HITACHI
DATA SYSTEMS

HiCommand® Device Manager Server Installation and Configuration Guide

MK-91HC002-21

Trademarks

OS/390 is a trademark of International Business Machines Corporation in the United States, other countries, or both.

RC2 is a registered trademark or trademark of RSA Security Inc. in the United States and/or other countries.

RC4 is a registered trademark or trademark of RSA Security Inc. in the United States and/or other countries.

Red Hat is a trademark or a registered trademark of Red Hat Inc. in the United States and other countries.

RSA is a registered trademark or trademark of RSA Security Inc. in the United States and/or other countries.

Java, JavaScript, Solaris, Sun, and Sun StorEdge are trademarks of Sun Microsystems, Inc.

SPARC is a registered trademark of SPARC International, Inc. Products bearing SPARC trademarks are based upon an architecture developed by Sun Microsystems, Inc.

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

Win32 is a registered trademark of Microsoft Corp. in the U.S. and other countries.

VMware and ESX Server are trademarks of VMware, Inc.

InstallAnywhere is a registered trademark of Zero G Software, Inc.

Windows Vista is either a registered trademark or trademark of Microsoft Corporation in the United States and/or other countries.

z/OS is a trademark of International Business Machines Corporation in the United States, other countries, or both.

This product includes software developed by Ben Laurie for use in the Apache-SSL HTTP server project.

This product includes software developed by Ralf S. Engelschall <rse@engelschall.com> for use in the mod_ssl project (http://www.modssl.org/).

HiCommand(R) Device Manager includes RSA BSAFE Cryptographic software from RSA Security Inc.

This product includes software developed by Borland Software Corp.

Portions of this software were developed at the National Center for Supercomputing Applications (NCSA) at the University of Illinois at Urbana-Champaign.

The file of interclient.jar was extracted from the InterClient Solaris version 2.0 as of November 15th, 2002, which "Original Code" was created by InterBase Software Corp and its successors, and which portions created by Borland/Inprise are Copyright © Borland/Inprise. All Rights Reserved.

This product includes altered versions of software originally developed by Henry Spencer.

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

Notice of Export Controls

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

Document Revision Level

Revision	Date	Description
MK-91HC002-00	September 2001	Initial Release
MK-91HC002-01	October 2001	Revision 1, supersedes and replaces MK-91HC002-00
MK-91HC002-02	November 2001	Revision 2, supersedes and replaces MK-91HC002-01
MK-91HC002-03	January 2002	Revision 3, supersedes and replaces MK-91HC002-02
MK-91HC002-04	February 2002	Revision 4, supersedes and replaces MK-91HC002-03
MK-91HC002-05	June 2002	Revision 5, supersedes and replaces MK-91HC002-04
MK-91HC002-06	November 2002	Revision 6, supersedes and replaces MK-91HC002-05
MK-91HC002-07	May 2003	Revision 7, supersedes and replaces MK-91HC002-06
MK-91HC002-08	July 2003	Revision 8, supersedes and replaces MK-91HC002-07
MK-91HC002-09	September 2003	Revision 9, supersedes and replaces MK-91HC002-08
MK-91HC002-10	February 2004	Revision 10, supersedes and replaces MK-91HC002-09
MK-91HC002-11	April 2004	Revision 11, supersedes and replaces MK-91HC002-10
MK-91HC002-12	August 2004	Revision 12, supersedes and replaces MK-91HC002-11
MK-91HC002-13	October 2004	Revision 13, supersedes and replaces MK-91HC002-12
MK-91HC002-14P	March 2005	Preliminary release of Revision 14, supersedes and replaces MK-91HC002-13
MK-91HC002-14	June 2005	Revision 14, supersedes and replaces MK-91HC002-14P
MK-91HC002-15	July 2005	Revision 15, supersedes and replaces MK-91HC002-14
MK-91HC002-16	September 2005	Revision 16, supersedes and replaces MK-91HC002-15
MK-91HC002-17	February 2006	Revision 17, supersedes and replaces MK-91HC002-16

MK-91HC002-18	June 2006	Revision 18, supersedes and replaces MK-91HC002-17
MK-91HC002-19	November 2006	Revision 19, supersedes and replaces MK-91HC002-18
MK-91HC002-20	February 2007	Revision 20, supersedes and replaces MK-91HC002-19
MK-91HC002-21	June 2007	Revision 21, supersedes and replaces MK-91HC002-20

Preface

This document describes how to install and operate HiCommand Device Manager (hereafter abbreviated to Device Manager) and HiCommand Suite Common Component. It also includes troubleshooting for these program products.

This user's guide assumes that you as a user have basic knowledge of the following:

- Management tools appropriate to the individual storage subsystem
- Storage Area Networks (SANs)
- The Windows, Solaris, or Linux operating system required for Device Manager

Please contact your Hitachi Data Systems account team or see the Hitachi Data Systems worldwide web site (http://www.hds.com) for additional information on subsystem features and functions.

Notes:

- This product includes software developed by Greg Stein <gstein@lyra.org> for use in the mod_dav module for Apache (http://www.webdav.org/mod_dav/).
- This product includes software developed by the Apache Software Foundation (http://www.apache.org/).
- This product includes software developed by the University of California, Berkeley and its contributors.
- This software contains code derived from the RSA Data Security Inc. MD5 Message-Digest Algorithm, including various modifications by Spyglass Inc., Carnegie Mellon University, and Bell Communications Research, Inc (Bellcore).

Software Version

This document revision applies to HiCommand Device Manager version 5.7.

Convention for Storage Capacity Values

Storage capacity values for hard disk drives are calculated based on the following values:

1 KB (kilobyte) = 1,000 bytes
1 MB (megabyte) = $1,000^2$ bytes
1 GB (gigabyte) = $1,000^3$ bytes
1 TB (terabyte) = $1,000^4$ bytes

Storage capacity values for logical devices (LDEVs) on the Universal Storage Platform 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 Web Client User's Guide*, MK-91HC001
- *HiCommand Device Manager Command Line Interface (CLI) User's Guide*, MK-91HC007
- *HiCommand Device Manager Agent Installation Guide*, MK-92HC019
- *Hitachi TagmaStore Universal Storage Platform and Network Storage Controller Storage Navigator User's Guide*, MK-94RD206
- *Hitachi TagmaStore(R) Adaptable Modular Storage and Workgroup Modular Storage Account Authentication User's Guide*, MP-96DF797.

Readme and Release Notes Contents

These files can be found on the installation CD. They contain requirements that may not be fully described in this manual. Be sure to review these files before installation.

Comments

Please send us your comments on this document. Make sure to include the document title, number, and revision. Please see 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 Introduction to HiCommand Device Manager

This chapter discusses the following topics:

- Overview of HiCommand Device Manager (see section 1.1)
- HiCommand Device Manager Software Components (see section 1.2)
- Basic Configuration (see section 1.3)
- Common Component (see section 1.4)
- Related Software Products (see section 1.5)
- New Functions in HiCommand Device Manager 5.7 (see section 1.6)

1.1 Overview of HiCommand Device Manager

HiCommand Device Manager provides a consistent, easy to use, and easy to configure interface for managing storage products. Device Manager provides a web-based graphical client interface for real-time interaction with managed storage arrays, as well as a command line interface (CLI) for scripting. Device Manager gives storage administrators access to the configuration, monitoring, and management features that are already integrated into existing Hitachi Data Systems software products.

Device Manager allows you to view the configuration of the storage subsystems added to the Device Manager system, and perform configuration operations such as allocating storage or securing LUNs. You can quickly discover storage subsystems based on key attributes, and efficiently manage complex and heterogeneous storage environments, even remotely through SSL-based communications. Device Manager also enables you to back up and restore your configuration database.

More specifically, HiCommand Device Manager provides:

- Storage subsystem discovery and configuration display
- Hierarchical group management for storage
- Alert presentation
- Volume (LUN) configuration
- Management of hosts and WWNs.
- Remote access to Disk Array Management Program (DAMP)

Device Manager also provides several levels of access and functionality for end users, including Access Control, Storage Management and System Support:

- Access Control handles support for the system administrator, storage administrator, maintenance user and guest user
- Storage Management handles storage configuration and manipulation
- System Support handles user administration, monitoring host agent activity and management of LUN security

Caution: When you change storage subsystem configuration information using HiCommand Device Manager, we recommend that you back up the information beforehand. For details on how to back up such information, see the manual for the relevant subsystem.

Important: HiCommand Device Manager cannot be used to set information for mainframe volumes in a mainframe system. However, it can be used to reference such volume information when that information is handled by Universal Storage Platform V, TagmaStore USP, Lightning 9900V, or Lightning 9900.

1.2 HiCommand Device Manager Software Components

This document describes and provides instructions for installing and configuring the Device Manager Server. HiCommand Device Manager consists of the following basic components:

Server. Device Manager Server communicates with Hitachi Data Systems 9900 V Series, 9900, 9500 V Series, and 9200 storage subsystems. In addition, the Device Manager Server manages client connections with the Device Manager Web Client and the Device Manager Host Agent(s) using the http protocol. The Device Manager Agent and the Device Manager Server can be installed on the same host machine.

Web Client. Device Manager Web Client is a web-based user interface for Device Manager functionality. The Web Client is a stand-alone Java-based application that is deployed using the Java Web Start (JWS) software. It communicates with and runs as a client of the Device Manager Server. For further information on Device Manager Web Client, see the *HiCommand Device Manager Web Client User's Guide*.

Command Line Interface (CLI). Device Manager CLI enables you to perform client operations by issuing commands from the system command-line prompt. For further information on the command-line interface, see the *HiCommand Device Manager Command Line Interface Application User Guide*.

Host Agent. Device Manager agent on a host runs on host computers attached to storage subsystems managed by Device Manager. The Host Agent collects data on the configuration and utilization of the attached storage and sends this information to the Device Manager Server. For further information on the Device Manager Host Agent, see the *HiCommand Device Manager Agent Installation Guide*. The Device Manager Agent and the Device Manager Server can be installed on the same host machine.

Device Manager VDS Provider. The Device Manager VDS provider is software that allows you to provide storage subsystem information in response to requests from VDS (Virtual Disk Service), a virtual disk service provided by Windows Server 2003, and to change storage subsystem configuration.

1.3 Basic Configuration

Figure 1.1 shows a basic Device Manager system configured for storage subsystem configuration management.

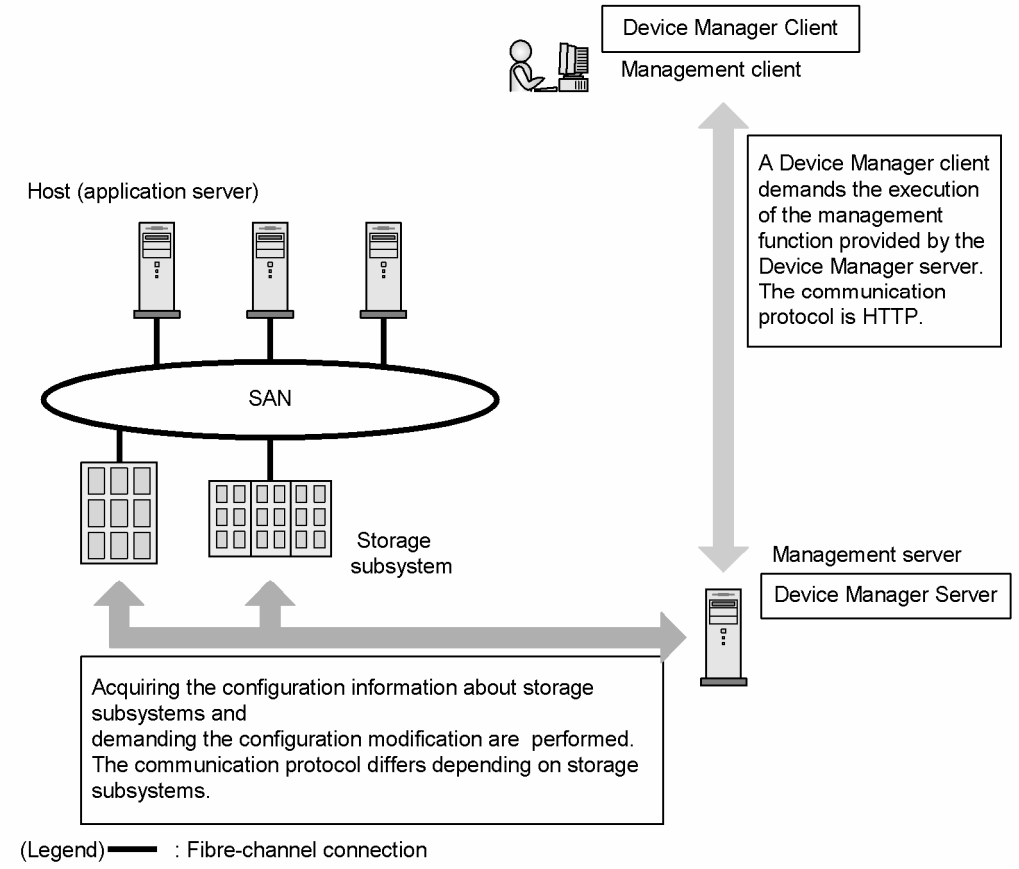

Figure 1.1 Basic System Configuration of Device Manager

When you need only to manage the configuration of storage subsystems, and do not need to manage the storage usage statuses from a host, you can construct the type of system illustrated in Figure 1.1

Note the following about Figure 1.1:

- The *management client* refers to the machine on which a Device Manager client runs.
- The *management server* refers to the machine on which the Device Manager server runs.
- A management client and a management server can be the same machine.
- The *host* refers to the machine that uses the volumes provided by a storage subsystem.
- A TCP/IP network must connect the management client and the management server.
- The HTTP protocol is used for communications.
- A TCP/IP network must connect the management server and the storage subsystem.
- The communication protocol used between a management server and a storage subsystem varies from one storage subsystem to another.
- A management server and a management client need not be connected to a storage subsystem by a Fibre Channel connection.

1.4 Common Component

HiCommand Suite Common Component is a package of features that are used by all HiCommand Suite products. It is installed as part of the Device Manager installation. The Common Component is discussed in detail in Chapter 5. Each HiCommand Suite product bundles the Common Component to use the following functions:

- HBase Storage Mgmt Common Service
- Integrated logging and repository
- HBase Storage Mgmt Web Service

1.5 Related Software Products

1.5.1 Required Products for the Storage Subsystem

When managing storage subsystems, you use management tools and application program interfaces (APIs) other than the HiCommand Device Manager components.

Caution: When you replace the microcode for a storage subsystem that is already registered as a Device Manager management target, you do not need to stop the HiCommand Device Manager server. Note, however, that the configuration of the storage subsystem must not be changed at this time (by performing, for example, refresh and path operations). After the microcode has been successfully replaced, refresh the storage subsystem.

Caution: When Physical View of the TagmaStore Universal Storage Platform(USP) or Storage Navigator of the Lightning 9900V is launched, Java Web Start and the web browser on the Web Client machine directly communicate with the storage subsystem. For this reason, if the Web Client machine and the storage subsystem exist on different networks, you must set up the networks so that the machine and the storage subsystem can directly communicate with each other.

This section describes the storage subsystem requirements for using Device Manager.

1.5.1.1 Required for Universal Storage Platform V

The following table lists the prerequisite firmware versions and software products:

Table 1.1 Prerequisite Firmware Versions and Software Products (for Universal Storage Platform V)

Prerequisite firmware versions	Prerequisite software products
▪ Controller microcode: 60-01-24-*xx*/*xx* or later ▪ Controller microcode to use the Universal Replicator setup function: 60-01-24-*xx*/*xx* or later ▪ Controller microcode to use the function that allows LU creation and LU formatting to be performed separately: 60-01-24-*xx*/*xx* or later	▪ Java API ▪ SNMP API ▪ LUN Manager To use functions for creating a LUSE or LDEV (CVS): ▪ OPEN Volume Management To use the copy pair functionality: ▪ ShadowImage ▪ TrueCopy ▪ Universal Replicator ▪ Copy-on-Write Snapshot# To use Physical View: ▪ Storage Navigator To use Universal Volume Manager: ▪ Universal Volume Manager To use storage logical partitioning (SLPR) or cache logical partitioning (CLPR): ▪ Virtual Partition Manager

For details on the models that support Copy-on-Write Snapshot, see the *Copy-on-Write Snapshot User's Guide*.

1.5.1.2 Required for the TagmaStore AMS/WMS Series

The Linux version does not support the TagmaStore AMS/WMS series.

The following table describes the prerequisite firmware versions and software products:

Table 1.2 Prerequisite Firmware Versions and Software Products (for the TagmaStore AMS/WMS Series)

Prerequisite Firmware Versions	Prerequisite Software Products
▪ TagmaStore AMS microcode: Any	To set up security for LUNs: ▪ LUN Manager#1

Prerequisite Firmware Versions	Prerequisite Software Products
▪ TagmaStore WMS microcode: Any	To use LUSE: ▪ LUN Expansion To use a lock system for devices accessed from HiCommand Device Manager: ▪ Password Protection ▪ Account Authentication#2 To use the copy pair functionality: ▪ ShadowImage in-system replication ▪ TrueCopy remote replication#3 ▪ TrueCopy Extended Distance ▪ Copy-on-Write Snapshot#4 To use Physical View: ▪ Storage Navigator Modular (for Web)

#1 If you want to use HiCommand Device Manager to configure LUN security, you need to use Storage Navigator Modular (for Web) or DAMP (for Web) to enable the mapping mode of LUN Manager. Make sure that the mapping mode of the storage subsystem is *M-TID*, *M-LUN*. When the mapping mode is disabled, you cannot use LUN Manager.

#2 For notes on using Account Authentication, see section 9.1.4.

#3 For details on the models that support TrueCopy, see the *TrueCopy Remote Replication User's Guide*.

#4 For details on the models that support Copy-on-Write Snapshot, see the *Copy-on-write SnapShot User's Guide*.

Caution: The Device Manager server communicates over TCP/IP to manage the TagmaStore AMS/WMS series and Thunder 9500V series storage subsystems. If you want to change the default port number (2000) used by all these storage subsystems for TCP/IP communication, you must set the new port number in the `services` file for the machine where the Device Manager server has been installed. If you operate the storage subsystems without setting the new port number in the `services` file, an error (code:`DMEA000006`) might occur and the operation might fail. If the port number of some storage subsystems is set to the default (2000) and the port number of other storage subsystems is set to a new number, and the new port number is specified in the `services` file, an error does not occur (although the operation might take a long time). For details on how to check the port number and how to set the `services` file, see the manual for the TagmaStore AMS/WMS series and Thunder 9500V series.

Note: For a NAS Modular subsystem of the TagmaStore AMS/WMS series, HiCommand Device Manager only allows you to add storage subsystems and to launch Storage Navigator Modular. To operate a NAS Modular subsystem, perform the operations from Storage Navigator Modular.

1.5.1.3 Required for TagmaStore USP

The following table describes the prerequisite firmware versions and software products:

Table 1.3 Prerequisite Firmware Versions and Software Products (for TagmaStore USP)

Prerequisite Firmware Versions	Prerequisite Software Products
▪ Controller microcode: 50-00-00-*xx*/*xx* or later ▪ Controller microcode to use CLIEX functions: 50-03-95-*xx*/*xx* or later ▪ Controller microcode to use the Virtual Partition Manager view function: 50-03-xx-xx/xx or later ▪ Controller microcode to use the Universal Replicator view function: 50-03-xx-xx/xx or later ▪ Controller microcode to use the Universal Replicator setup function: 50-05-37-*xx*/*xx* or later ▪ Controller microcode to use Universal Volume Manager to view the setting status of a remote command device: 50-07-00-xx/xx or later ▪ Controller microcode to use 3DC functionality: 50-08-00-*xx*/*xx* or later ▪ Controller microcode to use the function that allows LU creation and LU formatting to be performed separately: 50-09-00-*xx/xx* or later ▪ Controller microcode to use the function for acquiring the status of an LDEV: 50-09-00-xx/xx or later	▪ Java API ▪ SNMP API ▪ LUN Manager To use functions for creating a LUSE or LDEV (CVS): ▪ OPEN Volume Management To use the copy pair functionality: ▪ ShadowImage ▪ TrueCopy ▪ TrueCopy Asynchronous ▪ Universal Replicator ▪ Copy-on-Write Snapshot# To use Physical View: ▪ Storage Navigator To link with NAS Manager: ▪ NAS Blade Manager To use Universal Volume Manager: ▪ Universal Volume Manager To use storage logical partitioning (SLPR) or cache logical partitioning (CLPR): ▪ Virtual Partition Manager

For details on the models that support Copy-on-Write Snapshot, see the *Copy-on-Write Snapshot User's Guide*.

1.5.1.4 Required for Lightning 9900V

The following table describes the prerequisite firmware versions and software products:

Table 1.4 Prerequisite Firmware Versions and Software Products (for Lightning 9900V)

Prerequisite Firmware Versions	Prerequisite Software Products
▪ Controller microcode: 21-01-25-*xx*/*xx* or later ▪ Controller microcode to perform in-context launching of the Storage Navigator: 21-04-04-*xx*/*xx* or later ▪ Controller microcode to launch NAS Manager: 21-04-00-*xx*/*xx* or later ▪ Controller microcode to use CLIEX functions: 21-14-02-*xx*/*xx* or later	▪ Java API ▪ SNMP API ▪ LUN Management To use functions for creating a LUSE or LDEV (CVS): ▪ Open Volume Management To use the copy pair functionality: ▪ Hitachi ShadowImage ▪ Hitachi TrueCopy To link with Storage Navigator: ▪ Storage Navigator To link with NAS Manager: ▪ NAS/Management

For more information on installing and configuring program products, see the *9900V Remote Console – Storage Navigator User's Guide*.

1.5.1.5 Required for Lightning 9900

The following table describes the prerequisite firmware versions and software products:

Table 1.5 Prerequisite Firmware Versions and Software Products (for Lightning 9900)

Prerequisite Firmware Versions	Prerequisite Software Products
▪ Controller microcode: 01-18-09-00/00 or later ▪ Controller microcode to use CLIEX functions: 01-19-59-*xx*/*xx* or later	▪ SNMP Agent ▪ LUN Manager (LUNM) To set up security for LUNs: ▪ LUN Security To use functions for creating a LUSE or LDEV (CVS): ▪ LU Size Expansion (LUSE) ▪ Open Customizable Volume Size (OCVS) To use the copy pair functionality: ▪ Hitachi Multi-RAID Coupling Feature ▪ Hitachi Remote Copy ▪ Hitachi Remote Copy Asynchronous

Requirements not related to firmware versions or software products are as follows:

If you are setting up an alias for HPAV (Hitachi Parallel Access Volume), the LDEV number assigned for both the base volume and the alias volume must be in the same 32-LDEV boundary (for example, 0 to 31, 32 to 63). If they are not the same, you may get the following error message when you try to create an LDEV:

The volume to be created by the CVS operation is being used as the MAV function.

- For more information on PAV, see *Hitachi Parallel Access Volume User's Guide*.
- For more information on installing and configuring program products, see *Hitachi Lightning 9900 Remote Console User's Guide*.

1.5.1.6 Required for Thunder 9500V

Caution: The Linux version does not support Thunder 9500V.

The following table describes the prerequisite firmware versions and software products:

Table 1.6 Prerequisite Firmware Versions and Software Products (for Thunder 9500V)

Prerequisite Firmware Versions	Prerequisite Software Products
▪ Thunder 9570V or Thunder 9530V microcode: 0651 or later ▪ Thunder 9580V microcode: 1655/B or later ▪ Thunder 9585V microcode: 1657/A or later ▪ Microcode required to use QuickShadow: 0655/D or later#1, 1655/D or later#2 ▪ Microcode required to use SATA expansion enclosure: 0658 or later#1, 1658 or later#2	To set up security for LUNs: ▪ Fibre security control functionality or LUN Management#3 To use LUSE: ▪ LUN Expansion To use a lock system for devices accessed from HiCommand Device Manager: ▪ Password Protection To use the copy pair functionality: ▪ Hitachi ShadowImage ▪ Hitachi TrueCopy Basic ▪ Hitachi QuickShadow

#1: For Thunder 9570V or Thunder 9530V

#2: For Thunder 9580V or Thunder 9585V

#3 If you want to use HiCommand Device Manager to configure LUN security, you need to use Storage Navigator Modular (for Web) or DAMP (for Web) to enable the mapping mode of LUN Manager. When the mapping mode is disabled, you cannot use LUN Manager.

Requirements not related to firmware versions or software products are as follows:

- Before installation, use DAMP (for Web) or Storage Navigator Modular (for Web) to verify that there are no ports with a WWN node name consisting only of zeros. If there are, you must change the name or delete the WWN, or a node-name error message will be output.
- If the Password Protection option is installed and usable, any addition of a storage subsystem to HiCommand Device Manager requires a Password Protection user ID and password.

Caution: The Device Manager server communicates over TCP/IP to manage the TagmaStore AMS/WMS series and Thunder 9500V series storage subsystems. To change the default port number (2000) used by all these storage subsystems for TCP/IP communication, you must set the new port number in the `services` file for the machine where the Device Manager server has been installed. If you operate the storage subsystems without setting the new port number in the `services` file, an error (code:`DMEA000006`) might occur and the operation might fail. If the port number of some storage subsystems is set to the default (2000) and the port number of other storage subsystems is set to a new number, and the new port number is specified in the `services` file, an error does not occur (although the operation might take a long time). For details on how to check the port number and how to set the `services` file, see the manual for the TagmaStore AMS/WMS series and Thunder 9500V series.

1.5.1.7 Required for Thunder 9200

Caution: The Linux version does not support Thunder 9200.

Note: SCSI models are not supported.

The following table describes the prerequisite firmware versions and software products:

Table 1.7 Prerequisite Firmware Versions and Software Products (for Thunder 9200)

Prerequisite Firmware Versions	Prerequisite Software Products
Microcode: 0559 or later, 355E or later	To set up security for LUNs: ▪ Fibre security control functionality To use LUSE: ▪ LU integration functionality To use a lock system for devices accessed from HiCommand Device Manager: ▪ Password Protection To use the copy pair functionality: ▪ MRCF-Lite Remote Pack ▪ Synchronous Remote Copy function

Requirements not related to firmware versions or software products are as follows:

- Make sure that fibre-channel ports are supported, because HiCommand Device Manager does not support SCSI models.
- Make sure that the mapping mode of the storage subsystem is M-TID, M-LUN. If you attempt to perform an LUN management operation from HiCommand Device Manager when the mapping mode is not M-TID, M-LUN, an error may occur.

Important: Do not use Dynamic Host Configuration Protocol (DHCP) when you use Device Manager to manage the storage subsystem. Use DAMP (for Web) or Storage Navigator Modular (for Web) to make sure that DHCP is not selected.

Note: The Thunder 9200 series supports functionality to reserve LUNs for volumes that are not defined on it. If a user tries to assign such a reserved LUN to the storage unit for an applicable port, Device Manager displays an error message.

1.5.1.8 Required for SUN T3

Device Manager versions 5.7 and later do not support T3. If a T3 storage subsystem still remains as a Device Manager management target after upgrading Device Manager, use Web Client or the CLI to remove the T3 storage subsystem from the targets of Device Manager management. For details on Web Client, see the *HiCommand Device Manager Web Client User's Guide*. For details on the CLI, see the *HiCommand Device Manager Command Line Interface (CLI) User's Guide*.

1.5.2 Products Related to Device Manager

Dynamic Link Manager manages the storage access paths to and from the host on which it is installed. The Dynamic Link Manager GUI can be displayed from Device Manager Web Client. For more information on Dynamic Link Manager, please see the following documents.

When Dynamic Link Manager 5.8 or later is installed on the host:

- *HiCommand Dynamic Link Manager User's Guide (for AIX)*
- *HiCommand Dynamic Link Manager User's Guide (for Solaris)*
- *HiCommand Dynamic Link Manager User's Guide (for HP-UX)*
- *HiCommand Dynamic Link Manager User's Guide (for Linux)*
- *HiCommand Dynamic Link Manager User's Guide (for Windows)*

When the version of Dynamic Link Manager installed on the host is earlier than 5.8:

- *Hitachi Dynamic Link Manager User's Guide for AIX Subsystems.*
- *Hitachi Dynamic Link Manager User's Guide for HP-UX Subsystems.*
- *Hitachi Dynamic Link Manager User's Guide for Linux Subsystems.*
- *Hitachi Dynamic Link Manager User's Guide for Sun Solaris Subsystems.*
- *Hitachi Dynamic Link Manager User's Guide for Windows NT and Windows 2000 Subsystems.*

Note: The following table describes the versions of Dynamic Link Manager that can be displayed from Device Manager's Web Client.

Table 1.8 Versions of Dynamic Link Manager Supported by Device Manager

Host Machine Platform	Dynamic Link Manager Version
Windows	4.0 or later
Solaris	3.0, 3.0.2, 4.0 or later
AIX	4.0 or later
HP-UX	4.0 or later
Linux	4.0 or later

HiCommand Tuning Manager manages storage performance and capacity, and is installed on a host. You can install Tuning Manager and Device Manager in different hosts. The Tuning Manager GUI can be displayed from Device Manager Web Client.

WARNING: Do not install Tuning Manager version 4.0 or higher on the same server as Device Manager version 4.0 or higher.

For more information on Tuning Manager please see the following documents:

- *HiCommand Tuning Manager Administration Guide*.
- *HiCommand Tuning Manager Reference Guide*.
- *HiCommand Tuning Manager User's Guide*.
- *HiCommand Tuning Manager Installation Guide*.
- *HiCommand Tuning Manager Performance Reporter User's Guide*.

Note: The following table describes the versions of Tuning Manager supported by Device Manager.

Table 1.9 Versions of Tuning Manager Supported by Device Manager

Platform	Tuning Manager Version
Windows	1.0.1 or later
Solaris	1.0.1 or later

Provisioning Manager is a product whose purpose is to assign volumes to the server, and to expand file systems easily. Assigning volumes or expanding file systems requires a series of operations such as selecting the most appropriate storage for use, creating device files on the server, and creating and mounting file systems. Provisioning Manager automates such operations, reducing the workload on system administrators. For more information about Provisioning Manager, see the Provisioning Manager documentation:

- *HiCommand Provisioning Manager Installation and Configuration Guide*
- *HiCommand Provisioning Manager User's Guide*.

Note: The following table describes the versions of Provisioning Manager supported by Device Manager.

Table 1.10 Versions of Provisioning Manager Supported by Device Manager

Platform	Provisioning Manager Version
Windows	3.5.0 or later
Solaris	3.5.0 or later
Linux	5.1.0 or later

Protection Manager systematically controls storage subsystems, backup-management products, database products, and application products. If you are using Protection Manager, you will need Windows version 3.5 or later. For more information about HiCommand Protection Manager, please see the following documents:

- *HiCommand Protection Manager Command Line Interface User's Guide*.
- *HiCommand Protection Manager Command Reference User's Guide*.
- *HiCommand Protection Manager Error Codes*.
- *HiCommand Protection Manager Console User's Guide*.

Note: The following table describes the versions of Protection Manager supported by Device Manager.

Table 1.11 Versions of Protection Manager Supported by Device Manager

Platform	Protection Manager Version
Windows	3.5 or later

Tiered Storage Manager provides a method of transferring data to an appropriate storage subsystem according to the data characteristics (severity level and access frequency). Tiered Storage Manager optimizes the arrangement of data in an environment in which multiple storage subsystems have been centralized by using Universal Storage Platform V and TagmaStore USP. For more information about Tiered Storage Manager, see the Tiered Storage Manager documentation.

Note: The following table describes the versions of Tiered Storage Manager supported by Device Manager.

Table 1.12 Versions of Tiered Storage Manager Supported by Device Manager

Platform	Tiered Storage Manager Version
Windows	4.0.0-01 or later
Solaris	4.3.0 or later

Replication Monitor displays the copy pair configuration for the entire system in a way that is easy to understand from the viewpoint of the configuration definition of hosts, storage subsystems, and copy pairs. You can also set up monitoring so that Replication Monitor automatically notifies the user when an error is detected. For more information about Replication Monitor, see the Replication Monitor documentation.

Note: The following table describes the versions of Replication Monitor supported by Device Manager.

Table 1.13 Versions of Replication Monitor Supported by Device Manager

Platform	Replication Monitor Version
Windows	4.0 or later
Solaris	4.0 or later

Global Link Availability Manager provides centralized management of all paths when Dynamic Link Manager is installed on multiple hosts. This can reduce the administrator's workload in a large-scale system because path management does not have to be performed separately for each host. The Global Link Availability Manager GUI can be displayed from Device Manager Web Client. For details on Global Link Availability Manager, see the Global Link Availability Manager documentation.

Note: The following table describes the versions of Global Link Availability Manager supported by Device Manager.

Table 1.14 Versions of Global Link Availability Manager Supported by Device Manager

Platform	Global Link Availability Manager Version
Windows	5.0 or later
Solaris	5.0 or later

Mainframe Agent provides volume information on the storage subsystems managed by a mainframe host. This allows subsystems that could only be monitored on the mainframe host system to be monitored from a Device Manager client program, thereby facilitating centralized management of distributed resources. For details on Mainframe Agent, see the Mainframe Agent documentation. For information on setting the environment to link with Mainframe Agent, see the *HiCommand Device Manager Command Line Interface (CLI) User's Guide*.

Table 1.15 Versions of Mainframe Agent Supported by Device Manager

Mainframe host platform	Mainframe Agent Version
OS/390 (version: 2.10)	5.1 or later
z/OS (version: 1.4, 1.5, 1.6, or 1.7)	5.1 or later

HiCommand NAS Manager sets up, operates, and manages a NAS system on a TagmaStore AMS/WMS series storage subsystem. You can display the HiCommand NAS Manager GUI from Web Client. For details on HiCommand NAS Manager, see the manuals for HiCommand NAS Manager.

Caution: To display the HiCommand NAS Manager GUI from Web Client, install Device Manager 5.6 or later, and then install HiCommand NAS Manager. If you install HiCommand NAS Manager before installing Device Manager, you cannot display the HiCommand NAS Manager GUI from Web Client.

Note: The following table lists the versions of HiCommand NAS Manager supported by Device Manager.

Table 1.16 Versions of HiCommand NAS Manager Supported by Device Manager

Platform	NAS Manager Version
Windows	5.0 or later

Command Control Interface (CCI) is installed on a host, and manages TagmaStore, AMS, 9900V, 9900, 9500V and 9200 series from the command line. CCI tasks include collecting information about storage pair configurations and reporting the information to the Device Manager server. For more information about CCI, please see the following documents:

- *Hitachi TagmaStore USP and NSC, Lightning 9900 V Series and 9900 Command Control Interface (CCI) User's Guide*
- *Hitachi Thunder 9500 V Series Command Control Interface (CCI) User and Reference Guide*
- *Hitachi Thunder 9200 Command Control Interface (CCI) User and Reference Guide*

TrueCopy can create a replica of one or more volumes in a remote subsystem. For more information on TrueCopy, please see the following documents:

- *Hitachi TrueCopy Use's Guide'*
- *Hitachi TagmaStore USP and NSC TrueCopy User and Reference Guide*
- *Hitachi Lightning 9900 V Series TrueCopy User and Reference Guide*
- *Hitachi Lightning 9900 TrueCopy User and Reference Guide*
- *Hitachi Thunder 9500 V Series TrueCopy User's Guide*
- *Hitachi Thunder 9200 TrueCopy User's Guide*
- *Hitachi TagmaStore Adaptable Modular Storage TrueCopy Synchronous Remote Replication Software User's Guide*

Universal Replicator, which was developed from a TrueCopy function, can create a replica of volumes in another storage subsystem. For more information about Universal Replicator, please see the following documents:

- *Hitachi Universal Replicator User's Guide*
- *Hitachi TagmaStore USP and NSC Universal Replicator User's Guide*

Hitachi Virtual Partition Manager allows you to partition the storage and the cache of a TagmaStore subsystem.

Note: If you use Device Manager to directly manage storage logical partitions, you will need a separate Device Manager server for each partition. If you use Device Manager to link and launch Storage Navigator, you can use a single server to manage a partitioned subsystem.

For more information about VPM, please see the following documents:

- *Hitachi Virtual Partition Manager User's Guide*
- *Hitachi TagmaStore USP and NSC Virtual Partition Manager User's Guide*
- *Hitachi TagmaStore Adaptable Modular Storage Cache Partition Manager User's Guide*

ShadowImage can create a replica of one or more volumes in the same subsystem. For more information on ShadowImage, please see the following documents:

- *Hitachi ShadowImage User's Guide*
- *Hitachi TagmaStore USP and NSC ShadowImage User's Guide*

- *Hitachi TagmaStore Adaptable Modular Storage ShadowImage In-System Replication Software User's Guide*
- *Hitachi Lightning 9900 V Series ShadowImage User's Guide*
- *Hitachi Lightning 9900 ShadowImage User's Guide*
- *Hitachi Thunder 9500 V Series ShadowImage User's Guide*
- *Hitachi Thunder 9200 ShadowImage User's Guide*

Hitachi Copy on Write Snapshot allows you to internally retain a logical duplicate of the primary volume data, which is used to restore data if a logical error occurs in the primary volume. For more information on Copy on Write Snapshot, see the following documents:

- *Hitachi Copy-on-Write Snapshot User's Guide*
- *Hitachi TagmaStore* USP *Copy-on-Write Snapshot User's Guide*
- *Hitachi TagmaStore Adaptable Modular Storage Copy-on-write SnapShot Software User's Guide*
- *Hitachi Freedom Storage Thunder 9500 V Series Copy-on-Write Snapshot Software User's Guide*

HiCommand Storage Services Manager acts as the main console for heterogeneous storage infrastructure management software, providing SAN visualization and reporting, asset management, performance and capacity monitoring and planning, and policy-driven event management.

WARNING: Do not install HSSM on the same server as Device Manager.

For more information about Hitachi Storage Services Manager, please see the following documents:

- *HiCommand Storage Services Manager Installation and Configuration Guide*
- *User Guide for HiCommand Storage Services Manager, HiCommand Path Provisioning, and HiCommand Chargeback*
- *HiCommand Storage Services Manager CLI Guide*

1.6 New Functions in HiCommand Device Manager 5.7

HiCommand Device Manager 5.7 provides the following new functions:

- The Device Manager server now supports Universal Storage Platform V as a storage subsystem.
- The Open-Reserved group, which displays the open volumes that cannot be assigned a path, has been added to All Storage (My Storage) in Device Manager Web Client.
- Device Manager Web Client now supports the HDP function of Universal Storage Platform V.
  - The HDP volume attribute and HDP pool volume attribute are now supported as identifiable volume attributes.
  - The consumed capacity on an HDP volume can now be displayed.
  - A path can now be assigned to an HDP volume.
  - Copy pair operations for HDP volumes are now supported.
- Detailed Array Reports, which output LDEV detailed information in CSV format, have been added to the report functionality of Device Manager Web Client. CSV-formatted files can be output to the location specified in the Device Manager server properties.
- Device Manager Web Client can now display the actual amount of LDEV space in a storage subsystem.
- In the Device Manager server, by using the `hcmdssrv` command or performing an operation in the Windows Start menu, HiCommand Suite Common Component and all services of HiCommand Suite products can now be started and stopped at the same time.
- The `auto` option can now be specified in a command for operating a Device Manager server database. This option causes HiCommand Suite Common Component and all services of HiCommand Suite products to start or stop automatically before and after the database operation.
- In the Device Manager server, when installation or uninstallation is started, the services of HiCommand Suite products and HiCommand Suite Common Component can now be stopped automatically if they are running (in a non-cluster configuration).
- In the Device Manager server, it is now possible to select whether the services of HiCommand Suite products and HiCommand Suite Common Component are to be started automatically after installation or uninstallation is completed (in a non-cluster configuration).
- When the Device Manager server detects an alert that has occurred in a storage subsystem, the Device Manager server can now email the contents of the alert to any user.
- Device Manager VDS Provider can now obtain configuration information for the specified resource only.

HiCommand Device Manager 5.7 provides the following extensions:

- Support for new OSs
  - Device Manager Web Client now supports Windows Server 2003 SP2 and Windows Server 2003 R2 SP2.
  - Device Manager Web Client now supports Windows Vista and HP-UX 11i v3.
  - Device Manager server and Device Manager VDS Provider now supports Windows Server 2003 SP2, Windows Server 2003 x64 Edition SP2, and Windows Server 2003 R2 SP2.
- Support for new browsers
  - Device Manager Web Client now supports Internet Explorer 7.0.
  - In HP-UX 11i v3, Device Manager Web Client now supports Mozilla 1.7.13.01.
- Device Manager Web Client now supports JRE version 6.0.

For details about the new functions provided by Device Manager Web Client, see the *HiCommand Device Manager Web Client User's Guide*.

Chapter 2 HiCommand Device Manager Network Configuration

This chapter describes network configuration as it relates to security, as follows:

- Overview of Network Configuration (see section 2.1)
- Common Security Risks (see section 2.2)
- Server Network Configurations (see section 2.3)
- Working with a Network that Uses a Firewall (see section 2.4)
- Registering Firewall Exceptions in a Linux Environment (see section 2.5)
- Setting Up the Environment of a Server Machine That Has Multiple NICs (see section 2.6)

2.1 Overview of Network Configuration

Universal Storage Platform V, TagmaStore USP, Lightning 9900V, and Lightning 9900 come equipped with a *service processor*, which is usually abbreviated as *SVP*. The SVP has two Ethernet adapters. The first adapter is for a private (internal) Ethernet LAN, which is intended for intra-array communications only. There are only two devices that can access the internal LAN: the Service Processor (SVP), and the Remote Console for Lightning 9900. The second adapter is used for other applications to talk to the SVP. This LAN is referred to as the public LAN, because it is visible to other computers outside the array. HiCommand Device Manager, Enterprise Resource Manager and Enterprise Storage Resource Manager applications use the public LAN to communicate with the SVP about the array and configuration changes.

While Universal Storage Platform V, TagmaStore USP, Lightning 9900V, and Lightning 9900 are managed through their SVP interface, other managed storage subsystems (for example, the TagmaStore AMS/WMS series, Thunder 9500V, and Thunder 9200) do not have a private LAN. Instead, these storage subsystems have Ethernet network interfaces that are intended to be directly attached to a public LAN. Once attached to the LAN, each has its own remote management API, which can be accessed by a variety of management applications.

Warning: Universal Storage Platform V, TagmaStore USP, Lightning 9900V, and Lightning 9900 have a public LAN and a private LAN. Device Manager uses the public LAN to communicate with the SVP about the array and configuration changes. Do not under any circumstances attach the private LAN to an external network because this can cause serious problems on the array.

Figure 2.1 illustrates an **incorrect** LAN connection.

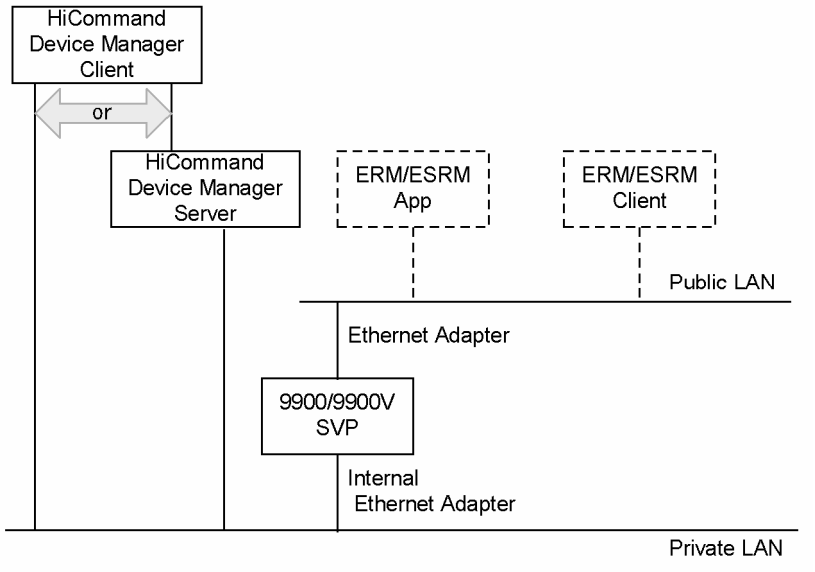

Figure 2.1 Incorrect Lightning 9900 and 9900V LAN Connection

2.2 Common Security Risks

The TagmaStore AMS/WMS series, Thunder 9500V, and Thunder 9200 are designed to be connected to a public LAN, so you must pay particular attention to security risks when you connect these subsystems to a public network.

System administrators frequently separate production LANs from management LANs. In such cases, management LANs act as a separate network, which isolates management traffic from a production network and reduces the risk of security-related threats. If a management controller such as the SVP exists on a production LAN, the storage subsystems are left open for any entity on the IP network to access. Whether the access is intentional or not, the resulting security risks can lead to actual outages characterized as Denial of Storage Service (DoS) attacks that may lead to a management session being hijacked for malignant purposes, such as unbinding a storage extent from a port during an I/O operation.

The following are guidelines for constructing management LANs:

- Traffic from the production LAN should not flow through, or be routed to the management LAN.
- If possible, all hosts with management interfaces or controllers on the management LAN should be hardened to their maximum level to reduce the potential that software other than the management interface will not lead to an exploit of the entire station or device. (In this case hardening should include removal of unnecessary software, shutting down nonessential services, and updating to the latest patches.)
- The management LAN should only intersect a production LAN on those hosts acting as an interface between the management LAN and the production LAN (for example, the HiCommand Device Manager Server).
- If possible, those hosts intersecting both private LAN and management LAN should be behind a firewall of some kind, further inhibiting unintended access.

2.3 Server Network Configurations

2.3.1 Most Secure Configuration: Separate Management LAN plus Firewall

In this case, the server hosting Device Manager must either be dual homed or have two NICs, and every other management application must be of similar configuration. The first NIC for each host is attached to a LAN dedicated to manage traffic between the management host and management-target devices. The management-target devices for HiCommand Device Manager include Universal Storage Platform V, TagmaStore USP, Lightning 9900V, Lightning 9900, the TagmaStore AMS/WMS series, Thunder 9500V, and Thunder 9200. A second NIC is attached to a LAN where access is governed by a firewall. As shown in Figure 2.2, each server could also be connected to a different LAN with a different firewall. The firewall contains strict access rules that allow access to the management servers only to Device Manager or specified management application clients.

This configuration is the most secure but least flexible implementation, as it requires overhead to manage all of the various network components, servers, and devices under management. Adding further security to this configuration requires that the underlying management application OS be hardened to the maximum possible limit. This might include disabling services such as Telnet, FTP, SMTP, or IIS. Additionally, all unnecessary packages should be removed if possible.

For a comprehensive overview of what is required to harden a server, see http://ist.uwaterloo.ca/security/howto/.

Caution: When Physical View of Universal Storage Platform V or TagmaStore USP, or Storage Navigator of Lightning 9900V is launched, Java Web Start and the web browser on the Web Client machine directly communicate with the storage subsystem. For this reason, if the Web Client machine and the storage subsystem exist on different networks, you must set up the networks so that the machine and the storage subsystem can directly communicate with each other.

Figure 2.2 illustrates a separate management LAN plus a firewall.

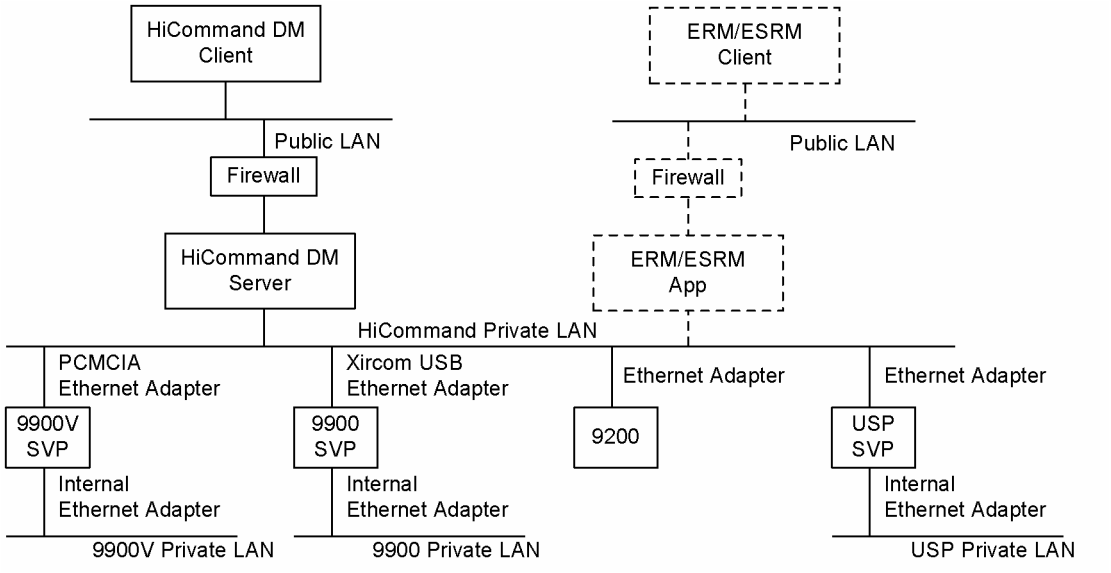

Figure 2.2 Most Secure Configuration: Separate Management LAN Plus Firewall

2.3.2 Second-Most Secure Configuration: Separate Management LAN plus Firewalled Devices under Management

In this configuration, the server hosting Device Manager Server and all other management servers may be single-homed, and the actual devices under management are separated from Device Manager by a firewall. The firewall's rules restrict access to the arrays to Device Manager Server and any other required management application. Management clients accessing Device Manager are not allowed to pass traffic through the firewall to directly talk to the managed arrays, but can participate in management operations directly with Device Manager or the management application.

This configuration is the second most secure, and is more flexible than the most secure option. While this configuration protects the devices under management, it does not protect the management application servers themselves. Therefore, all management application servers should be hardened to the maximum possible extent

Caution: When Physical View of Universal Storage Platform V or TagmaStore USP, or Storage Navigator of Lightning 9900V is launched, Java Web Start and the web browser on the Web Client machine directly communicate with the storage subsystem. For this reason, if the Web Client machine and the storage subsystem exist on different networks, you must set up the networks so that the machine and the storage subsystem can directly communicate with each other.

Figure 2.3 illustrates a separate management LAN plus firewalled devices under management.

