HITACHI
DATA SYSTEMS

HiCommand® Replication Monitor Installation and Configuration Guide

MK-96HC131-03

VERITAS is a trademark or 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 Server 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.

HiCommand Replication Monitor includes technologies developed in the Business Grid Computing Project promoted by Japan's Ministry of Economy, Trade and Industry for 3 years since the fiscal year 2003.

Other product and company names mentioned in this document may be the trademarks of their respective owners. Throughout this document Hitachi has attempted to distinguish trademarks from descriptive terms by writing the name with the capitalization used by the manufacturer, or by writing the name with initial capital letters. Hitachi cannot attest to the accuracy of this information. Use of a trademark in this document should not be regarded as affecting the validity of the trademark.

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-96HC131-00	June 2006	Initial Release
MK-96HC131-01	November 2006	Revision 1, supersedes and replaces MK-96HC131-00
MK-96HC131-02	February 2007	Revision 2, supersedes and replaces MK-96HC131-01
MK-96HC131-03	June 2007	Revision 3, supersedes and replaces MK-96HC131-02

Source Document(s) for this Revision

- *HiCommand Replication Monitor Installation and Configuration Guide* (Q code final) dated May 31, 2007

Preface

This manual describes the installation and configuration procedures for the HiCommand Replication Monitor. In this manual, HiCommand Replication Monitor is abbreviated to *Replication Monitor*.

Intended Readers

This manual is intended for those who use Replication Monitor to operate and manage a system that uses storage subsystems (magnetic disk array units).

In addition to reading this manual, Replication Monitor users should also read the manual *HiCommand Replication Monitor User's Guide* to gain a general understanding of the Replication Monitor products.

Replication Monitor users should have the following:

Knowledge of storage subsystems and related software

- A basic knowledge of SANs (Storage Area Networks) and management software used to operate storage subsystems
- Knowledge of storage subsystem volume replication functionality (such as ShadowImage or TrueCopy)

Knowledge of prerequisite products

- Ability to use a prerequisite operating system and a Web browser
- A basic knowledge of Device Manager
- A basic knowledge of Business Continuity Manager (when managing on a mainframe system)

Software Version

This document revision applies to HiCommand Replication Monitor version 5.7.

Convention for Storage Capacity Values

Storage capacity values displayed by HiCommand Replication Monitor 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™ Device Manager Server Installation and Configuration Guide*, MK-91HC002
- *HiCommand™ Device Manager Agent Installation Guide*, MK-92HC019
- *HiCommand™ Device Manager Web Client User's Guide*, MK-92HC001
- *HiCommand™ Device Manager Error Codes*, MK-92HC016
- *HiCommand™ Replication Monitor User's Guide*, MK-94HC093

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 Designing Systems

The first consideration when you decide to design a system in which Replication Monitor is used is whether Replication Monitor can be set up using the standard system configuration. If Replication Monitor cannot be implemented without deviating from the standard configuration, we recommend that you thoroughly examine the tasks and workflows you employ before making the necessary changes to the standard configuration.

This chapter explains the standard configuration, the functions of the system components, the relationships and installation locations of the components, the flow of control and data between components, and the points to consider before putting together a non-standard configuration.

- Standard Configuration of a Replication Monitor System (see section 1.1)
- Possible Non-Standard Configurations (see section 1.2)
- Relationship Among a System Configuration, Available Functions, and Information That Can Be Acquired (in an Open System) (see section 1.3)
- Replication Monitor-Related Programs (see section 1.4)
- Setting the Environment for Deploying Replication Monitor (see section 1.5)

1.1 Standard Configuration of a Replication Monitor System

This section explains the standard configuration of a system in which Replication Monitor is used.

Although this section describes configurations using open system hosts and mainframe system hosts separately, you can use Replication Monitor in mixed environments that include both open system and mainframe system hosts.

1.1.1 Standard Configuration of an Open System

The recommended standard configuration for an open system can incorporate multiple management servers or a single management server.

1.1.1.1 Open system configuration with multiple management servers

This configuration consists of two sites: a primary and a secondary site.

- Each site has its own management server.
- The Device Manager server installed on a management server manages the volumes of the storage subsystems located at that site.
- The Replication Monitor server runs on the management server at the primary site.

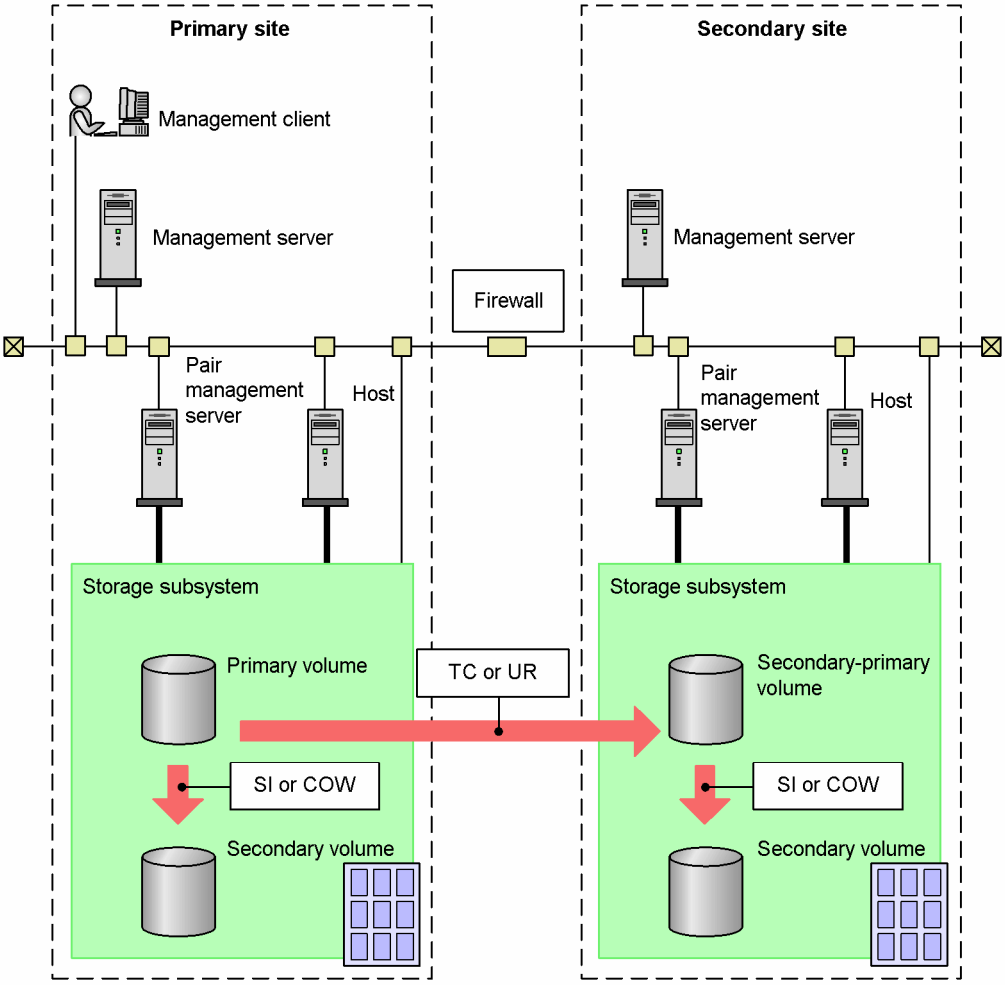

Figure 1.1 Standard Open System Configuration with Multiple Management Servers

Table 1.1 Hardware and Software Components (Open System with Multiple Management Servers)

Hardware Components		Software Components
Primary site	Management client	Web browser
	Management server	Device Manager server Replication Monitor server
	Pair management server	Device Manager agent CCI Replication Monitor agent
	Host (application server)	Device Manager agent User application programs
	Storage subsystem	--

Hardware Components		Software Components
Secondary site	Management server	Device Manager server Replication Monitor server#
	Pair management server	Device Manager agent CCI Replication Monitor agent
	Host (application server)	Device Manager agent User application programs
	Storage subsystem	--

As with the management server at the primary site, the purpose of the management server on which the Replication Monitor server is installed at the secondary site is to duplicate a management server at the primary site and the secondary site. If the management server at the primary site stops running, the management server at the secondary site can monitor copy pairs. If you will not duplicate the management server, you do not need to install the Replication Monitor server on the management server at the secondary site.

Note:

We recommend that you configure the system so that all copy pairs in the storage subsystems are managed by pair management servers. If you have to collect pair status information on copy pairs that are not managed by a pair management server, it takes a long time because you need to perform a Device Manager refresh operation (which updates the Device Manager database).

1.1.1.2 Open system configuration with one management server

This configuration consists of a single management server, a number of storage subsystems, and one or more pair management servers.

- The Device Manager server installed on the management server manages the volumes of all storage subsystems.
- The Replication Monitor server runs on the management server.

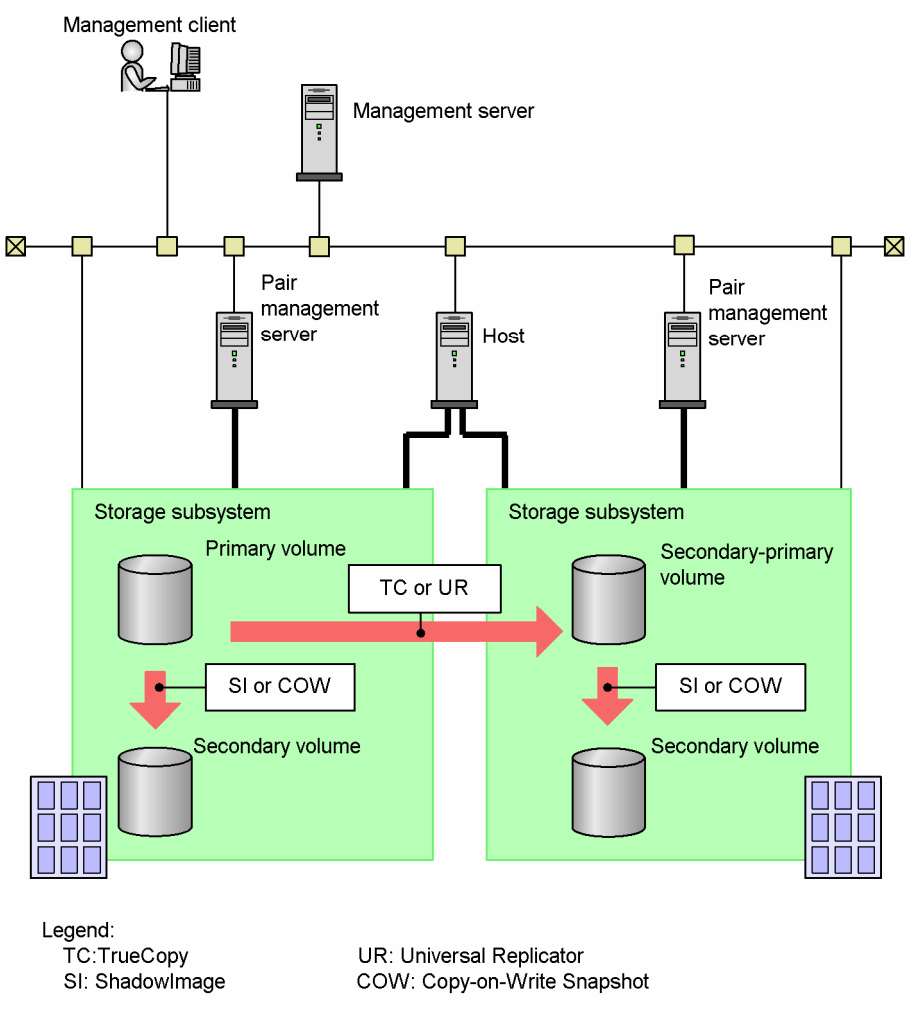

Figure 1.2 Standard Open System Configuration with One Management Server

Table 1.2 Hardware and Software Components (Open System with One Management Server)

Hardware Components	Software Components
Management client	Web browser
Management server	Device Manager server Replication Monitor server
Pair management server	Device Manager agent CCI Replication Monitor agent
Host (application server)	Device Manager agent User application programs
Storage subsystem	--

Note: We recommend that you configure the system so that all copy pairs in the storage subsystems are managed by pair management servers. If you have to collect pair status information on copy pairs that are not managed by a pair management server, it takes a long time because you need to perform a Device Manager refresh operation (which updates the Device Manager database).

1.1.2 Standard Configuration of a Mainframe System

Figure 1.3 illustrates the recommended standard configuration for a mainframe system.

This configuration consists of three sites: a primary, an intermediate, and a secondary site.

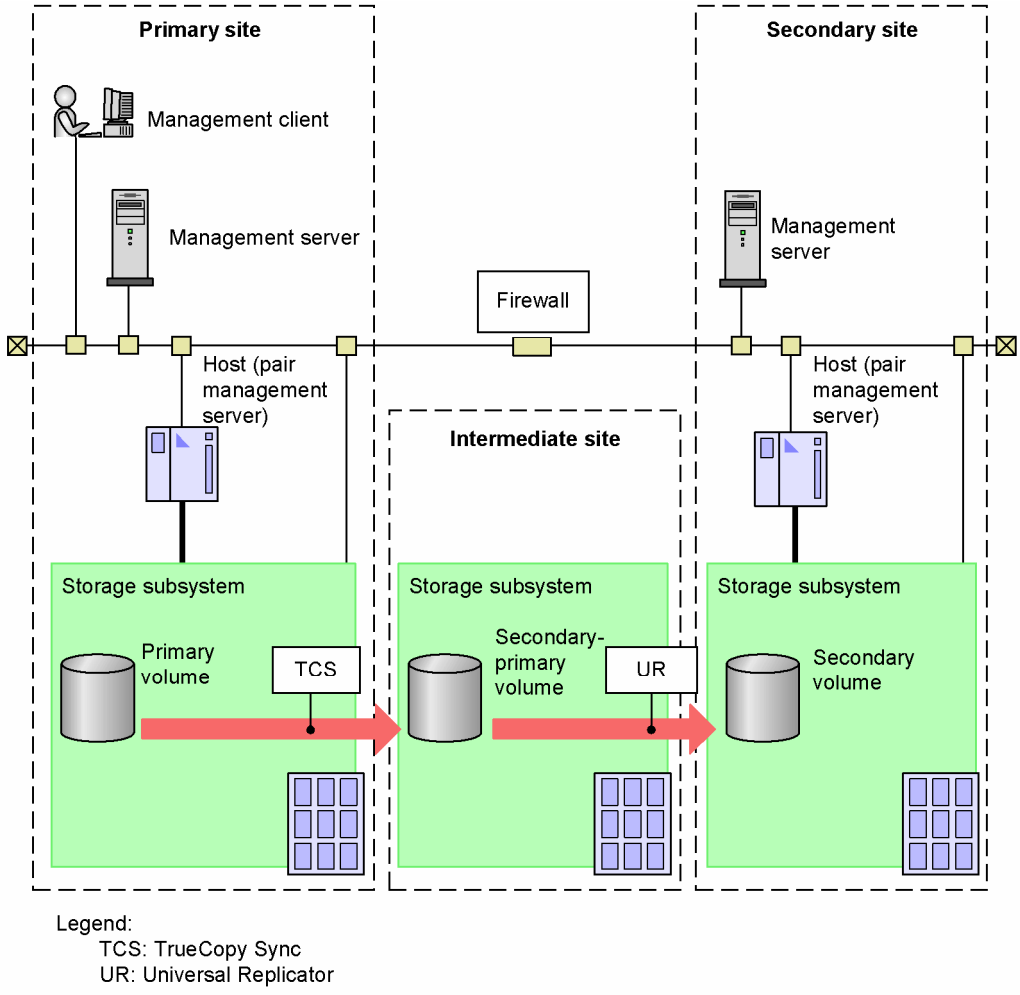

Figure 1.3 Standard System Configuration (Mainframe System)

Table 1.3 Hardware and Software Components (Mainframe System)

Hardware Components		Software Components
Primary site	Management client	Web browser
	Management server	Device Manager server Replication Monitor server
	Host (pair management server)	Business Continuity Manager User application programs
	Storage subsystem	--
Intermediate site	Storage subsystem	--
Secondary site	Management server#	Device Manager server Replication Monitor server
	Host (pair management server)	Business Continuity Manager User application programs
	Storage subsystem	--

As with the management server at the primary site, the purpose of the management server on which the Replication Monitor server is installed at the secondary site is to duplicate a management server at the primary site and the secondary site. If the management server at the primary site stops running, the management server at the secondary site can monitor copy pairs. If you will not duplicate the management server, you do not need the management server at the secondary site.

The standard configuration includes all of the independently installed hardware components that comprise a system.

The following tables describe the relationship between the hardware components and their installed software components, separated into open system and mainframe system configurations.

Table 1.4 Relationship Between Hardware and Software Components (Open System)

Hardware Component	Software Component					
	Device Manager Server	Replication Monitor Server	Device Manager Agent	Replication Monitor Agent	CCI	Web Browser
Management client	--	--	--	--	--	Y
Management server	Y	Y#1	--	--	--	--
Pair management server	--	--	Y	Y#2	Y	--
Host	--	--	Y#3	--	--	--

Legend:

Y: Denotes that the indicated software component is installed on the corresponding hardware component.

--: Not applicable

#1

Some management servers do not need to include the Replication Monitor server.

#2

Some pair management servers do not need to include the Replication Monitor agent. For details, see section 1.2.1.

#3

Some hosts do not need to include the Device Manager agent. For details, see section 1.2.1.

Table 1.5 Relationship Between Hardware and Software (Mainframe System)

Hardware Component	Software Component			
	Device Manager Server	Replication Monitor Server	Business Continuity Manager	Web Browser
Management client	--	--	--	Y
Management server	Y	Y	--	--
Host (pair management server)#	--	--	Y	--

Legend:

Y: Denotes that the indicated software component is installed on the corresponding hardware component.

--: Not applicable

#

On a mainframe system, a host running Business Continuity Manager is also referred to as a pair management server.

The following describes the relationship between the sites and the hardware components:

For an open system:

- Each site must have one management server.
- One of the sites must have a management server on which the Replication Monitor server is installed.
- Multiple pair management servers can be set up at a site.

For a mainframe system:

- One of the sites must have a management server on which the Replication Monitor server is installed. Other sites do not need any management servers.

1.1.3 Software Components Comprising a System

The following sections provide an overview of the functions of the software components, separated into open system and mainframe system descriptions.

1.1.3.1 Software Components (Open System)

- Replication Monitor server

  The Replication Monitor server is the core component of Replication Monitor. The Replication Monitor server maintains its own database containing information collected by the Device Manager server and copy pair information collected by the Device Manager agent and Replication Monitor agent, and provides this information to the user through Web Client. The Replication Monitor server also updates this database by collecting the most recent information when a user requests an update or when a periodic update is performed.

- Device Manager server

  The Device Manager server maintains a database of information collected by the Device Manager agent and information that this server collects directly from the storage subsystems, and provides this information to the Replication Monitor server. The Device Manager server also updates this database by collecting the most recent information when a user requests an update or when a periodic update is performed.

- Device Manager agent

  The Device Manager agent on a host provides information about that host to the Device Manager server.

  The Device Manager agent on a pair management server collects configuration information on the copy pairs being managed by that pair management server, and provides this information to the Replication Monitor server. Based on instructions from the Device Manager server, the Device Manager agent also passes along pair status change instructions to CCI.

- Replication Monitor agent

  The Replication Monitor agent collects status information on the copy pairs that are managed by its pair management server, and provides this information to the Replication Monitor server.

- CCI

  CCI collects information on its managed copy pairs, and provides this information to the Replication Monitor agent and the Device Manager agent. CCI also passes along pair status change instructions to the storage subsystem.

1.1.3.2 Software Components (Mainframe System)

- Replication Monitor server

  The Replication Monitor server is the core component of Replication Monitor.

The Replication Monitor server maintains its own database of information that it collects from the Business Continuity Manager on the hosts, and provides this information to the user through Web Client. The Replication Monitor server also updates this database by collecting the most recent information when a user requests an update or when a periodic update is performed.

- Device Manager server

  The Device Manager server is required when the Replication Monitor server is installed. However the Device Manager server has no functionality for mainframe systems.

- Business Continuity Manager

  Business Continuity Manager collects information about the copy pairs it manages and provides this information to the Replication Monitor server.

1.1.4 Hardware Components Comprising a System

The following provides a functional overview of and requirements for the hardware components.

- Management client

  The machine on which the user, utilizing a Web browser, runs Web Client for Replication Monitor.

- Management server

  The machine on which the Device Manager server is installed.

  The Replication Monitor server might or might not be installed on this machine.

- Pair management server (open system)

  The machine on which the Device Manager agent and CCI are installed. This server is used to manage and collect information on copy pairs defined in the CCI configuration definition file. You can collect configuration information and change the status of the copy pairs managed by a pair management server.

  The Replication Monitor agent might or might not be installed on this machine. If the Replication Monitor agent is installed, you can collect status information on the copy pairs managed by the pair management server.

  The pair management server can also be used as a host (application server).

- Pair management server (mainframe system)

  In a mainframe system, a host (application server) on which Business Continuity Manager is installed might also be called a pair management server.

- Host (open system)

  The machine on which application programs are installed. It is also called an application server. The Device Manager agent might or might not be installed on this machine. If the Device Manager agent is installed, information about that host can be collected.

- Host (mainframe system)

  The machine on which application programs are installed. It is also called an application server.

A host on which Business Continuity Manager is installed is also called a pair management server. Configuration information and pair status information on its managed copy pairs can be collected from a host that is configured in this way.

- Storage subsystem

  An external storage device that is connected to the host. With the exception of the T3, which is not supported, Replication Monitor supports the same storage subsystems that Device Manager supports. For details, see the *HiCommand Device Manager Server Installation and Configuration Guide*.

By using a standard configuration primary site as an example, this section explains the flow of control and data between programs.

1.1.5 Flow of Control and Data in an Open System

Figure 1.4 shows the flow of control and data between programs in an open system.

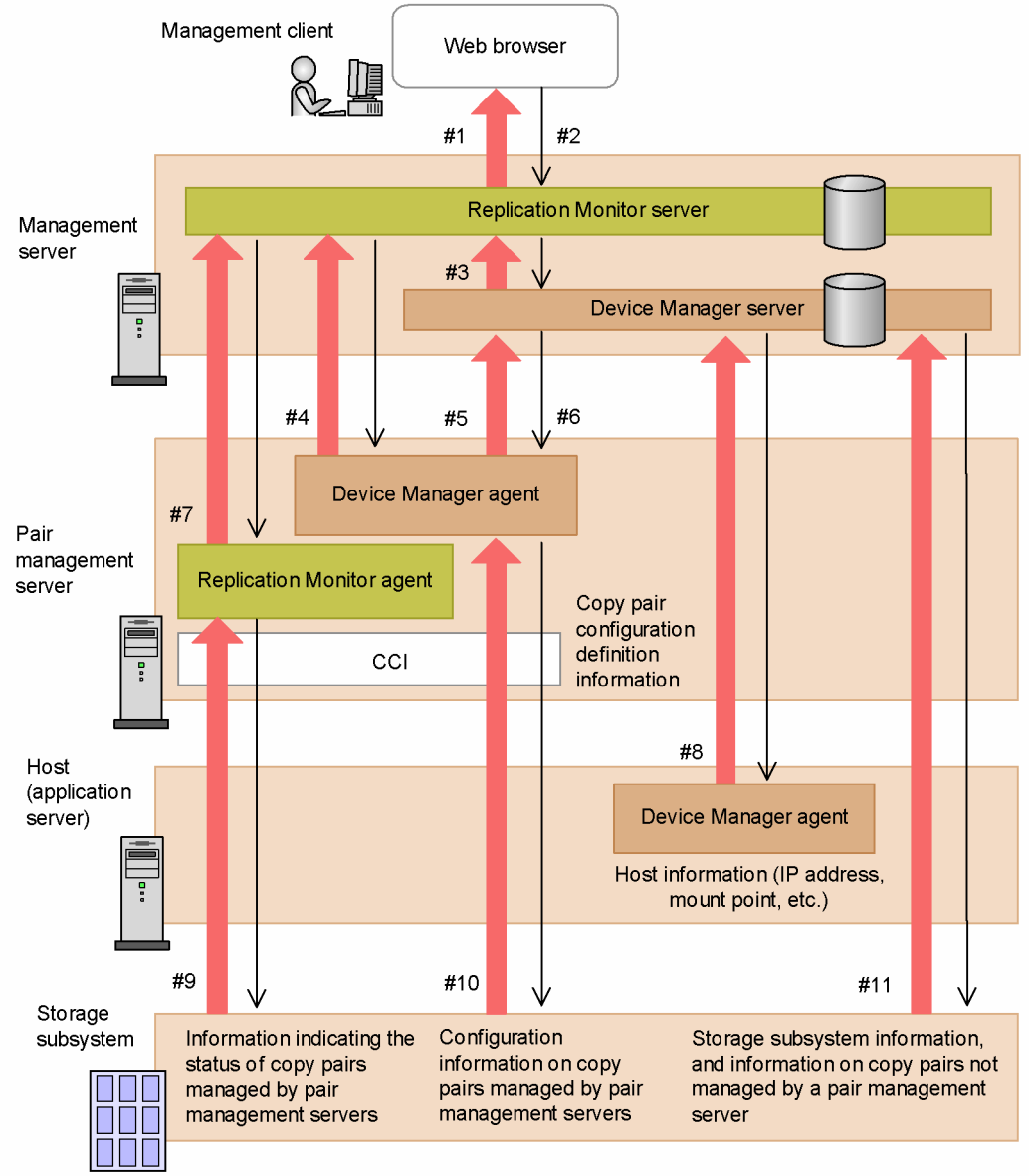

Figure 1.4 Flow of Control and Data (Open System)

The numbers that appear in the following explanations refer to the numbers next to the arrows in Figure 1.4.

Web browser on a management client

The Web browser collects the host, storage subsystem, and copy pair information (#1) maintained in the database from Replication Monitor server on the management server, and displays this information in a window.

In response to a request from a user to update the copy pair configuration information (#2) or copy pair status (#2), the Web browser asks the management server to update the information in the Replication Monitor server database. In response to a request from a user to change the copy pair status (#2), the Web browser asks the Device Manager server on the management server to implement the pair status change.

Replication Monitor server on the management server

The Replication Monitor server collects the following information from the Device Manager server, and from the Device Manager agent and Replication Monitor agent on the pair management servers, and updates this information in the Replication Monitor server database:

- Configuration information on copy pairs managed by the pair management servers (#3, #4)
- Information indicating the pair status of copy pairs managed by the pair management servers (#7)
- Host information (#3)
- Storage subsystem information (#3)
- Information on copy pairs not managed by a pair management server (#3)

The information in the Replication Monitor server database is updated periodically at the specified time intervals, or when there is a user request to update the copy pair configuration information or copy pair status (#2).

Device Manager server on the management server

The Device Manager server collects the following information from the storage subsystems, and from the Device Manager agent on the pair management servers and hosts, and uses this information to update the Device Manager server database:

- Configuration information on copy pairs managed by the pair management servers (#5)
- Host information (#8)
- Storage subsystem information (#11)
- Information on copy pairs not managed by a pair management server (#11)

The information in the Device Manager server database is updated periodically at the specified time intervals, or when there is a user request to update the copy pair configuration information or copy pair status (#2).

Device Manager agent on a pair management server

The Device Manager agent collects the following information (#10) from the storage subsystem by means of CCI:

- Configuration information on copy pairs managed by pair management servers

In response to instructions from the Device Manager server (#6), the Device Manager agent changes the pair status of copy pairs by means of CCI.

Replication Monitor agent on a pair management server

The Replication Monitor agent collects the following information (#9) from the storage subsystem by means of CCI:

- Information indicating the pair status of copy pairs managed by pair management servers

Device Manager agent on a host

The Device Manager agent sends the IP address, mount point of the LU, and other information about the host to the Device Manager server on the management server.

1.1.6 Flow of Control and Data in a Mainframe System

Figure 1.5 shows the flow of control and data between programs in a mainframe system.

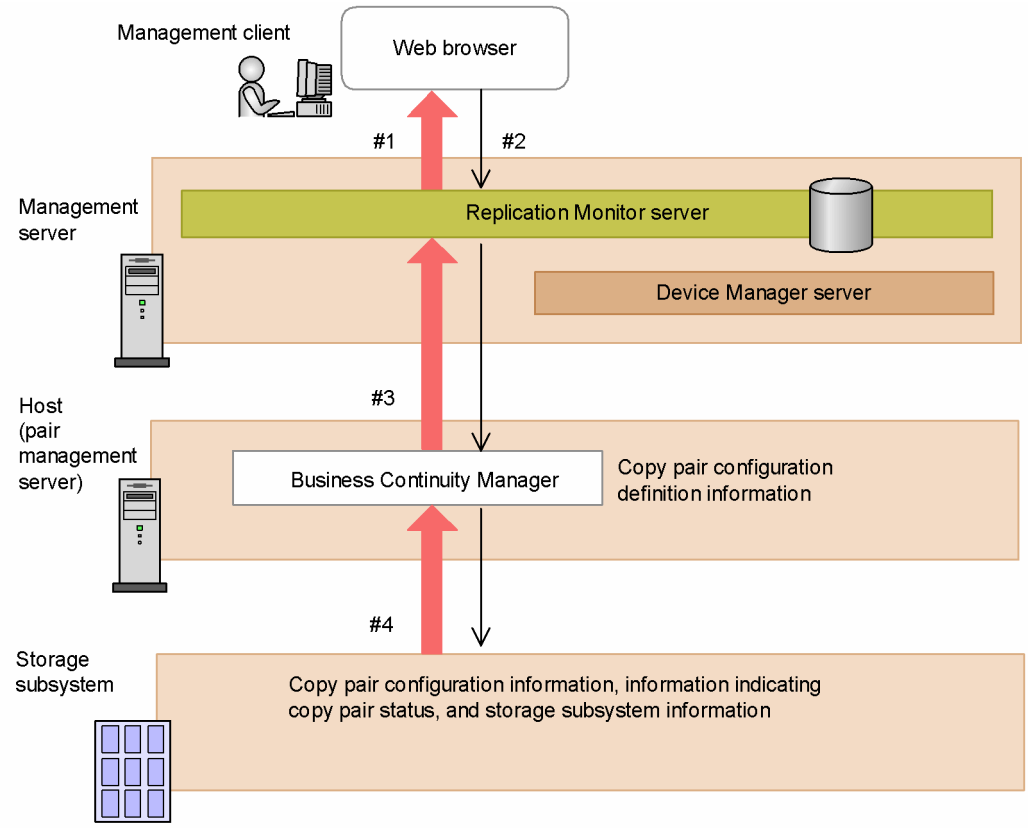

Figure 1.5 Flow of Control and Data (Mainframe System)

The numbers that appear in the following explanations refer to the numbers next to the arrows in Figure 1.5.

Web browser on a management client

The Web browser collects the host, storage subsystem, and copy pair information (#1) maintained in the database from the Replication Monitor server on the management server, and displays this information in a window.

In response to a request from the user to update the copy pair configuration information (#2) or copy pair status (#2), the Web browser asks the management server to update the information in the Replication Monitor server database.

Replication Monitor server on the management server

The Replication Monitor server collects the following information from the Business Continuity Manager on the hosts (#3), and maintains this information in the Replication Monitor server database:

– Configuration information on copy pairs managed by Business Continuity Manager

- Information indicating the pair status of copy pairs managed by Business Continuity Manager
- Host information
- Storage subsystem information

The information in the Replication Monitor server database is updated periodically at the specified time intervals, or when there is a user request to update the copy pair configuration information or copy pair status (#2).

Business Continuity Manager on a host

Business Continuity Manager obtains the following information (#4) from the storage subsystem:

- Configuration information on copy pairs managed by Business Continuity Manager
- Information indicating the pair status of copy pairs managed by Business Continuity Manager
- Storage subsystem information

1.2 Possible Non-Standard Configurations

This section describes considerations when you think about setting up a non-standard system configuration that uses Replication Monitor.

Note that there are functional limitations and restrictions on the information that can be acquired and viewed in a non-standard configuration. For details on available functions and information that can be viewed in each system configuration, see section 1.3.

1.2.1 Non-Standard Open System Configurations

If you are thinking about setting up a non-standard configuration with an open system, the three considerations listed below are important. These three considerations concern the tasks and workflows that you employ, and are designed to allow you to build a system that employs a non-standard configuration by helping you determine which of the many choices you should select.

1. Whether to install Replication Monitor agent on the pair management servers
2. Whether to set up the pair management servers independently of the hosts, whether to set up the pair management servers on the same machine as the hosts, or whether to not set up any pair management servers
3. Whether to install the Device Manager agent on hosts that do not act as pair management servers

The following describes differences in available functionality and performance between the choices derived from these three considerations.

- Installation of the Replication Monitor agent

  You can collect information on copy pair status via the Replication Monitor agent if the Replication Monitor agent is installed on the pair management server.

  You cannot collect information on copy pair status via the Replication Monitor agent, which means that updating information on copy pair status takes a long time, if the Replication Monitor agent is not installed on the pair management server.

- Setup of pair management servers

  Setting up the pair management servers independently of the hosts reduces the workload on the hosts, because the pair management servers handle the processing for collecting copy pair information.

  Setting up the pair management servers together with the hosts increases the workload on the hosts, due to the processing required to collect copy pair information.

  If there are no pair management servers, you cannot collect configuration or status information of copy pairs via agents, nor can you change copy pair status.

- Installation of the Device Manager agent on the host

  You can collect IP address, mount point, and other information about the host, if the Device Manager agent is installed on the host that does not act as a pair management server.

You cannot collect IP address, mount point, or other information about the host, if the Device Manager agent is not installed on the host that does not act as a pair management server.

1.2.2 Non-Standard Mainframe System Configurations

For a mainframe system, there are no special considerations relevant to the tasks and workflows you employ that might affect decisions about the configuration. So, there are no real non-standard configuration points to consider, other than those related to the number of sites or hosts (pair management servers) to set up.

1.3 Relationships Between Configuration, Functions, and Information (Open System)

This section describes how the functions you can use and the information you can acquire (view) in an open system relate to the system configuration.

1.3.1 System Configuration with One Management Server

If you use a system configuration that uses a single management server, the Device Manager server running on that management server manages the volumes of all storage subsystems.

The following configuration examples are discussed below: a standard configuration, and three non-standard configurations (A, B, and C shown below).

- Configuration A: A configuration in which no Device Manager agent exists on the host.
- Configuration B: A configuration in which no Device Manager agent exists on the host and no Replication Monitor agent exists on the pair management servers.
- Configuration C: A configuration in which neither the Replication Monitor agent nor the Device Manager agent exist.

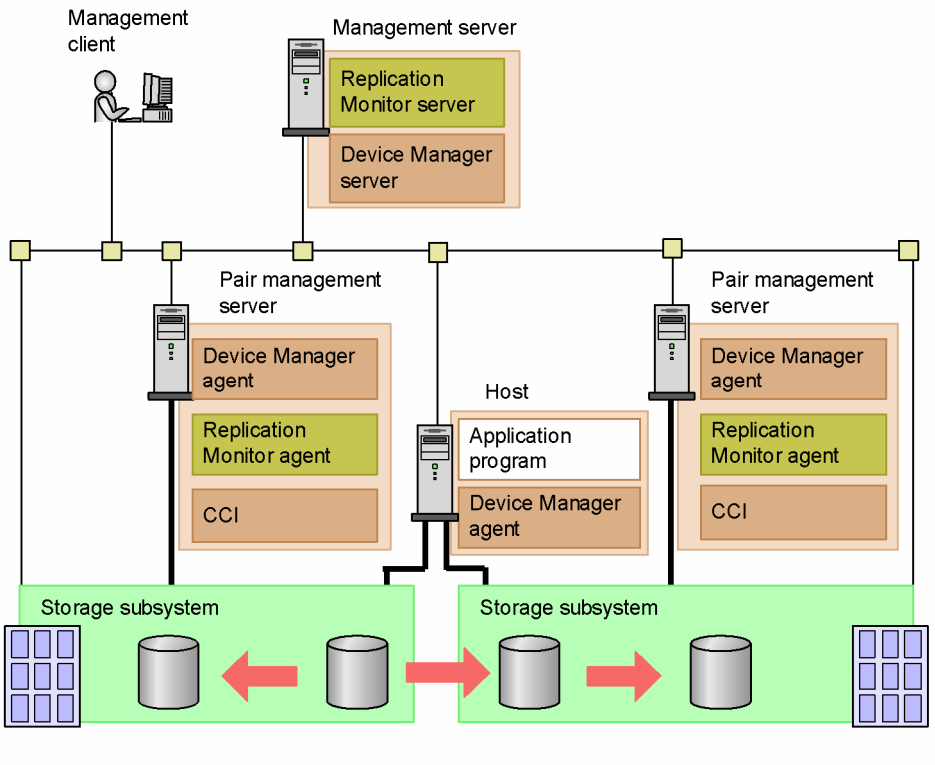

Figure 1.6 Standard Configuration (with Two Pair Management Servers)

In this standard configuration, you can use all Replication Monitor functions. Therefore, you can acquire (view) all information.

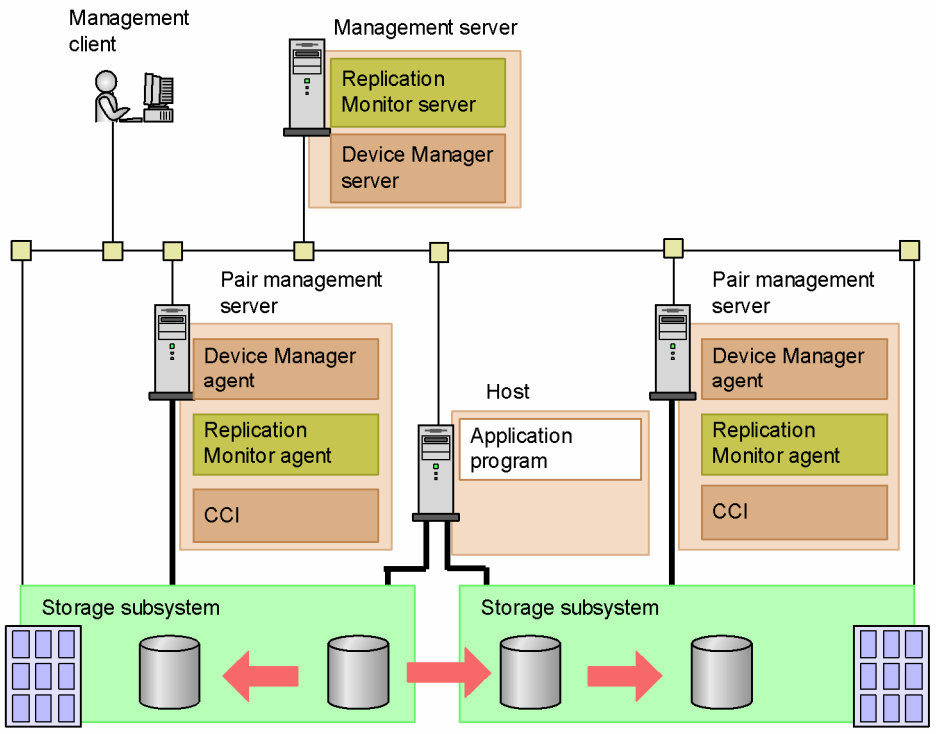

Figure 1.7 Configuration A (Without a Device Manager Agent on the Host)

Configuration A differs from the standard configuration as follows:

- The host information (the IP address and mount point) cannot be acquired (viewed) because a Device Manager agent does not exist on the host.

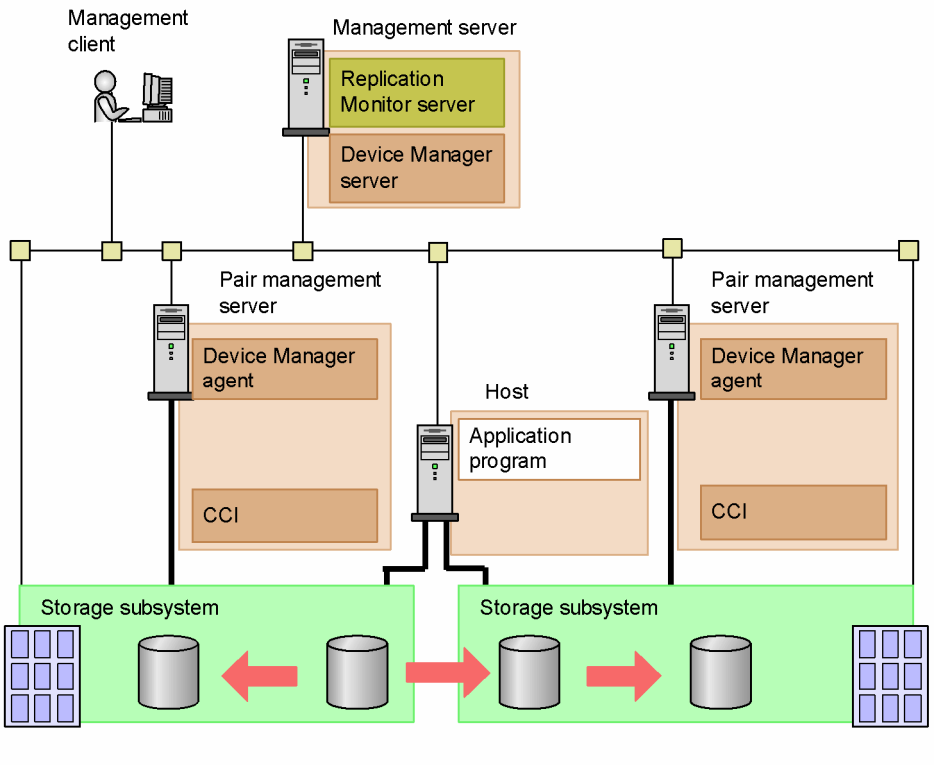

Figure 1.8 Configuration B (Without a Device Manager Agent on the Host and Without a Replication Monitor Agent on the Pair Management Servers)

Configuration B differs from the standard configuration as follows:

- The host information (the IP address and mount point) cannot be acquired (viewed) because a Device Manager agent does not exist on the host.
- The functions for setting a refresh interval on the pair management server, refreshing pair statuses through a Replication Monitor agent, and monitoring performance cannot be used because a Replication Monitor agent does not exist on the pair management servers. In addition, information about Remote Copy transmission delays and detailed information about the copy pair status on the secondary volume cannot be acquired (viewed).

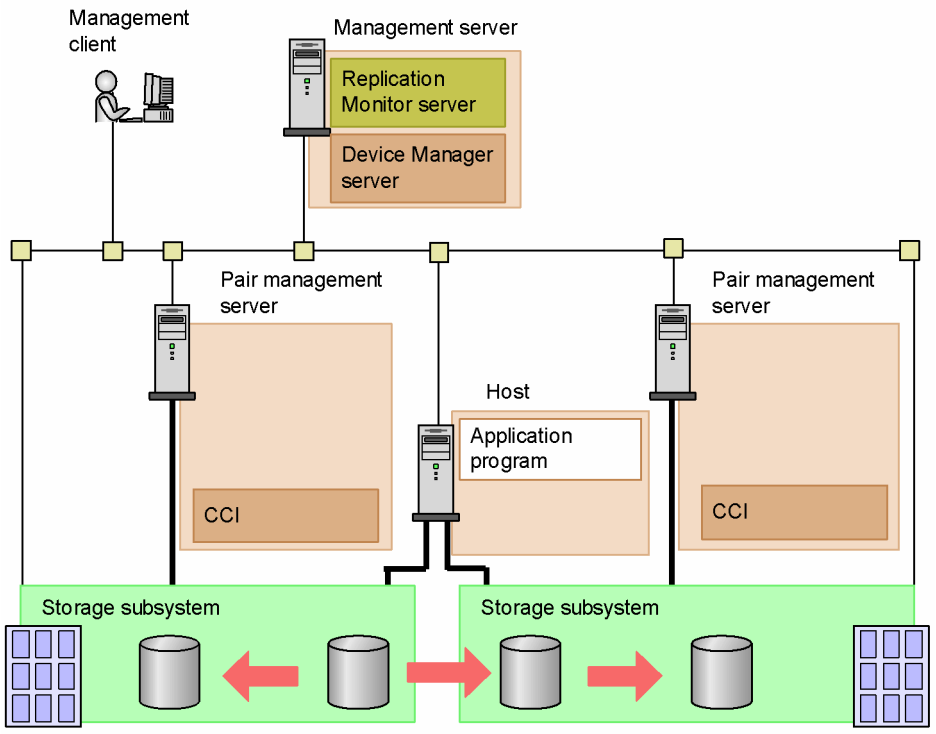

Figure 1.9 Configuration C (Without Replication Monitor Agents and Device Manager Agents)

Configuration C differs from the standard configuration as follows:

- The host information (the IP address and mount point) cannot be acquired (viewed) because a Device Manager agent does not exist on the host.
- The functions for setting a refresh interval on the pair management server, refreshing pair statuses through a Replication Monitor agent, and monitoring performance cannot be used because a Replication Monitor agent does not exist on the pair management servers. In addition, information about Remote Copy transmission delays and detailed information about the copy pair status on the secondary volume cannot be acquired (viewed).
- The functions for displaying the tree of the pair configuration definition view, displaying My Copy Groups, and changing the copy pair status cannot be used because a Device Manager agent does not exist on the pair management servers. In addition, information about names of the pair management servers, copy groups, and copy pairs cannot be acquired (viewed).

The following table describes the relationship among the system configuration, the functions you can use, and the information you can acquire (view)

Table 1.6 Relationship Among a System Configuration, Available Functions, and the Information That Can Be Acquired

		Standard Configuration	Configuration A	Configuration B	Configuration C
Functions	Displaying the tree of the Hosts view	Y	Y	Y	Y
	Displaying the tree of the Subsystems view	Y	Y	Y	Y
	Displaying the tree of the pair configuration definition view	Y	Y	Y	--
	Setting a refresh interval on a pair management server	Y	Y	--	--
	Refreshing pair statuses through a Replication Monitor agent	Y	Y	--	--
	Monitoring pair status	Y	Y	Y	Y
	Monitoring performance	Y	Y	--	--
	Displaying My Copy Groups	Y	Y	Y	--
	Changing copy pair status	Y	Y	Y	--
Restrictions on information that can be acquired or viewed		All information can be acquired and viewed	`n/a` is displayed for: ▪ Host's IP address and mount point	`n/a` is displayed for: ▪ Host's IP address and mount point ▪ Remote Copy transmission delays# `unknown` is displayed for: ▪ Detailed information about the copy pair status on the secondary volume	`n/a` is displayed for: ▪ Host's IP address and mount point ▪ Remote Copy transmission delays# ▪ Names of the pair management servers, copy groups, and copy pairs `unknown` is displayed for: ▪ Detailed information about the copy pair status on the secondary volume

Legend:

Y: The function can be used.

--: The function cannot be used.

#

When displaying Remote Copy transmission delays, you can view the write delay time data (C/T delta), side file usage, and journal volume usage.

1.3.2 System Configuration with Multiple Management Servers

If you use a system configuration that uses multiple management servers, the Device Manager server running on each management server manages the volumes in the management-target storage subsystem as shown below. The Device Manager servers running on the management servers are registered as information sources on the one management server on which the Replication Monitor server is installed.

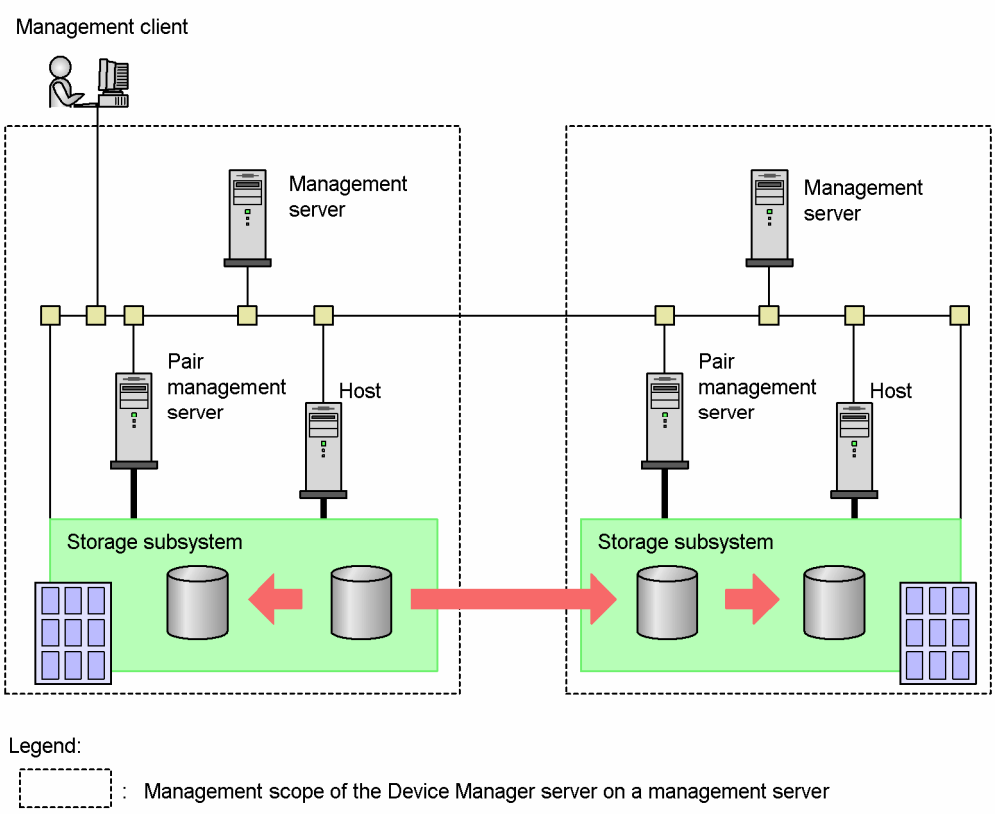

Figure 1.10 System Configuration With Multiple Management Servers

If you use a system configuration that uses multiple management servers, the relationship among the system configuration, the functions you can use, and the information you can acquire differs depending on how the primary and secondary volumes of a copy pair are managed, as follows:

- When the primary and secondary volumes of a copy pair are managed by the same Device Manager server (a copy pair whose primary and secondary volumes exist in one storage subsystem)

- When the primary and secondary volumes of a copy pair are managed by separate Device Manager servers (a copy pair whose primary and secondary volumes exist in different storage subsystems)

When the primary and secondary volumes of a copy pair are in the same storage subsystem, the relationship among the system configuration, the functions you can use, and the information you can acquire is the same as that shown in

Table 1.6.

When the primary and secondary volumes of the copy pair are in different storage subsystems and managed by separate Device Manager servers, even if a standard system configuration is used, the functions you can use and the information you can acquire differ depending on the type of the storage subsystem.

The following table describes the relationship among the type of storage subsystem, the functions you can use, and the information you can acquire when you use a standard system configuration and the primary and secondary volumes of a copy pair are managed by separate Device Manager servers:

Table 1.7 Relationship Among the Type of Storage Subsystem, Available Functions, and the Information That Can Be Acquired

		Lightning 9900, Thunder 9200	Thunder 9500V	Others
Functions	Displaying copy pair-related information of a copy pair in the host, subsystem, or pair configuration definition view	--	Y	Y
	Setting the refresh interval on the pair management server that manages the copy pair	--	Y	Y
	Refreshing pair status through a Replication Monitor agent	--	Y	Y
	Monitoring pair status	--	Y	Y
	Monitoring performance	--	Y	Y
	Displaying My Copy Groups	--	Y	Y
	Changing copy pair status	--	--	--
Restrictions on information that can be acquired or viewed		No information can be acquired or viewed	`n/a` is displayed for: ▪ LDEV number on the secondary volume ▪ Subsystem name on the secondary volume `unknown` is displayed for: ▪ Detailed information about the copy pair status on the secondary volume	All information can be acquired and viewed

Legend:

Y: The function can be used.

--: The function cannot be used.

If you use a non-standard system configuration, the restrictions shown in

Table 1.6 also apply.

