update Dialog Box (File System)

6.5.4 Deleting a Backup Job

The following describes how to delete a backup job that is no longer required.

Note: You cannot delete a ba ckup job that is already being executed. Wait until the backup job finishes, and then retry the operation.

To delete an unnecessary backup job:

1. Start Protection Manager Console and click the **Backup Job View** tab.

   The Backup Job View is displayed. For details on the displayed items, see section 6.1.5.1.

2. From the list in the Backup Job View, select a backup job you want to delete, and click the **Delete** button.

   A dialog box is displayed, asking if you are sure you want to delete the backup job.

3. If you want to delete the backup job, click the **OK** button.

6.5.5 Viewing the Execution Results of a Backup Job

The following describes how to view the execution results of a backup job in more detail than the results displayed in the Backup Job View. The maximum number of backup job execution results that can be displayed is 64 (or, the number specified in `MAX_JOB_RESULT_COUNT` of the `schd.conf`). For details on `MAX_JOB_RESULT_COUNT`, see section 4.3.4.4.

To view backup job execution results in more detail than those displayed in the Backup Job View:

1. Start Protection Manager Console and click the **Backup Job View** tab.

   The Backup Job View is displayed. For details on the displayed items, see section 6.1.5.1.

2. From the Backup Job View, select a backup job you want to view, and click the **Show Backup Job Results** button.

   The Backup Job Result Details window is displayed. For details on the displayed items, see section 6.1.5.2.

3. From the Executed Job List, select the Backup ID whose execution result you want to view, and click the **Show Job Output** button.

   Using the backup ID as a key, extract a list of logs. The results are displayed in the **Job Output** field.

   The execution result of the specified Backup ID is displayed in the **Job Output** field.

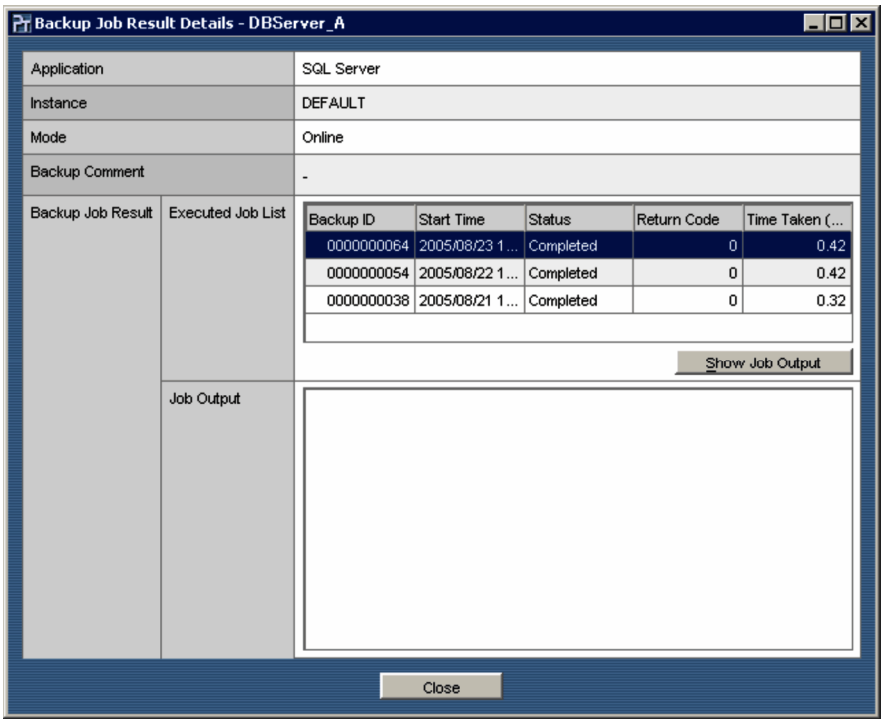


Figure 6.32 Example of the Backup Job Result Details Window

6.6 Locking a Copy Group

You can use Protection Manager Console to lock the contents of a particular copy group. You can also unlock a copy group that has already been locked. Protection Manager automatically selects the backup-destination secondary volume when executing backup. However, the lock function enables you to lock the contents of a particular secondary volume and continue backup using other secondary volumes only.

The following figure illustrates backup of multiple generations when a particular secondary volume has been locked. In this example, generation 1 is obtained, then secondary volume 1 is locked, and then the backed-up contents of generation 1 are locked. Thus, generation 4 and subsequent generations are backed up using the remaining secondary volumes (secondary volumes 2 and 3).

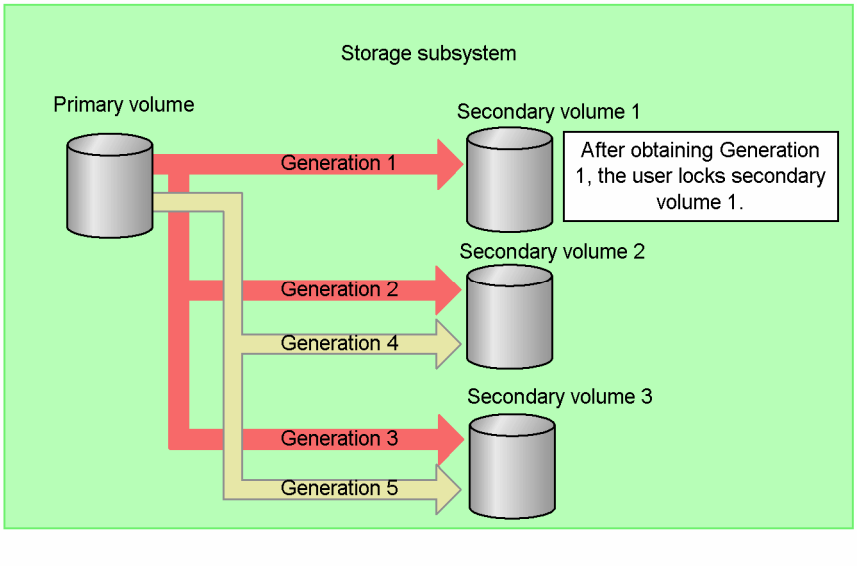


Figure 6.33 Backup of Multiple Generations When a Secondary Volume Has Been Locked

To lock a copy group:

1. Start Protection Manager Console, and then click the **Backup Catalog View** tab.

   The Backup Catalog View is displayed. For details on the displayed items, see Table 6.4.

2. Select the backup ID corresponding to the copy group to be locked.
3. Click the **Lock** button in the Backup Catalog View.

   The Lock dialog box, where you can set the lock options, is displayed.

4. Set the lock options:
   - To enable lock mode, select **Lock Mode**.
   - To lock a copy group, select the **Lock** radio button. (If the copy group is currently unlocked, the **Lock** radio button is selected by default.)
   - To unlock a copy group that is currently locked, select **Unlock**.

   Note: If - is displayed in Lock Status, the Lock radio button is selected by default.

5. Click the **OK** button.

   A confirmation dialog box for execution of the lock process is displayed.

6. Click the **OK** button to start the lock process.

   Lock processing starts. Quitting Protection Manager Console during lock processing does not terminate the command processing. When the lock processing is finished, a dialog box is displayed.