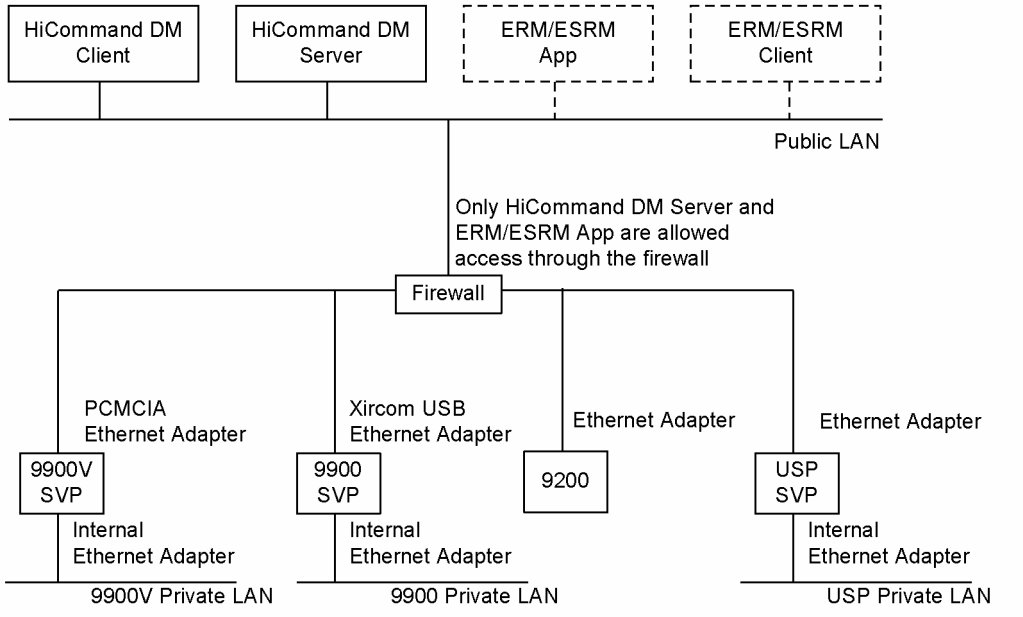

Figure 2.3 Second-Most Secure Configuration: Separate Management LAN plus Firewalled Devices

2.3.3 Third-Most Secure Configuration: Dual-Homed Management Servers plus Separate Management LAN

In this configuration, the management servers themselves act as the intersection point between the management LAN and a production LAN. The server running Device Manager or management applications is dual-homed. One NIC is attached to the management LAN along with the devices under management, and the second NIC is attached to a production LAN along with the management clients (e.g., the Device Manager GUI). Because the management application servers actually act as the gateway between the production LAN and the management LAN, and there is no additional firewall, you must be very sure that the server itself will not route traffic between the two networks.

This configuration is the third most secure, and is more flexible than either the most or second-most secure configurations. While it protects the devices under management, it does not protect the management application servers themselves. Therefore, all management application servers should be hardened to the maximum possible extent. Additionally, because the management application servers themselves act as gateways between the two LANs, OS hardening is very important.

Caution: When Physical View of Universal Storage Platform V or TagmaStore USP, or Storage Navigator of Lightning 9900V is launched, Java Web Start and the web browser on the Web Client machine directly communicate with the storage subsystem. For this reason, if the Web Client machine and the storage subsystem exist on different networks, you must set up the networks so that the machine and the storage subsystem can directly communicate with each other.

Figure 2.4 illustrates dual-homed management servers plus a separate management LAN.

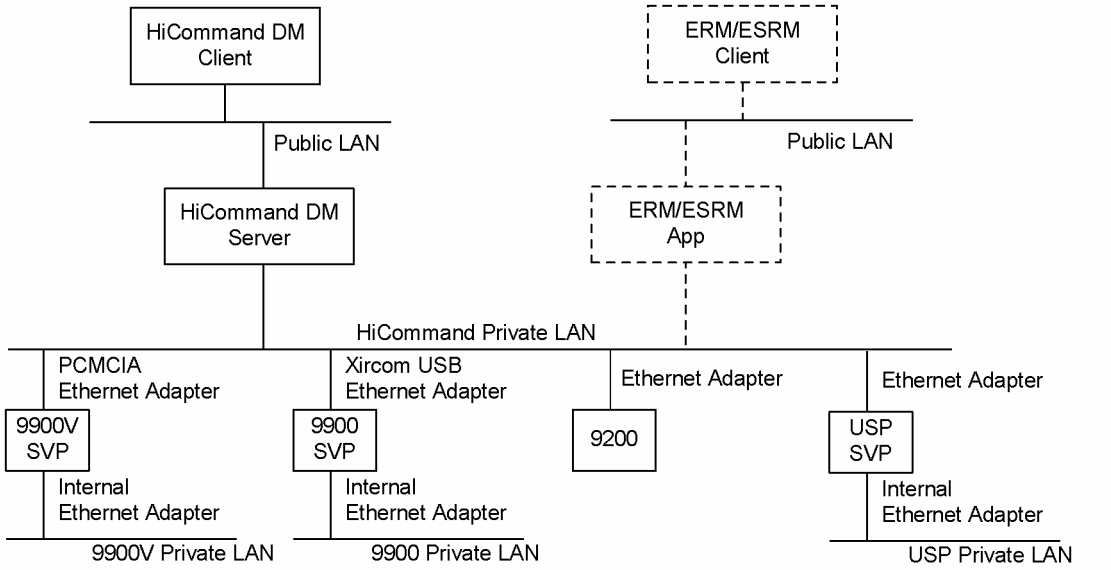

Figure 2.4 Third-Most Secure Configuration: Dual-Homed Management Servers Plus Separate Management LAN

2.3.4 Least Secure Configuration: Flat Network

Here, the management application servers, managed devices, and managed clients all coexist on the same network.

This configuration is the least secure, though it is the most flexible. It affords no protection to any of the components required for storage management operations, so management application server hardening is paramount. Additionally, you should consider microcode updates to any of the devices under management, especially if they are related in any way to security for the device management controllers themselves.

Note: This configuration may be a requirement if the implementation cannot accommodate a management LAN. For example, if you intend to use HDvM Client to launch the physical view of a USP/NSC TagmaStore, you must use a flat network configuration. In other configurations, differences between public and private LANs prevent HDvM from launching Storage Navigator on a client machine.

Figure 2.5 illustrates a flat network.

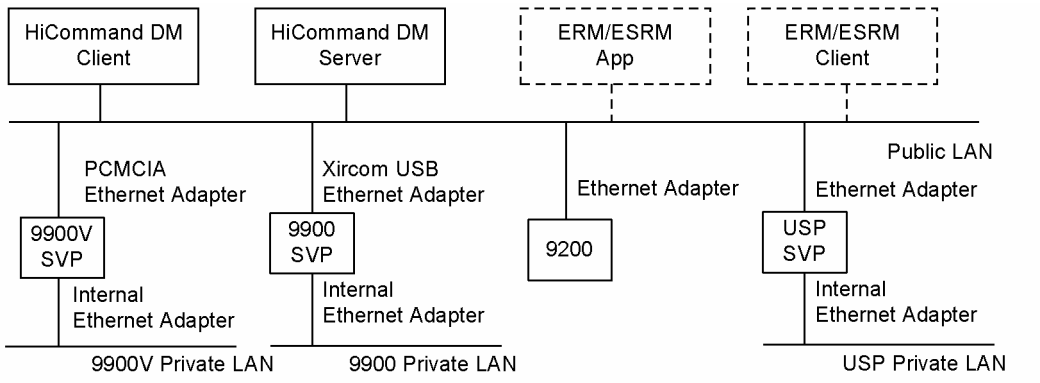

Figure 2.5 Least-Secure Configuration: Flat Network

2.4 Working with a Network that Uses a Firewall

If the host, storage subsystem, management client, and CIM client that are to be managed by the management server are inside a firewall, set the firewall so that these objects can communicate through each port with the management server. Table 2.1 to Table 2.6 list the port numbers relevant to this firewall setting.

A pound sign # next to a port number in these tables indicates that the port number can be changed.

Table 2.1 Ports Used for Communication Between the Management Server and a Management Client

Port Number	Originator	Destination	Remarks
23015/tcp#	Management client (Web Client)	Management server	This setting is required when non-SSL communication is used.
23016/tcp#	Management client (Web Client)	Management server	This setting is required when SSL communication is used.
2001/tcp#	Management client (Web Client or CLI)	Management server	This setting is required when non-SSL communication is used.
2443/tcp#	Management client (Web Client or CLI)	Management server	This setting is required when SSL communication is used.
1099/tcp	Management client (Web Client)	Management server	This setting is required for linking with Storage Navigator Modular (for Web) or with DAMP (for Web).

Table 2.2 Ports Used for Communication Between the Management Server and a Managed Host

Port Number	Originator	Destination	Remarks
24041/tcp#	Management server	Managed host	When the managed host is a mainframe host, this setting is not required.
24042/tcp#	Management server	Managed host	n/a
2001/tcp#	Managed host	Management server	When the managed host is a mainframe host, this setting is not required.

Table 2.3 Ports Used for Communication Between Management Server and Storage Subsystems

Port Number	Originator	Destination	Remarks
21/tcp	Management server	▪ Lightning 9900 ▪ Lightning 9900V ▪ TagmaStore USP ▪ Universal Storage Platform V	n/a
20/tcp	▪ Lightning 9900 ▪ Lightning 9900V ▪ TagmaStore USP ▪ Universal Storage Platform V	Management server	Set the firewall so that communication can be established from 20/tcp port of the storage subsystem to any port of the management server.
161/udp	Management server	Lightning 9900	n/a
162/udp	▪ Lightning 9900 ▪ Lightning 9900V ▪ TagmaStore USP ▪ Universal Storage Platform V	Management server	n/a
1099/tcp	Management server	▪ Lightning 9900V ▪ TagmaStore USP ▪ Universal Storage Platform V ▪ Thunder 9200 ▪ Thunder 9500V ▪ TagmaStore AMS/WMS series	n/a
51099/tcp	Management server	▪ Lightning 9900V ▪ TagmaStore USP ▪ Universal Storage Platform V	n/a
2000/tcp#	Management server	▪ Thunder 9200 ▪ Thunder 9500V ▪ TagmaStore AMS/WMS series	This setting is required for linking with Storage Navigator Modular (for Web) or with DAMP (for Web).

Table 2.4 Ports Used for Management Server to CIM Client Communication

Port Number	Originator	Destination	Remarks
427/tcp	CIM client	Management server	n/a
5988/tcp#	CIM client	Management server	This setting is required when non-SSL communication is used.
5989/tcp#	CIM client	Management server	This setting is required when SSL communication is used.

If there is a firewall between the management client (Web Client) and a storage subsystem, set the firewall so that the following port can be used to perform communication between them.

Table 2.5 Port Used for Communication Between the Management and Mail Servers

Port Number	Originator	Destination	Remarks
25/tcp	Management server (Storage Navigator Modular (for Web) or DAMP (for Web))	Mail server configured to send error information for the storage subsystems by using Storage Navigator Modular (for Web) or DAMP (for Web).	This setting is required when the email error report function is used while Device Manager is linked with Storage Navigator Modular (for Web) or DAMP (for Web).
25/tcp#	Management server (Device Manager server)	Mail server used for the email notification function of the Device Manager server.	This setting is required when the email notification function of the Device Manager server is used.

Table 2.6 Port Used for Management Client to Storage Subsystem Communication

Port Number	Originator	Destination	Remarks
2000/tcp#	Management client (Web Client)	▪ Thunder 9200 ▪ Thunder 9500V ▪ TagmaStore AMS/WMS series	This setting is required for linking with Storage Navigator Modular (for Web) or with DAMP (for Web).
1099/tcp	Management client (Web Client)	▪ Lightning 9900V ▪ TagmaStore USP ▪ Universal Storage Platform V	n/a
80/tcp	Management client (Web Client)	▪ Lightning 9900V ▪ TagmaStore USP ▪ Universal Storage Platform V	n/a
51099/tcp	Management client (Web Client)	▪ Lightning 9900V ▪ TagmaStore USP ▪ Universal Storage Platform V	n/a

2.5 Registering Firewall Exceptions in a Linux Environment

There is no single standardized firewall function provided by the OS in Linux environments, so firewall exceptions are not registered automatically when Device Manager server is installed. In Linux environments, the user must register firewall exceptions manually.

For details on ports to be registered, see section 2.4.

2.5.1 Using the Text Mode Setup Utility

The following uses an example to explain the procedure for using the text mode setup utility to register a firewall exception.

To register a firewall exception:

1. In a terminal window, execute the `setup` command.

   The Choose a Tool window of the text mode setup utility is displayed.

2. Select **Firewall configuration**, use the tab key to move to the **Run Tool** button, and then press **Enter**.

   The Firewall Configuration window is displayed.

3. Set **Security Level** to **Enabled** by pressing the space key to select **Enabled**, use the tab key to move to the **Customize** button, and then press **Enter**.

   The Firewall Configuration - Customize window is displayed.

4. In **Other ports** specify the port to be registered as an exception, use the tab key to move to the **OK** button, and then press **Enter**.

   Example: `Other ports 162:UDP,2001:TCP,23015:TCP`

   Important: If a port is already specified, use a comma to separate it from the new added entry.

5. After returning to the Firewall Configuration window, check that **Security Level** is **Enabled**, use the tab key to move to the **OK** button, and then press **Enter**.

2.6 Setting Up the Environment of a Server Machine That Has Multiple NICs

If the server machine on which Device Manager has been installed has multiple NICs and uses the bridge function, when you specify an IP address in the Device Manager settings, specify the IP address of the NIC that belongs to the network to which Web Client is connected. Do not specify the host name.

This section describes the network settings required for the configuration shown in Figure 2.6

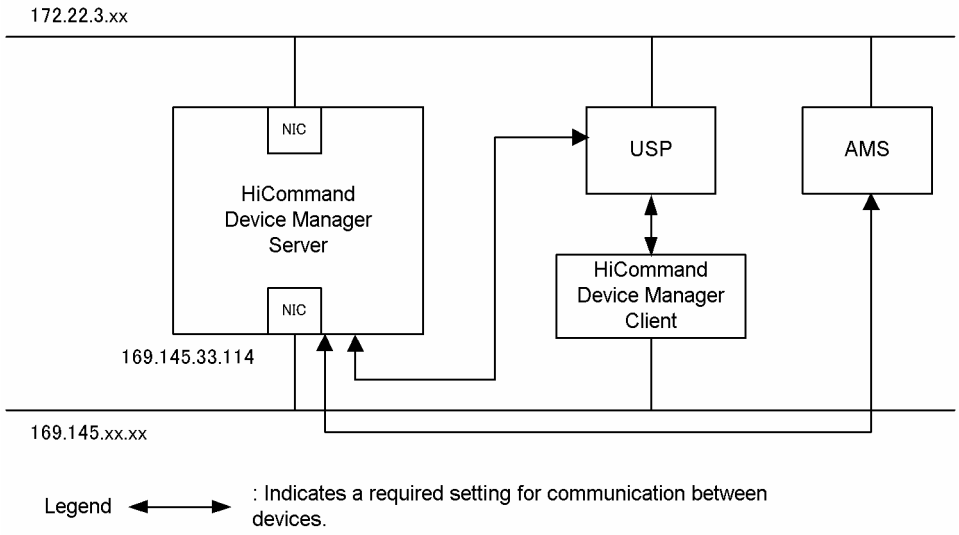

Figure 2.6 Configuration Example Using a Server Machine That Has Two NICs

2.6.1 Setting Up a Network

If you set up the configuration shown in Figure 2.6, set up routers, the client machine, and the server machine so that the following devices can communicate with each other as shown by the arrows in the figure:

- TagmaStore USP and the machine used for Web Client
- TagmaStore USP and a server machine (IP address: `169.145.33.114`) on which Device Manager has been installed
- TagmaStore AMS and a server machine (IP address: `169.145.33.114`) on which Device Manager has been installed

It is not necessary to set up communication between Web Client and TagmaStore AMS/WMS series because Storage Navigator Modular manages this communication.

2.6.2 Setting Up the Device Manager Server

When you specify an IP address for a Device Manager property, specify the IP address of the NIC that belongs to the network to which the client connects. The settings for the configuration in Figure 2.6 are as follows:

Setting for the Device Manager server property:

For the `server.http.host` property, specify the IP address of the host on which the web server function of Device Manager is used.

```
server.http.host=169.145.33.114
```

Setting for the property of launchable applications:

For the launchapp.damp.url property, specify the URL of the web server for Storage Navigator Modular (for Web) to be launched from the web browser of a client.

```
launchapp.damp.url=http://169.145.33.114:23015/program/DeviceManager/snm
```

For details about the Device Manager properties, see Chapter 8.

2.6.3 Setting Up Storage Navigator Modular

In the configuration example in Figure 2.6, if you use the simple setup tool (`launchapptool`) to set the IP address to be specified for the web server's URL, specify `169.145.33.114` for the IP address.

For details on Storage Navigator Modular (for Web), see the *Storage Navigator Modular (for Web) User's Guide*.

Chapter 3 Windows Systems Installation

This chapter explains how to install the HiCommand Device Manager Server on a Windows system, using the following topics:

- Installation Overview (see section 3.1)
- Installing to a Standard Windows Environment (see section 3.2)
- Installing to a Microsoft Cluster Server Environment (see section 3.3)
- Verifying and Troubleshooting Installation of HiCommand Device Manager Server and Common Component (see section 3.4)
- Starting and Stopping the Device Manager Server (see section 3.5)
- Operating the HiCommand Device Manager Server Database (see section 3.6)
- Converting a Device Manager Server Database (see section 3.7)
- Uninstalling the HiCommand Device Manager Server and Related Products (see section 3.8)

3.1 Installation Overview

Instructions in this section are for installing the Device Manager Server software on a single central server system. For instructions on installing and using the graphical Web Client software, see *HiCommand Device Manager Web Client User's Guide*.

WARNING: Device Manager does not support Web Client operations that use Windows terminal service. Device Manager does not support changing the configuration of the HiCommand Device Manager Server and HiCommand Device Manager Agent.

Note: Always read the release notes before installing Device Manager, and make sure that you have the minimum required microcode version on the subsystem.

3.1.1 Windows System and Media Requirements

WARNING: Do not install Device Manager and Hitachi Storage Services Manager on the same server.

Caution: HiCommand Device Manager does not support operations that use the terminal service function.

Important: The Device Manager server and agent must have the same software version to be able to communicate with each other.

Important: Do not install the Device Manager server in a system in which the client environment definitions of HiRDB-related products (e.g., HiRDB/Single Server, HiRDB/Parallel Server, HiRDB/Run Time, HiRDB/Developer's Kit, or HiRDB/Workgroup Server) are set in environment variables.

The following are the minimum suggested requirements for Windows systems:

- Operating System: The HiCommand Device Manager server runs on the following OSs:

Table 3.1 List of Windows Versions on Which HiCommand Device Manager Server Runs

Abbreviated name and architecture	Edition name	Service pack	Cluster environment support
Windows 2000	Professional Operating System Server Operating System Advanced Server Operating System Datacenter Server Operating System	SP3	--
		SP4	Y
Windows Server 2003 x86	Standard Edition Enterprise Edition Datacenter Edition	No SP	Y
		SP1	Y
		SP2	Y
Windows Server 2003 x64 Edition#	Standard x64 Edition Enterprise x64 Edition Datacenter x64 Edition	No SP	Y
		SP2	Y
Windows Server 2003 R2 x86#	Standard Edition Enterprise Edition Datacenter Edition	No SP	Y
		SP2	Y
Windows Server 2003 R2 x64 Edition#	Standard x64 Edition Enterprise x64 Edition Datacenter x64 Edition	No SP	Y
		SP2	Y
Windows XP#	Professional	SP2	--

Legend

Y: Operation in a cluster environment is supported.

--: Operation in a cluster environment is not supported.

For details about the supported cluster software and how to set up cluster environment, see section 3.3.

Note: Also supported on VMware ESX Server 3.0.1.

Installation using Remote Desktop is only supported for connection with a console session.

When using the Device Manager server in a time zone of the United States or Canada, set the OS of the machine on which the Device Manager server will be installed so that the OS is compatible with the new Daylight Saving Time (DST) rules. If the OS is not compatible with the new DST rules, the Device Manager server will also not be compatible with the new rules.

- Machine specifications: The following table describes the recommended specifications for the machine where the HiCommand Device Manager server is to be installed.

Table 3.2 Recommended Specifications for the Machine Where the HiCommand Device Manager Server Is to Be Installed

Item	Minimum	Recommended
Processor	1.0 GHz	2.0 GHz or faster
Memory	512 MB	At least 1 GB#
Disk space	4 GB	At least 5 GB

When the HiCommand Device Manager server is used concurrently with other software products, the memory requirements of all of the software products must be taken into account.

- Installation destination and its disk space requirements: The following table describes the installation paths and the required disk space for installation.

Table 3.3 Installation Path and Required Disk Space

Item	Default Installation Path	Required Disk Space (GB)
Installation destination for the HiCommand Device Manager server	`C:\Program Files\HiCommand\DeviceManager`#1	1.30
Installation destination for HiCommand Suite Common Component	`C:\Program Files\HiCommand\Base`#2	
Storage destination of the database for the HiCommand Device Manager server	`C:\Program Files\HiCommand\DeviceManager\HiCommandServer\database`#1	0.10
Storage destination of the database for HiCommand Suite Common Component#3	`C:\Program Files\HiCommand\Base\database`#1	1.20
A temporary folder#4	A folder specified by the environment variable `TMP`	0.30#5

#1 You can change this path.

#2 You can change this path. If you install the HiCommand Device Manager server later, install it in the same drive as this path indicates.

#3 This is not required if HiCommand Suite Common Component version 4.0 or later has already been installed.

#4 This is temporarily required during installation. However, this will be unnecessary after finishing installation.

#5 When the free disk space of the folder specified by the environment variable `TMP` is less than 200 MB, you will be asked to specify another folder during installation. In this case, the drive you specified must have 200 MB of free disk space and the drive of the folder specified by the environment variable `TMP` must have 100 MB of free disk space.

- Prerequisite program: J2SE Java Runtime Environment 1.4

  This program is automatically installed when you install the HiCommand Device Manager server.

- Monitor: XGA (1024 x 768 resolution) or higher
- CD-ROM drive
- 10/100 Ethernet LAN card (if the machine and the LAN cable are compatible with Gigabit Ethernet, you can use a Gigabit-class card).
- Static IP address
- Storage subsystem(s) and the Device Manager Server residing on the same network
- Administrator/root ID to install Device Manager
- TCP/IP installed and running
- LAN cables and connections to the subsystem
- The HiCommand Device Manager server only supports IPv4 (it does not support IPv6). Connect the HiCommand Device Manager server, Web Client, the HiCommand Device Manager agent, and a storage subsystem by using IPv4. For details about how to disable IPv6, refer to the appropriate documentation for each OS.
- When using one HiCommand Device Manager server, it is not possible to use separate storage partitions with different storage administrator accounts. If you want to manage individual storage partitions, a HiCommand Device Manager server is required for each storage partition.
- The estimated installation time is 20 to 30 minutes, for a new installation on a machine configured as follows:
  - OS: Windows 2000 SP4
  - Processor: Pentium 4 (2.4 GHz)
  - Memory: 1 GB

  For Windows XP SP2 or later, or Windows Server 2003 SP1 or later, the installation time requires approximately 15 more minutes, because the HiCommand(R) Device Manager server is added to the Windows firewall exceptions list during installation.

Caution: Depending on the language of the installed OS (such as German or Spanish) on the installation destination Windows(R) machine, the installation files and directories of the Device Manager server might be viewed, deleted, and operated by users who do not have Administrator permissions. (This problem does not occur in an English environment.) Regardless of the language of the installed OS, after installing Device Manager, do not manually delete or perform operations on files or directories.

3.1.2 Setting Memory Heap Size According To the Number of Managed Resources

The following table shows the number of resources that can be managed by the HiCommand Device Manager server. We recommend that you operate the HiCommand Device Manager server within these limits.

The default values in the table are used if you do not change the memory heap sizes of HBase Storage Mgmt Web Service and the Device Manager server. The number of LDEVs in the table is the total of the number of LDEVs for mainframes and the number of LDEVs for open systems.

Table 3.4 Maximum Value of the Number of Resources that Can Be Managed by the HiCommand Device Manager Server

Resource	Maximum setting	Default
Number of LUNs	128,000	32,000
Number of Securities	192,000	48,000
Number of LDEVs	128,000 (The maximum number of LDEVs for open systems only is 64,000.)	16,000

In an environment in which HiCommand Device Manager is used, if the assumed number of resources exceeds the default settings in the above table, you need to estimate the number of managed resources, and then set the memory heap sizes of HBase Storage Mgmt Web Service and the Device Manager server according to the estimated value.

The formula that can be used for estimating the number of managed resources is shown below. When multiple storage subsystems are to be managed, estimate the number of managed resources for each storage subsystem, and use the greatest value as a guideline.

Formula:

number-of-managed-resources = *number-of-LDEVs* x 2.5 + *total-number-of-paths*[#]

 # total-number-of-paths = *number-of-LDEVs* x *average-number-of-paths-per-LDEV*

If the *number-of-managed-resources* is 28,000 or greater or if an *Out Of Memory* error occurs while you are using Web Client to perform an operation such as displaying a list of LDEVs, set the memory heap size by following the procedures described in sections 3.1.2.1 and 3.1.2.2.

After the memory heap size is set, if *number-of-managed-resources* increases from 50,000 or less to 50,001 or greater, only set the memory heap size of the Device Manager server if the memory heap size of HBase Storage Mgmt Web Service has already been set.

The set value is valid until the Device Manager server is uninstalled.

3.1.2.1 Setting Memory Heap Size of HBase Storage Mgmt Web Service

When you set the memory heap size of HBase Storage Mgmt Web Service, note the following points:

- You can only increase the heap size that has been set. If you want to decrease it, uninstall the Device Manager server, re-install the Device Manager server, and then change the heap size to the size you want.
- In an environment in which multiple HiCommand Suite products are installed, the largest heap size of the sizes for the products takes effect.

To set the memory heap size of HBase Storage Mgmt Web Service:

1. If HiCommand Suite products whose versions are earlier than 5.7 have been installed, stop their services.

For details about how to stop these services, see the manual for your product version.

2. Stop the HiCommand Suite product services and HiCommand Suite Common Component as follows:

   Select **Start**, **Programs**, **HiCommand**, **Device Manager**, and then **Stop Server with Common Services**.

3. Execute the following command:

   "*installation-folder-for-HiCommand-Suite-Common-Component*\bin\hcmdsweb" /add /file "*installation-folder-for-the-Device-Manager-server*\HiCommandServer\webapps\DeviceManager.war" /server HiCommand /javaoption HDvM.serverpath="*installation-folder-for-the-Device-Manager-server*" /type DeviceManager /Xms256 /Xmx512

   The following shows an example of executing the command:

   ```
   "C:\Program Files\HiCommand\Base\bin\hcmdsweb" /add /file
   "C:\Program
   Files\HiCommand\DeviceManager\HiCommandServer\webapps\DeviceManage
   r.war" /server HiCommand /javaoption HDvM.serverpath="C:\Program
   Files\HiCommand\DeviceManager" /type DeviceManager /Xms256 /Xmx512
   ```

   Note: When setting the memory heap size of the Device Manager server at the same time:

   Before restarting the services in the next step, perform steps 1 and 2 (setting of the `HiCommandServer.lax` file) that are described in section 3.1.2.2. If you do this, you can omit the operations of stopping and starting the services when setting the memory heap size of the Device Manager server.

4. Restart the HiCommand Suite product services and HiCommand Suite Common Component as follows:

   Select **Start**, **Programs**, **HiCommand**, **Device Manager**, and then **Start Server with Common Services**.

5. If HiCommand Suite products whose versions are earlier than 5.7 have been installed, restart their services as required.

   For details about how to start these services, see the manual for your product version.

3.1.2.2 Setting Memory Heap Size of the Device Manager Server

To set the memory heap size of the Device Manager server:

1. Use a text editor to open the `HiCommandServer.lax` file in *installation-folder-for-the-Device-Manager-server*\`HiCommandServer`.

2. Specify the following value for `lax.nl.java.option.java.heap.size.max`.

   - When the number of managed resources is 50,000 or less: `536870912` (512 MB)
   - When the number of managed resources is more than 50,000: `1073741824` (1 GB)

   If you use the CLI to obtain information about the storage subsystem, more memory might be required. Therefore, compare the value calculated by using the following formula and the above value, and then specify the larger value (units: bytes):

Formula:

memory-heap-size = (*number-of-LDEVs* x 0.03 + *total-number-of-paths* x 0.03 + 140) x 1024 x 1024

3. Restart the Device Manager server as follows:

   Select **Start**, **Programs**, **HiCommand**, **Device Manager**, and then **Stop Server**.

   After the Device Manager server has stopped, select **Start**, **Programs**, **HiCommand**, **Device Manager**, and then **Start Server**.

3.1.2.3 Setting Memory Heap Size When Using CIM/WBEM

If CIM/WBEM functions are being used, you might have to increase the memory heap size of the Device Manager server, depending on the conditions. Note that the required memory heap size differs depending on the CIM client you are using.

To change the memory heap size:

1. Use a text editor to open the `HiCommandServer.lax` file in *installation-folder-for-the-Device-Manager-server*`\HiCommandServer`.
2. Change the value of `lax.nl.java.option.java.heap.size.max` to *new-setting-value* (units: bytes) calculated by using the following two formulas:
   - *calculation-value-for-SMI-S-Provider* = 30,000 x *number-of-LDEVs* x *number-of-paths-per-LDEV*

     If the value of *number-of-paths-per-LDEV* becomes less than 1, assume that this value is equal to 1 for the calculation.

     The value of *calculation-value-for-SMI-S-Provider* is expressed in bytes. If this value becomes less than 268,435,456 (256 MB), assume that this value is equal to 268,435,456 for the calculation.
   - *new-setting-value* = *current-setting-value* + *calculation-value-for-SMI-S-Provider*

     All of the values in the above formula are expressed in bytes.

   The value of *new-setting-value* obtained from the above formula is the memory heap size required for obtaining the class information that belongs to the bottom layer in a CIM class. When an upper-layer class is specified, some SMI-S clients might obtain information of all the classes below that class at the same time. In this case, required capacity will be larger than the value of *new-setting-value* obtained from this formula.
3. Restart the Device Manager server as follows:

   Select **Start**, **Programs**, **HiCommand**, **Device Manager**, and then **Stop Server**.

   After the Device Manager server has stopped, select **Start**, **Programs**, **HiCommand**, **Device Manager**, and then **Start Server**.

3.2 Installing to a Standard Windows Environment

The Device Manager Server is installed to:

c:\program files\HiCommand\Device Manager

The Common Component is installed to:

c:\program files\HiCommand\Base

3.2.1 Preparing for Installation

Caution: If Windows Firewall is enabled in Windows Server 2003 SP1 or Windows XP SP2, during installation, a warning dialog box might be output asking you whether you want to keep blocking the program. If it appears, choose **Unblock** or **Ask Me Later**. Also, after installation finishes, you need to set up Windows Firewall.

Before you start installation, check the usage status of the port numbers, the installation status of other programs, and other information as described below.

3.2.1.1 Check Port Numbers

Check whether the port numbers required to use HiCommand Device Manager are being used by another product on the machine on which the HiCommand Device Manager server is to be installed by using the `netstat` command.

Example: Check whether another program is using the port `162/udp`.

Execute the following command:

```
> netstat -anp UDP
```

In the command execution results, if there are no lines in which `UDP` for `Proto`, and `162` for `Local Address` appear, the port is not being used.

The following shows the ports required to use HiCommand Device Manager. For details about the intended use of each port, see section 2.4 and section 5.4.1.

Port numbers that must be checked

- From 23015 to 23018, and 23032: If another product is using any of these ports, change the settings of that product, or change the settings of HiCommand Device Manager. For details about how to change these port numbers, see section 5.4.2. If HiCommand Suite Common Component has been installed and these ports have been changed, you can install the HiCommand Device Manager server by using those ports. You do not need to set up the default ports.
- From 45001 to 49000: For these port numbers, the settings of HiCommand Device Manager cannot be changed. Therefore, you need to change the settings of any other products that are using the same ports as HiCommand Device Manager.

- 2001: If another product is using this port number, change the settings of that product, or change the port number to be used before HiCommand Device Manager starts. For details about how to change this port number, see section 8.2.2. We recommend that you change this port number to another number because this port number is included among the port numbers temporarily assigned by Windows (1024 to 5000). If another product is using this port number, the following message will be output to the event log file, and HiCommand Device Manager will not be able to start: `KAIC00114-E An attempt to start the HTTP server on port "2001" failed.`

Port numbers that must be checked when some functions are enabled

- 162: This port number is used when the SNMP Trap reception function of HiCommand(R) Device Manager is enabled. To disable the SNMP Trap reception function, select disable in the Setting for the SNMP Trap Reception Function panel during installation.
- 1099: This port number is used when the function to link with Storage Navigator Modular (for Web) (see section 9.1), or DAMP (for Web) (see section 9.1.4) is enabled. We recommend that you change this port number to another number because this port number is included among the port numbers temporarily assigned by Windows (1024 to 5000). For details about how to change the port number used to link with Storage Navigator Modular (for Web), see section 9.1.2. The port number for the function to link with DAMP (for Web) cannot be changed. When the port number 1099 is used by another product, perform one of the following operations so that other products do not use the port number 1099 at the same time as HiCommand Device Manager.

  If a product that uses the port number 1099 is always running, use different machines to run HiCommand Device Manager and that product respectively.

  If a product that uses the port number 1099 runs temporarily, restart DAMP (for Web).
- 2000: This port number is used when the function to link with Storage Navigator Modular (for Web) (see section 9.1) or DAMP (for Web) (see section 9.1.4) is enabled. For details about how to change this port number, see section 1.5.1.2 or 1.5.1.6. We recommend that you change this port number to another number because this port number is included among the port numbers temporarily assigned by Windows (1024 to 5000).
- 2443: This port number is used when SSL communication is enabled. For details about how to change this port number, see section 8.2.3. We recommend that you change this port number to another number because this port number is included among the port numbers temporarily assigned by Windows (1024 to 5000). If another product is using this port number, the following message will be output to the event log file, and HiCommand Device Manager will not be able to start: `KAIC00115-E An attempt to start the HTTPS server on port "2443" failed.`

3.2.1.2 Checking the Time of a Machine and the Functions that Adjust the Time

If the time of a machine is changed while the services of HiCommand Suite Common Component and HiCommand Suite products are running, Device Manager 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 Device Manager

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 Suite products.
2. Change the time of the machine.
3. Restart the machine.

3.2.1.3 Check Other Programs Related To Security

- Check whether the following programs are installed. If they are installed, take action by following the explanation below:
  - A program that monitors security

    Stop the program that monitors security, or change its settings so that Device Manager can be installed normally.
  - A program that detects viruses

    We recommend that you stop programs that detect viruses, and then install Device Manager.

    If a program that detects viruses is running during installation of Device Manager, the speed of installation might be reduced, installation might fail, or installation might finish in an incorrect state.
  - A program that monitors processes

Stop the program that monitors processes, or change its settings so that the program does not monitor the services or processes of the HiCommand Device Manager server and the HiCommand Suite Common Component.

If a program that monitors processes starts or stops the above services or processes during installation of Device Manager, installation might fail.

- For Windows Server 2003 SP1 or later, or Windows XP SP2 or later, disable Data Execution Prevention before starting the installer.

  To disable Data Execution Prevention:

  1. Log in to the system using a user ID with Administrator permissions.
  2. Insert the HiCommand Device Manager installation CD-ROM.
  3. From Control Panel, choose **System**.

     The **System Properties** dialog box appears.
  4. Choose the **Advanced** tab, and then click the **Settings** button under **Performance**.

     The Performance Options dialog box appears.
  5. Choose the **Data Execution Prevention** tab, and then select the radio button for **Turn on DEP for all programs and services except those I select**.
  6. Click the **Add** button.

     The dialog box for choosing a file appears.
  7. Choose `install.exe` in the root folder of the CD-ROM drive, and then click the **Open** button.
  8. Click the **OK** button.

3.2.1.4 Check Other Programs

- HiRDB Embedded Edition_HD0 must be always running when you are using any HiCommand Suite products version 4.0 or later. You can verify that HiRDB is running by checking the Services Panel.
- Open the property of the following services from the Services panel to make sure that **Startup Type** is not set to **Disabled**. If **Startup Type** is set to **Disabled**, change the setting to **Automatic** or **Manual**.
  - HBase Storage Mgmt Common Service
  - HBase Storage Mgmt Web Service
  - HiRDB/EmbeddedEdition _HD0
  - HiCommandServer
- Device Manager cannot be installed on a server on which Tuning Manager has been installed in a Large configuration. Trying to install Device Manager in such an environment will automatically cancel the installation. If that happens, install Tuning Manager and Device Manager separately on different servers.
- You cannot install a version of Tuning Manager earlier than 4.0 on a machine on which Device Manager 4.0 or later has been installed. The following installation sequences are allowed:
  - Device Manager 4.0 or later is installed after a version of Tuning Manager earlier than 4.0 has been installed.
  - Tuning Manager 4.0 or later is installed after a version of Device Manager earlier than 4.0 has been installed.
- When using another HiCommand Suite product, make sure that you back up the databases for that product before installing Device Manager. For details about how to back up other HiCommand Suite product databases, see the manual for each product.
- The HiCommand Device Manager server cannot coexist with the following HiRDB products. Therefore, do not install the Device Manager server on a machine on which any of the following HiRDB products are installed, or vice-versa.
  - HiRDB/Single Server
  - HiRDB/Parallel Server
  - HiRDB/Workgroup Server
  - HiRDB/Run Time
  - HiRDB/Developer's Kit
  - HiRDB SQL Executer

3.2.1.5 Check Other Information

- Make sure no other applications are running.
- The user's account must be a member of the Administrator group.
- Make sure that the following folders can be created, or that they have already been created and are write-enabled. The examples assume that the OS is on the C Drive, and that Device Manager is installed to the default installation folder.
  - `C:\Program Files\HiCommand`
  - `C:\Program Files\Hitachi\HNTRLib2`
  - `C:\Program Files\Common Files\Hitachi`
- You cannot perform a downgrade installation for Device Manager. For example, in an environment in which Device Manager 5.0 has been installed, you cannot install Device Manager 4.3 or an earlier version. However, a build to which patches have been applied can be overwritten by the same build without the patches, as long as the version numbers are the same. For example, after installing a build of Device Manager 5.0 to which patches have been applied, you can install a V5.0 build that does not contain the patches.
- When you specify virtual memory settings, allocate at least 1,536 MB as the paging file size. To set the paging file size, right-click **My Computer** and, in the displayed menu, choose **Properties**. Then, in the displayed dialog box, open the **Advanced** page and click **Performance Options**. The allocated paging file size must be at least 1,536 MB even after Device Manager server operation starts.
- When you install the Device Manager server, specify the host name or IP address of the server machine. When you specify the host name, make sure that the host name satisfies the following conditions:
  - Number of characters: 32 bytes or less
  - Available characters: `A-Z a-z 0-9 -`

    You cannot use a hyphen (-) at the beginning or end of the host name.

  When you install the Device Manager server in a cluster environment, specify a logical host name that satisfies the above conditions.
- If multiple NICs are installed on the machine, during installation you will need to specify the IP address that corresponds to one of those NICs. If multiple NICs are connected to different networks, use the IP address of the NIC that belongs to the network to which Web Client is connected.

  The IP address specified during installation is also used when you specify the following settings after installation is complete:
  - `server.http.host` property

    For details about how to set this property, see section *8.2.1*.
  - An environment for Storage Navigator Modular (for Web) or DAMP (for Web)

    You specify the host name or IP address when setting up an environment for linking with Storage Navigator Modular (for Web) or DAMP (for Web).

    For details about the procedure, see section *9.1* or *9.2*.

3.2.2 Reviewing the Contents of the Installation CD

The Device Manager Server installation CD includes the following applications:

- Java 2 Java Runtime Environment (JRE)
- HiCommand Suite Common Component software
- Device Manager Server software
- HiRDB/EmbeddedEdition_HD0 version 7.0

After these products are installed, the Device Manager Web Client software can be downloaded, installed, and updated on the client system from the Device Manager Server. For more information on using the Device Manager Web Client, please see the *HiCommand Device Manager Web Client User's Guide*.

3.2.3 Performing a New Installation of Device Manager Server

After finishing a new installation, be sure to back up the Device Manager Server database.

To perform a new installation of the Device Manager Server:

WARNING: Close the Services panel before you install the HiCommand Device Manager server.

1. Log on to the system as an administrator.

   If a user that is not from the administrators group attempts installation, a window is displayed indicating that the user must be from the administrators group to perform installation. The installation then stops.

2. Load the Device Manager installation CD-ROM.

   The installer usually starts automatically. If it does not start automatically, execute **install.exe** located in the root folder of the CD-ROM drive.

3. The panel for choosing the language is displayed. Select the appropriate language, and then select **OK** to continue.

   The following steps assume that English is selected.

4. The **Introduction** panel displays. Select **Next** to continue.

5. When the HiCommand Suite Common Component services are running in a non-cluster environment, the Stop HiCommand Suite Product Services panel is displayed. Select **Next** to continue.

   If the installer cannot stop all the services of HiCommand Suite Common Component and the HiCommand Suite products, the **Stop services error** panel is displayed. If this panel is displayed, select the **OK** button to close it, and then try again to stop the services. If the installer still fails to stop the services, cancel the installation, manually stop the services of HiCommand Suite Common Component and the HiCommand Suite products, and then perform the installation again.

6. If HiCommand Suite Common Component is already installed, the Backup recommendation panel is displayed. If a HiCommand Suite product other than Device Manager is installed, you should back up the databases for HiCommand Suite Common Component and other HiCommand Suite products before starting an installation. Otherwise, select **Next** to continue.
7. If Common Component is not installed, the **HiCommand Suite Common Component Not Installed** panel is displayed. Select **Next** to continue.
8. The License Agreement panel is displayed. Select **I accept the terms of the License Agreement**, and then **Next** to continue.
9. If port 162 is not used by any other products, the **SNMP Trap Note** panel displays. Select **Next** to continue.
10. If another product is using port 162, the **Setting for the SNMP Trap Reception Function** panel is displayed. If the SNMP Trap reception function is enabled when another product is using port 162, Device Manager will not start after installation. If you want to disable the SNMP Trap reception function to start Device Manager, choose **YES. Disable the function and continue installation**, and then **Next** to continue. If you want to change the settings of the product that is using port 162 and re-execute the installation, choose **NO. Stop the installation of Device Manager**, and then **Next** to cancel the installation.

    Caution: If you choose **YES. Disable the function and continue installation**, the properties for the SNMP Trap reception function are automatically changed to disable the function. You must reset these properties to the default values manually. For details about these properties, see section 8.5.8.
11. The **Choose Install Folder** panel (see Figure 3.1) displays. To accept the default folder, select **Next**. To change to another install folder, make that selection and then select **Next**.

    Caution: Specify an absolute path, using no more than 64 bytes. Do not enter the path delimiter (\) at the end of the folder path. Space characters and the following characters can be used for the path:

    A-Z a-z 0-9 . _ ( )

    The path cannot contain consecutive spaces. Folder names must not end with a period or space. Do not use parentheses, except when referring to the Program Files (x86) folder.
12. The **Install Folder Information** panel is displayed. Select **Next** to continue.

    Important: When the Common Component 4.0 or later is being installed, HiRDB is installed to manage the database. No dialogue box is displayed during the HiRD8 installation.
13. The **Choose the Database for HiCommand Suite Common Component** panel is displayed (see Figure 3.2). Specify the location where the database files used by HiCommand Suite Common Component are to be stored, in accordance with the following limitations:
    - Specify an absolute path, using no more than 90 bytes.
    - Do not enter a path delimiter (\) at the end of the folder path.
    - Do not use parentheses, except when referring to the Program Files (x86) folder.

- You can use alphanumeric characters, spaces, underscores and periods for the path name.
- Folder names must not end with a period or space.

14. Select **Next** to continue. The **Choose the Database for HiCommand Device Manager** panel is displayed (see Figure 3.3). Specify the file location for the Device Manager Server. The file name and path have the same restrictions as the Common Component file name and path. Select **Next** to continue.
15. The **Installation Server Information Settings** panel displays (see Figure 3.4). Enter the IP address or host name of the server machine, and the port number for the HBase Storage Mgmt Web Service used by Web Client, then select **Next**. The defaults are as follows:
    - IP address or host name: Default = None. Specify a valid host name or IP address on the network on which HiCommand Device Manager operates.
    - Port number: Default = 23015.

    Important: This is the port number for the HBase Storage Mgmt Web Service used by Web Client, not the Device Manager Server. If you use a port number other than the default, make sure that you also change the port number assigned to the Common Component. See section 5.4.2 for more information on changing Common Component ports.
16. If a Windows Firewall is installed on the system, the **Adding to the Windows Firewall Exceptions** panel is displayed. Check the contents of the panel, and select **Next** to continue.
17. The Setting for the SMI-S Provider Service panel is displayed (see Figure 3.5). If you want the SMI-S Provider service to start automatically when Device Manager starts, choose **YES. Automatically enable the function after installation**. If you do not want it to start automatically, choose **NO**. Then, choose **Next** to continue.

    If you choose **YES. Automatically enable the function after installation.**, the processing continues. If you choose **NO.**, the processing continues from step 20.

    Note: You can set up the SMI-S Provider service after installation. For details, see Chapter 11.
18. The Setting for the SMI-S SSL panel is displayed (see Figure 3.6). To enable SSL for the SMI-S Provider service, choose **YES**. To disable SSL, choose **NO**. To change the port number, enter the new port number in the **Change the port number if needed** text box. To enable two-way authentication for SSL-based object operations, select **Also use Two-way Authentication for Object operations.** To enable two-way authentication for SSL-based event indications, select **Also use Two-way Authentication for Event Indications**. Select **Next** to continue.

    Caution: Two-way authentication involves import and export of authentication files. For details, see section 7.4.

    Note: You can enable SSL, change the port number, and set up two-way authentication after installation. For details on the setup procedures, see the following section:

    To enable SSL and change the port number:

    Section 11.3.2.2

Section 11.4.1

To set up two-way authentication:

Section 7.4

19. The Setting for the SLP Service panel is displayed (see Figure 3.7). To install and enable the SLP service, choose **YES. Automatically enable the function after installation**. If you do not want to enable the SLP service, or if another SLP service is already installed and enabled, select **NO**. Select **Next** to continue.

    Note: You can enable the SLP service after installation. For details, see section 11.5.

20. In a non-cluster environment, the Set Services to Start After Installation panel is displayed. If you want to start the services of HiCommand Suite Common Component and related HiCommand Suite products after installation is complete, select **Yes**. If you do not want to start these services after installation is complete, select **No**. After you select **Yes** or **No**, select **Next** to go to the next step.

    Caution: The services of HiCommand Suite products whose versions are earlier than 5.7 are not started by selecting **Yes**. If you want to start the services of HiCommand Suite products after installation is complete, manually start the services. For details about how to start these services, see the manual for your product version.

21. The **Pre-installation Summary** panel displays. The product name, installation folder, information on installation disk capacity, the IP address or host name of the server machine, and the port number to be used are displayed. Verify that the information is correct, and then select **Install** to begin. The Progress panel will be displayed.
    - If you select **Cancel**, the **Cancellation Warning** panel displays, warning that if you cancel now installation will not complete.
    - If you let installation proceed without cancellation, the **Please Wait** panel displays, followed during post-installation setup by the Progress panel.

22. The **Secure Socket Certificates Note** panel displays.

23. If you plan to run secure socket communications, note the information in this panel for later use. For more information on configuring secure sockets, see Chapter 7. Select **Next** to continue.

24. The **Install Complete** panel displays.

25. Select **Finish** to complete the installation.

Important: After installing the HiCommand Device Manager server, you need to register a license key by using Web Client. For information about how to register a license key, see the *HiCommand Device Manager Web Client User's Guide*.