1.4 Replication Monitor-Related Programs

The following sections overview the functions of and provide usage notes on Replication Monitor-related programs.

1.4.1 HiCommand Suite Common Component

HiCommand Suite Common Component is a package that bundles a number of functions used in common by HiCommand products. It is installed as part of Replication Monitor. HiCommand Suite Common Component is also provided with other HiCommand products that use these common functions.

Replication Monitor users can use the following functions from HiCommand Suite Common Component.

- Single sign-on (by Link-and-Launch)

  When a user logs in to Replication Monitor and then executes Link-and-Launch, that user's authentication information is then passed to any other HiCommand product for which that user has login permissions. This means that a user does not need to re-enter the user ID and password for those other products.

- Integrated logs and databases

  All of the various information that HiCommand products generate is output once to an integrated log.

  Management information maintained by HiCommand products is also collected and managed in a single location as an integrated database. Batch execution commands for backing up and restoring management information are also provided.

- HBase Storage Mgmt Web Service

  This is the server that executes the Web services (Web Client, etc.) provided by HiCommand products. Web Client for Replication Monitor is also provided by HBase Storage Mgmt Web Service.

1.4.2 Device Manager

Device Manager is software designed to enable centralized operation and management of systems made up of multiple or heterogeneous storage subsystems. The Replication Monitor server collects the copy pair configuration and other information it needs by obtaining the information that has been collected by the Device Manager server and maintained in that server's database

The Device Manager server is a prerequisite program for the Replication Monitor server.

For details, see the Device Manager documentation.

1.4.3 CCI

CCI is software designed for controlling storage subsystems from open system hosts. By using CCI to issue commands from a host to a storage subsystem, you can control the storage subsystem's volume replication functionality (TrueCopy, ShadowImage, etc.). CCI also allows you to collect information about copy pair configuration and status. For details on CCI, see the CCI documentation.

Replication Monitor server collects information about the copy pair configuration and status, and changes the pair status, in conjunction with an agent (a Replication Monitor agent or Device Manager agent) and CCI.

1.4.4 Business Continuity Manager

Business Continuity Manager is software designed for controlling storage subsystems from mainframe system hosts. By using Business Continuity Manager to issue commands from a host to a storage subsystem, you can collect information about the copy pair configuration and status. For details, see the Business Continuity Manager documentation.

Replication Monitor server collects information about the copy pair configuration and status, in conjunction with Business Continuity Manager.

1.4.5 Software Provided with Storage Subsystems

1.4.5.1 Software That Provides Volume Replication Functionality

Hitachi disk array subsystems provide ShadowImage, QuickShadow, Copy-on-Write Snapshot, TrueCopy, and Universal Replicator as volume replication functionality. Replication Monitor can collect the copy pair information defined by the volume replication functionality, and display pair status separately for each type of software.

ShadowImage, QuickShadow, and Copy-on-Write Snapshot

ShadowImage, QuickShadow, and Copy-on-Write Snapshot duplicate volumes in the same storage subsystem. For details, see the ShadowImage, QuickShadow, and Copy-on-Write Snapshot documentation.

In the Web Client for Replication Monitor window, ShadowImage might be displayed as SI, and QuickShadow and Copy-on-Write Snapshot might be displayed as QuickShadow/Copy-on-Write Snapshot or QS/COW.

TrueCopy

TrueCopy duplicates volumes between storage subsystems. For details, see the TrueCopy documentation.

TrueCopy includes TrueCopy Sync (synchronous mode) and TrueCopy Async/TrueCopy Extended Distance (asynchronous mode). In the Web Client for Replication Monitor window, TrueCopy Sync might be displayed as TCS, TrueCopy Async might be displayed as TCA, and TrueCopy Extended Distance might be displayed as TCE.

Universal Replicator

Universal Replicator asynchronously duplicates volumes between storage subsystems. For details, see the Universal Replicator documentation.

In the Web Client for Replication Monitor window, Universal Replicator might be displayed as UR.

1.4.5.2 Software for Managing Storage Subsystem Operations

This software is used to manage operation of a wide range of storage subsystems (for example, Storage Navigator for Universal Storage Platform V, TagmaStore USP and Lightning 9900V, and DAMP for Thunder 9500V). By using storage subsystem operation management software, you can gain fine control over capabilities unique to each storage subsystem.

1.4.5.3 About Using Software Provided with the Storage Subsystem (Open Systems Only)

We recommend that you keep the following points in mind if you use software that is provided with the storage subsystem.

- If you use storage subsystem operation management software to create copy pairs, the copy pair information that Replication Monitor can collect is limited. If you are using Replication Monitor, we recommend that you work through Device Manager to create copy pairs.
- If you work directly in Device Manager, CCI, or storage subsystem operation management software (Storage Navigator, DAMP, etc.) to perform any of the operations listed below, always perform a Device Manager refresh operation to update the Device Manager server database with the most recent information.
  - Changing the configuration of a storage subsystem (by adding a new disk drive, for example)
  - Creating a copy pair or changing the status of a copy pair

  Note:

  If you do not update the Device Manager information, the most recent configuration information is not reflected in Replication Monitor.

1.5 Setting the Environment for Deploying Replication Monitor

This section describes how to deploy Replication Monitor when you need to begin by building a new environment for managing your storage subsystems and hosts by using Device Manager.

The following provides the general procedure for building an environment in an open system. For details, see the other chapters in this manual and the related manuals described in this section.

The following figure shows the workflow for setting up the environment.

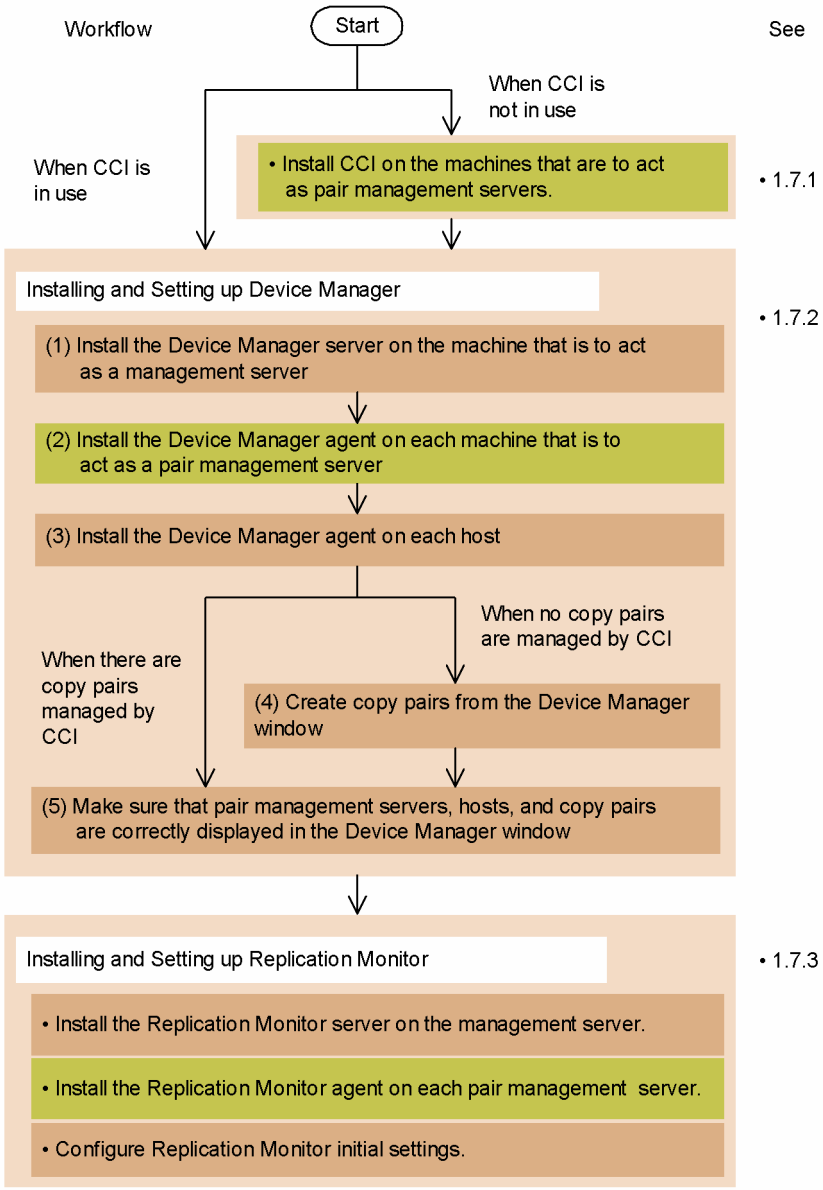

Figure 1.11 Workflow for Setting Up the Environment

1.5.1 Installing CCI

If you are not using CCI, you need to prepare an environment in which CCI can be used.

- Install CCI on the machines that are to act as pair management servers.

For details about the installation of CCI, see the CCI documentation.

1.5.2 Installing and Setting up Device Manager

1.5.2.1 Installing Device Manager Server on the management server

First, connect the machine that is to act as the management server and the storage subsystem SVP via a LAN.

1. Install the Device Manager server on the machine that is to act as a management server.

   For details about how to install, see the *HiCommand Device Manager Server Installation and Configuration Guide*.

2. Using the System account, log in to the Device Manager server, and then register a user account for performing all subsequent tasks.

   To allow all Device Manager operations to be performed with this account, grant **Admin** permission to the user, and assign **All Resources** as the user's resource group.

   Use this new user account in the following steps.

   For details about how to perform this step, step 3, and step 4, see the *HiCommand Device Manager Web Client User's Guide*.

3. Register the storage subsystems connected on the LAN with the Device Manager server.

   This operation allows all the volumes in the storage subsystems to be managed under **All Resources**.

4. Register all the hosts (host names and WWNs) connected to the storage subsystems with the Device Manager server.

   Perform this step using Web Client or the command line interface. Alternatively, you can use the LUN scanning function once you have installed the Device Manager agent on the pair management servers.

1.5.2.2 Installing Device Manager agent on each machine acting as a pair management server

Set up the machines on which CCI is installed as pair management servers. Before you proceed, the pair management servers must be connected to the LAN on which the Device Manager server is connected.

Perform the following steps on each machine that you are setting up as a pair management server.

For details about how to install the Device Manager agent, see the *HiCommand Device Manager Agent Installation Guide*.

If you want to centrally manage copy pairs, enable the central management method on each pair management server. For details about how to enable the central management method, see the *HiCommand Device Manager Server Installation and Configuration Guide*.

1. Install the Device Manager agent on each machine that will act as a pair management server.
2. Register the IP address and other information about the Device Manager server with each Device Manager agent.
3. If a pair management server is running a Windows OS, restart the Device Manager agent.

1.5.2.3 Installing the Device Manager agent on each host

Install the Device Manager agent on the hosts on which application programs are installed. This step is the same as steps 1 to 3 in procedure (2) above.

1.5.2.4 Creating copy pairs from the Device Manager window

If there are no copy pairs managed by CCI, use the Device Manager function for managing copy pairs to create copy pairs.

For details on how to create copy pairs, see the *HiCommand Device Manager Web Client User's Guide*.

1.5.2.5 Ensuring correct display in the Device Manager window

For detail about how to make sure that pair management servers, hosts, and copy pairs are displayed, see the *HiCommand Device Manager Web Client User's Guide*.

1. Make sure that the pair management servers and hosts can be correctly displayed in the Device Manager window.

   Before you check, refresh the host information as required by using the LUN scanning function.
2. In the Device Manager subwindow that is displayed by clicking a pair management server name or a host name, make sure that the managed copy pairs can be displayed correctly.

   Before you check, refresh the storage information as required.

1.5.3 Installing and Setting up Replication Monitor

After you make sure that pair management servers, hosts, and copy pairs are correctly displayed in the Device Manager window, perform the Replication Monitor installation and configure initial settings as follows:

- Install the Replication Monitor server on the management server.
- Install the Replication Monitor agent on each pair management server.

- Configure Replication Monitor initial settings.

For details about these procedures, see Chapter 2 and Chapter 3.

Chapter 2 Installing Replication Monitor

This chapter explains how to install and uninstall Replication Monitor.

There are two installation modes: a *new installation*, and an *overwrite installation*. A new installation is performed if Replication Monitor has not yet been installed, whereas an overwrite installation is performed at an upgrade or re-installation. The installer automatically determines whether to perform a new installation or an overwrite installation.

- About the Installation Task Flow (see section 2.1)
- Preparing for an Installation (see section 2.2)
- Installing a Replication Monitor Server on a Management Server (Windows) (see section 2.3)
- Installing a Replication Monitor Server on a Management Server (Solaris) (see section 2.4)
- Installing an Agent on a Pair Management Server (see section 2.5)
- Importing the Alert Settings for the Earlier Version (see section 2.6)
- After Finishing the Installation (see section 2.7)

2.1 About the Installation Task Flow

Figure 2.1 shows the task flow for installing Replication Monitor in a system.

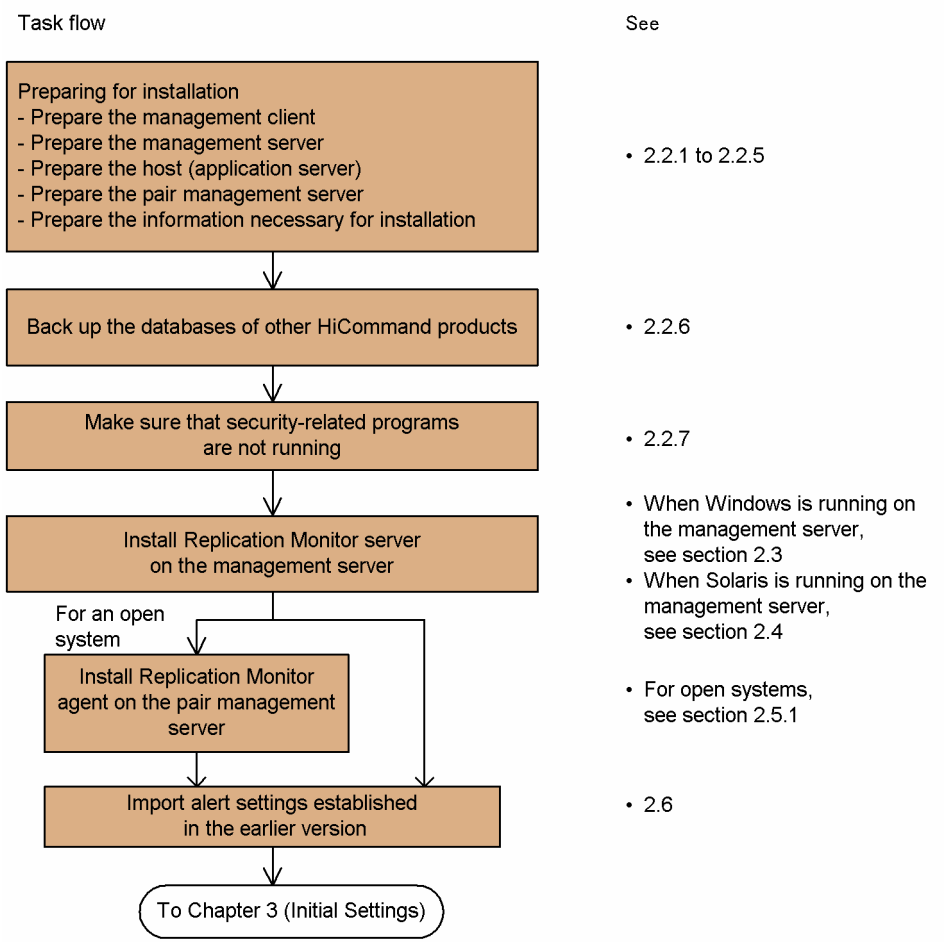

Figure 2.1 Task flow for Installing Replication Monitor

Note:

Installing Replication Monitor in a cluster environment involves different system requirements and installation procedures. To set up a cluster environment, read 6.11 first and then refer to the installation procedure in this chapter as needed.

2.2 Preparing for an Installation

This section explains items you must check and information you must prepare before installing Replication Monitor.

2.2.1 Preparing the Management Client

The management client must first be prepared as described below.

2.2.1.1 Prerequisite Conditions

Table 2.1 shows the prerequisite conditions for the management client. Please make sure that the management client satisfies these conditions.

Table 2.1 Prerequisite Conditions for the Management Client

OS		Prerequisite programs for the management client
Windows	▪ Windows 2000 SP3 ▪ Windows 2000 SP4 ▪ Windows Server 2003# ▪ Windows Server 2003 SP1# ▪ Windows Server 2003 SP2# ▪ Windows Server 2003 R2 ▪ Windows Server 2003 R2 SP2 ▪ Windows XP SP1 ▪ Windows XP SP2 ▪ Windows Vista	Internet Explorer 6.0, Internet Explorer 6.0 SP1, or Internet Explorer 7.0
Solaris	▪ Solaris 8 (for SPARC) ▪ Solaris 9 (for SPARC) ▪ Solaris 10 (for SPARC)	Mozilla 1.4 (for Solaris 8 or Solaris 9) or Mozilla 1.7 (for Solaris 10)
HP-UX	▪ HP-UX 11i v1 (PA-RISC) ▪ HP-UX 11i v2 ▪ HP-UX 11i v3	Mozilla 1.7.8.00, Mozilla 1.7.12.01, or Mozilla 1.7.13.01

Only the x86 architecture is supported.

2.2.2 Preparing the Management Server

The management server must first be prepared as described below.

2.2.2.1 Prerequisite Conditions

Table 2.2 shows the prerequisite conditions for the management server. Please make sure that the management server satisfies these conditions.

Table 2.2 Prerequisite Conditions for the Management Server

OS#1		Prerequisite programs for the management server
Windows	▪ Windows 2000 SP3 ▪ Windows 2000 SP4 ▪ Windows Server 2003#3#4 ▪ Windows Server 2003 SP1#3#4 ▪ Windows Server 2003 SP2#3#4 ▪ Windows Server 2003 R2#4 ▪ Windows Server 2003 R2 SP2#4 ▪ Windows Server 2003 R2 x64 Edition#5 ▪ Windows Server 2003 R2 x64 Edition SP2#5 ▪ Windows Server 2003 x64 Edition#5 ▪ Windows Server 2003 x64 Edition SP2#5 ▪ Windows XP SP2	Device Manager server of Device Manager 5.0 or a later version#2
Solaris	▪ Solaris 8 (for SPARC) ▪ Solaris 9 (for SPARC) ▪ Solaris 10 (for SPARC)	

#1 If the management server runs in a cluster environment, there are restrictions on usable OSs. For details about the OS requirements in a cluster environment, see section 7.1.

#2 Make sure that a Device Manager server of Device Manager 5.0 or a later version is installed and set up in a state where communications between the management server, management client, and storage subsystem can be established. For details about the Device Manager server installation and setup, see the *HiCommand Device Manager Server Installation and Configuration Guide*.

Even when Replication Monitor is to be used only for managing mainframe-based volume replication, you must install and set up the Device Manager server in the same management server where Replication Monitor is installed.

#3 Only the x86 architecture is supported.

#4 Also runs under VMware ESX Server 3.0.1.

#5 Runs in the 32-bit emulation mode.

2.2.2.2 Items To Be Checked

You must first check the following items for the management server:

- Ensure that the following types of hardware are available:

- A CD-ROM drive
- A 10/100 Ethernet LAN card

- Ensure that the following network settings are in place:
  - The TCP/IP protocol is running.
  - Static IP addresses have been set up.
- If volumes are in copy pair structures configured with the volume replication functions of the storage subsystem (such as ShadowImage, TrueCopy, QuickShadow, Copy-on-Write Snapshot, or Universal Replicator), copy pairs must be the management targets of Device Manager or Business Continuity Manager. For details about requirements for managing copy pairs with Device Manager, see the *HiCommand Device Manager Server Installation and Configuration Guide*. For details about requirements for managing copy pairs with Business Continuity Manager, see the *Hitachi Business Continuity Manager User's Guide*.
- In Windows, a resolution of SVGA (800 x 600) or greater is required.

2.2.3 Preparing the Hosts

Hosts (application servers) must first be prepared as described below.

2.2.3.1 Prerequisite Conditions for an Open System Host

Table 2.3 shows the prerequisite conditions for an open system host. Ensure that the host satisfies these conditions.

Table 2.3 Prerequisite Conditions for an Open System Host

OS		Prerequisite program for an open system host
Windows	▪ Windows 2000 SP4 ▪ Windows Server 2003 ▪ Windows Server 2003 SP1 ▪ Windows Server 2003 SP2 ▪ Windows Server 2003 R2 ▪ Windows Server 2003 R2 SP2 ▪ Windows Server 2003 x64 Edition #2 ▪ Windows Server 2003 x64 Edition SP2#2 ▪ Windows Server 2003 R2 x64 Edition#2 ▪ Windows Server 2003 R2 x64 Edition SP2#2	Device Manager agent#1
Solaris	▪ Solaris 8 (for SPARC) ▪ Solaris 9 (for SPARC) ▪ Solaris 10 (for SPARC)	
AIX	▪ AIX 5L(5.3)	
HP-UX	▪ HP-UX 11.00 ▪ HP-UX 11i v1 (PA-RISC 64/32bit)	

OS		Prerequisite program for an open system host
	▪ HP-UX 11i v2 (IPF/PA-RISC) ▪ HP-UX 11i v3 (IPF/PA-RISC)	
Linux	▪ Red Hat Enterprise Linux AS 4.0 Update3#3 ▪ Red Hat Enterprise Linux ES 4.0 Update3#3	

#1

- To use the Replication Monitor agent or use Replication Monitor to check host-related information, the Device Manager agent must be installed. For details about the Device Manager agent installation, see the *HiCommand Device Manager Agent Installation Guide*.
- To link the Device Manager agent with Replication Monitor, all of the following conditions must be satisfied:

  - The Device Manager agent must be of Device Manager 03-50 or later.

  However, if you want to use the Replication Monitor agent, the Device Manager agent of Device Manager 5.0, 5.1, 5.5, 5.6 or 5.7 must be installed.

  - The Device Manager agent version is one that can be used under the Device Manager server, which is a prerequisite of Replication Monitor.

  However, if the Device Manager agent version is earlier than the Device Manager server version, some of the Replication Monitor functions cannot be used. For details, see the *HiCommand Device Manager Server Installation and Configuration Guide*.

#2 Runs in the 32-bit emulation mode.

#3 Only the x86 and IPF architectures are supported.

2.2.3.2 Items to Be Checked for an Open System Host

In Replication Monitor, the Replication Monitor server on the primary site communicates with agents at other sites. If the use of private addresses or address conversion, such as NAT (Network Address Translation), is specified, the server might not be correctly connected to the agent.

To use Replication Monitor when address conversion occurs between sites in such a network environment, use the following method so that the IP address of the host on which the agent is installed can be determined from the host name:

- Define the host name and IP address of the host on which the agent is installed in the `hosts` file of the management server.

2.2.3.3 Prerequisite Conditions for a Mainframe Host

Table 2.4 shows the prerequisite conditions for a mainframe host. Ensure that the host satisfies these conditions.

Table 2.4 Prerequisite Conditions for a Mainframe Host

OS	Prerequisite program for a mainframe host#
Same as Business Continuity Manager	Business Continuity Manager - 5.0, 5.1, or 5.2

Notes:

For details about Business Continuity Manager installation and setup, see the *Hitachi Business Continuity Manager Installation Guide*.

#

Use Business Continuity Manager 5.1 or later to collect mainframe information when:

– Two or more `PREFIX` parameters are set in the Business Continuity Manager initial settings.

2.2.4 Preparing the Pair Management Server (for an Open System)

The pair management server must first be prepared as described below.

2.2.4.1 Prerequisite Conditions

The prerequisite conditions for the pair management server are the same as those for an open system host, except for those listed below. For the prerequisite conditions for an open system host, see section 2.2.3.1.

The prerequisite conditions unique to the pair management server are explained below.

- The Device Manager agent must be installed as a prerequisite program.#

  # The installation of the Device Manager agent is optional for a host, but it is required for the pair management server.

- CCI must be installed as a prerequisite program.
- When you install the Replication Monitor agent on the pair management server, make sure that the OS of the pair management server is supported because the OSs that the Device Manager agent and the Replication Monitor agent support are different.

2.2.4.2 Items to Be Checked

You must first check the following items for the pair management server:

- In the configuration definition information of the pair being used by CCI on the pair management server, ensure that the copy group of the configuration definition file matches the consistency group (the group defined to maintain consistency in the updating sequence of asynchronous copying operations among multiple volumes) of the actual storage subsystem. If these two groups do not match each other, correct operation of Replication Monitor cannot be guaranteed.
- When address conversion occurs between sites

In Replication Monitor, the Replication Monitor server on the primary site communicates with agents at other sites. If the use of private addresses or address conversion, such as NAT, is specified, the server might not be correctly connected to the agent.

To use Replication Monitor in such a network environment, use the following method so that the IP address of the pair management server on which the agent is installed can be determined from the host name:

- Define, in the `hosts` file of the management server, the host name and IP address of the pair management server on which the agent is installed.

2.2.5 Preparing Information Required for Installation

When installing the Replication Monitor server, you must enter the types of information listed below. Ensure that these types of information have been correctly entered.

Required information	OS running the management server				Remarks
	Windows		Solaris		
	NI	UR	NI	UR	
Installation folder for Replication Monitor	S	--	--	--	This information is required when the installation folder is not the default folder.
The storage destination for the database files used by Replication Monitor	S	--	S#	--	This information is required when the storage location is not the default, e.g., a cluster environment.
The Device Manager user account (user ID and password)	R	S	R	S	A user account is required that has the Modify permission in Device Manager and in which `All Resources` is allocated to its resource group. This information is required only when a user account different from the existing one is to be set up during upgrade installation or re-installation.
The port number that Device Manager uses for HTTP communications	S	--	S	--	This information is required when Device Manager is not using the default port number. This port number is specified for `server.http.port` in the `server.properties` file of the Device Manager server.
Administrators group user ID of the OS	R		--		--
Root permission account of the OS	--		R		--

Legend:

NI: New installation

UR: Upgrade installation or re-installation

R: Required information

S: Information required depending on the situation

--: Not applicable

You cannot use a path that includes a symbolic link as the directory name for the storage destination.

2.2.6 Backing up Databases of Other HiCommand Products

When using another HiCommand product, back up the database of the HiCommand product being used before installing Replication Monitor. For details about how to back up the databases of other HiCommand products, see the corresponding product manuals.

2.2.7 Checking Security-Related Programs

Check whether any of the following programs are installed. If any such program is installed, take the action indicated below:

- Security-monitoring program

  Stop the program or change the program settings so as not to impede Replication Monitor installation.

- Virus-detection program

  We recommend that you stop anti-virus programs before you install Replication Monitor.

  If an anti-virus program is active while Replication Monitor is being installed, the installation might be slow or fail, or Replication Monitor might be installed incorrectly.

- Process-monitoring program

  Stop the program or change the program settings so that the services and processes of the Device Manager server (a Replication Monitor prerequisite program) and of the HiCommand Suite Common Component will not be monitored.

  Installation might fail if any of these services or processes is stopped or started by the process-monitoring program during Replication Monitor installation.

2.2.8 Adjusting the Time of a Machine on Which Replication Monitor Is Installed

If the time of a machine is changed while the services of HiCommand Suite Common Component and HiCommand products are running, Replication Monitor might not operate correctly. If you need to change this time, do so before installation.

If you want to use functionality that automatically adjusts the time by using a protocol such as NTP, use a function that can gradually adjust the time of a machine without immediately synchronizing the time when the time of the machine is ahead of the actual time. There are some functions that gradually adjust the time if the difference between the time of a machine and the actual time is within a certain fixed period, or immediately synchronize the time if the time difference exceeds a certain fixed period. Therefore, set the frequency of the time adjustments for the function that you are using so that the time difference does not exceed the fixed period.

For example, the Windows Time service can gradually adjust the time of a machine without immediately synchronizing the time if the time is ahead of the actual time by a certain fixed period. Therefore, check the range in which the Windows Time service can gradually adjust the time, and then set the frequency of the time adjustments for the Windows Time service so that the difference between the time of the machine and the actual time does not exceed that range.

Changing the time after installing Replication Monitor

If you cannot use functionality that adjusts the time automatically, or if you need to change the time immediately, perform the following procedure to change the time of a machine:

1. Stop the services of HiCommand Suite Common Component and all HiCommand products.

   For details about how to stop services, see section 6.3.

2. Change the time of the machine.

3. Restart the machine.

   When the machine is restarted, the services of HiCommand Suite Common Component and all HiCommand products will automatically be started.

2.3 Installing a Replication Monitor Server on a Management Server (Windows)

This section explains how to install and uninstall the Replication Monitor server in the Windows OS.

Note:

Installing Replication Monitor in a cluster environment involves a different procedure. To set up a cluster environment, read section 7.2 first and then refer to the installation procedure in section 2.3 as needed.

2.3.1 Performing a New Installation

This section explains how to perform a new installation of the Replication Monitor server in Windows.

Check the following before performing a new installation:

- To install the Replication Monitor server, the following free disk space is required to store the program and database.

  - 150 MB or more for the Replication Monitor server program

  - 200 MB or more for the Replication Monitor server database

- 300 MB or more of free disk space is temporarily required in the drive in which Windows is installed to install the Replication Monitor server.

- Make sure that the embedded database HiRDB service `HiRDB/EmbeddedEdition _HD0` is active.

  You can check whether the HiRDB service is running by opening the Windows Services window. If the HiRDB service is active, its status appears as **Started**.

- Ensure that all of the preparations described in 2.2.2 and 2.2.5 are completed.

Note: Close the Windows Services window before you install the Replication Monitor server.

Note: Do not forcibly stop installation of the Replication Monitor server by any method other than clicking the **Cancel** button (for example, do not stop installation by restarting the machine). If you have used some other method to forcibly stop installation, see section 9.1.

To perform a new installation of the Replication Monitor server:

1. Log on to Windows using a user ID that belongs to the Administrators group.

   If you have logged on to Windows using a user ID that does not belong to the Administrators group, a window appears during installation informing you that the execution must be performed by a user that belongs to the Administrators group, and the installation process terminates.

2. Insert the Replication Monitor CD-ROM. Select **Start**, **Run**, and then **Browse**. Select the CD-ROM drive and execute `setup.exe` from the files in the root folder.

A window appears informing you of the start of the installation. This window displays a message that informs you that HiCommand products will be started and stopped during the installation and messages that prompt you to take the following actions:

- Back up the databases of all HiCommand products before you begin the installation.
- In a cluster configuration, manually stop the HiCommand Suite Common Component services (HBase Storage Mgmt Web Service and HBase Storage Mgmt Common Service) and all HiCommand product services.

Note:

When you attempt to install the Replication Monitor server in a machine with no prerequisite version of the Device Manager server installed, a message appears informing you that the prerequisite version of Device Manager has not been installed, and the installation stops.

When canceling the installation in the following procedures, click the **Cancel** button, and click the **Yes** button in the cancellation confirmation dialog. In the Installation Stopped window that appears, click the then click the **Finish** button to terminate the installer.

3. In the window informing you of the start of the installation, click the **Next** button.

   If any HiCommand Suite Common Component services are active:

   In a non-cluster configuration, a window appears reporting that the services will be stopped. Go to step 4.

   In a cluster configuration, an error message is displayed, and the window informing you of the start of the installation appears again.

   If all HiCommand Suite Common Component services are stopped:

   A window appears confirming the setup status of the embedded database HiRDB. Go to step 5.

   There are four setup statuses for HiRDB, as shown below. The installer identifies the status and guides you through the optimal installation for that status. When the setup status of HiRDB is not set, an error message appears and the installation stops.

   - *Not setup*: HiRDB is not set up.

   - *Non-cluster configuration*: HiRDB has been set up in a non-cluster configuration.

   - *Cluster configuration (executing node)*: HiRDB has been set up on the executing system in a cluster configuration.

   - *Cluster configuration (standby node)*: HiRDB has been set up on the standby system in a cluster configuration.

4. In the window reporting that the HiCommand product services will be stopped, click the **Next** button.

   Processing to stop the services is performed, and then a window for checking the setup status of the embedded database HiRDB appears.

5. To continue the installation according to the information shown in the window for checking the HiRDB setup status, click the **Next** button.

A window appears asking you to specify an installation folder for the Replication Monitor server.

6. When installing the Replication Monitor server in the default folder, click the **Next** button. When installing the Replication Monitor server in any other folder, select the folder, and then click the **Next** button.

   A window appears asking you to specify a location in which the database files for the Replication Monitor server are to be stored.

   Note:

   Clicking the **Browse** button displays a folder selection dialog box, which enables you to specify the folder. (This dialog box is also displayed when you specify the folder for storing the database files.)

   In a folder selection dialog box, if you manually specify a folder that does not exist, and then click the **OK** button, the specified folder is created. The created folder will be deleted if the installation is canceled or the Replication Monitor server is uninstalled. Among those created folders, the folders that are not specified as the installation folder for the Replication Monitor server can be manually deleted.

   If you change the case (for example, change an upper-case character to a lower-case character) when you manually enter an existing folder name in a folder selection dialog box, the displayed value will use the characters you entered, but the upper case and lower case characters in the folder name (used by the OS) will not change. For example, when the folder `C:\Program Files\HiCommand` exists in an environment, if in a folder selection dialog box you manually enter `C:\Program Files\hicommand`, and then click the **OK** button, the setting value viewed in the window displayed by clicking the **View** button is `C:\Program Files\hicommand`; however, the actual folder is `C:\Program Files\HiCommand`.

   Note:

   When installing the Replication Monitor server in a cluster configuration system, specify the same installation folder on both the executing and standby systems.

   Specify an installation folder using no more than 90 characters, including all characters, starting with the drive letter at the beginning, through to the last character. This maximum includes the characters that separate the folder names. The following characters can be used for specifying the folder:

   `A` to `Z` `a` to `z` `0` to `9` `#` `+` `-` `.` `@` `_` `(` `)` and single-byte spaces

   You can also use a colon (`:`) to delimit a drive latter and a backward slash (`\`) to separate folder names. However, single-byte spaces at the beginning and end of a path are ignored.

   If you specify a name that contains a two-byte character or a name reserved by the OS (such as `CON`, `AUX`, `NUL`, `PRN`, `CLOCK$`, `COM1` - `COM9`, or `LPT1` - `LPT9`), an error might occur.

   In the default, the Replication Monitor server is installed in the following folder:

OS	Default installation folder

OS	Default installation folder
▪ Windows 2000 ▪ Windows Server 2003 ▪ Windows Server 2003 R2 ▪ Windows XP	*system-drive*\Program Files\HiCommand\ReplicationMonitor
▪ Windows Server 2003 x64 Edition ▪ Windows Server 2003 R2 x64 Edition	*system-drive*\Program Files (x86)\HiCommand\ReplicationMonitor

If the user changes the installation destination, the Replication Monitor server is installed in the following folder:

user-specified-folder\ReplicationMonitor

When *Replication-Monitor-installation-folder* appears in the following descriptions, it refers to the above folder. For instance, if the Replication Monitor server is installed in the default folder in Windows 2000, *Replication-Monitor-installation-folder*\installation refers to the following.

system-drive\Program Files\HiCommand\ReplicationMonitor\inst

Installing the Replication Monitor server also installs a package called HiCommand Suite Common Component, which consists of functions shared among all the HiCommand products.

In the default, HiCommand Suite Common Component is installed in the following folder:

OS	Default installation folder
▪ Windows 2000 ▪ Windows Server 2003 ▪ Windows Server 2003 R2 ▪ Windows XP	*system-drive*\Program Files\HiCommand\Base
▪ Windows Server 2003 x64 Edition ▪ Windows Server 2003 R2 x64 Edition	*system-drive*\Program Files (x86)\HiCommand\Base

If the user changes the installation destination, HiCommand Suite Common Component is installed in the following folder:

user-specified-folder\Base

However, if another HiCommand product that bundles HiCommand Suite Common Component (for example, Device Manager) is installed in a non-default folder before the Replication Monitor server is installed, HiCommand Suite Common Component is installed in the following folder:

folder-specified-by-user-during-HiCommand-product-installation\Base

In this manual, the installation folder for HiCommand Suite Common Component indicates the above folder.

7. To store the database files for Replication Monitor in the displayed default folder, click the **Next** button. To store them in a different folder, enter that folder, and then click the **Next** button.

In a non-cluster configuration or cluster configuration (executing node):

A window appears prompting you to set the information required for Replication Monitor to access Device Manager. Go to step 8.

In a cluster configuration (standby node):

A confirmation window appears, indicating that preparation for the installation is complete. Go to step 10.

Note:

Once you specify the folder for storing database files and then click the **Next** button, changing the settings of the installation folder will not automatically change the settings for the database files folder. If you change the installation folder after specifying the default folder as the folder for storing the database files, manually change the folder for the database files, or cancel the installation and start installation again.

Note:

The following characters can be used for specifying the database file location:

`A` to `Z` `a` to `z` `0` to `9` `.` `_` `(` `)` and single-byte spaces

The following requirements also apply:

- The location must be 100 characters or less (this includes all characters from the drive letter to the last character).
- An absolute path must be specified.
- A name reserved by the OS (such as `CON`, `AUX`, `NUL`, `PRN`, `CLOCK$`, `COM1` - `COM9`, or `LPT1` - `LPT9`) cannot be used.
- The specified path must not end with the path delimiter.
- Single-byte spaces cannot be specified at the beginning or end of a path. (If single-byte spaces are specified in these locations, they will be ignored.)
- A location directly under the drive cannot be specified.

In a non-cluster configuration, depending on the length of the Replication Monitor server installation path name specified by the user, the default folder of the database file is as follows:

- When the installation path name is 72 bytes or less:

  installation-path`\ReplicationMonitor\database`

- When the installation path name exceeds 72 bytes:

  installation-path`\`

  If the following folder is used for the storage destination of the database file, the Replication Monitor server installation path name must be 72 bytes or less:

  installation-path`\ReplicationMonitor\database`

  If the installation path name contains the following characters, the default value cannot be set for the storage destination of the database file. Use specifiable characters to set a storage destination other than the default.

  `# + - @`

The location for the database file requires at least 200 MB of free space.

Note:

When installing the Replication Monitor server in a cluster configuration system, specify a shared disk in this step, and specify the same path on both the executing and standby systems. No default is displayed.

When you install the Replication Monitor server in the standby system, if there is no database file under the user-specified shared disk path (for example, if the specified shared disk path differs from the path specified when installing the Replication Monitor server in the executing system, or if the specified path is the same but is not a shared disk) an error message appears, prompting you to re-enter the information. For details about action to be taken in this case, see section 9.4.

8. Enter the Device Manager user account (user ID and password), and click the **Next** button. If you need to change the displayed port number (default value: `2001`) to another value, enter the user account and the new port number, and then click the **Next** button. The password must be entered twice (the second entry is compared with the first entry to confirm that they are identical).

   In a non-cluster configuration:

   A window appears, asking whether you want to start the HiCommand product services when the installation finishes. Go to step 9.

   In a cluster configuration (executing node):

   A confirmation window appears, indicating that preparation for the installation is complete. This window displays installation information such as the installation destination. Go to step 10.

   Note:

   When the user account and port number required for Replication Monitor to access Device Manager are not entered, or if the port number is outside the acceptable range, an error message appears prompting you to re-enter the information.

   The user account and port number set in this procedure are required for using Device Manager functions from Replication Monitor. The user account is used when Replication Monitor accesses Device Manager. To enable Replication Monitor to use Device Manager functions, a user account must be specified that has the Modify permission in Device Manager and in which `All Resources` is allocated to its resource group. Device Manager uses the port number for HTTP communications.

   When specifying a user ID or password, use from 1 to 256 characters. If you specify 257 characters or more, the operation might fail. Specifiable characters are as follows:

Item	Specifiable characters
User ID	`A-Z a-z 0-9 # + - . @ _`
Password	`A-Z a-z 0-9 ! # $ % & ' ( ) * + - . = @ \ ^ _ |`

   At this point, the user account specified in this procedure is not checked as to whether it is valid and effective as a Device Manager user account. This will be checked when installation has completed normally and Replication Monitor performs an automatic or manual refresh.

Enter the same password twice. If the first and second input values are not identical, an error message appears prompting you to re-enter the information.

The port number is specified for `server.http.port` of the `server.properties` file of the Device Manager server. Execute the port number change only when you need to change this port number to another value that is different from the displayed default value.

The number `2001` is the default value for the port number used by Device Manager in HTTP communications. If Device Manager has specified a port number other than the default, specify that port number.

The port number can be specified using a number from 1 to 65535.

9. In the window asking whether you want to start HiCommand product services, make sure that the **Yes** radio button is selected if you want to start the services. If you do not want to start the services, select the **No** radio button. Then click the **Next** button.

   A confirmation window appears, indicating that preparation for the installation is complete. This window displays installation information such as the installation destination.

10. Check the installation information displayed in this window, and then click the **Execution** button.

    Installation processing begins, and several windows appear indicating various statuses during processing.

    When the installation has completed normally, a window appears reporting that the installation is complete.

    In the following cases, a window appears reporting that the installation has stopped:

    - When the user instructs the installer to stop the installation by clicking the **Cancel** button.
    - When the installation is terminated because of an error that occurred during the installation.

11. In the window reporting that the installation is complete, click the **Finish** button to finish the installation.

    The window closes.

    When the installation has completed normally, the operating statuses of the HiCommand Suite Common Component services (HBase Storage Mgmt Web Service and HBase Storage Mgmt Common Service) are as follows:

    - When the setup status of HiRDB is *non-cluster configuration*

      If you selected **Yes** in the window asking whether you want to start the HiCommand product services when the installation finishes, the services start automatically and are enabled. The Device Manager service (`HiCommandServer`) also starts automatically.

      If you selected **No** in the window asking whether you want to start the HiCommand product services when the installation finishes, the services are disabled.

    - When the setup status of HiRDB is *cluster configuration*

The startup type of the services is set to **Manual** and the services are disabled.

For details about actions to be taken when installation fails, such as cases where the user cancels the installation via the **Cancel** button or when an error occurs during the installation, see section 9.1.

Before you start Replication Monitor, adjust the output size of the logs that record the operating status of Replication Monitor. Specify the log output size in the property file (`logger.properties`). For details on the `logger.properties` file, see section 6.10.2.

2.3.2 Upgrade Installation or Re-installation

This section explains how to perform an overwrite installation to upgrade or re-install the existing the Replication Monitor server in Windows.

Check the following before executing an overwrite installation:

- In an overwrite installation, you cannot revert to a version earlier than the current version. Check that the versions of the Replication Monitor server and Replication Monitor agent for the overwrite installation are the same as or later than the existing versions. If the versions before and after installation are the same, you can install the older iteration of Replication Monitor after installing the newer one.
- 300 MB or more of free disk space is temporarily required in the drive in which Windows is installed to install the Replication Monitor server.
- Make sure that the embedded database HiRDB service `HiRDB/EmbeddedEdition _HD0` is active.

  You can check whether the HiRDB service is running by opening the Windows Services window. If the HiRDB service is active, its status appears as **Started**.
- Ensure that all of the preparations described in 2.2.2 and 2.2.5 are completed.

Note:

Close the Windows Services window before you install the Replication Monitor server.

Note:

Do not forcibly stop installation of the Replication Monitor server by any method other than clicking the **Cancel** button (for example, do not stop installation by restarting the machine). If you have used some other method to forcibly stop installation, see section 9.1.

Note:

If you upgraded to this version from version 5.5.0-02 or earlier or from version 5.6, make sure that you delete or change the user authentication information so that the earlier information cannot be used.

When you perform an overwrite installation from version 4.0 or 4.2 to version 5.0 or later, user information will be inherited, but user management permissions will not be inherited automatically. If you want to inherit user management permissions, set the user permissions after the overwrite installation has completed. For details about how to set user permissions, see section 3.3.4.

For an overwrite installation, the parameter values in the existing property files can be used without change, except for those in the `serverstorageif.properties` file in the following situation:

When you upgrade Replication Monitor from a version earlier than 5.0 (The parameter values in the existing `serverstorageif.properties` file are not used).

We recommend that you back up the Replication Monitor operating environment information (property files and database) before executing an overwrite installation of the Replication Monitor server. For details about how to back up Replication Monitor operating environment information, see section 3.8.

To perform an overwrite installation of the Replication Monitor server:

1. Log on to Windows using a user ID that belongs to the Administrators group.

   If you have logged on to Windows with a user ID that does not belong to the Administrators group, a window appears during installation informing you that the execution must be performed by a user that belongs to the Administrators group, and the installation process terminates.

2. Insert the Replication Monitor CD-ROM. Select **Start**, **Run**, and then **Browse**. Select the CD-ROM drive and execute `setup.exe` from the files in the root folder.

   A window appears informing you of the start of the installation. This window displays a message that informs you that HiCommand products will be started and stopped during the installation and messages that prompt you to take the following actions:

   - Back up the databases of all HiCommand products before you begin the installation.
   - In a cluster configuration, manually stop the HiCommand Suite Common Component services (HBase Storage Mgmt Web Service and HBase Storage Mgmt Common Service) and all HiCommand product services.

   Note:

   When the version of the Replication Monitor server for the overwrite installation is earlier than that of the existing the Replication Monitor server, a message appears informing you that the installation cannot proceed because the version of the product to be installed is earlier than that of the existing the Replication Monitor server, and the installation stops.

   When canceling the installation in the following procedures, click the **Cancel** button, and click the **Yes** button in the cancellation confirmation dialog. In the Installation Stopped window that appears, click the **Finish** button to terminate the installer.

3. In the window informing you of the start of the installation, click the **Next** button.

   If any HiCommand Suite Common Component services are active:

   In a non-cluster configuration, a window appears reporting that the services will be stopped. Go to step 4.

In a cluster configuration, an error message is displayed and the window informing you of the start of the installation appears again.

If all HiCommand Suite Common Component services are stopped:

A window appears confirming the setup status of the embedded database HiRDB. Go to step 5.

There are four setup statuses for HiRDB, as shown below. The installer identifies the status and guides you through the optimal installation for that status. When the setup status of HiRDB is not set, an error message appears and the installation stops.

- *Not setup*: HiRDB is not set up.

- *Non-cluster configuration*: HiRDB has been set up in a non-cluster configuration.

- *Cluster configuration (executing node)*: HiRDB has been set up on the executing system in a cluster configuration.

- *Cluster configuration (standby node)*: HiRDB has been set up on the standby system in a cluster configuration.

4. In the window reporting that the HiCommand product services will be stopped, click the **Next** button.

   Processing to stop the services is performed and a window for checking the setup status of the embedded database HiRDB appears.

5. To continue the installation according to the information shown in the window for checking the HiRDB setup status, click the **Next** button.

   The steps to follow from this point differ depending on the version of the Replication Monitor server that is currently installed.

   When Replication Monitor 5.0 or a later version is installed:

   In a non-cluster configuration:

   A window appears, asking whether you want to start the HiCommand product services when the installation finishes. Go to step 9.

   In a cluster configuration:

   A confirmation window appears, indicating that preparation for the installation is complete. This window displays installation information such as the installation destination. Go to step 10.

   When a version of Replication Monitor earlier than 5.0 is installed:

   In a non-cluster configuration or cluster configuration (executing node):

   A window for selecting whether to reset Device Manager user account information appears. Go to step 6.

   In a cluster configuration (standby node):

   A confirmation window appears, indicating that preparation for the installation is complete. Go to step 10.

6. If you want to reset Device Manager user account information, choose **Yes** and click the **Next** button. If you do not want to reset the information, choose **No** and click the **Next** button.

When **Yes** is selected, a window for setting Device Manager user account information appears. Go to step 7.

When **No** is selected, the window for selecting whether to continue using the alert settings for the earlier version appears. Go to step 8.

7. Enter the Device Manager user account (user ID and password), and click the **Next** button. The password must be entered twice (the second entry is compared with the first entry to confirm that they are identical).

   A window for selecting whether to continue using the alert settings for the earlier version appears.

   A window for selecting whether to continue using the alert settings for the earlier version appears only when the HiRDB setup status is *non-cluster configuration* or *cluster-configuration (executing node)*.

   Note:

   If a user account for Replication Monitor to access Device Manager is not entered, an error message appears prompting you to re-enter the information.

   The user account that is set in this procedure is required for Replication Monitor to use Device Manager functionality. The user account is used when Replication Monitor accesses Device Manager. To enable Replication Monitor to use Device Manager functions, a user account must be specified that has the Modify permission in Device Manager and in which `All Resources` is allocated to its resource group.

   When specifying a user ID or password, use from 1 to 256 characters. If you specify 257 characters or more, the operation might fail. Specifiable characters are as follows:

Item	Specifiable characters
User ID	`A-Z a-z 0-9 # + - . @ _`
Password	`A-Z a-z 0-9 ! # $ % & ' ( ) * + - . = @ \ ^ _ |`

   At this point, the user account specified in this procedure is not checked as to whether it is valid and effective as a Device Manager user account. This will be checked when installation has completed normally and Replication Monitor performs an automatic or manual refresh.

   Enter the same password twice. If the first and second input values are not identical, an error message appears prompting you to re-enter the information.

8. To continue using the alert settings for the earlier version, choose **Yes** and then click **Next**. To not use the alert settings, choose **No** and then click **Next**.

   Selecting **Yes** exports the alert settings for the earlier version to a CSV file. In this case, after the installation completes, you need to import the settings from this file. For details on how to import the alert settings, see section 2.6.

   For a cluster configuration, the alert settings for the earlier version can be exported only from the executing node.

In a non-cluster configuration:

A window appears, asking whether you want to start the HiCommand product services when the installation finishes. Go to step 9.

In a cluster configuration (executing node):

A confirmation window appears, indicating that preparation for the installation is complete. This window displays installation information such as the installation destination. Go to step 10.

9. In the window asking whether you want to start HiCommand product services, make sure that the **Yes** radio button is selected if you want to start the services. If you do not want to start the services, select the **No** radio button. Then click the **Next** button.

   A confirmation window appears, indicating that preparation for the installation is complete. This window displays installation information such as the installation destination.

10. Check the installation information displayed in this window, and then click the **Execution** button.

    Installation processing begins, and several windows appear indicating various statuses during processing.

    When the installation has completed normally, a window appears reporting that the installation is complete.

    In the following cases, a window appears reporting that the installation has stopped:

    - When the user instructs the installer to stop the installation by clicking the **Cancel** button.
    - When the installation is terminated because of an error that occurred during the installation.

    Note:

    Do not cancel an upgrade installation or re-installation once the **Execution** button has been clicked. Doing so might damage files.

11. In the window reporting that the installation is complete, click the **Finish** button to finish the installation.

    The window closes.

    When the installation has completed normally, the operating statuses of the HiCommand Suite Common Component services (HBase Storage Mgmt Web Service and HBase Storage Mgmt Common Service) are as follows:

    - When the setup status of HiRDB is *non-cluster configuration*

      If you selected **Yes** in the window asking whether you want to start the HiCommand product services when the installation finishes, the services start automatically and are enabled. The Device Manager service (`HiCommandServer`) also starts automatically. Go to step 12.

      If you selected **No** in the window asking whether you want to start the HiCommand product services when the installation finishes, the services are disabled. Go to step 12.

    - When the setup status of HiRDB is *cluster configuration*

      The startup type of the services is set to **Manual** and the services are disabled. Go to step 18.

For details about actions to be taken when installation fails, such as cases where the user cancels the installation via the **Cancel** button or when an error occurs during the installation, see section 9.1.

12. Stop all HiCommand product services.

    If any HiCommand product services are active, execute the following command to stop them:

    ```
    installation-folder-for-HiCommand-Suite-Common-Component\bin\hcmdssrv /stop
    ```

    Note:

    The `hcmdssrv` command cannot be used to automatically stop services of the HiCommand product versions shown below. For details about how to stop the services, see the manual for each product.

    - Device Manager versions 5.6 or earlier
    - Tiered Storage Manager version 5.5 or eralier

    You can check whether the services are stopped by executing the following command:

    ```
    installation-folder-for-HiCommand-Suite-Common-Component\bin\hcmdssrv /status
    ```

13. Edit the `pdsys` file and `def_pdsys` file.

    Change the value for the `-x` option to the loopback address `127.0.0.1`.