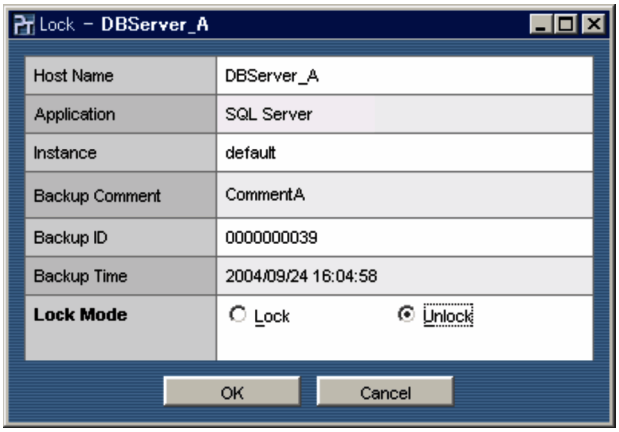


Figure 6.34 Lock Dialog Box

6.7 Resynchronizing a Copy Group

You can use Protection Manager Console to resynchronize a copy group.

To resynchronize a copy group:

1. Start Protection Manager Console, and then click the **Backup Catalog View** tab.

   The Backup Catalog View is displayed. For details on the displayed items, see Table 6.4.

2. Select the backup ID corresponding to the copy group to be resynchronized.

3. Click the **Resync** button in the Backup Catalog View.

   The Confirmation to Resync dialog box is displayed. This dialog box displays details on performing resynchronization.

4. Confirm the execution details, then click the **OK** button.

   Notes on performing resynchronization are displayed. Read these notes.

5. Click the **OK** button to perform resynchronization.

   Resynchronization processing starts. Quitting Protection Manager Console during resynchronization does not terminate the command processing. During resynchronization, the resynchronization progress status is displayed. When the resynchronization is finished, a dialog box is displayed.

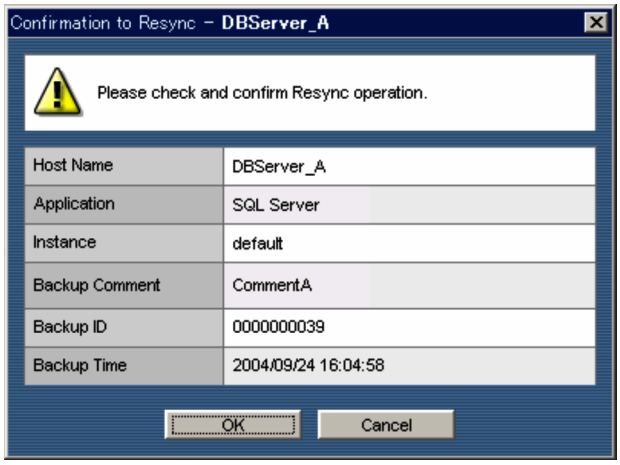


Figure 6.35 Confirmation to Resync Dialog Box

6.8 Mounting and Unmounting the Secondary Volume

To reference files and databases on a secondary volume, it is necessary to mount the secondary volume on the backup server. To perform backup or restoration in an application server, the secondary volume must be unmounted.

This section describes how to mount and unmount the secondary volume by using Protection Manager Console. This section also describes how to back up a mounted secondary volume to tape.

Notes: You cannot perform the following operations on a volume mounted by Protection Manager Console:

- Display application information on the backup server. You cannot view application information about the secondary volume on the backup server.
- Use the Protection Manager Copy Controller command (for example, the `drmmediabackup` command) to back up data to tape.
- Use the Protection Manager for SQL command (the drmsqlrestore, drmsqlrecover, and `drmsqlrecovertool` commands) to restore or recover a SQL Server database.
- If you have mounted a secondary volume and attached databases in order to view the contents of the files and databases on the secondary volume, then detach the databases and unmount the secondary volume after you finish viewing the contents.

6.8.1 Mounting the Secondary Volume

To mount a secondary volume, you must determine the name of the copy group to which that volume belongs. Use the following instructions to determine the name of the copy group.

To confirm the name of the copy group:

1. Display the **Backup Catalog View** from the Protection Manager Console on the file server or database server.

   For details on the displayed items, see Table 6.4.

2. In the **Backup Catalog View**, select the record of the Backup ID for the target file system or database instance, and display the **Backup Detail Information** window.

3. Check the copy group name in the **Pair Name** column of the list.

   Note: A secondary volume that has not been formatted as a file system and a secondary volume in the mirror status cannot be mounted.

To mount a secondary volume in a dynamic disk configuration in an LDM or VxVM environment, you must create, in advance, a definition file for mounting copy groups. To automatically mount all the secondary volumes in a dynamic disk configuration, specify one of the copy groups that make up the relevant disk group. An error occurs if you specify two or more copy groups.

For details about definition files for mounting copy groups, see the *HiCommand Protection Manager User's Guide*.

At this point, perform the following operations from the instance of Protection Manager Console on the backup server.

To mount a secondary volume:

1. Start the instance of Protection Manager Console on the backup server.

   When Protection Manager Console is started, sometimes a message is displayed at the top of the Information View or the `KAVX11005-W` message is output. However, if setup has completed, there is no problem, so continue to carry out the following procedure.

2. Choose **Action**, and then **Mount**.

   The Mount dialog box, where you can set the secondary volume to mount, is displayed.

3. Set the secondary volume to mount:

   - **Pair Name**

     Enter the name of the copy group belonging to the secondary volume to be mounted.

   - **Mount Point**

     Use an absolute path name to specify the mount point directory to which the secondary volume is to be mounted. Specify the drive letter, or the absolute path from the drive letter. Use characters that can be used for directory names in Windows (you cannot use space characters).

     - If you specify a drive letter, unused drive names are searched for, in alphabetical order beginning with the specified drive, and then the secondary volume is mounted on the first found drive.
     - If a path does not end with the \ character, the command assumes that a \ character is present at the end of the path. For example, D: and D:\ are assumed to be the same drive. Similarly, D:\MOUNTDIR and D:\MOUNTDIR\ are assumed to be the same directory.
     - When Mount Point is omitted, any drive not in use when the mount is executed will be used.

   To mount multiple secondary volumes, you can specify more than one volume. However, when specifying directory paths as mount points, enter them in the appropriate order based on the dependency relationship among the directory paths. Mounting is performed in order from the top line.

   You can edit lines used for Pair Name and Mount Point entry, by using the following operations:

   - Insert key

     Adds a new line above the selected line.

   - Tab key

     Moves to Mount Point when you select Pair Name. When you select Mount Point, the selected line moves to Pair Name on the next line. If there is no next line, a new line is added.

   - Delete key

     Deletes the selected line. If multiple lines are selected, multiple lines are deleted.

You can also use the right-click menu to edit lines used for Pair Name and Mount Point entry:

- Insert Row

  Adds a new line above the selected line.

- Delete Row(s)

  Deletes the selected line. If multiple lines are selected, multiple lines are deleted.

4. Click the **OK** button.

   A dialog box is displayed prompting you to confirm the mount execution.

5. If the copy group name and mount point entered are correct, click the **OK** button. Mount operations begin. Quitting Protection Manager Console during mount operations does not terminate the command processing.

   When mount operations are finished, a dialog box is displayed to indicate mount completion. During mount operations, the Mount Point column remains blank. After the operations finish, the Mount Point column displays the mount point name. If you plan to unmount the secondary volume later, we recommend that you save the information displayed about the mounted copy group.