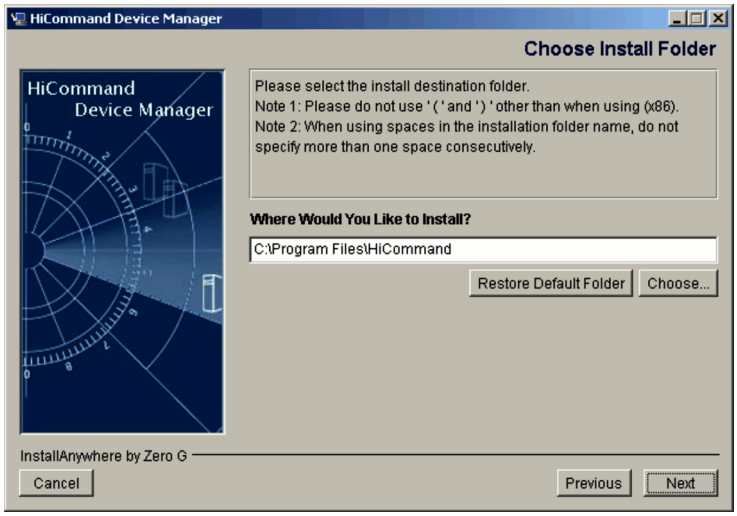

Figure 3.1 Choose Install Folder Panel

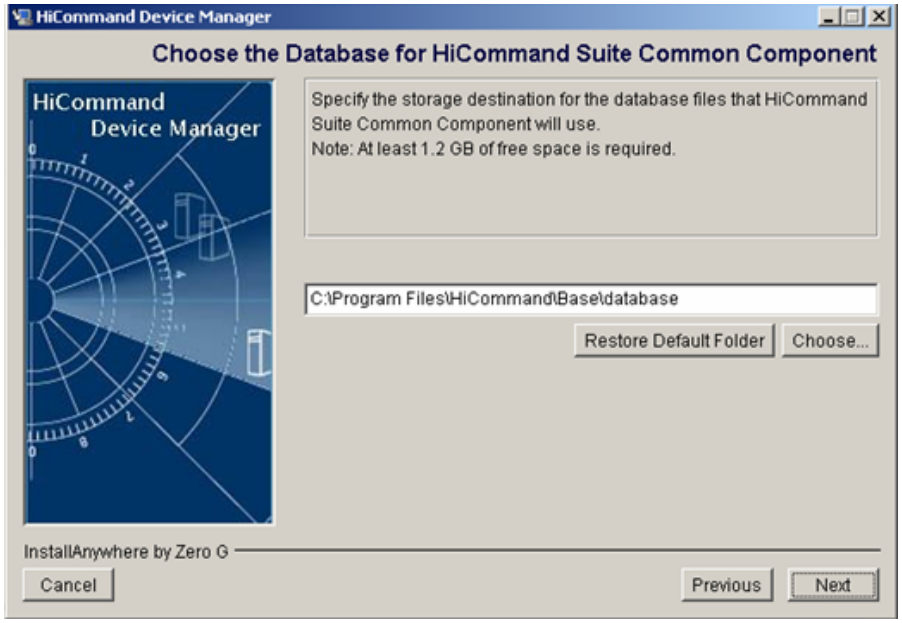

Figure 3.2 Choose the Database for HiCommand Suite Common Component Panel

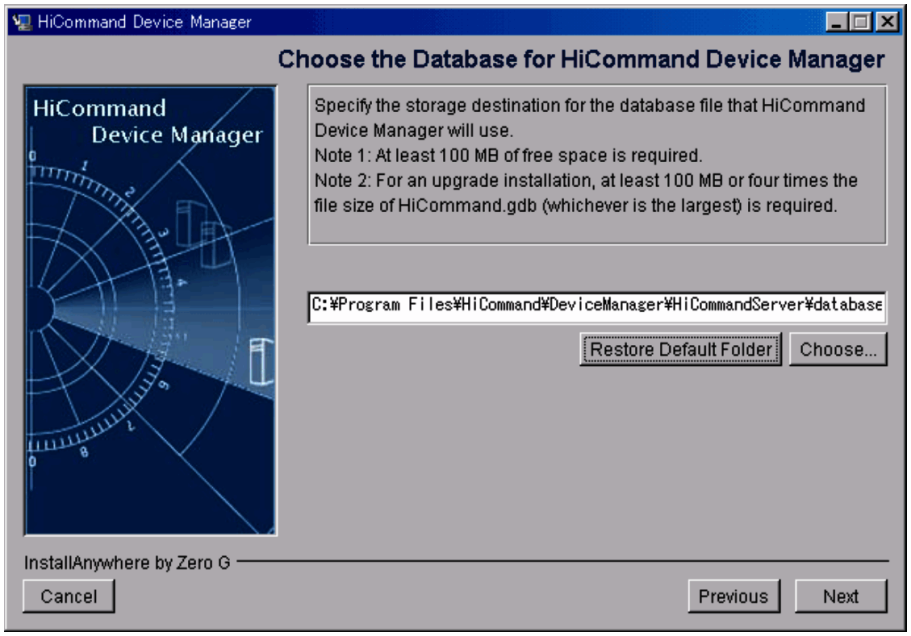

Figure 3.3 Choose the Database for HiCommand Device Manager Panel

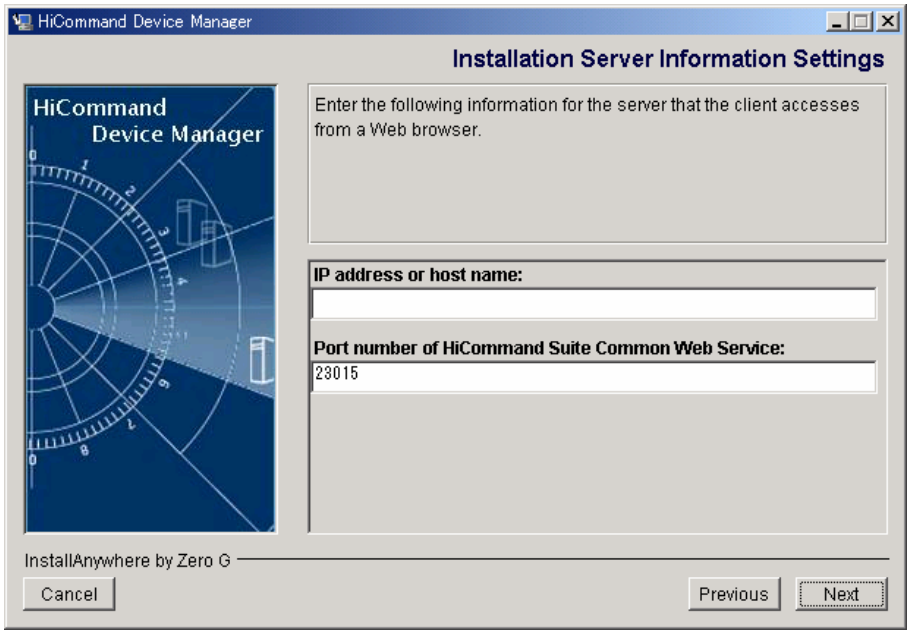

Figure 3.4 Installation Server Information Settings Panel

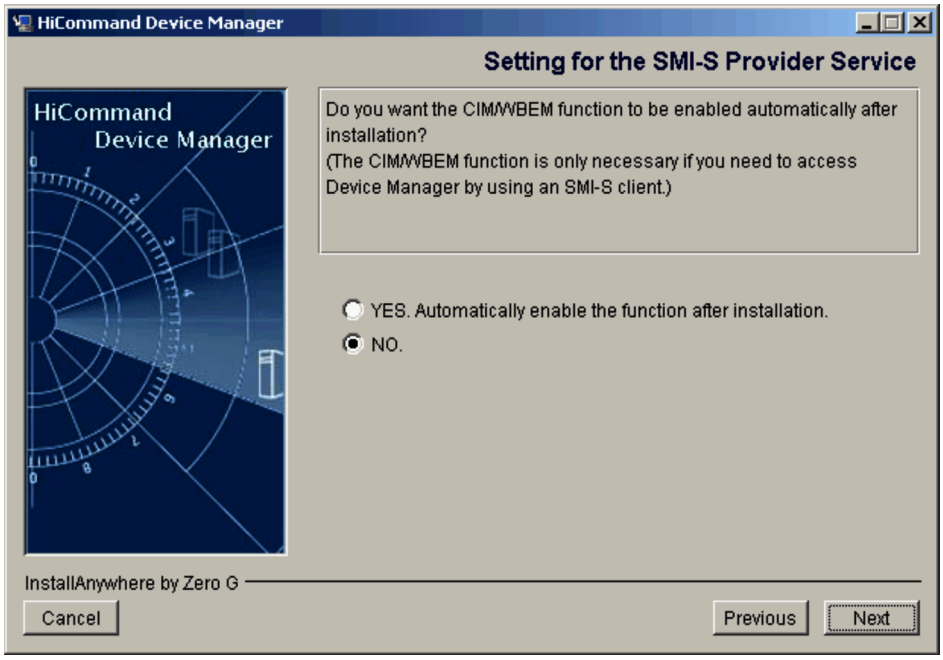

Figure 3.5 Setting for the SMI-S Provider Service Panel

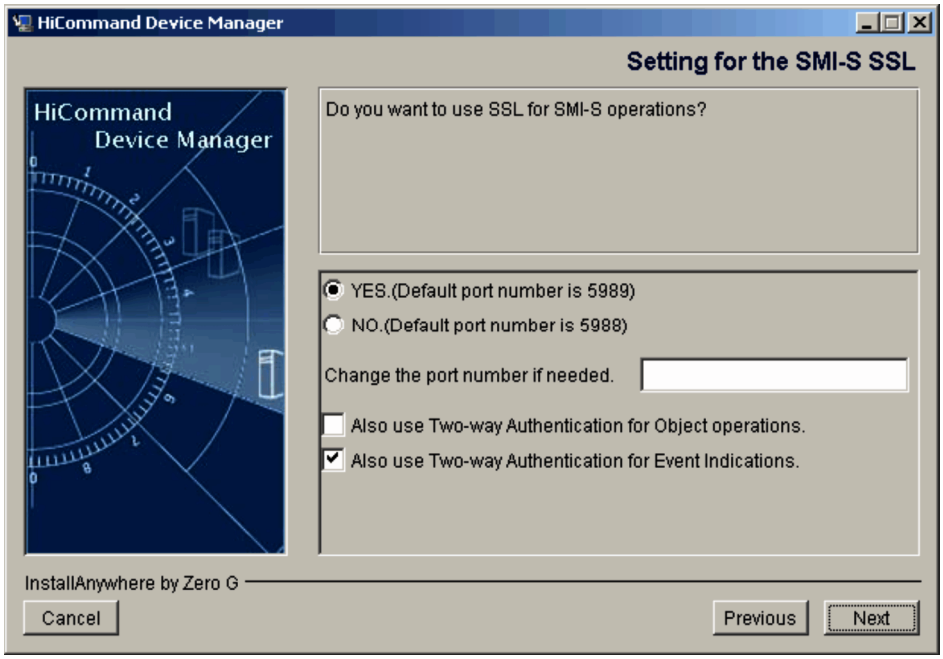

Figure 3.6 Setting for the SMI-S SSL Panel

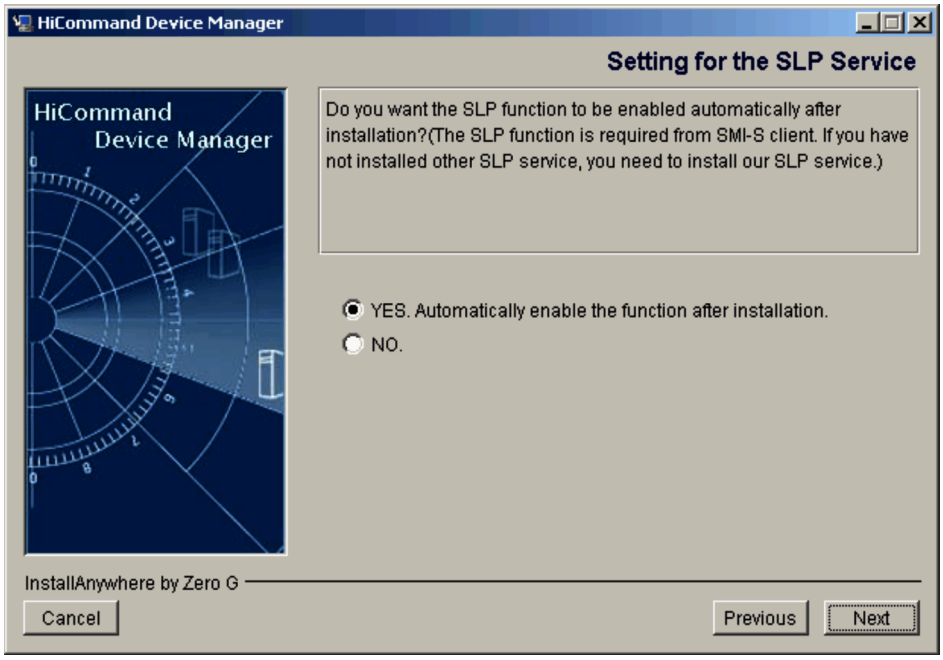

Figure 3.7 Setting for the SLP Service Panel

3.2.4 Upgrading or Re-installing Device Manager

After finishing an upgrade installation, be sure to back up the Device Manager Server database.

3.2.4.1 General Considerations for Upgrade and Re-installation

WARNING: Close the Services panel before you upgrade the HiCommand Device Manager server. Otherwise, the HiCommand Device Manager server service will be deleted when you close and then re-open the Services panel.

WARNING: Do not cancel in the middle of an upgrade or re-installation, because you could corrupt the files.

WARNING: If you are updating the Common Component database and an error occurs and auto-recovery fails, you must manually recover the database before you re-install the server. Once you upgrade or re-install the server, you will not be able to recover the Common Component database. To find a database update error, check the following log file: **<installation directory>\Base\log\hcmdsdbupdate.log**. You will want to restore the file named **<installation directory>\Base\database\hbase_vup_back.gbk**.

WARNING: Close the Services panel before you perform an upgrade installation or re-installation of the HiCommand Device Manager server. Otherwise, the HiCommand Device Manager server service will be deleted when you close and then re-open the Services panel.

Caution: If CIM/WBEM functions are being used when upgrading, you must release the registration of the SLP service from the Windows service before performing the upgrade. For details about releasing an SLP service registration, see the *HiCommand Device Manager CIM/WBEM User's Guide*.

If you have performed an upgrade installation without releasing the SLP service registration, it may fail to launch the SLP service after the installation.

In such a case, do the following:

1. Disable the Service Location Protocol service from the **Service** window in Windows.
2. Restart Windows.
3. Release the SLP service registration.
4. Register the SLP service again.

If you want to install a newer version of the Device Manager Server, install it over the existing version. Device Manager automatically updates your data and configurations to work with the latest version. The previous **HiCommandCLI.properties** file is saved as HiCommandCLI.properties.old in the same directory. The previous **TIA.properties** file is saved as TIA.properties.old in the same directory.

Important: If the `HiCommandCLI.properties` file contains multiple entries of the same key with different values, the value of the most recently specified key overrides the others. Although key duplication does not affect HiCommand CLI operations, we do not recommend that you specify the same key more than once with different values. We recommend that you eliminate unnecessary duplicate keys and their values. If there are duplicate keys that have different values during an upgrade installation, the new `HiCommandCLI.properties` file will inherit keys as follows:

If there are multiple `password` keys:

All `password` keys and their values in the old `HiCommandCLI.properties` file are written to the new file as is. The following shows an example:

- The `password` keys and their values in the old file:

  `password=AAA`

  `password=BBB`

- The `password` keys and their values written to the new file:

  `password=AAA`

  `password=BBB`

If there are duplicate keys other than `password`:

The name and value of the most recent duplicate key in the old `HiCommandCLI.properties` file are written to the new file as many times as there are duplicated keys. The following shows an example:

- The `user` keys and their values in the old file:

  `user=AAA`

  `user=BBB`

- The `user` keys and their values written to the new file:

  `user=BBB`

  `user=BBB`

Note: User-created files will not be saved as `*.old` during the upgrade.

If you want to manually make a backup before performing an upgrade installation or re-installation of the HiCommand Device Manager server, copy the following files and directories to another location:

- *installation-folder-for-the-Device-Manager-server*`\HiCommandServer\config\*.properties`

  The old `*.properties` files are backed up in the `config` file as `*.properties.old`. Note, however, that files created by a user will not be backed up.

- *installation-folder-for-the-Device-Manager-server*`\HiCommandServer\logs`

  To back up the log files, copy this folder to another location

- *installation-folder-for-the-Device-Manager-server*`\HiCommandCLI\HiCommandCLI.properties`

The old `HiCommandCLI.properties` files are backed up as `HiCommandCLI.properties.old` in the same folder.

- *installation-folder-for-the-Device-Manager-server*`\HiCommandCLI\legacy\R2.0\HiCommandCLI.properties`

  The old `HiCommandCLI.properties` files are backed up as `HiCommandCLI.properties.old` in the same folder.

- *installation-folder-for-the-Device-Manager-server*`\HiCommandCLI\legacy\R2.1\HiCommandCLI.properties`

  The old `HiCommandCLI.properties` files are backed up as `HiCommandCLI.properties.old` in the same folder.

- *installation-folder-for-the-Device-Manager-server*`\SupportTools\CollectTool\TIA.properties`

  The old `TIA.properties` files are backed up as `TIA.properties.old` in the same folder.

3.2.4.2 When Upgrading from Versions 2.2 Through 3.5 to Version 4.0 or Higher

WARNING: If either InterBase or InterServer have previously been installed, that service must be running when you upgrade the Device Manager Server.

WARNING: You cannot upgrade Device Manager version 2.2 or earlier directly to version 4.0 or later. You must first upgrade to a version between 2.3 and 3.5, and then upgrade to version 4.0 or later.

WARNING: If you have made any changes to **<common component installation folder>\conf\init.conf**, and you are upgrading from Device Manager version 3.0 or 3.1 to version 3.5 or later, you must first create a new folder for **<common component installation folder>\conf\user.conf**, and duplicate those changes in this file.

Important: The characters that can be used for user IDs in HiCommand Device Manager server (version 3.5 or later) are as follows:

A-Z a-z 0-9 - _ . @ + #.

User IDs containing characters other than the above cannot use version 3.5 or later. Thus, you must re-register users who have user IDs that contain unusable characters. If the User IDs of all the users who have the Admin permissions contain unusable characters, create new users by using the procedure in section 10.1.

Important: The characters that can be used for passwords in version 03-01-/A are as follows:

A-Z a-z 0-9 ! # $ % & ( ) * + - . = @ \ ^ _ | '

If a user cannot log in because their password contains a character other than the above, change the password for that user. If all users are unable to log in, view the procedure in section 10.1 and change the password to a password that contains only usable characters.

3.2.4.3 About User Information in Version 5.0 and Higher

Caution: In version 5.0 or later, user information is managed by using the user management functionality of HiCommand Suite Common Component. The registered user information is migrated to the HiCommand Suite Common Component repository when the Device Manager server program is started for the first time after the upgrade installation. For this migration, also note the following points:

- If there is user information that cannot be migrated to the HiCommand Suite Common Component repository due to data corruption or some other problem, that information is output to the Device Manager trace log file.
- If user accounts with the same user ID but different passwords have been registered in both HiCommand Suite Common Component and Device Manager, the user account in HiCommand Suite Common Component overrides the one in Device Manager. The user account registered in Device Manager becomes unavailable, and information to that effect is output to the Device Manager trace log file. For details about the Device Manager trace log file, see section 5.3.1.
- If user accounts that have the same user ID and password have been registered in both HiCommand Suite Common Component and Device Manager, the user account in Device Manager is added to the one in HiCommand Suite Common Component.
- You cannot migrate the user account whose user ID is `System`. The user management functionality of HiCommand Suite Common Component defines this user ID as having the `Admin` permission for all HiCommand Suite products (version 5.0 or later).

3.2.5 Performing an Upgrade Installation from Version 3.5 or Earlier

To upgrade the HiCommand Device Manager Server:

1. Log on to the system as an administrator.

   If a user who is not from the administrators group attempts installation, a window is displayed indicating that the user must be from the administrators group to perform installation. The installation then stops.

2. Load the HiCommand Device Manager installation CD-ROM.

   The installer usually starts automatically. If it does not start automatically, execute **install.exe** located in the root folder of the CD-ROM drive.

3. The HiCommand Device Manager Already Installed panel is displayed. Select **Next** to continue.

   WARNING: If you attempt to downgrade HiCommand Device Manager, the installer displays the HiCommand Device Manager Upgrade Error panel, and then exits. However, if the version and revision numbers of the builds before and after a downgrade are the same, the installer displays the WARNING: HiCommand Device Manager Downgrade panel. If there is no problem, select **Next** to continue.

4. When the HiCommand Suite Common Component services are running in a non-cluster environment, the Stop HiCommand Suite Product Services panel is displayed. Select **Next** to continue.

If the installer cannot stop all the services of HiCommand Suite Common Component and the HiCommand Suite products, the **Stop services error** panel is displayed. If this panel is displayed, select the **OK** button to close it, and then try again to stop the services. If the installer still fails to stop the services, cancel the installation, manually stop the services of HiCommand Suite Common Component and the HiCommand Suite products, and then perform the installation again.

To display the **Cancel Installation** panel, choose **Cancel**.

5. If the InterBase Not Installed panel or the Incorrect InterBase Version panel is displayed, choose **Cancel** to cancel the installation.

   If InterBase 6.0 has not been installed, uninstall the HiCommand Device Manager server and then start a new installation, or install HiCommand Device Manager 3.5 or earlier and then perform an upgrade installation.

   If the version of InterBase is incorrect, an upgrade installation cannot be performed. In this case, uninstall the HiCommand Device Manager server, and then start a new installation.

6. If the InterClient Not Installed panel or the Incorrect InterClient Version panel is displayed, choose **Cancel** to cancel the installation.

   If InterClient 2.0 has not been installed, uninstall the HiCommand Device Manager server and then start a new installation, or install HiCommand Device Manager 3.5 or earlier and then perform an upgrade installation.

   If the version of InterClient is incorrect, an upgrade installation cannot be performed. In this case, uninstall the HiCommand Device Manager server, and then start a new installation.

7. The License Agreement panel is displayed. Select **I accept the terms of the License Agreem**ent, and then **Next** to continue.

8. If Common Component 4.0 or later has not been installed, the **Choose the Database for HiCommand Suite Common Component** panel is displayed (see Figure 3.2). Specify the file location for Common Component. Use the following conventions for the path name:
   - Specify an absolute path, using no more than 90 bytes.
   - Do not enter a path delimiter (\) at the end of the folder path.
   - Do not use parentheses, except when referring to the Program Files (x86) folder.
   - You can use alphanumeric characters and spaces for the path name.
   - Folder names must not end with a period or space.

9. Select **Next** to continue. The **Choose the Database for HiCommand Device Manager** panel is displayed (see Figure 3.3).

10. Specify the file location for the Device Manager Server:
    - The file name and path have the same restrictions as the Common Component file name and path.

11. Select **Next** to continue. If the Common Component 3.0 or later has not been installed, the **Installation Server Information Settings** panel displays (see Figure 3.4).

12. Enter the IP address or host name of the server machine, and the port number for the HBase Storage Mgmt Web Service used by Web Client, and then select **Next**. The defaults are as follows:
    - IP address or host name: Default = None. Specify a valid host name or IP address on the network on which HiCommand Device Manager operates.
    - Port number: Default = 23015

    Important: This is the port number for the HBase Storage Mgmt Web Service used by Web Client, and not the HiCommand Device Manager server. If you use a port number other than the default, make sure that you also change the port number assigned to the Common Component. See section 5.4.2 for more information on changing Common Component ports.

13. In a non-cluster environment, the Set Services to Start After Installation panel is displayed. If you want to start the services of HiCommand Suite Common Component and related HiCommand Suite products after installation is complete, select **Yes**. If you do not want to start these services after installation is complete, select **No**. After you select **Yes** or **No**, select **Next** to go to the next step.

    Caution: The services of HiCommand Suite products whose versions are earlier than 5.7 are not started by selecting **Yes**. If you want to start the services of HiCommand Suite products after installation is complete, manually start the services. For details about how to start these services, see the manual for your product version.

    Important: To continue setup in a cluster environment after installation is complete, select **No**.

14. The Pre-installation Summary panel is displayed. The product name, installation folder, information on installation disk capacity, the IP address or host name of the server machine, and the port number to be used are displayed. Verify that the information is correct, then select **Install** to begin. The Progress panel will be displayed.

15. If you select **Cancel**, the **Cancellation Warning** panel will display, warning you that if you cancel now installation will not complete.

    WARNING: Choosing cancel after data conversion starts but before installation completes could damage the database.

16. **The Database Conversion** panel (see Figure 3.8) is displayed. When you select **Convert the database during installation**, the installer automatically converts the database:

    If the database conversion fails, the Database Convert Error panel (see Figure 3.9) is displayed.

    Important: If the upgrade operation is interrupted due to an error before the database conversion finishes, you must take specific recovery action. For instructions, see Chapter 10. Note that It might take a long time to convert the database. For example, if 8,000 LDEVs and 16,000 paths have been managed, the database conversion will take about 5 minutes in an environment that has a 1.5 GHz CPU and 1 GB of memory.

    Note: When you select **Next** in this window to display the subsequent window, you cannot return to this window by selecting **Previous** in the subsequent window.

17. When you select Convert the database after installation finishes, you will need to manually convert the database. For instructions, see section 3.7.

18. The **Please Wait** panel displays, followed by the **Progress** panel.

19. The Secure Socket Certificates Note panel is displayed. If you plan to run secure socket communications, note the information in this panel for later use. For more information on configuring secure sockets, see Chapter 7. Select **Next** to continue.
20. The **Install Complete** panel displays.
21. Select **Finish** to complete the installation.
22. Refresh all the registered subsystems to update the database.

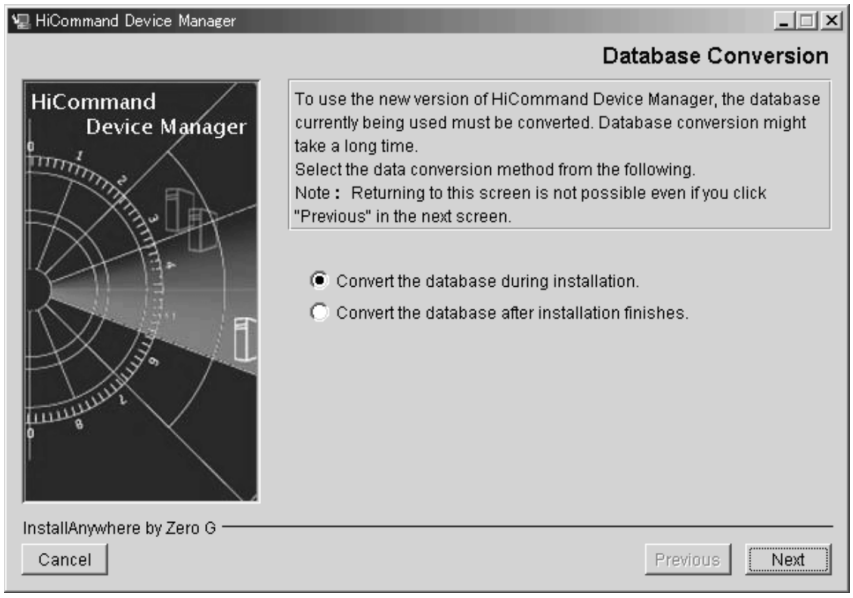

Figure 3.8 Database Conversion Panel

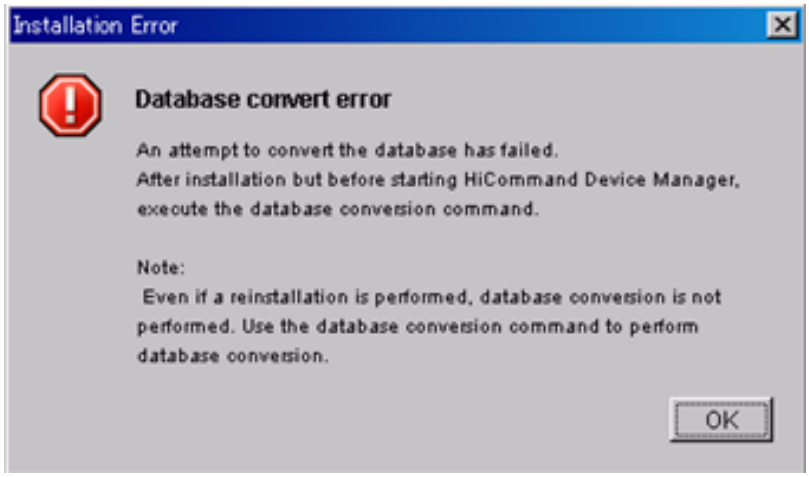

Figure 3.9 Database Convert Error Panel

3.2.6 Performing an Upgrade Installation from Version 4.0 or Later or Performing a Re-installation

The database can automatically be backed up or exported during installation. If you want to manually back up or export the database, perform the operations specified in section 3.6.1 or 3.6.3.4. Decide whether to back up or export the database by referring to the following points.

- If version 5.1 or earlier of a HiCommand Suite product is already installed, back up the database. You cannot export the database.
- If version 5.5 or later of a HiCommand Suite product has already been installed and you will perform an upgrade installation, we recommend you export the database.
- If you will perform a re-installation, we recommend you back up the database.

To perform an upgrade installation or re-installation of the HiCommand Device Manager server:

1. Log on to the system as an administrator.
2. Load the Device Manager Server Installation CD-ROM.

   The installer usually starts automatically. If it does not start automatically, execute **install.exe** located in the root folder of the CD-ROM drive.
3. The HiCommand Device Manager Already Installed panel is displayed. Select **Next** to continue.

   WARNING: If you attempt to downgrade HiCommand Device Manager, the installer displays the HiCommand Device Manager Upgrade Error panel and exits. However, if the version and revision numbers of the builds before and after a downgrade are the same, the installer displays the WARNING: HiCommand Device Manager Downgrade panel. If there is no problem, select **Next** to continue.
4. When the HiCommand Suite Common Component services are running in a non-cluster environment, the Stop HiCommand Suite Product Services panel is displayed.

   If the installer cannot stop all the services of HiCommand Suite Common Component and the HiCommand Suite products, the **Stop services error** panel is displayed. If this panel is displayed, select the **OK** button to close it, and then try again to stop the services. If the installer still fails to stop the services, cancel the installation, manually stop the services of HiCommand Suite Common Component and the HiCommand Suite products, and then perform the installation again.
5. The **Do you want to back up the database?** panel (see Figure 3.10) or the **Do you want to export the database?** panel (see Figure 3.11) is displayed. After you select whether to back up or export the database as described below, select **Next** to continue. The backup or export will be started based on the options you selected.
   - If you want to back up the database, select **YES. Back up the database during installation.** If you do not want to, select **NO. Do not back up or export the database during installation.**

– If you want to export the database, select **YES. Export the database during installation.** If you do not want to, select **NO. Do not export the database during installation.**

This operation backs up or exports all HiCommand Suite product databases. The following table describes the conditions whether the backup or export is performed, the backup-data storage destination folder, and the disk space required for the folder.

Table 3.5 Storage Destination of Backed up and Exported Data and Required Disk Space

Operation	Performing Conditions	Data storage destination folder#	Required Disk Space
Backup	▪ When the version of HiCommand Suite Common Component is 5.1 or earlier ▪ When the version of HiCommand Suite Common Component is 5.5 or later, and performing a re-installation of the same version and revision of HiCommand Device Manager	C:\Program Files\HiCommand\olddbbackup_hdb	See section 3.6.1.
Export	When the conditions for backing up data are not satisfied	C:\Program Files\HiCommand\olddbexported_hdb	See section 3.6.3.4.

#: The paths indicated in the table are those used when Device Manager is installed in the default installation folder.

Note: If the data storage destination folder already exists before backing up or exporting, the contents of the data storage destination folder are deleted. Before deletion, a deletion confirmation panel is displayed. If you want to save the old data, you need to copy it to another location beforehand, and then click the **OK** button in the deletion confirmation panel.

Note: Backing up or exporting can fail due to insufficient disk space, or for other reasons. If this occurs, back up or export the databases manually. Then, select **NO. Do not back up the database during installation** for backing up, or select **NO. Do not export the database during installation** for exporting, to continue the installation. For details about how to back up a database, see section 3.6.1. For information on how to export a database, see section 3.6.3.

Note: The **Do you want to back up the database?** panel or the **Do you want to export the database? panel** is skipped when you return from the next panel after performing backup or export operations.

6. The License Agreement panel is displayed. Select **I accept the terms of the License Agreement**, and then **Next** to continue.

7. If the Windows Firewall function is installed on the system, the Adding to the Windows Firewall exceptions panel is displayed. Check the contents of the panel, and select **Next** to continue.
8. In a non-cluster environment, the Set Services to Start After Installation panel is displayed. If you want to start the services of HiCommand Suite Common Component and related HiCommand Suite products after installation is complete, select **Yes**. If you do not want to start these services after installation is complete, select **No**. After you select **Yes** or **No**, select **Next** to go to the next step.

   Caution: The services of HiCommand Suite products whose versions are earlier than 5.7 are not started by selecting **Yes**. If you want to start the services of HiCommand Suite products after installation is complete, manually start the services. For details about how to start these services, see the manual for your product version.

   Important: To continue setup in a cluster environment after installation is complete, select **No**.
9. The **Pre-installation Summary** panel displays. The product name, installation folder, information on installation disk capacity, the IP address or host name of the server machine, and the port number to be used are displayed. Verify that the information is correct, then select **Install** to begin.
   - If you select **Cancel**, the **Cancellation Warning** panel displays, warning you that if you cancel now installation will not complete.
10. The **Please Wait** panel displays, and setup starts after installation, at which point the **Progress** panel displays.
11. The **Secure Socket Certificates Note** panel displays.
12. If you plan to run secure socket communications, note the information in this panel for later use. For more information on configuring secure sockets, see Chapter 7. Select **Next** to continue.
13. The **Install Complete** panel displays.
14. Select **Finish** to complete the installation.
15. Refresh all the registered subsystems to update the database.

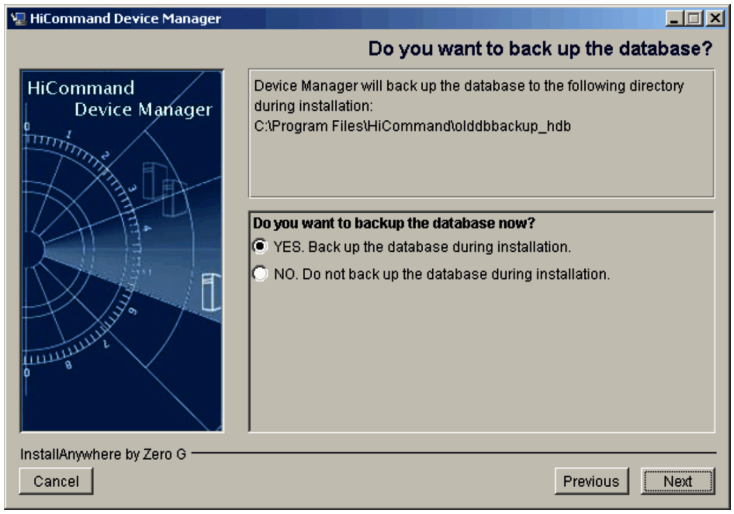

Figure 3.10 Do you want to back up the database? Panel

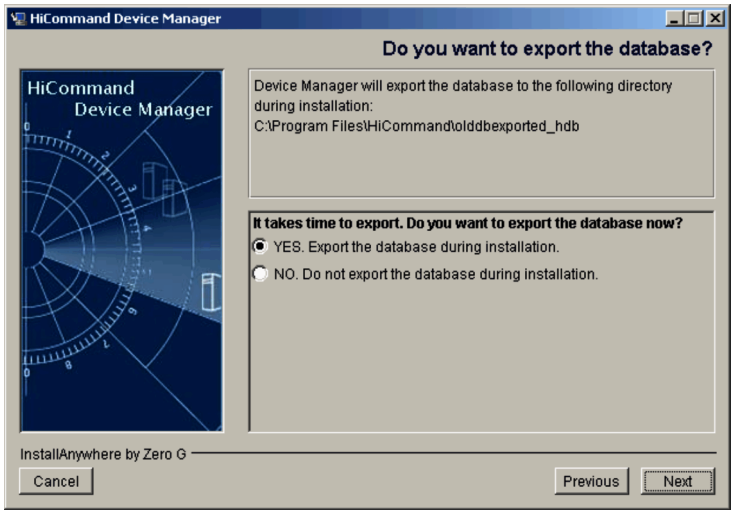

Figure 3.11 Do you want to export the database? Panel

3.3 Installing to a Microsoft Cluster Server Environment

HiCommand Device Manager Server can provide higher availability in a cluster environment. This section discusses the requirements and settings for a cluster environment.

You can change the environment in which the Device Manager system is already operating from a non-cluster configuration to a cluster configuration. For details, see section 3.3.6. If you want to install the Device Manager server in an environment in which other HiCommand Suite products are already installed in a cluster configuration, you need to make preparations such as canceling the cluster configuration. For details about the necessary preparations, see section 3.3.2.

3.3.1 System Requirements for a Cluster Server

The requirements for a cluster environment are as follows:

- Platform: See Table 3.1.
- Cluster software: Microsoft Cluster Service (MSCS)
- Number of nodes: 2
- Cluster configuration: Active-standby configuration

Caution: Disk configuration must be the same on all nodes that make up a cluster, and the installation folder for the Device Manager server must have the same name (including the drive letter and path name).

Caution: During installation, there is a step to back up and migrate the databases. Make sure that you secure the free disk space for backup and migration before installation. For the disk space required to back up, see section 3.6.1. The target disk (that is placed on the shared disk or local disk) to which the database is to be migrated must have the same free disk space or more as the database of the migration source.

Caution: To change the Device Manager settings after installation, specify the same settings for all nodes.

3.3.2 Preparations for Installing HiCommand Device Manager in an Environment Where Other HiCommand Suite Products Are Running

This section describes preparations required before installing Device Manager in an environment in which other HiCommand Suite products are running in a cluster configuration. In this procedure, the cluster configuration for other HiCommand Suite products is temporarily cancelled.

Caution: When you execute the `hcmdsdbmove` command or `hcmdsdbremake` command used in this procedure, the setting of the port that HiRDB uses will be restored to the default (23032). If you changed the port number from the default to another number, take a note of the port number that is being used so that you can set it again later.

1. Access the Cluster Administrator.
2. For each HiCommand Suite product and the HiRDB service, remove that product from the cluster monitoring target, as follows:
   - Place the target service offline.
   - Right-click each target service, select **Properties**, then select the **Advanced** tab. Select **Do not restart**, and then select **OK**.
3. Stop the services of all HiCommand Suite products in both the executing and standby nodes.

   For details about how to stop these services, see the manual for your product version.
4. Stop the Common Component in both the executing and standby nodes:

   <common component installation folder>\bin\hcmdssrv /stop

   The following shows an example of executing the command:

   C:\Program Files\HiCommand\Base\bin\hcmdssrv /stop

   Note: Do not stop the common component service while another HiCommand Suite common component service is running.
5. In Cluster Administrator, switch each group in which the HiCommand Suite product service has been registered in the executing system.

   In the Cluster Administrator, for each group where a HiCommand Suite product service has been registered, switch each group into the standby system by right-clicking a group then selecting **Move Group**.
6. Start HiRDB on the executing node.
   - Start HiRDB:

     <common component installation folder>\bin\hcmdsdbsrv /start

     The following shows an example of executing the command:

     C:\Program Files\HiCommand\Base\bin\hcmdsdbsrv /start
   - Back up the database (see section 3.6.1 if you need instructions).
7. Execute the command below to back up the database.

   For details about the options and cautions for backing up, see section 3.6.1.

   ```
   installation-folder-for-HiCommand-Suite-Common-Component\bin\hcmdsbackups /dir target-folder-for-storing-backup-files
   ```

   The following shows an example of executing the command:

   ```
   C:\Program Files\HiCommand\Base\bin\hcmdsbackups /dir C:\db_bkup01
   ```
8. On the executing node, back up the database contents.

   Delete or empty the *target-folder-for-outputting-data*, and then execute the following command.

   ```
   installation-folder-for-HiCommand-Suite-Common-Component\bin\hcmdsdbmove /export /datapath target-folder-for-outputting-data
   ```

   The following shows an example of executing the command:

   ```
   C:\Program Files\HiCommand\Base\bin\hcmdsdbmove /export /datapath C:\storing_data
   ```

   The following describes the `datapath` option.

datapath

Specify the folder to which you want to output the contents of the database. After this option name, specify the absolute path of a folder on a local disk. Note that the path name must not exceed 63 bytes. If the folder has already been created, empty the folder.

The characters that can be used to specify the path are shown below. In addition to these characters, a backslash (\), colon (:), or forward slash (/) can be used as path delimiters.

A-Z, a-z, 0-9, period (.), underscore (_)

Caution: You must not execute multiple instances of this command concurrently. Also, you must not execute this command and the hcmdsgetlogs command concurrently.

9. On the executing node, re-create the database system on a local disk.

   Execute the following command:

   ```
   installation-folder-for-HiCommand-Suite-Common-Component\bin\hcmdsdbremake
   /databasepath target-folder-for-re-creating-the-database
   ```

   The following shows an example of executing the command:

   ```
   C:\Program Files\HiCommand\Base\bin\hcmdsdbremake /databasepath D:\re_creating_db
   ```

   The following describes the databasepath option.

   databasepath

   Specify the folder in which you want to re-create the database. After this option name, specify the absolute path of an already created folder on a local disk. Note that the path name must not exceed 63 bytes.

   The characters that can be used to specify the path are shown below. In addition to these characters, a backslash (\), colon (:), or forward slash (/) can be used as path delimiters. However, a backslash (\) or forward slash (/) must not be specified as path delimiters at the end of the path name.

   A-Z, a-z, 0-9, period (.), underscore (_)

10. Register the contents of the database backed up in step 8, in the re-created database.

    Execute the command below. For *target-folder-for-inputting-data*, specify the absolute path of *target-folder-for-outputting-data* specified in step 8.

    ```
    installation-folder-for-HiCommand-Suite-Common-Component\bin\hcmdsdbmove /import
    /datapath target-folder-for-inputting-data
    ```

    The following shows an example of executing the command:

    ```
    C:\Program Files\HiCommand\Base\bin\hcmdsdbmove /import /datapath C:\storing_data
    ```

    Caution: You must not execute multiple instances of this command concurrently. Also, you must not execute this command and the hcmdsgetlogs command concurrently.

11. Copy *target-folder-for-outputting-data*, in which data was stored in step 8, onto the local disk of the standby node.

    A newly created folder made by this copy operation must satisfy the following conditions (so that the folder can be specified in the hcmdsdbmove command execution):

    - Absolute path for the copy target folder: no more than 63 bytes
    - Available characters for the copy target folder: A to Z, a to z, 0 to 9, period (.), and underscore (_).

12. In Cluster Administrator, switch each group in which the HiCommand Suite product service has been registered.

13. In the standby node, re-create the database system on a local disk.

    Execute the following command:

    ```
    installation-folder-for-HiCommand-Suite-Common-Component\bin\hcmdsdbremake
    /databasepath target-folder-for-re-creating-the-database
    ```

    The following shows an example of executing the command:

    ```
    C:\Program Files\HiCommand\Base\bin\hcmdsdbremake /databasepath D:\re_creating_db
    ```

    The following describes the `databasepath` option.

    `databasepath`

    Specify the folder in which you want to re-create the database. After this option name, specify the absolute path of an already created folder on a local disk. Note that the path name must not exceed 63 bytes.

    The characters that can be used to specify the path are shown below. In addition to these characters, a backslash (`\`), colon (`:`), or forward slash (`/`) can be used as path delimiters. However, a backslash (`\`) or forward slash (`/`) must not be specified as path delimiters at the end of the path name.

    `A-Z`, `a-z`, `0-9`, period (`.`), underscore (`_`)

14. On the standby node, register the contents of the database, in the re-created database.

    Execute the command below. For *target-folder-for-inputting-data*, specify the absolute path of the folder copied from the executing node in step 11.

    ```
    installation-folder-for-HiCommand-Suite-Common-Component\bin\hcmdsdbmove /import
    /datapath target-folder-for-inputting-data
    ```

    The following shows an example of executing the command:

    ```
    C:\Program Files\HiCommand\Base\bin\hcmdsdbmove /import /datapath C:\storing_data
    ```

    Caution: You must not execute multiple instances of this command concurrently. Also, you must not execute this command and the `hcmdsgetlogs` command concurrently.

15. On the executing or standby node, if HiCommand Suite Common Component is running, execute the following command to stop it:

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

    The following shows an example of executing the command:

    ```
    C:\Program Files\HiCommand\Base\bin\hcmdssrv /stop
    ```

16. If you changed the port number used by HiRDB from the default to another number, set the port number again on the executing and standby nodes.

    For details about how to set a port number, see section 5.4.2.

3.3.3 Performing a New Installation

After finishing a new installation, be sure to back up the Device Manager server database.

Caution: While performing cluster configuration, do not access HiCommand Device Manager.

Caution: Before starting installation, perform the following steps:

- If the cluster management IP address and shared disk are not enabled on the executing node, perform steps 1 to 5 in section 3.3.3.3 to place the resources of the cluster management IP address and shared disk online.
- If other HiCommand Suite products are already running in a cluster environment, make preparations such as canceling the cluster configuration. For details about the necessary preparations, see section 3.3.2.

3.3.3.1 Installing on the Executing Node

1. On the executing node, perform a new installation of the Device Manager server (see section 3.2.2). The following are the requirements for the installation:
   - Leave the settings specifying the location of the Common Component and the Device Manager Server databases at their default values (see Figure 3.2 and Figure 3.3).
   - For the IP address of the Device Manager Server, specify a logical host name (see Figure 3.4).

   Important: A logical host name indicates the name of a virtual host allocated to the cluster management IP address.
2. After the Device Manager Server is installed on the executing node, enter the license key by using the Web Client.

   Note: You should have received a CD that contains the HiCommand Device Manager License Key. You should upload the License Key file to a directory on the same server where Device Manager will be installed. That way you can select the button next to **License File** and browse for the License Key file. Once the file is found simply highlight the file and select the **Open** button. This will update Device Manager with the permanent License Key.
3. Use a text editor to create a cluster configuration file, as follows:
   - **mode:** Specify online.
   - **virtualhost:** Specify the logical host name.
   - **onlinehost:** Specify the host name of the executing node.
   - **standbyhost:** Specify the host name of the standby node.

   Sample command:

```
mode = online
virtualhost = hcmdserver
onlinehost = hcmdserver_1
standbyhost = hcmdserver_2
```

4. Save the created file as **cluster.conf** in **<common component installation folder>\conf**.

   Caution: You cannot specify an IP address for virtualhost, onlinehost, or standbyhost. Confirm that the IP address can be resolved from the host name.

   Caution: An IP address that is enabled and accessible must be assigned to the logical host name to be specified in `virtualhost`.

5. If HiCommand Suite products whose versions are earlier than 5.7 have been installed, stop their services.

   For details about how to stop these services, see the manual for your product version.

6. If HiCommand Suite Common Component is running, stop the services of HiCommand Suite Common Component and all HiCommand Suite products, and then start HiRDB.

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

   The following shows an example of executing the commands:

```
C:\Program Files\HiCommand\Base\bin\hcmdssrv /stop
C:\Program Files\HiCommand\Base\bin\hcmdsdbsrv /start
```

7. Execute the command below to back up the database.

   For details about the options and cautions for backing up, see section 3.6.1.

```
installation-folder-for-HiCommand-Suite-Common-Component\bin\hcmdsbackups /dir target-folder-for-storing-backup-files
```

   The following shows an example of executing the command:

```
C:\Program Files\HiCommand\Base\bin\hcmdsbackups /dir C:\db_bkup01
```

8. Migrate the database to the shared disk.

   Delete or empty *target-folder-for-storing-data*, and then execute the following command. When this command is executed, the setting of the port that HiRDB uses will be restored to the default (23032). If you changed the port number from the default to another number, take a note of the port number that is being used so that you can set it again later.

```
installation-folder-for-HiCommand-Suite-Common-Component\bin\hcmdsdbclustersetup
/createcluster /databasepath target-folder-for-re-creating-the-database /exportpath
target-folder-for-storing-data /auto
```

   The following shows an example of executing the command:

```
C:\Program Files\HiCommand\Base\bin\hcmdsdbclustersetup /createcluster /databasepath
R:\re_creating_db /exportpath C:\storing_data /auto
```

   The following describes the options specified in the `hcmdsdbclustersetup` command.

   `databasepath`

   Specify the folder in which you want to re-create the database. After this option name, specify the absolute path of a folder on a shared disk. Note that the path name must not exceed 63 bytes.

   The characters that can be used to specify the path are as follows. In addition to these characters, a backslash (`\`), colon (`:`), or forward slash (`/`) can be used as path delimiters.

   `A-Z`, `a-z`, `0-9`, period (`.`), underscore (`_`)

   `exportpath`

Specify the folder in which you want to store backup data. After this option name, specify the absolute path of a folder on the local disk. Note that the path name must not exceed 63 bytes. If the folder has already been created, delete its contents. The characters that can be used to specify the path are the same as for `databasepath`.

`auto`

Specify this option to stop the HiCommand Suite product services and to start HiRDB automatically as preparation for processing the database. After the command is executed, the HiCommand Suite product services and HiRDB are stopped. Note that the services of HiCommand Suite products whose versions are earlier than 5.7 are not stopped automatically.

Caution: You must not execute multiple instances of this command concurrently. Also, you must not execute this command and the `hcmdsgetlogs` command concurrently.

Caution: For details about how to set the port that HiRDB uses, see section 5.4.2.

Note: This operation restarts HiCommand Suite Common Component.

9. If HiCommand(R) Suite Common Component is running, execute the following command to stop it.

   <common component installation folder>\bin\hcmdssrv /stop

   The following shows an example of executing the command:

   C:\Program Files\HiCommand\Base\bin\hcmdssrv /stop

   Note: Do not stop the common component service while another HiCommand Suite common component service is running.

10. Open the **Services** panel. For each of the following services, open the property, and then change Startup Type from **Automatic** to **Manual**:
    - HBase Storage Mgmt Common Service
    - HBase Storage Mgmt Web Service
    - HiCommand Server

3.3.3.2 Installing on Standby Node

The following are the specific requirements for installation on the standby node:

- Specify the same installation path as on the executing node (see Figure 3.1).
- Leave the settings specifying the location of the Common Component and the Device Manager Server databases at the default values (see Figure 3.2 and Figure 3.3).
- For the IP address of the Device Manager Server, specify a logical host name (see Figure 3.4).

1. On the standby node, perform a new installation of the Device Manager Server. When the Back up the database panel displays (see Figure 3.10), select **NO. Do not back up or export the database during installation.**

   Important: A logical host name indicates the name of a virtual host allocated to the cluster management IP address.

2. After the Device Manager Server is installed on the standby node, enter the license key by using the Web Client. For more information on using the Web Client, please see the *HiCommand Device Manager Web Client User's Guide*.

   Note: You should have received a CD that contains the HiCommand Device Manager License Key. You should upload the License Key file to a directory on the same server where Device Manager will be installed. That way you can select the button next to **License File** and browse for the License Key file. Once the file is found simply highlight the file and select the **Open** button. This will update Device Manager with the permanent License Key.

3. Use the IP address of the standby node to access the Device Manager Server.

4. Use a text editor to create a cluster configuration file. The items to be specified in the cluster configuration file are as follows:

   - **mode**: Specify standby.
   - **virtualhost**: Specify the logical host name.
   - **onlinehost**: Specify the host name of the executing node.
   - **standbyhost**: Specify the host name of the standby node.

   Sample command:

```
mode = standby
virtualhost = hcmdserver
onlinehost = hcmdserver_1
standbyhost = hcmdserver_2
```

5. Save the created file as cluster.conf in **<common component installation folder>\conf**.

   Caution: You cannot specify an IP address for virtualhost, onlinehost, or standbyhost. Confirm that the IP address can be resolved from the host name.

6. If HiCommand Suite products whose versions are earlier than 5.7 have been installed, stop their services.

   For details about how to stop these services, see the manual for your product version.

7. Change the setting so that the database on the shared disk is to be used.

   After deleting or emptying *target-folder-for-storing-data*, execute the following command.When this command is executed, the setting of the port that HiRDB uses will be restored to the default (23032). If you changed the port number from the default to another number, take a note of the port number that is being used so that you can set it again later.

```
installation-folder-for-HiCommand-Suite-Common-Component\bin\hcmdsdbclustersetup
/createcluster /databasepath target-folder-for-re-creating-database /exportpath
target-folder-for-storing-data /auto
```

   The following shows an example of executing the command:

```
C:\Program Files\HiCommand\Base\bin\hcmdsdbclustersetup /createcluster
/databasepath R:\re_creating_db /exportpath C:\storing_data /auto
```

   The following describes the options specified in the `hcmdsdbclustersetup` command.