    The following describes the storage destinations for the pdsys file and def_pdsys file.

    ```
    installation-folder-for-HiCommand-Suite-Common-Component\HDB\CONF\pdsys
    installation-folder-for-HiCommand-Suite-Common-Component\database\work\def_pdsys
    ```

14. Edit the `pdutsys` file and `def_pdutsys` file.

    Change the value for the `pd_hostname` parameter to the loopback address `127.0.0.1`. If the `pd_hostname` parameter does not exist, add the `pd_hostname` parameter, specifying the host name or loopback address after the change.

    The following describes the storage destinations for the `pdutsys` file and `def_pdutsys` file.

    ```
    installation-folder-for-HiCommand-Suite-Common-Component\HDB\CONF\pdutsys
    installation-folder-for-HiCommand-Suite-Common-Component\database\work\def_pdutsys
    ```

15. Edit the `HiRDB.ini` file.

    Change the value for the `PDHOST` parameter to the loopback address `127.0.0.1`.

    The following describes the storage destination for the `HiRDB.ini` file.

    ```
    installation-folder-for-HiCommand-Suite-Common-Component\HDB\CONF\emb\HiRDB.ini
    ```

16. Restart the machine.

17. Make sure that the HiCommand Suite Common Component service is running.

    ```
    installation-folder-for-HiCommand-Suite-Common-Component\bin\hcmdssrv /status
    ```

18. Refresh the storage subsystem of Device Manager to update the database data with the latest data, and then update the Replication Monitor configuration.

    Before you start Replication Monitor, adjust the output size of the logs that record the operating status of Replication Monitor. Specify the log output size in the property file (`logger.properties`). For details on the `logger.properties` file, see section 6.10.2.

2.3.3 Uninstalling Replication Monitor Server

This section explains how to uninstall the Replication Monitor server in Windows.

Note:

When you uninstall the Replication Monitor server, its property files are deleted. Do not uninstall the Replication Monitor server except in cases where you need to completely re-install the program due to problems in the machine.

Make sure that the embedded database HiRDB service `HiRDB/EmbeddedEdition _HD0` is active.

You can check whether the HiRDB service is running by opening the Windows Services window. If the HiRDB service is active, its status appears as **Started**.

To uninstall the Replication Monitor server:

1. Log on to Windows using a user ID that belongs to the Administrators group.

   If you have logged on to Windows using a user ID that does not belong to the Administrators group, a window appears during the uninstallation informing you that the execution must be performed by a user that belongs to the Administrators group, and the uninstallation process terminates.

2. Select **Start**, **Settings**, **Control Panel**, **Add/Remove Programs**, select HiCommand Replication Monitor in the Add/Remove Programs window, and then click the **Add/Remove** button.

   A window appears informing you of the start of the uninstallation. This window displays a message that informs you that HiCommand products will be started and stopped during the uninstallation and messages that prompt you to take the following actions:

   - Back up the databases of all HiCommand products before you begin the uninstallation.
   - If you are uninstalling the Replication Monitor server from a cluster configuration, manually stop the HiCommand Suite Common Component services (HBase Storage Mgmt Web Service and HBase Storage Mgmt Common Service) and all HiCommand product services.

3. In the window informing you of the start of the uninstallation, click the **Next** button.

   If any HiCommand Suite Common Component services are active:

   In a non-cluster configuration, a window appears reporting that the services will be stopped. Go to step 4.

   In a cluster configuration, an error message is displayed, and the window informing you of the start of the uninstallation appears again.

   If all HiCommand Suite Common Component services are stopped:

   In a non-cluster configuration, a window appears, asking whether you want to start the HiCommand product services when the uninstallation finishes. Go to step 5.

   In a cluster configuration, a confirmation window appears, indicating that preparation for the uninstallation is complete. This window displays the processing that will be executed at uninstallation. Go to step 6.

4. In the window reporting that the HiCommand product services will be stopped, click the **Next** button.

   Processing to stop the services is performed. A window appears, asking whether you want to start the HiCommand product services when the uninstallation finishes.

5. In the window asking whether you want to start HiCommand product services when the uninstallation finishes, make sure that the **Yes** radio button is selected if you want to start the services. If you do not want to start the services, select the **No** radio button. Then click the **Next** button.

   A confirmation window appears indicating that preparation for the uninstallation is complete. This window displays the content of the processing that is executed during the uninstallation.

6. Check the uninstallation information displayed in this window, and then click the **Execution** button.

   Uninstallation processing begins, and several windows appear indicating various statuses during processing.

   When the uninstallation has completed normally, a window appears reporting that the uninstallation is complete.

   In the following cases, a window appears reporting that the uninstallation has stopped:

   - When the user instructs the uninstaller to stop the uninstallation by clicking the **Cancel** button.
   - When the uninstallation is terminated because of an error that occurred during the uninstallation.

7. In the window reporting that the uninstallation is complete, click the **Finish** button to finish the uninstallation.

   The Uninstallation Complete Window closes.

   If the uninstallation is successful, the operating status of the HiCommand Suite Common Component services (HBase Storage Mgmt Web Service and HBase Storage Mgmt Common Service) is as follows:

   - In a non-cluster configuration:

     If you selected **Yes** in the window asking whether you want to start the HiCommand product services when the uninstallation finishes, the services start automatically and are enabled. The Device Manager service (`HiCommandServer`) also starts automatically.

     If you selected **No** in the window asking whether you want to start the HiCommand product services when the uninstallation finishes, the services are disabled.

   - When the setup status of HiRDB is *cluster configuration*

     The services are disabled.

     For details about actions to be taken when uninstallation fails, such as cases when an error occurs during uninstallation, see section 9.1.

2.4 Installing a Replication Monitor Server on a Management Server (Solaris)

This section explains how to install and uninstall the Replication Monitor server in the Solaris OS.

Note:

Installing Replication Monitor in a cluster environment involves a different procedure. To set up a cluster environment, read section 7.2 first and then refer to the installation procedure in section 7.2 as needed.

2.4.1 Performing a New Installation

This section explains how to perform a new installation of the Replication Monitor server in Solaris. The installation directories of the Replication Monitor server are as follows:

```
/opt/HiCommand/ReplicationMonitor
```

and

```
/var/opt/HiCommand/ReplicationMonitor
```

Check the following before performing a new installation:

- Make sure that no other application is running.
- To install the Replication Monitor server, the following free disk space is required to store the program and database.

  - 100 MB or more for the Replication Monitor server program

  - 200 MB or more for the Replication Monitor server database
- The following amount of free disk space is temporarily required to install the Replication Monitor server:
  - 1 GB or more under `/tmp`
  - 1 GB or more under `/var`
- Ensure that all of the preparations described in 2.2.2 and 2.2.5 are completed.
- You cannot install the Replication Monitor server under a directory referenced by a symbolic link. Similarly, you cannot specify a directory that includes a symbolic link as the storage destination for database files. Make sure that the installation destinations for the Replication Monitor server and the database files are not symbolic links.

Note:

Do not interrupt the installation by, for example, pressing the **Ctrl** and **C** keys together during execution of the installation. If you have interrupted the installation, execute `# pkginfo HRPM` to check whether information about Replication Monitor appears. If the information appears, uninstall the Replication Monitor server, and then re-execute the installation.

To perform a new installation of the Replication Monitor server:

1. Log in to Solaris as root.

   If you have logged into Solaris with an account other than root, an error message appears during the installation and the installation stops.

2. Insert the Replication Monitor CD-ROM.

3. Move to the directory where `install.sh` is stored (*CD-ROM-mount-directory*), and enter the following command:

```
# ./install.sh
```

   Processing begins. After preliminary checks (such as checks to determine whether the account is root and whether the Device Manager server has been installed), a message advises you that HiCommand products will be started and stopped during the installation. Further messages prompt you to take the following actions:

   - Back up the databases of all HiCommand products before you begin the installation.
   - In a cluster configuration, stop the HiCommand Suite Common Component daemons and all HiCommand product daemons.

   A message asks whether you want to continue with the installation.

   Note:

   If the current directory is other than the directory containing `install.sh`, an error message appears and the installation stops.

   Note:

   When you attempt to install the Replication Monitor server in a machine with no prerequisite version of the Device Manager server installed, a message appears informing you that the prerequisite version of Device Manager has not been installed, and the installation stops.

4. To continue executing the installation, enter `y` and press the **Enter** key.

   If any HiCommand Suite Common Component daemons are active:

   In a non-cluster configuration, a message appears reporting that the daemons will be stopped. Go to step 5.

   In a cluster configuration, an error message is displayed and then the message informing you of the start of the installation appears again.

   If all HiCommand Suite Common Component daemons are stopped:

   A message appears confirming the setup status of the embedded database HiRDB. Go to step 6.

   To interrupt the installation, enter `n` and then press the **Enter** key.

   There are four setup statuses for HiRDB, as shown below. The installer identifies the status and guides you through the optimal installation for that status. When the setup status of HiRDB is not set, an error message appears and the installation stops.

   - *Not setup*: HiRDB is not set up.

   - *Non-cluster configuration*: HiRDB has been set up in a non-cluster configuration.

   - *Cluster configuration (executing node)*: HiRDB has been set up on the executing system in a cluster configuration.

- *Cluster configuration (standby node)*: HiRDB has been set up on the standby system in a cluster configuration.

5. In response to the message reporting that the HiCommand product daemons will be stopped, enter `y` and then press the **Enter** key.

   Processing to stop the daemons is performed and a message confirming the setup status of the embedded database HiRDB appears.

6. To continue the installation according to the information shown in the message confirming the HiRDB setup status, enter `y` and then press the **Enter** key.

   A message appears asking you to specify a location in which the database files for the Replication Monitor server are to be stored.

   To interrupt the installation, enter `n` and then press the **Enter** key.

7. To store the database files for the Replication Monitor server in the displayed default location press the **Enter** key. To store them in a different location, enter that location, and then press the **Enter** key.

   A message appears prompting you to check the location in which the database files are to be stored.

   The following characters can be used for specifying the database file location:

   A to Z a to z 0 to 9 . and _single-byte spaces

   The following requirements also apply:

   - The location must be 100 characters or less (this includes all characters from the first character to the last character).
   - An absolute path must be specified.

     The specified path must not end with the path delimiter (`/`).
   - The location for the database file requires at least 200 MB of free space.

     For a cluster configuration, specify a shared disk at this step. No default is displayed. Also, specify the same path on both the executing and standby systems.

     When you install the Replication Monitor server in the standby system, if there is no database file under the user-specified shared disk path (for example, if the specified shared disk path differs from the path specified when the Replication Monitor server was installed in the executing system, or if the specified path is the same but is not a shared disk), an error message appears and installation stops. For details about action to be taken in this case, see section 9.4.

8. To continue the installation according to the information shown in the message prompting you check the location for storing the database files, enter `y` and then press the **Enter** key.

   In a non-cluster configuration or cluster configuration (executing node):

   A message appears prompting you to enter the user ID required for Replication Monitor to access Device Manager. Go to step 9.

   In a cluster configuration (standby node):

   The installation process begins and a message indicating the processing status is displayed. Go to step 14.

Entering `n` and then pressing the **Enter** key allows you to go back to step 7, in which you enter a destination for storing the database files. Entering `q` and then pressing the **Enter** key interrupts installation.

9. Enter the user ID required for Replication Monitor to access Device Manager, and press the **Enter** key.

   A message appears prompting you to enter the password required for Replication Monitor to access Device Manager.

   Note:

   When specifying a user ID or password, use from 1 to 256 characters. If you specify 257 characters or more, the operation might fail. Specifiable characters are as follows:

Item	Specifiable characters
User ID	`A-Z a-z 0-9 # + - . @ _`
Password	

   If the user account that has the Modify permission in Device Manager and in which `All Resources` is allocated to its resource group contains a character other than the above, specify a temporary user account by using the specifiable characters to complete installation, and then reset the account by using Web Client of Replication Monitor. For details about using Web Client to set up a Device Manager user account, see section 3.4.1.

   At this point, the user account specified in this procedure is not checked as to whether it is valid and effective as a Device Manager user account. This will be checked when installation has completed normally and Replication Monitor performs an automatic or manual refresh.

   Note:

   In steps 9 to 11, if the user account and port number required for Replication Monitor to access Device Manager are not entered, or the port number is outside the acceptable range, an error message appears prompting you to re-enter the information.

   The user account that is set in steps 9 and 10 (user ID and password) is used when Replication Monitor accesses Device Manager. To enable Replication Monitor to use Device Manager functions, a user account must be specified that has the Modify permission in Device Manager and in which `All Resources` is allocated to its resource group.

10. Enter the password required for Replication Monitor to access Device Manager, and press the **Enter** key. The password must be entered twice (the second entry is compared with the first entry to confirm that they are identical).

    A message appears prompting you to enter the port number for Device Manager to accept processing requests from Replication Monitor. Enter the same password twice. If the first and the second input values are not identical, an error message appears prompting you to re-enter the information.

11. If you do not need to change the displayed default value (port number: `2001`), press the **Enter** key. If you need to change the default value to another value, enter the port number and press the **Enter** key.

A message appears confirming the user account and port number for Device manager.

Device Manager uses the port number set in this step for HTTP communications. This port number is also specified for `server.http.port` of the `server.properties` file of the Device Manager server.

Execute the port number change only when you need to change the port number to a value that is different from the displayed default value, such as when another application that uses the same port number exists on the platform that executes the Replication Monitor server.

The number `2001` is the default value for the port number used by Device Manager in HTTP communications. If Device Manager has specified a port number other than the default, specify that port number.

The port number can be specified using a number from 1 to 65535.

If you press the **Enter** key without entering a port number, the default value is set.

12. To perform the installation according to the information shown in the message confirming the user account and port number, enter `y` and then press the **Enter** key.

    In a non-cluster configuration:

    A message appears, asking whether you want to start the HiCommand product daemons when the installation finishes. Go to step 13.

    In a cluster configuration (executing node):

    The installation process begins and a message indicating the processing status is displayed. Go to step 14.

    Entering `n` and then pressing the **Enter** key allows you to go back to step 9, in which you enter a user ID. Entering `q` and then pressing the **Enter** key interrupts installation.

13. In the message asking whether you want to start HiCommand product daemons when the installation finishes, enter `y` to start the daemons or `n` if you do not want to start the daemons. Then press the **Enter** key.

    Installation processing begins and a message appears indicating various statuses during processing.

    If you press the **Enter** key without entering a value, `y` is assumed.

14. Check the installation result.

    If the installation has completed normally, a message appears stating that the installation has completed normally, and that a trace log file for the installation (`/var/opt/HiCommand/ReplicationMonitor/logs/HRpM_InstallLog.log`) has been created. If the installation is terminated during processing, a message appears stating that the installation has failed and that a trace log file for the installation (`/var/opt/HiCommand/ReplicationMonitor/logs/HRpM_InstallLog.log`) has been created.

    If an error occurs during the installation, then an error message appears, and if the user has entered a command to stop the installation, then a message appears stating that the cancellation request was accepted, and the installation is terminated.

If the installation is successful, the operating status of the HiCommand Suite Common Component daemons (HBase Storage Mgmt Web Service and HBase Storage Mgmt Common Service) is as follows, according to how you responded to the message asking if you want to start the HiCommand product daemons when the installation finishes.

– When the setup status of HiRDB is *non-cluster configuration*

  If you entered `y` in response to the message about starting the HiCommand product daemons:

  The daemons start automatically and are enabled. The Device Manager daemon (HiCommandServer) also starts automatically.

  If you entered `n` in response to the message about starting the HiCommand product daemons:

  The daemons are disabled.

– When the setup status of HiRDB is *cluster configuration*.

  The startup type of the daemons is set to **Manual** and the daemons are disabled.

  For details about actions to be taken when installation fails, such as cases where the user cancels the installation or when an error occurs during the installation, see section 9.1.

  Before you start Replication Monitor, adjust the output size of the logs that record the operating status of Replication Monitor. Specify the log output size in the property file (`logger.properties`). For details on the `logger.properties` file, see section 6.10.2.

2.4.2 Upgrade Installation or Re-installation

This section explains how to perform an overwrite installation to upgrade or re-install the existing the Replication Monitor server in Solaris.

We recommend that you back up the Replication Monitor operating environment information (property files and database) before executing an overwrite installation of the Replication Monitor server. For details about how to back up Replication Monitor operating environment information, see section 3.8.

For an overwrite installation, the parameter values in the existing property files can be used without change, except for those in the `serverstorageif.properties` file when you upgrade Replication Monitor from a version earlier than 5.0 (The parameter values in the existing `serverstorageif.properties` file are not used).

Check the following before executing an overwrite installation:

- For an overwrite installation, you cannot revert to a version earlier than the current version. Check that the versions of the Replication Monitor server and Replication Monitor agent for the overwrite installation are the same as or later than the existing versions. If the version or revision is the same, you can install the older iteration of Replication Monitor after installing the newer one.
- The following amount of free disk space is temporarily required to install the Replication Monitor server:

- 1 GB or more under `/tmp`
- 1 GB or more under `/var`

- Ensure that all of the preparations described in 2.2.2 and 2.2.5 are completed.

Note:

Do not interrupt the installation by, for example, pressing the **Ctrl** and **C** keys together during execution of the installation. If you have interrupted the installation, execute `# pkginfo HRPM` to check whether information about Replication Monitor appears. If the information appears, uninstall the Replication Monitor server, and then re-execute the installation.

Note:

If you upgraded to this version from version 5.5.0-02 or earlier or from version 5.6, make sure that you delete or change the user authentication information so that the earlier information cannot be used.

Note:

When you perform an overwrite installation from version 4.0 or 4.2 to version 5.0 or later, user information will be inherited but user management permissions will not be inherited automatically. If you want to inherit user management permissions, set the user permissions after the overwrite installation has completed. For details about how to set user permissions, see section 3.3.4.

To perform an overwrite installation of the Replication Monitor server:

1. Log in to Solaris as root.

   If you have logged in to Solaris with an account other than root, an error message appears during the installation and the installation stops.

2. Insert the Replication Monitor CD-ROM.

3. Move to the directory where `install.sh` is stored (*CD-ROM-mount-directory*), and enter the following command:

   ```
   # ./install.sh
   ```

   Processing begins. After preliminary checks (such as checks to determine whether the account is root and whether the Device Manager server has been installed), a message advises you that HiCommand products will be started and stopped during the installation. Further messages prompt you to take the following actions:

   - Back up the databases of all HiCommand products before you begin the installation.
   - In a cluster configuration, stop the HiCommand Suite Common Component daemons and all HiCommand product daemons.

   A message asks whether you want to continue with the installation.

   Note:

   If the current directory is other than the directory containing `install.sh`, an error message appears and the installation stops.

   Note:

When you attempt to install the Replication Monitor server in a machine with no Device Manager server installed, a message appears informing you that Device Manager has not been installed, and the installation stops.

4. To continue executing installation, enter `y` and press the **Enter** key.

   If any HiCommand Suite Common Component daemons are active:

   In a non-cluster configuration, a message appears reporting that the daemons will be stopped. Go to step 5.

   In a cluster configuration, an error message is displayed and the message informing you of the start of the installation appears again.

   If all HiCommand Suite Common Component daemons are stopped:

   A message appears confirming the setup status of the embedded database HiRDB. Go to step 6.

   There are four setup statuses for HiRDB, as shown below. The installer identifies the status and guides you through the optimal installation for that status. When the setup status of HiRDB is not set, an error message appears and the installation stops.

   - *Not setup*: HiRDB is not set up.

   - *Non-cluster configuration*: HiRDB has been set up in a non-cluster configuration.

   - *Cluster configuration (executing node)*: HiRDB has been set up on the executing system in a cluster configuration.

   - *Cluster configuration (standby node)*: HiRDB has been set up on the standby system in a cluster configuration.

5. In response to the message reporting that the HiCommand product daemons will be stopped, enter `y` and then press the **Enter** key.

   Processing to stop the daemons is performed and a message confirming the setup status of the embedded database HiRDB appears.

6. To continue the installation according to the information shown in the message confirming the HiRDB setup status, enter `y` and then press the **Enter** key.

   The steps to follow from this point differ depending on the version of the Replication Monitor server that is currently installed.

   When Replication Monitor 5.0 or a later version is installed:

   In a non-cluster configuration:

   A message appears, asking whether you want to start the HiCommand product services when the installation finishes. Go to step 12.

   In a cluster configuration:

   The installation process begins and a message indicating the processing status is displayed. Go to step 13.

   When a version of Replication Monitor earlier than 5.0 is installed:

   In a non-cluster configuration or cluster configuration (executing node):

   A message for selecting whether to reset the Device Manager user account information necessary for enabling Replication Monitor to access Device Manager appears. Go to step 7.

In a cluster configuration (standby node):

The installation process begins and a message indicating the processing status is displayed. Go to step 13.

7. If you want to reset Device Manager user account information, enter `y` and press the **Enter** key. If you do not want to reset the information, enter `n` and press the **Enter** key. If you want to stop the installation, enter `q` and press the **Enter** key.

   If you entered `y` and pressed the **Enter** key, a message appears prompting you to enter the user ID required for Replication Monitor to access Device Manager. Go to step 8.

   If you entered `n` and pressed the **Enter** key, the message for selecting whether to continue using the alert settings for the earlier version appears. Go to step 11.

   Note:

   When you want to reset the user account information, enter `n` if the current user account contains a character other than the specifiable characters listed in step 8. After installation finishes, use Web Client of Replication Monitor to reset the user account information. For details, see section 3.4.1.

8. Enter the user ID required for Replication Monitor to access Device Manager and press the **Enter** key.

   A message appears prompting you to enter the password required for Replication Monitor to access Device Manager.

   Note:

   When specifying a user ID or password, use from 1 to 256 characters. If you specify 257 characters or more, the operation might fail. Specifiable characters are as follows:

Item	Specifiable characters
User ID	`A-Z a-z 0-9 # + - . @ _`
Password	

   If the user account that has the Modify permission in Device Manager and in which `All Resources` is allocated to its resource group contains a character other than the above, specify a temporary user account by using the specifiable characters to complete installation, and then reset the account by using Web Client of Replication Monitor. For details about using Web Client to set up a Device Manager user account, see section 3.4.1.

   At this point, the user account specified in this procedure is not checked as to whether it is valid and effective as a Device Manager user account. This will be checked when the installation has completed normally and Replication Monitor performs an automatic or manual refresh.

   Note:

   In steps 8 and 9, if the user account required for Replication Monitor to access Device Manager is not entered, or if the port number is outside the acceptable range, an error message appears prompting you to re-enter the information.

The user account set in steps 8 and 9 (user ID and password) is used when Replication Monitor accesses Device Manager. To enable Replication Monitor to use the Device Manager functions, a user account must be specified that has the Modify permission in Device Manager and in which `All Resources` is allocated to its resource group.

9. Enter the password required for Replication Monitor to access Device Manager, and press the **Enter** key. The password must be entered twice (the second entry is compared with the first entry to confirm that they are identical).

   A message asking you to confirm the user account appears.

   Enter the same password twice. If the first and the second input values are not identical, an error message appears prompting you to re-enter the information.

10. To perform the installation according to the information shown in the message for confirming the user account, enter `y` and then press the **Enter** key.

    A message for selecting whether to continue using the alert settings for the earlier version appears.

    Entering `n` and then pressing the **Enter** key allows you to go back to step 8, in which you enter a user ID. Entering `q` and then pressing the **Enter** key interrupts installation.

11. To continue using the alert settings for the earlier version, enter `y` and then press the **Enter** key. To not use the alert settings, enter `n` and then press the **Enter** key.

- In a non-cluster configuration:

  A message appears, asking whether you want to start the HiCommand product daemons when the installation finishes. Go to step 12.

- In a cluster configuration (executing node):

  Installation processing begins and a message appears showing various statuses during processing. When the installation processing has completed, the result is displayed. Go to step 13.

12. In the message asking whether you want to start HiCommand product daemons when the installation finishes, enter `y` to start the daemons or `n` if you do not want to start the daemons. Then press the **Enter** key.

    Installation processing begins and a message appears showing various statuses during processing.

13. Check the result of the installation.

    If the installation has completed normally, a message appears stating that the installation has completed normally, and that a trace log file for the installation (`/var/opt/HiCommand/ReplicationMonitor/logs/HRpM_InstallLog.log`) has been created. If the installation is terminated during processing, a message appears stating that the installation has failed and that a trace log file for the installation (`/var/opt/HiCommand/ReplicationMonitor/logs/HRpM_InstallLog.log`) has been created.

    If an error occurs during the installation, then an error message appears, and if the user has entered a command to stop the installation, then a message appears stating that the cancellation request was accepted, and the installation is terminated.

If the installation is successful, the operating status of the HiCommand Suite Common Component daemons (HBase Storage Mgmt Web Service and HBase Storage Mgmt Common Service) is as follows, according to how you responded to the message asking if you want to start the HiCommand product daemons when the installation finishes.

- When the setup status of HiRDB is *non-cluster configuration*

  If you entered `y` in response to the message about starting the HiCommand product daemons:

  The daemons start automatically and are enabled. The Device Manager daemon (HiCommandServer) also starts automatically. Go to step 14.

  If you entered `n` in response to the message about starting the HiCommand product daemons:

  The daemons are disabled. Go to step 14.

- When the setup status of HiRDB is *cluster configuration*.

  The startup type of the daemons is set to **Manual** and the daemons are disabled. Go to step 20.

  For details about actions to be taken when installation fails, such as cases where the user cancels installation or when an error occurs during the installation, see section 9.1.

14. Stop all HiCommand product daemons.

    If any HiCommand product daemons are active, execute the following command to stop them:

```
# /opt/HiCommand/Base/bin/hcmdssrv -stop
```

    Note:

    The `hcmdssrv` command cannot be used to automatically stop daemons of the For HiCommand product versions shown below. For details about how to stop the daemons, see the manual for each product.

    - Device Manager versions 5.6 or earlier
    - Tiered Storage Manager version 5.5 or eralier

    You can check whether the daemons are stopped by executing the following command:

```
# /opt/HiCommand/Base/bin/hcmdssrv -status
```

15. Edit the `pdsys` file and `def_pdsys` file.

    Change the value for the `-x` option to the loopback address `127.0.0.1`.

    The following describes the storage destinations for the `pdsys` file and `def_pdsys` file.

```
/opt/HiCommand/Base/HDB/conf/pdsys
/opt/HiCommand/Base/database/work/def_pdsys
```

16. Edit the `pdutsys` file and `def_pdutsys` file.

    Change the value for the `pd_hostname` parameter to the loopback address `127.0.0.1`. If the `pd_hostname` parameter does not exist, add the `pd_hostname` parameter, specifying the host name or loopback address after the change.

    The following describes the storage destinations for the `pdutsys` file and `def_pdutsys` file.

```
/opt/HiCommand/Base/HDB/conf/pdutsys
```

```
/opt/HiCommand/Base/database/work/def_pdutsys
```

17. Edit the `HiRDB.ini` file.

    Change the value for the `PDHOST` parameter to the loopback address `127.0.0.1`.

    The following describes the storage destination for the HiRDB.ini file.

```
/opt/HiCommand/Base/HDB/conf/emb/HiRDB.ini
```

18. Restart the machine.

19. Make sure that the HiCommand Suite Common Component daemons are running.

```
opt/HiCommand/Base/bin/hcmdssrv –status
```

20. Refresh the storage subsystem of Device Manager to update the database data with the latest data, and then update the Replication Monitor configuration.

    Before you start Replication Monitor, adjust the output size of the logs that record the operating status of Replication Monitor. Specify the log output size in the property file (`logger.properties`). For details on the `logger.properties` file, see 6.10.2.

2.4.3 Uninstalling Replication Monitor Server in Solaris

When you uninstall the Replication Monitor server, its property files are deleted. Do not uninstall the Replication Monitor server except in cases where you need to completely re-install the program due to problems in the machine.

We recommend that you back up the Replication Monitor operating environment information (property files and database) before executing an overwrite installation of the Replication Monitor server. For details about how to back up Replication Monitor operating environment information, see section 3.8.

To uninstall the Replication Monitor server:

1. Log in to Solaris as root.

   If you have logged in to Solaris with an account other than root, an error message appears during the uninstallation and the uninstallation stops.

2. Enter the following command and press the **Enter** key:

```
# /opt/HiCommand/ReplicationMonitor/inst/uninstall.sh
```

   Processing begins. After preliminary checks (such as checks to determine whether the account is root), a message advises you that HiCommand products will be started and stopped during the uninstallation. Further messages prompt you to take the following actions:

   - Back up the databases of all HiCommand products before you begin the uninstallation.
   - In a cluster configuration, stop the HiCommand Suite Common Component daemons (HBase Storage Mgmt Web Service and HBase Storage Mgmt Common Service) and all HiCommand product daemons.

   A message asks whether you want to continue the processing.

3. To continue with the uninstallation, enter `y` and press the **Enter** key.

   If any HiCommand Suite Common Component daemons are active:

In a non-cluster configuration, a message appears reporting that the daemons will be stopped. Go to step 4.

In a cluster configuration, an error message is displayed and the message informing you of the start of the uninstallation appears again.

If all HiCommand Suite Common Component daemons are stopped:

In a non-cluster configuration, a message appears, asking whether you want to start the daemons when the uninstallation finishes. Go to step 5.

In a cluster configuration, the uninstallation process begins and a message indicating the processing status is displayed. Go to step 6.

If you want to stop the uninstallation, enter `n` and press the **Enter** key.

4. In response to the message reporting that the HiCommand product daemons will be stopped, enter `y` and then press the **Enter** key.

   Processing to stop the HiCommand product daemons is performed. A message appears, asking whether you want to start the HiCommand product daemons when the uninstallation finishes.

5. In response to the message asking whether you want to start the HiCommand product daemons when the uninstallation finishes, enter `y` to start the daemons or `n` if you do not want to start the daemons. Then press the **Enter** key.

   Uninstallation processing begins and a message appears showing various statuses during processing.

   If you press the **Enter** key without entering a value, `y` is assumed.

6. Check the uninstallation result.

   If the uninstallation has completed normally, a message appears showing that the uninstallation has succeeded. If the uninstallation terminates during processing, a message appears showing that the uninstallation has failed, and that a trace log file for the uninstallation (`/var/opt/HiCommand/ReplicationMonitor/logs/HRpM_UninstallLog.log`) has been created.

   If an error occurs during the uninstallation, then an error message appears, and if the user has entered a command to stop the uninstallation, then a message appears stating that the cancellation request was accepted, and the uninstallation is terminated.

   For details about actions to be taken when uninstallation fails, such as cases where the user cancels the uninstallation or when an error occurs during the uninstallation, see section 9.1.

2.5 Installing an Agent on a Pair Management Server

In an open system, installing a Replication Monitor agent in the pair management server enables the Replication Monitor functions to be used more effectively.

Before you can install the Replication Monitor agent, the Device Manager agent must be installed as a prerequisite program. For details about the Device Manager agent, see section 2.2.3.

The following section explains how to install a Replication Monitor agent.

2.5.1 Installing a Replication Monitor Agent on a Pair Management Server (For Open Systems)

This section describes how to install and uninstall a Replication Monitor agent on the pair management server in an open system.

Prior to installation or uninstallation, check the following points:

- When the target pair management server uses Windows as its OS, the user must have logged in using a user ID in the `Administrator` group.
- When the target pair management server uses Solaris, HP-UX, AIX, or Linux as its OS, the user must have logged in using a user ID in the root.
- The Device Manager agent must already have been installed on the pair management server and it must be able to communicate with the Device Manager server.
- The OS of the target pair management server must be supported (the OSs that the Device Manager agent and the Replication Monitor agent support are different).
- All the preparations described in section 2.2.4 must have been completed.

Unless otherwise specified, execute all the operations described below at the pair management server where the Replication Monitor agent is installed.

The Replication Monitor agent cannot be registered in the cluster resources because the Replication Monitor agent is not compatible with a logical host. The Replication Monitor agent operates on each physical host (the pair management server) that makes up the cluster, and collects information of each pair management server.

Although the Replication Monitor agent can be installed on servers in a cluster environment, cluster functionality is not available to the Replication Monitor agent.

Note: Do not uninstall the Device Manager agent before uninstalling the Replication Monitor agent. If you uninstall the Device Manager agent by mistake, make sure that you also uninstall the Replication Monitor agent.

2.5.1.1 Performing a New Agent Installation

To perform a new installation of a Replication Monitor agent, first download the Replication Monitor agent installer to the target pair management server. Next, execute the installer to install the Replication Monitor agent. The following describes the procedure.

To download the Replication Monitor agent installer:

1. Log in to the Replication Monitor server on the management server.

   Start the Web browser and enter the URL to connect to Replication Monitor's Web Client. The URL is as follows:

   ```
   http://Replication-Monitor-address:port-number/ReplicationMonitor/
   ```

   - In *Replication-Monitor-address*, specify the Replication Monitor's IP address or host name.
   - In *port-number*, specify the port number of HBase Storage Mgmt Web Service (default: `23015`).

     Note: For SSL, use `https` and port `23016` (default).

   When the URL is entered, the start window and the Login window are displayed.

2. In the Login window, enter the user ID and password and then click the **Log in** button.

   Web Client's main window appears.

3. From the menu in the global tasks bar area (the menu located in the upper part of the window), choose **Go**, and then **Download**.

   A dialog box for downloading Replication Monitor agent is displayed.

4. From the **Download** column, choose the download link appropriate to the OS of the pair management server.

   The Replication Monitor agent installer is downloaded to the pair management server.

   The names of the files to be downloaded are as follows:

   `hrpmAgent_win.exe` for Windows

   `hrpmAgent_sol.tar` for Solaris

   `hrpmAgent_hp.tar` for HP-UX

   `hrpmAgent_aix.tar` for AIX

   `hrpmAgent_linuxx86.tar` for Linux (x86)

   `hrpmAgent_linuxipf.tar` for Linux (IPF)

The subsequent procedure depends on whether the OS of the pair management server is Windows, Solaris, HP-UX, AIX, or Linux.

When the OS of the pair management server is Windows

To install a Replication Monitor agent (for Windows):

1. Execute the downloaded file (`hrpmAgent_win.exe`).

   The installer starts and displays a message asking whether to continue the installation of the Replication Monitor agent.

2. To continue with the installation, click the **Yes** button.

   Following an installation progress message, a message reporting that installation has finished is displayed.

3. Click the **OK** button.

   The installer is terminated.

When the OS of the pair management server is Solaris, HP-UX, AIX, or Linux

To install a Replication Monitor agent (for Solaris, HP-UX, AIX, or Linux):

1. Expand the downloaded file (`hrpmAgent_sol.tar`, `hrpmAgent_hp.tar`, `hrpmAgent_aix.tar`, `hrpmAgent_linuxx86.tar`, or `hrpmAgent_linuxipf.tar`) to the desired directory.

   The files required for the installation are expanded.

2. From the expanded files, execute `hrpmAgent.sh`.

   The installer starts and displays a message asking whether to continue the installation of the Replication Monitor agent.

3. To continue with the installation, press the **y** key.

   Following an installation progress message, a message reporting that installation has finished is displayed, and the installer is terminated.

After installing the Replication Monitor agent, update the Replication Monitor configuration. This enables Replication Monitor to recognize the Replication Monitor agent. To use the Replication Monitor agent after installation, you must perform the setup. See section 2.5.1.3. After performing the setup, update the Replication Monitor configuration again.

2.5.1.2 Performing an Overwrite Installation

The installation procedure for overwriting a Replication Monitor agent is the same as for a new installation. Note the following:

Checking before installation

When an attempt is made to overwrite a Replication Monitor agent, the installer displays a message to confirm the execution of the overwrite installation. The installation begins when you click the **Yes** button in Windows or the **y** key in Solaris, HP-UX, AIX, or Linux.

Versions supporting overwrite installation

Overwrite installation cannot be used to return to a version that is earlier than the current version. Make sure that the version of the Replication Monitor agent to be installed by overwriting is the same as or newer than the version of the existing Replication Monitor agent. If the version or revision is the same, you can install the updated version of the Replication Monitor agent and then install the pre-updated version of the Replication Monitor agent. For example, you can install the updated version of the Replication Monitor agent 5.0 and then install the pre-updated version of the Replication Monitor agent 5.0.

To check the version of the currently installed Replication Monitor agent, use the following command:

For Windows

Execute `hrpm_agentversion.bat` in *Device-Manager-agent-installation-directory*`\bin\`. The specification format is as follows:

Device-Manager-agent-installation-directory`\bin\hrpm_agentversion`

For Solaris, HP-UX, AIX, or Linux

Execute `hrpm_agentversion` in *Device-Manager-agent-installation-directory*`/bin/`. The specification format is as follows:

Device-Manager-agent-installation-directory`/bin/hrpm_agentversion`

Note:If you have unintentionally uninstalled the Device Manager agent, make sure that you also temporarily uninstall the Replication Monitor agent. If you reinstall the Device Manager agent without having first uninstalled the Replication Monitor agent, the Replication Monitor agent will not operate.

2.5.1.3 Setup After Installation

After you have completed the installation of the Replication Monitor agent, specify the following settings according to the pair management server environment:

Specifying the CCI installation directory

If CCI is not in the default location, edit the Device Manager agent's property file `server.properties`.

The property file is stored at the following location:

Device-Manager-agent-installation-directory`/agent/config/`

The parameter to be edited is as follows:

- `server.agent.rm.location`

  Specifies the CCI installation directory. Note that even in Windows, use a forward slash (`/`) as a delimiter for directories, not a backslash (`\`).

Specifying the location of the CCI configuration definition file

If the CCI configuration definition file is not in the default location, edit the Replication Monitor agent's property file `agent.properties`.

The property file is stored at the following location:

Device-Manager-agent-installation-directory`/mod/hrpm/config/`

The parameter to be edited is as follows:

- `agent.rm.horcmSource`

  Specifies the location of the CCI configuration definition file. Note that even in Windows, use a forward slash (`/`) as a delimiter for directories, not a backslash (`\`).

  By default, the following value is specified:

For Windows

Windows-system-directory

(Use a forward slash (/) as a delimiter for directories.)

For Solaris, HP-UX, AIX, or Linux

/etc

Specifying a port number for Replication Monitor and a Replication Monitor agent

To connect Replication Monitor and a Replication Monitor agent, it is necessary to specify the same port number for both. To specify a port number, edit the following property files:

- Replication Monitor's property file agentif.properties
- Replication Monitor agent's property file server.properties (the property file shared with the Device Manager agent and other agents)

The storage locations for the Replication Monitor server's property file agentif.properties are as follows:

- For Windows

  Replication-Monitor-installation-directory/conf

- For Solaris

  /opt/HiCommand/ReplicationMonitor/conf

The parameter to be edited for the Replication Monitor server's property file agentif.properties is as follows:

- agentif.agentPort

  A value from 1024 to 49151 can be set as the TCP port number to be used when Replication Monitor connects to the Replication Monitor agent service or daemon.

The storage locations for the Replication Monitor agent's property file server.properties are as follows:

- For Windows

  HiCommand-Suite-Common-Component-installation-directory/agent/config

- For Solaris, HP-UX, and Linux

  /opt/HDVM/HBaseAgent/agent/config

- For AIX

  /usr/HDVM/HBaseAgent/agent/config

The parameter to be edited for the Replication Monitor agent's property file server.properties is as follows:

- server.agent.port

  A value from 1024 to 49151 can be set as the TCP port number to be used by the Replication Monitor agent service or daemon.

Note:

- The property file server.properties is used by the Device Manager agent and other agents. Accordingly, you must pay particular attention when you edit this file because any changes will affect the operation of the Device Manager agent.

- Specify the same port number for all Replication Monitor agents that connect to Replication Monitor.
- In an environment where the following Device Manager agents co-exist, the port numbers specified in their respective `server.properties` property files might differ: (i) a Device Manager agent that was upgraded to version 5.0 or later from a version earlier than 5.0, and (ii) a Device Manager agent version 5.0 or later that was newly installed. In these `server.properties` property files, specify the same port number as the one in the Replication Monitor's `agentif.properties` property file.

If you edit the property file, you must restart the Device Manager agent's service. For details about how to start and stop the service, see section 6.3.2.

2.5.1.4 Uninstalling the Replication Monitor Agent

This section describes how to uninstall the Replication Monitor agent.

Note:

If the CCI instance is running, stop it before uninstallation. For details about how to stop the CCI instance, see section 6.3.3.

When the OS of the pair management server is Windows

To uninstall the Replication Monitor agent (for Windows):

1. From the **Start** menu, choose **Settings**, **Control Panel**, and then **Add or Remove Programs**. In the Add or Remove Programs window, choose **Replication Monitor - Agent** and then click the **Change/Remove** Button.

   The installer starts.

   A window indicating that the preparations for uninstallation are underway is displayed and then a message is displayed asking whether to continue uninstallation of the Replication Monitor agent.

2. To continue with the uninstallation, click the **Yes** button.

   Following an uninstallation progress message, a message reporting that uninstallation has finished is displayed.

3. Click the **OK** button.

   The installer is terminated.

4. From the property file, delete unneeded parameters.

   Of the parameters that were added to the property file `server.properties` during the installation, delete those items that are not used by other agents, such as the Device Manager agent.

   If you uninstall the Replication Monitor agent after uninstalling the Device Manager agent, folders that were created during the Device Manager agent installation might not be deleted. Therefore, delete such folders manually.

If there are files remaining in folders that were not deleted, other HiCommand products might be using these folders and files. In such a case, make sure that you do not delete these folders and files.

When the OS of the pair management server is Solaris, HP-UX, AIX, or Linux

To uninstall the Replication Monitor agent (for Solaris, HP-UX, AIX, or Linux):

1. Enter the following command and then press the **Enter** key:

   ```
   # Device-Manager-agent-installation-directory/bin/hrpm_uninst.sh
   ```

   The installer starts and displays a message asking whether to continue uninstallation of the Replication Monitor agent.

2. To continue with the uninstallation, press the **y** key.

   Following an uninstallation progress message, a message reporting that uninstallation has finished is displayed, and then the installer is terminated.

3. From the property file, delete unneeded parameters.

   Of the parameters that were added to the property file `server.properties` during the installation, delete those items that are not used by other agents, such as the Device Manager agent.

2.6 Importing the Alert Settings for the Earlier Version

When performing an upgrade installation of the Replication Monitor server, during the installation procedure, you can specify whether to continue using the alert settings for the earlier version. If you specify that you continue using the settings, the settings will be exported. In this case, after the upgrade installation completes normally, you need to import the settings to the Replication Monitor server.

To import the alert settings, use the `hrpmdbconvert` command. In a Windows system, only a member of the Administrators group can execute this command. In a Solaris system, only a user who logged in as root can execute this command.

The format and storage destination directory for the file that contains the alert settings, which is created in the export processing during the installation are as follows:

File format: CSV

File storage destination directory:

- In a Windows system:

```
installation-directory-for-Replication-Monitor\tmp\HRpMAlertSettingData
```

- In a Solaris system:

```
/var/opt/HiCommand/ReplicationMonitor/tmp
```

The format and installation directory for the `hrpmdbconvert` command are as follows:

Command format:

- In a Windows system:

```
hrpmdbconvert.bat /datapath name-of-the-directory-storing-the-alert-settings-files
```

- In a Solaris system:

```
hrpmdbconvert.sh -datapath name-of-the-directory-storing-the-alert-settings-files
```

Use the absolute path when specifying the directory name in the `datapath` parameter.

Command installation directory:

- In a Windows system:

```
Replication-Monitor-server-installation-directory\bin
```

- In a Solaris system:

```
/opt/HiCommand/ReplicationMonitor/bin
```

To import the alert settings for the earlier version:

1. Acquire the most recent configuration information

   From the management client, log in to Replication Monitor to acquire copy pair configuration information. For details on how to acquire the configuration information, see section 3.7.

2. Stop the HiCommand Suite Common Component services and the Device Manager service.

In the management server, stop the HiCommand Suite Common Component services (HBase Storage Mgmt Web Service and HBase Storage Mgmt Common Service) and the Device Manager service.

3. Execute the `hrpmdbconvert` command to import the alert settings.

   In the management server, execute the `hrpmdbconvert` command.

   The following example shows how to specify the `hrpmdbconvert` command (when the management server OS is Solaris):

```
# hrpmdbconvert.sh -datapath
"/var/opt/HiCommand/ReplicationMonitor/tmp/HRpMAlertSettingData"
```

   In a cluster configuration, perform this step on the executing node.

4. Restart the HiCommand Suite Common Component services and the Device Manager service.

   In the management server, restart the HiCommand Suite Common Component services (HBase Storage Mgmt Web Service and HBase Storage Mgmt Common Service) and the Device Manager service.

2.7 After Finishing the Installation

2.7.1 Notes on Uninstalling Device Manager

Do not uninstall Device Manager in an environment where Replication Monitor is installed. When uninstalling Device Manager, first uninstall Replication Monitor.

If Device Manager is uninstalled in an environment where Replication Monitor is installed, even if Device Manager is re-installed, Replication Monitor cannot be used. To use Replication Monitor, you must first uninstall Replication Monitor, install and set up Device Manager, and then re-install Replication Monitor.

Note:

If Replication Monitor is uninstalled when it is the only HiCommand product installed on the management server, the HiCommand product user management information also is lost.

2.7.2 Notes on Stopping HiCommand Product Services and Daemons

This section gives notes on stopping a service or daemon by using the `hcmdssrv` command in an environment where Device Manager has been installed.

- Executing the `hcmdssrv` command with the `stop` option specified stops the following services or daemons and all HiCommand product services or daemons:
  - HBase Storage Mgmt Web Service
  - HBase Storage Mgmt Common Service
  - HiCommandServer
  - HiCommand Tiered Storage Manager
  - HiRDB

  Note:

  The `hcmdssrv` command cannot be used to automatically stop services or daemons of the For HiCommand product versions shown below. For details about how to stop the services or daemons, see the manual for each product.

  - Device Manager version 5.6 or earlier
  - Tiered Storage Manager version 5.5 or earlier
- In Windows, `HiRDB/EmbeddedEdition _HD0` must always be running for HiCommand products. Check whether `HiRDB/EmbeddedEdition _HD0` is running by viewing the list in the Windows Services window. If `HiRDB/EmbeddedEdition _HD0` is not running, start `HiRDB/EmbeddedEdition _HD0`.

- In Windows, do not start or stop `HiRDB/EmbeddedEdition _HD0` by using the Windows Services window. Doing so prevents the `hcmdssrv` command from operating normally. If you mistakenly perform the operation, make sure that **Startup Type** for `HiRDB/EmbeddedEdition _HD0` is set to **Automatic**, and then restart the computer.

Chapter 3 Configuring Replication Monitor Initial Settings

This chapter explains the task flow for configuring Replication Monitor's initial settings; it also explains how to operate Replication Monitor.

- About the Initial Settings Task Flow (see section 3.1)
- Registering License Information (see section 3.2)
- Setting Up User Information (see section 3.3)
- Registering an Information Source (see section 3.4)
- Setting Up the Refresh Function (see section 3.5)
- Setting Up Data Retention (see section 3.6)
- Acquiring the Most Recent Configuration Information (see section 3.7)
- Backing Up Operating Environment Information (see section 3.8)

3.1 About the Initial Settings Task Flow

Figure 3.1 shows the task flow for configuring the initial settings after you have installed Replication Monitor.

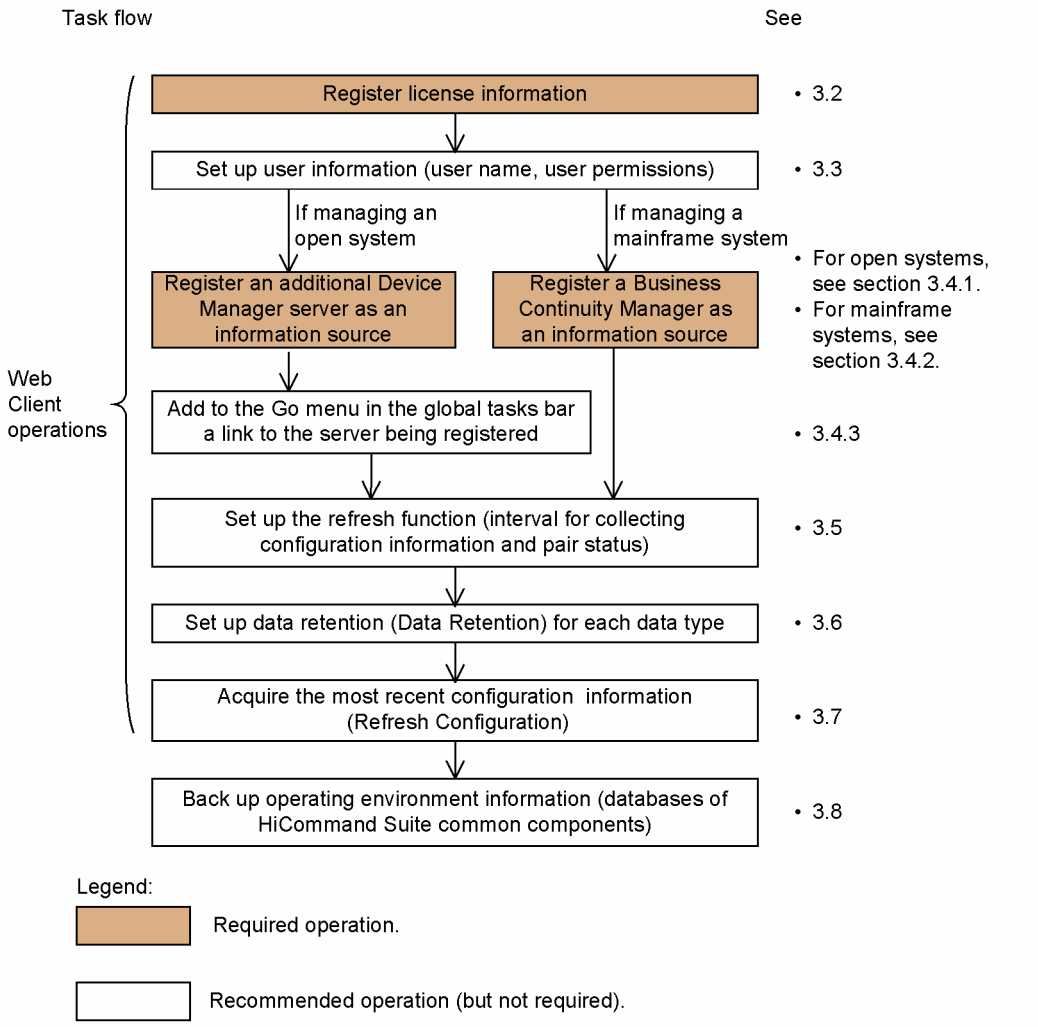

Figure 3.1 Task Flow for Initial Settings

3.2 Registering License Information

This section explains how to register license information into Replication Monitor, and how to view license information that has been registered in Replication Monitor.

3.2.1 About License Keys

Before you can use Replication Monitor, you must use a license key to register license information into the Replication Monitor server. The following lists the license key types:

License Type: **Permanent**

A permanent license key allows permanent use of the relevant Replication Monitor product. This key is provided for each management-target storage subsystem.

License Type: **Temporary**

A temporary license key allows temporary use of the relevant Replication Monitor product. This key is provided for each system.

License Type: **Emergency**

An emergency license key allows temporary use of the relevant Replication Monitor product in an emergency situation. This key is provided for each system. If an emergency key is added in an environment where a permanent key is already registered, the emergency key information will take precedence.

3.2.2 Registering License Information (License Key)

The first time you log in from the Web Client after you have installed Replication Monitor, you must register license information.

You register license information by using the Replication Monitor Web Client to specify a license key or to specify a license file that contains the license key.

To register license information:

1. Specify the Replication Monitor URL in the browser.

   `http://`*Replication-Monitor-address*`:`*port-number*`/ReplicationMonitor/`

   In *Replication-Monitor-address*, specify the IP address or host name of Replication Monitor server.

   In *port-number*, specify the port number for HBase Storage Mgmt Web Service (default is 23015).