   If mount operations fail, a dialog box indicating the error is displayed and mount operations are canceled. Only those mount points for which mounting was successfully performed are displayed in the Mount dialog box.

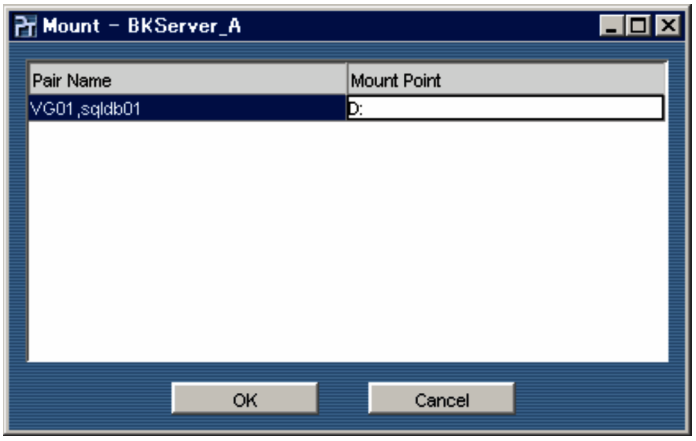


Figure 6.36 Mount Dialog Box

6.8.2 Unmounting the Secondary Volume

To unmount a secondary volume, you must determine the name of the copy group to which that volume belongs. The following method can be used to determine the name of the copy group:

To confirm the name of the copy group:

1. Display the **Backup Catalog View** from the Protection Manager Console on the file server or database server.

   For details on the displayed items, see Table 6.4.

2. In the Backup Catalog View, select the record of the Backup ID for the target file system or database instance, and display the Backup Detail Information window.

3. Check the copy group name in the Pair Name column of the list.

To automatically mount all secondary volumes in a dynamic disk configuration in an LDM or VxVM environment, you must specify one of the copy groups that make up the relevant disk group.

At this point, perform the following operations from the instance of Protection Manager Console on the backup server.

To unmount a secondary volume:

1. Start the instance of Protection Manager Console on the backup server.

2. Select **Action** and then **Unmount**.
   The Unmount dialog box, where you can set the secondary volume to unmount, is displayed.

3. Set the secondary volume to unmount:

   – Pair Name

     Enter the name of the copy group belonging to the secondary volume to be unmounted. To unmount multiple secondary volumes, specify the volumes.

   You can edit lines used for Pair Name entry, by using the following operations:

   – Insert key

     Adds a new line above the selected line.

   – Tab key

     Moves to the next line. If there is no next line, a new line is added.

   – Delete key

     Deletes the selected line. If multiple lines are selected, multiple lines are deleted.

   You can also use the right-click menu to edit lines used for Pair Name entry:

   – Insert Row

     Adds a new line above the selected line.

   – Delete Row(s)

     Deletes the selected line. If multiple lines are selected, multiple lines are deleted.

4. Click the **OK** button.

   A dialog box is displayed prompting you to confirm the unmount execution.

5. If the copy group name and unmount point entered are correct, Click the **OK** button. Unmount operations begin. Quitting Protection Manager Console during unmount operations does not terminate the command processing.

   When unmount operations are finished, a dialog box is displayed to indicate unmount completion. The mount point used when mounting was performed is displayed in this dialog box.

   If unmount operations fail, a dialog box indicating the error is displayed and unmount operations are canceled. Only those mount points for which unmounting was successfully performed are displayed in the Unmount dialog box.

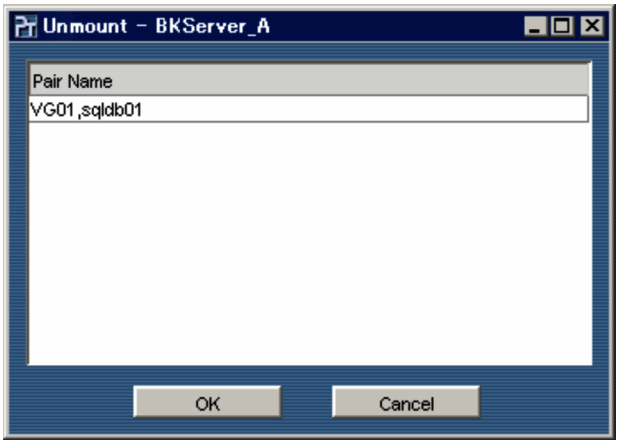


Figure 6.37 Unmount Dialog Box

6.8.3 Backing up or Restoring the Secondary Volume using Tape Media

You can use backup management software (such as VERITAS NetBackup and VERITAS Backup Exec) to back up a secondary volume mounted by Protection Manager Console to backup media, such as tape, or to restore the data from such backup media to a mounted secondary volume.

For details on how to back up data to tape or restore data from tape by using the Protection Manager Copy Controller command, see the *HiCommand Protection Manager User's Guide*.

6.9 Using a User Script

This section explains how to perform backups by using a user script.

6.9.1 Backing up by Using a User Script

If you specify a *user script* when you perform a backup, the commands written in the script are executed at the following points:

- *User Preprocessing* is executed before a backup (PRE_PROC)
- *User Postprocessing* is executed after a backup (POST_PROC)
- User processing is executed after pair resynchronization (RESYNC_PROC)
- User processing is executed after pair splitting (SPLIT_PROC)
- User processing is executed before finishing processing (FINISH_PROC)

Note: The following processing in the user script cannot be edited in the Protection Manager Console:

- User processing executed after pair resynchronization (RESYNC_PROC)
- User processing executed after pair splitting (SPLIT_PROC)
- User processing executed before finishing processing (FINISH_PROC)

However, you can open the user script that includes the processing above to add *User Preprocessing* and *User Postprocessing*.

The following figure shows where in the processing a user script that includes *User Preprocessing* (PRE_PROC) and *User Postprocessing* (POST_PROC) is run.