   `databasepath`

Specify the folder in which you want to re-create the database. After this option name, specify the absolute path of the same folder as *target-folder-for-re-creating-database* specified for the executing node. This folder must be located on a shared disk, and the absolute path must not exceed 63 bytes.

The characters that can be used to specify the path are as follows. In addition to these characters, a backslash (\), colon (:), or forward slash (/) can be used as path delimiters.

A-Z, a-z, 0-9, period (.), underscore (_)

`exportpath`

Specify the folder in which you want to store backup data. After this option name, specify the absolute path of a folder on the local disk. Note that the path name must not exceed 63 bytes. If the folder has already been created, delete its contents. The characters that can be used to specify the path are the same as for `databasepath`.

`auto`

Specify this option to stop the HiCommand Suite product services and to start HiRDB automatically as preparation for processing the database. After the command is executed, the HiCommand Suite product services and HiRDB are stopped. Note that the services of HiCommand Suite products whose versions are earlier than 5.7 are not stopped automatically.

Caution: You must not execute multiple instances of this command concurrently. Also, you must not execute this command and the `hcmdsgetlogs` command concurrently.

Caution: For details about how to set the port that HiRDB uses, see section 5.4.2.

Note: This operation restarts the Common Component.

8. If HiCommand(R) Suite Common Component is running, execute the following command to stop it.

   <common component installation folder>\bin\hcmdssrv /stop

   The following shows an example of executing the command:

   C:\Program Files\HiCommand\Base\bin\hcmdssrv /stop

   Note: Do not stop the common component service while another HiCommand Suite common component service is running.

9. Open the **Services** panel. For each of the following services, open the property, and then change Startup Type from **Automatic** to **Manual**:
   - HBase Storage Mgmt Common Service
   - HBase Storage Mgmt Web Service
   - HiCommand Server

3.3.3.3 Configuring Microsoft Cluster Server During a New Installation

1. Open the Cluster Administrator:

   Select **Start, Settings, Control Panel, Administrative Tools,** and then **Cluster Administrator.**

2. If there is an existing group in which to register the Device Manager service, select that group. If there is not, create one.

   Caution: Use only resources related to HiCommand Suite products to configure the resource group.

3. Select **IP address** in **Resource type** to register the cluster management IP address to a resource group.
4. Select **Network name** in **Resource type** to register the logical host name to a resource group.
5. Select **Physical disk** in **Resource type** to register the shared disk to a resource group.
6. Register HBase Storage Mgmt Common Service, HBase Storage Mgmt Web Service, HiCommandServer, and HiRDB as resources. Select **New**, and then **Resource**. In each panel, specify the settings as shown in the following tables.

Table 3.6 Settings to Register HiRDB as a Resource

Dialog Box Name	Setting
New Resource	Name: `HiRDB` (optional) Resource type: Generic Service.
Possible Owners	Make sure that the executing and standby nodes have been added.
Dependencies	Register the drive of the shared disk drive and network name.
Generic Service Parameters	Service Name: `HiRDBClusterService_HD0` Start parameters: Specify nothing.
Registry Replication	Specify nothing.

Table 3.7 Settings to Register the HBase Storage Mgmt Common Service as a Resource

Dialog Box Name	Setting
New Resource	Name: `Mgmt Common Service` (optional) Resource type: Generic Service.
Possible Owners	Make sure that the executing and standby nodes have been added.
Dependencies	Register HiRDB.
Generic Service Parameters	Service Name: `HBaseStgMgmtComService` Start parameters: Specify nothing.
Registry Replication	Specify nothing.

Table 3.8 Settings to Register the HBase Storage Mgmt Web Service as a Resource

Dialog Box Name	Setting
New Resource	Name: `Mgmt Web Service` (optional) Resource type: Generic Service.
Possible Owners	Make sure that the executing and standby nodes have been added.
Dependencies	Register Mgmt Common Service.
Generic Service Parameters	Service Name: `HBaseStgMgmtWebService` Start parameters: Specify nothing.
Registry Replication	Specify nothing.

Table 3.9 Settings to Register the HiCommand Device Manager Server as a Resource

Dialog Box Name	Setting
New Resource	Name: `HiCommandServer` (optional) Resource type: Generic Service.
Possible Owners	Make sure that the executing and standby nodes have been added.
Dependencies	Register the Mgmt Web Service.
Generic Service Parameters	Service Name: `HiCommandServer` Start parameters: Specify nothing.
Registry Replication	Specify nothing.

7. In Cluster Administrator, place the group to which the HiCommand Device Manager service has been registered online.

3.3.4 Performing an Upgrade Installation from Version 3.5 or Earlier

After finishing an upgrade installation, be sure to back up the HiCommand Device Manager server database.

Caution: Before starting installation, perform the following steps:

- When *installation-folder-for-HiCommand-Suite-Common-Component*\conf\init.conf has been changed, if you want to upgrade Device Manager version 3.0 or 3.1 to 3.5 or later, create *installation-folder-for-HiCommand-Suite-Common-Component*\conf\user.conf, and then write any changes in init.conf into the created user.conf.
- If Device Manager and other HiCommand Suite products are already running in a cluster environment, make preparations such as canceling the cluster configuration. For details about the necessary preparations, see section 3.3.2.

3.3.4.1 Upgrading Device Manager on the Executing Node

1. Display the cluster administrator:

   Start → Settings Control Panel Programs → Administrative Tools → Cluster Administrator

   Note: When the Device Manager Server is upgraded from version 3.5 or earlier to 4.0 or later, these menu options are deleted.

2. Place the following services offline:
   - HiCommand Server
   - HBase Storage Mgmt Web Service
   - HBase Storage Mgmt Common Service

   The above services are represented by the resource names registered in section 3.3.3.3.

3. For each of those services, in the Cluster Administrator, right-click the service, select **Properties**, select the **Advanced** tab, select **Do not restart**, and then select **OK**.

4. Stop the HiCommand Suite product services.

   For details about how to stop these services, see the manual for your product version.

5. Stop HiCommand Suite Common Component, and then start HiRDB.

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

   The following shows an example of executing the commands:

   ```
   C:\Program Files\HiCommand\Base\bin\hcmdssrv /stop
   C:\Program Files\HiCommand\Base\bin\hcmdsdbsrv /start
   ```

6. Execute the command below to back up the databases.

   For details about the options and cautions for backing up, see section 3.6.1.

   ```
   installation-folder-for-HiCommand-Suite-Common-Component\bin\hcmdsbackups /dir target-folder-for-storing-backup-files
   ```

   The following shows an example of executing the command:

   ```
   C:\Program Files\HiCommand\Base\bin\hcmdsbackups /dir C:\db_bkup01
   ```

7. Execute the following command to stop HiCommand Suite Common Component:

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

   The following shows an example of executing the command:

```
C:\Program Files\HiCommand\Base\bin\hcmdssrv /stop
```

8. When you perform the upgrade installation, be sure to specify the local disk as the location of the Common Component and HiCommand Device Manager Server databases (see Figure 3.2 and Figure 3.3), and perform database conversion during the installation (see Figure 3.8).

9. Use a text editor to create a cluster configuration file, as follows:

   - **mode:** Specify `online`.
   - **virtualhost:** Specify the logical host name.
   - **onlinehost:** Specify the host name of the executing node.
   - **standbyhost:** Specify the host name of the standby node.

   Sample command:

```
mode = online
virtualhost = hcmdserver
onlinehost = hcmdserver_1
standbyhost = hcmdserver_2
```

10. Save the created file as cluster.conf in **<common component installation folder>\conf**.

    Caution: You cannot specify an IP address for virtualhost, onlinehost, or standbyhost. Confirm that the IP address can be resolved from the host name.

11. If HiCommand Suite products whose versions are earlier than 5.7 have been installed, stop their services.

    For details about how to stop these services, see the manual for your product version.

12. If HiCommand Suite Common Component is running, stop the services of HiCommand Suite Common Component and all HiCommand Suite products, and then start HiRDB.

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

    The following shows an example of executing the commands:

```
C:\Program Files\HiCommand\Base\bin\hcmdssrv /stop
C:\Program Files\HiCommand\Base\bin\hcmdsdbsrv /start
```

13. Execute the command below to back up the database.

    For details about the options and cautions for backing up, see section 3.6.1.

```
installation-folder-for-HiCommand-Suite-Common-Component\bin\hcmdsbackups /dir target-folder-for-storing-backup-files
```

    The following shows an example of executing the command:

```
C:\Program Files\HiCommand\Base\bin\hcmdsbackups /dir C:\db_bkup01
```

14. Migrate the database to the shared disk.

Delete or empty *target-folder-for-storing-data*, and then execute the following command. When this command is executed, the setting of the port that HiRDB uses will be restored to the default (23032). If you changed the port number from the default to another number, take a note of the port number that is being used so that you can set it again later.

```
installation-folder-for-HiCommand-Suite-Common-Component\bin\hcmdsdbclustersetup
/createcluster /databasepath target-folder-for-re-creating-the-database /exportpath
target-folder-for-storing-data /auto
```

The following shows an example of executing the command:

```
C:\Program Files\HiCommand\Base\bin\hcmdsdbclustersetup /createcluster /databasepath
R:\re_creating_db /exportpath C:\storing_data /auto
```

The following describes the options specified in the `hcmdsdbclustersetup` command.

`databasepath`

Specify the folder in which you want to re-create the database. After this option name, specify the absolute path of a folder on a shared disk. Note that the path name must not exceed 63 bytes.

The characters that can be used to specify the path are as follows. In addition to these characters, a backslash (`\`), colon (`:`), or forward slash (`/`) can be used as path delimiters.

`A-Z`, `a-z`, `0-9`, period (`.`), underscore (`_`)

`exportpath`

Specify the folder in which you want to store backup data. After this option name, specify the absolute path of a folder on the local disk. Note that the path name must not exceed 63 bytes. If the folder has already been created, delete its contents. The characters that can be used to specify the path are the same as for `databasepath`.

`auto`

Specify this option to stop the HiCommand Suite product services and to start HiRDB automatically as preparation for processing the database. After the command is executed, the HiCommand Suite product services and HiRDB are stopped. Note that the services of HiCommand Suite products whose versions are earlier than 5.7 are not stopped automatically.

Caution: You must not execute multiple instances of this command concurrently. Also, you must not execute this command and the `hcmdsgetlogs` command concurrently.

Caution: For details about how to set the port that HiRDB uses, see section 5.4.2.

15. If HiCommand(R) Suite Common Component is running, execute the following command to stop it.

    <common component installation folder>\bin\hcmdssrv /stop

    The following shows an example of executing the command:

    C:\Program Files\HiCommand\Base\bin\hcmdssrv /stop

    Note: Do not stop the common component service while another HiCommand Suite common component service is running.

16. Open the Services panel. Open the property for the following services, and then change **Startup Type** from **Automatic** to **Manual**:

    – HBase Storage Mgmt Common Service

- HBase Storage Mgmt Web Service
- HiCommand Server

3.3.4.2 Upgrading Device Manager on the Standby Node

1. Open the Services panel. Start the following services:
   - InterBase
   - InterBase Server
2. Access **<server installation folder>\HiCommandServer\database\interbase**.
3. Change the file name of the **HICOMMAND.GDB_org** file to **HICOMMAND.GDB**.
4. Change the file name of the **HiCommand.gbk_org** file to **HiCommand.gbk.**
5. Use a text editor to open the following property file:

   <server installation folder>\HiCommandServer\config\database.properties
6. Change the line beginning with **dbm.url=** as shown below:

   dbm.url=jdbc:interbase://localhost/<server installation folder>/HiCommandServer/database/interbase/HICOMMAND.GDB

   Caution: Use a forward slash (/), not a backslash (\) for the path delimiter.
7. Access **<common component installation folder>\database**.
8. Change the file name of the **HBASE.GDB_org** file to **HBASE.GDB**.
9. Use a text editor to open the following file:

   <common component installation folder>\conf\user.conf
10. If this file does not already exist, create the file.
11. Change the line beginning with DATABASE.path= as shown below:

    DATABASE.path= <common component installation folder>/database/HBASE.GDB

    If this line does not already exist, create the line.

    Caution: Use a forward slash (/), not a backslash (\) for the path delimiter.
12. Stop the services of HiCommand Suite products.

    For details about how to stop these services, see the manual for your product version.
13. Stop HiCommand Suite Common Component.

    Execute the following command:

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

    The following shows an example of executing the command:

    ```
    C:\Program Files\HiCommand\Base\bin\hcmdssrv /stop
    ```
14. On the standby node, perform an upgrade installation of the Device Manager Server. Make sure of the following:

    Leave the settings specifying the location of the Common Component and the Device Manager Server as the default values (see Figure 3.2 and Figure 3.3).

If you are upgrading from version 4.0 or higher, do not convert the database (see Figure 3.8).

15. Use a text editor to create a cluster configuration file.
16. The items to be specified in the cluster configuration file are as follows:
    - **virtualhost:** Specify the logical host name.
    - **onlinehost:** Specify the host name of the executing node.
    - **standbyhost:** Specify the host name of the standby node.

    Sample command:

```
mode = standby
virtualhost = hcmdserver
onlinehost = hcmdserver_1
standbyhost = hcmdserver_2
```

17. Save the created file as cluster.conf in **<common component installation folder>\conf**.

    Caution: You cannot specify an IP address for virtualhost, onlinehost, or standbyhost. Confirm that the IP address can be resolved from the host name.

18. If HiCommand Suite products whose versions are earlier than 5.7 have been installed, stop their services.

    For details about how to stop these services, see the manual for your product version.

19. Change the setting so that the database on the shared disk is to be used.

    After deleting or emptying *target-folder-for-storing-data*, execute the following command.When this command is executed, the setting of the port that HiRDB uses will be restored to the default (23032). If you changed the port number from the default to another number, take a note of the port number that is being used so that you can set it again later.

```
installation-folder-for-HiCommand-Suite-Common-Component\bin\hcmdsdbclustersetup
/createcluster /databasepath target-folder-for-re-creating-database /exportpath
target-folder-for-storing-data /auto
```

    The following shows an example of executing the command:

```
C:\Program Files\HiCommand\Base\bin\hcmdsdbclustersetup /createcluster /databasepath
R:\re_creating_db /exportpath C:\storing_data /auto
```

    The following describes the options specified in the `hcmdsdbclustersetup` command.

    `databasepath`

    Specify the folder in which you want to re-create the database. After this option name, specify the absolute path of the same folder as *target-folder-for-re-creating-database* specified for the executing node. This folder must be located on a shared disk, and the absolute path must not exceed 63 bytes.

    The characters that can be used to specify the path are as follows. In addition to these characters, a backslash (`\`), colon (`:`), or forward slash (`/`) can be used as path delimiters.

    `A-Z`, `a-z`, `0-9`, period (`.`), underscore (`_`)

    `exportpath`

Specify the folder in which you want to store backup data. After this option name, specify the absolute path of a folder on the local disk. Note that the path name must not exceed 63 bytes. If the folder has already been created, delete its contents. The characters that can be used to specify the path are the same as for `databasepath`.

`auto`

Specify this option to stop the HiCommand Suite product services and to start HiRDB automatically as preparation for processing the database. After the command is executed, the HiCommand Suite product services and HiRDB are stopped. Note that the services of HiCommand Suite products whose versions are earlier than 5.7 are not stopped automatically.

Caution: You must not execute multiple instances of this command concurrently. Also, you must not execute this command and the `hcmdsgetlogs` command concurrently.

Caution: For details about how to set the port that HiRDB uses, see section 5.4.2.

Note: This operation restarts the Common Component.

20. If HiCommand(R) Suite Common Component is running, execute the following command to stop it.

    <common component installation folder>\bin\hcmdssrv /stop

    The following shows an example of executing the command:

    C:\Program Files\HiCommand\Base\bin\hcmdssrv /stop

    Note: Do not stop the common component service while another HiCommand Suite common component service is running.

21. In the Services panel, open the properties for the following services, and then change **Startup Type** from **Automatic** to **Manual**:

    - HBase Storage Mgmt Common Service
    - HBase Storage Mgmt Web Service
    - HiCommand Server

3.3.4.3 Configuring Microsoft Cluster Server During an Upgrade Installation

1. Display the Cluster Administrator:

   Start → Settings Control Panel Programs → Administrative Tools → Cluster Administrator

   Note: When the Device Manager Server is upgraded from version 3.5 or earlier to 4.0 or later, these menu options are deleted.

2. Specify the following services in the cluster resources. Make the same settings for each parameter of the resources as in a new installation:

   - HBase Storage Mgmt Web Service
   - HBase Storage Mgmt Common Service
   - HiCommand Server
   - HiRDB

3. If no other resources are depending on InterBase and InterBase Server, you can delete them.
4. In Cluster Administrator, right-click the following services, select **Properties**, select the **Advanced** tab, select **Restart**, and then select **OK**:
   - HBase Storage Mgmt Common Service
   - HBase Storage Mgmt Web Service
   - HiCommand Server

   The above services are represented by the resource names registered in step 2.
5. In Cluster Administrator, place the group to which the Device Manager service has been registered online.

3.3.5 Performing an Upgrade Installation from Version 4.0 or Later or Performing a Re-installation

This section describes how to perform an upgrade installation of HiCommand Device Manager from version 4.0 or later and how to re-install the same version of HiCommand Device Manager by overwriting in a cluster environment.

Warning: After finishing an upgrade installation or re-installation, make sure to back up the HiCommand Device Manager server database.

Caution: Before starting installation, perform the following steps:

- If the services on the executing node are offline, place them online.
- If Device Manager and other HiCommand Suite products are already running in a cluster environment, make preparations such as canceling the cluster configuration. For details about the necessary preparations, see section 3.3.2.

3.3.5.1 Performing an Upgrade or Re-installation of Device Manager on the Executing Node

1. Display Cluster Administrator:

   Select **Start**, **Settings**, **Control Panel**, **Administrative Tools**, and then **Cluster Administrator**.
2. Place the following services offline:
   - HiCommand Server
   - HBase Storage Mgmt Web Service
   - HBase Storage Mgmt Common Service

   The above services are represented by the resource names registered in section 3.3.3.3.
3. Stop the services of HiCommand Suite products.

   For details about how to stop these services, see the manual for your product version.
4. Stop the Common Component:

   <common component installation folder>\bin\hcmdssrv /stop

   The following shows an example of executing the command:

C:\Program Files\HiCommand\Base\bin\hcmdssrv /stop

Note: Do not stop the common component service while another HiCommand Suite common component service is running.

5. In Cluster Administrator, place the **HiRDB** service offline.

   The above service is represented by the resource name registered in section 3.3.3.3.

6. In Cluster Administrator, right-click the following services, select **Properties**, select the **Advanced** tab, **Do not restart**, and then **OK**:
   - HBase Storage Mgmt Common Service
   - HBase Storage Mgmt Web Service
   - HiCommand Server
   - HiRDB

   The above services are represented by the resource names registered in section 3.3.3.3.

7. erform an upgrade installation or re-installation of the HiCommand Device Manager server (see section 3.2.6). When the **Do you want to back up the database?** panel is displayed, choose **YES. Back up the database during installation** (see Figure 3.10). When the **Do you want to export the database?** panel is displayed, choose **YES. Export the database during installation** (see Figure 3.11).

8. If HiCommand Suite Common Component is running, stop it as follows:

   Select **Start**, **Programs**, **HiCommand, Device Manager**, and then **Stop Server with Common Services**.

9. In the **Services** panel, open the properties for the following services, and then change **Startup Type** from **Automatic** to **Manual**:
   - HBase Storage Mgmt Common Service
   - HBase Storage Mgmt Web Service
   - HiCommand Server

10. Switch, to the standby node, the group in which the HiCommand Device Manager service has been registered.

    In Cluster Administrator, right-click the group to which the HiCommand Device Manager service has been registered, and then choose **Move Group**.

3.3.5.2 Performing an Upgrade or Re-installation of Device Manager on the Standby Node

1. Stop the services of HiCommand Suite products.

   For details about how to stop these services, see the manual for your product version.

2. Stop HiCommand Suite Common Component.

   Execute the following command:

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

   The following shows an example of executing the command:

   ```
   C:\Program Files\HiCommand\Base\bin\hcmdssrv /stop
   ```

3. Perform an upgrade installation or re-installation of the HiCommand Device Manager server (see section 3.2.6). Do NOT back up the database during installation.

   Caution: Even when the **Do you want to back up the database?** panel or the **Do you want to export the database?** panel is displayed, do not perform either operation. If you perform the backup or export operation, installation will fail (see Figure 3.10 and Figure 3.11).

4. If HiCommand Suite Common Component is running, stop it as follows:

   Select **Start, Programs, HiCommand, Device Manager,** and then **Stop Server with Common Services**.

5. In the **Services** panel, open the property for the following services, and then change Startup Type from **Automatic** to **Manual**:
   - HBase Storage Mgmt Common Service
   - HBase Storage Mgmt Web Service
   - HiCommand Server

6. In Cluster Administrator, right-click the following services, select **Properties**, select the **Advanced** tab, select **Restart**, and then select **OK**:
   - HBase Storage Mgmt Common Service
   - HBase Storage Mgmt Web Service
   - HiCommand Server
   - HiRDB

   The above services are represented by the resource names registered in section 3.3.3.3.

7. In Cluster Administrator, place the group to which the HiCommand Device Manager service has been registered online.

3.3.6 Changing to a Cluster Environment after Starting HiCommand Device Manager Server

When you want to change to a cluster configuration after the HiCommand Device Manager system operations have started in a non-cluster configuration, carry out the following procedure. In this example, the HiCommand Device Manager server whose operations are already running is treated as an executing node.

1. Install the HiCommand Device Manager server on the host to be used as a standby node.
2. On the standby node, display the Web Client login window and then enter the license key.
3. On the executing node and standby node, use the text editor to create a cluster-configuration file for each node.

   The items to be specified in the cluster-configuration file are as follows:

   `mode`: Specify `online` for the executing node, and `standby` for the standby node.

   `virtualhost`: Specify the logical host name.

   `onlinehost`: Specify the host name of the executing node.

   `standbyhost`: Specify the host name of the standby node.

The following shows a coding example in the cluster-configuration file on the executing node:

```
mode = online
virtualhost = hcmdserver
onlinehost = hcmdserver_1
standbyhost = hcmdserver_2
```

Save the created file as `cluster.conf` in *installation-folder-for-HiCommand-Suite-Common-Component*`\conf`.

Caution: An IP address cannot be specified for `virtualhost`, `onlinehost`, or `standbyhost`. Make sure that the IP address can be resolved from the host name.

Caution: An IP address that is enabled and accessible must be assigned to the logical host name to be specified in `virtualhost`.

4. On the executing or standby node, if HiCommand Suite products whose versions are earlier than 5.7 have been installed, stop their services.

   For details about how to stop these services, see the manual for your product version.

5. On the executing or standby node, If HiCommand Suite Common Component is running, stop the services of HiCommand Suite Common Component and all HiCommand Suite products, and then start HiRDB.

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

   The following shows an example of executing the commands:

   ```
   C:\Program Files\HiCommand\Base\bin\hcmdssrv /stop
   C:\Program Files\HiCommand\Base\bin\hcmdsdbsrv /start
   ```

6. Execute the command below to back up the database on the executing node.

   For details about the options and cautions for backing up, see section 3.6.1.

   ```
   installation-folder-for-HiCommand-Suite-Common-Component\bin\hcmdsbackups /dir target-folder-for-storing-backup-files
   ```

   The following shows an example of executing the command:

   ```
   C:\Program Files\HiCommand\Base\bin\hcmdsbackups /dir C:\db_bkup01
   ```

7. In the executing node, migrate the database to shared disk.

   Delete or empty *target-folder-for-storing-data*, and then execute the following command. When this command is executed, the setting of the port that HiRDB uses will be restored to the default (23032). If you changed the port number from the default to another number, take a note of the port number that is being used so that you can set it again later.

   ```
   installation-folder-for-HiCommand-Suite-Common-Component\bin\hcmdsdbclustersetup
   /createcluster /databasepath target-folder-for-re-creating-the-database /exportpath
   target-folder-for-storing-data /auto
   ```

   The following shows an example of executing the command:

   ```
   C:\Program Files\HiCommand\Base\bin\hcmdsdbclustersetup /createcluster /databasepath
   R:\re_creating_db /exportpath C:\storing_data /auto
   ```

   The following describes the options specified in the `hcmdsdbclustersetup` command.

   `databasepath`

   Specify the folder in which you want to re-create the database. After this option name, specify the absolute path of a folder on a shared disk. Note that the path name must not exceed 63 bytes.

The characters that can be used to specify the path are as follows. In addition to these characters, a backslash (\), colon (:), or forward slash (/) can be used as path delimiters.

A-Z, a-z, 0-9, period (.), underscore (_)

exportpath

Specify the folder in which you want to store backup data. After this option name, specify the absolute path of a folder on the local disk. Note that the path name must not exceed 63 bytes. If the folder has already been created, delete its contents. The characters that can be used to specify the path are the same as for databasepath.

auto

Specify this option to stop the HiCommand Suite product services and to start HiRDB automatically as preparation for processing the database. After the command is executed, the HiCommand Suite product services and HiRDB are stopped. Note that the services of HiCommand Suite products whose versions are earlier than 5.7 are not stopped automatically.

Caution: You must not execute multiple instances of this command concurrently. Also, you must not execute this command and the hcmdsgetlogs command concurrently.

Caution: For details about how to set the port that HiRDB uses, see section 5.4.2.

8. On the standby node, change the setting so that the database on the shared disk is to be used.

   After deleting or emptying *target-folder-for-storing-data*, execute the following command. When this command is executed, the setting of the port that HiRDB uses will be restored to the default (23032). If you changed the port number from the default to another number, take a note of the port number that is being used so that you can set it again later.

   ```
   installation-folder-for-HiCommand-Suite-Common-Component\bin\hcmdsdbclustersetup
   /createcluster /databasepath target-folder-for-re-creating-database /exportpath target-
   folder-for-storing-data /auto
   ```

   The following shows an example of executing the command:

   ```
   C:\Program Files\HiCommand\Base\bin\hcmdsdbclustersetup /createcluster /databasepath
   R:\re_creating_db /exportpath C:\storing_data /auto
   ```

   The following describes the options specified in the hcmdsdbclustersetup command.

   databasepath

   Specify the folder in which you want to re-create the database. After this option name, specify the absolute path of the same folder as *target-folder-for-re-creating-database* specified for the executing node. This folder must be located on a shared disk, and the absolute path must not exceed 63 bytes.

   The characters that can be used to specify the path are as follows. In addition to these characters, a backslash (\), colon (:), or forward slash (/) can be used as path delimiters.

   A-Z, a-z, 0-9, period (.), underscore (_)

   exportpath

Specify the folder in which you want to store backup data. After this option name, specify the absolute path of a folder on the local disk. Note that the path name must not exceed 63 bytes. If the folder has already been created, delete its contents. The characters that can be used to specify the path are the same as for `databasepath`.

`auto`

Specify this option to stop the HiCommand Suite product services and to start HiRDB automatically as preparation for processing the database. After the command is executed, the HiCommand Suite product services and HiRDB are stopped. Note that the services of HiCommand Suite products whose versions are earlier than 5.7 are not stopped automatically.

Caution: You must not execute multiple instances of this command concurrently. Also, you must not execute this command and the `hcmdsgetlogs` command concurrently.

Caution: For details about how to set the port that HiRDB uses, see section 5.4.2.

Note: This operation restarts HiCommand Suite Common Component on the standby node.

9. If HiCommand(R) Suite Common Component is running on both the executing and standby nodes, execute the following command to stop it.

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

The following shows an example of executing the command:

```
C:\Program Files\HiCommand\Base\bin\hcmdssrv /stop
```

10. In both the executing node and standby node, change the settings so that the following services start manually.
    - HBase Storage Mgmt Common Service
    - HBase Storage Mgmt Web Service
    - HiCommandServer

    In the Services panel, open the properties of each service, and then change **Automatic** to **Manual** in **Startup Type**.

11. Register (in the cluster software) the resource.

    For details on how to register a cluster resource, see section 3.3.3.3.

3.4 Verifying Installation of Device Manager Server and Common Component

After you complete the installation, you need to verify that the following services are either running or can be started manually:

- HBase Storage Mgmt Web Service
- HBase Storage Mgmt Common Service
- Device Manager Server

If all of these services can be started, the installation was successful. If one or more of these services either does not appear in the **Services** panel or cannot be started, the installation has failed.

1. Enter the following command to verify that the Common Component is installed:

   <installation folder>\Base\sample\conf\build

2. If the Common Component is installed, you will see a six-digit build number (for example, 030501) in the file.

Caution: Even if installation of HiCommand Device Manager fails, the **GO** menu command for starting HiCommand Device Manager might appear in the Dashboard of other HiCommand Suite products. To remove **GO**, a user with User Management permissions must execute the following command. When this command is executed, the HiCommand Suite Common Component services must be running.

```
installation-folder-for-HiCommand-Suite-Common-Component\bin\hcmdsintg /delete /type
DeviceManager /user user-ID /pass password
```

The following shows an example of executing the command:

```
C:\Program Files\HiCommand\Base\bin\hcmdsintg /delete /type DeviceManager /user dvmuser1
/pass sys0305
```

3.4.1 HBase Storage Mgmt Common Service or HBase Storage Mgmt Web Service Fails to Start

If the HBase Storage Management Common or Web Service fails to start, possible problems and solutions include the following:

- The port number might already be in use. If this is the case, change the port number. See section 8.2 for instructions on how to change the port.
- The amount of installed memory might be insufficient. To increase the amount of installed memory as needed, see section 3.1.2.

Caution: Even after attempting to fix the problem, if the HBase Storage Mgmt Common Service and HBase Storage Mgmt Web Service still do not start, restart the Device Manager server.

Caution: If the cause of the problem is uncertain, and the HBase Storage Mgmt Common Service or Web Service still fail to start, use the **hcmdsgetlogs** command to collect maintenance information, and then contact Customer Support. For more information on the **hcmdsgetlogs** command, see section 10.2.1.

3.4.2 HBase Storage Mgmt Common or Web Service Does Not Appear in Services

If either the HBase Storage Mgmt Common Service or the HBase Storage Mgmt Web Service is not displayed in the **Services** panel, installation of the Common Component may have failed.

Check the install log, which is in the installation directory. If you find the error, follow the instructions in the error message.

If problems still exist, uninstall Device Manager (see section 3.8.1 for instructions), reboot the system, and re-install Device Manager (see section 3.2.2 for instructions).

3.4.3 Device Manager Server Fails to Start

If the Device Manager Server fails to start, the installation may have failed. Examine the trace log at **installation-folder-for-the-Device-Manager-server\HiCommandServer\log\HDvMtrace*.log**, review the error codes, and follow the recommended actions. For more information about error codes, see *HiCommand Device Manager Error Codes* (MK-92HC016).

3.4.4 The HiCommand Device Manager Server Does Not Appear in the Services Panel

If the Device Manager Server does not appear in the **Services** panel, the installation may have failed.

The basic troubleshooting procedure in the event of installation failure or other problems is to uninstall Device Manager (see 3.8.2 for instructions), and reboot the system. Verify that all of the requirements have been met (see sections 3.1.1 and 3.1.2), then re-install Device Manager (see section 3.2 for instructions).

3.5 Starting and Stopping Device Manager Server

This section describes how to start and stop the Device Manager server. This section also describes processes that are resident during the startup of the Device Manager server and HiCommand Suite Common Component.

WARNING: If a Device Manager client (e.g., Web Client, Device Manager CLI, or Device Manager Agent) is accessing the Device Manager Server when that machine is shut down, the Device Manager client processing will terminate. Make sure that Device Manager clients are not accessing the server before shutting down a machine that is running the Device Manager Server.

3.5.1 Starting and Stopping Using Windows Functions

This section describes how to start or stop the HiCommand Device Manager server and HiCommand Suite Common Component from the **Start** menu.

- To start the HiCommand Device Manager server:

  Select **Start → Programs → HiCommand → Device Manager → Start Server**

- To Start the HiCommand Device Manager Server and Common Component:

  Select **Start → Programs → HiCommand → Device Manager → Start Server with Common Services**

  Services of other HiCommand Suite products whose versions are 5.7 or later are also started at the same time. For details, see *Caution* below.

To check status, use one of the following sequences:

- **Start → Programs → HiCommand → Device Manager → Server Status**
- **Start → Programs → HiCommand → Device Manager → Server and Common Services Status**
- To stop the Device Manager Server alone:

  Start → Programs → HiCommand → Device Manager → Stop Server

- To stop the Device Manager Server together with the Common Component:

  Start → Programs → HiCommand → Device Manager → Stop Server with Common Services

  - Services of other HiCommand Suite products whose versions are 5.7 or later are also stopped at the same time. For details, see *Caution* below.
  - If Replication Monitor 5.6 or earlier is installed, you cannot stop the Device Manager server by selecting **Stop Server with Common Services**. Stop the Device Manager server by itself, and then stop other services by selecting **Stop Server with Common Services**.

Caution: When starting or stopping the Device Manager server and HiCommand Suite Common Component concurrently:

- If you start or stop the Device Manager server and HiCommand Suite Common Component concurrently, services of other HiCommand Suite products whose versions are 5.7 or later are also started or stopped at the same time. For details about how to start or stop services of HiCommand Suite products whose versions are earlier than 5.7, see the manual for your product version.
- If the HiCommand Suite Common Component services are already running when you select **Start Server with Common Services**, the service of the Device Manager server or of the Tiered Storage Manager server will not be started. In this case, start the service of the Device Manager server or the service of the Tiered Storage Manager server individually (without HiCommand Suite Common Component).

  For details about how to check the status of the service of the Tiered Storage Manager server and how to start the service, see the *HiCommand Tiered Storage Manager Server Installation and Configuration Guide*.

3.5.2 Starting and Stopping Using Device Manager Commands

This section describes how to start or stop the HiCommand Device Manager server and HiCommand Suite Common Component by using commands.

- To start the Device Manager Server, execute the following command:

  <Device Manager Server installation folder>\suitesrvcntl /start_hdvm

  The following shows an example of executing the command:

  C:\Program Files\HiCommand\DeviceManager\suitesrvcntl /start_hdvm

This command outputs the following messages:

```
The start_hdvm request was accepted.
The Device Manager server started.
```

This indicates that HiCommand Device Manager is up and running normally.

- To stop the Device Manager Server, execute the following command:

  <Device Manager Server installation folder>\suitesrvcntl /stop_hdvm

- To check the status of the Device Manager Server, execute the following command:

  <Device Manager Server installation folder>\suitesrvcntl /status_hdvm

- To start the HiCommand Device Manager server and HiCommand Suite Common Component, execute the following command:

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

  Services of other HiCommand Suite products whose versions are 5.7 or later are also started at the same time. For details, see *Caution* below.

- To stop the HiCommand Device Manager server and HiCommand Suite Common Component, execute the following command:

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

  – Services of other HiCommand Suite products whose versions are 5.7 or later are also stopped at the same time. For details, see *Caution* below.

- If Replication Monitor 5.6 or earlier is installed, you cannot stop the Device Manager server by executing the `hcmdssrv /stop` command. Stop the Device Manager server by itself, and then stop other services by executing the `hcmdssrv /stop` command.

- To check the status of the HiCommand Device Manager server and HiCommand Suite Common Component, execute the following command:

  installation-folder-for-the-Device-Manager-server`\suitesrvcntl /status_all`

Caution: When starting or stopping the Device Manager server and HiCommand Suite Common Component concurrently:

- If you start or stop the Device Manager server and HiCommand Suite Common Component concurrently, services of other HiCommand Suite products whose versions are 5.7 or later are also started or stopped at the same time. For details about how to start or stop services of HiCommand Suite products whose versions are earlier than 5.7, see the manual for your product version.
- If the HiCommand Suite Common Component services are already running when you execute the `hcmdssrv /start` command, the service of the Device Manager server and of the Tiered Storage Manager server will not be started. In this case, start the service of the Device Manager server or the service of the Tiered Storage Manager server individually (without HiCommand Suite Common Component).

  For details on how to check the status of the Tiered Storage Manager server service and how to start the service, see the *HiCommand Tiered Storage Manager Server Installation and Configuration Guide*.

Caution: Do not execute the `hicommand`, `hcmdssrv`, or `suitesrvcntl` command while the `suitesrvcntl` command is being executed. If you do so, the `suitesrvcntl` command may not operate correctly. If you have done so inadvertently, re-execute the `suitesrvcntl` command. Also, do not execute the `suitesrvcntl` command while the `hicommand` or `hcmdssrv` command is being executed.

3.5.3 Resident Processes of the Device Manager Server and HiCommand Suite Common Component

The following table describes the resident processes of the Device Manager server and HiCommand Suite Common Component:

Table 3.10 Resident Processes of the Device Manager server and HiCommand Suite Common Component (In Windows)

Process name	Service name	Function
`HiCommandServer`	HiCommandServer	The Device Manager server
`hcmdssvctl.exe`	HBase Storage Mgmt Common Service	HiCommand Suite servlet service If the Device Manager server and other HiCommand Suite products are installed on the same machine, a process of a service other than HBase Storage Mgmt Common Service might be started by using the `hcmdssvctl.exe` name.
`httpsd.exe`	HBase Storage Mgmt Web Service	HiCommand Suite common web service Multiple processes of this might be started.
`hntr2mon.exe`	Hitachi Network Objectplaza Trace Monitor 2	HiCommand Suite common trace information collection (collects integrated trace information.)
`hntr2srv.exe`		HiCommand Suite common trace service (processes events from the Services panel.)

3.6 Operating the HiCommand Device Manager Server Database

This section describes how to perform the following operations for the Device Manager server database:

- Backing up
- Restoring the backed-up data
- Migrating the database (export and import)
- Initializing the database

The following table shows the differences in the functions between backing up and restoring verses exporting and importing.

Table 3.11 Backing Up and Restoring Verses Exporting and Importing

Item	Backing Up and Restoring	Exporting and Importing
Conditions of the HiCommand Suite Common Component version	No limitation.	HiCommand Suite Common Component version 5.5 or later must be installed on the machine used for the export source or the import destination.
Main purpose of use	To recover the current operating environment when a failure occurs in the server machine.	To migrate the server machine from the current environment to a different environment (such as a machine with a different OS).
Target data	▪ Databases for HiCommand Suite products ▪ The HiCommand Suite Common Component database	▪ Databases for HiCommand Suite products ▪ User information included in the HiCommand Suite Common Component database
Conditions for the machine used for the restore destination or the import destination	The following must be the same in the backup source machine and the restore destination machine: ▪ Types, versions, and revisions of the installed HiCommand Suite products ▪ Installation locations for each HiCommand Suite product, HiCommand Suite Common Component, each HiCommand Suite product database, and HiCommand Suite Common Component database ▪ The IP address and host name of the machine	▪ The HiCommand Suite products whose databases to be imported must be installed. ▪ The versions of the installed HiCommand Suite products must be the same as or higher than the ones on the export source machine.

The following section describe the procedure for each operation separately.

3.6.1 Backing Up the Server Database

Note: If you upgraded Device Manager from version 3.5 or earlier to version 4.0 or later, the menu options (**Start**, **Programs**, **HiCommand**, **Device Manager**, and **Back Up Database**) are deleted.

Caution: To back up the Device Manager database, a folder for storing the backup file is required. The capacity of this folder must be at least the total size of the following two folders:

- The folder storing the Device Manager database
- The folder storing the HiCommand Suite Common Component database

This capacity is a guideline value applied when only the Device Manager database is installed. If HiCommand Suite products other than Device Manager are also installed, take the capacities of those databases into account as well.

To back up the database:

1. If HiCommand Suite products whose versions are earlier than 5.7 have been installed, stop their services.

   For details about how to stop these services, see the manual for your product version.

2. If HiCommand Suite products whose versions are 5.7 or later have not been installed, stop HiCommand Suite Common Component, and then start HiRDB. Execute the following commands from the command prompt to start HiRDB:

   <common component installation folder>\bin\hcmdssrv /stop

   <common component installation folder>\bin\hcmdsdbsrv /start

   The following shows an example of executing the command:

   C:\Program Files\HiCommand\Base\bin\hcmdssrv /stop

   C:\Program Files\HiCommand\Base\bin\hcmdsdbsrv /start

3. Execute the **hcmdsbackups** command from the command prompt:

   <common component installation folder>\bin\hcmdsbackups.bat

   The command format is as follows. The `auto` option can be specified only when HiCommand Suite products whose versions are 5.7 or later have been installed:

   `hcmdsbackups /dir` *target-folder-for-storing-backup-files* `/auto`

   The following shows an example of executing the command:

   C:\Program Files\HiCommand\Base\bin\hcmdsbackups /dir C:\db_bkup01 /auto

   The specifiable option is as follows:

   dir

   Specify the absolute path of the folder, on the local disk, that stores the backup files of the HiCommand(R) Device Manager server database.

   auto

Specify this option to stop the HiCommand Suite product services and to start HiRDB automatically as preparation for processing the database. After the command is executed, the HiCommand Suite product services and HiRDB are started. Note that the services of HiCommand Suite products whose versions are earlier than 5.7 are not started and stopped automatically.

Note: When you execute the **hcmdsbackups** command, a folder named **database** will be created in the target folder for storing backup files, and the database backup file will be stored with the name **backup.hdb**.

4. If you have stopped HiCommand Suite Common Component in step 2, execute the following command to restart HiCommand Suite Common Component:

   <common component installation folder>\bin\hcmdssrv /start

   The following shows an example of executing the command:

   C:\Program Files\HiCommand\Base\bin\hcmdssrv /start

5. If HiCommand Suite products whose versions are earlier than 5.7 have been installed, restart their services as required.

   For details about how to start these services, see the manual for your product version.

3.6.2 Restoring the Server Database

WARNING: Before restoring the database, be sure to confirm that the following are the same in the backup source Device Manager server and the restore destination Device Manager server. If the following are not the same, the database cannot be restored.

- Types, versions, and revisions of the installed HiCommand Suite products
- Installation location for each HiCommand Suite product, HiCommand Suite Common Component, each HiCommand Suite product database, and HiCommand Suite Common Component database
- The IP address and host name of the machines

Caution: When the HiCommand Device Manager server is upgraded from version 3.5 or earlier to 4.0 or later, the menu options (**Start**, **Programs**, **HiCommand**, **Device Manager**, and **Restore Database**) are deleted

To restore a database:

1. If HiCommand Suite products whose versions are earlier than 5.7 have been installed, stop their services.

   For details about how to stop these services, see the manual for your product version.

2. Execute the **hcmdsdb** command from the command prompt. The default destination for this command is as follows:

   `<Common Component installation folder>\bin\hcmdsdb.bat`

   The command format is as follows:

   `hcmdsdb /restore` ***backup-file*** `/type` ***name-of-HiCommand-Suite-product-to-be-restored*** `/auto`

The following shows an example of executing the command:

C:\Program Files\HiCommand\Base\bin\hcmdsdb /restore C:\db_bkup01\database\backup.hdb /type DeviceManager /auto

The specifiable options are as follows:

restore

Specify the absolute path of the Device Manager Server database backup file (backup.hdb).

type

Specify the name of the HiCommand Suite product to be restored. Specify **DeviceManager** to restore the Device Manager database only, or specify **ALL** (all capital letters) if you want to restore all HiCommand Suite product databases at once. Specify **ALL** if you want to restore the databases when you are uninstalling and then reinstalling all the HiCommand Suite products.

auto

Specify this option to stop the HiCommand Suite product services and HiRDB automatically as preparation for processing the database. After the command is executed, the HiCommand Suite product services and HiRDB are stopped. Note that the services of HiCommand Suite products whose versions are earlier than 5.7 are not stopped automatically.

Note: If you specify **DeviceManager** for the type option, specify **true** for the **server.base.initialsynchro** property in the server.properties file. See section 8.2.23 for more information.

Note: This sample command used the C:\TMP directory as the backup location. Use the backup location that you previously specified.

3. Restart the HiCommand Suite product services and HiCommand Suite Common Component as follows:

   Select **Start → Programs → HiCommand → Device Manager → Start Server with Common Services**

   Caution: The services of HiCommand Suite products whose versions are earlier than 5.7 are not started. If such HiCommand Suite products have been installed, restart their services manually as required. For details about how to start these services, see the manual for your product version.

4. Change the value of the `server.base.initialsynchro` property in the `server.properties` file back to `false`.

3.6.3 Migrating the Server Database

If HiCommand Suite products are used for an extended period of time, you may need a higher performance machine in order to accommodate product version upgrades and the increased number of objects to be managed. If this occurs, database migration will be one important component of the machine replacement process. In HiCommand Suite products, you can migrate the database by using the `hcmdsdbtrans` command. The `hcmdsdbtrans` command migrates all information stored in the database of each HiCommand Suite product as well as user information managed by the HiCommand Suite Common Component.

You can use the `hcmdsdbtrans` command to migrate the Device Manager database to a machine that has a different environment than the currently operating server machine, as shown in the following cases:

- Migration to a different platform machine
- Migration to a machine on which the installation locations for HiCommand Suite products are different from the ones on the migration source
- Migration to a machine on which the versions of HiCommand Suite products are newer than the ones on the migration source

3.6.3.1 Notes When Migrating the Database

The following are notes for the types, versions, and user information of the HiCommand Suite products on the migration source and migration destination servers.

Notes for types and versions of the HiCommand Suite products on the migration source and migration destination servers:

- The database of a HiCommand Suite product that is not installed on the migration destination server cannot be migrated. Install all necessary HiCommand Suite products on the migration destination server.
- If any of the versions of the HiCommand Suite products installed on the migration destination server is older than the ones on the migration source server, the database cannot be migrated. On the migration destination server, install the HiCommand Suite products whose versions are the same as or higher than the ones on the migration source server.
- The database of Replication Monitor version 4.2 or earlier cannot be migrated. If you need to migrate the database of Replication Monitor version 4.2 or earlier, upgrade Replication Monitor to version 5.0 or later on both the migration source and destination servers beforehand.
- The following limitations apply when you migrate the database in Tuning Manager.
- The database can be migrated when the database configuration (Small or Medium) is the same on both the migration source and the destination server, or when the database configuration on the migration destination server becomes much larger than that on the source server.
- In the database configuration on the migration source server, if the number of the management target resources exceeds 70% of the management limit, the database cannot be migrated to a database that has the same configuration.

Notes for user information:

- If there is user information on the migration destination server, this user information will be replaced with the user information from the migration source server. Therefore, do not perform a migration to the machine on which user information for the HiCommand suite products already exists.

- If the databases of several HiCommand Suite products installed on a management server are migrated in multiple operations, the user information is replaced with new information at each operation, and eventually only the user information for the products migrated during the last operation will remain. When you perform migration for multiple products, be sure to migrate the databases in one operation so that user information for every products can be migrated.
- You cannot perform migration to integrate the HiCommand Suite products that were running on multiple management servers on to one management server because user information will be overwritten with each successive migration.

3.6.3.2 Procedure for Migrating Databases

To migrate databases:

1. Install on the migration destination server, the HiCommand Suite products whose databases will be migrated.
2. Export the databases at the migration source server by using the `hcmdsdbtrans` command.
3. Transfer the archive file from the migration source server to the migration destination server.
4. Import the database at the migration destination server by using the `hcmdsdbtrans` command.

The following sections describe the details of each procedure. To perform migration between heterogeneous platforms, also see section 4.6.3.

3.6.3.3 Installing the HiCommand Suite Products on the Migration Destination Server

Install, on the migration destination server, the HiCommand Suite products whose databases will be migrated. The version of each HiCommand Suite product installed on the migration destination server must be the same as or higher than the one on the migration source server.

3.6.3.4 Exporting the Database at the Migration Source Server

To export the database of Device Manager, a folder for temporarily storing the information of the database, and a folder for storing the archive file are required. Each of these folders requires the as much capacity as the total size of the following two folders:

- The folder storing the Device Manager database
- The folder storing the HiCommand Suite Common Component database (excluding the `SYS` folder and the folders beneath it)

This capacity is a guideline value applied when only the Device Manager database is installed. If HiCommand Suite products other than Device Manager are also installed, take the capacities of those databases into account as well.

Caution: If the total capacity of the database exceeds 2 GB, an attempt to create the archive file fails when the database is exported. In this case, instead of using the archive file, transfer to the migration destination the database information collected when exporting the database.

To export the database at the migration source server:

1. If HiCommand Suite products whose versions are earlier than 5.7 have been installed, stop their services.

   For details about how to stop these services, see the manual for your product version.

2. If HiCommand Suite products whose versions are 5.7 or later have not been installed, stop HiCommand Suite Common Component, and then start HiRDB.

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

   The following shows an example of executing the commands:

   ```
   C:\Program Files\HiCommand\Base\bin\hcmdssrv /stop
   C:\Program Files\HiCommand\Base\bin\hcmdsdbsrv /start
   ```

3. From the command prompt, execute the `hcmdsdbtrans` command.

   The default installation location of the `hcmdsdbtrans` command is as follows:

   ```
   installation-folder-for-HiCommand-Suite-Common-Component\bin\hcmdsdbtrans
   ```

   The command format is as follows. The `auto` option can be specified only when HiCommand Suite products whose versions are 5.7 or later have been installed:

   ```
   hcmdsdbtrans /export /workpath working-folder /file archive-file /auto
   ```

   The following shows an example of executing the command:

   ```
   C:\Program Files\HiCommand\Base\bin\hcmdsdbtrans /export /workpath D:\trans_work /file
   D:\trans_file\db_arc /auto
   ```

   In the `hcmdsdbtrans` command, you can specify the following options:

   `workpath`

   Specify the absolute path to the folder where you wish to temporarily store database information. Specify a folder on your local disk.

   Caution: Specify an empty folder for the workpath option. If you specify a folder other than an empty folder, export processing will be cancelled. If this occurs, specify an empty folder and execute the `hcmdsdbtrans` command again.

   `file`

   Specify the absolute path to the archive file of the database to be exported.

   `auto`

   Specify this option to stop the HiCommand Suite product services and to start HiRDB automatically as preparation for processing the database. After the command is executed, the HiCommand Suite product services and HiRDB are started. Note that the services of HiCommand Suite products whose versions are earlier than 5.7 are not started and stopped automatically.

4. Transfer the exported file to the migration destination server.

   If the archive file cannot be created, transfer all the files stored in the folder specified by the `workpath` option. In that case, do not change the file structure in the folder specified by the `workpath` option.