   Note: For SSL, use `https` and the port `23016` (default).

   Entering URL displays the Start Replication Monitor window and the Login window.

2. Click the **License** button in the log-in window, see Figure 3.2.

A dialog box for registering license information is displayed. This dialog box includes an area that displays the Replication Monitor version and license type. If license information has not been registered, **Unregistered** is displayed in the **License Type** field.

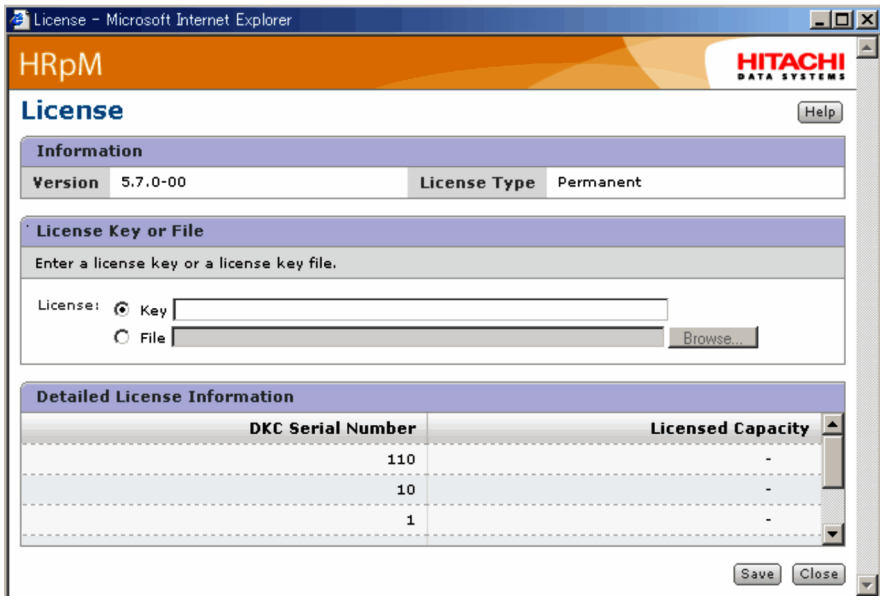

Figure 3.2 Dialog Box for Registering License Information

3. Select the **Key** or the **File** radio button, and then specify either a license key or a license file for registration.

   When you specify a license file, you may either specify the file's absolute path or choose the file from the file selection window that is displayed when you click the **Browse** button.

4. Click the **Save** button to register the information associated with the specified license key.

   The license information is registered into the system.

5. Click the **Close** button.

   The login window is displayed again.

6. To continue with login after you have registered the license information, enter your user ID and password, and then click the **Login** button.

   The Replication Monitor main window is displayed.

   Note:

   The first time you log in with the Web Client, in advance ask a user who has the User Management permission to create a new user account for Replication Monitor, and use the user ID and password of the user who has that user account.

   You can also use the default user account (the user ID is `System` and its corresponding default password is `manager`).

3.2.3 Viewing License Information

There are two ways to view the license information that has been registered in Replication Monitor:

- From the **Explorer** menu, choose **Settings** and then **License Info** to view license information in the subwindow that is displayed in the application area.

  To change the registered license information, click the **Edit License** button in the subwindow to display a dialog box for editing license information.

- From the global tasks bar area, choose **Help** and then **About** to view license information in the dialog box that is displayed.

  You can also change the registered license information from this dialog box.

With either method, if you are using a temporary or emergency license, the number of days remaining until the license expires and the license's expiration dates are displayed in the area that displays the Replication Monitor version and license type.

3.3 Setting Up User Information

This section explains how to register a new user who will use Replication Monitor, how to assign user permissions, and how to change user information.

Note: Changed user information might not be updated immediately in the windows. To refresh the display, click the **Refresh Tree** button.

3.3.1 User Permissions That Can Be Set With Replication Monitor

The features of Replication Monitor that a user is able to use are determined by the user permissions that have been assigned to the user. The user permission types are listed below:

User Management

Allows user management operations, such as creating user accounts and setting user permissions.

Modify

Allows modification of various settings for managed targets (storage subsystems, hosts).

View

Allows viewing of information associated with managed targets (storage subsystems, hosts).

Multiple permission types can be assigned to a user. The following table shows the combinations of permissions supported by Replication Monitor.

Table 3.1 Possible Combinations of User Permissions

Combination No.	User Management	Modify	View
1	Y	Y	Y
2	Y	N	Y
3	Y	N	N
4	N	Y	Y
5	N	N	Y

Legend:

Y: Permission that is assigned.

N: Permission that is not assigned.

3.3.2 Creating a New User Account

You register a new user into Replication Monitor by creating a user account for that user. This operation can be performed only by a user who has the User Management permission.

To create a new user account:

1. From the **Explorer** menu, choose **Administration** and then **Users and Permissions**.

   An object tree from which you can select **Users** is displayed in the navigation area, and a list of user management items is displayed in the application area.

2. Either choose **Users** in the object tree or click the **Users** in the list.

   A user list is displayed in the application area.

3. Click the **Add User** button.

   A dialog box for adding a user account to the system is displayed, see Figure 3.3.

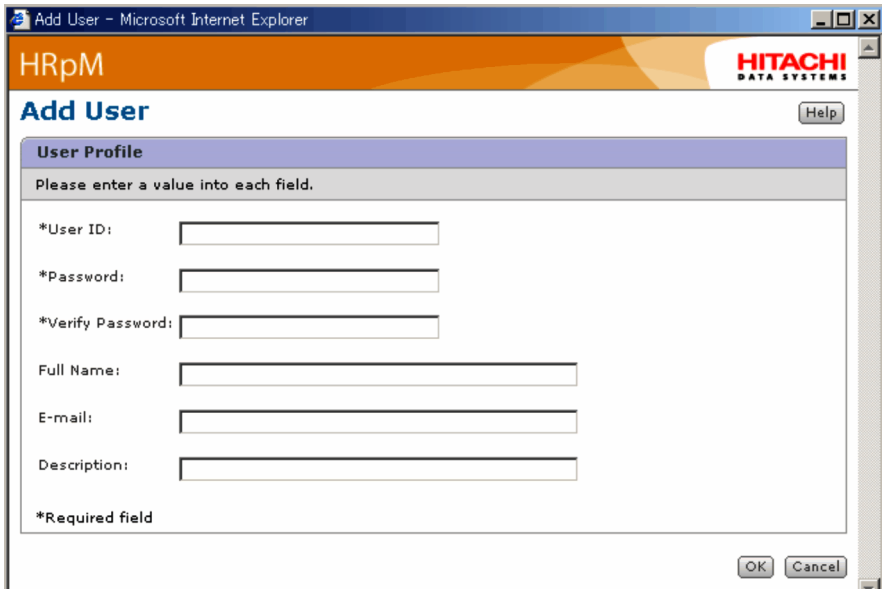

Figure 3.3 Dialog Box for Adding a User Account

4. Enter a user ID and password for the user account that is to be created.

   Enter the password in the password field, and then re-enter the same password in the verification field below.

   Note:

   You must make an entry in each field marked with an asterisk (*), such as the user ID (Login ID) and password.

   Note:

   You must enter the user ID and password by following the rules set by the user administrator. The following characters can be specified. The user IDs are not case-sensitive. However, the user IDs are displayed exactly as they are entered by the user.

Item	Characters that can be specified
User ID	A to Z, a to z, 0 to 9, #, +, -, ., @, _
Password	A to Z, a to z, 0 to 9, ! #, $, %, &, ', (,), *, +, -, ., =, @, \, ^, _, |

Note:

In the HiCommand programs prior to version 5.5, user IDs consisted of 4 to 25 characters. In an environment where such an earlier version coexists with a HiCommand program version 5.5 or later, set from 4 to 25 characters in the user ID.

5. If necessary, also enter the user's full name, email address, and description.
   - **Full Name** (optional)

     Enter no more than 80 characters, using Basic Latin.

     Basic Latin refers to the following characters:

     Basic Latin (Unicode characters from 0020 to 007E):

     `A-Z a-z 0-9 ! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [ \ ] ^ _ ` { | } ~` (space)

     Note:

     You cannot specify two or more consecutive dollar signs (`$$` or `$$$`, for example).
   - **E-mail** (optional)

     Enter no more than one-byte 255 alphanumeric characters.
   - **Description** (optional) (for example, job title)

     Enter no more than 80 characters, using Basic Latin.
6. Click the **OK** button.

   The window for adding a user account closes. The user account that you added is displayed in the user list in the application area.

3.3.3 Setting Auto Locking for User Accounts

Users who have the User Management permission can set auto locking for user accounts.

If auto locking is set for a user account, the user account is locked automatically after repeated input of an invalid password. When you enable this feature, you can specify the number of unsuccessful login attempts to allow before the user account is locked.

You can also set auto locking for a user account in a `security.conf` file. For details, see section 6.7.

Unsuccessful attempts to log in to other products in the HiCommand that use the Single Sign-On function are counted in the number of unsuccessful login attempts. For example, if the number of unsuccessful attempts is set to `3`, and a user fails to log in to Device Manager once, fails to log in to Provisioning Manager once, and then fails to log in to Tiered Storage Manager once, the user account will be locked automatically.

Changing the number of unsuccessful login attempts does not affect users who have already made unsuccessful attempts or whose account is locked. For example, if you change the number of unsuccessful login attempts from 5 to 2, the account of a user who has already made three unsuccessful attempts will remain active. But if that user fails to log in at the next attempt, his or her account will be locked.

If a third party uses an incorrect password for the account of a user who is already logged in, and the number of unsuccessful login attempts reaches the specified value, the account that is logged in will be automatically locked. If this occurs, the logged-in user can still continue operations until the user logs out. However, the user will be unable to start Tuning Manager from the **Dashboard**.

If an account is automatically locked, the user cannot log in until the account is unlocked. When a user whose account has been locked tries to log in, the normal authentication error will appear and the user will not be notified that his or her account has been locked. Check the **Status** field in the **User List** to see if a user account has been locked. For details about unlocking a locked account, see section 3.3.6.

Note:

The System account is not locked when auto locking is set.

To set auto locking for user accounts:

1. From the **Explorer** menu, choose **Administration**, and then **Security**. Then in the navigation area, click **Account Lock**.

   The Account Lock subwindow appears in the application area. If auto locking is set for user accounts, the maximum number of consecutive unsuccessful login attempts is displayed. If auto locking is not set, **unlimited** appears.

2. To change the auto lock setting, click the **Edit Settings** button.

   A dialog box for setting auto lock appears.

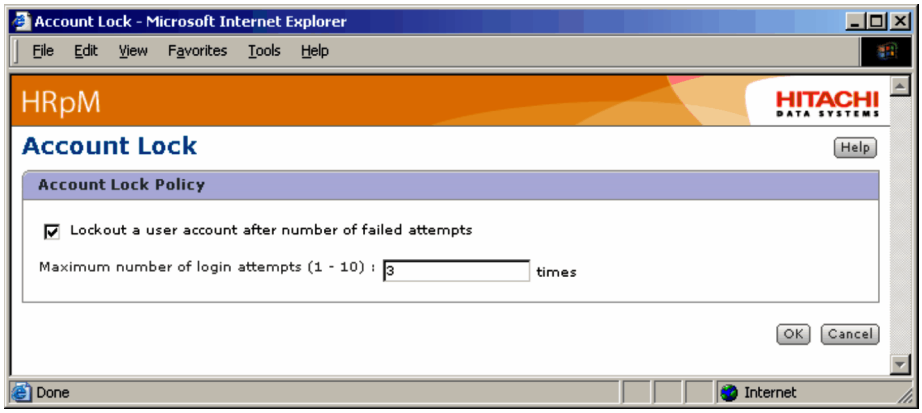

Figure 3.4 Dialog Box for Setting Auto Lock

3. In the Account Lock dialog box, change the auto lock setting for user accounts.

   To enable auto locking, select **Lockout a user account after number of failed attempts** and enter a value in **Maximum number of login attempts**. You can specify a value from 1 to 10.

4. Click the **OK** button to apply the auto lock setting.

   You are returned to the Account Lock subwindow. The auto lock setting for user accounts is changed to the new setting. If you want to cancel the changes of the auto lock setting, click the **Cancel** button.

3.3.4 Setting User Permissions

User permissions for a user registered in Replication Monitor can be set only by a user who has the User Management permission.

To set user permissions:

1. From the **Explorer** menu, choose **Administration** and then **Users and Permissions**.

   An object tree from which you can select **Users** is displayed in the navigation area, and a list of user management items is displayed in the application area.

2. Either choose **Users** in the object tree or click the **Users** in the list.

   A user list is displayed in the application area.

3. Select the user whose user permissions you want to set, by clicking the link in the user list.

   The user account details for the selected user are displayed in the application area.

   Note:

   Instead of performing steps 2 and 3, you can also select a user for which you want to set user permissions by expanding the object tree in the navigation area.

4. Click the **Change Permissions** button.

   A dialog box for changing user permissions is displayed, see Figure 3.5.

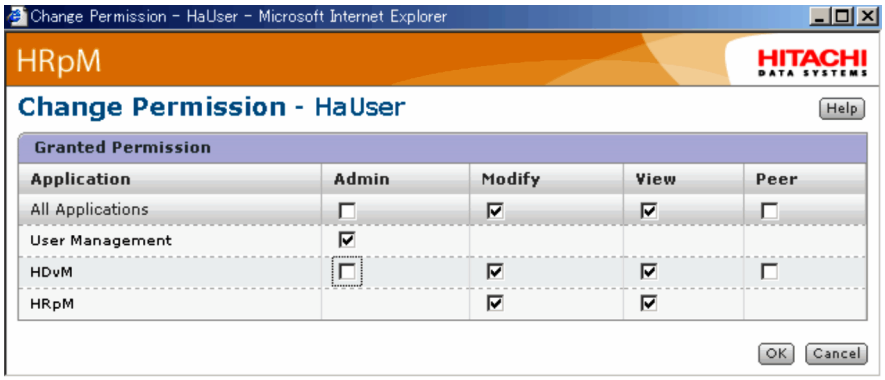

Figure 3.5 Dialog Box for Changing User Permissions

5. Select the checkbox for the combination of permissions you want to set, and then click the **OK** button.

   The dialog box closes, and the permissions you set are displayed in the user account details.

3.3.5 Setting Password Conditions

Users who have the User Management permission can set password conditions.

To prevent user passwords from being guessed by a third party, Replication Monitor allows password conditions (minimum length, combination of characters, and so on) to be specified. You can also set password conditions in the `security.conf` file. For details, see section 6.7.

Password conditions apply when a user account is added or a password is changed. Because password conditions do not apply to passwords for existing user accounts, a user can log in to the system even if the entered password does not satisfy the set conditions.

To set password conditions:

1. From the **Explorer** menu, choose **Administration**, and then **Security**. Then in the navigation area, click **Password**.

   The Password subwindow appears in the application area, displaying the password conditions that have been set.

2. To change the password conditions, click the **Edit Settings** button.

   A dialog box for changing the password conditions appears.

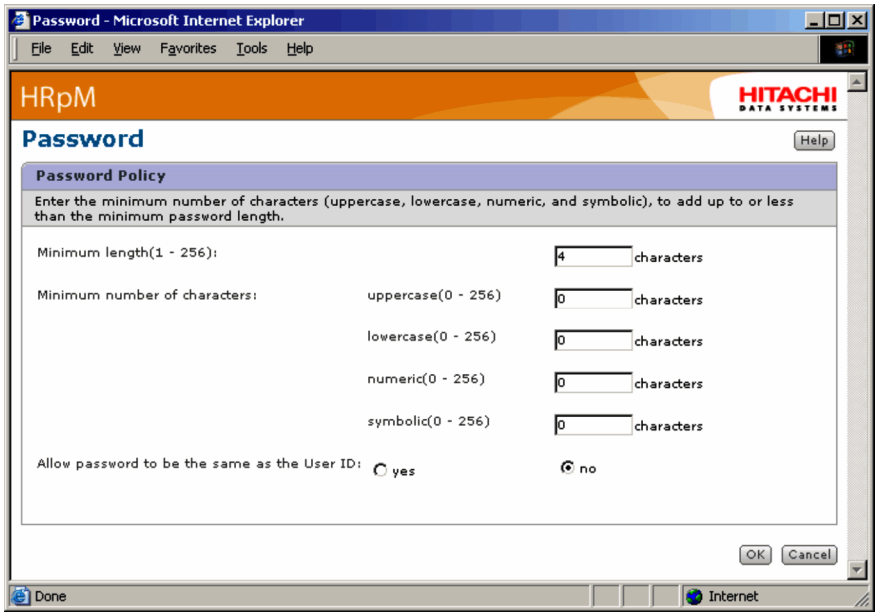

Figure 3.6 Dialog Box for Changing the Password Conditions

3. Enter the following information about the password conditions:
   - **Minimum length**

     Specify the minimum number of characters that can be set as a password. You can enter a value from 1 to 256. The default is 4.
   - **Minimum number of characters**

Specify the minimum number of upper-case characters, lower-case characters, numeric characters, and symbols that must be included in a password. Make sure that you specify the number of characters for each setting so that the total number of characters does not exceed the minimum length.

uppercase: Specify the minimum number of upper-case characters that must be included in a password.

lowercase: Specify the minimum number of lower-case characters that must be included in a password.

numeric: Specify the minimum number of numeric characters that must be included in a password.

symbolic: Specify the minimum number of symbols that must be included in a password.

You can specify a value from 0 to 256 for each setting. The defaults are 0. However, specify the number or characters for each setting so that the total number of characters is 256 or less.

- **Allow password to be the same as the User ID**

  Select **No** to prohibit setting of a password that is the same as the user ID. **Yes** is selected by default.

4. Click the **OK** button to apply the password conditions.

   You are returned to the Password subwindow. The password conditions are changed to the new settings. If you want to cancel the changes of the password conditions, click the **Cancel** button.

3.3.6 Changing the Lock Status of a User Account

Users who have the User Management permission can lock and unlock a selected user account.

A user with a locked account cannot log in to any products in the HiCommand until his or her account is unlocked.

You can also unlock a user account that was locked automatically after a number of unsuccessful login attempts. For details about how to set auto locking for user accounts, see section 3.3.3.

Notes:

- The user account `system` cannot be locked.
- Users with the User Management permission cannot lock their own account.
- If you lock the account of a user who is currently logged in, the user will not be able to continue operations. Before locking a user account, make sure that the target user is not logged in to Replication Monitor.

To change the lock status of a user account:

1. From the **Explorer** menu, choose **Administration**, and then **Users and Permissions**. Then in the navigation area, select **Users**.

   A subwindow for selecting a user appears.

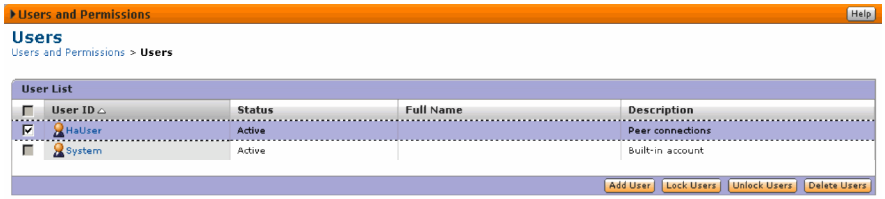

Figure 3.7 Subwindow for selecting a user

2. In **User List**, select the checkbox of the user whose account lock status you want to change, and then click the **Lock Users** button or **Unlock Users** button.

   To change the lock status of all the listed user accounts, select the checkbox in the title bar.

3. A dialog box for confirming the lock status change appears. Click the **OK** button to change the lock status.

   You are returned to the Users subwindow. The **Status** field is updated in the **User List**. If you want to cancel the changes of the lock status, click the **Cancel** button.

3.3.7 Changing a User Password

The user password for a user who is already registered in Replication Monitor can be changed only by a user who has the User Management permission.

Note:

A user can change his or her own password in the User Profile window, which is displayed by choosing **Settings** and then **User Profile** from the **Explorer** menu. To change your own password, you must first enter your current password.

Note: You can change the password of a user who is currently logged in. Although the user whose password has been changed can still operate the Replication Monitor, the user will be unable to start the Tuning Manager from the **Dashboard** until the user logs in again with the newly changed password.

To change a user password:

1. From the **Explorer** menu, choose **Administration** and then **Users and Permissions**.

   An object tree from which you can select **Users** is displayed in the navigation area, and a list of user management items is displayed in the application area.

2. Either choose **Users** in the object tree or click the **Users** in the list.

   A user list is displayed in the application area.

3. Select the user whose password you want to change, by clicking the link in the user list.

   The user account details for the selected user are displayed in the application area.

Note:

Instead of performing steps 2 and 3, you can also select a user of which you want to change the password by expanding the object tree in the navigation area.

4. Click the **Change Password** button.

   A dialog box for changing the password is displayed, see Figure 3.8.

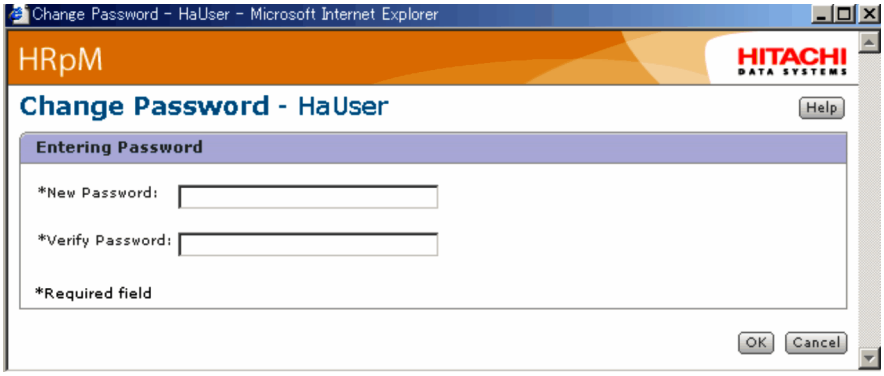

Figure 3.8 Dialog Box for Changing a Password

5. Enter the new password, and click the **OK** button.

   A dialog box indicating that the change has been accepted is displayed.

   Notes:

   – Passwords are case sensitive and must be entered by following the rule set by the user administrator. You can use the following characters:

     `0-9 a-z A-Z ! # $ % & ' ( ) * + - . = @ \ ^ _ |`

     Conditions may apply to the minimum length or combination of characters that can be set as a password. Passwords that do not meet these conditions cannot be specified. For information on the conditions set for passwords, contact your user administrator.

   – In HiCommand products prior to version 5.5, passwords consisted of 4 to 25 characters. In an environment where a HiCommand product earlier then version 5.5 coexists with a HiCommand Suite product version 5.5 or later, set from 4 to 25 characters in a password.

6. Click the **Close** button.

   The dialog box closes.

3.3.8 Deleting a User Account

To delete a registered user from Replication Monitor, you must delete that user's user account. This operation can be performed only by a user who has the User Management permission.

Note:

You cannot delete the account of the user whose name is `System`.

You can delete a user account when the application area display is in one of the following states:

- The user account details for the user who is to be deleted are displayed
- The user list is displayed

To delete a user account when the user account details of the user to be deleted are displayed:

1. Click the **Delete User** button.

   A dialog box requesting confirmation that you want to delete the indicated user's user account is displayed, see Figure 3.9.

2. Click the **OK** button.

   The dialog box closes, and the user list in the application area is displayed with the user account deleted.

To delete user accounts when the user list is displayed:

3. Select the checkboxes of the user accounts you wish to delete, and click the **Delete Users** button.

   A dialog box containing a list of the users to be deleted is displayed, and a message requests confirmation that you want to delete the user accounts in the list.

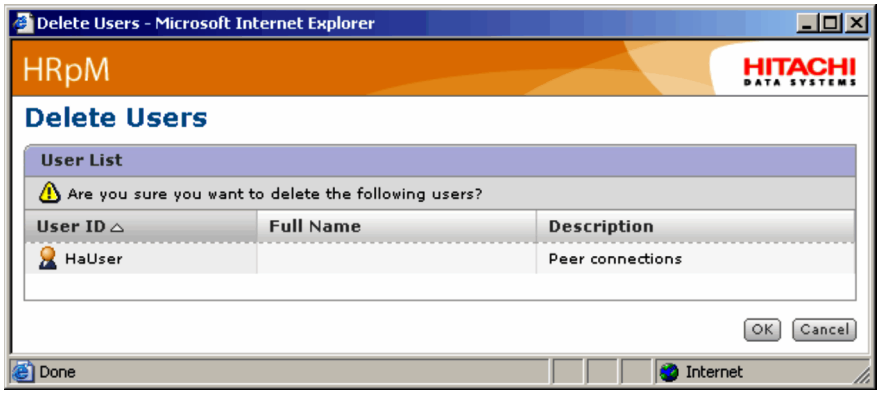

Figure 3.9 Dialog Box for Confirming Accounts To Be Deleted

4. Click the **OK** button.

   The dialog box closes, and the user list in the application area is displayed with the user accounts deleted.

3.3.9 Setting a Warning Banner Message

Users who have the User Management permission can set a warning banner message.

In Replication Monitor, a message can be displayed in the Login window as a security measure when a user logs in.

You can set a warning banner message by using the `hcmdsbanner` command. There are no restrictions on the HTML tags you can use. You can set a different message for each locale. For details on setting a warning banner message by using the `hcmdsbanner` command, see section 6.8.

Note:

In Web Client, you can only edit the message displayed as the default warning banner. You cannot edit a message set by using the `hcmdsbanner` command if the message contains any HTML tags that are not supported in Web Client. If you specify the locale option by using the `hcmdsbanner` command, you cannot edit messages in Web Client.

To edit the warning banner message:

1. From the **Explorer** menu, choose **Administration**, and then **Security**. Then in the navigation area, click **Warning Banner**.

   The Warning Banner subwindow appears in the application area, displaying the set message. If no message is set, `No Message` appears in the subwindow.

2. To edit the message, click the **Edit Message** button.

   The Edit Message dialog box appears.

3. In the **Message** text box, change the displayed message. If you want to delete the message, click the **Delete** button.

   Edit the message in HTML format. You can use a maximum of 1,000 characters, including HTML tags. When editing the message in Web Client, you can use the following HTML tags:

   ```
   <b> </b> <i> </i> <center> </center> <br>
   <div dir="ltr"> <div dir="rtl"> <div style="direction:rtl">
   <div style="direction:ltr"> </div>
   ```

   HTML tags are not case sensitive.

   Notes:

   - To display characters used in HTML tags as ordinary characters in the message, use HTML escape sequences.
   - You can enter line breaks at any position in the message, using the HTML tag `<br>`. Line breaks entered when editing a message are ignored when the message is registered.

4. Click the **Preview** button to check the edited message.

   If you edited the message correctly, it will appear in HTML form in the **Preview** field. If you used any unsupported tags or if there is a problem with the HTML syntax, an error message appears and the **Preview** field is blank.

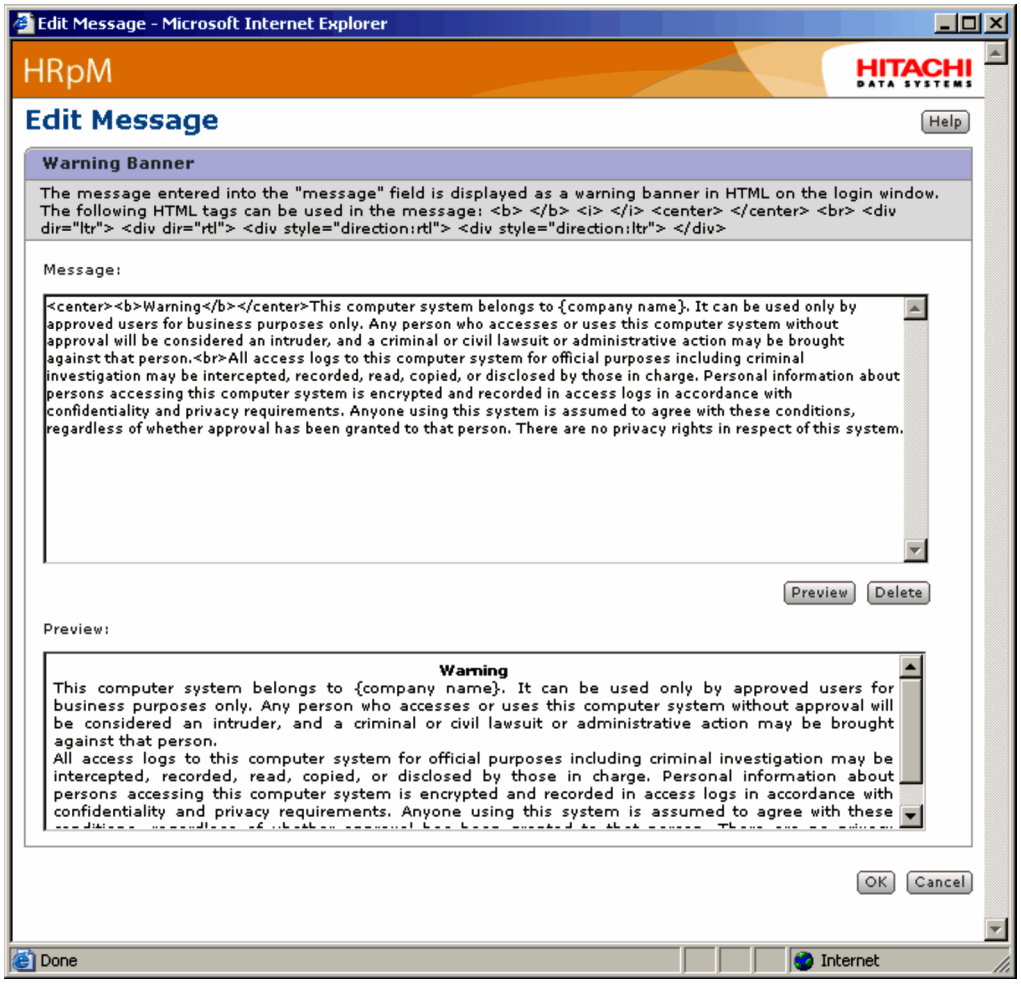

Figure 3.10 Correctly Edited Banner Message

5. After checking that the message displays correctly, click the **OK** button to save the new message. If you want to cancel the editing, click the **Cancel** button.

To edit the warning banner message in a cluster environment, switch between the executing node and the standby node as appropriate, and edit the warning banner message for each node.

3.4 Registering an Information Source

A database that is used as an original source of information for Replication Monitor is called an *information source*; examples of information sources include Device Manager servers and Business Continuity Managers. This section explains how to register information sources.

Note:

You do not need to use this procedure to register as an information source the management server (Device Manager server) that is located where the Replication Monitor you are configuring is installed. This Device Manager server is registered automatically when you install Replication Monitor and is displayed as the local server on the list of information sources.

The original sources of information that can be used by Replication Monitor to collect information on hosts, storage subsystems, volume pairs, and other devices depend on whether the host is an open system or a mainframe system.

For an open system, Device Manager servers and pair management servers and hosts managed by the Device Manager servers constitute the original sources of information. Information indicating the volume pair status is collected principally through Replication Monitor agents installed on the pair management servers.

For a mainframe system, Business Continuity Managers constitute the original sources of information.

When you register an information source into the system, you must specify the following information about the Device Manager server or Business Continuity Manager:

- Name (nickname) of the Device Manager server or Business Continuity Manager
- IP address or host name
- Port number

When the information source to be registered is a Device Manager server, you must also specify the following information:

- Protocol used for communication with Replication Monitor
- User ID for connecting to the Device Manager server
- Password for connecting to the Device Manager server

During information source registration, you can also specify that configuration information is not to be collected from an information source. The default setting is that configuration information is collected and the collected information is stored in the database maintained by Replication Monitor.

You can also change any of the above information after you have registered an information source. When you change the settings on the information source side, you must also change the settings of the information source on Replication Monitor accordingly. When you change the IP address (or host name), protocol, or port number, in addition to the processing performed to change this information, processing to collect configuration information from the information source is also performed.

3.4.1 Registering a Device Manager Server as an Information Source

This section explains the procedure for registering a Device Manager server as an information source. It also explains the procedure for changing the information associated with an information source after the information source has been registered.

To register a Device Manager server as an information source:

1. From the **Explorer** menu, choose **Settings** and then **Information Source**.

   An object tree from which you can select an information source is displayed in the navigation area, and an information source list is displayed in the application area, see Figure 3.11.

2. Choose **Device Manager** from the object tree or from the list.

   A list of registered Device Manager servers is displayed in the application area.

3. Click the **Add HDvM** button.

   A dialog box for adding a Device Manager server is displayed.

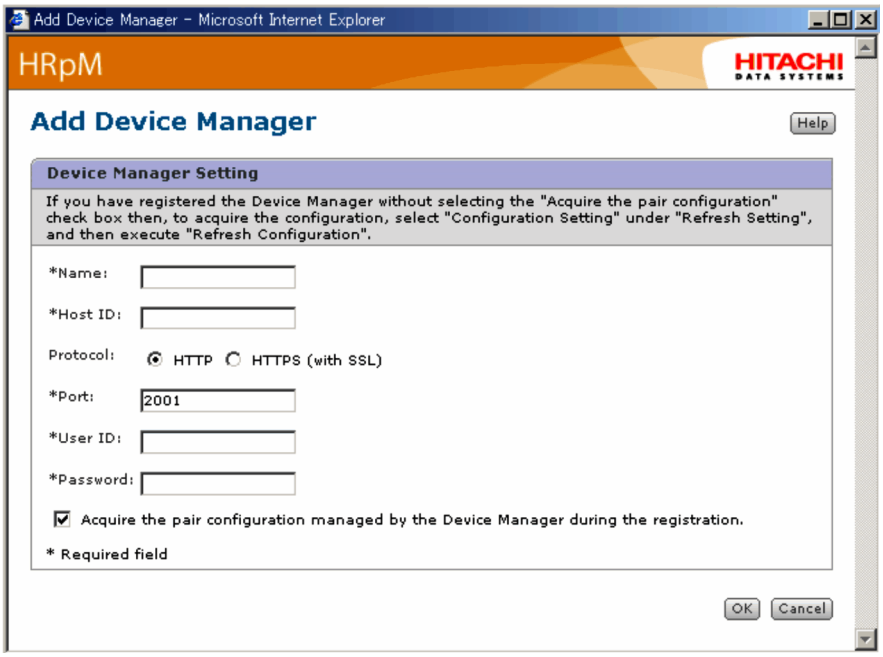

Figure 3.11 Dialog Box for Adding a Device Manager Server

4. Enter the name (nickname) and the IP address or host name (Host ID) of the Device Manager server.

5. To change the default values that are displayed for the protocol and port number, select the appropriate radio button for the protocol, or enter the desired value for the port number.

   Note:

   The port number entered in this step is specified for `server.http.port` of the `server.properties` file of the Device Manager server.

6. Enter the user ID and password for connecting to the Device Manager server.

   Note:

   The user account of the user whose user ID and password are specified here must include the Device Manager Modify permission and **All Resources** must be assigned to the resource group. This user ID and password are used by Replication Monitor to access Device Manager for viewing and setting Device Manager-related parameters.

7. To suppress collection of configuration information from the Device Manager server, clear the **Acquire the pair configuration managed by the Device Manager during the registration** checkbox.

   Note:

   When you register multiple information sources, you can collect all the configuration information from them together after the registration if you register them with the **Acquire the pair configuration managed by the Device Manager during the registration** checkbox cleared. For details about how to collect all the configuration information from multiple information sources at once, see section 3.7.

8. Click the **OK** button.

   A dialog box requesting that you confirm the information specified for adding the Device Manager server is displayed.

9. Select the checkbox that indicates confirmation of the specified information, and then click the **Confirm** button.

   A dialog box that shows the progress of adding the Device Manager server is displayed. Once the processing is complete, a dialog box indicating that the Device Manager server addition processing has been completed is displayed.

   Note:

   If you leave the **Acquire the pair configuration managed by the Device Manager during the registration** checkbox selected, the processing to collect the configuration information from the Device Manager server will also be performed.

10. Click the **Close** button.

    The dialog box indicating completion of Device Manager server addition processing closes.

To change the information for a registered information source:

1. From the **Explorer** menu, choose **Settings** and then **Information Source**.

   An object tree from which you can select an information source is displayed in the navigation area, and an information source list is displayed in the application area.

2. Choose **Device Manager** from the object tree or from the list.

   A list of registered Device Manager servers is displayed in the application area.

3. Click the icon to the left of the name of the Device Manager whose information you wish to change.

   A dialog box for changing the information registered in the Device Manager server is displayed. Enter the new information in this dialog box. The remainder of this procedure is the same as for registering an information source, except that you cannot specify whether to collect configuration information from the Device Manager server.

   Note:

   If you change the IP address or host name (Host ID) of the Device Manager server, or if you change the protocol or port number, the processing to collect the configuration information from the Device Manager server will also be performed.

3.4.2 Registering a Business Continuity Manager as an Information Source

This section explains the procedure for registering a Business Continuity Manager as an information source. It also explains the procedure for changing the information associated with an information source after the information source has been registered.

To register a Business Continuity Manager as an information source:

1. From the **Explorer** menu, choose **Settings** and then **Information Source**.

   An object tree from which you can select an information source is displayed in the navigation area, and an information source list is displayed in the application area, see Figure 3.12.

2. Choose **Business Continuity Manager** from the object tree or from the list.

   A list of registered Business Continuity Managers is displayed in the application area.

3. Click the **Add BCM** button.

   A dialog box for adding a Business Continuity Manager is displayed.

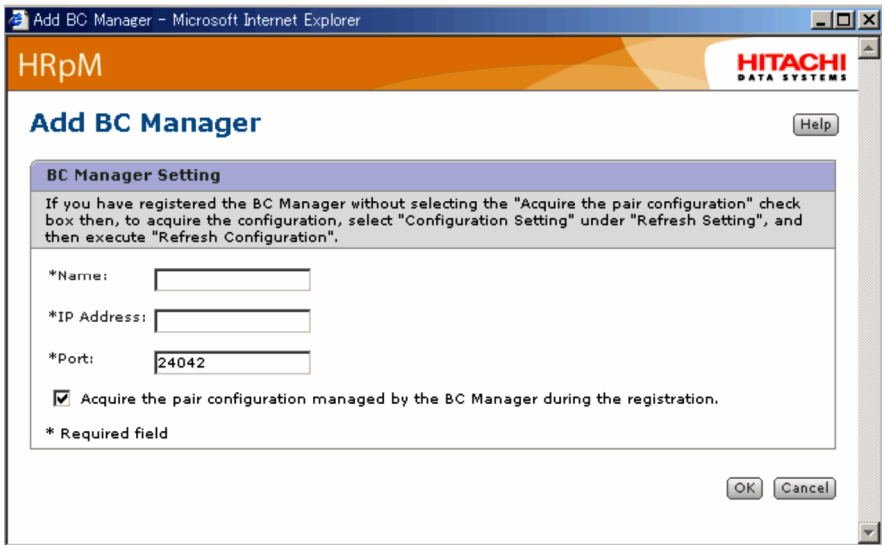

Figure 3.12 Dialog Box for Adding a Business Continuity Manager

4. Enter the name (nickname) and IP address of the Business Continuity Manager.
5. To change the default value displayed for the port number, enter the desired value for the port number.
6. To suppress collection of configuration information from the Business Continuity Manager, clear the **Acquire the pair configuration managed by the BC Manager during the registration** checkbox.

   Note:

   When you register multiple information sources, you can collect all the configuration information from them together after the registration if you register them with the **Acquire the pair configuration managed by the BC Manager during the registration** checkbox cleared. For details about how to collect all the configuration information from multiple information sources at once, see section 3.7.
7. Click the **OK** button.

   A dialog box requesting that you confirm the information specified for adding the Business Continuity Manager is displayed.
8. Select the checkbox that indicates confirmation of the specified information, and click the **Confirm** button.

   A dialog box that shows the progress of adding the Business Continuity Manager is displayed. Once the processing is complete, a dialog box indicating that the Business Continuity Manager addition processing has been completed is displayed.

   Note:

   If you leave the **Acquire the pair configuration managed by the BC Manager during the registration** checkbox selected, the processing to collect the configuration information from the Business Continuity Manager will also be performed.
9. Click the **Close** button.

   The dialog box indicating completion of Business Continuity Manager addition processing closes.

To change the information for a registered information source:

1 From the **Explorer** menu, choose **Settings** and then **Information Source**.

An object tree from which you can select an information source is displayed in the navigation area, and an information source list is displayed in the application area.

2 Choose **Business Continuity Manager** from the object tree or from the list.

A list of registered Business Continuity Managers is displayed in the application area.

3 Click the icon to the left of the name of the Business Continuity Manager whose information you wish to change.

A dialog box for changing the information registered to the Business Continuity Manager is displayed. Enter the new information in this dialog box. The remainder of this procedure is the same as for registering an information source, except that you cannot specify whether to collect configuration information from the Business Continuity Manager.

Note:

If you change the IP address or port number of the Business Continuity Manager, the processing to collect the configuration information from the Business Continuity Manager will also be performed

3.4.3 Setting a Link to an Information Source (Device Manager) Using Hcmdslink

To configure the system so that you can call an information source (a Device Manager server) from the Web Client, you must set a link to the information source (URL of the information source server) in the dialog box that is displayed when you choose **Go** and then **Links** from the global tasks bar area. You can use the `hcmdslink` command to set up this link.

The following shows an example of using the `hcmdslink` command when the managed server is running a Windows OS:

```
hcmdslink /add /file C:\SampleLink.txt /user system /pass manager
```

With the `add` option specified in the `hcmdslink` command, the link target is specified in the `file` option. The `file` option is used to specify a text file that contains settings, such as the name of the link destination program, its URL, and the name to display in the dialog box.

In the following example, the name of this text file is `SampleLink.txt`.

The following shows an example of the text file's contents:

```
@TOOL-LINK
@NAME SampleApp
@URL http://SampleApp/index.html
@DISPLAYNAME SampleApplication
@DISPLAYORDER 10
@ICONURL http://SampleApp/graphic/icon.gif
@TOOL-END
```

This example specifies that the link destination program is displayed with the name `SampleApplication` in the dialog box, and that an icon with the image name provided by `@ICONURL` is to be set next to the link.

For details about the `hcmdslink` command, see the *HiCommand Device Manager Server Installation and Configuration Guide*.

3.5 Setting Up the Refresh Function

To *refresh* means to update to the latest status the information in the database maintained by Replication Monitor. The database stores copy pair configuration information and information related to copy pair status that is obtained from Device Manager servers, Business Continuity Managers, and agents. The process of obtaining information from an information source or agent is called *information collection*.

You can set the refresh function so that refreshing is performed automatically at a set interval or manually by the user. If you use automatic refreshing, you must also specify the information collection interval.

- Collecting configuration information

  You can set the collection interval and the collection start time for each information source.

- Collecting information related to copy pair status

  You can set the collection interval.

  For Device Manager servers, you can set a collection interval for each pair management server and each information source.

  For Business Continuity Managers, you can set a collection interval for each information source.

The following table shows the units that can be used to set the collection interval for information related to copy pair status and the relationship to the copy pairs that are targeted.

Table 3.2 Setting Units for Information Collection Interval and Targeted Copy Pairs

Information Source	Setting Unit	Original Source of Information	Targeted Copy Pairs
Device Manager server	Pair management server	Agent#2	Copy pairs managed by the pair management server
	Information source#1	Agent#2	
		Device Manager server#3	All copy pairs in the storage subsystems managed by the Device Manager server
Business Continuity Manager	Information source	Business Continuity Manager	Copy pairs managed by the information source

#1

The same settings are used for all copy pairs of the information source.

#2

The existing settings for each pair management server are overwritten by each information source. If you need the settings of a particular pair management server, specify the pair management server settings after you specify the settings for each information source.

#3

You can configure the system so that a Device Manager refresh is not performed when you perform a manual refresh.

Figure 3.13 shows an example of collection interval settings for collecting information related to copy pair status when the information source is a Device Manager server. In this figure the pair management server A and B are managed by the management server 1, and the pair management server C is managed by the management server 2.

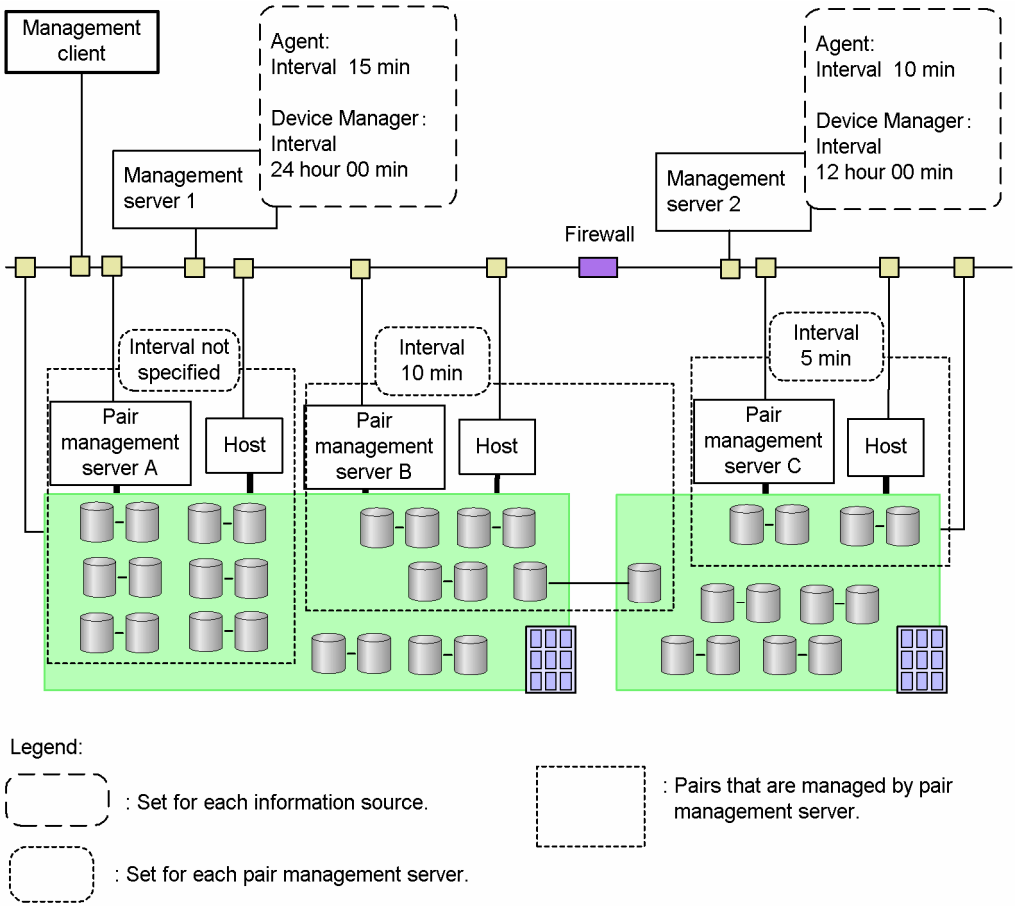

Figure 3.13 Collection Interval Settings for Collecting Information Related to Copy Pair Status

Assuming that the collection interval for information related to copy pair status is set as shown in this figure, and assuming that the information collection interval is set in order of 1) each information source, and 2) each pair management server, the information collection intervals for the copy pairs managed by each pair management server are 15, 10, and 5 minutes each for pair management servers A, B, and C, respectively.

3.5.1 Setting the Interval for Collecting Configuration Information

To set the interval for collecting configuration information from an information source:

1. From the **Explorer** menu, choose **Settings** and then **Refresh Setting**.

2. From the object tree or subwindow, choose **Configuration Setting**.

   In the application area, a list of information sources is displayed, consisting of columns containing **Interval**, **Start Time**, and **Last Refresh** settings associated with collection of configuration information.

3. From the list of information sources, click the icon of the information source whose information collection interval you wish to set.

   A dialog box for setting the collection interval and start time for the selected information source is displayed, see Figure 3.14.

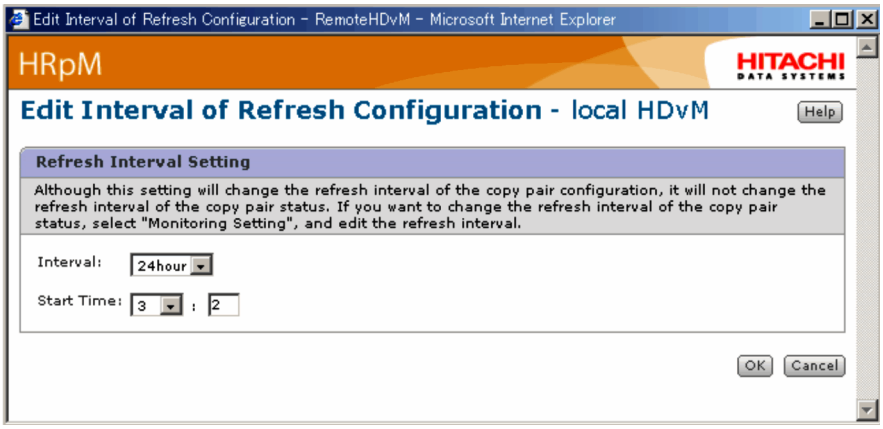

Figure 3.14 Dialog Box for Setting the Collection Interval and Start Time

4. Choose the collection interval from the **Interval** drop-down list.
5. Choose the collection start time hour from the **Start Time** drop-down list, and then enter the collection start time minute (0-59).
6. Click the **OK** button.

   The dialog box for setting the collection interval and start time closes.

3.5.2 Collecting Copy Pair Status Information for an Information Source

This section explains two procedures for setting the interval for collecting copy pair status information for an information source: the procedure for a Device Manager server and the procedure for a Business Continuity Manager.

To set the interval for collecting copy pair status information for a Device Manager server:

1. From the **Explorer** menu, choose **Settings** and then **Refresh Setting**.
2. From the object tree or subwindow, choose **Monitoring Setting.**

   In the application area, a list of information sources is displayed, consisting of columns containing **Periodical Interval** and **Manual Refresh** settings associated with collection of copy pair status information.

3. From the list of information sources, click the icon of a Device Manager server.

A dialog box for setting the copy pair status information collection interval for the selected information source is displayed, see Figure 3.15.

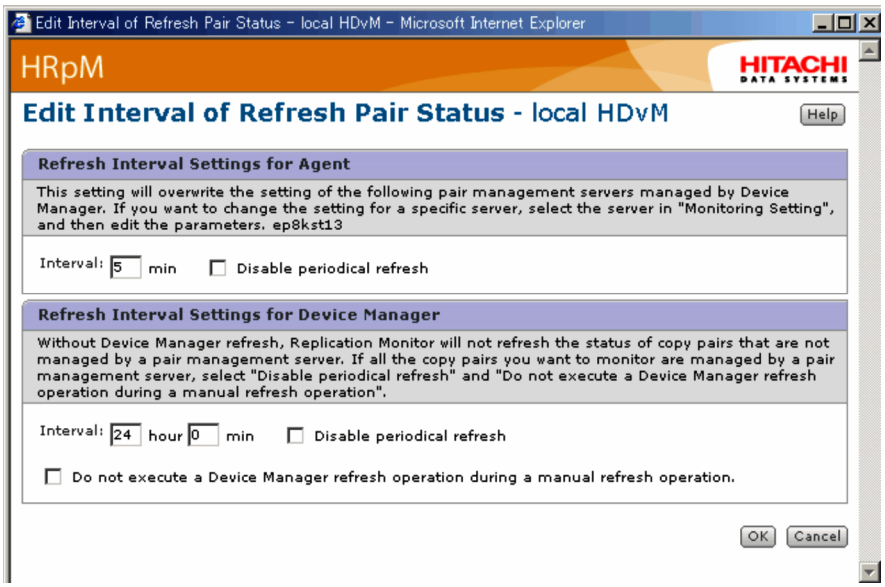

Figure 3.15 Dialog Box for Setting Copy Pair Status Monitoring (Device Manager Server)

4. If you do not want copy pair status information to be collected automatically from the agent, select the **Disable periodical refresh** checkbox under **Refresh Interval Settings for Agent**.