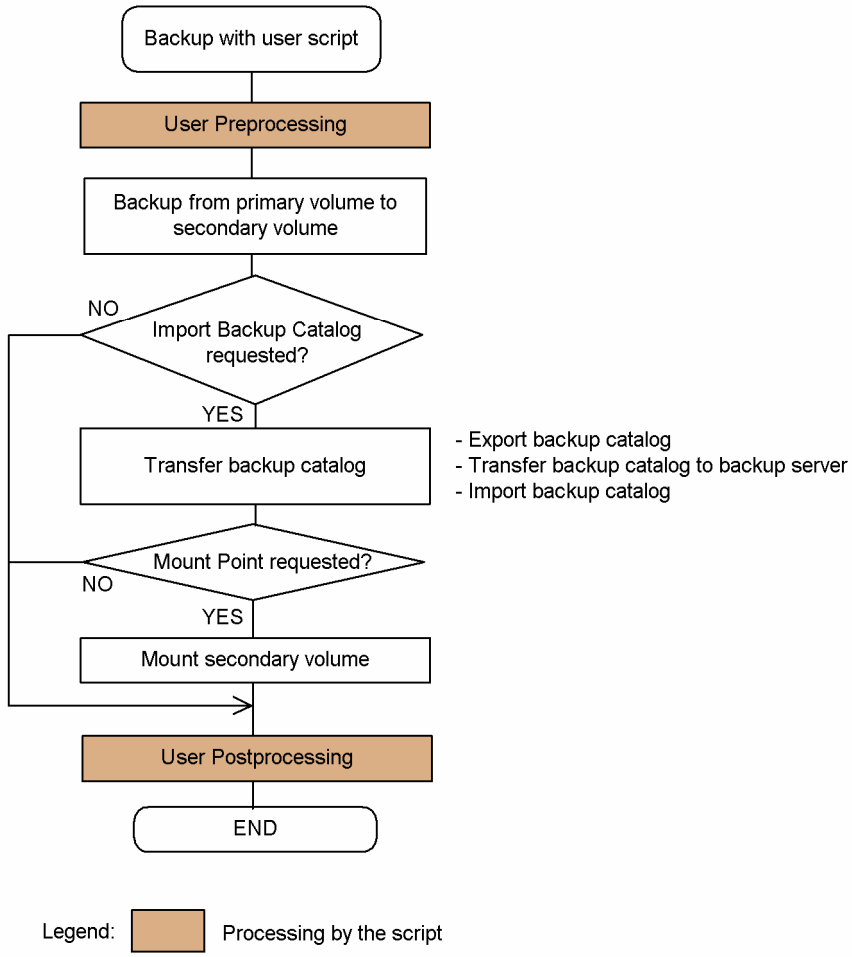


Figure 6.38 Where the User Script Is Run

Note: The dialog box for setting up backup options differs depending on the application that is in use (file system, SQL Server database, or Exchange database). In the procedures below, these backup option setup dialog boxes are generically called the *Backup dialog box*.

6.9.2 Configuring Backup Options for a User Script

To configure backup options regarding the use of a user script:

1. Start Protection Manager Console on a file server or a database server and choose the **Application View** tab.

   The Application View is displayed.

2. Select a record that you want to back up from the Application View list, and click the **Backup** button.

   The Backup dialog box is displayed.

3. Click the **Pre/Post Job** button of the **Advanced Options**.

   The Advanced Options dialog box is displayed.

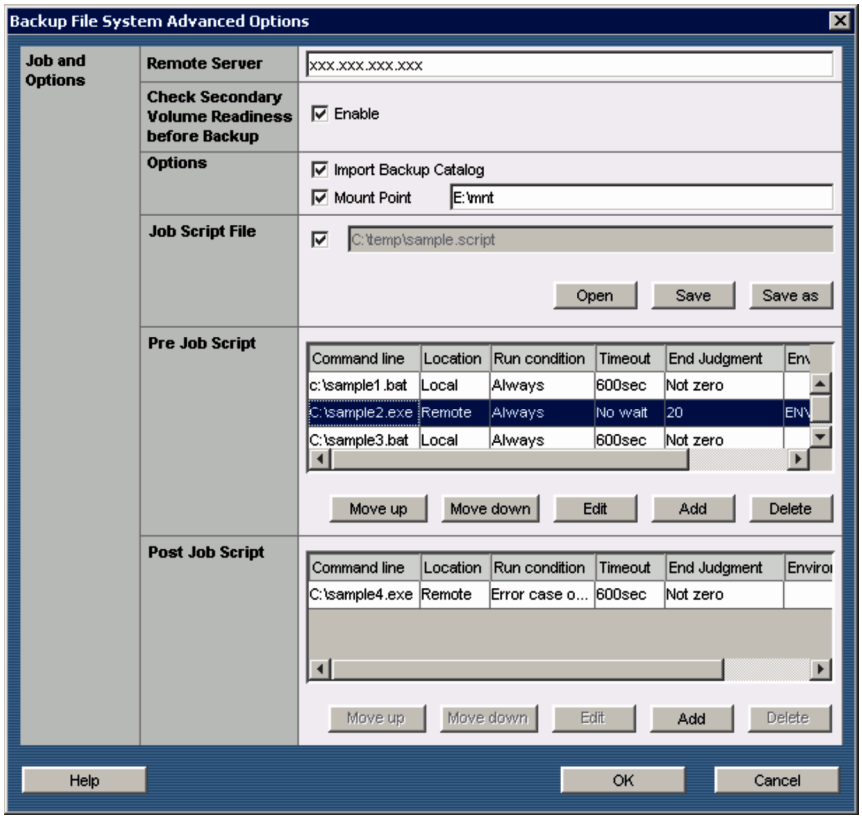


Figure 6.39 The Advanced Options Dialog Box (File System)

4. Configure backup options as required. The options are as follows:

   – **Remote Server**

     If you have specified `run remotely` in your user script, specify the backup server on which you want your user script to run.

   – **Check Secondary Volume Readiness before Backup**

Select the **Enable** check box to check the status of a secondary volume on a backup server. This option must be specified concurrently with the **Remote Server** field. Checking the status of a secondary volume prevents backup or restoration failures. Items, targets, and conditions to be checked are as follows:

Table 6.14 Status Check of a Secondary Volume

Check item	Volume to be checked	Check condition
A secondary volume is hidden from a backup server	All secondary volumes defined for a backup-target primary volume	Checked when a primary volume is defined in pairs with secondary volumes of multiple generations and either of the following items is applicable: - A primary volume is a cluster resource. - A primary volume is a dynamic disk. - A backup by using VSS is performed.
A secondary volume is not mounted on a backup server	A secondary volume to be the next backup destination	Always checked.

– **Options**

Select the **Import Backup Catalog** checkbox if you want a backup catalog to be automatically transferred to the remote backup server when the backup to the secondary volume finishes.

Select the **Mount Point** checkbox and specify the mount point directory name if you want the secondary volume to be automatically mounted on the backup server when the backup to the secondary volume finishes. The mount point directory name must be no more than 64 bytes in length.

Use an absolute path name to specify the mount point directory to which the secondary volume is to be mounted. Specify the drive letter, or specify the absolute path from the drive letter. Use characters that can be used for directory names in Windows. You cannot use space characters.

If you specify a drive letter, unused drive names are searched for, in alphabetical order beginning with the specified drive, and then the secondary volume is mounted on the first found drive.

If a path does not end with the \ character, the command assumes that a \ character is present at the end of the path. For example, `D:` and `D:\` are assumed to be the same drive. Similarly, `D:\MOUNTDIR` and `D:\MOUNTDIR\` are assumed to be the same directory.

When the mount point directory name is omitted, any drive not in use when the mount is executed will be used.

– **Job Script File**

Specify the user script file name. Click the **Open** button to display the Open dialog box. If you have started Protection Manager Console locally, next click the **Browse** button, and then select the file name in the file selection dialog box. If you have started Protection Manager Console remotely from Device Manager, input the absolute path name of the user script directly.

When you input the absolute path name of the user script directly, specify no more than 255 bytes of characters that can be used for directory names in Windows.

After you click the **OK** button, the user script file name is displayed in the **Job Script File** field of the Advanced Options dialog box. In **Pre Job Script** and **Post Job Script**, settings are displayed.

Select the top check box to enable the user script. Clear the top check box to disable the user script. Note that, even if you clear the check box, the settings will remain in **Pre Job Script** and **Post Job Script**.

6.9.3 Creating or Modifying a User Script

You can create a new user script or modify an existing one in the Advanced Options dialog box.