3.6.3.5 Importing the Database at the Migration Destination Server

Caution: If the OS of the migration destination server is Solaris or Linux, follow the procedure in section 4.6.3.5.

To import the database at the migration destination server:

1. If HiCommand Suite products whose versions are earlier than 5.7 have been installed, stop their services.

   For details about how to stop these services, see the manual for your product version.

2. From the command prompt, execute the `hcmdsdbtrans` command.

   The default installation location of the `hcmdsdbtrans` command is as follows:

   ```
   installation-folder-for-HiCommand-Suite-Common-Component\bin\hcmdsdbtrans
   ```

   The format of the command is as follows:

   ```
   hcmdsdbtrans /import /workpath working-folder [/file archive-file] /type {ALL |
   HiCommand-Suite-products-whose-databases-will-be-migrated} /auto
   ```

   The following shows an example of executing the command:

   ```
   C:\Program Files\HiCommand\Base\bin\hcmdsdbtrans /import /workpath D:\trans_work /file
   D:\trans_file\db_arc /type ALL /auto
   ```

   In the `hcmdsdbtrans` command, you can specify the following options:

   `workpath`

   When using an archive file during the import:

   Specify the absolute path to the folder used to extract the archive file. Specify a folder on your local disk. If you use an archive file, the `file` option must be specified.

   Caution: Specify an empty folder for the `workpath` option. If you specify a folder other than an empty folder, import processing will be cancelled. If this occurs, specify an empty folder, and then execute the `hcmdsdbtrans` command again.

   When not using the archive file during the import:

   Specify the folder that stores the database information transferred from the migration source server. Do not change the file structure in the transferred folder. Also, do not specify the `file` option.

   `file`

   Specify the absolute path to the archive file of the databases transferred from the migration source server. If the database information transferred from the migration source server is stored in the folder specified by `workpath`, you do not need to specify this option.

   `type`

   Specify the names of the HiCommand Suite products whose databases will be migrated. Only the databases of the specified products are migrated.

   When you migrate the Device Manager database, specify `DeviceManager`. For details on the names to be specified when you migrate databases of other products, see the relevant manual for each product. To specify multiple product names, use a comma as the delimiter between the names.

To migrate the databases of all the installed HiCommand Suite products at a time, specify `ALL`. The databases of the HiCommand Suite products installed on the migration destination server are automatically selected and migrated.

You can use the `type` option to migrate databases only when the databases of all the specified products exist in the folder specified in the archive file or the `workpath` option, and all the specified products are installed on the migration destination server. If any of the products do not meet the conditions above, migration will not be performed.

`auto`

Specify this option to stop the HiCommand Suite product services and to start HiRDB automatically as preparation for processing the database. After the command is executed, the HiCommand Suite product services and HiRDB are stopped. Note that the services of HiCommand Suite products whose versions are earlier than 5.7 are not stopped automatically.

Caution: If Replication Monitor version 4.2 or earlier is installed on the migration source machine, you cannot migrate the database. Therefore, upgrade Replication Monitor on the migration source and migration destination machines to version 5.0 or later, and then perform migration. If Replication Monitor cannot be upgraded to version 5.0 or later, or the Replication Monitor database does not have to be migrated, use the `type` option and specify all products other than Replication Monitor when you execute the command.

3. Synchronize the repository information with the imported Device Manager database information.

   Specify `true` for the `server.base.initialsynchro` property in the `server.properties` file.

   Since, other than user information, the `hcmdsdbtrans` command does not migrate the HiCommand Suite Common Component repository, you need to synchronize the repository information with the database information of the imported Device Manager.

   For information on the `server.base.initialsynchro` property, see section 8.2.22.

4. Restart the HiCommand Suite product services and HiCommand Suite Common Component as follows:

   Select **Start, Programs, HiCommand, Device Manager, Start Server with Common Services**.

   Caution: The services of HiCommand Suite products, whose versions are earlier than 5.7, are not started. If such HiCommand Suite products have been installed, restart their services manually as required. For details about how to start these services, see the manual for your product version.

5. Change the value of the `server.base.initialsynchro` property in the `server.properties` file back to `false`.

3.6.4 Initializing a HiCommand Device Manager Server Database

To initialize the database:

1. Stop the Device Manager Server:

   Select **Start → Programs → HiCommand → Device Manager → Stop Server**

2. Enter the following command from the command prompt to make sure that the HiCommand Suite Common Component service is running:

   <common component installation folder>\bin\hcmdssrv /status

   The following shows an example of executing the command:

   C:\Program Files\HiCommand\Base\bin\hcmdssrv /status

   If the following messages appear, the services are running:

   KAPM06440-I The HiRDB service has already started.

   KAPM05007-I Already started service. service-name=HBase Storage Mgmt Web Service

   KAPM05007-I Already started service. service-name=HBase Storage Mgmt Common Service

3. If the HiCommand Suite Common Component service is not running, execute the following command from the command prompt:

   <common component installation folder>\bin\hcmdssrv /start /server HBase

   The following shows an example of executing the command:

   C:\Program Files\HiCommand\Base\bin\hcmdssrv /start /server HBase

4. From the command prompt, execute the **database** command.

   - The default installation location is as follows:
     <server installation folder>\database.bat
   - The following shows an example of executing the command:
     C:\Program Files\HiCommand\DeviceManager\database initialize
   - The command format is as follows: **database initialize**

5. Specify **true** for the **server.base.initialsynchro** property in the server.properties file. For details, see section 8.2.23.

6. Restart the Device Manager Server:

   Select **Start → Programs → HiCommand → Device Manager → Start** Server

7. Change the value of the `server.base.initialsynchro` property in the `server.properties` file back to `false`.

3.7 Converting a Device Manager Server Database

To use a database that has been used before the upgrade when upgrading the Device Manager server version 2.3 through 3.5 to 4.0 or later, you must first convert it to HiRDB.

Caution: The conversion function is available only when the upgrade is from the Device Manager server version 2.3 through 3.5 to Device Manager server version 4.0 or later.

3.7.1 About Converting from InterBase to HiRDB

If you have a Device Manager database for versions 2.3 through 3.5, it is based on InterBase. Databases for versions 4.0 and higher are based on HiRDB, so if you are upgrading to that level you will need to convert the database.

Caution: InterBase, InterServer, and HiRDB must all be running when you convert the database.

Note: Database conversion can be a lengthy process. For example, if 8,000 LDEVs and 16,000 paths have been managed, the database conversion will take about 5 minutes in an environment that has a 1.5 GHz CPU and 1 GB of memory. See the Release Notes for more information.

3.7.2 Converting Manually to HiRDB

You can either convert the database automatically when you install the Device Manager Server, or manually after the installation using the following procedure.

To manually convert a database:

1. If HiCommand Suite products whose versions are earlier than 5.7 have been installed, stop their services.

   For details about how to stop these services, see the manual for your product version.

2. Stop the HiCommand Suite product services and HiCommand Suite Common Component as follows:

   Select **Start → Programs → HiCommand → Device Manager → Stop Server with Common Services**.

3. Access the **Services** panel, and verify that the following services are running:
   - InterBase Server
   - InterServer

4. Execute the following command from the command prompt to start HiRDB:

   <common component installation folder>\bin\hcmdsdbsrv /start

   The following shows an example of executing the command:

   C:\Program Files\HiCommand\Base\bin\hcmdsdbsrv /start

5. From the command prompt, execute the **migrateFmIB** command.

   The default installation folder for the migrateFmIB command is as follows:

   <server installation folder>\migrateFmIB.bat

   The command format is as follows:

   migrateFmIB [-d InterBase-GDB-file-name | InterBase-GBK-file-name] [-u InterBase-user-id] [-p InterBase-password]

   The following shows an example of executing the command:

   C:\Program Files\HiCommand\DeviceManager\migrateFmIB -d C:\IBdata\ibase.gdb -u ibuser1 -p sys0305

   The following options can be specified for the migrateFmIB command:

   -d: Specify an absolute path for the name of the GDB or GBK file for InterBase. If this option is not specified, the following file is used
   <Device Manager Server installation folder>\HiCommandServer\database\interbase\HiCommand.gdb

   -u: Specify the InterBase user ID. The default InterBase user ID is assumed if the -u option is not specified.

   -p: Specify the InterBase password. The password of the default InterBase user ID is used if the -p option is not specified.

6. Specify **true** for the **server.base.initialsynchro** property in the server.properties file. See section 8.2.23 for more information.

7. Restart the HiCommand Suite product services and HiCommand Suite Common Component as follows:

   Select **Start → Programs → HiCommand → Device Manager → Start Server with Common Services**

   Caution: The services of HiCommand Suite products whose versions are earlier than 5.7 are not started. If such HiCommand Suite products have been installed, restart their services manually as required. For details about how to start these services, see the manual for your product version.

8. In the server.properties file, change the **server.base.initialsynchro** property back to false.

Note: When the **migrateFmIB** command is used, one of the following return codes is returned as a result:

Table 3.12 Return Codes for migrateFmIB Command

Return code	Description
0	The command terminated normally.
1	InterBase is not running.
2	HiRDB is not running.
3	An InterBase authentication error occurred.
4	A HiRDB authentication error occurred.

Return code	Description
5 to 19	(Reserved)
20	The HiCommand Device Manager Server is running.
21 to 29	(Reserved)
30	The database file to be converted does not exist.
31 to 39	(Reserved)
40	An attempt to change the database definition has failed.
41 to 49	(Reserved)
50	An attempt to convert the database has failed.
51 to 253	(Reserved)
254	An error occurred during conversion processing.
255	Internal error

3.8 Uninstalling the HiCommand Device Manager Server and Related Products

Caution: If an error occurs during uninstallation and then uninstallation is stopped, execute the `hcmdsgetlogs` command to collect the maintenance information, and then contact maintenance personnel.

3.8.1 Uninstalling the HiCommand Device Manager Server in a Standard Environment

WARNING: Unless you are experiencing problems and need to redo a complete installation, you should not uninstall Device Manager. If you need to uninstall the Device Manager Server, make sure to first back up your configuration (see section 3.6.1 for instructions).

WARNING: The Device Manager provides user management functions for the HBase Storage Mgmt Common Service. When you are using the HBase Storage Mgmt Common Service function, and Device Manager Server and Tuning Manager are installed on the same machine, the HBase Storage Mgmt Common Service function is deleted when Device Manager is uninstalled.

WARNING: Close the Services panel before you uninstall the Device Manager server.

Notes:

- Files that were added to the installation folder after installation might not be deleted when you uninstall. If this occurs, delete the files manually.
- If services and files remain after uninstallation, If this type of problem occurs, delete the **<install directory>\UninstallerData** folder, re-install Device Manager, and then uninstall again.

- If no other program is using the Common Component, it will be uninstalled during the uninstallation of Device Manager. If another program is using the Common Component, it will remain installed. You cannot uninstall the Common Component by itself.
- When you uninstall HiCommand Device Manager, *installation-folder-for-the-Device-Manager-server*, together with the files and subfolders it contains, will be deleted. However, the parent folder of the installation folder will remain after the uninstallation. If the directory is not necessary, you can delete it manually. Note that certain files that remain may be in use by another HiCommand product.
- Even though InstallAnywhere indicates that it uninstalls all components that were installed by that program, only the Device Manager Server will actually be uninstalled.
- The Uninstaller is executed in the same language display as the language that was selected during the original Device Manager installation. If the original installation was performed in one language, but the system local parameters were later modified to another language and the uninstallation processing is performed in the second language, then the characters on the Uninstaller screen will be garbled.
- If CIM/WBEM functions are being used, you must release the registration of the SLP service from the Windows service before performing the uninstallation. For details about releasing an SLP service registration, see the *HiCommand Device Manager CIM/WBEM User's Guide*.
- ***Caution:*** Open the property of the following services from the Services panel to make sure that **Startup Type** is not set to **Disabled**. If **Startup Type** is set to **Disabled**, change the setting to **Automatic** or **Manual**.
  - HBase Storage Mgmt Common Service
  - HBase Storage Mgmt Web Service
  - HiRDB/EmbeddedEdition _HD0
  - HiCommandServer
- ***Caution:*** Check whether the following programs are installed. If they are installed, take action by following the explanation below:
  - A program that monitors security

    Stop the program that monitors security, or change its settings so that Device Manager can be uninstalled normally.
  - A program that detects viruses

    We recommend that you stop programs that detect viruses, and then uninstall Device Manager.

    If a program that detects viruses is running during uninstallation of Device Manager, the speed of uninstallation might be reduced, uninstallation might fail, or uninstallation might finish in an incorrect state.
  - A program that monitors processes

    Stop the program that monitors processes, or change its settings so that the program does not monitor the services or processes of the HiCommand Device Manager server and the HiCommand Suite Common Component.

    If a program that monitors processes starts or stops the above services or processes during uninstallation of Device Manager, uninstallation might fail.

- ***Caution:*** Any user who is not a member of the Administrators group can uninstall the HiCommand Device Manager server. If this is not desirable, change the security settings in the following file to prevent uninstallation by other users:

  `<device manager server installation folder>\UninstallerData\Uninstall_HiCommand.exe`

- ***Caution:*** Sometimes, even when a message has notified you that uninstallation was successful, uninstallation has actually failed. For example, the `HiCommandServer` service and some installation files may remain. If uninstallation has failed, manually delete the *`installation-folder-for-the-Device-Manager-server`*`\UninstallerData` folder, re-install the HiCommand Device Manager server program, and then perform uninstallation again.

- ***Caution:*** When you uninstall HiCommand Device Manager from a computer on which another HiCommand Suite product is installed, the **GO** menu command for launching Device Manager remains on the dashboard of that program. To remove **GO**, a user with User Management permissions must execute the following command. When this command is executed, the HiCommand Suite Common Component services must be running.

```
installation-folder-for-HiCommand-Suite-Common-Component\bin\hcmdsintg /delete /type
DeviceManager /user user-ID /pass password
```

The following shows an example of executing the command:

```
C:\Program Files\HiCommand\Base\bin\hcmdsintg /delete /type DeviceManager /user dvmuser1
/pass sys0305
```

To uninstall the HiCommand Device Manager server:

1. Access the **Uninstall HiCommand Device Manager** panel using one of the following:
   - The Windows Add/Remove Programs utility
   - Select **Start → Programs → HiCommand → Device Manager → Uninstall Device Manager**
2. When the HiCommand Suite Common Component services are running, the Stop HiCommand Suite Product Services panel is displayed. Select **OK** to continue.

   If the uninstaller cannot stop all the services of HiCommand Suite Common Component and the HiCommand Suite products, the **Stop services error** panel is displayed. If this panel is displayed, select the **OK** button to close it, and then try again to stop the services. If the uninstaller still fails to stop the services, cancel the installation, manually stop the services of HiCommand Suite Common Component and the HiCommand Suite products, and then perform the uninstallation again.

   Caution: The services of HiCommand Suite products whose versions are earlier than 5.7 are not stopped. Stop the services manually, and then continue the uninstallation. For details about how to stop these services, see the manual for your product version.
3. In a non-cluster environment, the Set Services to Start After Uninstallation panel is displayed. If you want to start the services of HiCommand Suite Common Component and related HiCommand Suite products after uninstallation is complete, select **Yes**. If you do not want to start these services after uninstallation is complete, select **No**. Select **Next** to continue.

Caution: Even if **Yes** is selected, services of HiCommand Suite products whose versions are earlier than 5.7 will not start. After uninstallation finishes, manually start services of HiCommand Suite products as required. For details about how to start these services, see the manual for your product version.

4. After the message `All items were successfully uninstalled.` is displayed, select **Done** to exit. If Windows OS indicates that certain files were not uninstalled, you must manually delete them.

WARNING: If you uninstall HiCommand Suite Common Component, sometimes the Warning Panel shown in Figure 3.12 may display. In this case, you need to restart the system after the uninstallation. If you install a HiCommand Suite product continuously without restarting the system after the uninstallation, when the system restarts after the installation, the files required for the HiCommand Suite product operations will be deleted.

Caution: If the following message is displayed, release the SLP service from the Windows services manually. If the folders and files that are related to the SLP remain, delete them manually as necessary. For information on how to release the SLP service, see section 11.5.1.1.

```
An attempt to release the SLP service has failed. After uninstallation, release
the SLP service manually.
Uninstallation continues
```

Figure 3.12 Warning Panel

3.8.2 Uninstalling the Device Manager Server in a Cluster Environment

This section describes uninstallation of the Device Manager server when a cluster environment has been set up using Microsoft Cluster Service.

Caution: If the service is not online on the executing node, first place it online, and then perform the uninstall procedure.

To uninstall the HiCommand Device Manager Server in a Microsoft Cluster Service environment, perform the following procedure:

1. Open the cluster administrator:

   Select **Start → Settings → Control Panel → Administrative Tools → Cluster Administrator**.

2. If the standby node is the owner of the group in which the HiCommand Device Manager service has been registered, switch to the executing node.

   In Cluster Administrator, right-click the group in which the Device Manager service has been registered, and then select **Move Group**.

3. Place the following services offline:
   - HiCommand Server
   - HBase Storage Mgmt Web Service
   - HBase Storage Mgmt Common Service

   The above services are represented by the resource names registered in section 3.3.3.3.
4. Stop the HiCommand Suite product services and HiCommand Suite Common Component as follows:

   Select **Start**, **Programs**, **HiCommand**, **Device Manager**, and then **Stop Server with Common Services**.

   Caution: The services of HiCommand Suite products whose versions are earlier than 5.7 are not stopped. Stop the services manually, and then go to the next step. For details about how to stop these services, see the manual for your product version.
5. Place the **HiRDB** service offline.

   The above service is represented by the resource name registered in section 3.3.3.3.
6. If the following resources are not in use by another application, delete them:
   - HBase Storage Mgmt Common Service
   - HBase Storage Mgmt Web Service
   - HiCommandServer
   - HiRDB

   The above services are represented by the resource names registered in section 3.3.3.3.
7. Perform the following operation on the services listed in step 6 that you do not want to delete.

   In the Cluster Administrator, right-click each service, select **Properties**, select the **Advanced** tab, select **Do not restart**, and then select **OK**.
8. On the executing node, uninstall the Device Manager Server by selecting **Start**, **Programs**, **HiCommand**, **Device Manager**, and then **Uninstall Device Manager**.
9. On the executing node, delete any files and folders that are no longer necessary, including those created during the installation in the cluster environment.
10. Switch, to the standby node, the group in the HiCommand Device Manager service has been registered.

    In the Cluster Administrator, right-click the group to which the HiCommand Device Manager service has been registered, and then choose **Move Group**.
11. On the standby node, uninstall the Device Manager Server by selecting **Start**, **Programs**, **HiCommand**, **Device Manager**, and then **Uninstall Device Manager**.
12. On the standby node, delete any files and folders that are no longer necessary, including those created during the installation in the cluster environment.
13. If the following resources are not being used by another application, first place the corresponding resource offline, and then delete it:
    - IP address

- Shared disk

14. If the group where the HiCommand Device Manager resources are registered is no longer necessary, delete that as well.
15. Return the service that was set to **Do not restart** in step 7 to **Restart**.

3.8.3 Uninstalling InterBase Server and Client

WARNING: Do not uninstall InterBase Server if it is being used by another product, on the same machine, including another HiCommand Suite product that has not yet been upgraded to version 4.0 or higher.

To uninstall InterBase Server:

1. Before you uninstall the InterBase Server, stop the service by accessing the Services Panel.

   Select **Start → Programs → HiCommand → Device Manager → Stop HiCommand**.

   WARNING: Do not use the **Services** panel to stop the Device Manager Server.
2. Access the **Services** Panel.
3. Select **InterBase Guardian → Stop**.
4. The **Microsoft Management Console** displays. Select **OK** to continue.

   Note: If the InterBase Guardian service cannot be stopped, an error message appears (see Figure 3.13). Select **OK** to continue.
5. Use the Windows **Add/Remove Programs** utility to remove the entries for the InterBase software (the exact details are determined by your existing configuration).
6. The InterBase uninstallation program may leave a directory structure on your system. The default location is c:\Program Files\Borland\InterBase. You can delete the directories manually if they are no longer necessary.
7. After the uninstallation, select the **View Log** button on the uninstaller to make sure that no errors occurred.
8. Reboot the system. If you are also going to uninstall the InterClient software, the reboot can wait until after InterClient is uninstalled.

Notes:

If the uninstallation fails, retry the operation. If it fails again, restart the machine, re-install the InterBase Server, and then uninstall the InterBase Server again.

Figure 3.13 Microsoft Management Console Error Message 997

3.8.4 Uninstalling InterClient

WARNING: Do not uninstall InterClient if it is being used by another product, including another HiCommand Suite product that has not yet been upgraded to version 4.0 or higher.

To uninstall the InterClient software:

1. Before you uninstall InterClient, stop the InterServer service by accessing the Services Panel., then select **Interserver→ Stop**.
2. Choose **Start**, **Programs**, **InterBase InterClient**, and then **InterServer Configuration Utility**.
3. Choose the **Advanced** tab, and then click the **Remove** button. A message asking whether you want to delete the service appears.
4. Click the **OK** button.
5. From the `services` file (*`system-folder`*`\system32\drivers\etc\services`), delete the following line:

```
interserver      3060/tcp            # InterBase InterServer
```

6. Use the Windows **Add/Remove Programs** utility to remove the InterClient software (the exact details are determined by your existing configuration).
7. The InterClient uninstallation program may leave a directory structure on your system. The default location is **c:\Program Files\Borland\InterClient**. You can delete the directories manually if they are no longer necessary.

Notes:

- If the InterClient software is uninstalled, you must restart before you can re-install.
- If the uninstallation fails, retry the operation.

Chapter 4 Solaris and Linux Systems Installation

This chapter contains instructions for installing the Device Manager Server software on a single central server system. For instructions on installing and using the graphical Web Client software, see the *HiCommand Device Manager Web Client User's Guide*.

This chapter discusses the following topics:

- Installation Prerequisites for Solaris and Linux Systems (see sections 4.1.1 and 4.1.2)
- Installing to a Solaris or Linux Environment (see section 4.2)
- Installing the Device Manager Server in a Cluster Server Environment (see section 4.3)
- Verifying HiCommand Device Manager Installation (see section 4.4)
- Starting and Stopping Device Manager Server (see section 4.5)
- Operating the HiCommand Device Manager Server Database (see section 4.6)
- Converting a Device Manager Server Database (see section 4.7)
- Uninstalling the HiCommand Device Manager Server and Related Products (see section 4.8)
- Setting Kernel Parameters on Solaris (see section 4.10)
- Setting Kernel Parameters and Shell Restrictions on Linux (see section 4.11)

4.1 Installation Prerequisites for Solaris and Linux Systems

Note: Always read the Release Notes before installing Device Manager, and make sure that you have the minimum required microcode on the subsystem.

4.1.1 Solaris and Linux System and Media Requirements

The following are the system requirements for Sun Solaris and Linux systems:

- Solaris workstation: SPARC
- Operating system:
  - The following Solaris versions are supported:

Table 4.1 The OSs on Which the HiCommand Device Manager Server Can Run (Solaris)

Abbreviated Name	Full Name	Cluster environment support
Solaris 8 or Solaris#1	Sun Microsystems Solaris 8 (for SPARC)	--
Solaris 9 or Solaris	Sun Microsystems Solaris 9 (for SPARC)	Y
Solaris 10 or Solaris#2#3	Sun Microsystems Solaris 10 (for SPARC)	--

Legend

Y: Operation in a cluster environment is supported.

--: Operation in a cluster environment is not supported.

For details about the supported cluster software and how to set up cluster environment, see section 4.3.

#1 The following patches are required:

Patch Cluster, 108652-59, 111293-04, 108714-07, 108827-30

#2 Patch 120664-01 is required.

#3 The HiCommand Device Manager server runs in the usual global environment (global zone) only. If a non-global zone has been created, install the HiCommand Device Manager server in the global zone.

  - The following Linux versions are supported:

Table 4.2 The OSs on Which the HiCommand Device Manager Server Can Run (Linux)

Abbreviated Name	Full Name	Cluster environment support
Linux x86#	Red Hat Enterprise Linux AS 4.0 Update1	--
	Red Hat Enterprise Linux ES 4.0 Update1	--

Legend

--: Operation in a cluster environment is not supported.

The `compat-libstdc++-33-3.2.3-47.3` library must be installed. Make sure that the `compat-libstdc++-33-3.2.3-47.3` library is installed before you install the Device Manager server.

When using the Device Manager server in a time zone of the United States or Canada, set the OS of the machine on which the Device Manager server will be installed so that the OS is compatible with the new Daylight Saving Time (DST) rules. If the OS is not compatible with the new DST rules, the Device Manager server will also not be compatible with the new rules.

- Machine specifications:
  - Recommended specifications for Solaris machines are as follows:

Table 4.3 Recommended Specifications for the Machine Where the HiCommand Device Manager Server Is to Be Installed (Solaris)

Item	Minimum	Recommended
Processor	1.0 GHz	1.2 GHz or faster
Memory	1 GB	At least 2 GB#
Disk space	4 GB	At least 5 GB

  - Recommended specifications for Linux machines are as follows:

Table 4.4 Recommended Specifications for the Machine Where the HiCommand Device Manager Server Is to Be Installed (Linux)

Item	Minimum	Recommended
Processor	1.0 GHz	2.0 GHz or faster
Memory	1 GB	At least 2 GB#
Disk space	4 GB	At least 5 GB

When the HiCommand Device Manager server is used concurrently with other software products, the memory requirements of all of the software products must be taken into account.

- Installation destination and its disk space requirements: The following table describes the installation paths and the required disk space for installation.

Table 4.5 Installation Path and Required Disk Space

Item	Installation Path	Required Disk Space (GB)
Installation destination for the HiCommand Device Manager server	`/opt/HiCommand`	1.30
Installation destination for	`/opt/HiCommand/Base`	

Item	Installation Path	Required Disk Space (GB)
HiCommand Suite Common Component	/var/opt/HiCommand/Base	0.01
Storage destination of the database for the HiCommand Device Manager server	/opt/HiCommand/HiCommandServer/database	0.10
Storage destination of the database for HiCommand Suite Common Component#1	/var/opt/HiCommand/Base/database	1.20
A temporary directory#2	/var/tmp	1.30

#1 This is not required if HiCommand Suite Common Component version 4.0 or later has already been installed.

#2 This is temporarily required during installation. However, this will be unnecessary after finishing installation.

- Prerequisite programs: J2SE Java Runtime Environment 1.4

  The JRE is installed automatically when you install the HiCommand Device Manager server.

- CD-ROM drive
- Static IP address (used to test the LAN connections and allow access to the Device Manager Server)
- Device Manager Server residing on the same network as the storage subsystem(s)
- The HiCommand Device Manager server only supports IPv4 (it does not support IPv6). Connect the HiCommand Device Manager server, Web Client, the HiCommand Device Manager agent, and a storage subsystem by using IPv4. For details about how to disable IPv6, refer to the appropriate documentation for each OS.
- The following package for unpacking the installer (which has been packed by using gzip)

  For Solaris: SUNWgzip

  For Linux: gzip

- LAN cables, connections to the storage subsystem, and a 10/100 Ethernet LAN card that has TCP/IP installed and available. (If the machine and the LAN cable are compatible with Gigabit Ethernet, you can use a Gigabit-class card.)
- When using one HiCommand Device Manager server, it is not possible to use separate storage partitions with different storage administrator accounts. If you want to manage individual storage partitions, a HiCommand Device Manager server is required for each storage partition.
- Performing a new installation will take the following amount of time:
  - For Solaris: About 15 minute

(OS: Solaris 9, processor: UltraSPARC-III+ (1.2 GHz), memory: 2 GB)

- For Linux: About 10 minutes

  (OS: Linux AS 4.0, processor: Pentium 4 (3.2 GHz), memory: 2 GB)

WARNING: Do not install Device Manager and Hitachi Storage Services Manager on the same server.

Caution: HiCommand Device Manager does not support operations that use the terminal service function.

Important: The Device Manager server and agent must have the same version to be able to communicate with each other.

4.1.2 Setting Memory Heap Size According To the Number of Managed Resources

The following table shows the maximum number of resources that can be managed by the HiCommand Device Manager server. We recommend that you operate the HiCommand Device Manager server within these limits.

The default value in the table is used if you do not change the memory heap sizes of HBase Storage Mgmt Web Service and the Device Manager server. The number of LDEVs in the table is the total of the number of LDEVs for mainframes and the number of LDEVs for open systems.

Table 4.6 Maximum Number of Resources Managed by the HiCommand Device Manager Server

Resource	Maximum setting	Default
Number of LUNs	128,000	32,000
Number of Securities	192,000	48,000
Number of LDEVs	128,000 (The maximum number of LDEVs for open systems only is 64,000.)	16,000

In an environment in which HiCommand Device Manager is used, if the assumed number of resources exceeds the default settings in the above table, you need to estimate the number of managed resources, and then set the memory heap sizes of HBase Storage Mgmt Web Service and the Device Manager server according to the estimated value.

The formula that can be used for estimating the number of managed resources is shown below. When multiple storage subsystems are to be managed, estimate the number of managed resources for each storage subsystem, and use the greatest value as a guideline.

Formula:

number-of-managed-resources = *number-of-LDEVs* x 2.5 + *total-number-of-paths*[#]

 # total-number-of-paths = *number-of-LDEVs* x *average-number-of-paths-per-LDEV*

If the *number-of-managed-resources* is 28,000 or greater or if an *Out Of Memory* error occurs while you are using Web Client to perform an operation such as displaying a list of LDEVs, set the memory heap size by following the procedures described in sections 4.1.2.1 and 4.1.2.2.

After the memory heap size is set, if *number-of-managed-resources* increases from 50,000 or less to 50,001 or greater, only set the memory heap size of the Device Manager server if the memory heap size of HBase Storage Mgmt Web Service has already been set.

The set value is valid until the Device Manager server is uninstalled.

4.1.2.1 Setting Memory Heap Size of HBase Storage Mgmt Web Service

When you set the memory heap size of HBase Storage Mgmt Web Service, note the following points:

- You can only increase the heap size that has been set. If you want to decrease it, uninstall the Device Manager server, re-install the Device Manager server, and then change the heap size to the size you want.
- In an environment in which multiple HiCommand Suite products are installed, the largest heap size of the sizes for the products takes effect.

To set the memory heap size of HBase Storage Mgmt Web Service:

1. If HiCommand Suite products whose versions are earlier than 5.7 have been installed, stop their services.

   For details about how to stop these services, see the manual for your product version.

2. Execute the following command to stop the HiCommand Suite product services and HiCommand Suite Common Component:

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

3. Execute the following command:

   ```
   # /opt/HiCommand/Base/bin/hcmdsweb -add -file
   /opt/HiCommand/HiCommandServer/webapps/DeviceManager.war –server
   HiCommand -javaoption HDvM.serverpath=/opt/HiCommand –type
   DeviceManager -Xms256 -Xmx512
   ```

   Note: When setting the memory heap size of the Device Manager server at the same time:

   Before restarting the services in the next step, perform steps 1 and 2 (setting of the `hicommand.sh` file) that are described in section 4.1.2.2. If you do this, you can omit the operations of stopping and starting the services when setting the memory heap size of the Device Manager server.

4. Execute the following command to restart the HiCommand Suite product services and HiCommand Suite Common Component:

   ```
   # /opt/HiCommand/Base/bin/hcmdssrv –start
   ```

5. If HiCommand Suite products whose versions are earlier than 5.7 have been installed, restart their services as required.

For details about how to start these services, see the manual for your product version.

4.1.2.2 Setting Memory Heap Size of the Device Manager Server

To set the memory heap size of the Device Manager server:

1. Use an editor to open the `hicommand.sh` file in `/opt/HiCommand`.
2. Specify the following value for the `-Xmx` option of the `java` command specified in the `start` option script:
   - When the number of managed resources is 50,000 or less: `512m` (512 MB)
   - When the number of managed resources is more than 50,000: `1024m` (1 GB)

   If you use the CLI to obtain information about the storage subsystem, more memory might be required. Therefore, compare the value calculated by using the following formula and the above value, and then specify the larger value:

   Formula:

   memory-heap-size = *number-of-LDEVs* x 0.03 + *total-number-of-paths* x 0.03 + 140
3. Restart the Device Manager server as follows:

   Execute the following command:

   ```
   # /opt/HiCommand/suitesrvcntl -stop_hdvm
   ```

   After the Device Manager server has stopped, execute the following command:

   ```
   # /opt/HiCommand/suitesrvcntl -start_hdvm
   ```

4.1.2.3 Setting Memory Heap Size When Using CIM/WBEM

If CIM/WBEM functions are being used, you might have to increase the memory heap size of the Device Manager server, depending on the conditions. Note that the required memory heap size differs depending on the CIM client you are using.

To change the memory heap size:

1. Use a text editor to open the `hicommand.sh` file in `/opt/HiCommand`.
2. Open the `hicommand.sh` file in a text editor, and change the value of the `-Xmx` option of the `java` command specified in the `start` option script to *new-setting-value* (units: MB) calculated using the following two formulas:
   - *calculation-value-for-SMI-S-Provider* = 30000 x *number-of-LDEVs* x *number-of-paths-per-LDEV* / 1048576

     If the value of *number-of-paths-per-LDEV* becomes less than 1, assume that this value is equal to 1 for the calculation.

     The value of *calculation-value-for-SMI-S-Provider* is expressed in megabytes. For this value, round up the value to the next whole number. If this value becomes less than 256 (MB), assume that this value is equal to 256 for the calculation.
   - *new-setting-value* = *current-setting-value* + *calculation-value-for-SMI-S-Provider*

All of the values in the above formula are expressed in megabytes.

The value of *new-setting-value* obtained from the above formula is the memory heap size required for obtaining the class information that belongs to the bottom layer in a CIM class. When an upper-layer class is specified, some SMI-S clients might obtain information of all the classes below that class at the same time. In this case, required capacity will be larger than the value of *new-setting-value* obtained from this formula.

Example of changing the value (when the *new-setting-value* is calculated to be 512 MB):

Before: `java -Xmx256m -classpath ...`

After: `java -Xmx512m -classpath ...`

3. Restart the Device Manager server as follows:

   Execute the following command:

   ```
   # /opt/HiCommand/suitesrvcntl -stop_hdvm
   ```

   After the Device Manager server has stopped, execute the following command:

   ```
   # /opt/HiCommand/suitesrvcntl -start_hdvm
   ```

4.2 Installing to a Solaris or Linux Environment

Device Manager Server will be installed in **/opt/HiCommand**.

The Common Component will be installed in **/opt/HiCommand/Base**.

4.2.1 Preparing for Installation

Before you start installation, check the usage status of the port numbers, the installation status of other programs, and other information as described below.

4.2.1.1 Checking Port Numbers

Check whether the port numbers required to use HiCommand Device Manager are being used by another product on the machine on which the HiCommand Device Manager server is to be installed by using the `netstat` command.

Example: Check whether another program is using the port `162/udp`.

Execute the following command:

In Solaris: `netstat -an -P udp`

In Linux: `netstat -uan`

In the command execution results, if there are no lines in which `Local Address` is `162`, the port is not being used.

The following shows the ports required to use HiCommand Device Manager. For details about the intended use of each port, see section 2.4 and section 5.4.1.

- Port numbers that must be checked:
  - From 23015 to 23018, and 23032: If another product is using any of these ports, change the settings of that product, or change the settings of HiCommand Device Manager. For details about how to change these port numbers, see section 5.4.2. If HiCommand Suite Common Component has been installed and these ports have been changed, you can install the HiCommand Device Manager server by using those ports. You do not need to set up the default ports.
  - From 45001 to 49000: For these port numbers, the settings of HiCommand Device Manager cannot be changed. Therefore, you need to change the settings of any other products that are using the same ports as HiCommand Device Manager.
  - 2001: If another product is using this port number, change the settings of that product, or change the port number to be used before HiCommand Device Manager starts. For details about how to change this port number, see section 8.2.2. If another product is using this port number, the following message will be output to the syslog file, and HiCommand Device Manager will not be able to start: `KAIC00114-E An attempt to start the HTTP server on port "2001" failed.`

- Port numbers that must be checked when some functions are enabled:
  - 162: This port number is used when the SNMP Trap reception function of HiCommand(R) Device Manager is enabled. To disable the SNMP Trap reception function, select disable in the Setting for the SNMP Trap Reception Function panel during installation (see Figure 4.7).
  - 1099: This port number is used when the function to link with Storage Navigator Modular (for Web) (see section 9.1), or DAMP (for Web) (see section 9.1.4) is enabled. For details about how to change the port number used to link with Storage Navigator Modular (for Web), see section 9.1.2. The port number for the function to link with DAMP (for Web) cannot be changed. When the port number 1099 is used by another product, perform one of the following operations so that other products do not use the port number 1099 at the same time as HiCommand Device Manager.

    If a product that uses the port number 1099 is always running, use different machines to run HiCommand Device Manager and that product respectively.

    If a product that uses the port number 1099 runs temporarily, restart DAMP (for Web).
  - 2000: This port number is used when the function to link with Storage Navigator Modular (for Web) (see section 9.1) or DAMP (for Web) (see section 9.1.4) is enabled. For details about how to change this port number, see section 1.5.1.2 or 1.5.1.6.
  - 2443: This port number is used when SSL communication is enabled. For details about how to change this port number, see section 8.2.3. If another product is using this port number, the following message will be output to the syslog file, and HiCommand Device Manager will not be able to start: `KAIC00115-E An attempt to start the HTTPS server on port "2443" failed.`

4.2.1.2 Checking the Time of a Machine and the Functions that Adjust the Time

If the time of a machine is changed while the services of HiCommand Suite Common Component and HiCommand Suite products are running, Device Manager 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.

Changing the time after installing Device Manager

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 Suite products.

2. Change the time of the machine.
3. Restart the machine.

4.2.1.3 Checking Other Programs Related to Security

- Check whether the following programs are installed. If they are installed, take action by following the explanation below:
  - A program that monitors security

    Stop the program that monitors security, or change its settings so that Device Manager can be installed normally.
  - A program that detects viruses

    We recommend that you stop programs that detect viruses, and then install Device Manager.

    If a program that detects viruses is running during installation of Device Manager, the speed of installation might be reduced, installation might fail, or installation might finish in an incorrect state.
  - A program that monitors processes

    Stop the program that monitors processes, or change its settings so that the program does not monitor the processes of the HiCommand Device Manager server and the HiCommand Suite Common Component.

    If a program that monitors processes starts or stops the above processes during installation of Device Manager, installation might fail.

4.2.1.4 Checking Other Programs

- HiCommand Device Manager cannot be installed on the server on which Tuning Manager has been installed with a Large configuration. If you try to install HiCommand Device Manager in such an environment, the installation is canceled. If that happens, install Tuning Manager and HiCommand Device Manager separately on different servers.
- You cannot install a version of Tuning Manager earlier than 4.0 on a machine on which Device Manager 4.0 or later has been installed.
- When using another HiCommand Suite product, make sure that you back up the database for the relevant product.
- The HiCommand Device Manager server cannot coexist with the following HiRDB products. Therefore, do not install the HiCommand Device Manager server on a machine on which any of the following HiRDB products are installed. In addition, do not install these HiRDB products on a machine on which the HiCommand Device Manager server is installed.
  - HiRDB/Single Server
  - HiRDB/Parallel Server
  - HiRDB/Workgroup Server
  - HiRDB/Run Time

- HiRDB/Developer's Kit
- HiRDB SQL Executer

4.2.1.5 Checking Other Information

- You must log on as a root user.
- You must revise the Solaris or Linux OS parameters (kernel parameters and shell restrictions). To change the kernel parameters to the appropriate values, see 4.10 for Solaris, or section 4.11 for Linux. If the kernel parameter setting is not correct, installation will fail.
- Verify that the following directories can be created, or that they have already been created and are write-enabled.
  - `/etc/init.d`
  - `/opt/HiCommand`
  - `/opt/hitachi`
  - `/var/opt/HiCommand`
  - `/var/opt/hitachi/HNTRLib2`
- Verify that symbolic links that have the following names have not been created. If they have been created, installation might fail.
  - `/opt`
  - `/var/opt`
  - `/var/tmp`
  - The names of the directories in `/opt/HiCommand` (including `/opt/HiCommand`)
  - The names of the directories in `/var/opt/HiCommand` (including `/var/opt/HiCommand`)
  - The names of the Device Manager server database storage destination directory and its subordinate directories

    Default storage destination: `/opt/HiCommand/HiCommandServer/database`
  - The names of the HiCommand Suite Common Component database storage directory and its subordinate directories

    Default storage destination: `/var/opt/HiCommand/Base/database`
- Do not attempt a downgrade installation for Device Manager. For example, in an environment in which Device Manager 5.0 has been installed, you cannot install Device Manager 4.3 or an earlier version. However, a build to which patches have been applied can be overwritten by a build without the patches, as long as the version-revision numbers are the same.
- To use the service discovery feature in Solaris, the SLP daemon must be enabled before HiCommand Device Manager is installed (perform setup so that the SLP daemon starts automatically when the system starts). For information on how to enable the SLP daemon in Solaris, see section 11.5.1.2.

- In Linux, firewall exceptions must be registered manually before installation. For details on how to do this, see section 2.5.
- Do not specify the system's zone settings during installation in Solaris 10 system. If you do specify the settings, installation might finish abnormally.
- When you install the Device Manager server, specify the host name or IP address of the server machine. When you specify the host name, make sure that the host name satisfies the following conditions:
  - Number of characters: 32 bytes or less
  - Available characters: `A-Z a-z 0-9 -`

    You cannot use a hyphen (-) at the beginning or end of the host name.

  When you install the Device Manager server in a cluster environment, specify a logical host name that satisfies the above conditions.
- If multiple NICs are installed on the machine, during installation you will need to specify the IP address that corresponds to one of those NICs. If multiple NICs are connected to different networks, use the IP address of the NIC that belongs to the network to which Web Client is connected.

  The IP address specified during installation is also used when you specify the following settings after installation is complete:
  - `server.http.host` property

    For details about how to set this property, see section 8.2.1
  - An environment for Storage Navigator Modular (for Web) or DAMP (for Web)

    You specify the host name or IP address when setting up an environment for linking with Storage Navigator Modular (for Web) or DAMP (for Web). For details about the procedure, see section 9.1 or 9.2.

4.2.2 Reviewing the Contents of the Installation CD

The Device Manager Server installation CD includes the following applications:

- Java 2 JRE software: version 1.4.2_06
- Device Manager Server software
- HiCommand Suite Common Component software
- HiRDB Database version 7.0

Once these products are installed, the Device Manager client software can be downloaded, installed and updated on the client systems from the Device Manager Server.

Installation requires root access, so you must be logged in as root to run the installation. You can use the **su** command to assume root privileges to run the installation.

4.2.3 Performing a New Installation of Device Manager Server

After finishing a new installation, be sure to back up the HiCommand Device Manager server database.

To install Device Manager Server:

1. Log on to the Solaris(TM) or Linux system as the root user.
2. Insert the HiCommand Device Manager CD-ROM. If the CD-ROM is not automatically mounted, mount the CD-ROM to `/mnt/cdrom`.
3. Move the current directory to the directory that stores the installer of Device Manager (`install.sh`). And then, execute the following command:

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

   WARNING: Do not use **Ctrl + C** to stop in the middle of the installation. If you stop the installation, check the installation progress as follows:

   - For Solaris:

     Execute the `pkginfo HDVM` command.

   - For Linux:

     Execute the `rpm -qi HDVM` command.

   If the Device Manager information is displayed, uninstall (see section 4.8.1 for instructions) and then re-install the Device Manager Server.

4. A message displays, asking whether the kernel parameter has been set up (see Figure 4.1). If the parameter has not been set up, select **n** to cancel the installation. If the parameter has been set up, select **y** to continue. For details about setup of the kernel parameters, see 4.10 for Solaris, or see section 4.11 for Linux

   Caution: If the kernel parameters are not set correctly, a message notifies you that the machine must be restarted after the kernel parameters are reset, and installation stops (see Figure 4.2).

   Caution: Figure 4.1 and Figure 4.2 show the output examples in Solaris In Linux, `kernel parameter` will be replaced with `OS parameter`.

5. When the HiCommand Suite Common Component services are running in a non-cluster environment, a message indicating that the installer will stop these services is displayed. If you want to stop the installation, select **n**. If you want to continue the installation, select **y** (see Figure 4.3).

   If the installer cannot stop all the services of HiCommand Suite Common Component and the HiCommand Suite products, a message indicating that the installer failed to stop the services is displayed (see Figure 4.4). If this message is displayed, choose **y** to try to stop the services again. If the installer still fails to stop the services, cancel the installation, manually stop the services of HiCommand Suite Common Component and the HiCommand Suite products, and then perform the installation again.

6. If HiCommand Suite Common Component is already installed, a message appears, recommending that you make a backup (see Figure 4.5). For more information about how to back up the database other HiCommand Suite products databases, see the relevant manual for each product. If you have not yet performed a backup, select **2** to cancel the installation. If a backup is not needed or has already been performed, select **1**.

7. In Solaris, HiCommand Device Manager is displayed as an available package. Press **Enter** to continue.

   Important: When the Common Component is being installed at version 4.0 or later, the HiRDB database will also be installed for database management functionality.

8. The license agreement displays. Select **y** to continue.

9. The SNMP Trap Note message displays (see Figure 4.6). Make sure that no other software products are using port 162 (if this is not the case, the error message in Figure 4.7 is displayed), and then press **Enter**.

   If you want to disable the SNMP Trap reception function to start Device Manager, choose Yes to continue. If you want to change the settings of the product that is using port 162 and re-execute the installation, choose No to cancel the installation.

   Caution: If you choose **y**, the properties for the SNMP Trap reception function are automatically changed to disable the function. You must reset these properties to the default values manually.

10. If the Common Component 4.0 or later has not already been installed, specify a directory for the Common Component database files (see Figure 4.8).

    Caution: The file name has the following requirements:

    - The file name must be 90 bytes or fewer, and you must specify an absolute path to it.
    - Do not enter a path delimiter (/) at the end of the directory path.
    - You can use alphanumeric characters, underscores and periods for the path name

11. Specify a directory for the Device Manager Server database files. The server database file name has the same restrictions as the Common Component database file name (see Figure 4.9).

12. A message appears, prompting you to enter the IP address or host name of the target server, and the port number to be used (see Figure 4.10).

    Important: The default port number is 23015, which will automatically be selected if you press **Enter** without changing the number. If you change the port number, you must also change that port number in the Common Component. For information on how to change a Common Component port number, see section 5.4.2.

13. A message about the settings for the SMI-S Provider service appears (Figure 4.11). If you want the SMI-S Provider service to start automatically when Device Manager starts, select **1** to continue. If you do not want it to start automatically, select **2** to continue.

    If you selected **1**, go to the next step. If you selected **2**, go to step 18.

    Note: You can set up the SMI-S Provider service after installation. For details, see Chapter 11.

14. A message about the SSL settings for SMI-S appears (see Figure 4.12). If you want to use SSL with SMI-S using the default port number (5989), select **1** to continue. If you want to use SSL with SMI-S, but you want to specify the port number yourself, select **2** to continue. If you want to use the default port number (5988) for SMI-S, but you do not want to use SSL, select **3** to continue. If you want to specify the port number for SMI-S by yourself, but do not want to use SSL, select **4** to continue.

    Note: You can enable SSL and set the port number after installation. For details, see section 11.3.2.2 and 11.4.1.

15. A message about changing the port number appears (see Figure 4.13). Enter the port number to be used, as required.

16. A message about two-way authentication for object operations and event indications appears (see Figure 4.14). If you do not want to use two-way authentication, select **1** to continue. If you want to use two-way authentication only for object operations, select **2** to continue. If you want to use two-way authentication only for event indications, select **3** to continue. If you want to use two-way authentication for both object operations and event indications, select **4** to continue.

    Caution: Two-way authentication involves import and export of authentication files. For details, see section 7.4.

    Note: You can enter settings to enable two-way authentication after installation. For details, see section 7.4.

17. A message about the settings for the SLP daemon appears (see Figure 4.15). To install and enable the SLP daemon, select **1** and then proceed to the next step. If you do not want to enable the SLP daemon, or if another SLP daemon is already installed and enabled, select **2** and then proceed to the next step.

    Important: In Solaris, the SLP daemon must be enabled before HiCommand Device Manager is installed. Accordingly, select **2** here.

    Note: In Linux, it is possible to enable the SLP daemon after installing HiCommand Device Manager. For details, see section 11.5.

18. In a non-cluster environment, a message asking whether you want to start the HiCommand Suite product services after installation is complete is displayed (see Figure 4.16). If you want to start the services after installation is complete, choose **y**. The services of HiCommand Suite Common Component and HiCommand Suite products will then be started after installation is complete. If you do not want to start the services after installation is complete, choose **n**.

    Caution: The services of HiCommand Suite products whose versions are earlier than 5.7 are not started by choosing **y**. If you want to start the services of HiCommand Suite products after installation is complete, manually start the services. For details about how to start these services, see the manual for your product version.

19. In Solaris, the Installation Continuation Confirmation message is displayed (see Figure 4.17). In Linux, the HiCommand Device Manager package confirmation message is displayed (see Figure 4.18). Select **y** to start the installation. If the Common Component has not previously been installed at version 4.0 or higher, it will be installed during the Device Manager installation.

20. The **Secure Socket Certificates Note** panel displays (see Figure 4.19). Press **Enter** to continue.

21. A message displays indicating that the installation completed successfully and the Server and Common Component are starting. Be sure to refresh all registered subsystems at this point.

Note: If the installer ends with an error, follow the instructions on the error message and re-install Device Manager. Check the installation progress as follows.

- For Solaris:

  Execute the `pkginfo HDVM` command.

- For Linux:

  Execute the `rpm -qi HDVM` command.

  If the Device Manager information is displayed, first uninstall and then reinstall Device Manager. See section 4.8 for instructions on uninstalling the Device Manager server.