   If you select this checkbox, **Interval** becomes inactive, so skip to step 6.

5. Enter the number of minutes for the collection interval in **Interval** under **Refresh Interval Settings for Agent**.

   Note:

   The collection interval you set here overwrites the value set for each host (pair management server).

6. If you do not want copy pair status information to be collected automatically from the Device Manager server, select the **Disable periodical refresh** checkbox under **Refresh Interval Settings for Device Manager**.

   If you select this checkbox, **Interval** becomes inactive, so skip to step 8.

   Note:

   If all the copy pairs you want to monitor are managed under a pair management server, specify this setting so that copy pair status information is not collected automatically from the Device Manager server.

7. Enter a collection interval hour and minute in **Interval** under **Refresh Interval Settings for Device Manager**.

8. If you do not want a Device Manager refresh to occur when you collect copy pair status information manually, select the **Do not execute a Device Manager refresh operation during a manual refresh operation** checkbox.

   Note:

If all the copy pairs you want to monitor are managed under a pair management server, specify this setting so that a Device Manager server refresh operation does not occur.

9. Click the **OK** button.

   The dialog box for setting the copy pair status information collection interval closes.

To set the interval for collecting copy pair status information for a Business Continuity Manager:

1. From the **Explorer** menu, choose **Settings** and then **Refresh Setting**.
2. From the object tree or subwindow, choose **Monitoring Setting**.

   In the application area, a list of information sources is displayed, consisting of columns containing **Periodical Interval** and **Manual Refresh** settings associated with collection of copy pair status information.

3. From the list of information sources, click the icon of a Business Continuity Manager.

   A dialog box for setting the copy pair status information collection interval for the selected information source is displayed, see Figure 3.16.

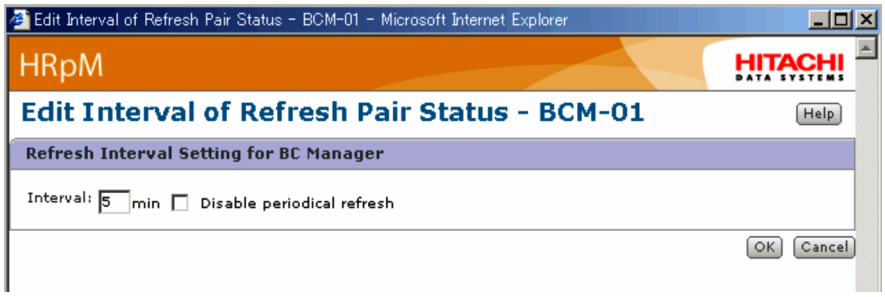

Figure 3.16 Dialog Box for Setting Copy Pair Status Monitoring (Business Continuity Manager)

4. If you do not want copy pair status information to be collected automatically, select the **Disable periodical refresh** checkbox.

   If you select this checkbox, **Interval** becomes inactive, so skip to step 6.

5. Enter the number of minutes for the collection interval in **Interval**.
6. Click the **OK** button.

   The dialog box for setting the copy pair status information collection interval closes.

3.5.3 Collecting Copy Pair Status for a Pair Management Server (Open Systems Only)

To set the copy pair status information collection interval for a pair management server:

1. From the **Explore** menu, choose **Settings** and then **Refresh Setting**.
2. From the object tree or subwindow, choose **Monitoring Setting**.

In the application area, a list of information sources is displayed, consisting of columns containing **Periodical Interval** and **Manual Refresh** settings associated with collection of copy pair status information.

3. From the object tree or subwindow (list of information sources), choose a Device Manager server.

   In the application area, a list of hosts (pair management servers) managed under the selected Device Manager server is displayed.

4. Click an icon to select a host (pair management server).

   A dialog box for setting copy pair status monitoring for the selected host (pair management server) is displayed, see Figure 3.17.

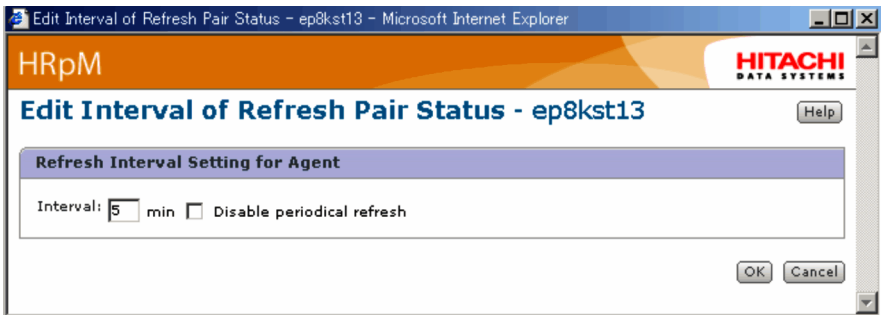

Figure 3.17 Dialog Box for Setting Copy Pair Status Monitoring

5. If you do not want copy pair status information to be collected automatically, select the **Disable periodical refresh** checkbox.

   If you select this checkbox, **Interval** becomes inactive, so skip to step 7.

6. Enter the number of minutes for the collection interval in **Interval**.

7. Click the **OK** button.

   The dialog box for setting the copy pair status information collection interval closes.

3.6 Setting Up Data Retention

You can specify settings for saving the following six types of data:

- Alert history
- Write delay time data (C/T delta) for open systems
- Write delay time data (C/T delta) for mainframe systems
- Event log
- Side file and journal volume usage for open systems
- Side file and journal volume usage for mainframe systems

You can specify separately whether to save data of each data type.

If you decide to save a type of data, you can set the following items:

- Retention period (number of days the data is to be retained)
- Start time for deleting data whose retention period has elapsed (time at which data deletion is to start each day)

Note:

If the total number of the history data retained by Replication Monitor exceeds 26,000,000, some of the old data might be deleted even if the retention period for the data has not expired. The total number of the history data is equal to the total number of the history data for the issued alerts, event logs, and performance information (side file usage, journal volume usage, and C/T delta). In this case, take action by using either of the following methods:

- Disable the retention of unnecessary data, or shorten the retention period.
- Increase the interval at which information is acquired by refreshing.

To specify the settings for saving data:

1. From the **Explorer** menu, choose **Settings** and then **Data Retention**.

   In the application area, a list of data types for which you can specify a data retention period is displayed. Repeat steps 2 - 7 below for each data type.

2. Click an icon to select a data type.

   A dialog box for setting a data retention period for the selected data type is displayed, see Figure 3.18.

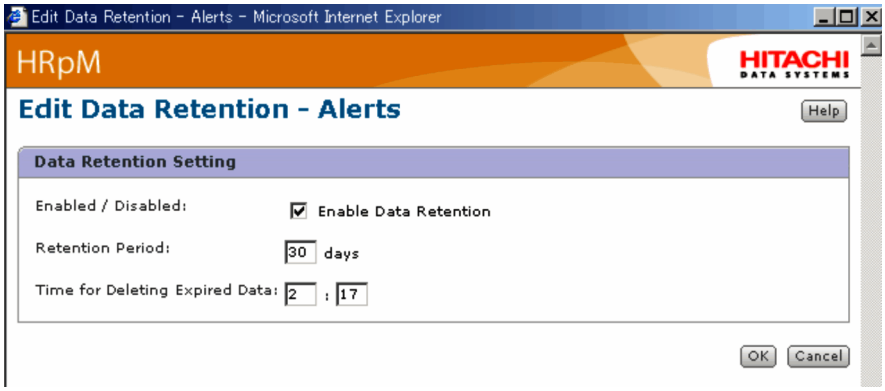

Figure 3.18 Dialog Box for Setting the Data Retention Period

3. To enable data saving, make sure that the **Enable Data Retention** checkbox of **Enabled / Disabled** is selected.
4. To disable data saving, clear the **Enable Data Retention** checkbox of **Enabled / Disabled**.

   If you cleared the **Enable Data Retention** checkbox, skip to step 7.
5. In **Retention Period**, enter the period (number of days) for which the data is to be saved.
6. In **Time for Deleting Expired Data**, enter the daily start time for deleting data whose retention period has elapsed.
7. Click the **OK** button.

   The settings for data saving are registered, and the dialog box closes.

3.7 Acquiring the Most Recent Configuration Information

To update the results of the initial settings to the database maintained by the Replication Monitor server, you must collect the latest configuration information. You can collect configuration information by selecting an information source.

Note:

You do not need to acquire the recent configuration information again, because the information is already acquired if you selected the check box in the dialog to retrieve configuration information of copy pairs managed by information sources (Device Manager or Business Continuity Manager) during the registration when you registered the information source.

You can set up Replication Monitor to automatically synchronize with the Device Manager server database when the Device Manager server database is updated. For details, see the description in section 6.10.6.

To collect the latest configuration information:

1. From the **Explorer** menu, choose **Settings** and then **Refresh Setting**.
2. From the object tree or subwindow, choose **Configuration Setting**.

   In the application area, a list of information sources is displayed, consisting of columns containing **Interval**, **Start Time**, and **Last Refresh** settings associated with collection of configuration information, see Figure 3.19.

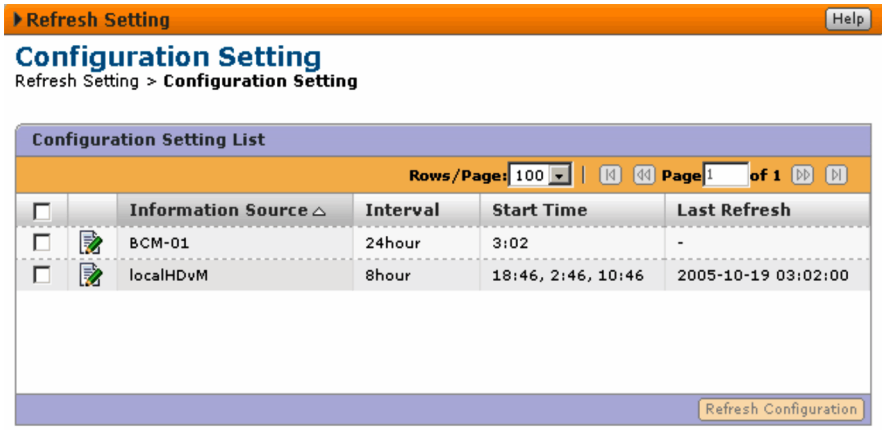

Figure 3.19 List of Information Sources

3. Select a checkbox to choose an information source from which to collect configuration information.

   The **Refresh Configuration** button becomes active when an information source is selected.

4. Click the **Refresh Configuration** button.

   A dialog box requesting that you confirm that configuration information is to be collected is displayed.

5. To collect the information, select the **Yes. I have confirmed the above information and wish to refresh configuration** checkbox, and click the **Confirm** button.

   Information collection processing begins, and a dialog box that shows the progress of collecting the information is displayed. Once processing has been completed, a dialog box indicating that processing has ended is displayed.

6. Click the **Close** button.

   The dialog box closes. The list of information sources in the application area is updated, and the update time is displayed in the **Last Refresh** column of the information source whose configuration information was collected.

3.8 Backing Up Operating Environment Information

This section explains how to back up operating environment information of Replication Monitor (database and property file), and how to restore databases.

3.8.1 Backing Up Databases and Property files

To back up operating Replication Monitor environment information (database and property file), execute the `hcmdsbackups` command of HiCommand Suite Common Component.

The `hcmdsbackups` command is stored in the directories shown below:

In Windows:

```
HiCommand-Suite-Common-Component-installation-folder\bin\
```

In Solaris:

```
/opt/HiCommand/Base/bin/
```

Note:

Back up the operating Replication Monitor environment information while the embedded database HiRDB is running. For details about how to check if HiRDB is running, see section 6.3.1.

3.8.1.1 Backup Command Formats

In Windows:

```
hcmdsbackups /dir backup-directory-name
```

In Solaris:

```
hcmdsbackups -dir backup-directory-name
```

3.8.1.2 Backup Command Description

Targets the data of HiCommand products on the same management server for backup.

3.8.1.3 Backup Command Arguments

`dir` *backup-directory-name*

Specify, using an absolute path, the name of the directory where the backup data is to be stored. Note that in Solaris, a directory that includes a space character cannot be specified. If the specified directory does not exist, it is created. If the specified directory is not empty, an error message is output and backup stops.

In the specified directory, a directory that has the name of the backed up HiCommand products and `database` directory are created. The directory that has the name of the backed up HiCommand products stores data on a product basis and the `database` directory stores databases of HiCommand products containing HiCommand Suite Common Component.

You can specify characters other than ASCII code characters (from 0x20 to 0x7E) and some symbols (`\ / : , ; * ? " < > | $ % & ' ` `). Also, the following characters can be specified as delimiter characters:

In Windows:

`\ / :`

In Solaris:

`/`

3.8.1.4 Command Return Values

`0`: Normal termination

`1`: Error in the arguments

`2`: Termination with an error

3.8.1.5 About the Backup Command(s)

- To execute this command, the following user must be logged in to the system:

  In Windows:

  An administrator group user

  In Solaris:

  A root user

- From the operating environment information for Replication Monitor, property files are stored as follows:

  In Windows:

  directory-specified-in-/dir-option`\ReplicationMonitor`

  In Solaris:

  directory-specified-in--dir-option`/ReplicationMonitor`

- The database of HiCommand Suite Common Component is always backed up. The backup files for the databases of the HiCommand products containing HiCommand Suite Common Component are stored in the following location and the following file names are assigned:

  In Windows:

  directory-specified-by-/dir-option`\database\backup.hdb`

  In Solaris:

  directory-specified-by--dir-option`/database/backup.hdb`

- Do not execute multiple instances of this command at the same time.

3.8.1.6 Execution Examples

In the following example, the command backs up data of all installed HiCommand products:

```
>hcmdsbackups /dir C:\Backups
```

3.8.2 Restoring Databases

To restore the Replication Monitor server database, execute the `hcmdsdb` command of HiCommand Suite Common Component.

- To execute this command, the following user must be logged in to the system:

  In Windows:

  An administrator group user

  In Solaris:

  A root user

- Do not execute multiple instances of this command at the same time.

The `hcmdsdb` command is stored in the directories shown below:

In Windows:

```
HiCommand-Suite-Common-Component-installation-folder\bin\
```

In Solaris:

```
/opt/HiCommand/Base/bin/
```

Note:

Execute restoration after terminating services of HiCommand Suite Common Component and services of other HiCommand products.

3.8.2.1 Restoring Database Command Formats

In Windows:

```
hcmdsdb /restore backup-file-name
        /type HiCommand-product-name
```

In Solaris:

```
hcmdsdb -restore backup-file-name
        -type HiCommand-product-name
```

3.8.2.2 Restoring Command Description

For HiCommand products on the same management server, the databases are restored from the backup data.

3.8.2.3 Restoring Command Arguments

`restore` *backup-file-name*

Specify the absolute path of the backup file for the target HiCommand product database.

When the `hcmdsbackups` command is executed, specify the absolute path of the backup file (`backup.hdb`) for the database stored in the `database` directory under the directory (specified in the `dir` option).

`type` *HiCommand-product-name*

Specify the name of the HiCommand product to be restored. The database areas of the specified HiCommand product are recovered.

If `ALL` is specified for a HiCommand product name, data of all HiCommand products on the same management server will be restored.

To restore the Replication Monitor server database, specify `ReplicationMonitor` for the HiCommand product name.

3.8.2.4 Return Values

`0`: Normal termination

`255`: Termination with an error

3.8.2.5 Execution Examples

In the following example, the command restores the Replication Monitor server database:

```
>hcmdsdb /restore C:\Backups\database\backup.hdb /type ReplicationMonitor
```

In the following example, the command restores the database of all installed HiCommand products:

```
>hcmdsdb /restore C:\Backups\database\backup.hdb /type ALL
```

3.8.2.6 Database Backup Notes

When using the `hcmdsbackups` command to back up the database, all databases of HiCommand products are backed up. However, when using the `hcmdsdb` command and specifying `ReplicationMonitor` in the `type` option to restore the database, only the Replication Monitor server database is restored. The databases of other HiCommand products containing HiCommand Suite Common Component are not restored. Therefore, inconsistency between the HiCommand Suite Common Component database and the Replication Monitor server database might occur and Replication Monitor might not operate correctly.

Therefore, if you specify `ReplicationMonitor` in the `type` option and restore the database, use the **Refresh Configuration** button in the Configuration Setting subwindow to collect the latest configuration before you resume using Replication Monitor. For details about the **Refresh Configuration** button, see section 3.7.

If restoration is performed with `ALL` specified, all the databases of HiCommand products at the time backup was performed are restored. Therefore, information about HiCommand products installed after backup was performed is deleted. If you change the HiCommand product configuration on the same management server, always obtain a backup.

Chapter 4 Changing the Configuration of Replication Monitor

This chapter describes the procedures for adding information sources to and deleting information sources from the system, which you must do when the system configuration changes. The chapter also explains the task flows for these procedures.

- Adding an Information Source (see section 4.1)
- Deleting an Information Source (see section 4.2)

4.1 Adding an Information Source

Adding an information source entails an understanding of information flow, together with the procedures for initial setup and registration of an information source that also apply to information source addition.

4.1.1 Flow of Information Source Addition Tasks

Figure 4.1 shows the task flow for information source addition processing.

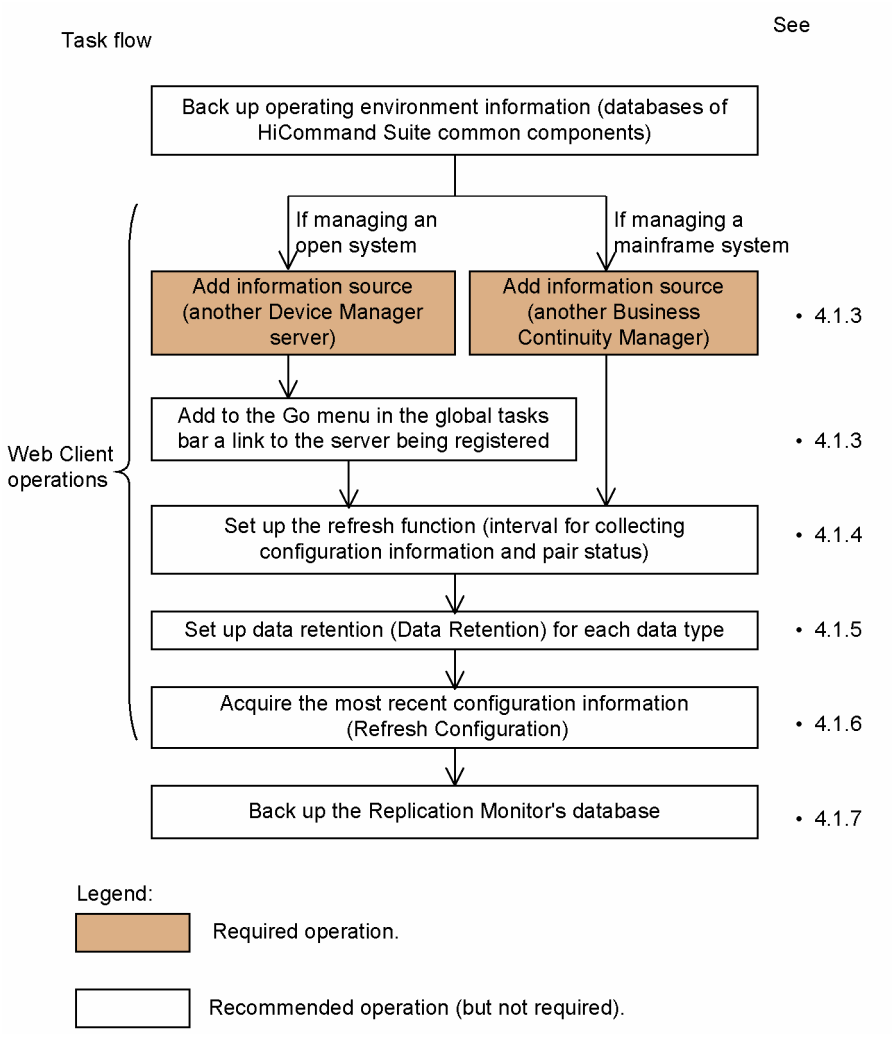

Figure 4.1 Task flow for Information Source Addition

4.1.2 Preparations Before Adding an Information Source

Before adding an information source to the system, you must use HiCommand Suite Common Component's `hcmdsbackups` command to back up the database. For details about backing up a database, see section 3.8.

4.1.3 Procedure for Adding an Information Source

The procedures for adding a Device Manager server or a Business Continuity Manager to the system as an information source, as well as for specifying the settings that enable an information source's applications to be called from the Web Client, are the same as for initial setup, as described in section 3.3.9.

4.1.3.1 Adding a Device Manager Server

The procedure for adding a Device Manager server to the system as an information source is the same as the procedure for registering an information source at the time of initial setup. For details, see section 3.4.1.

4.1.3.2 Adding a Business Continuity Manager

The procedure for adding a Business Continuity Manager to the system as an information source is the same as the procedure for registering an information source at the time of initial setup. For details, see section 3.4.2.

4.1.3.3 Calling Source Applications from the Web Client (hcmdslink command)

To enable an information source's applications to be called from the Web Client, you must set a link to the information source (URL of the information source's server) in the dialog box that is displayed by choosing **Go** and then **Links** from the global tasks bar area. You use the `hcmdslink` command to set this link. For details about the operation, see the *HiCommand Device Manager Server Installation and Configuration Guide*.

4.1.4 Specifying the Refresh Function

You can specify and change the settings for whether automatic refreshing is to be performed and the information collection cycle if automatic refreshing is to be enabled; these settings are described below.

Collecting configuration information

You can set and change the collection interval and the collection start time for each information source.

Collecting information related to copy pair status

You can set and change the collection interval.

If the information source is a Device Manager server, you can set and change the collection interval for each pair management server and for each information source. In the case of an information source, you can specify settings for the agent and for the Device Manager server, depending on the target copy pair.

If the information source is a Business Continuity Manager, you can set and change the collection interval for each information source.

The procedure for specifying the refresh settings is the same as for initial setup, as described in section 3.5.

- Setting the interval for collecting configuration information
- Setting the interval for collecting copy pair status information for each information source
- Setting the interval for collecting copy pair status information for each pair management server (open systems only)

For details about the procedures, see the applicable sections in section 3.5.

4.1.5 Setting up Data Retention

You can specify settings for saving the following six types of data:

- Alert history
- Write delay time data (C/T delta) for open systems
- Write delay time data (C/T delta) for mainframe systems
- Event log
- Side file and journal volume usage for open systems
- Side file and journal volume usage for mainframe systems

You can specify separately whether to save data of each data type. If you decide to save a type of data, you can set the following items:

- Retention period (number of days the data is to be retained)
- Start time for deleting data whose retention period has elapsed (time at which data deletion is to start each day)

The procedures for specifying and changing the data retention settings are the same as for initial setup. For details, see section 3.6.

4.1.6 Acquiring the Most Recent Configuration Information

The procedure for acquiring the most recent configuration information is the same as for initial setup, as described in Chapter 3; for details, see section 3.7.

Note:

You do not need to acquire the recent configuration information again, because the information is already acquired if you selected the check box in the dialog box so that configuration information of copy pairs managed by information sources (Device Manager or Business Continuity Manager) is collected when you registered the information source.

4.1.7 Backing up the Replication Monitor Server Database

You must back up the Replication Monitor server database when its contents have changed due to addition of information sources and updating of configuration information.

To back up the Replication Monitor server database, execute the HiCommand Suite Common Component `hcmdsbackups` command. For details about executing the `hcmdsbackups` command, see section 3.8.

4.2 Deleting an Information Source

Figure 4.2 shows the task flow for information source deletion processing.

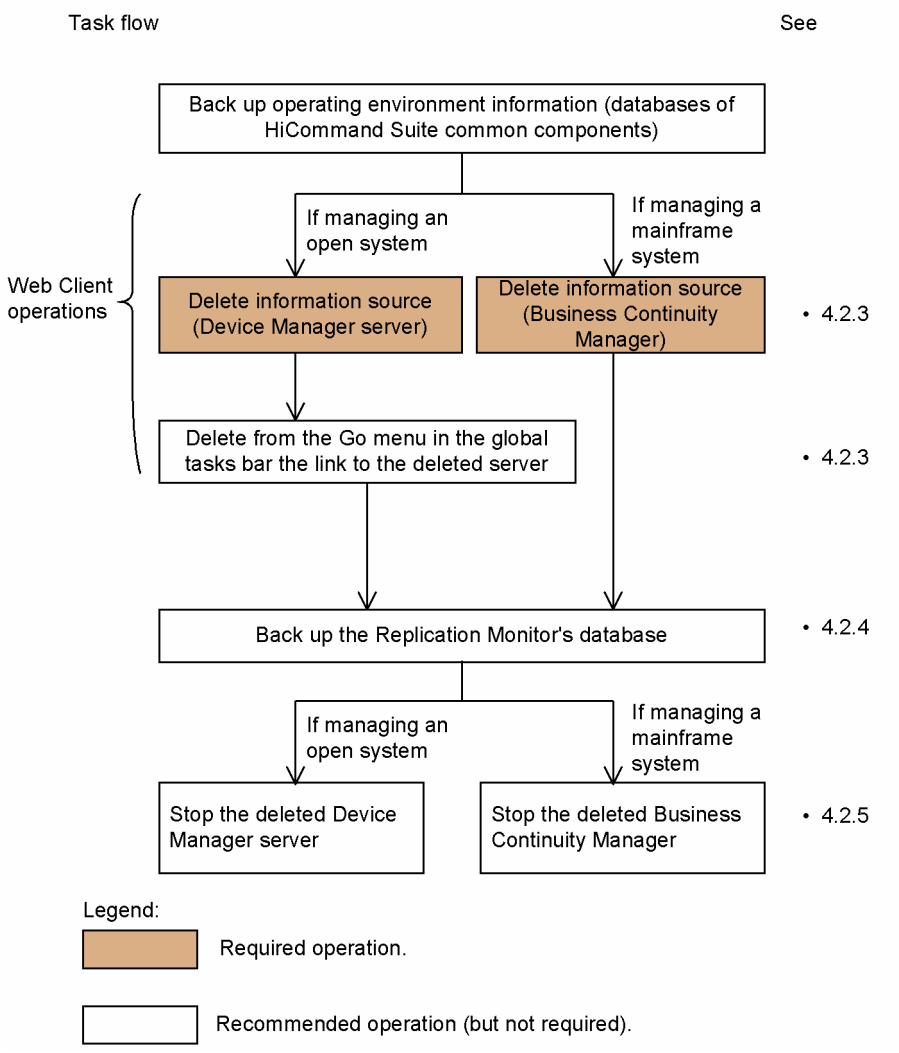

Figure 4.2 Task flow for Information Source Deletion

4.2.1 Preparations Before Deleting an Information Source

Before deleting an information source from the system, you must use HiCommand Suite Common Component's `hcmdsbackups` command to back up the database. For details about backing up a database, see section 3.8.

4.2.1.1 Deleting a Device Manager Server

To delete a Device Manager server that is used as an information source:

1. In Explorer, choose **Settings** and then **Information Source**.

   An object tree from which you can select an information source is displayed in the navigation area, and an information source list is displayed in the application area.

2. Choose **Device Manager** from the object tree or from the list.

   A list of registered Device Manager servers is displayed in the application area.

3. Select the check box to the left of the name of the Device Manager server that you want to delete.

   The **Remove HDvMs** button is enabled.

4. Click the **Remove HDvMs** button.

   A dialog box requesting that you confirm that the Device Manager server is to be deleted is displayed, see Figure 4.3.

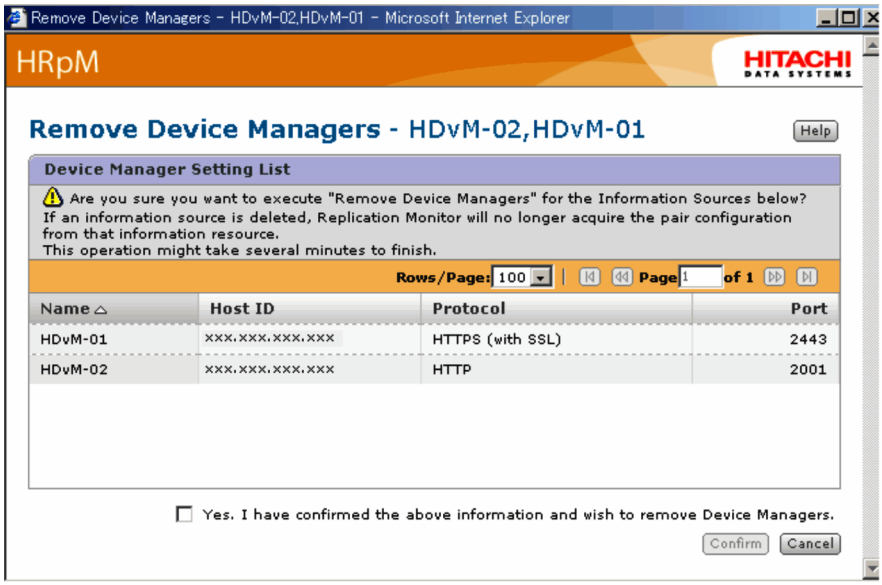

Figure 4.3 Dialog Box for Confirming Deletion of a Device Manager Server

5. Select the **Yes. I have confirmed the above information and wish to remove Device Managers.** check box.

   The **Confirm** button is enabled.

6. Click the **Confirm** button.

   Deletion processing begins and a dialog box that shows the progress of the deletion processing is displayed. Once the processing is complete, a dialog box indicating that the Device Manager server deletion processing has been completed is displayed.

4.2.1.2 Deleting Business Continuity Manager

To delete a Business Continuity Manager that is used as an information source:

1. In Explorer, choose **Settings**, and then **Information Source**.

An object tree from which you can select an information source is displayed in the navigation area, and an information source list is displayed in the application area.

2. Choose **Business Continuity Manager** from the object tree or from the list.

   A list of registered Business Continuity Managers is displayed in the application area.

3. Select the check box to the left of the name of the Business Continuity Manager that you want to delete.

   The **Remove BCMs** button is enabled.

4. Click the **Remove BCMs** button.

   A dialog box requesting that you confirm that the Business Continuity Manager is to be deleted is displayed, see Figure 4.4.

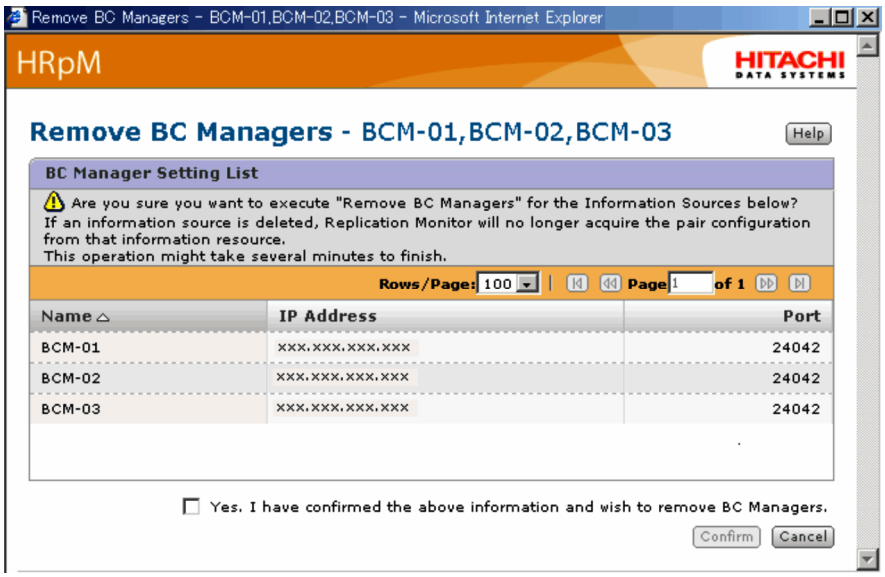

Figure 4.4 Dialog Box for Confirming Deletion of a Business Continuity Manager

5. Select the **Yes. I have confirmed the above information and wish to remove Business Continuity Managers.** check box.

   The **Confirm** button is enabled.

6. Click the **Confirm** button.

   Deletion processing begins and a dialog box that shows the progress of the deletion processing is displayed. Once the processing is complete, a dialog box indicating that the Business Continuity Manager deletion processing has been completed is displayed.

4.2.1.3 Deleting the Link to the Information Source (Device Manager)

You can use the dialog box that is displayed when you choose **Go** and then **Links** in the global tasks bar area to set a link to an information source (URL of the information source's server). This enables the information source (the Device Manager server) to be called from the Web Client. If you subsequently delete the information source, you must use the `hcmdslink` command to delete the link.

An example of the hcmdslink command for deleting a link is shown below (in this example, the management server uses a Windows OS):

```
hcmdslink /delete /file C:\SampleLink.txt /user system /pass manager
```

You specify the delete option in the hcmdslink command, together with the file option that specifies the link to be deleted. The file option must specify the same text file that was used when the link was set.

The following shows an example of such a text file:

```
@TOOL-LINK
@NAME SampleApp
@URL http://SampleApp/index.html
@DISPLAYNAME SampleApplication
@DISPLAYORDER 10
@ICONURL http://SampleApp/graphic/icon.gif
@TOOL-END
```

This example deletes the link to the program named SampleApplication, which is displayed in the dialog box.

For details about the hcmdslink command, see the *HiCommand Device Manager Server Installation and Configuration Guide*.

4.2.2 Backing Up the Replication Monitor Server Database

You must back up the Replication Monitor server database when its contents have changed due to deletion of an information source.

To back up the Replication Monitor server database, execute the HiCommand Suite Common Component hcmdsbackups command. For details about executing the hcmdsbackups command, see section 3.8.

4.2.3 Stopping a Deleted Information Source

After you have deleted an information source from the system, you must use the appropriate procedure described below to stop the deleted information source.

4.2.3.1 Stopping a Device Manager Server

If the Device Manager server uses a Windows OS, use either of the following methods to stop the Device Manager server:

- From the Windows **Start** menu, choose the appropriate menu item.
- Use the hicommand.bat command.

If the Device Manager server uses a Solaris OS, use the hicommand.sh command to stop the Device Manager server.

For details about stopping a Device Manager server, see the *HiCommand Device Manager Server Installation and Configuration Guide*.

4.2.3.2 Stopping a Business Continuity Manager

If the information source is a Business Continuity Manager, enter the `STOP` command from the mainframe host's console.

For details about stopping a Business Continuity Manager, see the *Hitachi Business Continuity Manager User's Guide*.

Chapter 5 Managing Replication Monitor Security

This chapter explains security management using Replication Monitor.

- Security Related to User Permissions (see section 5.1)
- Security Related to Network Access (see section 5.2)

5.1 Security Related to User Permissions

To allow only those users having the correct permissions to access HiCommand products, including Replication Monitor, Replication Monitor is equipped with a security management facility that is based on user authentication.

A user can access Replication Monitor using one of the following methods:

- A user can log in to Replication Monitor directly from Web Client.
- A user who is using another HiCommand product, such as Device Manager, can use a Link-and-Launch operation to access Replication Monitor.

A user who is using Replication Monitor also accesses other HiCommand products in the following cases:

- When the user who is using Replication Monitor uses a Link-and-Launch operation to access another HiCommand product, such as Device Manager.
- While using Replication Monitor, the user accesses the Device Manager server that is the information acquisition source of the Replication Monitor server.

5.1.1 User Permissions Necessary for Login

When a user is attempting to log in to Replication Monitor from Web Client, user authentication is performed with a user ID and a password. Only those users who have the User Management, Modify, or View permission or who have a combination of these permissions are allowed to log in to and access Replication Monitor.

Only a user who has the user management permission (User Management) can register users in Replication Monitor and assign these permissions to users.

For details on user permissions and how to set them, see section 3.3.

5.1.2 Inheriting User Authentication During a Link-and-Launch Operation

For a user who has permissions to log in to both Replication Monitor and other HiCommand products, that user's user authentication information is inherited during a Link-and-Launch operation. Therefore, the user need not log in again when accessing another HiCommand product from Replication Monitor or vice versa using a Link-and-Launch operation.

To use Link-and-Launch from the logged-in Replication Monitor to another HiCommand product, select the HiCommand product to be accessed from the **Dashboard** menu. In this case, if the user who is using Replication Monitor has the login permission to access the destination HiCommand product, the user can simply access it. If the user does not have a login permission, the login window is displayed, and the user needs to enter the name of a user having a login permission and a password.

If a logged-in user who is using a Link-and-Launch operation from another HiCommand product to Replication Monitor has a permission to log in to Replication Monitor, the user can simply access it. If the user does not have a login permission, an authentication error occurs.

5.1.3 User Permission for Accessing the Device Manager Server

When a user who is using Replication Monitor accesses the Device Manager server, the Replication Monitor server uses the following special user ID that has a Device Manager user account:

- When the Device Manager server is on the local server, the user ID specified during Replication Monitor installation is used.
- When the Device Manager server has been registered as the information source, the user ID specified during Device Manager server registration is used.

Regardless of the user who is logged in to Replication Monitor, one of the above user ID is used for accessing the Device Manager server from Replication Monitor.

The user account under the user ID specified during Replication Monitor installation or the user ID specified during the registration of the Device Manager server as the information source must be assigned the Modify permission for Device Manager, and `All Resources` must be allocated to the resource group.

5.2 Security Related to Network Access

When Replication Monitor is running, the following three types of communication routes in the network are used by the management server and the management client:

(1) Communication route between the Replication Monitor server of the management server and the Device Manager server of another management server

(2) Communication route between the Replication Monitor server and the Device Manager server inside the management server

(3) Communication route between the management client and the Replication Monitor server of the management server

This section explains the communication security in these communication routes. The numbers (1), (2), and (3) correspond to those in the figure shown below.

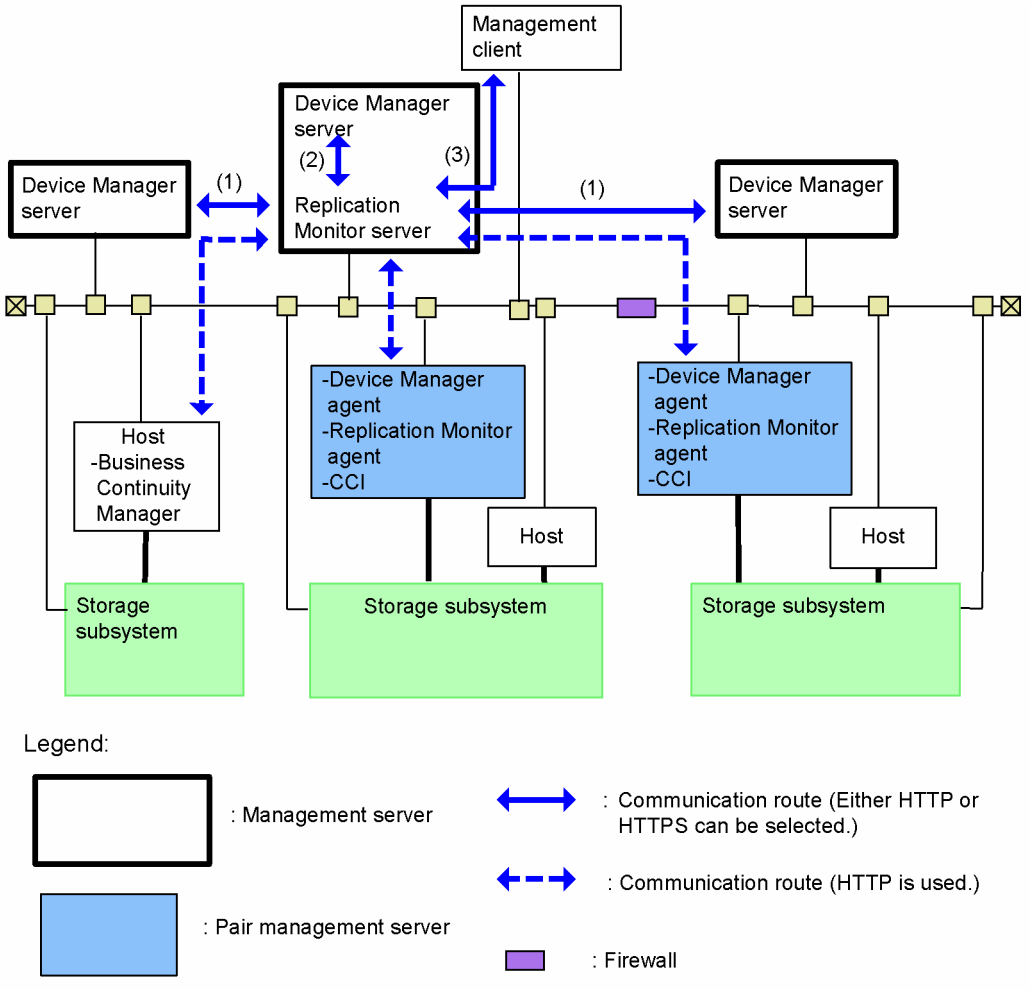

Figure 5.1 Communication Routes Used by Replication Monitor

The following two other types of communication routes also are used:

- Communication route between the Replication Monitor server of the management server and the Device Manager agent of the pair management server
- Communication route between the Replication Monitor server of the management server and the Business Continuity Manager

For these two communication routes, HTTP is used as the communication protocol.

5.2.1 Securing Communication Within a Management Server and Between Management Servers

For communication within a management server or between multiple management servers (between the Replication Monitor server and the Device Manager server), you can encrypt the communication by using HTTPS as the communication protocol.

To encrypt the communication between the Replication Monitor server and the Device Manager server, the following two operations are required:

- Selecting HTTPS as the communication protocol when registering the Device Manager server as the information source.
- Setting SSL on the Device Manager server.

For details on the procedure for setting SSL on the Device Manager server, see the *HiCommand Device Manager Server Installation and Configuration Guide*.

If you do not wish to use the HTTPS communication protocol, you can use HTTP. In this case, HTTP basic authentication is performed according to the specifications of the Device Manager HTTP (Web) server communication protocol.

5.2.2 Securing Communication Between a Management Client and a Management Server

In the standard setting, HTTP is used as the communication protocol between a management client (Web browser) and the Remote Installation Manager server inside a management server. However, if you specify SSL in the HBase Storage Mgmt Web Service being used by Replication Monitor, you can encrypt the communication and use HTTPS as the communication protocol.

To use SSL, you need a server certificate. The HBase Storage Mgmt Web Service supports SSL Versions 2 and 3.

For details on the security procedure when using the HBase Storage Mgmt Web Service, see the *HiCommand Device Manager Server Installation and Configuration Guide*.

Chapter 6 Maintaining and Tuning the System

This chapter explains how to operate, maintain, and tune the system on which Replication Monitor is running.

- Changing Operation Modes of Replication Monitor (see section 6.1)
- Changing the Host Name for the Management Server (see section 6.2)
- Starting or Terminating Services (see section 6.3)
- Viewing an Event Log (see section 6.4)
- Changing License Information (see section 6.5)
- Viewing the Replication Monitor Agent Version Information (see section 6.6)
- Setting Security for User Accounts(see section 6.7)
- Editing a Warning Banner (see section 6.8)
- Migrating the Replication Monitor Server Database(see section 6.9)
- Tuning the Property File Settings (see section 6.10)
- Generating Audit Logs (see section 6.11)

6.1 Changing Operation Modes of Replication Monitor

To prevent Replication Monitor from performing an operation on a storage device, such as during micro code conversion in a storage subsystem, you must set the operation mode to the maintenance mode. This section explains how to change the operation mode.

6.1.1 Replication Monitor Operation Modes

Replication Monitor can operate in the normal or maintenance mode.

Normal mode

This is the default mode. In this mode, all operations, including auto refresh, manual refresh, and copy pair manipulation, can be performed.

Maintenance mode

In this mode, auto refresh is stopped, and manual refresh, copy pair manipulation, and configuration information acquisition are all disabled. The buttons used for executing these operations are disabled and cannot be clicked.

The mode area showing the Replication Monitor information on the **Dashboard** displays **Running** in the normal mode and **Maintenance** in the maintenance mode. If the mode is being changed from the normal mode to the maintenance mode, the mode area displays **Transition to Maintenance**.

To change the mode, from the **Explorer** menu, choose **Administration** and then **Maintenance**, and use the subwindow that opens.

6.1.2 Changing the Operation Mode

To change from the normal mode to the maintenance mode:

1. From the **Explorer** menu, choose **Administration** and then **Maintenance**.

   The application area shows that the current mode is Normal.

2. Click the **Change Mode** button.

   A dialog box for confirming the change to the maintenance mode opens, see Figure 6.1.

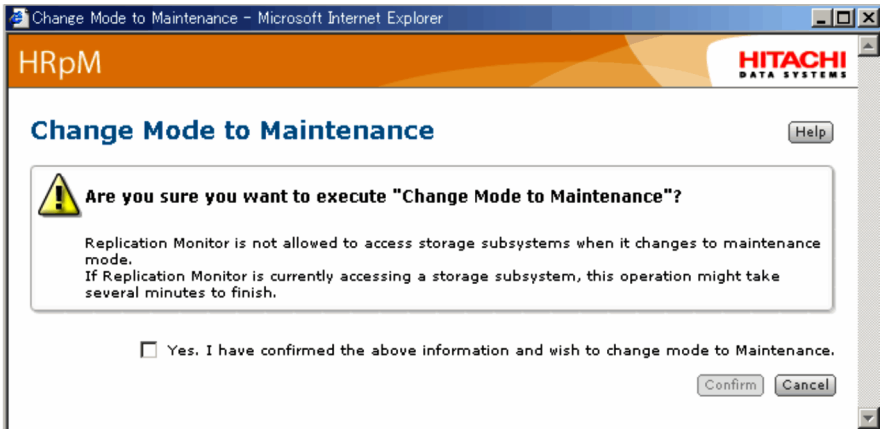

Figure 6.1 Dialog Box for Confirming the Change to the Maintenance Mode

3. Select the **Yes. I have confirmed the above information and wish to change mode to Maintenance** check box.

   The **Confirm** button is enabled.

4. Click the **Confirm** button.

   A dialog box indicating that a mode change is in progress opens. When the change is finished, a dialog box indicating that the mode change has finished opens.

To change from the maintenance mode to the normal mode:

1. From the **Explorer** menu, choose **Administration** and then **Maintenance**.

   The application area shows that the current mode is Maintenance.

2. Click the **Change Mode** button.

   A dialog box for confirming the change to the normal mode opens, see Figure 6.2.

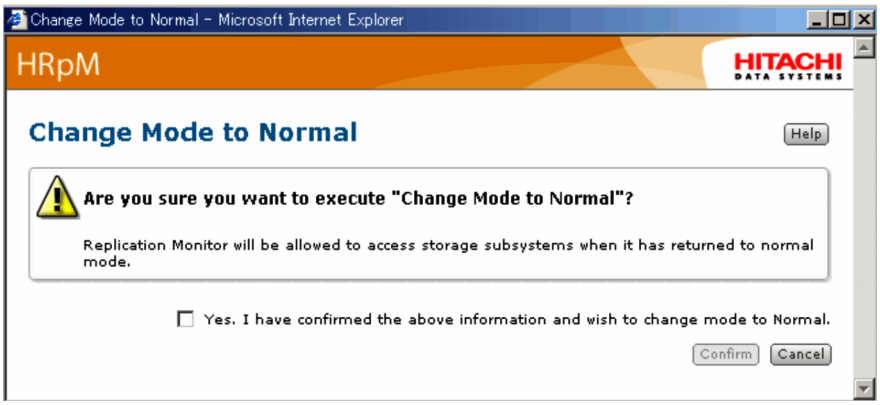

Figure 6.2 Dialog Box for Confirming the Change to the Normal Mode

3. Select the **Yes. I have confirmed the above information and wish to change mode to Normal** check box.

   The **Confirm** button is enabled.

4. Click the **Confirm** button.

   A dialog box indicating that a mode change is in progress opens. When the change is finished, a dialog box indicating that the mode change has finished opens.

6.2 Changing the Host Name for the Management Server

Before you can change the host name or IP address for the management server on which Replication Monitor is installed, you must edit several setting files of HiCommand Suite Common Component. You must also use the `hcmdschgurl` command to change the host name or IP address of the management server saved in the HiCommand Suite Common Component database. In this section, *host name or IP address* is abbreviated as *host name*.

Note:

If you change the host name for the management server, an error might occur in other products installed on the management server. Before you change the host name, make sure that an error will not occur in other products.

If the management server host name described in the following files is the loopback address `127.0.0.1`, the operations in steps 4, 5, and 6 shown below (host name change operations) are not necessary.

- `pdsys` file and `def_pdsys` file
- `pdutsys` file and `def_pdutsys` file
- `HiRDB.ini` file

To change the host name for the management server:

1. Stop all HiCommand product services or daemons.

   For details on how to stop the services or daemons of HiCommand products, see section 2.7.2.

2. If the SSL settings have been configured, configure them again.

   Use the host name after the change to configure the SSL settings. For details on how to configure SSL settings, see the *HiCommand Device Manager Server Installation and Configuration Guide*.

3. Edit the `httpsd.conf` file.

   Change the value for the `ServerName` parameter to the host name after the change.

   The following describes the storage destination for the `httpsd.conf` file.

   - For Windows:

     installation-folder-for-HiCommand-Suite-Common-Component`\httpsd\conf\`

   - For Solaris:

     `/opt/HiCommand/Base/httpsd/conf/`

   If SSL is set, you must also do the following:

   - Change the host name specified for the `<VirtualHost>` tag to the host name after the change.
   - Change the value for the `ServerName` parameter in the `<VirtualHost>` tag to the host name after the change.

Proceed to the next step according to the following cases:

- For a cluster configuration:

  Proceed to step 4.

- For a non-cluster configuration:

  If you performed a new installation of version 5.0 or later, or performed a re-installation of version 5.0 or later, skip to step 8. In other cases, proceed to step 4.

4. Edit the `pdsys` file and `def_pdsys` file.

   Change the value for the `-x` option for the `pdunit` parameter to the host name after the change or the loopback address `127.0.0.1`. If the value is changed to `127.0.0.1`, this step is not necessary even if the host name is changed again.

   Note: Specify a virtual host name for a cluster configuration.

   The following describes the storage destinations for the `pdsys` file and `def_pdsys` file.

   - For Windows:

     installation-folder-for-HiCommand-Suite-Common-Component`\HDB\conf\pdsys`

     installation-folder-for-HiCommand-Suite-Common-Component`\database\work\def_pdsys`

   - For Solaris:

     `/opt/HiCommand/Base/HDB/conf/pdsys`

     `/opt/HiCommand/Base/database/work/def_pdsys`

5. Edit the `pdutsys` file and `def_pdutsys` file.

   Change the value for the `pd_hostname` parameter to the host name after the change or the loopback address `127.0.0.1`. If the value is changed to `127.0.0.1`, this step is not necessary even if the host name is changed again. If `pd_hostname` does not exist, you do not need to edit these files.

   Note: For a cluster configuration, edit the `pdutsys` file and `def_pdutsys` file on both the executing node and standby node. In such a case, for `pd_hostname`, specify the host name for the executing node.

   The following describes the storage destinations for the `pdutsys` file and `def_pdutsys` file.

   - For Windows:

     installation-folder-for-HiCommand-Suite-Common-Component`\HDB\conf\pdutsys`

     installation-folder-for-HiCommand-Suite-Common-Component\database\work\def_pd`utsys`

   - For Solaris:

     `/opt/HiCommand/Base/HDB/conf/pdutsys`

     `/opt/HiCommand/Base/database/work/def_pdutsys`

6. Edit the `HiRDB.ini` file.

   Change the value for the `PDHOST` parameter to the host name after the change or the loopback address `127.0.0.1`. If the value is changed to `127.0.0.1`, this step is not necessary even if the host name is changed again.

Note: Specify a virtual host name for a cluster configuration.

The following describes the storage destination for the `HiRDB.ini` file.