Create or modify a user script in the lower part of the Advanced Options dialog box, below **Job Script File**. Items in this part of the dialog box are the same as those for the Pre/Post Job Template window in Setup GUI. For details on how to create or modify a user script, see the descriptions of the Pre/Post Job Template window in the *HiCommand Protection Manager User's Guide*.

6.9.4 Backing up a Volume to a Magnetic Tape by Using a User Script

If you specify a backup to a magnetic tape in the user script, you can perform a backup to a magnetic tape from the primary volume through the secondary volume. For details on how to create a user script for a tape backup, see the section *Creating a User Script* in the *HiCommand Protection Manager User's Guide*.

Chapter 7 Troubleshooting

This chapter describes appropriate actions to be taken with respect to problems that might occur during operation of Protection Manager Console:

- Troubleshooting Protection Manager Console (see section 7.1)
- Working with Protection Manager Console Detailed Messages (see section 7.2)
- Responding to Detailed Messages (see section 7.3)
- Troubleshooting Issues that Cannot be Resolved Using Detailed Messages (see section 7.4)
- Reviewing the Protection Manager Console Log Information (see section 7.5)
- Reviewing Data from Prerequisite Products (see section 7.6)
- Calling the Hitachi Data Systems Support Center (see section 7.7)

7.1 Troubleshooting Protection Manager Console

To resolve any issues that may occur during the operation of Protection Manager Console, follow these steps.

1. Check the conditions under which the problem occurred.

   Check the operating conditions under which the problem occurred, and the message displayed in the Protection Manager Console dialog box. Then, take action as appropriate to the message to resolve the problem. For details on Protection Manager Console messages, see the *HiCommand Protection Manager Messages*.

   Depending on the status of the problem, a detailed message (location and cause of the error) may be displayed along with the message. For details about detailed messages, see section 7.2.

2. Collect log information and other data that can be used to identify the cause.
   If the problem persists after step 1, collect references such as log information.

   - Collect Protection Manager Console log information

     When the problem cannot be solved through the information given by the Protection Manager Console detailed message (location and cause of the error), collect the log information that is output from Protection Manager Console. For details on the log files to be collected, see section 7.5.

   - Collect Protection Manager Console version information

     Collect the version information file for Protection Manager Console. This file is in the following location:

     Protection-Manager-Console-installation-directory\.version_con

   - Collect log information and environment settings information for prerequisite products.

     If it appears as though the cause of the error might be external to Protection Manager Console, collect references such as the output logs from prerequisite products (OS, Protection Manager Copy Controller, RAID Manager, and so on) and their environment settings information. For an outline of the data to be collected, see section 7.5.4.

3. Based on the data collected, investigate the cause and analyze the problem. If you still cannot determine the cause of the problem after this step, contact the dealer from which you purchased the product.

7.2 Working with Protection Manager Console Detailed Messages

Depending on the type of error, the location and cause of the error might be displayed in a message dialog box. This is called a detailed message.

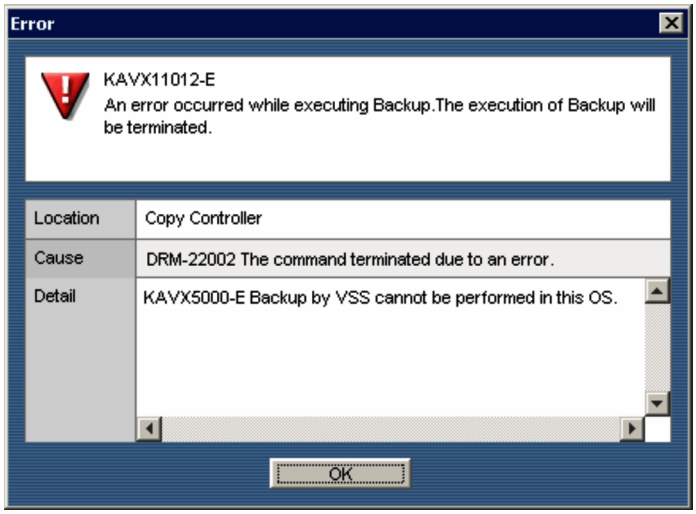


Figure 7.1 Example of a Detailed Message Displayed in a Dialog Box

Table 7.1 lists the items that are displayed as part of a detailed message.

Table 7.1 Contents of a Detailed Message

Item	Details
Location	Displays either Console, Copy Controller or Agent to indicate the location of the error. If there is no information for this item, - is displayed. ▪ Console Indicates that the error has occurred in Protection Manager Console. ▪ Copy Controller Indicates that the error has occurred in Protection Manager Copy Controller. ▪ Agent Indicates that the error has occurred in the Protection Manager Agent in an environment that is linked with Device Manager. Protection Manager Agent is a plug-in for Device Manager Agent, and is used to link with Device Manager.
Cause	Displays a detailed message (for which the message ID is DRM-nnnnn) to indicate the cause of the error. DRM Indicates that the message is a Protection Manager detailed message, and *nnnnn* indicates the message sequence number. If there is no information for this item, - is displayed.
Detail	Displays details on the cause of the error. If there is no information for this item, - is displayed. If the error occurred due to a Protection Products command execution failure, all of the standard output of the command is also displayed.

If an error occurred due to a Protection Manager command execution failure, a part of the standard output of the command is also displayed. For details about Protection Manager command messages, see the *HiCommand Protection Manager Messages* manual.

7.3 Responding to Detailed Messages

This section describes how to respond to a detailed message that may display during the operation of Protection Manager Console.

Important: If any of the operations that are associated with a particular message do not resolve the problem, please see the *HiCommand Protection Manager User's Guide*.

7.3.1 Responding to a Message in the Application Detail Window

If the items listed in Table 7.2 are displayed in the message dialog box, backup or restoration processing might be in progress on the connected application server.

Table 7.2 Error Data Shown in the Application Detail Window

Item	Contents	
Message	KAVX11003-E	KAVX11003-E
Location	Copy Controller	Copy Controller
Cause	DRM-22002	DRM-22002
Detail	Command: drmfsdisplay.exe KAVX0016-E, KAVX0017-E, or KAVX0105-E	Command: drmexgdisplay.exe KAVX0006-E Cause = DRM-10104

To resolve the issue, do the following:

- Wait for a while, and then re-display the Application Detail window.
- Check whether backup or restoration is currently in progress on the connected application server.
- Backup or restoration processing is currently in progress, if either of the following cases hold:
  - A dialog box indicating that backup or restoration is in progress is displayed in the Protection Manager Console that is connected to the application server.
  - On the application server, drmxxxbackup.exe or drmxxxrestore.exe is displayed as running, on the Processes page of Task Manager.
- If backup or restoration is being performed, you can display the Application Detail window once the processing has finished.

7.3.2 Responding to a Message in the Backup Catalog View

If the items listed in Table 7.3 are displayed in the message dialog box, one of the following might be the case: Protection Manager Copy Controller has not performed backup for the connected application server in the past, or a backup is in progress on the connected application server. If a backup is in progress, an error occurs because the dictionary map is updated during backup.

Table 7.3 Error Data Shown in the Backup Catalog View

Item	Contents
Message	KAVX11005-W
Location	Copy Controller
Cause	DRM-22004
Detail	Command: drmappcat.exe KAVX0024-E

To resolve the issue, make sure that Protection Manager Copy Controller has performed backup for the connected application server at least once.