  Important: After installing the HiCommand Device Manager server, you need to register a license key by using Web Client. For information about how to register a license key, see the *HiCommand Device Manager Web Client User's Guide*.

```
WARNING: The kernel parameters must be set before installing HiCommand Device
Manager.
If the kernel parameters have already been set for another application, the
value for HiCommand Device Manager must be added to the existing settings.
If the kernel parameters have not been set, enter n to cancel installation.
If the kernel parameters have been set, enter y to continue installation.
Have the kernel parameters for HiCommand Device Manager been set?  [y/n]
```

Figure 4.1 Message that Confirms the Setup of the Kernel Parameter

```
ERROR: The value of an effective kernel parameter(parameter) doesn't fill the
lower bound value of Device Manager. Please check the settings of the kernel
parameter and reboot the system. The installation is stopped.
```

Figure 4.2 Error Message for the Setup of the Kernel Parameter

```
Stop HiCommand Suite Product Services:
HiCommand Suite product services are running. If you continue the
installation, the services of all HiCommand Suite products will be stopped.

Do you want to continue installation? [y/n]
```

Figure 4.3 Message that Confirms Stopping of Services (appears during installation)

```
ERROR: An attempt to stop the services of HiCommand Suite products has failed.
```

Figure 4.4 Error Message Reporting That an Attempt to Stop a Service Has Failed

```
Backup recommendation:
If HiCommand Suite products have already been installed, it is strongly
recommended that you back up the HiCommand Suite Common Component database and
the databases for each installed HiCommand Suite product. What do you want to
do?
  1. Continue the installation.
  2. Stop the installation to manually perform backup.
Enter 1 or 2:
```

Figure 4.5 Backup Recommendation Reminder

```
SNMP Trap Note:
HiCommand Device Manager uses UDP port 162 to listen for SNMP traps.
If another product uses port 162, after installation you need to disable
listening for SNMP traps by changing the property of HiCommand Device Manager.
Hit Enter Key to Continue.
```

Figure 4.6 SNMP Trap Note

```
Setting for the SNMP Trap Reception Function:
Another application is using the port used to listen for SNMP traps.
To use Device Manager, you must disable the SNMP trap reception function of
Device Manager.
Do you want to disable the SNMP trap reception function of Device Manager?
Do you want to continue installation? (Y/N):
```

Figure 4.7 Settings for the SNMP Trap Reception Function

```
Specify the storage destination for the database files that HiCommand Suite
Common Component will use.
Note: At least 1.2 GB of free space is required.
[default=/var/opt/HiCommand/Base/database]
```

Figure 4.8 Specifying Common Component Database Files

```
Specify the storage destination for the database file that HiCommand Device
Manager will use.
Note 1: At least 100 MB of free space is required.
Note 2: For an upgrade installation, at least 100 MB or four times the file
size of HiCommand.gdb (whichever is the largest) is required.
[default=/opt/HiCommand/HiCommandServer/database]
```

Figure 4.9 Specifying HiCommand Device Manager Database Files

```
Enter the IP address or host name of the server that the client accesses from
a Web browser:
> 10.60.71.15
Enter the port number of the server that the client accesses from a Web
browser [default=23015]:
```

Figure 4.10 Entering IP address and Port Number

```
Setting for the SMI-S Provider Service:
Do you want the CIM/WBEM function to be enabled automatically after
installation?
(The CIM/WBEM function is only necessary if you need to access Device Manager
by using an SMI-S client.)

1. YES. Automatically enable the function after installation.
2. No.
Enter 1 or 2. [default=2]:
```

Figure 4.11 Settings for the SMI-S Provider Service

```
Setting for the SMI-S SSL:
Do you want to use SSL for SMI-S operations?
1. YES. (Default port number is 5989.)
2. YES. (I will change the port number.)
3. NO. (Default port number is 5988.)
4. NO. (I will change the port number.)
Enter 1, 2, 3 or 4. [default=1]:
```

Figure 4.12 SSL Settings for SMI-S

```
Change the port number if needed.
Enter the port number:
```

Figure 4.13 Changing the Port Number

```
Do you want to also use Two-way Authentication for the following operations?
1. NO.
2. Also use Two-way Authentication for Object operations.
3. Also use Two-way Authentication for Event Indications.
4. Also use Two-way Authentication for both Object operations and Event
Indications.
Enter 1, 2, 3 or 4. [default=3]:
```

Figure 4.14 Two-way Authentication for Object Operations and Event Indications

```
Setting for the SLP Daemon:
Do you want the SLP function to be enabled automatically after installation?
(The SLP function is required from SMI-S client. If you have not installed
other SLP daemon, you need to install our SLP daemon.)

1.YES. Automatically enable the function after installation.
2.NO.
Enter 1 or 2. [default=1]:
```

Figure 4.15 Setting the SLP Daemon

```
Set Services to Start After Installation:
Do you want the services of all HiCommand Suite products to start after the
installation finishes? (y/n) [default=y]:
```

Figure 4.16 Setting Services to Start After Installation (appears during installation)

```
This package contains scripts which will be executed with super-user
permission during the process of installing this package.

Do you want to continue with the installation of <HDVM> [y,n,?]
```

Figure 4.17 Installation Continuation Confirmation Message (in Solaris)

```
This will install the following package:
  HiCommand Device Manager 5.7.0(5.7.0-00)
Do you want to install this package? (y/n)
```

Figure 4.18 HiCommand Device Manager Package Confirmation Message (in Linux)

```
Secure Socket Certificates Note:
If secure socket communications (https://) with HiCommand Device Manager are
expected, it is necessary to generate a certificate for the following two
servers.

1) HiCommand Device Manager Server
2) HBase Storage Mgmt Web Service
Hit Enter Key to Continue.
```

Figure 4.19 Secure Socket Certificates Note

4.2.4 Upgrading or Re-installing Device Manager

After finishing an upgrade installation, be sure to back up the HiCommand Device Manager Server database.

4.2.4.1 General Considerations for Upgrade and Re-installation

CAUTION: Wait several minutes after the upgrade or re-installation finishes before stopping the service, because the database must be updated with the latest information.

WARNING: Do not cancel in the middle of an upgrade or re-installation, because doing so could corrupt the files.

If you are updating the Common Component database and an error occurs and auto-recovery fails, you must manually recover the database before you re-install the server. Once you upgrade or re-install the server, you will not be able to recover the Common Component database. To find a database update error, check the following log file:

<installation directory>/Base/log/hcmdsdbupdate.log. You will want to restore the file named **<installation directory>/Base/database/hbase_vup_back.gbk**.

If you install a new version of the Device Manager server, the new version overwrites the existing version. Device Manager automatically updates your data and configurations to work with the latest version. The previous **HiCommandCLI.properties** file is saved as HiCommandCLI.properties.old in the same directory. The previous **TIA.properties** file is saved as **TIA.properties.old** in the same directory.

Important: If the `HiCommandCLI.properties` file contains multiple entries of the same key with different values, the value of the most recently specified key overrides the others. Although key duplication does not affect HiCommand CLI operations, we do not recommend that you specify the same key more than once with different values. Instead, eliminate unnecessary duplicate keys and their values. If there are duplicate keys that have different values during an upgrade installation, the new `HiCommandCLI.properties` file will inherit keys as follows:

If there are multiple `password` keys:

All `password` keys and their values in the old `HiCommandCLI.properties` file are written to the new file as is. The following shows an example:

- The `password` keys and their values in the old file:

  ```
  password=AAA
  password=BBB
  ```

- The `password` keys and their values written to the new file:

  ```
  password=AAA
  password=BBB
  ```

If there are duplicate keys other than `password`:

The name and value of the most recent duplicate key in the old `HiCommandCLI.properties` file are written to the new file as many times as there are duplicated keys. The following shows an example:

- The `user` keys and their values in the old file:

  `user=AAA`

  `user=BBB`

- The `user` keys and their values written to the new file:

  `user=BBB`

  `user=BBB`

Note: User-created files will not be saved as `*.old` during the upgrade.

To manually make a backup before performing an upgrade installation or re-installation of the Device Manager server, copy the following files and directories to another location:

- `/opt/HiCommand/HiCommandServer/config/*.properties`

  The old `*.properties` files are backed up in the `config` directory as `*.properties.old`. Note, however, that files created by a user will not be backed up.

- `/opt/HiCommand/HiCommandServer/logs`

  To back up the log files, copy this directory to another location

- `/opt/HiCommand/HiCommandCLI/HiCommandCLI.properties`

  The old `HiCommandCLI.properties` files are backed up as `HiCommandCLI.properties.old` in the same directory.

- `/opt/HiCommand/HiCommandCLI/legacy/R2.0/HiCommandCLI.properties`

  The old `HiCommandCLI.properties` files are backed up as `HiCommandCLI.properties.old` in the same directory.

- `/opt/HiCommand/HiCommandCLI/legacy/R2.1/HiCommandCLI.properties`

  The old `HiCommandCLI.properties` files are backed up as `HiCommandCLI.properties.old` in the same directory.

- `/opt/HiCommand/SupportTools/CollectTool/TIA.properties`

  The old `TIA.properties` files are backed up as `TIA.properties.old` in the same directory.

4.2.4.2 When Upgrading from Versions 2.2 Through 3.5 to Version 4.0 or Higher

You cannot upgrade directly from Device Manager version 2.2 to version 4.0 or higher. You must first upgrade to a version between 2.3 and 3.5, and then upgrade to version 4.0 or higher.

Caution: If either InterBase or InterServer has previously been installed, that service must be running when you upgrade the Device Manager Server.

Caution: If version 2.2 or earlier of the HiCommand Device Manager server has been installed, the users `hicmd` and `interbase`, and the user group `hicmd` have been created. If the package was installed more than once, users `hicom0` to `hicom999` and user groups `interb0` to `interb99` might have been created. Version 2.3 or later of the HiCommand Device Manager server does not use these users. If these users are not necessary, delete them manually.

Caution: When version 1.1 or earlier of the HiCommand Device Manager server is installed and an overwrite installation is performed, every volume in each logical group is displayed as a CVS volume. Also, disk usage information is not displayed. To avoid this problem, refresh all storage subsystems which were discovered by version 1.1 or earlier of the HiCommand Device Manager server.

WARNING: If you have made any changes to **/opt/HiCommand/Base/conf/init.conf**, and you are upgrading from Device Manager version 3.0 or 3.1 to version 3.5 or later, you must first create a new folder for **/opt/HiCommand/Base/conf/user.conf**, and duplicate those changes in this file.

Important: The characters that can be used for user IDs in HiCommand Device Manager server (version 3.5 or later) are as follows:

A-Z a-z 0-9 - _ . @ + #.

Important: The characters that can be used for passwords in version 03-01-/A are as follows:

A-Z a-z 0-9 ! # $ % & ( ) * + - . = @ \ ^ _ | '

If you have user IDs or passwords with unusable characters, you need to re-register those users.

If all of the System Administrators have user IDs or passwords with unusable characters, create a new System Administrator user ID, as follows:

1. Back up the current server database. See section 3.6.1 for instructions.
2. Uninstall the Device Manager Server (version 3.5 or later). See section 4.8.1 for instructions.
3. Install the Device Manager Server at version 2.4 or earlier.
4. Restore the database. See section 4.6.2 for instructions.
5. Create a new user by using the appropriate characters for user IDs and passwords.
6. Re-install the Device Manager Server at version 3.5 or later.
7. Clear the cache in Java Web Start.

Note: If the older version of HiCommand Device Manager was not installed in `/opt/HiCommand/`, the upgrade of HiCommand Device Manager will not execute properly. If this is the case:

- Back up old files manually.
- Uninstall the older version of the HiCommand Device Manager server.

- Move the current directory to the root (/), and then execute the following command:

  # ***installation-directory-for-the-Device-Manager-server***/Uninstall/uninstall.sh

- Perform a new installation to install the new version of the HiCommand Device Manager server.

4.2.4.3 About User Information in Version 5.0 and Higher

In version 5.0 or higher, user information is managed by using the user management functionality of HiCommand Suite Common Component. The registered user information is migrated to the HiCommand Suite Common Component repository when the Device Manager server is started for the first time after the upgrade installation. For this migration, also note the following points:

- If there is user information that cannot be migrated to the HiCommand Suite Common Component repository due to data corruption or another problem, that information is output to the Device Manager trace log file.
- If user accounts with the same user ID but different passwords have been registered in both HiCommand Suite Common Component and Device Manager, the user account in HiCommand Suite Common Component overrides the one in Device Manager. The user account registered in Device Manager becomes unavailable, and information to that effect is output to the Device Manager trace log file.
- If user accounts that have the same user ID and password have been registered in both HiCommand Suite Common Component and Device Manager, the user account in Device Manager is added to the one in HiCommand Suite Common Component.
- You cannot migrate the user account whose user ID is System. The user management functionality of HiCommand Suite Common Component defines this user ID as having the Admin permission for all HiCommand Suite products (version 5.0 or later).

4.2.5 Performing an Upgrade Installation from Version 3.5 or Earlier

To upgrade the HiCommand Device Manager Server:

1. Log on to the Solaris system as the root user.
2. Insert the HiCommand Device Manager CD-ROM. If the CD-ROM is not automatically mounted, mount the CD-ROM to /mnt/cdrom.
3. Move the current directory to the directory that stores the installer of Device Manager (install.sh). And then, execute the following command:

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

WARNING: Do not use **Ctrl + C** to stop in the middle of the installation. If you stop the installation, check the installation progress as follows:

Execute the pkginfo HDVM command.

4. A message displays, asking whether the kernel parameters have been set up (see Figure 4.1). If the parameters have not been set up, select **n** to cancel the installation; otherwise, select **y** to continue.

   Caution: If the kernel parameters are not set correctly, a message notifies you that the machine must be restarted after the kernel parameters are reset, and installation stops (see Figure 4.2).

5. When the HiCommand Suite Common Component services are running in a non-cluster environment, a message indicating that the installer will stop these services is displayed. If you want to stop the installation, select **n**. If you want to continue the installation, select **y** (see Figure 4.3).

   If the installer cannot stop all the services of HiCommand Suite Common Component and the HiCommand Suite products, a message indicating that the installer failed to stop the services is displayed (see Figure 4.4). If this message is displayed, choose **y** to try to stop the services again. If the installer still fails to stop the services, cancel the installation, manually stop the services of HiCommand Suite Common Component and the HiCommand Suite products, and then perform the installation again.

6. If InterBase has not been installed (see Figure 4.20), or if the InterBase version is not 6.0 (see Figure 4.21), an upgrade installation cannot be performed without InterBase 6.0 installed.

   If InterBase 6.0 has not been installed, uninstall the HiCommand Device Manager server and then start a new installation, or install HiCommand Device Manager 3.5 or earlier and then perform an upgrade installation.

   If the version of InterBase is incorrect, an upgrade installation cannot be performed. In this case, uninstall the HiCommand Device Manager server, and then start a new installation.

7. If InterClient has not been installed (see Figure 4.22), or the version of InterClient is not 2.0 (see Figure 4.23), an upgrade installation cannot be performed without InterClient 2.0 installed.

   If InterClient 2.0 has not been installed, uninstall the HiCommand Device Manager server and then start a new installation, or install HiCommand Device Manager 3.5 or earlier and then perform an upgrade installation.

   If the version of InterClient is incorrect, an upgrade installation cannot be performed. In this case, uninstall the HiCommand Device Manager server, and then start a new installation.

8. Device Manager is displayed as an available package. Press **Enter** to continue.

   Warning: If you attempt to do so, an error message (Figure 4.24) displays and installation stops. However, if the version and revision numbers of the builds before and after a selected package are the same, and the selected package has an earlier (outdated) service pack, the HiCommand Device Manager downgrade message appears (Figure 4.25). In that case, select **y** to continue.

9. The license agreement displays. Select **y** to continue.

10. If the Common Component 4.0 or later has not already been installed, specify a directory for the Common Component database files. (see Figure 4.8).

    Caution: The file name has the following requirements:

- The file name must be 90 bytes or fewer, and you must specify an absolute path to it.
- Do not enter a path delimiter (/) at the end of the directory path.
- You can use alphanumeric characters and spaces for the path name

11. Specify a directory for the Device Manager Server database files. The server database file name has the same restrictions as the Common Component database file name (see Figure 4.9).
12. If HiCommand Suite Common Component 3.0 or later has not been installed, a message appears, prompting you to enter the IP address or host name of the installation-target server, and the port number to be used (see Figure 4.10).

    Important: If you press the **Enter** key without entering anything, the default port 23015 is specified. When changing the port, you must also change the port in HiCommand Suite Common Component. For details on how to change the HiCommand Suite Common Component port, see section 5.4.2.
13. In a non-cluster environment, a message asking whether you want to start the HiCommand Suite product services after installation is complete is displayed (see Figure 4.16). If you want to start the services after installation is complete, choose **y**. The services of HiCommand Suite Common Component and HiCommand Suite products will then be started after installation is complete. If you do not want to start the services after installation is complete, choose **n**.

    Caution: The services of HiCommand Suite products whose versions are earlier than 5.7 are not started by choosing **y**. If you want to start the services of HiCommand Suite products after installation is complete, manually start the services. For details about how to start these services, see the manual for your product version.

    Important: To continue setup in a cluster environment after installation is complete, choose **n**.
14. In Solaris, the Installation Continuation Confirmation message is displayed (see Figure 4.17). In Linux, the HiCommand Device Manager package confirmation message is displayed (see Figure 4.18). Select **y** to start the installation. If HiCommand Suite Common Component has not been installed, it is installed during the installation of HiCommand Device Manager.
15. If you are upgrading from Device Manager version 3.5 or lower to version 4.0 or higher, the Database conversion message displays (see Figure 4.26).

    If you select **1**, the installer automatically converts the database. If the database conversion fails, an error message displays (see Figure 4.27).

    Important: If an error occurs during the database conversion, you may need to take corrective action. For more information, see Chapter 10.

    Note: It may take a long time to convert the database. For example, if 8,000 LDEVs and 16,000 paths have been managed, the database conversion will take about 10 minutes in an environment that has a 900 MHz CPU and 2 GB of memory.

    If you select **2**, the installer will not convert the database. Convert the database manually after the installation finishes. For more information, see section 4.7.
16. The Secure Socket Certificates Note panel displays (see Figure 4.19). Press **Enter** to continue.

17. A message displays indicating that the installation completed successfully and the Server and Common Component are starting. Be sure to refresh all registered subsystems at this point.

Note: If the installer ends with an error, follow the instructions on the error message and re-install Device Manager. Check the installation progress as follows.

- For Solaris:

  Execute the `pkginfo HDVM` command.

- For Linux:

  Execute the `rpm -qi HDVM` command.

  If the Device Manager information is displayed, first uninstall and then reinstall Device Manager. See section 4.8 for instructions on uninstalling the Device Manager server.

```
ERROR:InterBase is required for an upgrade installation of HiCommand Device
Manager.
For a new installation, uninstall any installed HiCommand Device Manager, and
then install the new HiCommand Device Manager.For an upgrade installation,
install HiCommand Device Manager version 3.5 or earlier, and then install the
current version of HiCommand Device Manager.
```

Figure 4.20 When InterBase is Not Installed

```
ERROR: InterBase version is incorrect. An upgrade installation cannot be
performed because the operating environment of HiCommand Device Manager is
incorrect. Uninstall HiCommand Device Manager, and then perform the
installation.
```

Figure 4.21 Incorrect InterBase Version

```
ERROR:InterClient is required for an upgrade installation of HiCommand Device
Manager.
For a new installation, uninstall any installed HiCommand Device Manager, and
then install the new HiCommand Device Manager.
For an upgrade installation, install HiCommand Device Manager version 3.5 or
earlier, and then install the current version of HiCommand Device Manager.
```

Figure 4.22 InterClient Not Installed

```
ERROR: InterClient version is incorrect. An upgrade installation cannot be
performed because the operating environment of HiCommand Device Manager is
incorrect. Uninstall HiCommand Device Manager, and then perform the
installation.
```

Figure 4.23 Incorrect InterClient Version

```
ERROR: A newer version of HiCommand Device Manager is already installed on
this system.
You cannot downgrade HiCommand Device Manager.
For example:
1. If 5.0.0(5.0.0-xx) is already installed, you cannot install 4.2.0(4.2.0-xx)
in an update installation.
2. If 4.3.0(4.3.0-xx) is already installed, you cannot install 4.2.0(4.2.0-xx)
in an update installation.
```

Figure 4.24 Upgrade Error Message

```
WARNING: A newer version of HiCommand Device Manager is already installed on
this system.
If you continue installation, you will downgrade HiCommand Device Manager.
For example:
1. If 5.0.0(5.0.0-xx) is already installed, you cannot install 4.2.0(4.2.0-xx)
in an update installation.
2. If 4.3.0(4.3.0-xx) is already installed, you cannot install 4.2.0(4.2.0-xx)
in an update installation.

Do you want to continue installation? (Y/N):
```

Figure 4.25 Downgrade Error Message

```
Database Conversion:
To use the new version of HiCommand Device Manager, the database currently
being used must be converted. Database conversion might take a long time.
Select the data conversion method from the following:
1. Convert the database during installation.
2. Convert the database after installation finishes, by using the database
conversion command.
To convert the database during installation, enter [1].
To convert the database after installation, enter [2].
```

Figure 4.26 Database Conversion Message

```
ERROR: An attempt to convert the database has failed.
After installation but before starting HiCommand Device Manager, execute the
database conversion command.
Note: Even if a reinstallation is performed, database conversion is not
performed.
Use the database conversion command to perform database conversion.
```

Figure 4.27 Data Update Error Message

4.2.6 Performing an Upgrade Installation from Version 4.0 or Later or a Re-installation

The database can automatically be backed up or exported during installation. If you want to manually back up or export the database, perform the operations specified in section 4.6.1 or 4.6.3.1. Decide whether to back up or export the database by referring to the following points.

- If version 5.1 or earlier of a HiCommand Suite product is already installed, back up the database. You cannot export the database.
- If version 5.5 or later of a HiCommand Suite product has already been installed and you will perform an upgrade installation, we recommend you export the database.
- If you will perform a re-installation, we recommend you back up the database.

To perform an upgrade installation or re-installation of the HiCommand Device Manager server:

1. Log onto the Solaris or Linux system as **root**.
2. Insert the HiCommand Device Manager CD-ROM. If the CD-ROM is not automatically mounted, mount the CD-ROM to `/mnt/cdrom`.
3. Move the current directory to the directory that stores the installer of Device Manager (`install.sh`). And then, execute the following command:

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

   WARNING: Do not use **Ctrl + C** to stop in the middle of the installation. If you stop the installation, run the **#pkginfo HDVM** command. If the Device Manager information is displayed, uninstall and then re-install the Device Manager Server.
4. A message appears, asking whether the kernel parameters have been set up (see Figure 4.1). If the parameters have not been set up, select **n** to cancel the installation. If the parameters have been set up, select **y** to continue. For details about setup of the kernel parameters, see 4.10 for Solaris, or see section 4.11 for Linux.

   Caution: If the kernel parameters are not set correctly, a message notifies you that the machine must be restarted after the kernel parameters are reset, and installation stops (see Figure 4.2).

   Caution: Figure 4.1 and Figure 4.2 show the output examples in Solaris. In Linux, `kernel parameter` will be replaced with `OS parameter`.
5. When the HiCommand Suite Common Component services are running in a non-cluster environment, a message indicating that the installer will stop these services is displayed. To stop the installation, select **n**. To continue the installation, select **y** (see Figure 4.3).

   If the installer cannot stop all the services of HiCommand Suite Common Component and the HiCommand Suite products, a message indicating that the installer failed to stop the services is displayed (see Figure 4.4). If this message is displayed, choose **y** to try to stop the services again. If the installer still fails to stop the services, cancel the installation, manually stop the services of HiCommand Suite Common Component and the HiCommand Suite products, and then perform the installation again.

6. A message asking whether you want to back up the database (see Figure 4.28) or export the database (see Figure 4.29) is displayed. If you want to back up or export the database, select **y** to start the backup or export. If you do not want to back up or export, select **n** to continue.

   This operation backs up or exports all HiCommand Suite product databases. The following table describes the conditions whether the backup or export is performed, the backup-data storage destination directory, and the disk space required for the directory.

Table 4.7 Storage Destination of Backed up and Exported Data and Required Disk Space

Operation	Performing Conditions	Data Storage Destination Directory	Required Disk Space
Backup	▪ When the version of HiCommand Suite Common Component is 5.1 or earlier ▪ When the version of HiCommand Suite Common Component is 5.5 or later, and performing a re-installation of the same version and revision of HiCommand Device Manager	/var/opt/HiCommand/olddbbackup_hdb	See section 4.6.1.
Export	When the conditions for backing up data are not satisfied	/var/opt/HiCommand/olddbexported_hdb	See section 4.6.3.4.

   Caution: If the data storage destination directory already exists before backing up or exporting, the contents of the data storage destination directory are deleted. Before deletion, a deletion confirmation message (Figure 4.30 or Figure 4.31) is displayed. If you want to save the old data, you need to copy it to another location beforehand, and then choose **y** in the deletion confirmation message.

   Caution Backing up or exporting can fail due to insufficient disk space, or for other reasons. If this occurs, back up or export the databases manually. Then, select **n** to continue installation. For details about how to back up a database, see section 4.6.1. For details about how to export a database, see section 4.6.3.

7. In Solaris, HiCommand Device Manager is displayed as an available package. Press **Enter** to continue.

   Warning: You cannot downgrade Device Manager. If you attempt to do so, an error message will display (see Figure 4.24). However, if the version and revision numbers of the builds before and after a downgrade are the same, the HiCommand Device Manager downgrade message appears.

8. The license agreement displays. Select **y** to continue.
9. In a non-cluster environment, a message asking whether you want to start the HiCommand Suite product services after installation is complete is displayed (see Figure 4.16). If you want to start the services after installation is complete, choose **y**. The services of HiCommand Suite Common Component and HiCommand Suite products will then be started after installation is complete. If you do not want to start the services after installation is complete, choose **n**.

   Caution: The services of HiCommand Suite products whose versions are earlier than 5.7 are not started by choosing **y**. If you want to start the services of HiCommand Suite products after installation is complete, manually start the services. For details about how to start these services, see the manual for your product version.

   Important: To continue setup in a cluster environment after installation is complete, choose **n**.
10. The SNMP Trap message displays (see Figure 4.6). Verify that you have no other software products using port 162, then press **Enter**.
11. The Secure Socket Certificates Note panel (see Figure 4.19) displays. Press **Enter** to continue.
12. A message displays indicating that the installation completed successfully.
13. Refresh all the registered subsystems to update the database.

Note: If the installer ends with an error, follow the instructions on the error message and re-install HiCommand Device Manager. If the **pkginfo HDVM** command displays the package information, first uninstall and then re-install HiCommand Device Manager.

```
Device Manager will back up the database to the following directory during
installation:
/var/opt/HiComamnd/olddbbackup_hdb
Do you want to backup the database now? [y/n]
```

Figure 4.28 Selection Message for Backing Up the Database

```
Device Manager will export the database to the following directory during
installation:
/var/opt/HiComamnd/olddbexported_hdb
It takes time to export. Do you want to export the database now? [y/n]
```

Figure 4.29 Selection Message for Exporting the Database

```
Installer will backup the database to /var/opt/HiCommand/olddbbackup_hdb.
If this file exists, it will be replaced with a new backup file.
Do you want to continue? [y/n]
```

Figure 4.30 Backup Directory Deletion Confirmation Message

```
Before exporting the database, the following directory will be erased:
 /var/opt/HiCommand/olddbexported_hdb.
Do you want to continue? [y/n]
```

Figure 4.31 Export Directory Deletion Confirmation Message

4.3 Installing Device Manager in a Cluster Server Environment

Caution: HiCommand Device Manager Server only supports Solaris cluster environments.

The HiCommand Device Manager server can provide higher availability in a cluster environment. This section discusses the requirements and settings for a supported cluster environment.

If you want to install the Device Manager server in an environment in which other HiCommand Suite products are already installed in a cluster configuration, you need to make preparations such as canceling the cluster configuration. For details about the necessary preparations, see section 4.3.2. Also, you can change the environment in which the Device Manager system is already operating from a non-cluster configuration to a cluster configuration. For details, see section 4.3.6.

4.3.1 System Requirements

The requirements for a cluster environment are as follows:

- Platform: Solaris 9 (32-bit or 64-bit kernel mode)
- Cluster software: VERITAS Cluster Server 3.5 or Sun Cluster 3.1
- Number of nodes: 2
- Cluster configuration: Active-standby configuration

Caution: During installation, there is a step to back up and migrate the databases. Make sure that you secure the free disk space for backup and migration before installation. For the disk space required to back up, see section 4.6.1. The target disk (that is placed on the shared disk or local disk) to which the database is to be migrated must have the same free disk space or more as the database of the migration source.

Caution: To change the Device Manager settings after installation, specify the same settings for all nodes.

4.3.2 Preparations for Installing HiCommand Device Manager in an Environment Where Other HiCommand Suite Products Are Running

This section describes preparations required before installing Device Manager in an environment in which other HiCommand Suite products are running in a cluster configuration. In this procedure, the cluster configuration for other HiCommand Suite products is temporarily cancelled.

Caution: When you execute the `hcmdsdbmove` command or `hcmdsdbremake` command that is used in this procedure, the setting of the port that HiRDB uses will be restored to the default (23032). If you changed the port number from the default to another number, take a note of the port number that is being used so that you can set it again later.

Important: When you execute this command, it will change the port used by HiRDB to its default (23032). If you are using a port other than the default, you must change it back.

1. Remove the services for all other HiCommand Suite products and the HiRDB service from the cluster monitoring target.
2. If you are using VERITAS Cluster Server:
   - Start Cluster Manager on the Java Console.
   - For each HiCommand Suite service, do the following:

     Place the service offline by right-clicking the service and then clearing **Enabled** from the menu.

     In the Cluster Explorer window, select the **Service Groups** tab, then select the group in which the HiCommand Suite product service has been registered.

     Right-click the service, and select **Freeze** and then **Temporary**.
3. If you are using Sun Cluster Server:
   - Disable the resource monitoring for each HiCommand Suite product service:

     # /usr/cluster/bin/scswitch -n -M -j resource-name
   - Disable the resources for each HiCommand Suite product service:

     # /usr/cluster/bin/scswitch -n -j resource-name
4. Stop the services of all HiCommand Suite products in both the executing and standby nodes.

   For details about how to stop these services, see the manual for your product version.
5. Stop the Common Component in both the executing and standby nodes:

   # /opt/HiCommand/Base/bin/hcmdssrv -stop
6. Switch, to the executing node, each group in which the HiCommand Suite product service has been registered.
7. If you are using VERITAS Cluster Server, switch each group where a HiCommand Suite product service has been registered into the standby system, as follows:
   - In the Cluster Explorer window, select the **Service Groups** tab.
   - For each group in which the HiCommand Suite product service has been registered, do the following:

     Right-click the group, then select **Unfreeze** from the pop-up menu.

     Right-click the group, then select **Switch To** and then select the host name of the executing node.

     Right-click the group. Select **Freeze** and then **Temporary** from the pop-up menu.
8. If you are using Sun Cluster, switch each group where a HiCommand Suite product service has been registered into the standby system, as follows:

   # /usr/*cluster*/bin/scswitch -z -g group-name -h host-name
9. Start HiRDB on the executing node.
   - Start HiRDB:

     # /opt/HiCommand/Base/bin/hcmdsdbsrv -start
10. Execute the command below to back up the database.

For details about the options and a caution for backing up, see section 4.6.1.

```
# /opt/HiCommand/Base/bin/hcmdsbackups -dir target-directory-for-storing-backup-files
```

The following shows an example of executing the command:

```
# /opt/HiCommand/Base/bin/hcmdsbackups -dir /opt/db_bkup01
```

11. On the executing node, back up the database contents.

    Delete or empty *target-directory-for-outputting-data*, and then execute the following command:

    # /opt/HiCommand/Base/bin/hcmdsdbmove -export -datapath target-directory-for-outputting-data

    The following shows an example of executing the command:

    # /opt/HiCommand/Base/bin/hcmdsdbmove -export -datapath /opt/storing_data

    The following describes the `datapath` option:

    `datapath`

    Specify the directory to which you want to output the database contents. After this option name, specify the absolute path of a directory on the local disk. Note that the path name must not exceed 63 bytes. If the directory has already been created, empty the directory.

    The characters that can be used to specify the path are shown below. In addition to these characters, a forward slash (`/`) can be used as path delimiters. You cannot use a space in the path.

    `A-Z`, `a-z`, `0-9`, period (`.`), underscore (`_`)

    Caution: You must not execute multiple instances of this command concurrently. Also, you must not execute this command and the `hcmdsgetlogs` command concurrently.

12. On the executing node, re-create the database system on the local disk.

    Execute the following command:

    ```
    # /opt/HiCommand/Base/bin/hcmdsdbremake -databasepath target-directory-for-re-creating-database
    ```

    The following shows an example of executing the command:

    ```
    # /opt/HiCommand/Base/bin/hcmdsdbremake -databasepath /root/re_creating_db
    ```

    The following describes the `databasepath` option:

    `databasepath`

    Specify the directory in which you want to re-create the database. After this option name, specify the absolute path of an already created directory on the local disk. Note that the path name must not exceed 63 bytes.

    The characters that can be used to specify the path are shown below. In addition to these characters, a forward slash (`/`) can usually be used as path delimiters. However, you must not specify a forward slash (`/`) at the end of the path, as a path delimiter. You cannot use a space in the path.

    `A-Z`, `a-z`, `0-9`, period (`.`), underscore (`_`)

13. Register the database contents backed up in step 11 into the re-created database.

Execute the command below. For *target-directory-for-inputting-data*, specify the absolute path of *target-directory-for-outputting-data* specified in step 11.

```
# /opt/HiCommand/Base/bin/hcmdsdbmove -import -datapath target-directory-for-inputting-data
```

The following shows an example of executing the command:

```
# /opt/HiCommand/Base/bin/hcmdsdbmove -import -datapath /opt/storing_data
```

Caution: You must not execute multiple instances of this command concurrently. Also, you must not execute this command and the `hcmdsgetlogs` command concurrently.

14. Copy *target-directory-for-outputting-data*, in which data was stored in step 11, onto the local disk of the standby node.

    A new directory created by this copy operation must satisfy the following conditions (so that the directory can be specified in the `hcmdsdbmove` command execution):

    - Absolute path for the copy target directory: no more than 63 bytes
    - Available characters for the copy target directory: `A` to `Z`, `a` to `z`, `0` to `9`, period (`.`), and underscore (`_`).

15. Switch, to the standby node, each group in which the HiCommand Suite product service has been registered.

16. On the standby node, re-create the database system on your local disk.

    Execute the following command:

    # /opt/HiCommand/Base/bin/hcmdsdbremake -databasepath target-directory-for-recreating-database

    The following shows an example of executing the command:

    # /opt/HiCommand/Base/bin/hcmdsdbremake -databasepath /root/re_creating_db

    The following describes the `databasepath` option:

    `databasepath`

    Specify the directory in which you want to re-create the database. After this option name, specify the absolute path of an already created directory on the local disk. Note that the path name must not exceed 63 bytes.

    The characters that can be used to specify the path are shown below. In addition to these characters, a forward slash (`/`) can usually be used as path delimiters. However, you must not specify a forward slash (`/`) at the end of the path, as a path delimiter. You cannot use a space in the path.

    `A-Z`, `a-z`, `0-9`, period (`.`), underscore (`_`)

17. On the standby node, register the database contents into the re-created database.

    Execute the command below. For *target-directory-for-inputting-data*, specify the absolute path of the directory copied from the executing node in step 10.

```
# /opt/HiCommand/Base/bin/hcmdsdbmove -import -datapath target-directory-for-inputting-data
```

    The following shows an example of executing the command:

```
# /opt/HiCommand/Base/bin/hcmdsdbmove -import -datapath /opt/storing_data
```

    Caution: You must not execute multiple instances of this command concurrently. Also, you must not execute this command and the `hcmdsgetlogs` command concurrently.

18. On the executing or standby node, if HiCommand Suite Common Component is running, execute the following command to stop it:

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

19. If you changed the port number used by HiRDB from the default to another number, set the port number again on both the executing node and standby node.

    For details about how to set the port number, see section 5.4.2.

4.3.3 Performing a New Device Manager Installation

After finishing a new installation, be sure to back up the Device Manager server database.

Caution: Before starting installation, perform the following steps:

- If the cluster management IP address and shared disk are not enabled on the executing node, perform steps 5 to 8 in section 4.3.3.5 or steps 1 to 3 in section 4.3.3.6 to place the resources of the cluster management IP address and shared disk online.
- If other HiCommand Suite products are already running in a cluster environment, make preparations such as canceling the cluster configuration. For details about the necessary preparations, see section 4.3.2.

4.3.3.1 Installing and Configuring the Executing Node

Caution: While performing cluster configuration, do not access HiCommand Device Manager.

1. On the executing node (see section 4.2.3 if you need instructions). Note the following requirements:
   - Leave the settings specifying the location of the databases for the Common Component and the Device Manager Server as the default values (see Figure 4.8 and Figure 4.9).
   - For the IP address of the Device Manager Server, specify a logical host name(see Figure 4.10).

     Important: A logical host name indicates the name of a virtual host allocated to the cluster management IP address, which must be enabled and accessible.
2. After the Device Manager Server is installed on the executing node, use the Web Client to enter the license key. For further information on the Device Manager Web Client, please see the *HiCommand Device Manager Web Client User's Guide*.

   Note: You should have received a CD that contains the HiCommand Device Manager License Key. Upload the License Key file to a directory on the same server where Device Manager will be installed. That way you can select the button next to **License File** and browse for the License Key file. Once the file is found simply highlight the file and select the **Open** button. This will update Device Manager with the permanent License Key.
3. Use a text editor to create a cluster configuration file, and specify the following items:
   - mode: Specify `online`.
   - virtualhost: the logical host name.

- onlinehost: the executing node host name.
- standbyhost: the standby node host name.

The following shows a coding example in the cluster-configuration file:

```
mode = online
virtualhost = hcmdserver
onlinehost = hcmdserver_1
standbyhost = hcmdserver_2
```

4. Save the created file as **cluster.conf** in /opt/HiCommand/Base/conf.

   Caution: An IP address cannot be specified for `virtualhost`, `onlinehost`, or `standbyhost`. Make sure that the IP address can be resolved from the host name. An IP address that is enabled and accessible must be assigned to the logical host name to be specified in `virtualhost`.

5. If HiCommand Suite products whose versions are earlier than 5.7 have been installed, stop their services.

   For details about how to stop these services, see the manual for your product version.

6. If HiCommand Suite Common Component is running, stop the services of HiCommand Suite Common Component and all HiCommand Suite products, and then start HiRDB.

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

7. Execute the command below to back up the database.

   For details about the options and a caution for backing up, see section 4.6.1.

```
hcmdsbackups -dir target-directory-for-storing-backup-files
```

   The following shows an example of executing the command:

```
# /opt/HiCommand/Base/bin/hcmdsbackups -dir /opt/db_bkup01
```

8. Migrate the database to the shared disk.

   Delete or empty *target-directory-for-storing-data*, and then execute the following command. When this command is executed, the setting of the port that HiRDB uses will be restored to the default (23032). If you changed the port number from the default to another number, take a note of the port number that is being used so that you can set it again later.

   # /opt/HiCommand/Base/bin/hcmdsdbclustersetup -createcluster -databasepath target-directory-for-re-creating-database -exportpath target-directory-for-storing-data -auto

   The following shows an example of executing the command:

   # /opt/HiCommand/Base/bin/hcmdsdbclustersetup -createcluster -databasepath /root/re_creating_db -exportpath /opt/storing_data -auto

   The following describes the options specified in the `hcmdsdbclustersetup` command.

   `databasepath`

   Specify the directory in which you want to re-create the database. After this option name, specify the absolute path of a directory on a shared disk. Note that the path name must not exceed 63 bytes.

The characters that can be used to specify the path are as follows. In addition to these characters, a forward slash (/) can be used as path delimiters. You cannot use a space in the path.

A-Z, a-z, 0-9, period (.), underscore (_)

exportpath

Specify the directory in which you want to store backup data. After this option name, specify the absolute path of a directory on the local disk. Note that the path name must not exceed 63 bytes. If the directory has already been created, delete its contents. The characters that can be used to specify the path are the same as for databasepath.

auto

Specify this option to stop the HiCommand Suite product services and to start HiRDB automatically as preparation for processing the database. After the command is executed, the HiCommand Suite product services and HiRDB are stopped. Note that the services of HiCommand Suite products whose versions are earlier than 5.7 are not stopped automatically.

Caution: You must not execute multiple instances of this command concurrently. Also, you must not execute this command and the hcmdsgetlogs command concurrently.

Caution: For details about how to set the port that HiRDB uses, see section 5.4.2.

9. If HiCommand(R) Suite Common Component is running, execute the following command to stop it.

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

   Note: Do not stop the common component service while another HiCommand Suite common component service is running.

10. Set the Common Component so that it does not start automatically when the machine starts:

    # /opt/HiCommand/Base/bin/hcmdssrv -starttype manual -all

11. Set the Device Manager server so that it does not start automatically when the machine starts, either by moving the following file to another directory, or by changing its file name.

    Important: the new file name should not begin with either k or s:

    /etc/rc3.d/S99hicommand

4.3.3.2 Installing and Configuring on the Standby Node

1. Install Device Manager on the executing node (see section 4.2.3 if you need instructions). Note the following requirements:
   - Leave the settings specifying the location of the databases for the Common Component and the Device Manager Server as the default values. (see Figure 4.8 and Figure 4.9)
   - For the IP address of the Device Manager Server, specify a logical host name. (see Figure 4.10) A logical host name indicates the name of a virtual host allocated to the cluster management IP address, which must be enabled and accessible.

2. After the Device Manager Server is installed on the standby node, use the Web Client to enter the license key.

   Note: You should have received a CD that contains the HiCommand Device Manager License Key. Upload the License Key file to a directory on the same server where Device Manager will be installed. That way you can select the button next to **License File** and browse for the License Key file. Once the file is found, highlight the file and select the **Open** button. This will update Device Manager with the permanent License Key.

3. Use the IP address of the standby node to access the Device Manager Server.

4. Use a text editor to create a cluster configuration file, and specify the following items:

   - **mode:** Specify `standby`.
   - **virtualhost:** the logical host name.
   - **onlinehost:** the executing node host name.
   - **standbyhost:** the standby node host name.

5. Save the created file as **cluster.conf** in **/opt/HiCommand/Base/conf**.

   Caution: You cannot specify an IP address for virtualhost, onlinehost, or standbyhost. Confirm that the IP address can be resolved from the host name.

6. If HiCommand Suite products whose versions are earlier than 5.7 have been installed, stop their services.

   For details about how to stop these services, see the manual for your product version.

7. Set the database system on the shared disk as the one to be referenced.

   After deleting or emptying *target-directory-for-storing-data*, execute the following command. When this command is executed, the setting of the port that HiRDB uses will be restored to the default (23032). If you changed the port number from the default to another number, take a note of the port number that is being used so that you can set it again later.

   # /opt/HiCommand/Base/bin/hcmdsdbclustersetup -createcluster -databasepath target-directory-for-re-creating-database -exportpath target-directory-for-storing-data -auto

   The following shows an example of executing the command:

   # /opt/HiCommand/Base/bin/hcmdsdbclustersetup -createcluster -databasepath /root/re_creating_db -exportpath /opt/storing_data -auto

   The following describes the options specified in the `hcmdsdbclustersetup` command.

   `databasepath`

   Specify the directory in which you want to re-create the database. After this option name, specify the absolute path of the same directory as *target-directory-for-re-creating-database* specified for the executing node. This directory must be located on a shared disk, and the absolute path must not exceed 63 bytes.

   The characters that can be used to specify the path are as follows. In addition to these characters, a forward slash (`/`) can be used as path delimiters. You cannot use a space in the path.

   `A-Z`, `a-z`, `0-9`, period (`.`), underscore (`_`)

`exportpath`

Specify the directory in which you want to store backup data. After this option name, specify the absolute path of a directory on the local disk. Note that the path name must not exceed 63 bytes. If the directory has already been created, delete its contents. The characters that can be used to specify the path are the same as for `databasepath`.

`auto`

Specify this option to stop the HiCommand Suite product services and to start HiRDB automatically as preparation for processing the database. After the command is executed, the HiCommand Suite product services and HiRDB are stopped. Note that the services of HiCommand Suite products whose versions are earlier than 5.7 are not stopped automatically.

Caution: You must not execute multiple instances of this command concurrently. Also, you must not execute this command and the `hcmdsgetlogs` command concurrently.

Caution: For details about how to set the port that HiRDB uses, see section 5.4.2.

Deploy the directory in which the database is to be re-created on the shared disk.

8. If HiCommand Suite Common Component is running, execute the following command to stop it.

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

   Note: Do not stop the common component service while another HiCommand Suite common component service is running.

9. Perform setup so that the Common Component service does not start automatically when the machine starts, using the following command:

   # /opt/HiCommand/Base/bin/hcmdssrv -starttype manual -all

10. Set the Device Manager server so that it does not start automatically when the machine starts, either by moving the following file to another directory, or by changing its file name.

    /etc/rc3.d/S99hicommand.

    Important: the new file name should not begin with either k or s.

4.3.3.3 Creating Scripts for VERITAS Cluster Server

Note: If you are using Sun Cluster Server, skip this section and go to section 4.3.3.4.

1. After installing and setting up HiCommand Device Manager on the executing node and standby node, you must create the script for HiRDB on both nodes.
2. Create the dummy file for monitoring the HiRDB service from VERITAS Cluster Server.
   - File name: **/opt/HiCommand/Base/HDB/.pdveritas**
   - Details: This is an empty file.
3. Create the script that defines the resource types for the HiRDB service.
   - File name: **/etc/VRTSvcs/conf/config/HiRDB_STypes.cf**
   - Details: Create a file containing the following:

```
type HiRDB_S (
static str ArgList[] = { PdDir, PdConfPath, Ld_Library_Path, DummyFilePath }
str PdDir
str PdConfPath
str Ld_Library_Path
str DummyFilePath)
```

4. Define the agent for HiRDB.

   # mkdir /opt/VRTSvcs/bin/HiRDB_S
   # cp /opt/VRTSvcs/bin/ScriptAgent /opt/VRTSvcs/bin/HiRDB_S/HiRDB_SAgent

5. Create the script that is used to put the HiRDB service online.
   - File name: **/opt/VRTSvcs/bin/HiRDB_S/online**
   - Details: Create a file containing the following:

```
#!/bin/sh
PATH=/sbin:/usr/bin:/usr/sbin:/etc:/bin:/opt/VRTSvcs/bin:"$2"/bin
export PATH
PDDIR="$2"
PDCONFPATH="$3"
LD_LIBRARY_PATH="$4"
export PDDIR PDCONFPATH LD_LIBRARY_PATH
$PDDIR/bin/pdstart
/bin/touch "$5"
/bin/chmod 0400 "$5"
```

6. Create the script that is used to place the HiRDB service offline.
   - File name: **/opt/VRTSvcs/bin/HiRDB_S/offline**
   - Details: Create a file containing the following:

```
#!/bin/sh
PATH=/sbin:/usr/bin:/usr/sbin:/etc:/bin:/opt/VRTSvcs/bin:"$2"/bin
export PATH
PDDIR="$2"
PDCONFPATH="$3"
LD_LIBRARY_PATH="$4"
export PDDIR PDCONFPATH LD_LIBRARY_PATH
$PDDIR/bin/pdstop -f -q
/bin/rm -f "$5"
```

7. Create the script that is used to monitor the HiRDB service.
   - File name: **/opt/VRTSvcs/bin/HiRDB_S/monitor**
   - Details: Create a file containing the following:

```
#!/bin/sh
if /bin/test -f "$5"
then
  exit 110
else
  exit 100
fi
```

8. Assign execution permissions to the created scripts.
   - **# chmod u+x /opt/VRTSvcs/bin/HiRDB_S/online**
   - **# chmod u+x /opt/VRTSvcs/bin/HiRDB_S/offline**
   - **# chmod u+x /opt/VRTSvcs/bin/HiRDB_S/monitor**

4.3.3.4 Creating Scripts for Sun Cluster

After installing and setting up HiCommand Device Manager on the executing node and standby node, you must create the script for registering Common Component service in the cluster on both nodes.

Create the following six script files:

1. Create the script for HBase Storage Management Web Service.
   - File name: **/etc/init.d/sc_hicommand-CWS**
   - Details: Create a file containing the following:

```
#!/bin/sh
#
# Sample sc_hicommand-CWS
#
# Usage: sc_hicommand-CWS [start|stop|status]
#
# This Script executes /etc/init.d/hicommand-CWS internally.
ALIVE_VALUE=0
DOWN_VALUE=1
exec_cmd() {
    echo `date "+%y/%m/%d %H:%M:%S " `"exec    : $*"
    # Execute Command with operand
    $*
    # Set return value to RC
    RC=$?
    echo `date "+%y/%m/%d %H:%M:%S " `"exec-end: $*  (RC=$RC)"
    if [ $RC -ne 0 ]; then
        if [ $RC -ne 1 ]; then
                exit $RC
        fi
    fi
}

# Switch operation according to the first operand of this shell.
case $1 in
start)
```

```
    exec_cmd "/etc/init.d/hicommand-CWS start"
    ;;
stop)
    exec_cmd "/etc/init.d/hicommand-CWS stop"
    ;;
status)
    /etc/init.d/hicommand-CWS status
    # The result is equal to 1
    if [ $? -eq 1 ]; then
        # running
        RET_CODE=$ALIVE_VALUE
    else
        # not running
        RET_CODE=$DOWN_VALUE
    fi
    exit $RET_CODE
    ;;
*)
    echo "Invalid argument"
    exit 1
esac

exit 0
```

2. Create a script for the HBase Storage Mgmt Common Service.
   - File name: **/etc/init.d/sc_hicommand-SSOS**
   - Details: Create a file containing the following:

```
#!/bin/sh
#
# Sample sc_hicommand-SSOS
#
# Usage: sc_hicommand-SSOS [start|stop|status]
#
# This Script executes /etc/init.d/hicommand-SSOS internally.
ALIVE_VALUE=0
DOWN_VALUE=1

exec_cmd() {
    echo `date "+%y/%m/%d %H:%M:%S " `"exec    : $*"
    # Execute Command with operand
    $*
    # Set return value to RC
    RC=$?
    echo `date "+%y/%m/%d %H:%M:%S " `"exec-end: $*  (RC=$RC)"
    if [ $RC -ne 0 ]; then
        if [ $RC -ne 1 ]; then
                exit $RC
        fi
    fi
}
# Switch operation according to the first operand of this shell.
case $1 in
start)
    exec_cmd "/etc/init.d/hicommand-SSOS start"
    ;;
stop)
    exec_cmd "/etc/init.d/hicommand-SSOS stop"
    ;;
status)
    /etc/init.d/hicommand-SSOS status
    # The result is equal to 1
    if [ $? -eq 1 ]; then
```

```
        # running
        RET_CODE=$ALIVE_VALUE
    else
        # not running
        RET_CODE=$DOWN_VALUE
    fi
    exit $RET_CODE
    ;;
*)
    echo "Invalid argument"
    exit 1
esac

exit 0
```

3. Create a script for starting HiRDB.
   - File name: **/etc/init.d/hirdb_start**
   - Details: Create a file containing the following:

```
#!/bin/sh
PATH=/usr/sbin:/usr/bin:$PDDIR/bin:.:/usr/cluster/bin
export PATH
PDDIR=/opt/HiCommand/Base/HDB
PDCONFPATH=$PDDIR/conf
LD_LIBRARY_PATH=$PDDIR/lib
PDHOST=logical-host-name
export PDDIR PDCONFPATH LD_LIBRARY_PATH PDHOST

$PDDIR/bin/pdstart

/etc/init.d/hirdb_monitor
```

4. Create a script for stopping HiRDB.
   - File name: **/etc/init.d/hirdb_stop**
   - Details: Create a file containing the following:

```
#!/bin/sh

PATH=/usr/sbin:/usr/bin:$PDDIR/bin:.:/usr/cluster/bin
export PATH
PDDIR=/opt/HiCommand/Base/HDB
PDCONFPATH=$PDDIR/conf
LD_LIBRARY_PATH=$PDDIR/lib
PDHOST=logical-host-name
export PDDIR PDCONFPATH LD_LIBRARY_PATH PDHOST

$PDDIR/bin/pdstop -f -q
```

5. Create a script for monitoring HiRDB.
   - File name: **/etc/init.d/hirdb_probe**
   - Details: Create a file containing the following:

```
#!/bin/sh

ps -ef | grep root | grep pdprcd | awk -F' ' '{print $8}' | grep pdprcd
if [ $? = 0 ];then
    echo "exit 0"
    exit 0
else
    echo "exit 1"
    exit 1
fi
```

6. Create a HiRDB resident script.
   - File name: **/etc/init.d/hirdb_monitor**
   - Details: Create a file containing the following:

```
#!/bin/sh

trap exit 5
while true
do
  sleep 5
done
exit
```

7. After creating the scripts, assign execution permissions to the scripts using the following command:

   # chmod u+x script-file-name

4.3.3.5 Setting Up the Cluster Resource for VERITAS Cluster Server

If you are using Sun Cluster Server, skip this section and go to section 4.3.3.6.