- For Windows:

  installation-folder-for-HiCommand-Suite-Common-Component`\HDB\conf\emb\HiRDB.ini`

- For Solaris:

  `/opt/HiCommand/Base/HDB/conf/emb/HiRDB.ini`

7. Edit the `cluster.conf` file (only for a cluster configuration).

   From among the virtual host name, host name for the executing node, and host name for the standby node, change the corresponding host name to the host name after the change.

   The following describes the storage destination for the `cluster.conf` file.

   - For Windows:

     installation-folder-for-HiCommand-Suite-Common-Component`\conf\cluster.conf`

   - For Solaris:

     `/opt/HiCommand/Base/conf/cluster.conf`

8. Change the host name for the management server, and then restart the machine.

   If the host name for the management server has already been changed, simply restart the machine.

9. Make sure that the HiCommand Suite Common Component service is running.

   - For Windows:

     installation-folder-for-HiCommand-Suite-Common-Component`\bin\hcmdssrv /status`

   - For Solaris:

     `opt/HiCommand/Base/bin/hcmdssrv –status`

10. Execute the `hcmdschgurl` command to change the host name in the URL for starting Web Client.

    The `hcmdschgurl` command is used for updating the access information (URL information) used for starting an application saved in the HiCommand Suite Common Component database.

    For details on how to use the `hcmdschgurl` command, see the *HiCommand Device Manager Server Installation and Configuration Guide*.

6.3 Starting or Terminating Services

This section explains how to start and stop the services of the Replication Monitor server and the Replication Monitor agent, and how to stop an instance of CCI used by Replication Monitor.

To execute the open system commands explained in this section, the user must log in as the following user:

In Windows:

An administrator group user

In Solaris:

A root user

6.3.1 Starting or Terminating Services of Replication Monitor in Management Server

This section explains how to start and stop the Replication Monitor server services.

Replication Monitor operates as part of HBase Storage Mgmt Web Service, a service of HiCommand Suite Common Component. Therefore, starting and stopping of the Replication Monitor server services are performed by starting and stopping HiCommand Suite Common Component services.

6.3.1.1 Starting Services of Replication Monitor Server

To start the Replication Monitor server services, execute the following command:

In Windows:

```
HiCommand-Suite-Common-Component-installation-folder\bin\hcmdssrv /start
```

In Solaris:

```
/opt/HiCommand/Base/bin/hcmdssrv -start
```

Device Manager must be running for Replication Monitor to operate normally. When you execute the `hcmdssrv` command as described above, the Device Manager server service also starts.

When you execute the `hcmdssrv` command with the start option specified, the services of the embedded database HiRDB, Device Manager, and other HiCommand products also start.

Note:

- When you execute the hcmdssrv command with the start option specified, if the HiCommand Suite Common Component services are already running, the service of the Device Manager server and the service of the Tiered Storage Manager server will not be started. In this case, you need to start these services separately.
- You cannot use the hcmdssrv command to automatically start the services of the following HiCommand product versions:

- Device Manager version 5.6 or earlier
- Tiered Storage Manager version 5.5 or earlier

For details on how to start the services of the Device Manager server or Tiered Storage Manager server, and how to check whether these services are running, see the HiCommand Device Manager Server Installation and Configuration Guide or the HiCommand Tiered Storage Manager Server Installation and Configuration Guide.

6.3.1.2 Terminating Services of Replication Monitor Server

To stop the Replication Monitor server services, execute the following command:

In Windows:

```
HiCommand-Suite-Common-Component-installation-folder\bin\hcmdssrv /stop
```

In Solaris:

```
/opt/HiCommand/Base/bin/hcmdssrv -stop
```

When the `hcmdssrv` command is executed as described above, the Device Manager and other HiCommand product services also stop. Do not stop any HiCommand Suite Common Component services except when you need to stop all HiCommand products.

Note:

You cannot use the `hcmdssrv` command to automatically stop the services of the following HiCommand product versions. For details on how to stop the services of those versions, see the manual for each product.

- Device Manager version 5.6 or earlier
- Tiered Storage Manager version 5.5 or earlier

If other HiCommand products have stopped and the `hcmdssrv` command is executed as described above, the embedded database HiRDB also stops.

6.3.1.3 Checking Operation Status of Replication Monitor Server

To check whether the Replication Monitor server services are operating, execute the following command:

In Windows:

```
HiCommand-Suite-Common-Component-installation-folder\bin\hcmdssrv /status
```

In Solaris:

```
/opt/HiCommand/Base/bin/hcmdssrv -status
```

Example 1: Execution results when the Replication Monitor server services are operating

```
>hcmdssrv /status
KAPM05007-I Already started service. service-name=HBase Storage Mgmt Web Service
KAPM05007-I Already started service. service-name=HBase Storage Mgmt Common Service
```

Example 2: Execution results when the Replication Monitor server services are stopped

```
>hcmdssrv /status
KAPM05009-I Already stopped service. service-name=HBase Storage Mgmt Web Service
KAPM05009-I Already stopped service. service-name=HBase Storage Mgmt Common Service
```

If the `hcmdssrv` command is executed as described above, you can also check whether the embedded database HiRDB is running. If the embedded database HiRDB is running, the following message appears in the execution result described above:

```
KAPM06440-I The HiRDB service has already started.
```

The following message appears if the embedded database HiRDB is inactive:

```
KAPM06441-I The HiRDB service has already stopped.
```

6.3.2 Starting or Terminating Services of an Agent in a Pair Management Server

This section explains how to start and stop the Replication Monitor agent.

The Replication Monitor agent operates as part of the Device Manager agent. Therefore, starting and stopping of the Replication Monitor agent services are performed by starting and stopping the Device Manager agent.

To start the Device Manager agent services, use the following command on the pair management server:

In Windows:

Device-Manager-agent-installation-folder`\bin\hbsasrv.exe start`

In Solaris, HP-UX, Linux:

```
/opt/HDVM/HBaseAgent/bin/hbsasrv start
```

In AIX:

```
/usr/HDVM/HBaseAgent/bin/hbsasrv start
```

To stop the Device Manager agent services, use the following command on the pair management server:

In Windows:

Device-Manager-agent-installation-folder`\bin\hbsasrv.exe stop`

In Solaris, HP-UX, Linux:

```
/opt/HDVM/HBaseAgent/bin/hbsasrv stop
```

In AIX:

```
/usr/HDVM/HBaseAgent/bin/hbsasrv stop
```

For details about how to start and stop the Device Manager agent services, see the *HiCommand Device Manager Agent Installation Guide*.

6.3.3 Terminating an Instance of CCI Used by an Agent

You can use one of the following two methods for starting and stopping an instance of CCI (HORCM instance for monitoring) used by the Replication Monitor agent:

- Automatically start or stop whenever a request is issued to the copy pair.
- Automatically start when the first request is issued to the copy pair. No automatic stopping is performed.

Which of these methods is used is determined by the setting in the `agent.properties` property file. The default is the latter method.

With the latter method, the user must use a command to stop an instance of CCI (HORCM instance for monitoring) as needed. To stop the instance, execute the following command:

```
hrpm_horcmctrl -stop
```

If you execute the `hrpm_horcmctrl` command without specifying `-stop`, you can view the running status of the instance.

Note:

If you execute the `hrpm_horcmctrl` command in Windows, in advance, you must change the user who will execute the Device Manager agent service (the HBsA Service service) to a user who has the Administrator permissions. By default, the user who will execute the HBsA Service service is set to be a user who has the LocalSystem permissions.

For details about how to change the user who will execute the HBsA Service service, see the *HiCommand Device Manager Agent Installation Guide*.

6.4 Viewing an Event Log

You can view those Replication Monitor event logs that affect operations in the event log list displayed in the application area. You can also select a log from the list and view its details. You can also export the event log list to a CSV or HTML file.

To view an event log:

1. From the **Explorer** menu, choose **Administration** and then **Event Logs**.

   An event log list subwindow appears in the application area, see Figure 6.3.

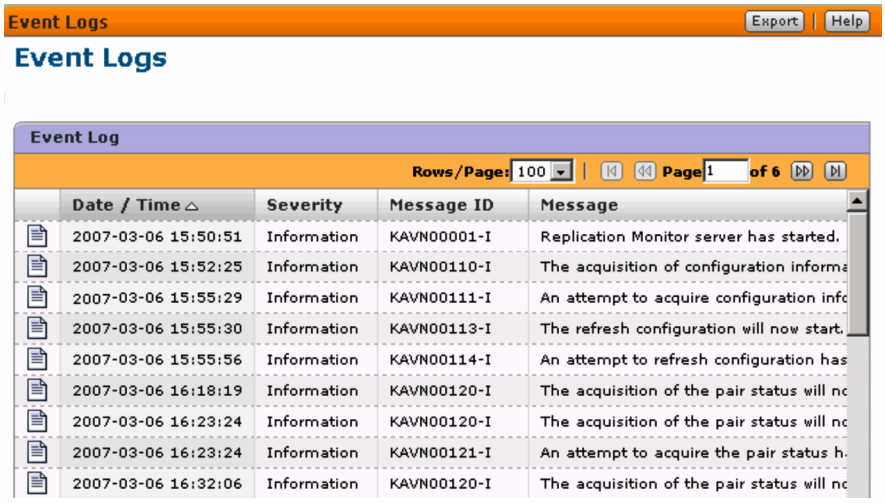

Figure 6.3 Event Log List Subwindow

2. To view the details of a particular event log, click the icon to the left of it.

   The details of the specified log are displayed.

To export an event log:

1. From the **Explorer** menu, choose **Administration** and then **Event Logs**.

   A list of event log subwindows appears in the application area.

2. Click the **Export** button.

   A dialog box for exporting an event log opens, see Figure 6.4.

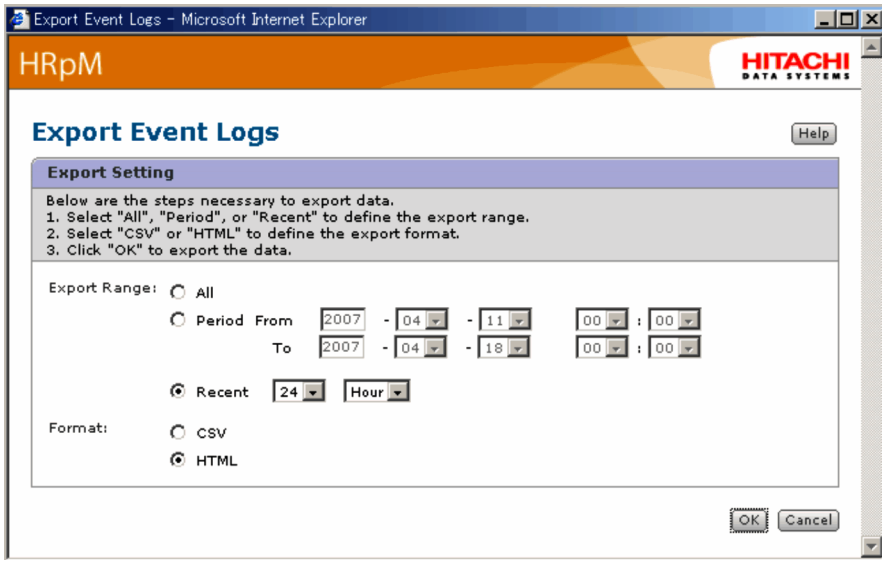

Figure 6.4 Dialog Box for Exporting an Event Log

3. To specify the range to be exported, select the **All**, **Period**, or **Recent** radio button.

   If you select **Period**, enter the date and time for the start and finish points. If you select **Recent**, enter the number of days or hours up to the present.

4. Select the **CSV** or **HTML** radio button to specify the exporting format.

5. Click the **OK** button.

   The specified range of event logs is exported to a file in the specified format.

Note:

Replication Monitor exports a CSV file in UTF-8 encoding. To view the file exported in the CSV format, use Excel 2003 or a text editor that supports UTF-8 encoding.

6.5 Changing License Information

This section explains how to change the license information, for example, from a temporary license to a permanent license. To change the license information, use the dialog box for registering or changing the license key. To open this dialog box, you can use any of the following three methods:

- Click **License** in the Login window.
- From the **Explorer** menu, choose **Settings** and then **License Info**. Then, in the subwindow displayed in the application area, click the **Edit License** button.
- Choose **Help** and then **About** from the global tasks bar area.

To change the license key from the **Explorer** menu, follow the procedure described below.

1. From the **Explorer** menu, choose **Settings** and then **License Info**.

   The version of the Replication Monitor currently being used, the license type, and the DKC information of the subsystem that corresponds to the license key are displayed in the application area.

   If a temporary or emergency license is being used, the number of days remaining in the license is displayed in the area that indicates the version and license type of the Replication Monitor currently being used.

2. Click the **Edit License** button.

   A dialog box for changing the license information opens, see Figure 6.5.

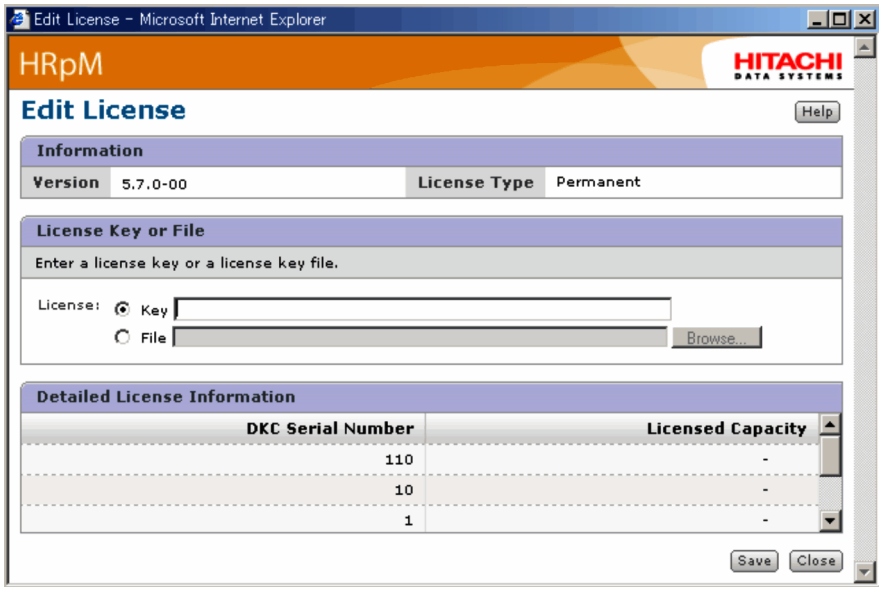

Figure 6.5 Dialog Box for Changing the License Information

3. Select the **Key** or **File** radio button, and specify the license key or license file to be registered.

   When specifying a license file, either use an absolute path to specify a file name or click the **Browse** button to display a file selection window and select the appropriate file from this window.

4. To register the information corresponding to the specified license key, click the **Save** button.

   This operation registers the license information in the system.

5. Click the **Close** button.

   The dialog box for changing license information closes. The license type after the change and the DKC information of the subsystem that corresponds to the license key are displayed in the application area.

6.6 Viewing the Replication Monitor Agent Version Information

When upgrading the Replication Monitor server, also check the Replication Monitor agent version. You can use the `hrpm_agentversion` command to view the Replication Monitor agent version information.

To view the Replication Monitor agent version information:

1. Execute the following command.
   - In Windows:

     Device-Manager-agent-installation-folder`\bin\hrpm_agentversion`

     An example of command execution is shown below.

     ```
     C:\Program Files\HiCommand\Base\bin\hrpm_agentversion
     ```
   - In Solaris:

     ```
     # Device-Manager-agent-installation-directory/bin/hrpm_agentversion
     ```
2. The Replication Monitor agent version information is output.

   An example of the results of command execution is shown below.

```
Module name: hrpm
Explanation: Replication Monitor - Agent
Version    : 05.7.0.0000
Condition  : Activated
```

6.7 Setting Security for User Accounts

Replication Monitor supports the setting of password conditions (minimum length, combination of characters, and so on) to prevent passwords from being guessed by a third party. A user account can also be locked automatically when invalid passwords are entered repeatedly for the same user ID.

Note:

User account locking and the password complexity check become available when Replication Monitor version 5.5, 5.6, or 5.7 is installed. These functions apply to users of all HiCommand products on the machine on which Replication Monitor is installed. For this reason, the following anomalies might occur when using a version of HiCommand product that is 5.0 or earlier:

- Login fails although the user ID and password are correct.

  The user account might be locked. Take appropriate action, by unlocking the account or registering a new user account.

- A password cannot be changed, or a user account cannot be added.

  The specified password might not comply with the password rules. Specify an appropriate password, in accordance with the output message.

Set password conditions and account lock settings in the `security.conf` file.

The `security.conf` file resides in the following location:

- In Windows:

```
HiCommand-Suite-Common-Component-installation-folder\conf\sec
```

- In Solaris:

```
/opt/HiCommand/Base/conf/sec
```

The password conditions set in the `security.conf` file apply when a user account is added or a password is changed. Because password conditions do not apply to passwords for existing user accounts, a user with an existing account can log in to the system even if the entered password does not satisfy the set conditions.

When you change the settings in the `security.conf` file, the new settings apply immediately.

The properties set in the `security.conf` file are described next.

6.7.1 password.min.length

Specify the minimum number of characters in a password. You can specify a value from 4 to 256.

Default: `4`

6.7.2 password.min.uppercase

Specify the minimum number of upper-case characters in a password. You can specify a value from 0 to 256. If you specify 0, there is no minimum number of upper-case characters.

Default: `0` (no minimum)

6.7.3 password.min.lowercase

Specify the minimum number of lower-case characters in a password. You can specify a value from 0 to 256. If you specify 0, there is no minimum number of lower-case characters.

Default: `0` (no minimum)

6.7.4 password.min.numeric

Specify the minimum number of numeric characters in a password. You can specify a value from 0 to 256. If you specify 0, there is no minimum number of numeric characters.

Default: `0` (no minimum)

6.7.5 password.min.symbol

Specify the minimum number of symbols in a password. You can specify a value from 0 to 256. If you specify 0, there is no minimum number of symbols.

Default: `0` (no minimum)

6.7.6 password.check.userID

Specify whether to prohibit the setting of a password that is the same as the user ID. You can specify `true` or `false`. If you specify `true`, a password matching the user ID cannot be set. If you specify `false`, a password matching the user ID can be set.

Default: `false` (a password that is the same as the user ID can be set)

6.7.7 account.lock.num

Specify the number of unsuccessful login attempts allowed before the user account is locked automatically. When the number of times that a user continuously fails to log in reaches the specified value, the user account is locked automatically. Note that the `System` account cannot be locked. You can specify a value from 0 to 10. If you specify 0, the user account will not be locked no matter how many times a user fails to log in.

Default: 0 (user accounts are not locked automatically)

Unsuccessful attempts to log in to other HiCommand products that use the Single Sign-On function are counted in the number of unsuccessful login attempts. For example, if the number of unsuccessful attempts is set to `3`, and a user fails to log in to Device Manager once, fails to log in to Provisioning Manager once, and then fails to log in to Global Link Availability Manager once, the user account will be locked automatically

Changing the `account.lock.num` property does not affect users who have already made unsuccessful login attempts or whose account is locked. For example, if you change the property from `5` to `2`, the account of a user who has already made three unsuccessful attempts will remain active. If the user then logs in successfully, or if the user fails to log in twice more and the account is therefore locked, the count is reset to zero at that point and the new setting of `2` applies from the next time the user logs in.

If a third party uses an incorrect password for the account of a user who is already logged in, and the number of unsuccessful login attempts reaches the specified value, the account that is logged in will be automatically locked. If this occurs, the logged-in user can still continue operations until the user logs out. However, the user will be unable to start Tuning Manager from the **Dashboard**.

If an account is automatically locked, the user cannot log in until the account is unlocked. When a user whose account has been locked tries to log in, the normal authentication error will appear and the user will not be notified that his or her account has been locked. Check the **Status** field in the **User List** to see if a user account has been locked.

You can unlock a user account from a management client. You must have the User Management permission to unlock a user account. For details, see section 3.3.6.

6.8 Editing a Warning Banner

In version 5.1 or later of the HiCommand Suite Common Component, a message (warning banner) can be displayed as a security measure when a user logs in. By issuing a warning in advance to a third party attempting unauthorized access, you can reduce the risk of data destruction or disclosure.

The message displayed in the Login window can be a maximum of 1,000 characters. You can register the same message in a different language for each locale. The displayed message will be switched automatically according to the locale of the user's Web browser.

To set a warning message, you must have Administrator permission (in Windows) or log in as root (in Solaris).

6.8.1 Editing a Message

Use the HTML file format when editing a message. You can use a maximum of 1,000 characters. In addition to ordinary characters, you can use HTML tags (included in the character count) to change a font attribute, place a line break anywhere you like, or perform other such editing operations. Unicode (UTF-8) must be used.

An example of a message in HTML format and the displayed result after the message is registered are shown below.

```
<center><b>Warning Notice!</b></center>
This is a {Company Name Here} computer system, which may be accessed and used only for authorized {Company Name Here} business by authorized personnel. Unauthorized access or use of this computer system may subject violators to criminal, civil, and/or administrative action. <br>
All information on this computer system may be intercepted, recorded, read, copied, and disclosed by and to authorized personnel for official purposes, including criminal investigations. Such information includes sensitive data encrypted to comply with confidentiality and privacy requirements. Access or use of this computer system by any person, whether authorized or unauthorized, constitutes consent to these terms. There is no right of privacy in this system.
```

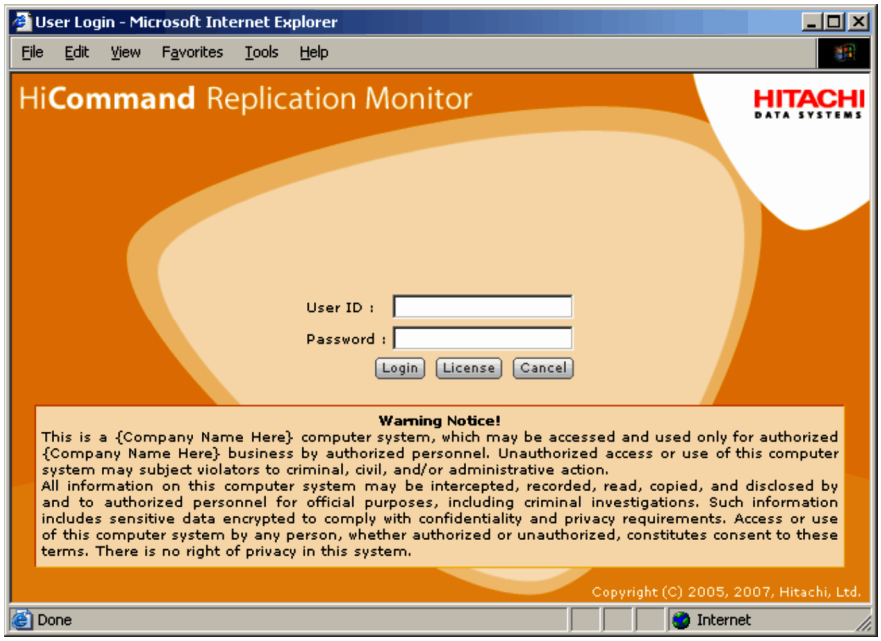

Figure 6.6 Display Result of Registered Message

Note:

The HTML syntax is not checked or corrected when a message is registered. Make sure that you follow the HTML syntax rules, because the message will be registered exactly as written. If there is a syntax problem, the message might not be displayed correctly.

Note:

There are no character restrictions, except that the character code used in the message must be Unicode (UTF-8). Use HTML escape sequences to display characters that are used in HTML syntax (such as `<`, `>`, `"`, `'`, and `&`) as ordinary characters. For example, to display the character & in the Login window, write the sequence `&` in the HTML file.

Note:

To enter a line break at a particular place in the message to be displayed, use the HTML tag `<br>`. Line breaks are ignored when the message is registered.

Sample message files in English (`bannermsg.txt`) and Japanese (`bannermsg_ja.txt`) can be found in the following locations:

– In Windows:

```
HiCommand-Suite-Common-Component-installation-folder\sample\resource
```

– In Solaris:

```
/opt/HiCommand/Base/sample/resource
```

As these sample files are overwritten at installation, copy and edit the file you wish to use.

6.8.2 Registering a Message

Use the `hcmdsbanner` command to register an edited message.

To register a message:

1. Execute the following command:

   – In Windows:

```
HiCommand-Suite-Common-Component-installation-folder\bin\hcmdsbanner /add /file
file-name [/locale locale-name]
```

   An example of command execution is shown below:

```
C:\Program Files\HiCommand\Base\bin\hcmdsbanner /add /file C:\W_Banner\wbfile1 /locale en
```

   – In Solaris:

```
# /opt/HiCommand/Base/bin/hcmdsbanner -add -file file-name [-locale locale-name]
```

   file-name: Specify the file containing the message by using the absolute path.

   locale-name: Specify the locale name of the language in which the message is written (`en` for English, or `ja` for Japanese). When this argument is omitted, the default locale is assumed.

   Return values

   `0`: Normal termination

   `253`: Message length exceeds 1,000 characters.

   `255`: Failed

   Note:

   – The registered message replaces any previously registered message for the same locale.

   – If you specify the `locale` option, you cannot edit messages in Web Client.

   – To use a warning banner in a cluster environment, register the message on both the executing node and the standby node.

     The execution result of the `hcmdsbanner` command is also output to `hcmdsbanner[n].log`.

2. Display the Login window and check whether the message appears correctly.

6.8.3 Deleting a Message

Use the `hcmdsbanner` command to delete a registered message.

To delete a message:

1. Execute the following command:

   – In Windows:

```
HiCommand-Suite-Common-Component-installation-folder\bin\hcmdsbanner /delete [/locale
locale-name]
```

   An example of command execution is shown below:

```
C:\Program Files\HiCommand\Base\bin\hcmdsbanner /delete /locale en
```

   – In Solaris:

```
# /opt/HiCommand/Base/bin/hcmdsbanner -delete [-locale locale-name]
```

   locale-name: Specify the locale of the message to be deleted (en for English, or ja for Japanese). When this argument is omitted, the default locale is assumed.

Return values

0: Normal termination

254: No message is registered for the specified locale.

255: Failed

The execution result of the hcmdsbanner command is also output to hcmdsbanner[n].log.

2. Restart HiCommand Suite Common Component for the message deletion to take effect.

   - In Windows:

```
HiCommand-Suite-Common-Component-installation-folder\bin\hcmdssrv /stop
HiCommand-Suite-Common-Component-installation-folder\bin\hcmdssrv /start
```

   - In Solaris:

```
# /opt/HiCommand/Base/bin/hcmdssrv -stop
# /opt/HiCommand/Base/bin/hcmdssrv -start
```

6.9 Migrating the Replication Monitor Server Database

If you use the HiCommand products over a long period, and upgrade the products or add more objects that need to be managed, you may need a more powerful machine than before. One of the tasks entailed when you replace a computer system is migrating the databases. You can migrate the HiCommand databases by using the `hcmdsdbtrans` command. This command migrates all the information stored in the database of the specific HiCommand product, together with all user information managed by HiCommand Suite Common Component.

By using the `hcmdsdbtrans` command, you can migrate the Replication Monitor server database to a machine whose environment is different from that of the server machine you are using, as shown below:

- Migration to a machine of a different platform
- Migration to a machine where the HiCommand products are installed in a different location
- Migration to a machine where the HiCommand product version is newer than that of the source server.

Notes on migrating database:

The following provides notes on the type, version, and user information of the HiCommand products on the source server and destination server.

Notes on the type and version of the HiCommand products on the source and destination servers:

- You cannot migrate databases of the HiCommand products that are not installed on the destination server. Make sure that you install all the necessary HiCommand products on the destination server.
- If the version of any of the HiCommand products installed on the destination server is earlier than that of the source server, you cannot migrate databases. Make sure that you install the HiCommand products whose versions are equal to or later than those of the HiCommand products installed on the source server.
- You cannot migrate the Replication Monitor server database for the Replication Monitor version 4.0 and 4.2. If you need to do this, we recommend that you upgrade to Replication Monitor 5.0 or later on both the source and destination servers in advance.
- When migrating the database for Tuning Manager, the following restrictions apply:
  - You can migrate the database when the database configurations (small or medium) of the source and destination servers are the same, or when the database configuration of the destination server is larger than that of the source server.
  - You cannot migrate the database to the same database configuration when, in the database configuration of the source server, the number of resources to be managed exceeds 70% of the maximum number that can be managed.

Notes on the user information:

- When there is user information on the destination server, that information will be replaced with that of the source server. Therefore, do not migrate databases to a machine that already has user information for HiCommand products.
- If you migrate the databases of the HiCommand products installed on a single management server in several operations, the user information is replaced each time you migrate the database and only the user information of the last-migrated product remains. When migrating multiple product databases, make sure that you migrate them in a single operation so that user information for all products is migrated.
- You cannot migrate the HiCommand products operating on multiple management servers and integrate them on a single management server because the user information is replaced.

Flow of procedures for a migrating database:

To migrate a database:

1. On the destination server, install the HiCommand product whose database is to be migrated.
2. On the source server, export the database (using the hcmdsdbtrans command).
3. Transfer the archive file from the source server to the destination server.
4. On the destination server, import the database (using the hcmdsdbtrans command).

The following sections describe the details of each step, separately for Windows and Solaris. When you perform migration between different platforms, check the procedures for both Windows and Solaris, and then perform the migration.

Note:

The procedure shown below includes steps at which you must stop the HiCommand product services (daemons). However, the services (daemons) of the following HiCommand product versions cannot be stopped even if you execute the `hcmdssrv` command with the `stop` option specified.

For details on how to stop those services, see the manual for each product.

- Device Manager version 5.6 or earlier
- Tiered Storage Manager version 5.5 or earlier

6.9.1 Migration Procedures for Windows

6.9.1.1 Installing HiCommand products on the Destination Server

Install on the destination server every HiCommand product whose database is to be migrated. The version of the HiCommand products installed on the destination server must be equal to or later than the version of the HiCommand products installed on the source server.

6.9.1.2 Exporting the Database from the Source Server

This section describes the procedure for exporting the database from the source server.

To export the Replication Monitor server database, a folder for temporarily storing database information and a folder for storing an archive file are required. Make sure that both folders have as much capacity as the total size of the following three folders:

- The folder that stores the Replication Monitor server database
- The folder that stores the Device Manager server database
- The folder that stores the HiCommand Suite Common Component database, not including subfolders and files under the sys folder.

This capacity is the approximate estimate value when only the Replication Monitor server and Device Manager server databases are installed. If HiCommand products other than Replication Monitor and Device Manager are installed, take into account the capacity of their databases.

Note:

If the database exceeds 2GB, creation of an archive file will fail when the database is exported. In this case, transfer to the destination server the database information collected during the export processing, instead of an archive file.

To export the database on the source server:

1. Execute the following command to stop the HiCommand Suite Common Component service:

```
HiCommand-Suite-Common-Component-installation-folder\bin\hcmdssrv /stop
```

   Executing this command also stops the services of other HiCommand products.

2. Execute the following command at the command prompt to start HiRDB:

```
HiCommand-Suite-Common-Component-installation-folder\bin\hcmdsdbsrv /start
```

   An example of command execution is shown below:

```
C:\Program Files\HiCommand\Base\bin\hcmdsdbsrv /start
```

3. Execute the `hcmdsdbtrans` command at the command prompt:

   The default folder of the `hcmdsdbtrans` command is as follows:

```
HiCommand-Suite-Common-Component-installation-folder\bin\hcmdsdbtrans
```

   The command format is as follows:

```
hcmdsdbtrans /export /workpath work-folder /file archive-file
```

   An example of command execution is shown below:

```
C:\Program Files\HiCommand\Base\bin\hcmdsdbtrans /export /workpath D:\trans_work /file
D:\db_arc
```

Note:

When the command is successful, the work folder and its subfolders are emptied. Therefore, make sure you do not output the archive file to the work folder or one of its subfolders.

The `hcmdsdbtrans` command has the following options:

`workpath`:

Specify a work folder for temporarily storing database information. Specify a folder on the local disk by using the absolute path.

Note:

Specify an empty folder in the workpath option. If the specified folder is not empty, export processing will be canceled. If this happens, specifying an empty folder, and then re-execute the hcmdsdbtrans command.

`file`:

Specify the archive file of the database you are exporting by using the absolute path.

The following table lists and describes the actions that you need to take when an error message appears. If the message has an ID other than those in the following table, take the action recommended in the message.

Table 6.1 What to Do When an Error Message Appears During the Export (in Windows)

Message ID	Action Taken
KAPM05909-E	Collect maintenance information, and then contact Customer Support.
KAPM05910-E	Make sure that the product is installed correctly, and take appropriate action. If you cannot resolve the problem after taking the action, collect maintenance information, and then contact Customer Support.
KAPM05922-E	Free up enough disk space for the folder in which the archive file is stored. If you cannot resolve the problem even after doing this, collect maintenance information, and then contact Customer Support.
KAPM05923-E	Transfer the data stored in the folder specified by using the `workpath` option to the destination server, instead of the archive file.

4. Transfer the archive file to the destination server.

   If you cannot create an archive file, transfer all the files stored in the folder specified by using the `workpath` option.

6.9.1.3 Importing the Database at the Destination Server

Note:

If you are migrating the database to a Solaris server, follow the steps in section 6.9.2.3.

To import the database at the destination server:

1. Execute the following command at the command prompt to stop the HiCommand Suite Common Component service:

```
HiCommand-Suite-Common-Component-installation-folder\bin\hcmdssrv /stop
```

Executing this command also stops the services of other HiCommand products.

2. Execute the following command at the command prompt to start HiRDB:

```
HiCommand-Suite-Common-Component-installation-folder\bin\hcmdsdbsrv /start
```

An example of command execution is shown below:

```
C:\Program Files\HiCommand\Base\bin\hcmdsdbsrv /start
```

3. Execute the `hcmdsdbtrans` command at the command prompt:

The default folder of the `hcmdsdbtrans` command is as follows:

```
HiCommand-Suite-Common-Component-installation-folder\bin\hcmdsdbtrans
```

The command format is as follows:

```
hcmdsdbtrans /import /workpath work-folder /file archive-file [/type {ALL |
name-of-HiCommand-product-whose-database-to-be-migrated}]
```

An example of command execution is shown below:

```
C:\Program Files\HiCommand\Base\bin\hcmdsdbtrans /import /workpath D:\trans_work /file D:
\db arc /type ALL
```

The `hcmdsdbtrans` command has the following options:

`workpath`:

When importing by using an archive file:

Specify a folder in which the archive file is extracted. Specify a folder on the local disk, by using the absolute path. You must specify the `file` option when using the archive file.

Note:

Specify an empty folder in the workpath option. If the specified folder is not empty, import processing will be canceled. If this occurs, specify an empty folder, and then re-execute the `hcmdsdbtrans` command.

When importing by not using an archive file:

Specify the folder in which the database information transferred from the source server was stored. Do not specify the `file` option.

`file`:

Use an absolute path to specify the database archive file transferred from the source server. If the database information transferred from the source server is in the folder specified in the `workpath` option and the archive file has been extracted, you do not need to specify this option.

`type`:

Specify the name of the HiCommand products you are migrating. Only the databases of the products you specified are migrated.

You can use the `type` option to migrate databases only when all the databases of the products you specified exist in the archive file or in the folder specified in the `workpath` option, and all the specified products have been installed in the destination server. If there are any products that do not satisfy the requirements, the migration will not be performed.

When you migrate the Replication Monitor server database, specify `ReplicationMonitor`. For details on names that you need to specify when migrating databases for other products, see the manual for each product. If you specify more than one product, use a comma to separate the names. Specify `ALL` to migrate the databases of all installed HiCommand products in a batch. The databases of the HiCommand products installed on the destination server are automatically selected and migrated.

Note:

You cannot migrate a database if Replication Monitor 4.0 or 4.2 is installed on the source server. We recommend that you upgrade to Replication Monitor 5.0 or later on both the source and destination servers, and then migrate the database. If you cannot upgrade Replication Monitor to 5.0 or later or if you do not need to migrate the database, use the type option to specify all products other than Replication Monitor, and then execute the command.

The following table lists and describes the actions that you need to take when an error message appears. If the message has an ID other than those in the following table, take the action recommended in the message.

Table 6.2 What to Do When an Error Message Appears During the Import (In Windows)

Message ID	Action Taken
KAPM05909-E	Collect maintenance information, and then contact Customer Support.
KAPM05910-E	Make sure that the product is installed correctly, and take appropriate action. If you cannot resolve the problem, collect maintenance information, and then contact Customer Support.
KAPM05911-E	Check the version of the product. If the version is not subject to migration, use the type option to import products other than the relevant product.
KAPM05913-E	Perform either of the following operations: ▪ Install the product that has not been installed on the destination server. ▪ Use the type option to import only the products that are already installed on the destination server.
KAPM05914-E	Specify only the products that exist in the archive file or in the folder specified in the `workpath` option.
KAPM05915-E	Check the data to be imported.
KAPM05916-E	Check the data to be imported and the settings of the server to which the data is imported.
KAPM05921-E	Check the following, and then take appropriate action: ▪ There is sufficient disk space for the folder specified in the `workpath` option. ▪ The archive file is the one specified in the `hcmdsdbtrans` command. If you cannot resolve the problem, collect maintenance information, and then contact Customer Support.
KAPM05926-E	▪ When the `file` option has been specified: Check whether the specified archive file is the one specified in the `hcmdsdbtrans` command. ▪ When the file option has not been specified: Check whether all the contents of the archive file are extracted in the folder specified in the `workpath`

	option, or whether the database information transferred from the source server is stored in that folder. If you cannot resolve the problem after taking the action, collect maintenance information, and then contact Customer Support.

4. Synchronize the repository data with the information in the imported Device Manager server database.

   Specify `true` in the `server.base.initialsynchro` property in the server.properties file.

   The `hcmdsdbtrans` command does not migrate HiCommand Suite Common Component repositories other than user information. Therefore, you must synchronize the repository data with the information in the imported Device Manager server database.

   For details about the `server.base.initialsynchro` property, see the *HiCommand Device Manager Server Installation and Configuration Guide*.

5. Execute the following command at the command prompt to restart the HiCommand Suite Common Component service:

```
HiCommand-Suite-Common-Component-installation-folder\bin\hcmdssrv /stop
HiCommand-Suite-Common-Component-installation-folder\bin\hcmdssrv /start
```

6. Start the Replication Monitor Web Client and collect the configuration information again.

   For details on how to collect configuration information again, see section 3.7.

   Note:

   To collect the configuration information again, Device Manager services must be running.

6.9.2 Migration Procedures for Solaris

6.9.2.1 Installing HiCommand Products in the Destination Server

Install on the destination server every HiCommand product whose database is to be migrated. The version of the HiCommand products installed on the destination server must be equal to or later than the version of the HiCommand products installed on the source server.

6.9.2.2 Exporting the Database from the Source Server

This section describes the procedure for exporting the database from the source server.

To export the Replication Monitor server database, a directory for temporarily storing database information and a directory for storing an archive file are required. Make sure that both directories have as much capacity as the total size of the following three directories:

- The directory that stores the Replication Monitor server database
- The directory that stores the Device Manager server database

- The directory that stores the HiCommand Suite Common Component database, not including subdirectories and files under the sys directory.

This capacity is the approximate estimate value when only the Replication Monitor server and Device Manager server databases are installed. If HiCommand products other than Replication Monitor and Device Manager are installed, take into account the capacity of their databases.

Note:

If the database exceeds 2GB, creation of an archive file will fail when the database is exported. In this case, transfer to the destination server the database information collected during the export processing, instead of an archive file.

To export the database from the source server:

1. Execute the following command from the terminal window to stop the HiCommand Suite Common Component daemon:

```
# /opt/HiCommand/suitesrvcntl -stop_all
```

   Executing this command also stops the daemons of other HiCommand products.

2. Execute the following command from the terminal window to start HiRDB:

```
# /opt/HiCommand/Base/bin/hcmdsdbsrv -start
```

3. Execute the `hcmdsdbtrans` command from the terminal window.

   The default directory of the `hcmdsdbtrans` command is as follows:

```
# /opt/HiCommand/Base/bin/hcmdsdbtrans
```

   The command format is as follows:

```
hcmdsdbtrans -export -workpath work-directory -file archive-file
```

   An example of command execution is shown below:

```
# /opt/HiCommand/Base/bin/hcmdsdbtrans -export -workpath /var/trans_work -file /var/db_arc
```

   The `hcmdsdbtrans` command has the following options:

   `workpath`:

   Specify a folder for temporarily storing database information. Specify a directory on the local disk by using the absolute path.

   Note:

   Specify an empty directory in the workpath option. If the specified directory is not empty, export processing will be canceled. If this occurs, specify an empty directory, and then re-execute the hcmdsdbtrans command.

   `file`:

   Specify the archive file of the database you are exporting by using the absolute path.

The following table lists and describes the actions that you need to take when an error message appears. If the message has an ID other than those in the following table, take the action recommended in the message.

Table 6.3 What to Do When an Error Message Appears During the Export (in Solaris)

Message ID	Action Taken
KAPM05909-E	Collect maintenance information, and then contact Customer Support.
KAPM05910-E	Make sure that the product is installed correctly, and take appropriate action. If you cannot resolve the problem after taking the action, collect maintenance information, and then contact Customer Support.
KAPM05922-E	Free up enough disk space for the folder in which the archive file is stored. If you cannot resolve the problem even after doing this, collect maintenance information, and then contact Customer Support.
KAPM05923-E	Transfer the data stored in the folder specified by using the `workpath` option to the destination server, instead of the archive file.

4. Transfer the archive file to the destination server.

   If you cannot create an archive file, transfer all the files stored in the directory specified by using the `workpath` option.

6.9.2.3 Importing the Database at the Destination Server

Note:

If you are migrating the database to a Windows server, follow the steps in section 6.9.1.3.

To import the database at the destination server:

1. Execute the following command from the terminal window to stop the HiCommand Suite Common Component daemon.

```
# /opt/HiCommand/suitesrvcntl -stop_all
```

   Executing this command also stops the daemons of other HiCommand products.

2. Execute the following command from the terminal window to start HiRDB:

```
# /opt/HiCommand/Base/bin/hcmdsdbsrv -start
```

3. Execute the `hcmdsdbtrans` command from the terminal window.

   The default directory of the `hcmdsdbtrans` command is as follows:

```
# /opt/HiCommand/Base/bin/hcmdsdbtrans
```

   The command format is as follows:

```
hcmdsdbtrans -import -workpath work-directory [-file archive-file] [-type {ALL |
name-of-HiCommand-product-whose-database-is-to-be-migrated}]
```

   An example of command execution is shown below:

```
# /opt/HiCommand/Base/bin/hcmdsdbtrans -import -workpath /var/trans_work -file /var/db arc
```

The `hcmdsdbtrans` command has the following options:

`workpath`:

When importing by using an archive file:

Specify a directory in which the archive file is extracted. Specify a directory on the local disk, by using the absolute path. You must specify the `file` option when using the archive file.

Note:

Specify an empty directory in the `workpath` option. If the specified directory is not empty, import processing will be canceled. If this occurs, specify an empty directory, and then re-execute the `hcmdsdbtrans` command.

When importing by not using an archive file:

Specify the directory in which the database information transferred from the source server was stored. Do not specify the `file` option.

`file`:

Specify the database archive file transferred from the source server by using the absolute path. If the database information transferred from the source server is in the directory specified in the `workpath` option and the archive file has been extracted, you do not need to specify this option.

`type`:

Specify the name of the HiCommand products you are migrating. Only the databases of the products you specified are migrated.

You can use the `type` option to migrate databases only when all the databases of the products you specified exist in the archive file or in the directory specified in the `workpath` option, and all the specified products have been installed in the destination server. If there are any products that do not satisfy the requirements, the migration will not be performed.

When you migrate the Replication Monitor server database, specify any of the following names: `DeviceManager`, `GlobalLinkAvailabilityManager`, `NASManager`, `ReplicationMonitor`, `TieredStorageManager`, or `TuningManager`. If you specify more than one product, separate the names with commas. Specify `ALL` to migrate the databases of all installed HiCommand products in a batch. The databases of the HiCommand products installed on the destination server are automatically selected and migrated.

Note:

You cannot migrate a database if Replication Monitor 4.0 or 4.2 is installed on the source server.

We recommend that you upgrade to Replication Monitor 5.0 or later on both the source and destination servers. If you cannot upgrade to 5.0 or later, or if you do not need to migrate the database, use the `type` option to specify all products other than Replication Monitor, and then execute the command.

The following table lists and describes the actions that you need to take when an error message appears. If the message has an ID other than those in the following table, take the action recommended in the message.

Table 6.4 What to Do When an Error Message Appears During the Import (In Solaris)

Message ID	Action Taken
KAPM05909-E	Collect maintenance information, and then contact Customer Support.
KAPM05910-E	Make sure that the product is installed correctly, and take appropriate action. If you cannot resolve the problem, collect maintenance information, and then contact Customer Support.
KAPM05911-E	Check the version of the product. If the version is not subject to migration, use the type option to import products other than the relevant product.
KAPM05913-E	Perform either of the following operations: ▪ Install the product that has not been installed on the destination server. ▪ Use the type option to import only the products that are already installed on the destination server.
KAPM05914-E	Specify only the products that exist in the archive file or in the folder specified in the `workpath` option.
KAPM05915-E	Check the data to be imported.
KAPM05916-E	Check the data to be imported and the settings of the server to which the data is imported.
KAPM05921-E	Check the following, and then take appropriate action: ▪ There is sufficient disk space for the folder specified in the `workpath` option. ▪ The archive file is the one specified in the `hcmdsdbtrans` command. If you cannot resolve the problem, collect maintenance information, and then contact Customer Support.
KAPM05926-E	▪ When the `file` option has been specified: Check whether the specified archive file is the one specified in the `hcmdsdbtrans` command. ▪ When the file option has not been specified: Check whether all the contents of the archive file are extracted in the folder specified in the `workpath` option, or whether the database information transferred from the source server is stored in that folder. If you cannot resolve the problem after taking the action, collect maintenance information, and then contact Customer Support.

4. Synchronize the repository data with the information in the imported Device Manager server database.

   Specify `true` in the `server.base.initialsynchro` property in the `server.properties` file.

   The `hcmdsdbtrans` command does not migrate HiCommand Suite Common Component repositories other than user information. Therefore, you must synchronize the repository data with the information in the imported Device Manager server database.

   For details about the `server.base.initialsynchro` property, see the *HiCommand Device Manager Server Installation and Configuration Guide*.

5. Execute the following command from the terminal window to restart the HiCommand Suite Common Component daemon.

```
# /opt/HiCommand/Base/bin/hcmdssrv -stop
# /opt/HiCommand/Base/bin/hcmdssrv -start
```

6. Start the Replication Monitor Web Client and collect the configuration information again.

For details on how to collect configuration information again, see section 3.7.

Note:

To collect the configuration information again, the Device Manager daemon must be running.

6.10 Tuning the Property File Settings

This section describes the parameter settings in Replication Monitor's property files and how to change the settings.

6.10.1 Replication Monitor-Related Parameters

The parameters required for Replication Monitor operations are set in the following property files that are stored in the management server or pair management server:

- Property files that are stored in the management server

  `logger.properties` file

  `serverstorageif.properties` file

  `bcmif.properties` file

  `agentif.properties` file

  `base.properties` file

  These files are stored in the following directory:

  For a Windows system

  Replication-Monitor-installation-directory`\conf`

  For a Solaris system

  `/opt/HiCommand/ReplicationMonitor/conf`

- Property files that are stored in the pair management server

  `server.properties` file

  This file is stored in the following directory:

  For a Windows system

  HiCommand-Agent-installation-directory`\agent\config`

  For a Solaris, HP-UX, or Linux system

  `/opt/HDVM/HBaseAgent/agent/config`

  For an AIX system

  `/usr/HDVM/HBaseAgent/agent/config`

  `agent.properties` file

  This file is stored in the following directory:

  For a Windows system

  HiCommand-Agent-installation-directory`\mod\hrpm\config`

  For a Solaris, HP-UX, or Linux system

  `/opt/HDVM/HBaseAgent/mod/hrpm/config`

  For an AIX system

  `/usr/HDVM/HBaseAgent/mod/hrpm/config`

Note that the `agent.properties` file exists only when the Replication Monitor agent is installed.

In this section, both the Device Manager agent and the Replication Monitor agent are called *HiCommand Agent* when they are installed on the pair management server.

After the start of Replication Monitor operation, you can change the parameters in the property files as needed. Note that inappropriate changes may result in unexpected operations. We recommend that you use the default values unless they lead to operational problems.

To change the parameters in the property files, use a text editor.

- If you change the parameters in the property files that are stored in the management server, you must restart the services of the Device Manager server and HiCommand Suite Common Component.
- If the management server is operated in a cluster environment, it is necessary to specify the same values in the property files of both the executing node and the standby node. If you change the values in the property file of the executing node, you must also change the values in the property file of the standby node (so the values are the same for both nodes).
- If you change the parameters in the property files that are stored in the pair management server, you must restart the Device Manager agent's service.

The following table lists the parameters and their default values in each property file:

Table 6.5 List of Replication Monitor-Related Parameters

Property file	Location of property file	Parameter	Default value (unit)
`logger.properties`	Management server	`logger.loglevel`	20
		`logger.sysloglevel`	0
		`logger.MaxBuckupIndex`	10 (files)
		`logger.MaxFileSize`	`4 MB`
`serverstorageif.properties`	Management server	`ssif.socketTimeout`	3600 (seconds)
		`ssif.socketConnectTimeout`	5 (seconds)
		`ssif.alertTimeout`	1800 (seconds)
`bcmif.properties`	Management server	`bcmif.socketTimeout`	3600 (seconds)
		`bcmif.socketConnectTimeout`	5 (seconds)
		`bcmif.ReconnectionInterval`	60 (seconds)
		`bcmif.ReconnectionCount`	5 (count)
`agentif.properties`	Management server	`agentif.connectTimeout` #	30 (seconds)
		`agentif.responseTimeout` #	3600 (seconds)
		`agentif.agentPort`	24041

Property file	Location of property file	Parameter	Default value (unit)
		hdvmagtif.connectTimeout #	30 (seconds)
		hdvmagtif.responseTimeout #	3600 (seconds)
		hdvmagtif.MaxPollingCount #	50 (count)
		hdvmagtif.PollingInterval #	30 (seconds)
base.properties	Management server	base.repositry.synchronize.polling	false
server.properties	Pair management server	server.agent.maxMemorySize #	64 (MB)
		server.agent.shutDownTime #	600000 (milliseconds)
		server.http.socket.bindAddress	Blank
		server.http.socket.agentAddress #	IP address acquired by the HiCommand Agent
		server.http.port	24042
		server.agent.port	24041
		server.http.security.clientIP	*.*.*.*
		server.agent.rm.exclusion.instance	Blank
		server.agent.rm.location	For a Windows system: *HiCommand-Agent-installation-drive*/HORCM For a UNIX system: /HORCM
agent.properties	Pair management server	agent.rm.TimeOut #	600 (seconds)
		agent.rm.everytimeShutdown #	false
		agent.rm.shutdownWait	5 (seconds)
		agent.rm.horcmInstance	4094
		agent.rm.horcmService	54323
		agent.rm.horcmSource	Windows system: Value obtained by converting \ in %WINDIR% to /. UNIX system: /etc
		agent.logger.loglevel	INFO
		agent.logger.MaxBackupIndex	5
		agent.logger.MaxFileSize	1 MB

Normally, the values set for these parameters do not need to be changed. To change their values, you need expert knowledge of agents.

6.10.2 Parameters in the logger.properties File

The `logger.properties` file is used to set the values of log output-related parameters.