If the above holds, do the following:

- Wait for a while, and then re-display the Backup Catalog View.
- Check whether or not a backup is in progress on the connected application server.
  - For details about how to perform such a check, see the part describing actions to be taken in section 7.3.1.
  - If a backup is currently in progress, you can display the Backup Catalog View once the backup processing has finished.

7.3.3 Responding to a Message in the Backup Detail Information Window

If the items listed in Table 7.4 are displayed in the message dialog box, a backup might be in progress on the connected application server. If a backup is currently in progress, an error occurs because the dictionary map is updated during processing.

Table 7.4 Error Data Shown in the Backup Detail Information Window

Item	Contents
Message	KAVX11003-E
Location	Copy Controller
Cause	DRM-22004
Detail	Command: drmfscat.exe or drmsqlcat.exe KAVX0024-E

To resolve the issue, do the following:

- Wait for a while, and then re-display the Backup Detail Information window.
- Check whether or not a backup is in progress on the connected application server.
  - For details about how to perform such a check, see the part describing actions to be taken in section 7.3.1.
  - If a backup is currently in progress, you can display the Backup Detail Information window once the backup processing has finished.

7.3.4 Responding to a Message During Mount Processing on a Backup Server

If the items listed in the table below are displayed in the message dialog box, one of the following might be the case: on the connected application server, either backup or restoration processing is currently in progress, or the item to be mounted is already mounted.

Table 7.5 Mount Processing Error Data

Item	Contents
Message	KAVX11011-E
Location	Copy Controller
Cause	DRM-22002
Detail	Command: EX_DRM_MOUNT.wsf KAVX0006-E Cause = DRM-10008 or Cause = DRM-10111

- If Cause = DRM-10008 is displayed, backup or restoration processing might be in progress on the application server. If backup or restoration processing is in progress on the application server, you cannot mount a copy group that is being backed up or restored on the backup server. To resolve the issue, do the following:

  a. Wait for a while, and then retry the mount operation.

  b. Check whether or not backup or restoration processing is in progress on the connected application server.

     For details about how to perform such a check, see the part describing actions to be taken in section 7.3.1.

     If backup or restoration processing is currently in progress, you can perform the mount operation once the processing has finished.

- If Cause = DRM-10111 is displayed, the mount operation might have been performed on a copy group that is already mounted on the backup server. To resolve the issue, check the copy group mounted on the backup server. For details about how to check the mounted copy group, see section 6.8.1.

7.4 Troubleshooting Issues that Cannot be Resolved Using Detailed Messages

If a problem remains unresolved, even after you have reviewed the detailed message, then consult the Protection Manager Console log information. For details, see section 7.5.

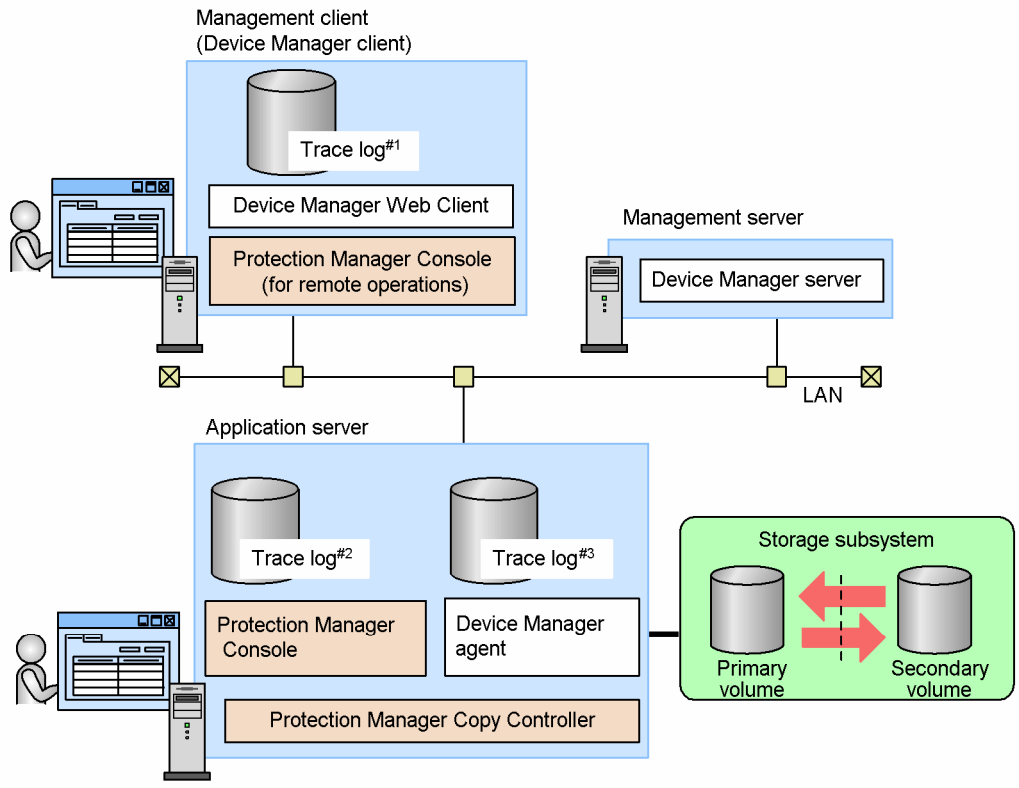
When the **OK** button is clicked in the error message dialog box where the detailed message is displayed, the application terminates in some cases, and does not in others. Though the cause of the error is not critical if the application does not terminate, we recommend analyzing the log and taking action as appropriate.

7.5 Reviewing the Protection Manager Console Log Information

If a problem remains unresolved, even after you have reviewed the error messages and detailed messages of Protection Manager Console, then identify the Protection Manager Console log files to be examined and analyze the information they provide (analysis of the Protection Manager Copy Controller log file might be necessary in some cases).

7.5.1 Analyzing Log Files

The log file to be analyzed can be identified by the Location information displayed in the detailed message. There are three types of Protection Manager Console log files, as shown in the following figure.



#1
application-server-IP-address or *host-name*_trace$.log
#2
trace$.log
#3
agt_trace.log, agt_trace.log.$

Figure 7.2 Protection Manager Console Log Files

The following terms (local execution, remote execution) are used in the descriptions.

- Local execution: Protection Manager Console is used on an application server.
- Remote execution: Protection Manager Console running on an application server is used from a management client (Device Manager client).

Refer to Table 7.6 to identify the log file to be analyzed, according to the mode of use for Protection Manager Console, and the error location displayed in the detailed message.

Table 7.6 Log Files to be Analyzed

Protection Manager Console Execution Method	Error Location Displayed in the Detailed Message	Log File to be Analyzed
Local execution	`Console`	`trace$.log`
	`Copy Controller`	▪ `trace$.log` ▪ A log file output from Protection Manager Copy Controller. See ***Note***
Remote execution	`Console`	*application-server-IP-address-or-host-name*`_trace$.log`
	`Copy Controller`	▪ *application-server-IP-address-or-host-name*`_trace$.log` ▪ A log file output from Protection Manager Copy Controller See ***Note***
	`Agent`	▪ agt_trace.log and agt_trace.log.*$* ▪ *application-server-IP-address-or- host-name*`_trace$.log`

Note: For details on log files output from Protection Manager Copy Controller, see the troubleshooting descriptions in the *HiCommand Protection Manager User's Guide*.