To set the cluster resources, do the following operation on the executing node or the standby node:

1. In Java Console, start Cluster Manager.
2. Open the VERITAS Cluster Server configuration file so that you can edit the file. From the **File** menu, choose **Open Configuration**.
3. Import the file created in section 4.3.3.3. From the **File** menu, choose **Import Types**.
4. Select the **/etc/VRTSvcs/conf/config/HiRDB_STypes.cf** file, and then choose **Import**.

5. If there is no group to which other HiCommand Suite products are registered, create the service group. In the **Edit** menu, select **Add** and then **Service Group**.

   Caution: Use only resources related to HiCommand Suite products to configure the resource group.

   - In Service Group Name, enter **HiCommand**.
   - Move both the executing and standby nodes from **Available Systems** to **Systems for Service Group**.
   - Select **OK**.

6. In the **Add New Resource** dialog box, from **Resource Type** choose **IP**, and then register the IP address (cluster management IP address) used to access the Device Manager Server.
7. Register a shared disk into the HiCommand group: In the **Add New Resource** dialog box, from **Resource Type** choose **Disk Reservation** to register device files on the shared disk. Enter **SharedDisk** for the resource name.
8. Register a mount point: In the **Add New Resource** dialog box, from **Resource Type** choose **Mount** to register the mount point on the shared disk. Enter **MountPoint** for the resource name.
9. In the **Edit** menu, select **Add** and then **Resource** to display the **Add Resource** panel.
10. Register HiRDB as a resource, as follows:
    - Resource Name: **HiRDB** (optional)
    - Resource Type: **HiRDB_S**
    - PdDir: **/opt/HiCommand/Base/HDB**
    - PdConfPath: **/opt/HiCommand/Base/HDB/conf**
    - Ld_Library_Path: **/opt/HiCommand/Base/HDB/lib**
    - DummyFilePath: **/opt/HiCommand/Base/HDB/.pdVERITAS**
    - Critical: **false**
11. Register the HBase Storage Mgmt Common Service as a resource, as follows:
    - Resource Name: **MgmtComService** (optional)
    - Resource Type: **Application**
    - Start Program Attribute: **Scalar Values:/etc/init.d/hicommand-SSOS start**
    - Stop Program Attribute: **Scalar Values:/etc/init.d/hicommand-SSOS stop**
    - PidFiles Attribute: **/var/opt/HiCommand/Base/tmp/HiCommand.pid**
12. Register the HBase Storage Mgmt Web Service as a resource, as follows:
    - Resource Name: **MgmtWebService** (optional)
    - Resource Type: **Application**
    - Start Program Attribute: **Scalar Values:/etc/init.d/hicommand-CWS start**
    - Stop Program Attribute: **Scalar Values:/etc/init.d/hicommand-CWS stop**
    - PidFiles Attribute: **/var/opt/HiCommand/Base/httpsd/logs/httpd.pid**

13. Register the Device Manager Server as a resource, as follows:
    - Resource Name: **HiCommandServer** (optional)
    - Resource Type: **Application**
    - Start Program Attribute: **Scalar Values:/etc/init.d/hicommand start**
    - Stop Program Attribute: **Scalar Values:/etc/init.d/hicommand stop**
    - Monitor Processes Attribute:
      Vector Values:/bin/sh /opt/HiCommand/HiCommandServer/hicmdserver

    Caution: If HiCommand Suite Common Component is forcibly stopped for any reason, some temporary files will be left undeleted. If these files are on the standby node, even if HiCommand Suite Common Component has stopped, a message indicating that HiCommand Suite Common Component cannot be placed offline is output to the VERITAS Cluster Server log. Even though this error message is output, there is no problem with the Device Manager server operation.

    To prevent the error message from being output, make sure the Common Component is not running by executing the following command:

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

    Then do the following:
    - Delete **HiCommand.pid** from the **/var/opt/HiCommand/Base/tmp** directory
    - Delete **httpd.pid** from the **/var/opt/HiCommand/Base/httpsd/logs** directory
14. Set up the resource dependency in the HiCommand group in the following order. The lower resource depends on the upper resources:
    - Device files on the shared disk
    - Mount point on the shared disk and IP address
    - HiRDB
    - HiCommand Storage Mgmt Common Service
    - HiCommand Storage Mgmt Web Service
    - HiCommandServer

    The above resource names are represented by the resource names registered from step 10 to step 13.
15. From the File menu, choose **Save Configuration.**
16. From the File menu, choose **Close Configuration.**
17. Apply the resource, and then close Cluster Manager.

4.3.3.6 Setting Up the Cluster Resource for Sun Cluster

To register resources for Sun Cluster, use the **scrgadm** command. For more information, see the Sun Cluster documentation.

Execute the following operation on the executing node or standby node:

1. If there is no group to which other HiCommand Suite products are registered, create a resource group:
   - Group name: **HiCommand**
   - Node: A host name of the executing node and host name of the standby node.
   - Sample command: **# /usr/cluster/bin/scrgadm -a -g HiCommand -h <executing node host name>,<standby node host name>**

   Caution: Use only resources related to HiCommand Suite products to configure the resource group.
2. Register the shared disk as a resource:
   - Resource type: **SUNW.HAStoragePlus**
   - Resource name: **SharedDisk**
3. Register a logical host name as a resource:
   - Resource name: **hdvm_ip**
4. Register HiRDB as a resource:
   - Resource type: **SUNW.gds**
   - Resource name: **HiRDB** (optional)
   - Related network: **hdvm_ip**
   - Resources on which HiRDB depends: **SharedDisk**
   - Start command for the service: **/etc/init.d/hirdb_start**
   - Stop command for the service: **/etc/init.d/hirdb_stop#**
   - Monitoring command for the service: **/etc/init.d/hirdb_probe#**
   - Port number to be used: **23032/tcp**

Note: For the service startup, stop and monitoring commands, register the script created in section 4.3.3.4, as follows:

```
# /usr/cluster/bin/scrgadm -a -j HiRDB -g HiCommand -t SUNW.gds
  -y Network_resources_used=hdvm_ip
  -y Resource_dependencies=SharedDisk
  -x Start_command="/etc/init.d/hirdb_start"
  -x Stop_command="/etc/init.d/hirdb_stop"
  -x Probe_command="/etc/init.d/hirdb_probe"
  -y Port_list="23032/tcp"
```

5. Register HBase Storage Mgmt Common Service as a resource:
   - Resource type: **SUNW.gds**
   - Resource name: **MgmtComService** (optional)
   - Related network: **None**
   - Resources on which HBase Storage Mgmt Common Service depends: **HiRDB**
   - Start command for the service: **/etc/init.d/sc_hicommand-SSOS start**
   - Stop command for the service: **/etc/init.d/sc_hicommand-SSOS stop**
   - Monitoring command for the service: **/etc/init.d/sc_hicommand-SSOS status**
   - Port number to be used: **23017/tcp**

Note: /etc/init.d/sc_hicommand-SSOS must be created in advance. For more information see section 4.3.3.4.

Sample command:

```
# /usr/cluster/bin/scrgadm -a -j MgmtComService -g HiCommand
  -t SUNW.gds-y Resource_dependencies=HiRDB
  -x Start_command="/etc/init.d/sc_hicommand-SSOS start"
  -x Stop_command="/etc/init.d/sc_hicommand-SSOS stop"
  -x Probe_command="/etc/init.d/sc_hicommand-SSOS status"
  -y Port_list="23017/tcp"
```

6. Register HBase Storage Mgmt Web Service as a resource:
   - Resource type: **SUNW.gds**
   - Resource name: **MgmtWebService** (optional)
   - Related network: **hdvm_ip**
   - Resources on which HBase Storage Mgmt Web Service depends: **MgmtComService**
   - Start command for the service: **/etc/init.d/sc_hicommand-CWS start**
   - Stop command for the service: **/etc/init.d/sc_hicommand-CWS stop**
   - Monitoring command for the service: **/etc/init.d/sc_hicommand-CWS status**
   - Port number to be used:
     - Other than SSL: 23015/tcp
     - For SSL: **23016/tcp**

Note: /etc/init.d/sc_hicommand-CWS must be created in advance. For more information, see section 4.3.3.4.

Sample command:

```
# /usr/cluster/bin/scrgadm -a -j MgmtWebService -g HiCommand -t SUNW.gds
  -y Network_resources_used=hdvm_ip
  -y Resource_dependencies=MgmtComService
  -x Start_command="/etc/init.d/sc_hicommand-CWS start"
  -x Stop_command="/etc/init.d/sc_hicommand-CWS stop"
  -x Probe_command="/etc/init.d/sc_hicommand-CWS status"
  -y Port_list="23015/tcp"
```

7. Register HiCommandServer as a resource:
   - Resource type: **SUNW.gds**
   - Resource name: **HiCommandServer** (optional)
   - Related network: **hdvm_ip**
   - Resources on which HiCommandServer depends: **MgmtWebService**
   - Start command for the service: **/etc/init.d/hicommand start**
   - Stop command for the service: **/etc/init.d/hicommand stop**
   - Monitoring command for the service: **/etc/init.d/hicommand status2**
   - Port number to be used:
     - Not for SSL: **2001/tcp**
     - For SSL: **2443/tcp**

   Sample command:

```
# /usr/cluster/bin/scrgadm -a -j HiCommandServer -g HiCommand -t SUNW.gds
  -y Network_resources_used=hdvm_ip
  -y Resource_dependencies=MgmtWebService
  -x Start_command="/etc/init.d/hicommand start"
  -x Stop_command="/etc/init.d/hicommand stop"
  -x Probe_command="/etc/init.d/hicommand status2"
  -y Port_list=2001/tcp
```

4.3.4 Performing an Upgrade Installation from Version 3.5 or Earlier

This section describes how to upgrade the Device Manager version 3.5 or earlier in a VERITAS Cluster Server configuration to Device Manager 4.0 or later.

After finishing an upgrade installation, be sure to back up the HiCommand Device Manager server database.

Caution: Before starting installation, perform the following steps:

- When **/opt/HiCommand/Base/conf/init.conf** has been changed, if you want to upgrade the HiCommand(R) Device Manager server version 3.0 or 3.1 to 3.5 or later, create **/opt/HiCommand/Base/conf/user.conf**, and write any changes in **init.conf** into the created **user.conf**.
- Upgrade VERITAS Cluster Server to version 4.0.
- If Device Manager and other HiCommand Suite products are already running in a cluster environment, make preparations such as canceling the cluster configuration. For details about the necessary preparations, see section 4.3.2.

4.3.4.1 Preparations in VERITAS Cluster Server

To prepare VERITAS Cluster Server in advance, execute the following operation on the executing node or standby node:

1. In Java Console, start the VERITAS Cluster Manager.

2. In the Cluster Explorer panel, select the **Service Groups** tab.
3. Take each of the following services offline, by selecting each of the following services, right-clicking to display a menu, selecting **Offline**, and then select the host name of the executing node or the standby node
   - HiCommand Server
   - HBase Storage Mgmt Web Service
   - HBase Storage Mgmt Common Service

   The above services are represented by the resource names registered in section 4.3.3.5.
4. Select each of the preceding services, right-click to display a menu, and then deselect **Enabled**.
5. Select the group to which the Device Manager Server service has been registered, right-click to display a menu, and select **Freeze** and then **Temporary**.

4.3.4.2 Upgrading Device Manager on the Executing Node

1. If HiCommand Suite products whose versions are earlier than 5.7 have been installed, stop their services.

   For details about how to stop these services, see the manual for your product version.
2. Stop HiCommand Suite Common Component, and then start HiRDB.
```
# /opt/HiCommand/Base/bin/hcmdssrv -stop
# /opt/HiCommand/Base/bin/hcmdsdbsrv -start
```
3. Execute the command below to back up the database.

   For details about the options and a caution for backing up, see section 4.6.1.
```
hcmdsbackups -dir target-directory-for-storing-backup-files
```
   The following shows an example of executing the command:
```
# /opt/HiCommand/Base/bin/hcmdsbackups -dir /opt/db_bkup01
```
4. Copy HBASE.GDB on the shared disk to the following directory on the standby node.

   /var/opt/HiCommand/Base/database/
5. Copy HiCommand.gdb on the shared disk to the following directory on the standby node.

   /opt/HiCommand/HiCommandServer/database/interbase
6. Execute the following command to stop HiCommand Suite Common Component:
```
# /opt/HiCommand/Base/bin/hcmdssrv -stop
```
7. On the executing node, perform an upgrade installation of the Device Manager Server to version 4.0 or higher (see section 4.2.5). The following are the requirements for the installation:
   - Leave the settings specifying the location of the databases for the Common Component and Device Manager Server as the default values (see Figure 4.8 and Figure 4.9).
   - Perform database conversion during the installation. (see Figure 4.26)
8. Use a text editor to create a cluster configuration file.

- mode: Specify `online`.
- virtualhost: Specify the logical host name.
- onlinehost: Specify the host name of the executing node.
- standbyhost: Specify the host name of the standby node
- mode = online.

Sample command:

```
virtualhost = hcmdserver
onlinehost = hcmdserver_1
standbyhost = hcmdserver_2
mode = online
```

9. Save the created file as cluster.conf in **/opt/HiCommand/Base/conf**.

   Caution: You cannot specify an IP address for **virtualhost**, **onlinehost**, or **standbyhost**. Confirm that the IP address can be resolved from the host name.

10. If HiCommand Suite products whose versions are earlier than 5.7 have been installed, stop their services.

    For details about how to stop these services, see the manual for your product version.

11. If HiCommand Suite Common Component is running, stop the services of HiCommand Suite Common Component and all HiCommand Suite products, and then start HiRDB.

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

12. Execute the command below to back up the database.

    For details about the options and a caution for backing up, see section 4.6.1.

```
hcmdsbackups -dir target-directory-for-storing-backup-files
```

    The following shows an example of executing the command:

```
# /opt/HiCommand/Base/bin/hcmdsbackups -dir /opt/db_bkup01
```

13. Migrate the database to the shared disk.

    Delete or empty *target-directory-for-storing-data*, and then execute the following command. When this command is executed, the setting of the port that HiRDB uses will be restored to the default (23032). If you changed the port number from the default to another number, take a note of the port number that is being used so that you can set it again later.

    # /opt/HiCommand/Base/bin/hcmdsdbclustersetup -createcluster -databasepath target-directory-for-re-creating-database -exportpath target-directory-for-storing-data -auto

    The following shows an example of executing the command:

    # /opt/HiCommand/Base/bin/hcmdsdbclustersetup -createcluster -databasepath /root/re_creating_db -exportpath /opt/storing_data -auto

    The following describes the options specified in the `hcmdsdbclustersetup` command.

    `databasepath`

    Specify the directory in which you want to re-create the database. After this option name, specify the absolute path of a directory on a shared disk. Note that the path name must not exceed 63 bytes.

The characters that can be used to specify the path are as follows. In addition to these characters, a forward slash (/) can be used as path delimiters. You cannot use a space in the path.

A-Z, a-z, 0-9, period (.), underscore (_)

exportpath

Specify the directory in which you want to store backup data. After this option name, specify the absolute path of a directory on the local disk. Note that the path name must not exceed 63 bytes. If the directory has already been created, delete its contents. The characters that can be used to specify the path are the same as for databasepath.

auto

Specify this option to stop the HiCommand Suite product services and to start HiRDB automatically as preparation for processing the database. After the command is executed, the HiCommand Suite product services and HiRDB are stopped. Note that the services of HiCommand Suite products whose versions are earlier than 5.7 are not stopped automatically.

Caution: You must not execute multiple instances of this command concurrently. Also, you must not execute this command and the hcmdsgetlogs command concurrently.

Caution: For details about how to set the port that HiRDB uses, see section 5.4.2.

14. If HiCommand Suite Common Component is running, execute the following command to stop it.

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

    Note: Do not stop the common component service while another HiCommand Suite common component service is running.

15. Set the Common Component so that it does not start automatically when the machine starts.

    # /opt/HiCommand/Base/bin/hcmdssrv -starttype manual -all

16. Set the Device Manager Server so that it does not start automatically when the machine starts, by moving the following file to another directory, or changing its file name.

    /etc/rc3.d/S99hicommand

    Note: When changing the file name, do not use a name beginning with K or S.

4.3.4.3 Upgrading HiCommand Device Manager on Standby Node

1. Start InterBase Server.

   # /etc/init.d/interbaseserver start

2. Use a text editor to open the following file.

   /opt/HiCommand/HiCommandServer/config/database.properties

3. Change the line beginning with dbm.url= as shown below:

   dbm.url=jdbc:interbase://localhost//opt/HiCommand/HiCommandServer/database/interbase/HiCommand.gdb

4. Use a text editor to open the following file. (If the file does not exist, create the file.)

   /opt/HiCommand/Base/conf/user.conf

5. Change the line beginning with DATABASE.path= as shown below:

   DATABASE.path=/var/opt/HiCommand/Base/database/HBASE.GDB

   Note: If no line begins with DATABASE.path=, add the line.

6. Stop HiCommand Suite products.

   For details about how to stop these products, see the manual for your product version.

7. Stop HiCommand Suite Common Component.

   Execute the following command:

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

8. On the standby node, perform an upgrade installation of HiCommand Device Manager Server (see section 4.2.5 if you need instructions). The following are the requirements for the installation:
   - Leave the settings specifying the location of the databases for the Common Component and the Device Manager Server as the default values. (see Figure 4.8 and Figure 4.9)
   - If you are upgrading from version 4.0 or higher, do not convert the database (see Figure 4.26).

9. Create the cluster configuration file. Specify the following items in the cluster configuration file:
   - mode: Specify `standby`.
   - virtualhost: Specify the logical host name.
   - onlinehost: Specify the host name of the executing node.
   - standbyhost: Specify the host name of the standby node.

   Sample command:

```
mode = standby
virtualhost = hcmdserver
onlinehost = hcmdserver_1
standbyhost = hcmdserver_2
```

10. Save the created file as cluster.conf in **/opt/HiCommand/Base/conf**.

    Caution: You cannot specify an IP address for virtualhost, onlinehost, or standbyhost. Confirm that the IP address can be resolved from the host name.

11. If HiCommand Suite products whose versions are earlier than 5.7 have been installed, stop their services.

    For details about how to stop these services, see the manual for your product version.

12. Change the setting so that the database system on the shared disk is to be referenced.

After deleting or emptying *target-directory-for-storing-data*, execute the following command.When this command is executed, the setting of the port that HiRDB uses will be restored to the default (23032). If you changed the port number from the default to another number, take a note of the port number that is being used so that you can set it again later.

 # /opt/HiCommand/Base/bin/hcmdsdbclustersetup -createcluster -databasepath target-directory-for-re-creating-the-database -exportpath target-directory-for-storing-data -auto

The following shows an example of executing the command:

 # /opt/HiCommand/Base/bin/hcmdsdbclustersetup /createcluster -databasepath /root/re_creating_db -exportpath /opt/storing_data -auto

The following describes the options specified in the `hcmdsdbclustersetup` command.

`databasepath`

Specify the directory in which you want to re-create the database. After this option name, specify the absolute path of the same directory as *target-directory-for-re-creating-database* specified for the executing node. This directory must be located on a shared disk, and the absolute path must not exceed 63 bytes.

The characters that can be used to specify the path are as follows. In addition to these characters, a forward slash (`/`) can be used as path delimiters. You cannot use a space in the path.

`A-Z`, `a-z`, `0-9`, period (`.`), underscore (`_`)

`exportpath`

Specify the directory in which you want to store backup data. After this option name, specify the absolute path of a directory on the local disk. Note that the path name must not exceed 63 bytes. If the directory has already been created, delete its contents. The characters that can be used to specify the path are the same as for `databasepath`.

`auto`

Specify this option to stop the HiCommand Suite product services and to start HiRDB automatically as preparation for processing the database. After the command is executed, the HiCommand Suite product services and HiRDB are stopped. Note that the services of HiCommand Suite products whose versions are earlier than 5.7 are not stopped automatically.

Caution: You must not execute multiple instances of this command concurrently. Also, you must not execute this command and the `hcmdsgetlogs` command concurrently.

Caution: For details about how to set the port that HiRDB uses, see section 5.4.2.

13. If HiCommand Suite Common Component is running, execute the following command to stop it.

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

    Note: Do not stop the common component service while another HiCommand Suite common component service is running.

14. Set the Common Component so that it does not start automatically when the machine starts.

 # /opt/HiCommand/Base/bin/hcmdssrv -starttype manual -all

15. Set the Device Manager Server so that it does not start automatically when the machine starts.

    /etc/rc3.d/S99hicommand

    Note: When changing the file name, do not use a name beginning with K or S.

4.3.4.4 Creating Scripts for HiRDB

After upgrading Device Manager on the executing node and standby node, you must create the script for HiRDB on both nodes. The procedure is the same as for an initial installation. For more information, see section 4.3.3.3.

4.3.4.5 Setting Up the Cluster Resource

1. In Java Console, start Cluster Manager.
2. In the Cluster Explorer window, select the **Service Groups** tab. Right-click the group to which the Device Manager services have been registered, and then choose **Unfreeze**.
3. In the Cluster Explorer panel, select the **Service Groups** tab. Select **InterBase services**, right-click to display a menu, and then select **Delete**.

   Note: Do not delete these resources if other resources depend on them.
4. For each of the following service parameters, specify the same value as for a new installation. For more information, see section 4.3.3.5.
   - HBase Storage Mgmt Common Service
   - HBase Storage Mgmt Web Service
   - Device Manager Server

   The above services are represented by the resource names registered in section 4.3.3.5.
5. On both the executing and standby nodes, delete the following files:
   - **/etc/init.d/cluster_hicommand-SSOS**
   - **/etc/init.d/cluster_hicommand-CWS**
6. Register the HiRDB service to the group to which the HiCommand Device Manager service has been registered. Use the same procedure as for a new installation. For more information, see section 4.3.3.5.
7. On the executing node, place online the group to which the HiCommand Device Manager service is registered.

4.3.5 Performing an Upgrade Installation from Version 4.0 or Later or Performing a Re-installation

This section describes how to perform an upgrade installation of HiCommand Device Manager from version 4.0 or later and how to re-install the same version of HiCommand Device Manager by overwriting in a VERITAS Cluster Server or Sun Cluster cluster environment.

Warning: After finishing an upgrade installation or re-installation, make sure to back up the HiCommand Device Manager server database.

Caution: Before starting installation, perform the following steps:

- If the services on the executing node are offline, place them online.
- If Device Manager and other HiCommand Suite products are already running in a cluster environment, make preparations such as canceling the cluster configuration. For details about the necessary preparations, see section 4.3.2.

4.3.5.1 Preparing for Re-installation in VERITAS Cluster Server

Note: If you are using Sun Cluster, skip this section and go to section 4.3.5.2.

To prepare for re-installation, perform the following operations on the executing node:

1. In Java Console, start Cluster Manager.
2. Place the following services offline:
   - Device Manager Server
   - HBase Storage Mgmt Web Service
   - HBase Storage Mgmt Common Service

   The above services are represented by the resource names registered in section 4.3.3.5.
3. For each of the preceding services, right-click to display a menu, and then deselect **Enabled**.
4. Stop the services of HiCommand Suite products.

   For details about how to stop these services, see the manual for your product version.
5. Stop the Common Component using the following command:

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

   Note: Do not stop the common component service while another HiCommand Suite common component service is running.
6. Place the HiRDB service offline by selecting the HiRDB service, right-clicking to display a menu, and then deselecting **Enabled**.
7. In the Cluster Explorer window, select the **Service Groups** tab.
8. Right-click the group to which the Device Manager services have been registered. Choose **Freeze** and then **Temporary**.

4.3.5.2 Preparing for Re-installation in Sun Cluster

Execute the following operations on the executing node:

1. Disable monitoring of the resources of the HBase Storage Mgmt Web Service, HiCommand Server, and HBase Storage Mgmt Common Service.

 # /usr/cluster/bin/scswitch -n -M -j MgmtWebService
 # /usr/cluster/bin/scswitch -n -M -j HiCommandServer
 # /usr/cluster/bin/scswitch -n -M -j SMgmtComService

For the resource names in the above commands, specify the resource names registered in section 4.3.3.6.

2. Execute the following command to disable the HBase Storage Mgmt Web Service, HiCommand Server, and HBase Storage Mgmt Common Service.

   # /usr/cluster/bin/scswitch -n -j MgmtWebService
   # /usr/cluster/bin/scswitch -n -j HiCommandServer
   # /usr/cluster/bin/scswitch -n -j MgmtComService

   For the resource names in the above commands, specify the resource names registered in section 4.3.3.6.

3. Stop the services of HiCommand Suite products.

   For details about how to stop these services, see the manual for your product version.

4. Stop HiCommand Suite Common Component.

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

   Note: Do not stop the common component service while another HiCommand Suite common component service is running.

5. Disable monitoring of the HiRDB resource.

   # /usr/cluster/bin/scswitch -n -M -j HiRDB

   For the resource names in the above commands, specify the resource names registered in section 4.3.3.6.

6. Disable the HiRDB resource.

   # /usr/cluster/bin/scswitch -n -j HiRDB

   For the resource names in the above commands, specify the resource names registered in section 4.3.3.6.

4.3.5.3 Performing an Upgrade or Re-installation of Device Manager on the Executing Node

1. Perform an upgrade installation or re-installation of the HiCommand Device Manager server (see section 4.3.5).

   Caution: During the upgrade installation or re-installation, backup or export the database.

2. If HiCommand Suite Common Component is running, stop it by using the following command:

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

3. Stop the Device Manager Server and Common Component.

   # /opt/HiCommand/suitesrvcntl -stop_all

   Note: Do not stop the common component service while another HiCommand Suite common component service is running.

4. Set the Common Component service so that it does not start automatically when the machine starts.

   # /opt/HiCommand/Base/bin/hcmdssrv -starttype manual -all

5. Set the Device Manager Server so that it does not start automatically when the machine starts.

   /etc/rc3.d/S99hicommand

   Note: Make sure that the file name does not start with K or S.

6. Place the group to which the HiCommand Device Manager service has been registered on standby.

7. Switch, to the standby node, the group in which the HiCommand Device Manager service has been registered.

   If you are using VERITAS Cluster Server:

   - In the Cluster Explorer window, select the **Service Groups** tab.
   - Select the group to which the HiCommand Device Manager service has been registered.
   - Right-click to display a menu.
   - Select **Unfreeze**.
   - Choose **Switch To**, and then select the host name of the standby node.
   - Choose **Freeze**, and then **Temporary**.

   If you are using Sun Cluster:

   - Execute the following command:

     /usr/cluster/bin/scswitch -z -g group-name -h host-name

4.3.5.4 Perform an Update or Re-installation of Device Manager on the Standby Node

1. Stop the services of HiCommand Suite products.

   For details about how to stop these services, see the manual for your product version.

2. Stop HiCommand Suite Common Component.

   Execute the following command:

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

3. Perform an update installation or re-installation of the HiCommand Device Manager server (see section 4.3.5).

   Caution: When a message appears prompting you to confirm whether you want to back up a database or whether you want to export a database, do not select **y**. If you select **y**, installation fails.

4. If HiCommand Suite Common Component is running, stop it by using the following command:

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

   Note: Do not stop the common component service while another HiCommand Suite common component service is running.

5. Set the Common Component service so that it does not start automatically when the machine starts.

   # /opt/HiCommand/Base/bin/hcmdssrv -starttype manual -all

6. Set the Device Manager Server so that it does not start automatically when the machine starts by moving the following file to another directory, or changing its file name:

   /etc/rc3.d/S99hicommand

Note: Make sure that the file name does not start with K or S.

4.3.5.5 Configuring the VERITAS Cluster Server

1. In Java Console, start Cluster Manager.
2. Access the Cluster Explorer panel.
3. Select the **Service Groups** tab.
4. Select the group to which HiCommand Device Manager service has been registered.
5. Right-click to display a menu, then select **Unfreeze**.
6. Select the group to which the HiCommand Device Manager service has been registered, right-click to display a menu, and select **Enable Resources**.
7. From the **File** menu, choose **Save Configuration**, and then **Close Configuration**.
8. On the executing node, place online the group where the Device Manager service is registered.

4.3.5.6 Configuring the Sun Cluster

1. Apply the Common Component and HiCommand Device Manager services.

   /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

   For the resource names in the above commands, specify the resource names registered in section 4.3.3.6.

2. Apply the monitoring of the Common Component and HiCommand Device Manager services.

   # /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

   For the resource names in the above commands, specify the resource names registered in section 4.3.3.6.

3. In Java Console, start Cluster Manager.

4. On the executing node, place online the group where the Device Manager service is registered.

4.3.6 Converting to a Cluster Configuration

Caution: HiCommand Device Manager server only supports Solaris cluster environments.

This section contains instructions for changing to a cluster configuration after you have already started operating under a non-cluster configuration. In this example, the Device Manager Server where operations are already running is treated as the executing node.

1. On the host that will be used as the standby node, install the Device Manager Server. see section 4.3 if you need instructions.
2. On the standby node, display the Web Client logon, then enter the license key.
3. On both the executing and standby nodes, use a text editor to create a cluster configuration file for each node. Specify the following:
   - mode: Specify online for the executing node, and standby for the standby node.
   - virtualhost: Specify the logical host name.
   - onlinehost: Specify the host name of the executing node.
   - standbyhost: Specify the host name of the standby node.
   - mode = online.

   Sample command:

```
mode = online
virtualhost = hcmdserver
onlinehost = hcmdserver_1
standbyhost = hcmdserver_2
```

4. Save the created file as cluster.conf in **/opt/HiCommand/Base/conf**.

   Caution: You cannot specify an IP address for virtualhost, onlinehost, or standbyhost. Confirm that the IP address can be resolved from the host name.

5. If HiCommand Suite products whose versions are earlier than 5.7 have been installed, stop their services.

   For details about how to stop these services, see the manual for your product version.

6. If HiCommand Suite Common Component is running, stop the services of HiCommand Suite Common Component and all HiCommand Suite products, and then start HiRDB.

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

7. Execute the command below to back up the database on the executing node.

   For details about the options and a caution for backing up, see section 4.6.1.

```
hcmdsbackups -dir target-directory-for-storing-backup-files
```

   The following shows an example of executing the command:

```
# /opt/HiCommand/Base/bin/hcmdsbackups -dir /opt/db_bkup01
```

8. In the executing node, migrate the database to the shared disk.

Delete or empty *target-directory-for-storing-data*, and then execute the following command. When this command is executed, the setting of the port that HiRDB uses will be restored to the default (23032). If you changed the port number from the default to another number, take a note of the port number that is being used so that you can set it again later.

 # /opt/HiCommand/Base/bin/hcmdsdbclustersetup -createcluster -databasepath target-directory-for-re-creating-the-database -exportpath target-directory-for-storing-data -auto

The following shows an example of executing the command:

 # /opt/HiCommand/Base/bin/hcmdsdbclustersetup -createcluster -databasepath /root/re_creating_db -exportpath /opt/storing_data -auto

The following describes the options specified in the `hcmdsdbclustersetup` command.

`databasepath`

Specify the directory in which you want to re-create the database. After this option name, specify the absolute path of a directory on a shared disk. Note that the path name must not exceed 63 bytes.

The characters that can be used to specify the path are as follows. In addition to these characters, a forward slash (`/`) can be used as path delimiters. You cannot use a space in the path.

`A-Z`, `a-z`, `0-9`, period (`.`), underscore (`_`)

`exportpath`

Specify the directory in which you want to store backup data. After this option name, specify the absolute path of a directory on the local disk. Note that the path name must not exceed 63 bytes. If the directory has already been created, delete its contents. The characters that can be used to specify the path are the same as for `databasepath`.

`auto`

Specify this option to stop the HiCommand Suite product services and to start HiRDB automatically as preparation for processing the database. After the command is executed, the HiCommand Suite product services and HiRDB are stopped. Note that the services of HiCommand Suite products whose versions are earlier than 5.7 are not stopped automatically.

Caution: You must not execute multiple instances of this command concurrently. Also, you must not execute this command and the `hcmdsgetlogs` command concurrently.

Caution: For details about how to set the port that HiRDB uses, see section 5.4.2.

9. On the standby node, change the settings so that a database on the shared disk is used.

   After deleting or emptying *target-directory-for-storing-data*, execute the following command. When this command is executed, the setting of the port that HiRDB uses will be restored to the default (23032). If you changed the port number from the default to another number, take a note of the port number that is being used so that you can set it again later.

   # /opt/HiCommand/Base/bin/hcmdsdbclustersetup -createcluster -databasepath target-directory-for-re-creating-database -exportpath target-directory-for-storing-data -auto

The following shows an example of executing the command:

 # /opt/HiCommand/Base/bin/hcmdsdbclustersetup -createcluster -databasepath /root/re_creating_db -exportpath /opt/storing_data -auto

The following describes the options specified in the `hcmdsdbclustersetup` command.

`databasepath`

Specify the directory in which you want to re-create the database. After this option name, specify the absolute path of the same directory as *target-directory-for-re-creating-database* specified for the executing node. This directory must be located on a shared disk, and the absolute path must not exceed 63 bytes.

The characters that can be used to specify the path are as follows. In addition to these characters, a forward slash (`/`) can be used as path delimiters. You cannot use a space in the path.

`A-Z`, `a-z`, `0-9`, period (`.`), underscore (_)

`exportpath`

Specify the directory in which you want to store backup data. After this option name, specify the absolute path of a directory on the local disk. Note that the path name must not exceed 63 bytes. If the directory has already been created, delete its contents. The characters that can be used to specify the path are the same as for `databasepath`.

`auto`

Specify this option to stop the HiCommand Suite product services and to start HiRDB automatically as preparation for processing the database. After the command is executed, the HiCommand Suite product services and HiRDB are stopped. Note that the services of HiCommand Suite products whose versions are earlier than 5.7 are not stopped automatically.

Caution: You must not execute multiple instances of this command concurrently. Also, you must not execute this command and the `hcmdsgetlogs` command concurrently.

Caution: For details about how to set the port that HiRDB uses, see section 5.4.2.

10. If HiCommand Suite Common Component is running on both the executing node and standby nodes, execute the following command to stop it.

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

    Note: Do not stop the common component service while another HiCommand Suite common component service is running.

11. Set the Common Component service so that it does not start automatically when the machine starts.

    # /opt/HiCommand/Base/bin/hcmdssrv -starttype manual -all

12. Set the Device Manager Server so that it does not start automatically when the machine starts.

    /etc/rc3.d/S99hicommand

    Note: Make sure that the file name does not start with K or S.

13. Complete setting up the cluster environment. For more information, see section 4.3.3.5 or 4.3.3.6.

4.4 Verifying HiCommand Device Manager Installation

This section describes the procedure for verifying that the Device Manager server and HiCommand Suite Common Component have been installed correctly.

Caution: Even if installation of HiCommand Device Manager fails, the **GO** menu command for starting HiCommand Device Manager might appear in the Dashboard of other HiCommand Suite products. To remove **GO**, a user with User Management permissions must execute the following command. When this command is executed, the HiCommand Suite Common Component services must be running.

```
# /opt/HiCommand/Base/bin/hcmdsintg -delete -type DeviceManager -user user-ID -pass
password
```

4.4.1 Verifying the HiCommand Device Manager Server Installation

Enter the following command to verify that Device Manager is running.

 # /opt/HiCommand/suitesrvcntl -status_hdvm

If HiCommand Device Manager is up and running normally, the following message appears:

```
The status_hdvm request was accepted.
The Device Manager server started.
```

4.4.2 Verifying HiCommand Suite Common Component Installation

1. Execute the following command to check whether HiCommand Suite Common Component is running:

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

2. If the following messages appear, the Common Component is running normally.

   ```
   KAPM06440-I The HiRDB service has already started.
   KAPM05007-I Already started service. service-name=HBase Storage
   Mgmt Web Service
   KAPM05007-I Already started service. service-name=HBase Storage
   Mgmt Common Service
   ```

3. If the Common Component is not running, execute the following command to start it.

   # /opt/HiCommand/Base/bin/hcmdssrv -start -server HBase

4. If the Common Component fails to start, the port number might already be in use. If this is the case, change the port number. See section 5.4.2 for instructions on how to change the port.

   Another possible cause for the Common Component failing to start is the insufficient installed memory. To increase the amount of installed memory, see sections 4.1.1 and 4.1.2.

   Alternately, process IDs for service processes of the Common Component might overlap. If they do, perform the following operations:

   – Stop the Common Component and the services of HiCommand Suite products:

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

   Note: Do not stop the common component service while another HiCommand Suite common component service is running.

   – Restart the Common Component.

     # /opt/HiCommand/Base/bin/hcmdssrv -start -server HBase

   – If the Common Component still does not start, stop the Common Component and the HiCommand Suite product services again:

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

   – Delete the following files.

     # /usr/bin/rm -rf /var/opt/HiCommand/Base/tmp/*.pid

   – Start the Common Component.

     # /opt/HiCommand/Base/bin/hcmdssrv -start -server HBase

5. If the Common Component still does not start, restart the Device Manager server.

   If the Common Component still fails to start, use the **hcmdsgetlogs** command to collect maintenance information, and then contact Customer Support. For more information on the **hcmdsgetlogs** command, see section 10.2.1.

6. If one or both of these processes are still not running, please check the install log and follow the instructions.

7. If the problem remains, uninstall Device Manager (see section 4.6.4 for instructions), reboot the system, and re-install Device Manager.

4.5 Starting and Stopping Device Manager Server

This section describes how to start and stop the Device Manager server. This section also describes processes that are resident during the startup of the Device Manager server and HiCommand Suite Common Component.

WARNING: If a Device Manager client (for example, Web Client, Device Manager CLI, or Device Manager Agent) is accessing the Device Manager Server when that machine is shut down, the Device Manager client processing will terminate. Make sure that Device Manager clients are not accessing the server before shutting down a machine that is running the Device Manager Server.

- To start the Device Manager Server, execute the following command:

  # /opt/HiCommand/suitesrvcntl-start_hdvm

  This command outputs the following messages:

  ```
  The start_hdvm request was accepted.
  The Device Manager server started.
  ```

  This indicates that Device Manager is up and running normally.

- To stop the Device Manager Server, enter the command:

  # /opt/HiCommand/suitesrvcntl -stop_hdvm

- To check the status of the Device Manager Server, enter one of the following commands:

  # /opt/HiCommand/suitesrvcntl -status_hdvm

- To start the HiCommand Device Manager server and HiCommand Suite Common Component, execute the following command:

  # /opt/HiCommand/Base/bin/hcmdssrv -start

  Services of other HiCommand Suite products whose versions are 5.7 or later are also started at the same time. For details, see *Caution* below.

- To stop the HiCommand Device Manager server and HiCommand Suite Common Component, execute the following command:

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

  - Services of other HiCommand Suite products whose versions are 5.7 or later are also stopped at the same time. For details, see *Caution* below.
  - If Replication Monitor 5.6 or earlier is installed, you cannot stop the Device Manager server by executing the `hcmdssrv -stop` command. Stop the Device Manager server by itself, and then stop other services by executing the `hcmdssrv -stop` command.

- To check the status of the HiCommand Device Manager server and HiCommand Suite Common Component, execute the following command:

  # /opt/HiCommand/suitesrvcntl -status_all

Caution: When starting or stopping the Device Manager server and HiCommand Suite Common Component concurrently:

- If you start or stop the Device Manager server and HiCommand Suite Common Component concurrently, services of other HiCommand Suite products whose versions are 5.7 or later are also started or stopped at the same time. For details about how to start or stop services of HiCommand Suite products whose versions are earlier than 5.7, see the manual for your product version.
- If the HiCommand Suite Common Component services are already running when you execute the `hcmdssrv -start` command, the service of the Device Manager server and of the Tiered Storage Manager server will not be started. In this case, start the service of the Device Manager server or the service of the Tiered Storage Manager server individually (without HiCommand Suite Common Component).

  For details about how to check the status of the Tiered Storage Manager server service and how to start the service, see the *HiCommand Tiered Storage Manager Server Installation and Configuration Guide*.

Caution: Do not execute the `hicommand`, `hcmdssrv`, or `suitesrvcntl` command while the `suitesrvcntl` command is being executed. If you do so, the `suitesrvcntl` command may not operate correctly. If you have done so inadvertently, re-execute the `suitesrvcntl` command. Also, do not execute the `suitesrvcntl` command while the `hicommand` or `hcmdssrv` command is being executed.

Caution: Do not execute the `hcmdssrv -stop` command (stop command) before startup of HiCommand Suite Common Component is complete. If you attempt to do so, the service status displayed by the `status` option might indicate that the service has stopped, although the resident processes for the services are running. Alternatively, you might not be able to stop the services any longer by specifying the `stop` option. If either situation occurs, restart the system.

The following table describes the resident processes of the Device Manager server and HiCommand Suite Common Component:

Table 4.8 Resident Processes of the Device Manager server and HiCommand Suite Common Component (In Solaris or Linux)

Process name	Function

`hicmdserver`	The Device Manager server
	In Solaris:
	`/bin/sh /opt/HiCommand/HiCommandServer/hicmdserver`
	In Linux:
	`/opt/HiCommand/HiCommandServer/hicmdserver`

`webcont.sh`	HiCommand Suite servlet service
	In Solaris:
	`/bin/sh /opt/HiCommand/Base/CC/web/containers/HiCommand/webcont.sh`
	In Linux:
	`/opt/HiCommand/Base/CC/web/containers/HiCommand/webcont.sh`

`/opt/HiCommand/Base/httpsd/sbin/httpsd`	HiCommand Suite common web service Multiple processes of this might be started.
`/opt/hitachi/HNTRLib2/bin/hntr2mon`	HiCommand Suite common trace information collection (collects integrated trace information.)

4.6 Operating the HiCommand Device Manager Server Database

This section describes how to perform the following operations for the Device Manager server database:

- Backing up
- Restoring the backed-up data
- Migrating the database (export and import)
- Initializing the database

The following table shows the differences in the functions between backing up and restoring verses exporting and importing.

Table 4.9 Backing Up and Restoring Verses Exporting and Importing

Item	Backing Up and Restoring	Exporting and Importing
Conditions of the HiCommand Suite Common Component version	No limitation.	HiCommand Suite Common Component version 5.5 or later must be installed on the machine used for the export source or the import destination.
Main purpose of use	To recover the current operating environment when a failure occurs in the server machine.	To migrate the server machine from the current environment to a different environment (such as a machine with a different OS).
Target data	▪ Databases for HiCommand Suite products ▪ The HiCommand Suite Common Component database	▪ Databases for HiCommand Suite products ▪ User information included in the HiCommand Suite Common Component database
Conditions for the machine used for the restore destination or the import destination	The following must be the same in the backup source machine and the restore destination machine: ▪ Types, versions, and revisions of the installed HiCommand Suite products ▪ Installation locations for each HiCommand Suite product, HiCommand Suite Common Component, each HiCommand Suite product database, and HiCommand Suite Common Component database ▪ The IP address and host name of the machine	▪ The HiCommand Suite products whose databases to be imported must be installed. ▪ The versions of the installed HiCommand Suite products must be the same as or higher than the ones on the export source machine.

The following section describe the procedure for each operation separately.

4.6.1 Backing Up the Server and Common Component Database

Caution: To back up the Device Manager database, a directory for storing the backup file is required. The capacity of this directory must be at least the total size of the following two directories:

- The directory storing the Device Manager database
- The directory storing the HiCommand Suite Common Component database

This capacity is a guideline value applied when only the Device Manager database is installed. If HiCommand Suite products other than Device Manager are also installed, take the capacities of those databases into account as well.

To back up a database:

1. If HiCommand Suite products whose versions are earlier than 5.7 have been installed, stop their services.

   For details about how to stop these services, see the manual for your product version.

2. If HiCommand Suite products whose versions are 5.7 or later have not been installed, stop HiCommand Suite Common Component, and then start HiRDB.

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

   # /opt/HiCommand/Base/bin/hcmdsdbsrv -start

3. Execute the **hcmdsbackups** command from the terminal window.

   # /opt/HiCommand/Base/bin/hcmdsbackups

   The command format is as follows. The `auto` option can be specified only when HiCommand Suite products whose versions are 5.7 or later have been installed:

   hcmdsbackups -dir target-directory-for-storing-backup-files -auto

   The following shows an example of executing the command:

   # /opt/HiCommand/Base/bin/hcmdsbackups -dir /opt/db_bkup01 -auto

   The specifiable options for this command are as follows:

   dir

   Specify the absolute path of the directory, on the local disk, that stores the backup files of the HiCommand Device Manager server database. Do not specify a path that includes a space.

   Caution: Specify an empty directory for the dir option. If you specify a directory that is not empty, the backup processing will be aborted. In such a case, specify an empty directory, and then re-execute the **hcmdsbackups** command.

   auto

   Specify this option to stop the HiCommand Suite product services and to start HiRDB automatically as preparation for processing the database. After the command is executed, the HiCommand Suite product services and HiRDB are started. Note that the services of HiCommand Suite products whose versions are earlier than 5.7 are not started and stopped automatically.

Note: When you execute the **hcmdsbackups** command, a directory named database will be created in the target directory for storing backup files, and the database backup file will be stored with the name **backup.hdb**.

4. If you have stopped HiCommand Suite Common Component in step 2, execute the following command to restart HiCommand Suite Common Component:

   # /opt/HiCommand/Base/bin/hcmdssrv -start

5. If HiCommand Suite products whose versions are earlier than 5.7 have been installed, restart their services as needed.

   For details about how to start these services, see the manual for your product version.

4.6.2 Restoring the Server Database

Warning: Before restoring the database, be sure to confirm that the following are the same in the backup source Device Manager server and the restore destination Device Manager server. If the following are not the same, the database cannot be restored.

- Types, versions, and revisions of the installed HiCommand Suite products
- Installation location for each HiCommand Suite product, HiCommand Suite Common Component, each HiCommand Suite product database, and HiCommand Suite Common Component database
- The IP address and host name of the machines

To restore the database:

1. If HiCommand Suite products whose versions are earlier than 5.7 have been installed, stop their services.

   For details about how to stop these services, see the manual for your product version.

2. Execute the **hcmdsdb** command from the terminal window.

   The execution destination is as follows:

   # /opt/HiCommand/Base/bin/hcmdsdb

   The command format is as follows:

   hcmdsdb -restore backup-file -type name-of-HiCommand-Suite-product-to-be-restored -auto

   The following shows an example of executing the command:

   # /opt/HiCommand/Base/bin/hcmdsdb -restore /opt/db_bkup01/database/backup.hdb -type DeviceManager -auto

   The specifiable options are as follows:

   restore

   Specify the absolute path of the Device Manager Server database backup file (backup.hdb) acquired by the hcmdsbackups command. Do not specify a path that includes a space.

   type

Specify the name of the HiCommand Suite product to be restored. To restore the HiCommand(R) Device Manager database only, specify **DeviceManager**. To restore all the HiCommand Suite products databases at once, specify **ALL**. To restore the databases when you are uninstalling and then reinstalling all the HiCommand Suite products, specify **ALL**.

auto

Specify this option to stop the HiCommand Suite product services and HiRDB automatically as preparation for processing the database. After the command is executed, the HiCommand Suite product services and HiRDB are stopped. Note that the services of HiCommand Suite products whose versions are earlier than 5.7 are not stopped automatically.

WARNING: If you do not want to restore the databases for other HiCommand Suite products, make sure that you specify **DeviceManager**.

3. If **DeviceManager** is specified for the type option, specify **true** for the value of the **server.base.initialsynchro** property in the **server.properties** file. For more information, see section 8.2.23.
4. Restart the HiCommand Suite product services and HiCommand Suite Common Component by executing the following command:

   # /opt/HiCommand/Base/bin/hcmdssrv -start

   Caution: The services of HiCommand Suite products whose versions are earlier than 5.7 are not started. If such products have been installed, restart their services manually as needed. For details about how to start these services, see the manual for your product version.
5. Change the value of the `server.base.initialsynchro` property in the `server.properties` file back to `false`.

4.6.3 Migrating the Server Database

If HiCommand Suite products are used for an extended period of time, you may need a higher performance machine in order to accommodate product version upgrades and the increased number of objects to be managed. If this occurs, database migration will be one important component of the machine replacement process. In HiCommand Suite products, you can migrate the database by using the `hcmdsdbtrans` command. The `hcmdsdbtrans` command migrates all information stored in the database of each HiCommand Suite product as well as user information managed by the HiCommand Suite Common Component.