The following table lists and describes the parameter settings in the `logger.properties` file:

Table 6.6 List of Parameters in the logger.properties File

Parameter	Setting
`logger.loglevel`	The threshold value for the Replication Monitor server's log file output level Messages with values that are equal to or less than this threshold value are output to the log file. The permitted values, in decreasing order of importance, are 0, 10, 20, and 30.
`logger.sysloglevel`	The threshold value for the Replication Monitor server's event log or `syslog` output level Messages with values that are equal to or less than this threshold value are output to the log file. The permitted values, in decreasing order of importance, are 0, 10, 20, and 30.
`logger.MaxBackupIndex`	The number of Replication Monitor server's log file generations Maximum number of log files that can be created. When the number of log files reaches this value, the existing files are reused, starting at the first file. The permitted value range is from 1 to 16.
`logger.MaxFileSize`	The size of the Replication Monitor server's log file Maximum size of a single log file. The value must be specified in bytes, kilobytes, or megabytes. If the specified value is not followed by KB or MB, it is treated as bytes. The permitted value range is from 4096 to 2147483647 bytes, from 4 KB to 2097151 KB (kilobytes), or from 1 MB to 2047 MB (megabytes).

About the log information size output by the Replication Monitor server

The information size output to the Replication Monitor server log files depends on the number of copy pairs monitored by Replication Monitor. The following table lists the number of monitored copy pairs and the output log information size.

Table 6.7 Number of Monitored Copy Pairs and Output Log Information Size

Number of monitored copy pairs	Output log information size
0–1,000	40 MB
1,001–3,000	120 MB
3,001–5,000	200 MB

Check and change (if necessary) the settings of the `logger.MaxFileSize` parameter and the `logger.MaxBackupIndex` parameter in the `logger.properties` file, according to the number of monitored copy pairs.

Example:

If the number of monitored copy pairs is 2,500 and the maximum log file size is 10 MB, set the parameters as follows:

- `logger.MaxFileSize` parameter: 10 MB
- `logger.MaxBackupIndex` parameter: 12

If the number of copy pairs you want to monitor is 5,001 or more, calculate the output log information size by using the following formula:

```
output-log-information-size (MB) = number-of-copy-pairs / 1,000 * 40
```

6.10.3 Parameters in the serverstorageif.properties File

The `serverstorageif.properties` file is used to set the value of parameters that are related to the interface between the Replication Monitor server and Device Manager server.

The following table lists and describes the parameter settings in the `serverstorageif.properties` file:

Table 6.8 List of Parameters in the serverstorageif.properties File

Parameter	Setting
`ssif.socketTimeout`	The time for blocking the data from the Device Manager server (seconds) The permitted value range is from 0 to 86400. A value of 0 means the blocking time is undefined.
`ssif.socketConnectTimeout`	The wait time when the Replication Monitor server connects to the Device Manager server (seconds) The permitted value range is from 0 to 3600. A value of 0 means that no timeout occurs.
`ssif.alertTimeout`	The wait time when an alert message query is issued to the Device Manager server (seconds) The permitted value range is from 1 to 3600.

6.10.4 Parameters in the bcmif.properties File

The `bcmif.properties` file is used to set the values of parameters that are related to the interface between the Replication Monitor server and Business Continuity Manager.

The following table lists and describes the parameter settings in the `bcmif.properties` file:

Table 6.9 List of Parameters in the bcmif.properties File

Parameter	Setting
`bcmif.socketTimeout`	The time for blocking the data from Business Continuity Manager (seconds) The permitted value range is from 0 to 86400. A value of 0 means the blocking time is undefined.
`bcmif.socketConnectTimeout`	The wait time when the Replication Monitor server connects to Business Continuity Manager (seconds) The permitted value range is from 0 to 3600. A value of 0 means that no timeout occurs.
`bcmif.ReconnectionInterval`	The retry interval when the Replication Monitor server's attempt to establish a connection with Business Continuity Manager fails (seconds) The permitted value range is from 0 to 1800. A value of 0 means an immediate retry.
`bcmif.ReconnectionCount`	The retry count when the Replication Monitor server's attempt to establish a connection with Business Continuity Manager fails (count) The permitted value range is from 0 to 100. A value of 0 means the retry count is undefined.

6.10.5 Parameters in the agentif.properties File

The `agentif.properties` file is used to set the values of parameters that are related to the interface between the Replication Monitor server and HiCommand Agent.

The following table lists and describes the parameter settings in the `agentif.properties` file:

Table 6.10 List of Parameters in the agentif.properties File

Parameter	Setting
`agentif.connectTimeout` #1	The wait time for the Replication Monitor server to connect to a Replication Monitor agent (seconds) The permitted value range is from 0 to 3600. A value of 0 means that no timeout occurs.
`agentif.responseTimeout` #1	The wait time for the Replication Monitor server to receive a reply from the Replication Monitor agent (seconds) The permitted value range is from 0 to 86400. A value of 0 means that no timeout occurs.
`agentif.agentPort`	The TCP port number used when the Replication Monitor server connects to the daemon (or service) of a Replication Monitor agent or Device Manager agent (HiCommand Agent) The permitted value range is from 1024 to 49151. This value must match the value of `server.agent.port` in `server.properties`.
`hdvmagtif.connectTimeou`	The wait time for the Replication Monitor server to connect to a Device Manager agent

Parameter	Setting
t[#1 #2]	(seconds) The permitted value range is from 0 to 3600. A value of 0 means that no timeout occurs.
hdvmagtif.responseTimeout[#1 #2]	The wait time for the Replication Monitor server to receive a reply from the Device Manager agent (seconds) The permitted value range is from 0 to 86400. A value of 0 means that no timeout occurs.
hdvmagtif.MaxPollingCount[#1 #2]	The maximum polling count after a request from the Replication Monitor server to a Device Manager agent times out The permitted value range is from 0 to 100. A value of 0 means an unlimited count.
hdvmagtif.PollingInterval[#1 #2]	The polling interval after a request from the Replication Monitor server to a Device Manager agent times out (seconds) The permitted value range is from 5 to 1200.

#1 Normally, the values set for these parameters do not need to be changed. To change their values, you need expert knowledge of agents.

#2 If you upgraded from Replication Monitor version 5.0, 5.5, or 5.6, the setting is not written in the property file.

6.10.6 Parameters in the base.properties File

The `base.properties` file is a property file to which the parameter values that are related to internal processing of the Replication Monitor server are to be set.

Table 6.11 List of Parameters in the base.properties File

Parameter	Setting
base.repositry.synchronize.polling	The setting that specifies whether Replication Monitor performs synchronization with the Device Manager server database The parameter can be set to `true` or `false`. The value `true` specifies that Replication Monitor performs synchronization. The value `false` specifies that Replication Monitor does not perform synchronization.

6.10.7 Parameters in the server.properties file

The `server.properties` file is a property file that stores the values of the parameters used by HiCommand Agent.

Note:

You must pay particular attention when you change the parameters in the `server.properties` file because this file is shared with the Device Manager agent, and this change might affect the Device Manage agent.

The following table lists and describes the parameter settings in the `server.properties` file:

Table 6.12 List of Parameters in the server.properties File

Parameter	Setting
server.agent.maxMemorySize #1	The maximum size of the memory heap to be used by the process of the Web server function of the Device Manager agent (MB) The permitted value range is from 32 to 4096. If this value is omitted, 64 MB will be assumed.
server.agent.shutDownTime #1	Length of time until HiCommand Agent's Web server function stops after sending or receiving the last HTTP/XML message (milliseconds) A value of 0 or less means the shutdown time is undefined.
server.http.socket.bindAddress	If HiCommand Agent is run on a platform where more than 1 network interface (NIC) is installed, this parameter specifies the NIC from which HiCommand Agent can accept requests (IP address: dotted decimal format). A blank means that HiCommand Agent can accept requests from any NIC.
server.http.socket.agentAddress #1	IP address that is reported from HiCommand Agent to Device Manager Server (IP address: dotted decimal format)
server.http.port	TCP port number used by HiCommand Agent's Web server function The permitted value range is from 1024 to 49151.
server.agent.port	TCP port number used by HiCommand Agent's daemon (service) The permitted value range is from 1024 to 49151. If this value is changed, the value of agentif.agentPort in agentif.properties must also be changed.
server.http.security.clientIP	IP address for connecting to HiCommand Agent (IP address: dotted decimal format) A wildcard (*) can be specified. To specify multiple values, separate each value with a comma (,).
server.agent.rm.exclusion.instance #2	CCI instance number specified for excluding from management by Device Manager a volume pair already being managed by CCI on a host that has a Device Manager agent installed. To specify multiple instance numbers, separate each number with a comma (,).
server.agent.rm.location	CCI installation directory For Windows, use a forward slash (/) as a delimiter for directories, not a backslash (\).

#1 Normally, the values set for these parameters do not need to be changed. To change their values, you need expert knowledge of agents.

#2 When an instance number is specified in server.agent.rm.exclusion.instance, neither the configuration definition file for the specified instance number nor any of the pair information contained in that file appear in the **Pair Configurations** view.

6.10.8 Parameters in the agent.properties File

The agent.properties file is a property file that stores the values of the parameters used by the Replication Monitor agent.

The table below shows the setting details for the parameters of the agent.properties file.

Table 6.13 Parameters of the agent.properties File

Parameter	Setting details
agent.rm.TimeOut #1	Time limit for a response from the CCI command used by the Replication Monitor agent (in seconds) A value between 0 and 86400 can be set. 0 means no time-out.
agent.rm.everytimeShutdown #1	Setting for whether to stop the HORCM instance for monitoring#2 every time Specify true or false. If true is specified, the instance stops every time. If false is specified, the instance does not stop
agent.rm.shutdownWait	Wait time when stopping the HORCM instance for monitoring#2 (in seconds) A value between 1 and 60 can be set.
agent.rm.horcmInstance	Instance number of the HORCM file for monitoring#2 A value between 0 and 4094 can be set. This value must be different from the instance number of the configuration definition file of another CCI. Do not set a value from 990 to 998 because Device Manager agent uses these values.
agent.rm.horcmService	UDP port number of the HORCM file for monitoring#2 A value between 0 and 65535 can be set. This value must be different from the port number of another application. Do not set a value from 53232 to 53330 because Device Manager agent uses these values.
agent.rm.horcmSource	Location (directory) of the configuration definition file of the existing CCI Use ASCII characters to specify a file location (directory).
agent.logger.loglevel	Log file output level for the Replication Monitor agent Logs that have levels equal to or higher than the value specified here are output. The following values (listed in ascending order of importance) can be specified: DEBUG, INFO, WARN, ERROR, FATAL
agent.logger.MaxBackupIndex	Number of generations of log files for the Replication Monitor agent Maximum number of log files to be generated. When the number of log files generated reaches this value, the log files are reused, beginning with the oldest one. A value between 1 and 20 can be set.
agent.logger.MaxFileSize	Size of log files for the Replication Monitor agent Maximum size of each log file. A value between 512 KB and 32 MB can be set. You can specify the value in bytes, kilobytes, or megabytes. If no unit is specified for the number, it is assumed to be in bytes.

#1 Normally, the values set for these parameters do not need to be changed. To change their values, you need expert knowledge of the Replication Monitor agent.

#2 The HORCM instance for monitoring means an instance of CCI used by the Replication Monitor agent. The HORCM file for monitoring means the configuration definition file of that CCI.

6.11 Generating Audit Logs

Audit logs for Replication Monitor and other Hitachi storage-related products can be generated in order to prove to auditors and evaluators the compliance with regulations, security evaluation standards, and other business standards. The following table lists and describes the categories of audit log data that can be generated from Hitachi storage-related products.

Table 6.14 Categories and Descriptions

Categories	Description
`StartStop`	Events indicating starting or stopping of hardware or software. ▪ Starting or shutting down an OS ▪ Starting or stopping a hardware component (including micro components) ▪ Starting or stopping software on Hitachi disk array subsystems or SVP, and HiCommand Suite products
`Failure`	Events indicating hardware or software failures. ▪ Hardware failures ▪ Software failures (memory error, etc.)
`LinkStatus`	Events indicating link status among devices. ▪ Whether a link is up or down
`ExternalService`	Events indicating communication results between Hitachi storage-related products and external services. ▪ Communication with a RADIUS, LDAP, NTP, and DNS server ▪ Communication with a management server (SNMP)
`Authentication`	Events indicating that a device, administrator, or end user succeeded or failed in connection or authentication. ▪ FC login ▪ Device authentication (FC-SP authentication, iSCSI login authentication, SSL server/client authentication) ▪ Administrator or end user authentication
`AccessControl`	Events indicating that a device, administrator, or end user succeeded or failed in gaining access to resources. ▪ Access control for devices (IP/FC LUN Security) ▪ Access control for the administrator or end users
`ContentAccess`	Events indicating that attempts to access important data succeeded or failed. ▪ Access to important files on NAS or to contents when HTTP is supported ▪ Access to audit logs
`ConfigurationAccess`	Events indicating that the administrator succeeded or failed in performing an allowed operation. ▪ Reference or update of the configuration information ▪ Update of account settings including addition or deletion of accounts ▪ Security configuration ▪ Reference or update of audit log settings
`Maintenance`	Events indicating that a performed maintenance operation succeeded or failed.

Categories	Description
	▪ Addition or deletion of hardware components ▪ Addition or deletion of software components
AnomalyEvent	Events indicating that anomalies such as a threshold excess occurred. ▪ Excess over network traffic threshold ▪ Excess over CPU load threshold ▪ Over-limit pre-notification or wraparound of audit log data temporarily saved internally
	Events indicating that abnormal communication occurred. ▪ SYN flood attacks to a regularly used port, or protocol violations ▪ Access to an unused port (port scanning, etc.)

Different products generate different types of audit log data. The following sections describe the audit log data that can be generated by using Replication Monitor. For details on the audit log data generated by other products, see the manual for the corresponding product.

6.11.1 Categories of Information Output to Audit Logs in Replication Monitor

The following table lists the categories of information output to audit logs in Replication Monitor and the audit events. Each audit event is assigned a severity level. You can filter audit log data to be output according to the severity levels of events.

Table 6.15 Categories of Information Output to Audit Logs, and Audit Events

Category	Type Description	Audit Event	Severity
StartStop	Start and stop of software	Successful SSO server start	6
		Failed SSO server start	3
		SSO server stop	6
Authentication	Administrator or end user authentication	Successful login	6
		Failed login (wrong user ID or password)	4
		Failed login (logged in as a locked user)	4
		Failed login (logged in as a non-existing user)	4
		Failed login (no permission)	3
		Failed login (authentication failure)	4
		Successful logout	6
	Automatic account lock	Automatic account lock (repeated authentication failure or expiration of account)	4
Configuration Access	User registration	Successful user registration	6
		Failed user registration	3
	User deletion	Successful single user deletion	6
		Failed single user deletion	3

Category	Type Description	Audit Event	Severity
		Successful multiple user deletion	6
		Failed multiple user deletion	3
	Password change (from the administrator panel)	Successful password change by the administrator	6
		Failed password change by the administrator	3
	Password change (from the user's own panel)	Failed in authentication processing for verifying old password	3
		Successful change of login user's own password (from the user's own panel)	6
		Failed change of login user's own password (from the user's own panel)	3
	Profile change	Successful profile change	6
		Failed profile change	3
	Permission change	Successful permission change	6
		Failed permission change	3
	Account lock	Successful account lock	6
		Failed account lock	3
	Account lock release	Successful account lock release	6
		Failed account lock release	3
	Database backup or restore	Successful backup using the `hcmdsdb` command	6
		Failed backup using the `hcmdsdb` command	3
		Successful full restore using the `hcmdsdb` command	6
		Failed full restore using the `hcmdsdb` command	3
		Successful partial restore using the `hcmdsdb` command	6
		Failed partial restore using the `hcmdsdb` command	3
	Database input/output	Successful data output using the `hcmdsdbmove` command	6
		Failed data output using the `hcmdsdbmove` command	3
		Successful data input using the `hcmdsdbmove` command	6
		Failed data input using the `hcmdsdbmove` command	3
	Database area creation or deletion	Successful database area creation using the `hcmdsdbsetup` command	6
		Failed database area creation using the `hcmdsdbsetup` command	3
		Successful database area deletion using the `hcmdsdbsetup` command	6
		Failed database area deletion using the `hcmdsdbsetup` command	3
	Authentication data input/output	Successful data output using the `hcmdsdbauthmove` command	6

Category	Type Description	Audit Event	Severity
		Failed data output using the hcmdsdbauthmove command	3
		Successful data input using the hcmdsdbauthmove command	6
		Failed data input using the hcmdsdbauthmove command	3

6.11.2 Editing Audit Log Environment Settings File

To generate Replication Monitor audit log data, you must edit the environment settings file (auditlog.conf). The audit log data can be generated by setting audit event categories, in Log.Event.Category of the environment settings file. For Windows, the audit log data is output to an event log file (the application log file). For Solaris(TM) , the data is output to the syslog file.

Caption: A large volume of audit log data might be output. Change the log size and back up or archive the generated logs accordingly.

The following describes the storage destination for the auditlog.conf file.

- For Windows(R):

```
installation-folder-for-HiCommand-Suite-Common-Component\conf\sec\auditlog.conf
```

- For Solaris(TM):

```
/opt/HiCommand/Base/conf/sec/auditlog.conf
```

The table below shows the items that are set for the auditlog.conf file.

Table 6.16 Set for auditlog.conf

item	Description
Log.Facility	Specify (by using a number) the facility to be used when the audit log messages are output to the syslog file. Log.Facility is used, in combination with the severity levels set for each audit event (see Table 6.15), for filtering the output to the syslog file. For details about the values that can be specified for Log.Facility, see Table 6.17. For details about the correspondence between the severity levels set for audit events and those set in the syslog.conf file, see Table 6.18. Log.Facility has an effect in Solaris(TM) only. Log.Facility is ignored in Windows, even if it is specified. Also, if an invalid value or a non-numeric character is specified, the default value is used. Default value: 1
Log.Event.Category	Specify the audit event categories to be generated. When specifying multiple categories, use commas (,) to separate them. If Log.Event.Category is not specified, audit log data is not output. For information about the available categories, see Table 6.15. Log.Event.Category is not case-sensitive. If an invalid category name is specified, the specified file name is ignored. Default value: (not specified)
Log.Level	Specify the severity level of audit events to be generated. Events with the specified severity level or lower will be output to the event log. For information about the audit events that are output from Replication Monitor

item	Description
	and their severity levels, see Table 6.15. For details about the correspondence between the severity levels of audit events and the types of event log data, see Table 6.18. `Log.Level` has an effect in Windows(R) only. `Log.Level` is ignored in Solaris(TM), even if it is specified. Also, if an invalid value or a non-numeric character is specified, the default value is used. Specifiable values: `0` to `6` (severity level) Default value: `6`

The table below shows the values that can be set for Log.Facility and the corresponding values specified in the syslog.conf file.

Table 6.17 Log.Facility Values and the Corresponding Values in syslog.conf

Facility	Corresponding Values in syslog.conf
1	`user`
2	`mail`#
3	`daemon`
4	`auth`#
6	`lpr`#
16	`local0`
17	`local1`
18	`local2`
19	`local3`
20	`local4`
21	`local5`
22	`local6`
23	`local7`

Although you can specify this value, we do not recommend that you specify it.

The table below shows the correspondence between the severity levels of audit events, the values indicating severity that are specified in the `syslog.conf` file, and the types of event log data.

Table 6.18 Correspondence Between the Severity Levels of Audit Events, the Severity Levels in syslog.conf, and the Types of Event Log Data

Severity of Audit Events	Severity in syslog.conf	Type of Event Log Data
0	`emerg`	Error
1	`alert`	
2	`crit`	

3	err	
4	warning	Warning
5	notice	Information
6	info	
7	debug	

The following shows an example of the auditlog.conf file:

```
Log.Facility  1
Log.Event.Category  Authentication,ConfigurationAccess
Log.Level 6
```

In the example above, the audit events related to Authentication or ConfigurationAccess are output. For Windows(R), Log.Level 6 outputs audit log data corresponding to the Error, Warning, and Information levels. For Solaris(TM), Log.Facility 1 outputs the audit log to the syslog file that is defined as the user facility in the syslog.conf file.

6.11.3 Format of Output Audit Log Data

This subsection describes the format of output audit log data.

- For Windows(R):

  When you open an event by choosing **Event Viewer** and then **Application**, the following is displayed in the **Description** area in the **Event Properties**.

  ```
  program-name [process-ID]: message-portion
  ```

- For Solaris(TM):

  The contents of a syslog file

  ```
  date-time server-name (or IP-address) program-name [process-ID]: message-portion
  ```

The format and contents of audit log data that is output to *message-portion* are described below.

Note: In *message-portion*, a maximum of 953 single-byte characters are displayed.

The output format of message-portion:

```
uniform-identifier,unified-specification-revision-number,serial-number,message-ID,date-and-time,detected-entity,detected-location,audit-event-type,audit-event-result,audit-event-result-subject-identification-information,hardware-identification-information,location-information,location-identification-information,FQDN,redundancy-identification-information,agent-information,request-source-host,request-source-port-number,request-destination-host,request-destination-port-number,batch-operation-identifier,log-type-information,application-identification-information,reserved-area,message-text
```

Table 6.19 Information Output to message-portion

item[#1]	Description
uniform-identifier	Fixed to CELFSS.
unified-specification-revision-number	Fixed to 1.1.

item[#1]	Description
serial-number	Serial number of audit log messages.
message-ID[#2]	Message ID.
date-and-time	The date and time when the message was output. This item is output in the format of `yyyy-mm-ddThh:mm:ss.s`*time-zone*.
detected-entity	Component or process name.
detected-location	Host name.
audit-event-type	Event type.
audit-event-result	Event result.
audit-event-result-subject-identification-information	Account ID, process ID, or IP address corresponding to the event.
hardware- identification-information	Hardware model or serial number.
location-information	Identification information for the hardware component.
location-identification-information	Location identification information.
FQDN	Fully qualified domain name.
redundancy-identification-information	Redundancy identification information.
agent-information	Agent information.
request-source-host	Host name of the request sender.
request-source-port-number	Port number of the request sender.
request-destination-host	Host name of the request destination.
request-destination-port-number	Port number of the request destination.
batch-operation-identifier	Serial number of operations through the program.
log-type-information	Fixed to `BasicLog`.
application-identification-information	Program identification information.
reserved-area	Not output. This is a reserved space.
message-text[#2]	The contents vary according to the audit events.

#1 Some items are not output for some audit events.

#2 For details on the message ID and the message text, see the *HiCommand Replication Monitor Messages*.

Example of audit log data output for the Login audit event:

```
CELFSS,1.1,0,KAPM01124-I,2006-05-15T14:08:23.1+09:00,HBase-SSO,management-host,Authenticati
on,Success,uid=system,,,,,,,,,,,BasicLog,,,"The login process has completed properly."
```

Chapter 7 Creating a Cluster Environment

This chapter explains how to create a cluster environment for the management server of Replication Monitor.

- Overview and Requirements of a Cluster Environment (see section 7.1)
- Installing and Uninstalling Replication Monitor in an Existing Cluster Environment (see section 7.2)
- Changing Replication Monitor to a Cluster Environment After Starting Operation (see section 7.3)

7.1 Overview and Requirements of a Cluster Environment

Using cluster software, you can dualize the management server of Replication Monitor and build a cluster configuration. This is called a cluster environment.

Building a cluster environment enables you to enhance the availability of Replication Monitor.

Requirements for cluster environments supported by Replication Monitor are as follows:

OS

- In Windows:

  Microsoft® Windows® 2000 Advanced Server Operating System (SP4),

  Microsoft® Windows Server 2003, Enterprise Edition Operating System[#],

  Microsoft Windows Server 2003, Enterprise Edition Operating System (SP1),[#]

  Microsoft Windows Server 2003, Enterprise Edition Operating System (SP2)[#],

  Microsoft Windows Server 2003 R2, Enterprise Edition Operating System[#], or

  Microsoft Windows Server 2003 R2, Enterprise Edition Operating System (SP2)[#]
- In Solaris:

  Solaris 9 (32-bit or 64-bit kernel mode)

#

Only the x86 architecture is supported.

Cluster software

- In Windows:

  Microsoft Cluster Service (MSCS)
- In Solaris:

  VERITAS Cluster Server 4.0 (VCS)

  or

  Sun Cluster 3.1

Cluster configuration

Two-node Active - Standby configuration

Disk configuration and the Replication Monitor server installation destination (Windows)

All nodes comprising the cluster must have the same disk configuration and the same Replication Monitor server installation destination (the drive letter, path name, etc.).

The following two methods are available for building a cluster environment for the management server of Replication Monitor:

- Creating a cluster environment for the management server first and then installing Replication Monitor

Before installing Replication Monitor, if a HiCommand product such as Device Manager is operating in a cluster environment, use this method to create a cluster environment.

For details, see section 7.2.

- Installing the Replication Monitor server first and then changing the management server to a cluster environment

  If Replication Monitor is already operating in a non-cluster configuration, use this method to create a cluster environment.

  For details, see section 7.3.

Note:

The Replication Monitor agent cannot be registered in the cluster resources, because it does not support logical hosts. Replication Monitor agents run on the physical hosts in a cluster system, and collect information at the specific physical host. For details about supported operating systems and cluster software, see the *HiCommand Device Manager Agent Installation Guide*.

7.2 Installing and Uninstalling Replication Monitor in an Existing Cluster Environment

This section describes how to install and uninstall the Replication Monitor server in a cluster configuration where Device Manager has been installed. For details about how to change the configuration to a cluster configuration after operation of Replication Monitor is started in a non-cluster environment, see section 7.3.For details about how to set up a cluster configuration for Device Manager, see the *HiCommand Device Manager Server Installation and Configuration Guide*.

The explanation in this section assumes the following conditions:

- In Windows, Device Manager has been installed in `C:\Program Files\HiCommand\` both on the executing and standby nodes.
- The HiCommand product services are online on the executing node.
- A shared disk that can be accessed from both the executing and standby nodes and is registered in the cluster resources. Additionally, the HiCommand product database is stored in the shared disk.

7.2.1 New Installation

This section describes the procedures for a new installation of the Replication Monitor server.

7.2.1.1 In Windows

Installing on the Executing Node

To install Replication Monitor on the executing node when the OS is Windows:

1. Choose **Start**, **Settings**, **Control Panel**, **Administrative Tools**, and then **Cluster Administrator** to open the Cluster Administrator window, and then place the following services offline:
   - HiCommandServer
   - HBase Storage Mgmt Web Service
   - HBase Storage Mgmt Common Service

   Note:

   Do not place the following resources offline:

   - Shared disk

   - Cluster management IP address

   - Virtual host name

   If placed offline, the shared disk cannot be specified during installation.

   If the cluster management IP address or virtual host name is placed offline, installation will fail.

2. Execute the following command to stop the HiCommand Suite Common Component services:

```
"C:\Program Files\HiCommand\Base\bin\hcmdssrv" /stop
```

3. In the Cluster Administrator window, place the following service offline:

   HiRDB/ClusterService _HD0

4. In the Cluster Administrator window, right-click the services that were placed offline in steps 1 and 3, choose **Property**, click the **Advanced** tab, select **Do not restart**, and then click **OK**.

5. Install the Replication Monitor server.

   For details, see section 2.3.1.

6. Open the Services window by choosing **Start**, **Settings**, **Control Panel**, **Administrative Tools**, and **Services**, and then make sure that **Startup Type** for each of the following services is set to **Manual**. If **Startup Type** is set to **Automatic**, change it to **Manual**.

   - HBase Storage Mgmt Common Service
   - HBase Storage Mgmt Web Service
   - HiCommandServer
   - HiRDB/ClusterService _HD0

7. In the Cluster Administrator window, right-click the group to which the Device Manager service (HiCommandServer) has been registered, and then choose **Move Group** to switch to the standby node.

Installing on the Standby Node

To install Replication Monitor on the standby node when the OS is Windows:

1. Execute the following command to make sure that the HiCommand Suite Common Component services have stopped:

```
"C:\Program Files\HiCommand\Base\bin\hcmdssrv" /status
```

   If any of the HiCommand Suite Common Component services is running, use the Cluster Administrator window to place the HiRDB/ClusterService _HD0 service online, and then execute the following command:

```
"C:\Program Files\HiCommand\Base\bin\hcmdssrv" /stop
```

   After the services have stopped, use the Cluster Administrator window to place the HiRDB/ClusterService _HD0 service offline.

2. Install the Replication Monitor server.

   For details, see section 2.3.1.

3. Open the Services window by choosing **Start**, **Settings**, **Control Panel**, **Administrative Tools**, and **Services**, and then make sure that **Startup Type** for each of the following services are set to **Manual**. If **Startup Type** is set to **Automatic**, change it to **Manual**.

   - HBase Storage Mgmt Common Service
   - HBase Storage Mgmt Web Service
   - HiCommandServer

- HiRDB/ClusterService _HD0

4. In the Cluster Administrator window, right-click the following services, choose **Property**, click the **Advanced** tab, select **Restart**, and then click **OK**.
   - HBase Storage Mgmt Common Service
   - HBase Storage Mgmt Web Service
   - HiCommandServer
   - HiRDB/ClusterService _HD0
5. In the Cluster Administrator window, right-click the group to which the Device Manager service (HiCommandServer) has been registered, and then choose **Move Group** to switch to the executing node.
6. In the Cluster Administrator window, right-click the group to which the Device Manager service (HiCommandServer) has been registered, and then choose **Online**.

7.2.1.2 In Solaris

Preparation in VCS (VERITAS Cluster Server)

To prepare for an installation in a cluster environment for VERITAS Cluster Server:

1. On the executing node, start Cluster Manager (Java Console).
2. Place the following daemons offline:
   - HiCommandServer
   - HBase Storage Mgmt Web Service
   - HBase Storage Mgmt Common Service

   Note:

   Do not place the following resources offline:

   - Shared disk

   - Cluster management IP address

   - Virtual host name

   If the shared disk, cluster management IP address, or virtual host name is placed offline, installation will fail.
3. Execute the following command to stop the HiCommand Suite Common Component daemons:

```
# /opt/HiCommand/Base/bin/hcmdssrv -stop
```

4. Place the HiRDB daemon offline.
5. Right-click the following resources, and then clear **Enabled** from the popup menu.
   - HiCommandServer
   - HBase Storage Mgmt Common Service
   - HBase Storage Mgmt Web Service
   - HiRDB

6. In the Cluster Explorer window, click the **Service Groups** tab.
7. Select and right-click the group to which the Device Manager service has been registered, and then in the displayed popup menu, choose **Freeze**, and then **Temporary**.

Preparation in a Sun Cluster Environment

To prepare for an installation in a cluster environment for Sun Cluster:

1. On the executing node, execute the following commands to disable monitoring the resources for HiCommand Suite Common Component, Device Manager, and HiRDB:

```
# /usr/cluster/bin/scswitch -n -M -j HiCommandServer
# /usr/cluster/bin/scswitch -n -M -j MgmtWebService
# /usr/cluster/bin/scswitch -n -M -j MgmtComService
# /usr/cluster/bin/scswitch -n -M -j HiRDB
```

2. Execute the following commands to disable the resources for HiCommand Suite Common Component and Device Manager:

```
# /usr/cluster/bin/scswitch -n -j HiCommandServer
# /usr/cluster/bin/scswitch -n -j MgmtWebService
# /usr/cluster/bin/scswitch -n -j MgmtComService
```

3. Execute the following command to stop the HiCommand Suite Common Component daemons:

```
# /opt/HiCommand/Base/bin/hcmdssrv -stop
```

4. Execute the following command to disable the HiRDB resources:

```
# /usr/cluster/bin/scswitch -n -j HiRDB
```

Installing on the Executing Node

To install Replication Monitor on the executing node:

1. Install the Replication Monitor server.

   For details about installation, see section 2.4.1.

2. Switch the group to which the Device Manager service has been registered to the standby node.

   If using VERITAS Cluster Server, carry out step 3 only. If using Sun Cluster, go to step 4.

3. When using VERITAS Cluster Server, in the Cluster Explorer window click the **Service Groups** tab, select and right-click the group to which the Device Manager daemon has been registered, and then in the displayed popup menu perform the following three operations in order:
   - Choose **Unfreeze**.
   - Choose **Switch To**, and then *standby-host-name*.
   - Choose **Freeze**, and then **Temporary**.
4. When using Sun Cluster, execute the following command:

```
/usr/cluster/bin/scswitch -z -g group-name -h standby-host-name
```

Installing on the Standby Node

To install Replication Monitor on the standby node:

1. Install the Replication Monitor server.

   For details about installation, see section 2.4.1.

2. Perform post-installation processing such as enabling the resources that were disabled in the preparation processing.

   If using VERITAS Cluster Server, carry out steps 3 to 5. If using Sun Cluster, carry out steps 6 to 8.

3. Select the **Service Groups** tab in the Cluster Explorer window, right click the group where the Device Manager daemon has been registered, and then select **Unfreeze** from the displayed popup menu.

4. Right-click the following resources, and then select **Enabled** from the displayed popup menu.

   - HiCommandServer
   - HBase Storage Mgmt Common Service
   - HBase Storage Mgmt Web Service
   - HiRDB

5. Select the **Service Groups** tab in the Cluster Explorer window, right click the group where the Device Manager daemon has been registered, and then perform the following operations from the displayed popup menu:

   - Select **Switch To**, and then *executing-host-name*.
   - Select **Online**, and then *executing-host-name*.

6. Execute the following command to switch the system to the executing node:

```
/usr/cluster/bin/scswitch -z -g group-name -h executing-host-name
```

7. Execute the following commands to enable the resources for HiRDB, HiCommand Suite Common Component, and Device Manager:

```
# /usr/cluster/bin/scswitch -e -j HiRDB
# /usr/cluster/bin/scswitch -e -j MgmtComService
# /usr/cluster/bin/scswitch -e -j MgmtWebService
# /usr/cluster/bin/scswitch -e -j HiCommandServer
```

8. Execute the following commands to enable monitoring of the resources for HiRDB, HiCommand Suite Common Component, and Device Manager:

```
# /usr/cluster/bin/scswitch -e -M -j HiRDB
# /usr/cluster/bin/scswitch -e -M -j MgmtComService
# /usr/cluster/bin/scswitch -e -M -j MgmtWebService
# /usr/cluster/bin/scswitch -e -M -j HiCommandServer
```

7.2.1.3 Registering License Information

In a cluster environment both in Windows and in Solaris, the license information must be registered on both the executing and standby nodes.

To register license information:

1. On the executing node, display the Login window for Web Client, and then register license information.

2. Switch to the standby system.
3. On the standby node, display the Login window for Web Client, and then register license information.
4. Switch to the executing system.

For details about how to register license information, see section 3.2. For details about how to switch between the executing and standby systems, see step 7 in *Installing on the Executing Node* for Windows in section 7.2.1.1, and steps 3 (only perform the **Switch To** operation from the bulleted list) and 4 in *Installing on the Executing Node* for Solaris in section 7.2.1.2.

7.2.2 Upgrade Installation and Re-installation

This section describes the procedures for upgrading or re-installing an existing Replication Monitor server.

7.2.2.1 In Windows

Upgrading or Re-installing on the Executing Node

To upgrade or re-install the Replication Monitor server on the executing node when the OS is Windows:

1. Open the Cluster Administrator window by choosing **Start**, **Settings**, **Control Panel**, **Administrative Tools**, and then **Cluster Administrator**, and then place the following services offline:
   - HiCommandServer
   - HBase Storage Mgmt Web Service
   - HBase Storage Mgmt Common Service

   Note:

   Do not place the following resources offline:

   - Shared disk

   - Cluster management IP address

   - Virtual host name

   If the shared disk, cluster management IP address, or virtual host name is placed offline, installation will fail.
2. Execute the following command to stop the HiCommand Suite Common Component service:

```
"C:\Program Files\HiCommand\Base\bin\hcmdssrv" /stop
```

3. In the Cluster Administrator window, place the following service offline:

```
HiRDB/ClusterService _HD0
```

4. In the Cluster Administrator window, right-click the services that were placed offline in steps 1 and 3, choose **Property**, click the **Advanced** tab, select **Do not restart**, and then click **OK**.

5. Perform an overwrite installation of the Replication Monitor server.

   For details about overwrite installation, see section 2.3.2.

6. In the Cluster Administrator window, right-click the group to which the Device Manager service (HiCommandServer) has been registered, and then choose **Move Group** to switch to the standby node.

Upgrading or Re-installing on the Standby Node

To upgrade or re-install Replication Monitor on the standby node when the OS is Windows:

1. Perform an overwrite installation of the Replication Monitor server.

   For details about overwrite installation, see section 2.3.2.

2. In the Cluster Administrator window, right-click the following services, choose **Property**, click the **Advanced** tab, select **Restart**, and then click **OK**.
   - HBase Storage Mgmt Common Service
   - HBase Storage Mgmt Web Service
   - HiCommandServer
   - HiRDB/ClusterService _HD0
3. In the Cluster Administrator window, right-click the group to which the Device Manager service (HiCommandServer) has been registered, and then choose **Move Group** to switch to the executing node.
4. In the Cluster Administrator window, right-click the group to which the Device Manager service (HiCommandServer) has been registered, and then select **Online**.

7.2.2.2 In Solaris

In Solaris, upgrading and re-installing an existing Replication Monitor server can be performed in the same manner as a new installation. For details, see section 7.2.1.2 *In Solaris*.

Note: that the cross-referencing part in sub-section 7.2.1.1 and 7.2.1.2. must be read as well as section 2.4.2. When upgrading or re-installing an existing Replication Monitor server, you do not need to register license information.

7.2.3 Uninstallation

This section describes the procedures for an uninstallation of the Replication Monitor server.

7.2.3.1 In Windows

1. On the executing node, choose **Start**, **Settings**, **Control Panel**, **Administrative Tools**, and then **Cluster Administrator** to open the Cluster Administrator window, and then place the following services offline:
   - HiCommandServer

- HBase Storage Mgmt Web Service
- HBase Storage Mgmt Common Service

Note:

Do not place the following resources offline:

- Shared disk

- Cluster management IP address

- Virtual host name

If the shared disk, cluster management IP address, or virtual host name is placed offline, uninstallation will fail.

2. On the executing node, execute the following command to stop the HiCommand Suite Common Component services:

```
"C:\Program Files\HiCommand\Base\bin\hcmdssrv" /stop
```

3. In the Cluster Administrator window, place the following service offline:

```
HiRDB/ClusterService _HD0
```

4. In the Cluster Administrator window, right-click the services that were placed offline in steps 1 and 3, choose **Property**, click the **Advanced** tab, select **Do not restart**, and then click **OK**.
5. On both the executing and standby nodes, uninstall the Replication Monitor server.

   For details about uninstallation, see section 2.3.3.
6. Change the services that were set to **Do not restart** in step 4 back to **Restart.**

7.2.3.2 In Solaris

In a VCS (VERITAS Cluster Server) Environment

To uninstall Replication Monitor in a cluster environment for VERITAS Cluster Server:

1. On the executing node, start Cluster Manager (Java Console).
2. Place the following daemons offline:
   - HiCommandServer
   - HBase Storage Mgmt Web Service
   - HBase Storage Mgmt Common Service

   Note:

   Do not place the following resources offline:

   - Shared disk

   - Cluster management IP address

   - Virtual host name

   If the shared disk, cluster management IP address, or virtual host name is placed offline, uninstallation will fail.

3. Execute the following command to stop the HiCommand Suite Common Component daemons:

```
# /opt/HiCommand/Base/bin/hcmdssrv -stop
```

4. Place the HiRDB daemon offline.
5. Select and right-click the following resources to display a popup menu, and then clear **Enabled**.
   - HBase Storage Mgmt Web Service
   - HBase Storage Mgmt Common Service
   - HiCommandServer
   - HiRDB
6. In the Cluster Explorer window, click the **Service Groups** tab.
7. Select and right-click the group to which the Device Manager daemon has been registered, and in the displayed popup menu, choose **Freeze**, and then **Temporary**.
8. On the executing node, uninstall the Replication Monitor server.
9. On the standby node, uninstall the Replication Monitor server.

   For details about uninstallation, see section 2.4.3.
10. In the Cluster Explorer window click the **Service Groups** tab, select the group to which the Device Manager daemon has been registered, and then in the displayed popup menu choose **Unfreeze**.
11. Enable the resources disabled in step 5.

In a Sun Cluster environment

To uninstall Replication Monitor in a cluster environment for Sun Cluster:

1. On the executing node, execute the following commands to disable monitoring the resources for HiCommand Suite Common Component, HiRDB, and Device Manager:

```
# /usr/cluster/bin/scswitch -n -M -j HiCommandServer
# /usr/cluster/bin/scswitch -n -M -j MgmtWebService
# /usr/cluster/bin/scswitch -n -M -j MgmtComService
# /usr/cluster/bin/scswitch -n -M -j HiRDB
```

2. Execute the following commands to disable the resources for HiCommand Suite Common Component, HiRDB, and Device Manager:

```
# /usr/cluster/bin/scswitch -n -j HiCommandServer
# /usr/cluster/bin/scswitch -n -j MgmtWebService
# /usr/cluster/bin/scswitch -n -j MgmtComService
# /usr/cluster/bin/scswitch -n -j HiRDB
```

3. On the executing node, uninstall the Replication Monitor server.

   For details about uninstallation, see section 2.4.3.
4. On the standby node, uninstall the Replication Monitor server.

   For details about uninstallation, see section 2.4.3.
5. Execute the following commands to enable the resources disabled in steps 1 and 2:

```
# /usr/cluster/bin/scswitch -e -j daemon-name
# /usr/cluster/bin/scswitch -e -M -j daemon-name
```

7.3 Changing Replication Monitor to a Cluster Environment After Starting Operation

Each of the following sections explains how to build a cluster configuration from an environment where Replication Monitor is already in operation in a non-cluster configuration.

Also, when you are changing the environment from a non-cluster configuration to a cluster configuration, always obtain a backup of the database. For details regarding backups, see section 3.8.

To execute the commands and operations described in this section, the following user must be logged in to the system:

In Windows:

An administrator group user

In Solaris:

A root user

Note:

The procedure shown below includes steps at which you must stop the HiCommand product services (daemons). However, the services (daemons) of the following HiCommand product versions cannot be stopped even if you execute the `hcmdssrv` command with the stop option specified.

For details on how to `stop` those services, see the manual for each product.

- Device Manager version 5.6 or earlier
- Tiered Storage Manager version 5.5 or earlier

7.3.1 Setting Up a Cluster Environment by Using MSCS

7.3.1.1 Settings on the Executing Node

This section explains how to specify settings for a cluster environment in the executing node in Windows.

The following procedures assume that cluster software and a shared disk are ready and that the management server with the Replication Monitor server already set up is set to be the executing node in a cluster configuration. It is also assumed that the HiCommand Suite Common Component services have already started.

To specify settings for a cluster environment in the executing node in Windows:

1. When other HiCommand products are in operation, stop the service tasks of those HiCommand products and services of HiCommand Suite Common Component (HBase Storage Mgmt Web Service and HBase Storage Mgmt Common Service).

   To stop the service tasks, execute the following command:

```
HiCommand-Suite-Common-Component-installation-folder\bin\hcmdssrv /stop
```

2. Start HiRDB.

   Execute the following command:

```
HiCommand-Suite-Common-Component-installation-folder\bin\hcmdsdbsrv /start
```

   An example of command execution is shown below:

```
C:\Program Files\HiCommand\Base\bin\hcmdsdbsrv /start
```

3. Create the cluster setting file `cluster.conf` using a text editor.

   In the cluster setting file, specify whether the node is the executing or standby node, and specify the host names of the virtual host, executing node, and standby node. Use the formats shown below:

```
mode = Specifies whether the node is the executing or standby node.
virtualhost = Specifies the host name of the virtual host.
onlinehost = Specifies the host name of the executing node.
standbyhost = Specifies the host name of the standby node.
```

   In the following example, items are specified for an executing node:

```
mode = online
virtualhost = virt99
onlinehost = hrpm5
standbyhost = hrpm7
```

   Store the created cluster file in *HiCommand-Suite-Common-Component-installation-folder*`\conf`.

   Note:

   In the cluster setting file `cluster.conf`, you cannot use IP addresses to specify the host names of the virtual host, executing node, or standby node.

   The virtual host name specified for `virtualhost` must be valid for the corresponding IP address and must be accessible.

4. Move the database to the shared disk.

   Delete or empty the folder where the data is to be stored, and then execute the following command. Executing this command changes the port number of the port used by HiRDB to the default port number (23032). If you changed the port number to a number other than the default, take note of the port number being used so that you can specify it later.

```
HiCommand-Suite-Common-Component-installation-folder\bin\hcmdsdbclustersetup
/createcluster /databasepath database-recreation-folder /exportpath
data-destination-folder
```

   An example of command execution is shown below:

```
C:\Program Files\HiCommand\Base\bin\hcmdsdbclustersetup /createcluster /databasepath
R:\re_creating_db /exportpath C:\storing_data
```

   Notes:

   - Specify *database-recreation-folder* and *data-destination-folder* by using the absolute path in no more than 63 bytes.
   - Specify the path of *database-recreation-folder* on a shared disk.

- You can use the following characters to specify *database-recreation-folder* and *data-destination-folder*. In addition, you can use a backslash (\), colon (:), or forward slash (/) as a delimiter.

```
A-Z a-z 0-9 . _
```

- For details about how to set the port used by HiRDB, see the *HiCommand Device Manager Server Installation and Configuration Guide*.
- After the command execution succeeds and the data becomes unnecessary, manually delete the backed-up data from the folder storing that data.

  Even when other HiCommand products are in operation, you only need to execute this step once.

  HiCommand Suite Common Component is restarted during this step.

  For the action to take if database registration fails, see section 9.2.

5. Execute the following command to stop HiCommand Suite Common Component services (HBase Storage Mgmt Web Service and HBase Storage Mgmt Common Service) and databases:

```
HiCommand-Suite-Common-Component-installation-folder\bin\hcmdssrv /stop
```

6. Choose **Start**, **Settings**, **Control Panel**, **Administrative Tools**, and **Services**. Open the following service properties in the Service window, and then change **Startup Type** from **Automatic** to **Manual**.
   - HBase Storage Mgmt Web Service
   - HBase Storage Mgmt Common Service
   - HiCommandServer

   When a HiCommand product other than Replication Monitor and Device Manager is operating on the same management server with the Replication Monitor server, see the manual for each product to determine whether **Startup Type** of the HiCommand product needs to be changed.

7. Register the resources shown below (such as shared resources and services) into the cluster software.

   For details on how to register resources into cluster software, see the *HiCommand Device Manager Server Installation and Configuration Guide*.
   - IP address of cluster manager
   - Virtual host name
   - The shared disk where the database is created
   - The following services:
     - HBase Storage Mgmt Web Service
     - HBase Storage Mgmt Common Service
     - HiCommandServer
     - HiRDB/ClusterService _HD0

When a HiCommand product other than Replication Monitor and Device Manager is operating on the same management server with the Replication Monitor server, see the manual for each product to determine whether the HiCommand product service needs to be registered in the cluster software.

7.3.1.2 Settings on the Standby Node

This section shows the procedures used to specify settings for a cluster environment in the standby node in Windows.

The following procedures assume that cluster software and a shared disk are ready and that the management server where the Replication Monitor server has been set up is set to be the standby node in a cluster configuration.

To specify settings for a cluster environment in the standby node in Windows:

1. When other HiCommand products are in operation, stop the service tasks of those HiCommand products and services of HiCommand Suite Common Component (HBase Storage Mgmt Web Service and HBase Storage Mgmt Common Service).

   Execute the following command to stop the service tasks:

   ```
   HiCommand-Suite-Common-Component-installation-folder\bin\hcmdssrv /stop
   ```

2. Create the cluster setting file `cluster.conf` using a text editor.

   In the cluster setting file, specify whether the node is the executing or standby node, and specify the host names of the virtual host, executing node, and standby node. Use the formats shown below:

   ```
   mode = Specifies whether the node is the executing or standby node.
   virtualhost = Specifies the host name of the virtual host.
   onlinehost = Specifies the host name of the executing node.
   standbyhost = Specifies the host name of the standby node.
   ```

   In the following example, items are specified for a standby node:

   ```
   mode = standby
   virtualhost = virt99
   onlinehost = hrpm5
   standbyhost = hrpm7
   ```

   Store the created cluster setting file in *HiCommand-Suite-Common-Component-installation-folder*`\conf`.

   In the cluster setting file `cluster.conf`, you cannot use IP addresses to specify the host names of the virtual host, executing node, or standby node.

   The virtual host name specified for `virtualhost` must be valid for the corresponding IP address and must be accessible.

3. Execute the following command to change the setting in order to use a database on a shared disk:

   Execute the following command. Executing this command changes the port number of the port used by HiRDB to the default port number (23032). If you changed the port number to a number other than the default, take note of the port number being used so that you can specify it later.

   ```
   HiCommand-Suite-Common-Component-installation-folder\bin\hcmdsdbremake /cluster
   /databasepath database-recreation-folder
   ```

An example of command execution is shown below:

```
C:\Program Files\HiCommand\Base\bin\hcmdsdbremake /cluster /databasepath
R:\re_creating_db
```

Note:

For *database-recreation-folder*, use an absolute path of no more than 63 bytes to specify the same folder that was specified when a database was re-created on the shared disk in the executing node.

Note that a file separator cannot be used at the end of a name for *database-recreation-folder*. If it is used, a command error occurs. In this case, remove the file separator, and re-execute the command.

Note:

For details about how to set the port used by HiRDB, see the *HiCommand Device Manager Server Installation and Configuration Guide*.

Even when other HiCommand products are in operation, you need to execute this step once only.]

HiCommand Suite Common Component is restarted on the standby node during this step.

4. Execute the following command to stop HiCommand Suite Common Component services (HBase Storage Mgmt Web Service and HBase Storage Mgmt Common Service) and databases:

```
HiCommand-Suite-Common-Component-installation-folder\bin\hcmdssrv /stop
```

5. Choose **Start**, **Settings**, **Control Panel**, **Administrative Tools**, and **Services**. Open the following service properties in the Service window, and then change **Startup Type** from **Automatic** to **Manual**.
   - HBase Storage Mgmt Web Service
   - HBase Storage Mgmt Common Service
   - HiCommandServer

     When HiCommand products other than Replication Monitor and Device Manager are operating on the same management server with the Replication Monitor server, see the manual for each product to determine whether **Startup Type** of the HiCommand product needs to be changed.

6. Register the resources shown below (such as shared resources and services) into the cluster software. However, if the resources have been registered on the executing node, you do not need to register the resources on the standby node.

   For details on how to register the resources into cluster software, see the *HiCommand Device Manager Server Installation and Configuration Guide*.
   - IP address of cluster manager
   - Virtual host name
   - The shared disk where the database is created
   - The following services:

     - HBase Storage Mgmt Web Service

- HBase Storage Mgmt Common Service

- HiCommandServer

- HiRDB/ClusterService _HD0

When HiCommand products other than Replication Monitor and Device Manager are operating on the same management server with the Replication Monitor server, see the manual for each product to determine whether the HiCommand product service needs to be registered in the cluster software.

7.3.1.3 Changing the URL Information to Start Web Client on the Executing Node

Execute the `hcmdschgurl` command on the executing node to change the URL information used for starting Web Client to include the virtual server name.

The `hcmdschgurl` command is used for updating the access information (URL information) used for starting an application saved in the HiCommand Suite Common Component database.

For details on how to use the `hcmdschgurl` command, see the *HiCommand Device Manager Server Installation and Configuration Guide*.

7.3.1.4 Setting Warning Banners on the Executing Node and the Standby Node

It is recommended that you make the same warning banner settings for both the executing node and the standby node. For details about making settings for warning banners, see section 6.8.

7.3.2 Setting Up a Cluster Environment by Using VCS or Sun Cluster

7.3.2.1 Settings on the Executing Node

This section shows the steps used to set up a cluster environment in the executing node in Solaris.

The following steps assume that cluster software and a shared disk are ready and that the management server where the Replication Monitor server has been set up is set to the executing node for cluster configuration. It is also assumed that the HiCommand Suite Common Component services have already started.

To set up a cluster environment in the executing node in Solaris:

1. When other HiCommand products are in operation, stop the daemons of those HiCommand products and daemons of HiCommand Suite Common Component (HBase Storage Mgmt Web Service and HBase Storage Mgmt Common Service).