7.5.2 Log File Storage Locations of Protection Manager Console

Table 7.7 lists the locations where the Protection Manager Console log files are stored.

Table 7.7 Storage Locations of the Log Files of Protection Manager Console

Type	Name of the Log File of Protection Manager Console	Storage Location
Log files for local execution	`trace$.log`	*Protection-Manager-Console-Installation-directory-in-the-application-server*`\log\`
Log files for remote execution	*application-server-IP-address-or-host-name*`_trace`*`$`*`.log`	In Windows: *user-home-directory-in-the-management-client*`\drm_console\log\` In Solaris: *home-directory-in-the-management-client*`/drm_console/log/`
	`agt_trace.log` `agt_trace.log.`*`$`*	*Protection-Manager-Console-Installation-directory-in-the-application-server*`\log\`

There are multiple log files (from 2 to a maximum of 10) for each of the respective log file types, and they are used in sequence. The character *$* in the file name indicates the file number—its use is described as follows:

- For `trace$.log` files and *application-server-IP-address-or-host-name*`_trace`*`$`*`.log` `0` indicates the most recent file, and the greater the number, the older the log file.
- For `agt_trace.log` (`agt_trace.log.`*`$`*) files, `agt_trace.log` is the most recent file. For the other log files (`agt_trace.log.`*`$`*), the greater the number, the older the log file.

  The size and maximum number of the log files can be specified in the Protection Manager Console settings file.
- When more than one Protection Manager Console is locally started concurrently on the same application server, the `trace$.log` files are created:
  - For the Protection Manager Console started first: `trace$.log`
  - For the Protection Manager Console started second: `trace$.log.1`
  - For the Protection Manager Console started (*n*+1)th: `trace$.log.`*n*
- When more than one Protection Manager Console is remotely started concurrently on the same application server from a management client, the corresponding *application-server-IP-address-or-host-name*`_trace$.log` files are created:
  - For the Protection Manager Console started first: *application-server-IP-address-or-host-name*`_trace$.log`
  - For the Protection Manager Console started second: *application-server-IP-address-or-host-name*`_trace$.log.1`
  - For the Protection Manager Console started (*n*+1)th: *application-server-IP-address-or-host-name*`_trace$.log.`*n*

7.5.3 Log File Output Information

The following information is output to the Protection Manager Console log files.

- Internal functions used by the internal processing sequence from the start to the end of a process specified by Protection Manager Console
- The time of execution and the command execution process ID for the processing that was performed at the system call level
- Keywords showing normal and abnormal processing
- Messages showing error causes

Table 7.8 lists the items that are output to the Protection Manager Console log files. The items are displayed in messages in the order shown in the table. The same log format is used to output log information for all three types of Protection Manager Console log files.

Table 7.8 Output Items in the Trace Logs of Protection Manager Console

Output Item	Description
Date	Date when the log was output, using the *yyyy/mm/dd* format
Time	Time when the log was output, using the *hh:mm:ss.sss* format
Process ID	Process ID
Thread ID	Thread ID
Class name	Class name. When the specified log level is `10` or less, a hyphen (–) is displayed.
Method name	Method name. When the specified log level is `10` or less, a hyphen (–) is displayed.
Message ID	ID of the message. When the specified log level is `0` or `10`, the message ID is formatted as `KAVX`*ppmmm–z*. ▪ `KAVX`: Prefix for Protection Manager messages ▪ *pp*: Component of Protection Manager. ▪ *mmm*: Message sequence number. ▪ `z`: Message type. Displays either `E`, `W`, or `I`. `E`: Error `W`: Warning `I`: Information
Text	Message Text.

The log file to be analyzed contain a line with the message ID which was displayed in the error message window, enabling you to analyze the information chronologically.

Note: For the log file agt_trace.log on the application server, chronological analysis may not be simple since the same log file is used for multiple connections, when the server is connected to multiple Device Manager clients. Find the most recent line with the message ID that was displayed on the error message window, to determine the thread ID on the line. Then, analyze the lines with the same thread ID chronologically.

7.5.4 Using the Data Collection Tool

In the case of local execution, you can execute the data collection tool to collect the necessary data for analyzing problems. For details about the data collection tool, see the description of troubleshooting in the *HiCommand Protection Manager User's Guide*. In the case of remote execution, the data collection tool cannot collect data on a management client.

7.6 Reviewing Data from Prerequisite Products

If a problem remains unresolved, even after you have reviewed the message and the log files output from Protection Manager Console, then collect data regarding the prerequisite products on the application server.

The following information should be collected. For details on how to collect and analyze the data, see the troubleshooting descriptions in the *HiCommand Protection Manager User's Guide*.

- OS information on the application server
- Protection Manager Copy Controller information
- RAID Manager information
- Database information (for SQL Server database or Exchange database only)

Device Manager agent information should also be collected as necessary, in an environment where Protection Manager Console is run by remote execution with linkage to Device Manager.

Note: If a problem remains unresolved, even after you have examined the Protection Manager Console log file agt_trace.log, then collect Device Manager agent information. For details on output messages and trace logs from the Device Manager agent, please see the chapter for Device Manager agent troubleshooting in the Device Manager manual.

7.7 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

Appendix A Environment Setting Command for Device Manager Linkage

In order to start Protection Manager Console from a Device Manager client, it is necessary to copy files required for linkage into the Device Manager agent installation directory.

Normally, the necessary files are copied into the Device Manager agent installation directory when Protection Manager Console is installed. The files are deleted when Protection Manager Console is uninstalled.

If the files copied to the Device Manager agent installation directory are corrupted after the Protection Manager Console installation, they must be deleted and re-copied.

Protection Manager Console provides commands to copy and delete the files that are necessary for linkage to Device Manager.

- The command that copies the files required for Device Manager linkage is `ptmguiinst.exe`
- The command that deletes the files required for Device Manager linkage is `ptmguiuninst.exe`

Execute these commands from the command prompt to copy or delete the files necessary for Device Manager linkage.

A.1 Copying Files Required for Device Manager Linkage

To copy the files required for Device Manager linkage to the installation directory of Device Manager agent, execute the `ptmguiinst.exe` command from the command prompt on the application server where Protection Manager Console and Device Manager agent are installed.

Make sure that the following conditions are satisfied before executing the command:

- Device Manager agent is installed.
- Services for Device Manager agent are stopped.
- Protection Manager Console is installed.

Command name:

`ptmguiinst.exe`

Installation destination:

Protection-Manager-Console-installation-directory`\bin`

Return code:

`0`: Normal termination

`1`: Termination with an error

The execution results for the `ptmguiinst.exe` command are output to the standard output. For details about output messages, see the *HiCommand Protection Manager Messages*.

A.2 Deleting Files Required for Device Manager Linkage

To delete the files required for Device Manager linkage from the installation directory of Device Manager agent, execute the `ptmguiuninst.exe` command from the command prompt on the application server where Protection Manager Console and Device Manager agent are installed.

Make sure that the following conditions are satisfied before executing the command:

- Device Manager agent is installed.
- Services for Device Manager agent are stopped.
- Protection Manager Console is installed.

Command name

`ptmguiuninst.exe`

Installation destination:

Protection-Manager-Console-installation-directory`\bin`

Return code:

`0`: Normal termination

`1`: Termination with an error

The execution results for the `ptmguiuninst.exe` command are output to the standard output. For details about output messages, see the *HiCommand Protection Manager Messages*.