   To stop the daemons, execute the following command:

   ```
   # /opt/HiCommand/Base/bin/hcmdssrv -stop
   ```

2. Start HiRDB.

Execute the following command:

```
# /opt/HiCommand/Base/bin/hcmdsdbsrv -start
```

3. Create the cluster setting file `cluster.conf` using a text editor.

   In the cluster setting file, specify whether the node is the executing or standby node, and specify the host names of the virtual host, executing node, and standby node. Use the formats shown below:

```
mode = Specifies whether the node is the executing or standby node.
virtualhost = Specifies the host name of the virtual host.
onlinehost = Specifies the host name of the executing node.
standbyhost = Specifies the host name of the standby node.
```

   In the following example, items are specified for an executing node:

```
mode = online
virtualhost = virt99
onlinehost = hrpm5
standbyhost = hrpm7
```

   Store the created cluster setting file in `/opt/HiCommand/Base/conf`.

   Note:

   In the cluster setting file `cluster.conf`, you cannot use IP addresses to specify the host names of the virtual host, executing node, or standby node.

   The virtual host name specified for `virtualhost` must be valid for the corresponding IP address and must be accessible.

4. Move the database to the shared disk.

   Delete or empty the folder where the data is to be stored, and then execute the following command. Executing this command changes the port number of the port used by HiRDB to the default port number (23032). If you changed the port number to a number other than the default, take note of the port number being used so that you can specify it later.

```
# /opt/HiCommand/Base/bin/hcmdsdbclustersetup -createcluster -databasepath
database-recreation-directory -exportpath data-destination-directory
```

   An example of command execution is shown below:

```
# /opt/HiCommand/Base/bin/hcmdsdbclustersetup -createcluster -databasepath
/root/re_creating_db -exportpath /opt/storing_data
```

   Notes:

   - Specify *database-recreation-directory* and *data-destination-directory* by using the absolute path in no more than 63 bytes.
   - Specify the path of *database-recreation-directory* on a shared disk.
   - You can use the following characters to specify *database-recreation-directory* and *data-destination-directory*. In addition, you can use a forward slash (/) as a delimiter.

```
A-Z a-z 0-9 . , _
```

   - For details about how to set the port used by HiRDB, see the *HiCommand Device Manager Server Installation and Configuration Guide*.

– After the command execution succeeds and the data becomes unnecessary, manually delete the backed-up data from the folder storing that data.

  Even when other HiCommand products are in operation, you only need to execute this step once.

  HiCommand Suite Common Component is restarted during this step.

  For the action to take if database registration fails, see section 9.2.

5. Execute the following command to stop HiCommand Suite Common Component daemons (HBase Storage Mgmt Web Service and HBase Storage Mgmt Common Service) and databases:

```
# /opt/HiCommand/Base/bin/hcmdssrv -stop
```

6. Execute the following command to change all daemons managed by HiCommand Suite Common Component so that they are not started automatically during startup:

```
# /opt/HiCommand/Base/bin/hcmdssrv -starttype manual -all
```

7. Move the following file to another directory or change the file name so that the daemons for the Device Manager server are not started automatically during startup:

   When changing the file name, do not use `K` or `S` at the beginning of the new name.

```
/etc/rc3.d/S99hicommand
```

8. Perform the necessary settings for the cluster environment such as registering the resources shown below (such as shared resources and daemons) into the cluster software.

   For details on how to perform the necessary settings for the cluster environment, see the *HiCommand Device Manager Server Installation and Configuration Guide*.

   – IP address of cluster manager

   – Virtual host name

   – The shared disk where the database is created

   – The following daemons:

     - HBase Storage Mgmt Web Service

     - HBase Storage Mgmt Common Service

     - HiCommandServer

     - HiRDB

     If HiCommand products other than Replication Monitor and Device Manager are operating on the same server as that of the Replication Monitor server, see the manual for each product to determine whether the HiCommand product daemon needs to be registered into the cluster software.

7.3.2.2 Settings on the Standby Node

This section shows the steps to set up a cluster environment in the standby node in Solaris.

The following steps assume that cluster software and a shared disk are ready and that the management server where the Replication Monitor server has been set up is set to the standby node for cluster configuration.

To set up a cluster environment in the standby node in Solaris:

1. When other HiCommand products are in operation, stop the daemons of those HiCommand products, as well as the daemons of HiCommand Suite Common Component (HBase Storage Mgmt Web Service and HBase Storage Mgmt Common Service).

   Execute the following command to stop the daemons:

   ```
   # /opt/HiCommand/Base/bin/hcmdssrv -stop
   ```

2. Create the cluster setting file `cluster.conf` using a text editor.

   In the cluster setting file, specify whether the node is the executing or standby node, and specify the host names of the virtual host, executing node, and standby node. Use the formats shown below:

   ```
   mode = Specifies whether the node is the executing or standby node.
   virtualhost = Specifies the host name of the virtual host.
   onlinehost = Specifies the host name of the executing node.
   standbyhost = Specifies the host name of the standby node.
   ```

   In the following example, items are specified for a standby node:

   ```
   mode = standby
   virtualhost = virt99
   onlinehost = hrpm5
   standbyhost = hrpm7
   ```

   Store the created cluster setting file in `/opt/HiCommand/Base/conf`.

   Note:

   In the cluster setting file `cluster.conf`, you cannot use IP addresses to specify the host names of the virtual host, executing node, or standby node.

   The virtual host name specified for `virtualhost` must be valid for the corresponding IP address and must be accessible.

3. To change the settings in order to use a database on a shared disk, execute the following command:

   Executing this command changes the port number of the port used by HiRDB to the default port number (23032). If you changed the port number to a number other than the default, take note of the port number being used so that you can specify it later.

   ```
   # /opt/HiCommand/Base/bin/hcmdsdbremake -cluster -databasepath
   database-recreation-directory
   ```

   An example of command execution is shown below:

   ```
   # /opt/HiCommand/Base/bin/hcmdsdbremake -cluster -databasepath /root/re_creating_db
   ```

   Note:

   For *database-recreation-directory*, use an absolute path of no more than 63 bytes to specify the same folder that was specified when a database was re-created on the shared disk in the executing node.

   Note that for *database-recreation-directory*, a directory that includes a space character cannot be specified.

   Also note that a file separator cannot be used at the end of a name for *database-recreation-directory*. If it is used, a command error occurs. In this case, remove the file separator, and re-execute the command.

Note:

For details about how to set the port used by HiRDB, see the *HiCommand Device Manager Server Installation and Configuration Guide*.

Even when other HiCommand products are operating, you only need to execute this step once.

4. Execute the following command to stop HiCommand Suite Common Component daemons (HBase Storage Mgmt Web Service and HBase Storage Mgmt Common Service) and databases:

```
# /opt/HiCommand/Base/bin/hcmdssrv -stop
```

5. Execute the following command to change all daemons managed by HiCommand Suite Common Component so that they are not started automatically:

```
# /opt/HiCommand/Base/bin/hcmdssrv -starttype manual -all
```

6. Move the following file to another directory or change the file name so that the daemons for the Device Manager server are not started automatically during startup:

   When changing the file name, do not use `K` or `S` at the beginning of the new name.

```
/etc/rc3.d/S99hicommand
```

7. Perform the necessary settings for the cluster environment such as registering the resources shown below (such as shared resources and daemons) into the cluster software. However, if the necessary settings have been performed on the executing node, you do not need to perform the necessary settings on the standby node.

   For details on how to perform the necessary settings for the cluster environment, see the *HiCommand Device Manager Server Installation and Configuration Guide*.

   - IP address of cluster manager
   - Virtual host name
   - The shared disk where the database is created
   - The following daemons:

     - HBase Storage Mgmt Web Service
     - HBase Storage Mgmt Common Service
     - HiCommandServer
     - HiRDB

     When HiCommand products other than Replication Monitor and Device Manager are operating on the same server with that of the Replication Monitor server, see the manual for each product to determine whether the HiCommand product daemon needs to be registered into the cluster software.

     Changing the URL Information to Start Web Client on the Executing Node

     Execute the `hcmdschgurl` command on the executing node to change the URL information used for starting Web Client to include the virtual server name.

     The `hcmdschgurl` command is used for updating the access information (URL information) used for starting an application saved in the HiCommand Suite Common Component database.

     For details on how to use the `hcmdschgurl` command, see the *HiCommand Device Manager Server Installation and Configuration Guide*.

7.3.2.3 Setting Warning Banners on the Executing Node and the Standby Node

It is recommended that you make the same warning banner settings for both the executing node and the standby node. For details about making settings for warning banners, see section 6.8.

Chapter 8 Linkage with Related Products

This chapter describes the settings for linking Replication Monitor with related products.

- Settings for Starting HSSM from the Dashboard Menu (see section 8.1)

8.1 Settings for Starting HSSM from the Dashboard Menu

To link with HSSM and start HSSM from the **Dashboard** menu, create the `StorageServiceManager.conf` file in the following folder if the file has not been created yet. The location of this file differs depending on the OS:

In a Windows system:

```
HiCommand-Suite-Common-Component-installation-folder\common
```

In a Solaris system:

```
/opt/HiCommand/Base/common
```

In the `StorageServiceManager.conf` file, specify the `LaunchURL` parameter in the format shown as follows:

Format of the StorageServiceManager.conf File

```
LaunchURL=HSSM-URL
```

In *HSSM-URL*, specify the URL used to start HSSM. For details about this URL, see the HSSM documentation.

For example, if the name of the HSSM management server is *machinename*, configure the `StorageServiceManager.conf` as follows:

For Secure Connections:

```
LaunchURL=https://machinename
```

For Nonsecure Connections:

```
LaunchURL=http://machinename
```

Chapter 9 Troubleshooting

This chapter describes how to handle errors that may occur when Replication Monitor is installed and uninstalled, as well as the errors associated with system creation.

- Troubleshooting for Installation and Uninstallation (see section 9.1)
- Troubleshooting for Building a Cluster Environment (see section 9.2)
- How to Handle Detailed Message RPM-00824 (see section 9.3)
- How to Handle Error Message KAVN01281-E (see section 9.4)
- Contacting the Hitachi Data Systems Technical Support Center (see section 9.5)

9.1 Troubleshooting for Installation and Uninstallation

9.1.1 Troubleshooting for a Windows Management Server

This section describes the actions to be taken when installation or uninstallation of the Replication Monitor server fails. In the following cases, installation or uninstallation may stop leaving the system in an incomplete state.

- When cancellation of an installation is attempted by clicking the **Cancel** button during file copy processing of an upgrade installation.
- When the installation or uninstallation fails because of an error that occurred during the processing

9.1.1.1 Actions to be Taken if Installation Fails

According to the displayed error message, take one of the following actions:

- Execute an overwrite installation
- Once you have uninstalled the Replication Monitor, reinstall it.

9.1.1.2 Trace Logs During Installation or Uninstallation

Records (trace logs) of installation or uninstallation processing and their results are output as the trace log file of the installer.

The output folder, file name, and output format of the installer trace log file are as follows:

- Output folder

  The output destination varies depending on whether the processing finished normally, or if an error occurred during the processing.

  - When the installation processing finishes normally

    Replication-Monitor-installation-folder`\logs`

  - When an error occurs during the installation or uninstallation processing

    If the Replication Monitor installation folder has been created, the trace log file is output to the following location:

    Replication-Monitor-installation-folder`\logs`

    If the Replication Monitor installation folder has not been created, the trace log file is output to the following location:

    system-drive`\`

  - When the uninstallation processing finishes normally

    In this case, the trace log file is deleted as the last step of the uninstallation processing.

- File name

  The file name differs depending on whether the log is for an installation or an uninstallation.

  HRpM_***xxxxxx***Log.log

  where ***xxxxxx*** is either Install (for installation) or Uninstall (for uninstallation).

- Output format

  The output format to the trace log file is as follows:

```
*** Begin Replication Monitor (Windows) setup process Trace Log
yyyy/mm/dd hh:mm:ss : (level) trace-information supplementary-information
 :
*** End Replication Monitor (Windows) setup process Trace Log
```

  The meaning of the output information is as follows:

  *** Begin Replication Monitor (Windows) setup process Trace Log

  A comment row showing the beginning of the trace log output.

  yyyy/*mm*/*dd hh*:*mm*:*ss*

  Processing date (*yyyy*/*mm*/*dd hh*:*mm*:*ss*: year/month/date hour:minute:second).

  level

  One of the following is output:

  I: Trace information for the notification level

  W: Trace information for the warning level

  E: Trace information showing that an error occurred.

  trace-information

  Parameter values for each executed process, and the specified formats of commands issued by the installer and their response results.

  supplementary-information

  Supplementary information that is output as needed.

  *** End Replication Monitor (Windows) setup process Trace Log

  A comment row indicating the end of the trace log output.

A standard InstallShield log is output in addition to the installer's trace log. This InstallShield standard log file is to be sent with customer inquiries, for when you cannot identify causes of problems during installation or uninstallation by referring to the trace log file.

The InstallShield standard log file is as follows:

OS	Output destination of the standard InstallShield log
▪ Windows 2000 ▪ Windows Server 2003 ▪ Windows Server 2003 R2 ▪ Windows XP	*system-drive*\Program Files\InstallShield Installation Information\{*ID*}\Setup.ilg

OS	Output destination of the standard InstallShield log
▪ Windows Server 2003 x64 Edition ▪ Windows Server 2003 R2 x64 Edition	*system-drive*\Program Files(x86)\InstallShield Installation Information\{*ID*}\Setup.ilg

ID: The ProductCode value determined by the installer.

If the installer's trace log has not been output, the installer may have been stopped forcibly. In this case, re-install the Replication Monitor. At this time, enter the same values as those you entered during the new installation for the set values of the installation path and other items.

Note that, if you re-install the Replication Monitor after an installation fails, the Replication Monitor server database will be initialized. In this case, you need to wait until the re-installation of the Replication Monitor finishes normally, and then restore the Replication Monitor server database. The database can be restored because it was backed up in advance. For details on backing up and restoring databases, see section 3.8.

9.1.1.3 Actions To Take if Upgrade Installation Fails

The following procedures show how to take corrective action when upgrade installation from an earlier version fails.

To take corrective action for upgrading from version 4.0 or 4.2 to 5.7:

1. Make sure that the `HRpMAlertSettingData` folder that stores the alert settings of an earlier version is backed up to the following location:

   Windows-installation-drive\

2. If the set values in the Replication Monitor property files have been changed from the default values, take notes of such values.
3. Remove the cause of the error shown in the displayed installation error message, and then perform an uninstallation of the Replication Monitor server.
4. After the uninstallation has been completed, perform a new installation of the Replication Monitor server.
5. After the installation has been completed, change the set values in the property files and import the alert settings as needed.

To take corrective action for upgrading from version 5.0 to 5.7:

1. Remove the cause of the error shown in the displayed installation error message, and then uninstall the Replication Monitor server.
2. After the uninstallation has been completed, perform a new installation of the version of the Replication Monitor server that had been used before the upgrade installation.
3. After the new installation has been completed, restore the database from a backup created before upgrade installation was performed.

   For details about how to restore the database, see section 3.8.2.

4. Re-execute upgrade installation.

9.1.2 Troubleshooting for a Solaris Management Server

This section describes the actions to be taken when installation or uninstallation of the Replication Monitor server fails. In the following cases, installation or uninstallation may stop, leaving the system in an incomplete state.

- When installation or uninstallation fails because of an error that occurred during the processing

9.1.2.1 Actions to be Taken if Installation Fails

According to the displayed error message, take one of the following actions:

- Execute an overwrite installation
- Once you have uninstalled the Replication Monitor, reinstall it.

If you have cancelled the installer by mistake, check the installed package information that is displayed by executing the following command:

```
# pkginfo HRPM
```

When the installed package information does not contain information about Replication Monitor

Re-install Replication Monitor.

When the installed package information contains information about Replication Monitor

The Replication Monitor server may not have been installed successfully. Check the trace log information that is displayed during installation, eliminate the cause of the error, uninstall the Replication Monitor server, and then re-install it.

9.1.2.2 Trace Logs During Installation or Uninstallation

Records (trace logs) of installation or uninstallation processing and their results are output as the trace log file of the installer.

The output destination, file name, and output format of the installer trace log file are as follows:

- Output directory

  The output destination varies depending on whether the processing finished before or after the creation of an installation directory, and whether writing for storing the trace log file succeeded.

  - When processing finishes after the creation of an installation directory and writing for storing the trace log file has succeeded

    `/var/opt/HiCommand/ReplicationMonitor/logs`

When processing finishes with an error, a message appears when the installer stops, stating the output destination and the file name of the trace log. Note these as needed.

Message example:

```
HRpM Installation Trace log file has been created.
/var/opt/HiCommand/ReplicationMonitor/logs/HRpM_InstallLog.log)
```

– When processing finishes before the creation of an installation directory or writing for storing the trace log file has failed

`/tmp`

In this case, regardless of whether an error has occurred, a message appears when the installer stops, stating the output destination and the file name of the trace log. Note these as needed.

Message example:

```
HRpM Installation Trace log file has been created.
(/tmp/HRpM_InstallLog.log)
```

- File name

The file name differs depending on whether the log is for an installation or an uninstallation.

```
HRpM_xxxxxxLog.log
```

where *xxxxxx* is either `Install` (for installation) or `Uninstall` (for uninstallation).

- Output format

The output format to the trace log file is as follows:

```
*** Begin Replication Monitor (Solaris) setup process Trace Log
yyyy/mm/dd hh:mm:ss : (level) trace-information supplementary-information
 :
*** End Replication Monitor (Solaris) setup process Trace Log
```

The meaning of the output information is as follows:

`*** Begin Replication Monitor (Solaris) setup process Trace Log`

A comment row showing the beginning of the trace log output.

yyyy/mm/dd hh:mm:ss

Processing date (*yyyy*/*mm*/*dd hh*:*mm*:*ss*: year/month/date hour:minute:second).

level

One of the following is output:

`I`: Trace information for the notification level

`W`: Trace information for the warning level

`E`: Trace information showing that an error occurred.

trace-information

Parameter values for each executed process, and the specified formats of commands issued by the installer and their response results.

supplementary-information

Supplementary information that is output as needed.

`*** End Replication Monitor (Solaris) setup process Trace Log`

A comment row indicating the end of the trace log output.

9.1.2.3 Actions To Be Taken When Upgrade Installation Fails

The following procedures show how to take corrective action when upgrade installation from an earlier version fails.

To take corrective action for upgrading from version 4.0 or 4.2 to 5.7:

1. Make sure that the `HRpMAlertSettingData` directory that stores the alert settings of an earlier version is backed up to the following location:

   `/tmp`

2. If the set values in the Replication Monitor property files have been changed from the default values, take notes of such values.
3. Remove the cause of the error shown in the displayed installation error message, and then perform an uninstallation of the Replication Monitor server.
4. After the uninstallation has been completed, perform a new installation of the Replication Monitor server.
5. After the installation has been completed, change the set values in the property files and import the alert settings as needed.

To take corrective action for upgrading from version 5.0 to 5.7:

1. Remove the cause of the error shown in the displayed installation error message, and then uninstall the Replication Monitor server.
2. After the uninstallation has been completed, perform a new installation of the version of the Replication Monitor server that had been used before the upgrade installation.
3. After the new installation has been completed, restore the database from a backup created before upgrade installation was performed.

   For details about how to restore the database, see section 3.8.2.

4. Re-execute upgrade installation.

9.1.3 Troubleshooting the Installation of the Replication Monitor Agent

This section describes troubleshooting related to the installation and uninstallation of the Replication Monitor agent.

9.1.3.1 When the Replication Monitor Agent Is Not Recognized by the Replication Monitor Server

When the Replication Monitor agent has been installed successfully, but it is not recognized by the Replication Monitor server, possible causes are as follows:

- The Device Manager agent has not been installed on the host or pair management server.

  Install the Device Manager agent. For details about the installation of the Device Manager agent, see the *HiCommand Device Manager Agent Installation Guide*.

- Communication has not been established between the Device Manager server and the Device Manager agent.

  Check and, if necessary, revise the settings, such as the host name and port number.

  If address conversion takes place between sites, problems may occur during server-agent communications. For details, see section 2.2.3.2.

9.1.3.2 Trace Log During Installation or Uninstallation

Information about the processing and results of installation or uninstallation is output to the installer's trace log file.

The output destination and file name of the installer's trace log file are as follows:

- Output destination directory

  For Windows

  system-drive\

  For Solaris, HP-UX, or AIX

  `/var/tmp/`

- File name

  `HRpMAgent_install.log`

The trace log file is created under this name during a new installation. During an overwrite installation or uninstallation, trace information is added to the same file.

When the Replication Monitor agent is uninstalled successfully, the trace log file is deleted.

9.2 Troubleshooting for Building a Cluster Environment

This section explains the countermeasures for when a database registration using the `hcmdsdbmove` command fails. The countermeasures differ depending on whether the Replication Monitor server database has been backed up.

9.2.1 Troubleshooting for a Windows Management Server

9.2.1.1 When Replication Monitor Server Database Was Backed Up

To recover the system in Windows when a backup has been taken, perform the following procedure:

1. Stop the Device Manager server by selecting **Start**, **Program**, **HiCommand**, **Device Manager**, and then **Stop HiCommand**.
2. Stop the HiCommand Suite Common Component services by executing the following command:

```
HiCommand-Suite-Common-Component-installation-folder\bin\hcmdssrv /stop
```

3. Restore the backup of the Replication Monitor server database.

   For details on the restoration methods, see section 3.8.

4. To resume the setup of the cluster environment, make sure that the HiCommand Suite Common Component services and the Device Manager server have stopped, and then execute the steps, starting with step 5 that are described in section 7.3.1.1.

9.2.1.2 When Replication Monitor Server Database Was Not Backed Up

To recover the system in Windows when a backup has not been taken, reinstall Replication Monitor and Device Manager by performing the following procedure:

1. Open the command prompt, and then restore the status of Replication Monitor by executing the following command:

```
cd HiCommand-Suite-Common-Component-installation-folder\HDB\bin
pdntcmd.bat
pdrels -r HRPM_RDAREA
```

2. Uninstall the Replication Monitor server.

   For details on how to uninstall the Replication Monitor server, see section 2.3.3.

3. Uninstall and then reinstall Device Manager.

   For details on how to uninstall and install Device Manager, see the *HiCommand Device Manager Server Installation and Configuration Guide*.

4. Install the Replication Monitor server.

   For details on how to install the Replication Monitor server, see section 2.3.1.

5. To resume the setup of the cluster environment, execute the steps starting with step 2 that are described in 7.3.1.1.

9.2.2 Troubleshooting for a Solaris Management Server

9.2.2.1 When Replication Monitor Server Database Was Backed Up

To recover the system in Solaris when a backup has been taken, perform the following procedure:

1. Stop the Device Manager server by executing the following command:
```
# /opt/HiCommand/hicommand.sh stop
```
2. Stop the daemons of HiCommand Suite Common Component by executing the following command:
```
# /opt/HiCommand/Base/bin/hcmdssrv -stop
```
3. Restore the backup of the Replication Monitor server database.

   For details on the restoration methods, see section 3.8.
4. To resume the setup of the cluster environment, make sure that the HiCommand Suite Common Component services and the Device Manager server have stopped, and then execute the steps starting with step 5 that are described in section 7.3.2.1.

9.2.2.2 When Replication Monitor Server Database Was Not Backed Up

To recover the system in Solaris when a backup has not been taken, reinstall the Replication Monitor server and Device Manager by performing the following procedure:

1. Restore the status of Replication Monitor by executing the following command:

   Use `sh` or `bash` as the shell for this step.
```
# cd /opt/HiCommand/Base/HDB/bin
# . pduxenv
# pdrels -r HRPM_RDAREA
```
2. Uninstall the Replication Monitor server.

   For details on how to uninstall the Replication Monitor server, see section 2.4.3.
3. Uninstall and then reinstall Device Manager.

   For details on how to uninstall and install Device Manager, see the *HiCommand Device Manager Server Installation and Configuration Guide*.
4. Install the Replication Monitor server.

   For details on how to install the Replication Monitor server, see section 2.4.1.
5. To resume the setup of the cluster environment, execute the steps starting with step 2 that are described in section 7.3.2.1.

9.3 Handling Detailed Message RPM-00824

Detailed message `RPM-00824` indicates that insufficient memory has been allocated to Replication Monitor from the HiCommand Suite Common Component database memory area. In such a case, take action as follows.

9.3.1 Checking the Disk Space

Check the amount of space available on the disk on which the Replication Monitor server is installed. If necessary, increase the available space by either:

- Deleting unnecessary files
- Transferring data out of the database and recreating it on another disk

For details on how to transfer database data to another disk, see section 9.3.2.

9.3.2 Transferring Data from the Common Component Database

If deleting unnecessary files does not free up enough disk space, then data needs to be transferred from the HiCommand Suite Common Component database onto another disk with more free space.

To transfer data from a HiCommand Suite Common Component database (for this procedure, it is assumed that the HiCommand Suite Common Component service is running):

1. Use the following command to output the contents of the database into files.

   In Windows:

   ```
   HiCommand-Suite-Common-Component-installation-folder\bin\hcmdsdbmove /export /datapath
   data-input-and-output-destination-folder
   ```

   In Solaris:

   ```
   # /opt/HiCommand/Base/bin/hcmdsdbmove -export -datapath
   data-input-and-output-destination-directory
   ```

   Note:

   Specify an absolute path for the data input and output destination directory.

   In Solaris, you cannot specify a directory name containing a space character for the data input and output destination directory.

2. If other HiCommand products are running, stop any HiCommand product service tasks and HiCommand Suite Common Component services (HBase Storage Mgmt Web Service and HBase Storage Mgmt Common Service).

   To stop the services, execute the following command:

   In Windows:

   ```
   HiCommand-Suite-Common-Component-installation-folder\bin\hcmdssrv /stop
   ```

   In Solaris:

   ```
   # /opt/HiCommand/Base/bin/hcmdssrv -stop
   ```

Note:

You cannot use the `hcmdssrv` command to stop the services of the following HiCommand product versions. For details on how to stop the services of those versions, see the manual for each product.

- Device Manager version 5.6 or earlier
- Tiered Storage Manager version 5.5 or earlier

3. Execute the following command to create a new database system on the target disk:

   In Windows:

   ```
   HiCommand-Suite-Common-Component-installation-folder\bin\hcmdsdbremake /databasepath
   new-database-destination-folder
   ```

   In Solaris:

   ```
   # /opt/HiCommand/Base/bin/hcmdsdbremake -databasepath new-database-destination-directory
   ```

   Note:

   Specify an absolute path for a new database destination directory (or folder) up to 63 bytes.

   A file separator cannot be specified for an end character in the destination name. If you specify a file separator for an end character, a command error occurs. In such a case, remove the file separator, and then re-execute the command.

   In Solaris, you cannot specify a directory name containing a space character for a new database destination directory.

   Note:

   If you execute the `hcmdsdbremake` command, the setting of the port number used by the built-in database HiRDB is changed back to the default (`23032`). Therefore, when using a port number other than the default and performing operations, the port number must be reset after the command is executed. For details on how to change the port number, see the *HiCommand Device Manager Server Installation and Configuration Guide*.

4. Execute the following command to register the database contents from step 1 into the database:

   In Windows:

   ```
   HiCommand-Suite-Common-Component-installation-folder\bin\hcmdsdbmove /import /datapath
   data-input-and-output-destination-folder
   ```

   In Solaris:

   ```
   # /opt/HiCommand/Base/bin/hcmdsdbmove -import -datapath
   data-input-and-output-destination-directory
   ```

   Note:

   Specify an absolute path for the data input and output destination directory.

   In Solaris, you cannot specify a directory name containing a space character for the data input and output destination directory.

9.4 Handling Error Message KAVN01281-E

This section explains the action to be taken when the error message KAVN01281-E is displayed during installation of a cluster configuration (standby system), and the cause of the error is that the path specified during installation of the executing system is not a shared disk (no shared disk was specified).

In Windows:

1. When the system is the standby system, switch to the executing system. Before doing this, confirm that the following services are offline:
   - HiCommandServer
   - HBase Storage Mgmt Web Service
   - HBase Storage Mgmt Common Service
   - HiRDB/ClusterService _HD0

   If these services are online on the standby system, use the following steps to place them offline and then switch the system.

   1. In the Cluster Administrator window, place the following services offline.
      - HiCommandServer
      - HBase Storage Mgmt Web Service
      - HBase Storage Mgmt Common Service
   2. Execute the following command on the standby node:

      HiCommand-Suite-Common-Component-installation-folder`\bin\hcmdssrv /stop`
   3. In the Cluster Administrator window, place the following service offline:

      `HiRDB/ClusterService _HD0`
   4. Switch to the executing system.
2. Uninstall the Replication Monitor server from the executing system.

   For details on uninstallation, see section 7.2.3.1.
3. Re-install the Replication Monitor server on the executing system. When doing so, specify a shared disk as the storage destination of the database file.

   For details on installation, see *Installing on the Executing Node* in section 7.2.1.1.
4. Install the Replication Monitor server on the standby system. Specify the same path to the storage destination of the database file as that on the executing system.

   For details on installation, see *Installing on the Standby Node* in section 7.2.1.1.

In Solaris:

1. When the system is the standby system, switch to the executing system. Before doing this, confirm that the following daemons are offline (unavailable):
   - HiCommandServer
   - HBase Storage Mgmt Web Service

- HBase Storage Mgmt Common Service
- HiRDB

If these daemons are online (available) on the standby system, use the following steps to place them offline (unavailable) and then switch the system.

In a VCS (VERITAS Cluster Server) environment:

1. Start Cluster Manager (Java Console).
2. Place the following daemons offline:

- HiCommandServer
- HBase Storage Mgmt Web Service
- HBase Storage Mgmt Common Service

3. Execute the following command on the standby node:

```
# /opt/HiCommand/Base/bin/hcmdssrv -stop
```

4. Place the following daemons offline:

```
HiRDB
```

5. Switch to the executing system.

In a Sun Cluster environment:

1. Execute the following commands to disable the resources:

```
# /usr/cluster/bin/scswitch -n -j HiCommandServer
# /usr/cluster/bin/scswitch -n -j MgmtWebService
# /usr/cluster/bin/scswitch -n -j MgmtComService
```

2. Execute the following command on the standby node:

```
# /opt/HiCommand/Base/bin/hcmdssrv -stop
```

3. Execute the following commands to disable the resources:

```
# /usr/cluster/bin/scswitch -n -j HiRDB
```

4. Switch to the executing system.

2. Uninstall the Replication Monitor server from the executing system.

   For details on uninstallation, see 7.2.3.2.

3. Re-install the Replication Monitor server on the executing system. When doing so, specify a shared disk as the storage destination of the database file.

   For details on installation, see *Installing on the Executing Node* in section 7.2.1.2.

4. Install the Replication Monitor server on the standby system. Specify the same path to the storage destination of the database file as that on the executing system.

   For details on installation, see *Installing on the Standby Node* in section 7.2.1.2.

9.5 Contacting the Hitachi Data Systems Technical Support Center

If you need to call the Hitachi Data Systems Support Center, make sure to provide as much information about the problem as possible, including the circumstances surrounding the error or failure, and the exact content of any error messages.

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 Collecting Copy Pair Configuration and Status

Replication Monitor collects information about the configuration and status of copy pairs at regular intervals set by the user (auto refresh function). When designing the system, bear in mind how Replication Monitor collects information and consider what intervals will be appropriate for your system configuration and operation.

This appendix describes the points you should consider when setting collection intervals. For the setting procedure, see section 3.5. For details about how the refresh function works, see the *HiCommand Replication Monitor User's Guide*.

A.1 Setting the Interval and Start Time for Collecting Copy Pair Configuration Information

In an open system, copy pair configuration information is collected from the Device Manager servers registered as information sources with Replication Monitor. In a mainframe system, information is collected from the Business Continuity Managers registered as information sources with Replication Monitor. You can set the following intervals for collecting copy pair configuration information. By default, the collection interval is set as 24 hours and the start time is set as 03:02.

- **NONE**: Do not refresh periodically.
- **8 hour**: Refresh every 8 hours.
- **12 hour**: Refresh every 12 hours.
- **24 hour**: Refresh every 24 hours.

Set the collection interval and start time at a time of day when the system is not busy, so as to minimize as much as possible the effects on application processing performance. You can choose not to collect configuration information at regular intervals if the copy pairs in your system remain unchanged.

In an open system, if the Device Manager server database is updated at regular intervals, set Replication Monitor to collect copy pair configuration information after a database update is performed.

A.2 Setting the Interval for Collecting Copy Pair Status Information

When the Replication Monitor agent is used in an open system, copy pair status information is collected from CCI on the pair management servers. When the Replication Monitor agent is used in a mainframe system, information is collected from the Business Continuity Managers on the pair management servers. You can set a value from 3 minutes to 60 minutes as the interval for periodically collecting copy pair status information. The default value is 5 minutes.

Decide the interval for collecting copy pair status information based on the number of copy pairs monitored by each pair management server. The following table describes guideline values.

TableA.1 Setting the interval for collecting copy pair status information

Number of Copy Pairs	Recommended Information Collection Interval
0 to 1,000	3 minutes
1,001 to 2,000	5 minutes
2,001 to 3,000	10 minutes
3,001 to 5,000	15 minutes

Note: Make sure that no more than 5,000 copy pairs are managed by one Replication Monitor server. If the number of managed copy pairs exceeds 5000, you need to set the memory heap size and timeout value. For details on how to set these values, see section *A.3*.

A.3 Considerations Regarding the Number of Managed Copy Pairs

This appendix describes the operations required when managing 5,000 or more copy pairs.

When 5,000 or more copy pairs are being managed, an out-of-memory error might occur during operations such as listing LDEVs in Web Client. To avoid this problem, set the memory heap size and timeout value as described below. This operation enables Replication Monitor to manage a maximum of 7,000 copy pairs#.

#

If the number of copy pairs is 5,000 or less per copy group, Replication Monitor can manage a maximum of 10,000 copy pairs.

1. On the management server, stop the services or daemons of other HiCommand products and of the HiCommand Suite Common Component.

   Use the `hcmdssrv` command to stop the services or daemons.

2. Execute the following commands.

   When the OS of the management server is Windows:

```
"HiCommand-Suite-Common-Component-installation-folder>\bin\hcmdsweb2" /add /webappdir
"Replication-Monitor-server-installation-folder\lib\webappdir" /jspdir
"Replication-Monitor-server-installation-folder\lib\jspdir" /server HiCommand
/javaoption
"replicationmonitor.conf=Replication-Monitor-server-installation-folder\conf\installati
on.properties" /type ReplicationMonitor /Xmx512
```

   When the OS of the management server is Solaris:

```
/opt/HiCommand/Base/bin/hcmdsweb2 -add -webappdir
/opt/HiCommand/ReplicationMonitor/lib/webappdir -jspdir
/opt/HiCommand/ReplicationMonitor/lib/jspdir -server HiCommand -javaoption
replicationmonitor.conf=/opt/HiCommand/ReplicationMonitor/conf/installation.properties
-nolog -type ReplicationMonitor -Xmx512
```

3. On the pair management server, set 192 for the `server.agent.maxMemorySize` parameter in the `server.properties` file of HiCommand Agent.

   Note:

   On the pair management server, a Device Manager agent of Device Manager version 5.5 or later must be installed.

4. Set 1200 for the `agent.rm.TimeOut` parameter in the `agent.properties` file of the Replication Monitor agent.
5. Stop the Replication Monitor agent, and then restart it.

   For details about how to start or stop the Replication Monitor agent, see section 6.3.2.
6. On the management server, start the services or daemons of the other HiCommand products and of the HiCommand Suite Common Component.

   Use the `hcmdssrv` command to start the services or daemons.

A.4 Installing a Pair Management Server (Open System)

To ensure adequate performance when collecting information in an open system, we recommend that you use a pair management server where the Replication Monitor agent is installed to manage the copy pairs to be monitored.

When monitoring the copy pairs that are not managed on a pair management server where the Replication Monitor agent is installed (such as copy pairs that are not defined in a CCI configuration definition file), Replication Monitor collects information from all the storage subsystems, using the Device Manager's refresh function. The refresh function updates the database maintained by Device Manager with the volume information and configuration information recorded in the connected storage subsystems. This processing may take from a few minutes to several tens of minutes for each storage subsystem.

Appendix B CCI Configuration Definition File Parameters Referenced by Replication Monitor

This appendix describes the parameters in CCI configuration definition files that are referenced by Replication Monitor agents.

The information in a configuration definition file is referenced by Replication Monitor from the CCI of the pair management server via a Replication Monitor agent. If the Replication Monitor agent is version 5.5 or 5.6, it might not work properly, depending on the parameters in the configuration definition file. Change the parameters as required if the configuration definition file contains any that are not supported by Replication Monitor agents. For details about the parameters in the configuration definition files, see the CCI documentation.

Table B.1 lists and describes the parameters in the configuration definition files managed by CCI that are referenced by the Replication Monitor agent.

When referencing configuration definition file information from CCI, the Replication Monitor agent checks the parameter format. If the parameter format is invalid, the Replication Monitor agent might not work properly. Table B.2 lists and describes the parameters that are checked and the scope of the check.

Table B.1 Configuration Definition File Parameters Referenced by the Replication Monitor Agent

Definition	Parameter	Setting		Version of Replication Monitor Agent			Remarks
				5.6 or 5.7	5.5	5.0	
HORCM_CMD	dev_name	UNIX	Special file	Y	Y	Y	
		Windows	Physical drive	Y	Y	Y	
			GUID format	Y	Y	Y	A GUID is created when a disk is partitioned using the disk management function (unformatted).
			CMD format 1	Y	Y	Y	Specify, without specifying an LDEV number, a port number, or host group. (Example: \\.\CMD-30095)
			CMD format 2	Y	Y	Y	Specify the multi-path command device. (Example: \\.\CMD-30095-250)
			CMD format 3	Y	Y	Y	Specify the port and host group by absolute path. (Example: \\.\CMD-30095-250-CL1-A-1)

Definition	Parameter	Setting		Version of Replication Monitor Agent			Remarks
				5.6 or 5.7	5.5	5.0	
			CMD format 4	Y	Y	Y	Specify, using a format other than the GUID format, CMD format 1, CMD format 2, or CMD format 3. (Examples: `\\.\CMD-30095-250-CL1-A`, `\\.\CMD-30095-250-CL1`)
		Redundancy specification		Y	Y	Y	This setting is used to specify multiple command devices in the same device.
		Multi-device specification		Y	Y	Y	This setting is used to specify the command devices in multiple devices.
HORCM_DEV	dev_group	Group name		Y	Y	Y	
	dev_name	Name of pair logical volume		Y	Y	Y	
	port#	Port name	Format 1	Y	Y	Y	Specify when there is no host group. (Examples: `CL1-A`, `CL1-A1`)
			Format 2	Y	(Y)#	(Y)#	Specify to set a host group on the port. (Examples: `CL1-A-2`, `CL1-A1-2`)
	targetID	SCSI/Fibre target ID		Y	Y	Y	Specify the target ID indicated by the `raidscan` command.
	LU#	SCSI/Fibre logical unit number		Y	Y	Y	Specify the LU number of the physical volume of the `targetID`.
	MU#	Mirror descriptor	Omitted (blank)	Y	Y	Y	
			Number	Y	Y	Y	
			h-suffix specification	Y	Y	Y	Specify to use the Universal Replicator mirror descriptor.
HORCM_LDEV	dev_group	Group name		Y	--	--	
	dev_name	Name of pair logical volume		Y	--	--	
	Serial#	Serial number of the large-scale disk array		Y	--	--	
	CU:LDEV (LDEV#)	Disk number of the large-scale disk array	Format 1	Y	--	--	Specify as a hexadecimal in the format *CU:LDEV*. (Example: `01:04`)
			Format 2	Y	--	--	Specify as a decimal. (Example: `260`)

Definition	Parameter	Setting		Version of Replication Monitor Agent			Remarks
				5.6 or 5.7	5.5	5.0	
			Format 3	Y	--	--	Specify as a hexadecimal. (Example: 0x104)
	MU#	Mirror descriptor		Y	--	--	

Legend:

Y: The Replication Monitor agent still works if the definition and value are specified in the configuration definition file.

(Y): The Replication Monitor agent still works if the definition and value are specified in the configuration definition file, but restrictions apply.

--: The Replication Monitor agent does not work if the definition and value are specified in the configuration definition file.

Note:

Of the information contained in the configuration definition files, Table B.1 describes only the parameters that are referenced by the Replication Monitor agent.

#

Host groups of two or more digits cannot be specified with Replication Monitor version 5.0.0-xx or 5.5.0-01.

Table B.2 Parameters Checked by Replication Monitor Agent and Check Scope

Definition	Parameter	Setting		Scope of the Check in CCI	Contents to Be Checked and the Scope
HORCM_CMD	dev_name	Redundancy specification		None	Command devices written in a single line are treated as being in a redundancy specification.
		Multi-device specification		None	Command devices written in separate lines are treated as being in a multi-device specification.
HORCM_DEV	port#	Port name	Format 1	Character string (maximum of 31 alphabetic characters)	Checks whether the port name is specified in the format CL*x*–*X* or CL*x*–*Xn*. (*x* is a string of two or more characters, *X* is a single character, and *n* is a number (multiple digits))
			Format 2		Checks whether the port name is specified in the format CL*x*–*X*–*g* or CL*x*–*Xn*–*g*. (*x* is a string of two or more characters, *X* is a single character, *n* is a number (multiple digits), and *g* is a string of two or more characters)

For details about the parameters in CCI configuration definition files that are referenced by Device Manager agents, see the manual *HiCommand Device Manager Agent Installation Guide*.

Appendix C Resident Processes

The following tables list and describe the resident processes of Replication Monitor.

In Windows

Table C.1 Resident Processes of Replication Monitor (Windows)

Process	Functionality
hntr2mon.exe	HiCommand Suite common trace information collection process
hntr2srv.exe	HiCommand Suite common trace service process
httpsd.exe	HiCommand Suite common web service
hcmdssvctl.exe	HiCommand Suite servlet service

For Solaris

Table C.2 Resident Processes of Replication Monitor (Solaris)

Process	Functionality
hntr2mon	HiCommand Suite common trace information collection process
httpsd	HiCommand Suite common web service

Glossary

3DC Multi-Target configuration	A configuration where a short-distance local site and long-distance remote site are established, and TrueCopy and Universal Replicator are used for copying from the primary site to the local site, and from the primary site to the remote site.
application server	The machine on which application programs are installed. Also called the *host*. The host uses the storage subsystem as an external storage device. In an open system, information about the host can be acquired if a Device Manager agent is installed on the host. In a mainframe system, the host on which Business Continuity Manager is installed is also called the *pair management server*. The pair management server can acquire copy pair configuration and status information about the copy pairs it manages.
batch collection command for maintenance information	Software that collects necessary information such as log files and property files, related to a problem that cannot be resolved at the user level, for forwarding on to customer support.
Business Continuity Manager	Software used to control the storage subsystem from the host in a mainframe system. By using Business Continuity Manager to issue commands from the host to the storage subsystem, you can acquire copy pair configuration and status information. A Replication Monitor server acquires information about copy pair configuration and status in conjunction with Business Continuity Manager.
cascade structure	A structure of consecutive copy pairs. In a cascade structure, the secondary volume of a given copy pair coincides with the primary volume of another copy pair. This volume is called the *secondary/primary volume* (*SP-VOL*).
CCI	Software used to control the storage subsystem from the host in an open system, which is used to control storage subsystem volume duplication features (such as TrueCopy and ShadowImage) by issuing commands from the host to the storage subsystem, and also is used for gathering information about pair configuration in the storage subsystem. Replication Monitor acquires information about copy pair configuration and status in conjunction with a Device Manager server, a Device Manager agent, and CCI.
cluster configuration	In the Replication Monitor operating environment, the term *cluster configuration* refers to the configuration of duplicated management servers consisting of an executing node and a standby node.

cluster software	Software required to be installed on management server nodes to boost overall availability by duplicating management servers as a cluster system. Available software depends on the OS that runs on the management server.
copy group	A group of multiple copy pairs. Operations such as pair status modification apply to all copy pairs in the group.
copy pair	Denotes a primary and secondary volume pair linked by the volume replication function of the storage subsystem. Also called a *pair volume*. In this manual, *copy pair* is sometimes written simply as *pair*.
copy pair state	Indicates in detail the current state of a copy pair status. Each copy pair *state* value is categorized into one of the six copy pair *status* values used in Replication Monitor (`error`, `suspend`, `copying`, `sync`, `simplex`, and `unknown`).
copy pair status	Indicates the current status of the copy pair. Replication Monitor uses six status values: `error`, `suspend`, `copying`, `sync`, `simplex`, and `unknown`. Also called *pair status*.
copy progress	Progress status of the volume replication function performed by the storage subsystem. Replication Monitor displays the copy progress , according to the copy pair status, for items that are **Active** or **Inactive**. For **Active** items, the copy progress is displayed when the copy pair status is `copying` or `sync`. For **Inactive** items, the copy progress is displayed when the copy pair status is error or suspend.
Copy-on-Write Snapshot	Software provided by the storage subsystem, used to duplicate volumes within a storage subsystem. For more information, see the Copy-on-Write Snapshot manual.
CU (Control Unit)	A virtual control unit created in an enterprise-class storage subsystem. Also called a CU image. The LDEVs created in a storage subsystem are connected to a single CU, and a number is assigned to each CU for identifying the LDEVs. Therefore, volumes (LDEVs) in a storage subsystem are specified by the CU number (CU#) and LDEV number.
delta resync	A status in which synchronization processing is performed by copying differential data to a Universal Replicator copy pair that exists between a local site and a remote site in a 3DC Multi-Target configuration.
Device Manager	Software used for the operation and/or management of a system that uses multiple or different types of storage subsystems. Device Manager consists of a Device Manager server and a Device Manager agent.

DEVN (Device Number)	A device number that is assigned to identify an LDEV when it is being used by a mainframe system. A DEVN is expressed as a 4-digit hexadecimal number.
HiCommand Suite Common Component	A component that provides functionality common to all HiCommand products, including login, output log, and Web services. Installed as part of a Replication Monitor server.
HiCommand Suite common log file	A log file for detailed information on events such as server startup. Used to check errors that occur during Replication Monitor operation.
Host	The machine on which application programs are installed. Also called the *application server*.
host storage domain	A group of volumes (LUs) in a storage subsystem and the hosts that can access those LUs. A host storage domain is defined to improve LU security. Device Manager can be used to define a host storage domain using the host group set by the LUN security function of a storage subsystem, such as Universal Storage Platform V, TagmaStore USP, Lightning 9900V, or Thunder 9500V.
installation related trace log file	A log file of detailed processing information generated during installation and uninstallation of Replication Monitor. Used to trace the source of errors that occur during installation and uninstallation.
journal group	A group used in Universal Replicator as a unit to keep the integrity of the update order for a volume.
LDEV (Logical Device)	A volume created in an enterprise-class storage subsystem. Also called a logical device.
LU (Logical Unit)	A volume created in a midrange storage subsystem. Also called a *logical unit*. When an LDEV volume created in an enterprise-class storage subsystem is used from an open system host, it is treated as an LU.
LUN (Logical Unit Number)	A management number assigned to LUs in a storage subsystem. A LUN is a number assigned to identify LUs for the port in the storage system to which the LU is connected, either by port or by host group assigned to the port. An open system host uses a LUN to access a particular LU.
management client	The machine on which the Replication Monitor Web Client is executed. Issues instructions to the Replication Monitor server on the management server for basic Replication Monitor operations, such as pair configuration browsing, pair status monitoring and pair status modification.

management server	The machine on which a Replication Monitor server and its prerequisite program, a Device Manager server, are installed. The management server requests information such as copy pair configuration and status information and host information from all pair management servers and hosts, and provides this information to management clients.
MIB (Management Information Base)	The structure of information used by the SNMP protocol is defined. The MIB used for Replication Monitor defines the information set for alerts, such as monitored targets, conditions, and messages.
Pair	In this manual, *pair* means *copy pair*.
pair management server	A server for managing copy pairs and for collecting information about copy pair configuration and status. In an open system, a Device Manager agent, CCI, and a Replication Monitor agent are installed on the pair management server. Once a pair management server, which is independent of the host, is installed, the load on the host is reduced. In a mainframe system, a host on which Business Continuity Manager is installed is a pair management server.
pair status	Indicates the current status of the copy pair. Replication Monitor uses six status values: `error`, `suspend`, `copying`, `sync`, `simplex`, and `unknown`. Pair status is also called *copy pair status*.
paired volume	Denotes a primary and secondary volume pair linked by the volume replication function of the storage subsystem. Also called a *copy pair*. In this manual, *copy pair* is sometimes written simply as *pair*.
Prefix	The name of the prefix portion of the copy group definition file (*prefix*`.GRP.`*copy-group-id*) created by Business Continuity Manager. Replication Monitor uses the prefix as a unique name to identify copy group definition files created by Business Continuity Manager.
primary volume (P-VOL)	The source volume that is copied to another volume using the volume replication function of the storage subsystem.
property files	Generic term for the files that define the Replication Monitor operating environment. The Replication Monitor operating environment can be modified by changing the appropriate property files.
QuickShadow	Software provided by the storage subsystem, used to duplicate volumes within a storage subsystem. For more information, see the QuickShadow manual.

Refresh	The term *refresh* refers to updating the database that is maintained by the Replication Monitor server, by using the most recent information. This database stores copy pair configuration information and copy pair status information obtained from the Device Manager server, the Replication Monitor agent, and Business Continuity Manager.
Secondary-primary volume (SP-VOL)	The volume located in the middle of the cascade structure, when a cascade structure is used by the volume replication function of the storage subsystem. Indicates the secondary volume in an upper level copy pair and the primary volume in a lower level copy pair.
Secondary volume (S-VOL)	The destination volume to which the primary volume is copied using the volume replication function of the storage subsystem.
ShadowImage	Software provided by the storage subsystem, used to duplicate volumes within a storage subsystem. For more information, see the ShadowImage manual.
subsystem	An external storage device (storage subsystem) connected to the host. In this manual, *subsystem* means *storage subsystem*.
summary pair status, displaying	By displaying only the most significant copy pair status in the upper levels that contain the copy pairs (such as at the host level from the host perspective, or at the storage subsystem level from the subsystem perspective), Replication Monitor allows viewers to quickly check copy pair status. Replication Monitor determines the most significant copy pair status for each copy function (such as ShadowImage and TrueCopy) in turn.
TIC (Trouble Information Collector)	A Trouble Information Collector, used to collect information for a Device Manager agent and various agents installed on the same pair management server. The TIC included with version 5.6 or later of Device Manager agent can also collect log files and system information needed to perform a failure analysis of a Replication Monitor agent.
trace log file	A log file containing detailed program processing information, used to analyze program processing in the event of an error during Replication Monitor operation.
TrueCopy	Software provided by the storage subsystem, used to duplicate volumes between storage subsystems. For more information, see the TrueCopy manual.
Universal Replicator	Software provided by the storage subsystem and used to asynchronously duplicate volumes between storage subsystems. For more information, see the Universal Replicator manual.
volume	A collective name for the logical devices (LDEVs) and logical units (LUs) that are created in the storage subsystem.

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.

Acronyms and Abbreviations

CCI	Command Control Interface
CSV	comma separated value
CU	Control Unit
DEVN	DEVice Number
DKC	DisK Controller
FTP	File Transfer Protocol
GUI	Graphical User Interface
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol Security
IP	Internet Protocol
LAN	Local Area Network
LDEV	Logical DEVice
LU	Logical Unit
LUN	Logical Unit Number
MSCS	Microsoft Cluster Service
NAT	Network Address Translation
OS	Operating System
P-VOL	Primary Volume
RAID	Redundant Array of Independent Disks
SAN	Storage Area Network
SP	Service Pack
SP-VOL	Secondary-Primary Volume
SSL	Secure Sockets Layer
S-VOL	Secondary Volume
TCA	TrueCopy Async
TCE	TrueCopy Extended Distance
TCS	TrueCopy Sync
UDP	User Datagram Protocol
URL	Uniform Resource Locator
USP	Universal Storage Platform
USP V	Universal Storage Platform V
VCS	VERITAS Cluster Service

Index

S

T

U

V

W