Glossary

application information	A list of file systems, database instances, and storage configuration information, that is to be backed up. It is displayed on the Application View in Protection Manager Console. You can execute a backup by selecting the objects to be backed up from the application information.
application map file	One of the map files making up a dictionary map file. Application map files are used to keep track of the mapping information between the application data to be backed up, and the files on the file system.
Application View	A page displayed on the main window of Protection Manager Console, on which application information is displayed, showing a list of file systems and database instances to be either backed up or restored.
backup catalog	A collection of information necessary to manage the history and generations of backups performed using Protection Products programs. When a backup is executed, a record containing information related to the backup is created within the backup catalog. When backed-up data is restored, Protection Products programs reference the backup catalog information, and execute accordingly.
Backup Catalog View	A page displayed on the main window of Protection Manager Console. Catalog information is displayed, showing a table of file systems and database instances that have been backed up thus far.
backup ID	A part of the information contained in the backup catalog. Backup IDs are used to differentiate backup data, and are assigned automatically when backups are performed using Protection Products.
backup information	Various information that is recorded in a backup catalog when Protection Products programs are used to perform a backup.
backup job information	A list of backup jobs to be automatically executed based on a specified schedule. This list is displayed in the Protection Manager Console Backup Job View. To register a backup job, select it from the application information.
Backup Job View	A page displayed on the Main window of Protection Manager Console. Backup Job View displays backup job information (a list of backup jobs to be automatically executed based on the schedule).

Catalog information	A list of file systems and database instances that have been backed up thus far. Catalog information can be viewed in the Protection Manager Console Backup Catalog View. Restoration can be performed by selecting the item to restore from the catalog information.
RAID Manager	Software used to control Hitachi TagmaStore/Lightning/Thunder Series storage subsystems. RAID Manager is installed on a host connected to the storage subsystem.
cluster software	Software used to enhance overall system performance through multiplex system configurations. For Windows, Microsoft Cluster Service is supported.
copy group	A *copy group* consists of a primary volume and secondary volume that are synchronized and split using volume replication functionality and RAID Manager functionality. A *copy group* can also be called a *pair volume*.
copy group map file	One of the map files making up a dictionary map file. Copy group map files are used to keep track of the mapping information between the primary volume and its corresponding secondary volumes.
core map file	One of the map files making up a dictionary map file. Core map files are used to keep track of the mapping information from the mount point directory on the file system to the disk number within the RAID device.
DBMS	An abbreviation for *Database Management System*. A DBMS consists of programs that manage databases.
dictionary map file	A file required for automating backup processing using Protection Products. A dictionary map file keeps track of mapping information, from the objects to be backed up to the RAID devices. A dictionary map file consists of three types of map files, and a backup catalog. Application map file Core map file Copy group map file Backup catalog
disk set	For Protection Products programs, in a dynamic disk configuration, a group consisting of one or more dynamic disks and one or more logical volumes allocated to the dynamic disks is called a *disk set*. In LDM environments, you can perform backups or restorations on units as small as disk groups.

dynamic disk	Dynamic disk functionality can be used to create a disk set by using the logical disk manager (LDM) that comes with Windows, or to create a disk group by using VxVM. The term *dynamic disk* indicates physical disks composing a disk group or disk set. You can combine or split one or more dynamic disks to create a logical volume (dynamic volume).
failover	The action of automatically switching to a backup system when an error occurs in a system that has been duplicated (that is, multiple instances of the system were made) using cluster software.
freezing a database	DBMS temporarily stops I/O operations for the disk on which the database is stored. Transactions from applications are controlled by DBMS until the database is thawed. If a database is frozen when a paired volume is synchronized, the primary and secondary volumes will be identical. Backing up the database in this state will ensure that its integrity is maintained during backup processing.
HiCommand Device Manager	A product that manages storage devices, including devices, logical volumes and physical volumes. It consists of agents that collect information from each host, and a manager that controls management functions.
HiCommand Protection Manager Console	This program allows the backup and restoration functionality provided by Protection Products programs to be used from a screen.
HiCommand Protection Manager Copy Controller	A program product that performs backups and restorations for Windows file systems. It is also a prerequisite program for backing up databases such as Exchange Server and SQL Server.
HiCommand Protection Manager for Exchange	A program that backs up and restores Exchange Server databases. HiCommand Protection Manager for Exchange is an optional program product.
HiCommand Protection Manager for SQL	A program that backs up and restores SQL Server databases. HiCommand Protection Manager for SQL is an optional program product.
HiCommand Protection Products	A general name for the following products. HiCommand Protection Manager Copy Controller HiCommand Protection Manager Copy Controller (x64) HiCommand Protection Manager for SQL HiCommand Protection Manager for Exchange HiCommand Protection Manager for Exchange 2007 HiCommand Protection Manager Console
pair volume	A pair of physical volumes that are mirror-controlled by RAID Manager and the volume replication functions.

Setup GUI	Functionality that allows you to set up an operating environment for Protection Manager via a GUI. Using the GUI means it is not necessary to execute commands or edit the configuration files. Setup GUI becomes available when Protection Manager Console is installed.
storage group	A method provided by Exchange Server for managing a grouping of multiple databases. Multiple databases can be managed together since databases within the same group use a common transaction log.
target ID	A number used to distinguish the devices connected via a SCSI bus. It is also called a SCSI ID.
VDI	An abbreviation of *Virtual Device Interface*: an application interface for volume replication functionality provided by SQL Server.
volume replication functions	Generic term used in this manual to refer to high-speed volume replication functions in the storage subsystem (such as ShadowImage and TrueCopy). The mirror control function provided by the storage subsystem can be used to quickly create a replica of the volume without passing through the LAN.
VSS	An An abbreviation of *Volume Shadow Copy Service*: one of the storage support functions usable in Windows Server 2003. Normally, when database data stored on a storage subsystem volume is copied to another volume, access from hosts (database applications) must be suspended and the database must be frozen. If VSS is used, however, the OS functionality can control transactions for database applications and I/O operations for a volume, and the database can be frozen without the previously mentioned suspensions. This provides higher reliability for backup operations. To use VSS to freeze a database application, however, VSS must support the database application. Protection Products programs handle Exchange Server 2003 as a database application supported by VSS, and support file system backup and restoration operations using VSS.

Acronyms and Abbreviations

API	application programming interface
CDE	Common Desktop Environment
CD-ROM	compact disk – read-only memory
CLI	command line interface
DB	database
DKC	Disk Contorller
DLL	dynamic linking library
DRM	Protection Manager detailed message prefix
GB	gigabyte
GUI	graphical user interface
IPF	Itanium Processor Family
JRE	Java Runtime Environment
JWS	Java Wedb Start
kB	kilobytes
LAN	local area network
LDEV	logical device
LU	logical unit
LUN	logical unit number
LVM	logical volume manager
MB	megabytes
MSCS	Micro Cluster Service
NTFS	NT file system
OS	operating system
PC	personal computer system
SAN	storage area network
SVP	service processor
TB	terabyte
TID	target ID
UR	Universal Replicator
VCS	VERITAS Cluster Server
VDI	virtual device interface
VSS	volume shadow copy service

Index