You can use the `hcmdsdbtrans` command to migrate the Device Manager database to a machine that has a different environment than the currently operating server machine, as shown in the following cases:

- Migration to a different platform machine
- Migration to a machine on which the installation locations for HiCommand Suite products are different from the ones on the migration source
- Migration to a machine on which the versions of HiCommand Suite products are newer than the ones on the migration source

4.6.3.1 Notes When Migrating the Database

The following are notes for the types, versions, and user information of the HiCommand Suite products on the migration source and migration destination servers.

Notes for types and versions of the HiCommand Suite products on the migration source and migration destination servers:

- The database of a HiCommand Suite product that is not installed on the migration destination server cannot be migrated. Install all necessary HiCommand Suite products on the migration destination server.
- If any of the versions of the HiCommand Suite products installed on the migration destination server is older than the ones on the migration source server, the database cannot be migrated. On the migration destination server, install the HiCommand Suite products whose versions are the same as or higher than the ones on the migration source server.
- The database of Replication Monitor version 4.2 or earlier cannot be migrated. If you need to migrate the database of Replication Monitor version 4.2 or earlier, upgrade Replication Monitor to version 5.0 or later on both the migration source and destination servers beforehand.
- The following limitations apply when you migrate the database in Tuning Manager.
- The database can be migrated when the database configuration (Small or Medium) is the same on both the migration source and the destination server, or when the database configuration on the migration destination server becomes much larger than that on the source server.
- In the database configuration on the migration source server, if the number of the management target resources exceeds 70% of the management limit, the database cannot be migrated to a database that has the same configuration.

Notes for user information:

- If there is user information on the migration destination server, this user information will be replaced with the user information from the migration source server. Therefore, do not perform a migration to the machine on which user information for the HiCommand suite products already exists.
- If the databases of several HiCommand Suite products installed on a management server are migrated in multiple operations, the user information is replaced with new information at each operation, and eventually only the user information for the products migrated during the last operation will remain. When you perform migration for multiple products, be sure to migrate the databases in one operation so that user information for every products can be migrated.
- You cannot perform migration to integrate the HiCommand Suite products that were running on multiple management servers on to one management server because user information will be overwritten with each successive migration.

4.6.3.2 Procedure for Migrating Databases

To migrate databases:

1. Install, on the migration destination server, the HiCommand Suite products whose databases will be migrated.
2. Export the databases at the migration source server by using the `hcmdsdbtrans` command.
3. Transfer the archive file from the migration source server to the migration destination server.
4. Import the database at the migration destination server by using the `hcmdsdbtrans` command.

The following section describe the details of each procedure. To perform migration between heterogeneous platforms, also see section 3.6.3.

4.6.3.3 Installing the HiCommand Suite Products on the Migration Destination Server

Install, on the migration destination server, the HiCommand Suite products whose databases will be migrated. The version of each HiCommand Suite product installed on the migration destination server must be the same as or higher than the one on the migration source server.

4.6.3.4 Exporting the Database at the Migration Source Server

To export the database of Device Manager, a directory for temporarily storing the information of the database, and a directory for storing the archive file are required. Each of these directories requires the as much capacity as the total size of the following two directories:

- The directory storing the Device Manager database
- The directory storing the HiCommand Suite Common Component database (excluding the `SYS` directory and the directories beneath it)

This capacity is a guideline value applied when only the Device Manager database is installed. If HiCommand Suite products other than Device Manager are also installed, take the capacities of those databases into account as well.

Caution: If the total capacity of the database exceeds 2 GB, an attempt to create the archive file fails when the database is exported. In this case, instead of using the archive file, transfer the database information collected when exporting the database, to the migration destination.

To export the database at the migration source server:

1. If HiCommand Suite products whose versions are earlier than 5.7 have been installed, stop their services.

   For details about how to stop these services, see the manual for your product version.

2. If HiCommand Suite products whose versions are 5.7 or later have not been installed, stop HiCommand Suite Common Component, and then start HiRDB.

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

   # /opt/HiCommand/Base/bin/hcmdsdbsrv -start

3. From the terminal window, execute the `hcmdsdbtrans` command.

   The default installation location of the `hcmdsdbtrans` command is as follows:

   # /opt/HiCommand/Base/bin/hcmdsdbtrans

   The command format is as follows. The `auto` option can be specified only when HiCommand Suite products whose versions are 5.7 or later have been installed:

   hcmdsdbtrans -export -workpath working-directory -file archive-file -auto

   The following shows an example of executing the command:

   # /opt/HiCommand/Base/bin/hcmdsdbtrans -export -workpath /opt/trans_work -file /opt/trans_file/db_arc -auto

   In the `hcmdsdbtrans` command, you can specify the following options:

   `workpath`

   Specify the absolute path to the working directory where you wish to temporarily store database information. Do not specify a path that includes a space. Specify a directory on your local disk.

   Caution: Specify an empty directory for the `workpath option. If you specify a` directory `other than an empty directory,` export processing will be cancelled. If this occurs, specify an empty directory and execute the `hcmdsdbtrans` command again.

   `file`

   Specify the absolute path to the archive file of the database to be exported. Make sure that the absolute path does not include a space.

   `auto`

   Specify this option to stop the HiCommand Suite product services and to start HiRDB automatically as preparation for processing the database. After the command is executed, the HiCommand Suite product services and HiRDB are started. Note that the services of HiCommand Suite products whose versions are earlier than 5.7 are not started and stopped automatically.

4. Transfer the exported file to the migration destination server.

   If the archive file cannot be created, transfer all the files stored in the directory specified by the `workpath` option. In that case, do not change the file structure in the directory specified by the `workpath` option.

4.6.3.5 Importing the Database at the Migration Destination Server

Caution: If the OS of the migration destination server is Windows, follow the procedure in section 3.6.3.5.

To import the database at the migration destination server:

1. If HiCommand Suite products whose versions are earlier than 5.7 have been installed, stop their services.

   For details about how to stop these services, see the manual for your product version.

2. From the terminal window, execute the `hcmdsdbtrans` command.

   The default installation location of the `hcmdsdbtrans` command is as follows:

   # /opt/HiCommand/Base/bin/hcmdsdbtrans

   The format of the command is as follows:

   hcmdsdbtrans -import -workpath working-directory [-file archive-file] -type {ALL | HiCommand-Suite-products-whose-databases-will-be-migrated} -auto

   The following shows an example of executing the command:

   # /opt/HiCommand/Base/bin/hcmdsdbtrans -import -workpath /opt/trans_work -file /opt/trans_file/db_arc -type ALL -auto

   In the `hcmdsdbtrans` command, you can specify the following options:

   `workpath`

   When using an archive file during the import:

   Specify the absolute path to the directory used to extract the archive file. Do not specify a path that includes a space. Specify a directory on your local disk. If you use an archive file, the `file` option must be specified.

   Caution: Specify an empty directory for the `workpath` option. If you specify a directory other than an empty directory, import processing will be cancelled. If this occurs, specify an empty directory, and then execute the `hcmdsdbtrans` command again.

   When not using the archive file during the import:

   Specify the directory that stores the database information transferred from the migration source server. Do not change the file structure in the transferred directory. Also, do not specify the `file` option.

   `file`

   Specify the absolute path to the archive file of the databases transferred from the migration source server. Make sure that the absolute path does not include a space. If the database information transferred from the migration source server is stored in the directory specified by `workpath`, you do not need to specify this option.

   `type`

   Specify the names of the HiCommand Suite products whose databases will be migrated. Only the databases of the specified products are migrated.

   When you migrate the Device Manager database, specify `DeviceManager`. For details on the names to be specified when you migrate databases of other products, see the relevant manual for each product. To specify multiple product names, use a comma as the delimiter between the names.

   To migrate the databases of all the installed HiCommand Suite products at a time, specify `ALL`. The databases of the HiCommand Suite products installed on the migration destination server are automatically selected and migrated.

You can use the `type` option to migrate databases only when the databases of all the specified products exist in the directory specified by the archive file or the `workpath` option, and all the specified products are installed on the migration destination server. If any of the products do not meet the above conditions, migration will not be performed.

`auto`

Specify this option to stop the HiCommand Suite product services and to start HiRDB automatically as preparation for processing the database. After the command is executed, the HiCommand Suite product services and HiRDB are stopped. Note that the services of HiCommand Suite products whose versions are earlier than 5.7 are not stopped automatically.

Caution: If Replication Monitor version 4.2 or earlier is installed on the migration source machine, you cannot migrate the database. We recommend that you upgrade Replication Monitor on the migration source and migration destination machines to version 5.0 or later, and then perform migration. If Replication Monitor cannot be upgraded to version 5.0 or later, or the Replication Monitor database does not have to be migrated, use the `type` option and specify all products other than Replication Monitor when you execute the command.

3. Synchronize the repository information with the imported Device Manager database information.

   Specify `true` for the `server.base.initialsynchro` property in the `server.properties` file.

   Since, other than user information, the `hcmdsdbtrans` command does not migrate the HiCommand Suite Common Component repository, you need to synchronize the repository information with the database information of the imported Device Manager.

   For information on the `server.base.initialsynchro` property, see section 8.2.22.

4. Execute the following command to restart the HiCommand Suite product services and HiCommand Suite Common Component of the migration destination:

   # /opt/HiCommand/Base/bin/hcmdssrv -start

   Caution: The services of HiCommand Suite products whose versions are earlier than 5.7 are not started. If such products have been installed, restart their services manually as needed. For details about how to start these services, see the manual for your product version.

5. Change the value of the `server.base.initialsynchro` property in the `server.properties` file back to `false`.

4.6.4 Initializing the Device Manager Server Database

To initialize the database:

1. From a terminal window, enter the following command to stop the Device Manager Server:

   # /opt/HiCommand/suitesrvcntl -stop_hdvm

2. Enter the following command to make sure that the HiCommand(R) Device Manager server is not running:

   # /opt/HiCommand/suitesrvcntl -status_hdvm

   This command outputs the following messages:

```
The status_hdvm request was accepted.
The Device Manager server is stopped.
```

   This indicates that HiCommand Device Manager is not running.

3. Execute the following command to make sure that the HiCommand Suite Common Component services are running:

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

   If the following messages appear, the services are running:

   KAPM06440-I The HiRDB service has already started.

   KAPM05007-I Already started service. service-name=HBase Storage Mgmt Web Service

   KAPM05007-I Already started service. service-name=HBase Storage Mgmt Common Service

4. If the HiCommand Suite Common Component services are not running, execute the following command:

   # /opt/HiCommand/Base/bin/hcmdssrv -start -server HBase

5. From the command prompt, execute the database command.

   # /opt/HiCommand/database.sh database initialize

6. Specify **true** for the **server.base.initialsynchro** property in the server.properties file. See section 8.2.23 for more information.

7. Restart the Device Manager Server.

   # /opt/HiCommand/suitesrvcntl -start_hdvm

8. Verify that the server is running.

   # /opt/HiCommand/suitesrvcntl -status_hdvm

   This command outputs the following messages:

```
The status_hdvm request was accepted.
The Device Manager server started.
```

   This indicates that HiCommand Device Manager is up and running normally.

9. Change the value of the `server.base.initialsynchro` property in the `server.properties` file back to `false`.

4.7 Converting a Device Manager Server Database

To use a database that has been used before the upgrade when upgrading the Device Manager server version 2.3 through 3.5 to 4.0 or later, you must first convert it to HiRDB.

Caution: The conversion function is available only when the upgrade is from the Device Manager server version 2.3 through 3.5 to Device Manager server version 4.0 or later.

4.7.1 About Converting from InterBase to HiRDB

If you have a Device Manager database for versions 2.3 through 3.5, it is based on InterBase. Databases for versions 4.0 and higher are based on HiRDB, so if you are upgrading to that level you will need to convert the database.

Caution: InterBase, InterServer and HiRDB must all be running when you convert the database.

Note: It might take a long time to convert the database. For example, if 8,000 LDEVs and 16,000 paths have been managed, the database conversion will take about 10 minutes in an environment that has a 900 MHz CPU and 2 GB of memory.

4.7.2 Converting Manually to HiRD8

You can either convert the database automatically when you install the Device Manager Server, or manually after the installation using these instructions.

To manually convert a database:

1. If HiCommand Suite products whose versions are earlier than 5.7 have been installed, stop their services.

   For details about how to stop these services, see the manual for your product version.

2. Stop the HiCommand Suite product services and HiCommand Suite Common Component by executing the following command from a terminal window:

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

3. InterBase and InterServer are not running, start them manually.

   # /etc/init.d/interbaseserver start

4. Execute the following command to start HiRDB:

   # /opt/HiCommand/Base/bin/hcmdsdbsrv -start

5. To convert the database for the specified file, use the script file, along with the following parameters.

   # /opt/HiCommand/migrateFmIB.sh [-d InterBase-GDB-file-name | InterBase-GBK-file-name] [-u InterBase-user-id] [-p InterBase-password]

   The following options can be specified for the **migrateFmIB** command.

-d: Specify an absolute path for the name of the GDB or GBK file for InterBase. The following file is used if the **-d** option is not specified:

/opt/HiCommand/HiCommandServer/database/interbase/HiCommand.gdb

-u: Specify the InterBase user ID. The default InterBase user ID is assumed if the -u option is not specified.

-p: Specify the InterBase password. The password of the default InterBase user ID is used if the -p option is not specified.

6. Specify **true** for the **server.base.initialsynchro** property in the **server.properties** file. See section 8.2.23 for more information.
7. Restart the HiCommand Suite product services and HiCommand Suite Common Component by executing the following command:

   # /opt/HiCommand/Base/bin/hcmdssrv -start

   Caution: The services of HiCommand Suite products whose versions are earlier than 5.7 are not started. If such products have been installed, restart their services manually as needed. For details about how to start these services, see the manual for your product version.
8. Change the value of the `server.base.initialsynchro` property in the `server.properties` file back to `false`.

Note: When the `migrateFmIB` command is used, one of the following return codes is returned as a result:

Table 4.10 Return Codes for the migrateFmIB Command

Return Code	Description
0	The command terminated normally.
1	InterBase is not running.
2	HiRDB is not running.
3	An InterBase authentication error occurred.
4	A HiRDB authentication error occurred.
5 to 19	(Reserved)
20	The Device Manager Server is running.
21 to 29	(Reserved)
30	The database file to be converted does not exist.
31 to 39	(Reserved)
40	An attempt to change the database definition has failed.
41 to 49	(Reserved)
50	An attempt to convert the database has failed.
51 to 253	(Reserved)
254	An error occurred during the convert.
255	Internal error.

4.8 Uninstalling the HiCommand Device Manager Server and Related Products

Caution: You must restore the kernel parameters after uninstalling the Device Manager server. To restore the kernel parameters that have been set, see 4.10 for Solaris, or see section 4.11 for Linux.

Caution: If an error occurs during uninstallation and then uninstallation stops, execute the `hcmdsgetlogs` command to collect the maintenance information, and then contact maintenance personnel.

4.8.1 Uninstalling Device Manager Server in a Standard Environment

Unless you are experiencing problems and need to completely re-do an installation, you should not uninstall Device Manager. If you need to uninstall the Device Manager Server, make sure to first back up your configuration (see section 4.6.1 for instructions).

WARNING: When you are using the Single Sign-On function and a HiCommand Device Manager server and HiCommand Tuning Manager are installed on the same machine, the HBase Storage Mgmt Common Service is deleted when HiCommand Device Manager is uninstalled.

Warning: Do not specify the system's zone settings during uninstallation in Solaris 10 system. If you do specify the settings, uninstallation might finish abnormally.

If no other program is using the Common Component, it will be uninstalled during the uninstallation of Device Manager. If another program is using the Common Component, it will remain installed. You cannot uninstall the Common Component by itself.

When you uninstall Device Manager, the directories and files under the *installation-directory-for-the-Device-Manager-server* will be deleted, but the directory itself will remain after the uninstallation. If the directory is not necessary you can delete it manually.

WARNING: Files may remain in the installation directory, especially if they were added manually after installation. You can delete unnecessary files, but do not delete this directory if another HiCommand Suite product is being used.

Caution: When you uninstall HiCommand Device Manager from a computer on which another HiCommand Suite product is installed, a **GO** menu command for launching Device Manager remains on the dashboard of that program. To remove **GO**, a user with User Management permissions must execute the following command. When this command is executed, the HiCommand Suite Common Component services must be running.

```
/opt/HiCommand/Base/bin/hcmdsintg -delete -type DeviceManager -user user-ID -pass password
```

Caution: Check whether the following programs are installed. If they are installed, take action by following the explanation below:

- A program that monitors security

  Stop the program that monitors security, or change its settings so that Device Manager can be uninstalled normally.

- A program that detects viruses

  We recommend that you stop programs that detect viruses, and then uninstall Device Manager.

  If a program that detects viruses is running during uninstallation of Device Manager, the speed of uninstallation might be reduced, uninstallation might fail, or uninstallation might finish in an incorrect state.

- A program that monitors processes

  Stop the program that monitors processes, or change its settings so that the program does not monitor the processes of the HiCommand Device Manager server and the HiCommand Suite Common Component.

  If a program that monitors processes starts or stops the above processes during uninstallation of Device Manager, uninstallation might fail.

Note: HiCommand Device Manager provides user management functions for the HBase Storage Mgmt Common Service. When the HiCommand Device Manager Server is uninstalled, the HBase Storage Mgmt Common Service Service no longer operates. Therefore, if you are using Tuning Manager installed on the same machine as the Device Manager Server, Tuning Manager will not have access to the HBase Storage Mgmt Common Service after Device Manager is uninstalled. Before you uninstall the Device Manager, you must disable use of the HBase Storage Mgmt Common Service Service in the Tuning Manager settings.

To uninstall the Device Manager Server:

1. Enter the Device Manager package removal command.

   Move the current directory to the root (/), and then execute the following command:

   # /opt/HiCommand/Uninstall/uninstall.sh

2. A message confirming that you want to delete Device Manager Server and the Common Component is displayed. Enter **y** to begin the uninstallation.

3. When the HiCommand Suite Common Component services are running, a message indicating that the uninstaller will stop these services is displayed (see Figure 4.32) To stop the uninstallation, select **n**. To continue the uninstallation, select **y**.

   If the uninstaller cannot stop all the services of HiCommand Suite Common Component and the HiCommand Suite products, a message indicating that the uninstaller failed to stop the services is displayed (see Figure 4.4). If this message is displayed, choose **y** to try to stop the services again. If the uninstaller still fails to stop the services, cancel the installation, manually stop the services of HiCommand Suite Common Component and the HiCommand Suite products, and then perform the uninstallation again.

   Caution: The services of HiCommand Suite products whose versions are earlier than 5.7 are not stopped. Stop the services manually, and then continue the uninstallation. For details about how to stop these services, see the manual for your product version.

4. In a non-cluster environment, a message asking whether you want to start the HiCommand Suite product services after uninstallation is complete is displayed (see Figure 4.33). If you want to start the services after uninstallation is complete, choose **y**. The services of HiCommand Suite Common Component and HiCommand Suite products will then be started after uninstallation is complete. If you do not want to start the services after uninstallation is complete, choose **n**.

   Caution: The services of HiCommand Suite products whose versions are earlier than 5.7 are not started by choosing **y**. If you want to start the services of HiCommand Suite products after uninstallation is complete, manually start the services as required. For details about how to start these services, see the manual for your product version.

Caution: If the following message is displayed in Linux, manually release the SLP daemon from the Linux daemon. If directories and files related to SLP remain, manually delete them as necessary. For details about how to release the SLP daemon, see section 11.5.1.3.

```
WARNING: An attempt to release the SLP daemon has failed. After
uninstallation, release the SLP daemon manually. Uninstallation continues.
```

Note: Files can remain in the installation directory. Do not delete this directory if another HiCommand Suite product is being used.

Note: If no program is using the Common Component, the Common Component will be uninstalled during the uninstallation of the Device Manager Server. If one or more other programs are using the Common Component, it will be uninstalled only when you uninstall the last program that is using it.

If you uninstall the HiCommand Device Manager server from a machine where software containing HiCommand Suite Common Component has already been installed, HiCommand Suite Common Component will not be uninstalled.

```
Stop HiCommand Suite Product Services:
HiCommand Suite product services are running. If you continue the
uninstallation, the services of all HiCommand Suite products will be stopped.

Do you want to continue uninstallation? [y/n]
```

Figure 4.32 Message that Confirms Stopping of Services (appears during uninstallation)

```
Set Services to Start After Uninstallation:
Do you want the services of all HiCommand Suite products to start after the
uninstallation finishes? (y/n) [default=y]:
```

Figure 4.33 Setting Services to Start After Uninstallation (appears during uninstallation)

4.8.2 Uninstalling Device Manager Server in a VERITAS Server Environment

Note: Before uninstalling, you must confirm that the services on the executing node are online. If the services are offline on the executing node, switch them online.

To uninstall the Device Manager server in a VERITAS Cluster Server environment:

1. Start Cluster Manager (Java Console).
2. Switch, to the executing node, each group in which HiCommand Suite product service has been registered.

   In the Cluster Explorer panel, select **Service Groups**. Select the group in which the HiCommand Device Manager service has been registered, right-click to display a menu, and then:

   - Choose **Unfreeze**.
   - Choose **Switch To**, and then select the host name of the executing node.
   - Choose **Freeze**, and then **Temporary**.
3. Place the following services offline: (See section 5.2.2 if you need instructions.)
   - HiCommand Server
   - HBase Storage Mgmt Web Service
   - HBase Storage Mgmt Common Service

   The above services are represented by the resource names registered in section 4.3.3.5.
4. Stop HiCommand Suite product services and HiCommand Suite Common Component.

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

   Caution: The services of HiCommand Suite products whose versions are earlier than 5.7 are not stopped. Stop the services manually, and then continue the uninstallation.

   For details about how to stop these services, see the manual for your product version.
5. Place the HiRDB service offline.
6. Delete the following resources, provided that no other applications are using them:
   - HBase Storage Mgmt Web Service
   - HBase Storage Agent Common Service
   - HiCommand Server
   - HiRDB

   The above services are represented by the resource names registered in section 4.3.3.5.

   Caution: Do not use this procedure to delete the IP address and shared disk resources.
7. For resources that you will not be deleting, right-click to display a menu, and then deselect **Enabled**.
8. In the Cluster Explorer window do the following, select the **Service Groups** tab.
9. Right-click the group to which the HiCommand Device Manager services have been registered, and choose **Freeze** and then **Temporary**.
10. Uninstall the Device Manager Server on the executing node.

    Move the current directory to the root (/), and then execute the following command:

    # /opt/HiCommand/Uninstall/uninstall.sh

    Caution:Manually delete the unnecessary files and directories that were created during installation in the cluster environment.

11. Switch, to the standby node, each group in which HiCommand Suite product service has been registered.

    In the Cluster Explorer panel, do the following:

    - Select **Service Groups.**
    - Select the group to which the HiCommand Device Manager service has been registered.
    - Right-click to display a menu.
    - Choose **Unfreeze.**
    - Choose **Switch To**, and then select the host name of the standby node**.**
    - Choose **Freeze**, and then **Temporary.**

12. Uninstall HiCommand Device Manager on the standby node.

    Move the current directory to the root (/), and then execute the following command:

    # /opt/HiCommand/Uninstall/uninstall.sh

13. Manually delete the unnecessary files and directories that were created during installation in the cluster environment.
14. Delete the following resources, provided that no other applications are using them:
    - IP address
    - Shared disk
15. For the group to which the HiCommand Device Manager resources were registered, do the following:
    - If is no longer necessary, delete it.
    - If it is still necessary, in the Cluster Explorer window, select the **Service Groups** tab. Right-click the group to which the HiCommand Device Manager services have been registered, and then choose **Unfreeze**.
16. Apply the resources that you disabled in step 7.

4.8.3 Uninstalling Device Manager Server in a Sun Cluster Environment

Caution: Before uninstalling, you must confirm that the services on the executing node are online. If the services are offline on the executing node, switch them online.

To uninstall the Device Manager server in a Sun Cluster environment:

1. Execute the following command to switch, to the executing node, the group in which HiCommand Device Manager service has been registered.

   # /usr/cluster/bin/scswitch -z -g *group-name* -h *host-name*

2. On the executing node, disable the monitoring of the resources of the HiCommand Suite Common Component and HiCommand 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

For the resource names in the above commands, specify the resource names registered section 4.3.3.6.

3. Disable the following service resources.

   # /usr/cluster/bin/scswitch -n -j HiCommandServer

   # /usr/cluster/bin/scswitch -n -M -j MgmtWebService

   # /usr/cluster/bin/scswitch -n -M -j MgmtComService

   For the resource names in the above commands, specify the resource names registered section 4.3.3.6.

4. Execute the following command to stop services of HiCommand Suite products and HiCommand Suite Common Component:

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

   Caution: The services of HiCommand Suite products whose versions are earlier than 5.7 are not stopped. Stop the services manually, and then go to the next step. For details about how to stop these services, see the manual for your product version.

5. Execute the command below to disable the service resource of HiRDB.

   For the resource name of HiRDB, specify the resource name registered in section 4.3.3.6.

```
# /usr/cluster/bin/scswitch -n -j HiRDB
```

6. Delete the following resources, provided that no other applications are using them:
   - HBase Storage Management Web Service
   - HBase Storage Mgmt Common Service
   - HiCommand Server
   - HiRDB

   The above services are represented by the resource names registered in section 4.3.3.6.

   Caution: Do not use this procedure to delete the IP address and shared disk resources.

7. Uninstall the Device Manager Server on the executing node.

   Move the current directory to the root (/), and then execute the following command:

   # /opt/HiCommand/Uninstall/uninstall.sh

   Caution: Manually delete the unnecessary files and directories that were created during installation in the cluster environment.

8. Execute the following command to switch, to the standby node, the group in which HiCommand Device Manager service has been registered.

   # /usr/cluster/bin/scswitch -z -g group-name -h host-name

9. Uninstall HiCommand Device Manager on the standby node.

   Move the current directory to the root (/), and then execute the following command:

   # /opt/HiCommand/Uninstall/uninstall.sh

10. Manually delete the unnecessary files and directories that were created during installation in the cluster environment.
11. Delete the following resources, provided that no other applications are using them:
    - IP address
    - Shared disk
12. For the group to which the HiCommand Device Manager resources were registered, do the following:
    - If is no longer necessary, delete it.
    - If it is still necessary, execute the following commands for those services:

      # /usr/cluster/bin/scswitch -e -j *service-name*

      # /usr/cluster/bin/scswitch -e -M -j *service-name*

4.9 Uninstalling InterBase Components

Notes: You will only have InterBase Server and Client installed if you were previously using Device Manager version 3.5 or lower, or if you were using another product that has InterBase as its database. Do not uninstall InterBase Server and Client if another product is using them.

4.9.1 Uninstalling InterBase Server

Note: When an InterBase process is running, you cannot uninstall InterBase. You can end an InterBase process using one of in the following methods:

- If an **/etc/init.d/interbaseserver** file exists, type the following command:

  # /etc/init.d/interbaseserver stop

- If no **/etc/init.d/interbaseserver** file exists, type the following command:

  # kill -TERM `ps -ef |grep ibserver|grep -v grep|awk' {print $2}'`

To uninstall InterBase:

1. Log on as the root user.
2. Stop InterBase by using one of the following methods:
   - If Device Manager is already installed:

     # /etc/init.d/interbaseserver stop

   - If Device Manager is not already installed:

     # kill -TERM `ps -ef | grep ibserver | grep -v grep | awk '{print $2}'`
3. Enter the command:

   # pkgrm IBCSN60
4. Answer **y** to the verification prompts.

   Note: A directory structure may have been left on disk as a result of the InterBase installation log file that is generated. Enter the following command to remove this directory:

   # rm -rf /opt/interbase
5. Delete the following links and file manually:
   - **/etc/rc2.d/K99interbaseserver**
   - **/etc/rc3.d/S98interbaseserver**
   - **/etc/init.d/interbaseserver**

4.9.2 Uninstalling InterClient

Note: You will only have InterClient installed if you were previously using Device Manager version 3.5 or lower, or if you were using another product that has InterBase as its database. Do not uninstall InterClient if another product is using them.

To uninstall the InterClient software:

1. Enter the following command:

   rm -rf /usr/interclient

   Note: If /usr/interclient is a link, then you also need to delete its linked directory.

2. Delete the entry for the InterServer software in the /etc/services file (for example, **interserver 3060/tcp**).

3. Delete the entry for the InterServer software in the **/etc/ometd/conf file**.

4. Either reboot the system, or force the inetd daemon to re-read its configuration file by entering the following command:

```
# kill -HUP `ps -ef | grep inetd | grep -v grep | awk '{print $2}'`
```

4.10 Setting Kernel Parameters on Solaris

Before installing the Device Manager server, you must set the OS parameters (kernel parameters). If the kernel parameters have not been set correctly, installation fails.

When you uninstall the Device Manager server, you must change the kernel parameters back to the previous settings specified before the installation of the Device Manager server.

4.10.1 When No Other HiCommand Suite Product (version 4.0 or later) is Installed

The following describes the procedure for setting the kernel parameters in a Solaris environment.

Before changing kernel parameter settings, save the current kernel parameter settings by following the instructions for the version of your OS as shown below. After uninstalling the Device Manager server, you can use the saved settings to restore the previous kernel parameter settings.

For Solaris 8 or Solaris 9:

Create a backup of the `/etc/system` file.

For Solaris 10:

Check the current settings by using a command such as `prct1`, and then record the settings. (For details about how to check the settings, see the manuals for the OS.)

Table 4.11 and Table 4.12 below list the recommended values for the kernel parameters you must set.

Refer to Table 4.11 or Table 4.12, and then set the kernel parameters according to the following formula (in the formula, "Max {x, y, z}" means using the maximum value among x, y, and z):

- Parameters other than `shmsys:shminfo_shmmax` for Solaris 8 or Solaris 9, or parameters other than `project.max-shm-memory` for Solaris 10:

  setting-value-of-the-kernel-parameter =

  currently-set-value-for-the-kernel-parameter#1 + Max {recommended-value-for-HiCommand-Suite-Common-Component + recommended-value-for-Device-Manager-server, recommended-value-for-HiRDB}

- `shmsys:shminfo_shmmax` (for Solaris 8 or Solaris 9):

  setting-value-of-the-kernel-parameter =

  Max {*currently-set-value-for-the-kernel-parameter*[#1], recommended-value-for-HiCommand-Suite-Common-Component + recommended-value-for-Device-Manager-server, recommended-value-for-HiRDB}

- `project.max-shm-memory` (for Solaris 10):

  setting-value-of-the-kernel-parameter =

  value-already-used-for-operation[#2] + *recommended-value-for-HiCommand-Suite-Common-Component* + *recommended-value-for-Device-Manager-server*

#1: A user specified value or an initial value of the OS

#2: Total amount of shared memory that is used by the applications other than Device Manager running on the machine on which the server is installed

Caution: In Solaris 10, specify the kernel parameters for both the user.root project and the system project.

Caution: The maximum value of each kernel parameter must not exceed the value defined for the OS.

Caution: After changing the kernel parameters, execute the `shutdown -y -i6 -g0` command to restart the system.

The installer of the Device Manager server checks each kernel parameter by referring to the installer checking values listed in Table 4.11 or Table 4.12. If the specified value of a kernel parameter is less than the corresponding installer checking value, installation fails.

Table 4.11 Recommended Values for Kernel Parameters (for Solaris 8 or Solaris 9)

Kernel Parameter	Recommended Value for HiRDB	Recommended Value for HiCommand Suite Common Component	Recommended Value for the Device Manager Server	Installer Checking Value
msgsys:msginfo_msgmni	0	32	0	82
msgsys:msginfo_msgtql	0	480	0	520
semsys:seminfo_semmni	1024	9	1	1024
semsys:seminfo_semmns	7200	80	44	7200
semsys:seminfo_semmnu	1024	0	0	1024
semsys:seminfo_semume	512	0	0	512
semsys:seminfo_semmsl	128	0	0	128
semsys:seminfo_semopm	128	0	0	128
shmsys:shminfo_shmmax	200000000	11542528	130000000	200000000
shmsys:shminfo_shmmni	2000	0	0	2000
shmsys:shminfo_shmseg#	240	0	0	240

In Solaris 9, the setting of this kernel parameter is not necessary. This parameter remains only when checking for compatibility with Solaris 8 (installer checking is performed only when Solaris 8 is used).

Table 4.12 Recommended values for kernel parameters (for Solaris 10)

Kernel Parameter	Recommended Value for HiRDB	Recommended Value for HiCommand Suite Common Component	Recommended Value for the Device Manager Server	Installer Checking Value
process.max-msg-messages	0	480	0	8192
process.max-sem-nsems	128	0	0	512
process.max-sem-ops	128	0	0	512
project.max-msg-ids	0	32	0	128
project.max-sem-ids	1024	9	1	1024
project.max-shm-ids	2000	0	0	2000
project.max-shm-memory	0	26214400	235929600	262144000

Caution: In Solaris 10, even if you set the kernel parameters, the settings might not be applied properly. In this case, specify the following in the file `/etc/system`, and then restart the machine:

```
set msgsys:msginfo_msgmni=128
set msgsys:msginfo_msgtql=8192
set semsys:seminfo_semmni=1024
set semsys:seminfo_semmsl=512
set semsys:seminfo_semopm=512
set shmsys:shminfo_shmmax=262144000
set shmsys:shminfo_shmmni=2000
```

4.10.2 When Another HiCommand Suite Product (version 4.0 or later) is Installed

If another HiCommand Suite product (version 4.0 or later) is already installed, the kernel parameter values recommended for that product are required.

For each kernel parameter, set the sum of the recommended values for the HiCommand Suite Common Component, Device Manager server, and the existing HiCommand Suite product.

For the recommended values for the HiCommand Suite product, see the appropriate product manual or Release Notes.

Caution: In Solaris 10, specify the kernel parameters for both the user.root project and the system project.

Caution: After changing the kernel parameters, execute the `shutdown -y -i6 -g0` command to restart the system.

4.10.3 Setup Needed After Uninstallation of the Device Manager Server

If kernel parameters were already set when you installed the Device Manager server, restore them to their previous settings by following the instructions for the version of your OS as shown below:

For Solaris 8 or Solaris 9:

Replace the current file with the `/etc/system` file that you backed up.

For Solaris 10:

Set the recorded settings. (For details about how to do this, see the manuals of the OS.)

If kernel parameters were not set, and you did not back up the above file, restore the settings to the initial values for the OS.

Caution: After changing the kernel parameters, execute the `shutdown -y -i6 -g0` command to restart the system.

4.11 Setting Kernel Parameters and Shell Restrictions on Linux

Before installing the Device Manager server, you must set the OS parameters (kernel parameters and shell restrictions). If the kernel parameters have not been set correctly, installation fails.

When you uninstall the Device Manager server, you must change the kernel parameters and shell restrictions back to the previous settings specified before the installation of the Device Manager server.

The following describes the procedure for setting the kernel parameters and shell restrictions in a Linux environment.

Before changing kernel parameter settings and shell restrictions, back up the `/etc/sysctl.conf` file and `/etc/security/limits.conf` file. You can use the backup files to restore the previous kernel parameter settings and shell restrictions after you uninstall the Device Manager server.

Table 4.13 below shows the recommended values for the shell restrictions and Table 4.14 shows the recommended values for the kernel parameters you must set.

Refer to these two tables, to set the shell restrictions and kernel parameters according to the following formula (in the formula, "Max {x, y, z}" means using the maximum value among x, y, and z).

- `kernel.shmmax`:

  setting-value-of-the-kernel-parameter =

  Max {*currently-set-value-for-the-kernel-parameter*#, recommended-value-for-HiCommand-Suite-Common-Component + recommended-value-for-the-Device-Manager-server, recommended-value-for-HiRDB}

- `kernel.shmall`:

  setting-value-of-the-kernel-parameter =

  currently-set-value-for-the-kernel-parameter#+ recommended-value-for-HiCommand-Suite-Common-Component + recommended-value-for-the-Device-Manager-server + recommended-value-for-HiRDB

- All other kernel parameters and shell restrictions:

  setting-value-of-the-shell-restriction-or-kernel-parameter =

  Max {*currently-set-value-for-the-kernel-parameter*#+ recommended-value-for-HiCommand-Suite-Common-Component + recommended-value-for-the-Device-Manager-server, recommended-value-for-HiRDB}

#: A user specified value or an initial value of the OS

Caution: The setting value of each kernel parameter and shell restriction must not exceed the maximum value defined for the OS.

Caution: Set the shell restrictions for both `soft` and `hard`. At this time, you must set the value for `soft` to a value that is smaller than the value for `hard`.

Caution: After changing the kernel parameters or shell restrictions, execute the `reboot` command to restart the system.

The installer of the Device Manager server checks each kernel parameter and shell restriction by referring to the installer checking values listed in the table below. If a specified value is less than the corresponding installer checking value, installation fails.

Table 4.13 Recommended Values for Shell Restrictions (`/etc/security/limits.conf`)

Shell Restriction	Recommended Value for HiRDB	Recommended Value for HiCommand Suite Common Component	Recommended Value for the Device Manager Server	Installer Checking Value
`nofile (soft/hard)`	1344	572	0	1596
`nproc (soft/hard)`	512	165	1	5862

An example of setting shell restrictions is shown below.

```
#<domain>      <type>  <item>         <value>
#
*               soft    nofile          1596
*               hard    nofile          1596
*               soft    nproc           5862
*               hard    nproc           5862
```

Table 4.14 Recommended Values for Kernel Parameters (`/etc/sysctl.conf`)

Kernel Parameter	Recommended Value for HiRDB	Recommended Value for HiCommand Suite Common Component	Recommended Value for the Device Manager Server	Installer Checking Value
`fs.file-max`	53898	53898	1075	90150
`kernel.threads-max`	576	184	20	11596
`kernel.msgmni`	32	32	0	48
`kernel.sem` (4th parameter)	1024	9	1	1024
`kernel.sem` (2nd parameter)	7200	80	44	32124
`kernel.shmmax`	200000000	11542528	74022920	200000000
`kernel.shmmni`	2000	0	0	4096
`kernel.shmall`	22418432	22418432	79520488	126454504

4.11.1 Setup Needed After Uninstallation of the Device Manager Server

If kernel parameters and shell restrictions were already set when you installed the Device Manager server, restore them to their previous settings from the following files that you backed up before installation.

- `/etc/sysctl.conf`
- `/etc/security/limits.conf`

If kernel parameters and shell restrictions were not set, and you did not back up the above files, change the settings to the initial values of the OS.

Caution: After changing the kernel parameters or shell restrictions, execute the `reboot` command to restart the system.

Chapter 5 Using the HiCommand Suite Common Component

The HiCommand Suite Common Component provides features that are used by all HiCommand Suite products. Each HiCommand Suite product will bundle the Common Component.

This chapter discusses the following functions:

- Installing and Uninstalling the Common Component (see section 5.1)
- Starting and Stopping the Common Component (see section 5.2)
- Integrated Logging (see section 5.3)
- Ports Used By the Common Component (see section 5.4)
- Setup for Starting a Web Application From Web Client (see section 5.5)
- Settings When Changing the Network Settings for the Management Server or When Performing Maintenance (see section 5.6)
- Security Settings for User Accounts (see section 5.7)
- Warning Banner Settings (see section 5.8)
- Generating Audit Logs (see section 5.9)

5.1 Installing and Uninstalling HiCommand Suite Common Component

The Common Component must be installed or uninstalled as part of the installation or uninstallation of another HiCommand product, e.g., Device Manager or Tuning Manager. You cannot install or uninstall just the Common Component.

Installation of the Common Component will include the Hitachi Network Objectplaza trace common library.

Whether the Common Component is either installed or upgraded during Device Manager installation is determined by following factors:

- If the Common Component is not previously installed on the system, the Device Manager installer will install it.
- If the previously installed Common Component version is earlier than or the same as the Common Component version to be installed, the Device Manager installer will upgrade Common Component by overwriting the previous version.
- If the previously installed Common Component version is older than or equal to the installing Common Component version, the Device Manager installer will upgrade the Common Component by overwriting the previous installation.
- If the previously installed Common Component version is newer than the installing Common Component version, the previously installed version is left intact.

Whether the Common Component is uninstalled or left in place during Device Manager uninstallation is determined by the following factors:

- If any other HiCommand Suite products are using the Common Component, the Common Component will not be uninstalled. The Common Component will not be uninstalled until the last HiCommand Suite product that uses the Common Component is uninstalled.
- If the Common Component is being used by only by Device Manager, it will be uninstalled as part of the Device Manager uninstallation process.

Table 5.1 describes the Common Component elements that are used by Device Manager.

Table 5.1 Device Manager Common Component Elements

Function	Description
HBase Storage Mgmt Common Service	A customer who operates multiple HiCommand Suite products is not prompted to re-enter their user ID and password if that customer is using those products simultaneously. HBase Storage Mgmt Common Service provides a unified user authentication mechanism.
Integrated logging information	Operation and other types of logs are concentrated by an integrated logging information feature. Providing a common log repository allows all HiCommand Suite log files to be in the same file.

5.2 Starting and Stopping HiCommand Suite Common Component

5.2.1 Starting the Common Component

Ordinarily you should not need to manually start the Common Component.

To start HiCommand Suite Common Component, start the following services:

- HBase Storage Mgmt Web Service
- HBase Storage Mgmt Common Service
- HiRDB

To start the Common Component in a Windows environment:

1. Log in to the system as a user with Administrator privileges.
2. Start the Common Component.

   <common component installation folder>\bin\hcmdssrv /start /server HBase

   The following shows an example of executing the command:

   C:\Program Files\HiCommand\Base\bin\hcmdssrv /start /server HBase
3. Verify that the Common Component has started.

   <common component installation folder>\bin\hcmdssrv /status

   The following shows an example of executing the command:

   C:\Program Files\HiCommand\Base\bin\hcmdssrv /status
4. If the following messages appear, the services are running:

   KAPM06440-I The HiRDB service has already started.

   KAPM05007-I Already started service. service-name=HBase Storage Mgmt Web Service

   KAPM05007-I Already started service. service-name=HBase Storage Mgmt Common Service

To start the HiCommand Suite Common Component in a Solaris or Linux environment:

1. Log in to the system as root.
2. Start the Common Component.

   # /opt/HiCommand/Base/bin/hcmdssrv -start -server HBase
3. Verify that the Common Component has started.

   # /opt/HiCommand/Base/bin/hcmdssrv -status
4. If the following messages appear, the services are running:

   KAPM06440-I The HiRDB service has already started.

   KAPM05007-I Already started service. service-name=HBase Storage Mgmt Web Service

KAPM05007-I Already started service. service-name=HBase Storage Mgmt Common Service

5.2.2 Stopping the Common Component

To stop HiCommand Suite Common Component, stop the following services:

- HBase Storage Mgmt Web Service
- HBase Storage Mgmt Common Service
- HiRDB

When you stop the above services, you must also stop the services of HiCommand Suite products at the same time. For details about how to stop HiCommand Suite Common Component and the services of HiCommand Suite products at the same time, see section 3.5 in Windows, and see section 4.5 in Solaris and Linux.

You might want to stop HBase Storage Mgmt Common Service in order, for example, for the changes to properties to take effect. The following shows how to stop HBase Storage Mgmt Common Service.

To stop HBase Storage Mgmt Common Service in a Windows environment:

1. Log on as an administrator.
2. Stop the Common Component using the following command:

   <common component installation folder>\bin\hcmdssrv /stop /server HBase

   The following shows an example of executing the command:

   C:\Program Files\HiCommand\Base\bin\hcmdssrv /stop /server HBase
3. Execute the following command to check whether HBase Storage Mgmt Common Service has stopped:

   <common component installation folder>\bin\hcmdssrv /status /server HBase

   The following shows an example of executing the command:

   C:\Program Files\HiCommand\Base\bin\hcmdssrv /status /server HBase
4. If the following messages appear, the services have stopped:

   KAPM05009-I Already stopped service. service-name= HBase Storage Mgmt Common Service.

To stop HBase Storage Mgmt Common Service in a Solaris or Linux environment:

Caution: When stopping HiCommand Suite Common Component in a Solaris or Linux environment, do not execute the stop command (`hcmdssrv -stop`) before HiCommand Suite Common Component has completed startup. Regardless of whether a resident process for the service is running, the service status displayed by the `status` option might indicate that the service has stopped, and the service might be unable to be stopped by the `stop` option. In such cases, reboot the system.

1. Log in to the system as root.

2. Stop the Common Component.

   # /opt/HiCommand/Base/bin/hcmdssrv -stop -server HBase

3. Execute the following command to check whether HBase Storage Mgmt Common Service has stopped:

   # /opt/HiCommand/Base/bin/hcmdssrv -status -server HBase

4. If the following messages appear, the services have stopped:

   KAPM05009-I Already stopped service. service-name=HBase Storage Mgmt Common Service

5.3 Integrated Logging

5.3.1 Integrated Log Output

The Common Component provides common log files and a common library for log output for each program product in the HiCommand Suite. Device Manager uses this information to show the details for the log files.

Table 5.2 Integrated Log Output

Log Type	Log Name	Description	Location (Windows)	Location (Solaris, Linux)
Common trace log file	hntr2*.log	Integrated trace log information produced by the Common Component. The asterisk (*) in the file name indicates a file number. For details on specifying the number and size of files, see section 5.3.2 The characters below will be output after being converted as follows if they are contained in a message whose error code is in the range from `KAIC00000` to `KAIC09999`: ▪ Line feed character: Converted to an at mark (`@`). ▪ At mark (`@`): Converted to `\@`.	`C:\Program Files\Hitachi\HNTRLib2\spool`	`/var/opt/hitachi/HNTRLib2/spool`
Event log/syslog file	Eventlog	Windows event log (including the audit log). For details on the audit logs, see section 5.9	Event viewer	N/A
	syslog	Solaris or Linux system log (including the audit log). For details on the audit logs, see section 5.9	N/A	Defined by `/etc/syslog.co`
Device Manager log file	version	Version information about the operating environment of the Device Manager Server (Device Manager Server, Java VM, and operating system)	*<installation directory>*`\HiCommandServer\logs`	`/opt/HiCommand/HiCommandServer/logs`

Log Type	Log Name	Description	Location (Windows)	Location (Solaris, Linux)
Device Manager trace log file (Common Component)	HDvMtrace*.log	Trace log information output by the Common Component and used by the Device Manager Server. The asterisk (*) in the file name indicates a file number. The characters below will be output after being converted as follows if they are contained in a message whose error code is in the range from KAIC00000 to KAIC09999: ▪ Line feed character: Converted to an at mark (@). ▪ At mark (@): Converted to \@.	<*installation directory*>\HiCommandServer\logs	/opt/HiCommand/HiCommandServer/logs

5.3.2 Common Component Trace Log Properties

WARNING: Changing the common trace log settings affects other program products that use the common trace log.

You can specify a maximum of 16 for the number of trace log files (see section 5.3.2.2). Larger numbers of trace log files can make it more difficult to find specific information.

You can also specify the size of each Common Component trace log file, from 8 KB to 4 MB (4096 KB) (see section 5.3.2.2). The Common Component trace log monitoring program switches to the next file when the current output file reaches the specified size.

Note: The value should be larger than the value that you have set in the buffer.

5.3.2.1 Specifying the Number of Trace Log Files (Windows)

The Windows **HNTRLib2** utility is located as follows:

C**:\Program Files\Hitachi\HNTRLib2\bin\hntr2util.exe**

To specify the number of trace log files:

1. Log in to the system as a user with **administrator** privileges.
2. Execute hntr2util.exe.

   The Hitachi Network Objectplaza Trace Utility 2 panel is displayed.

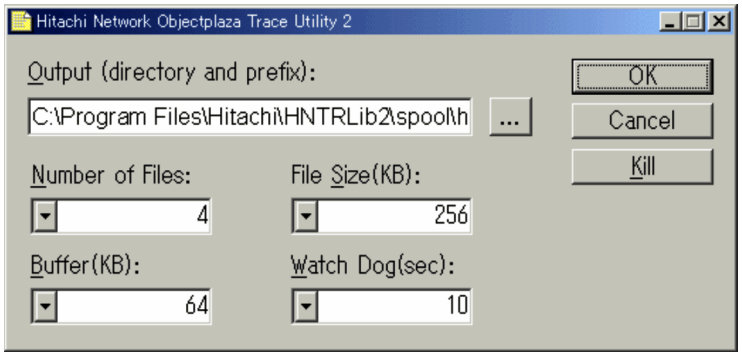

Figure 5.1 Hitachi Network Objectplaza Trace Utility 2 Panel

3. Type the desired number of trace log files, and then select **OK.**

5.3.2.2 Specifying the Size of Trace Log Files (Windows)

The Windows **HNTRLib2** utility is stored on the following path:

C:\Program Files\Hitachi\HNTRLib2\bin\hntr2util.exe

To change the size of the trace log files:

1. Log in to the system as a user with Administrator privileges.
2. Execute hntr2util.exe.

   The Hitachi Network Objectplaza Trace Utility 2 panel is displayed (see Figure 5.2).
3. Type the desired size for the trace log files, and then select OK.

5.3.2.3 Specifying the Number of Trace Log Files (Solaris or Linux)

Solaris or Linux:

The utility program is stored in the following path:

 # /opt/hitachi/HNTRLib2/bin/hntr2util

1. Log in to the system as root.
2. Execute `hntr2util`.

   A menu appears.
3. From the menu, select **Number of log files**.

   The submenu appears.

```
Hitachi Network Objectplaza Trace Library 2 - Configuration Utility Rel 1.0
  Type the number of files [1-16] (Type '!' to return)

  Current Number: 4
      New Number:
```

4. In the submenu, enter the desired number for trace log files, and then press **Enter**. If you do not want to change the number, enter `!`, and then press **Enter**.

5. Check the contents you specified, enter `e`, and then press **Enter**.

   A message appears to check if you want to save the changes.

6. Enter `y` to save your changes or enter `n` to exit without saving your changes.

5.3.2.4 Selecting the Size of Trace Log Files (Solaris and Linux)

Solaris or Linux:

The utility program is stored in the following path:

/opt/hitachi/HNTRLib2/bin/hntr2util

To change the size of the trace log files:

1. Log in to the system as root.
2. Execute `hntr2util`.

   A menu appears.

3. From the menu, select **Size of a log file**.

   The submenu appears.

```
Hitachi Network Objectplaza Trace Library 2 - Configuration Utility Rel 1.0
  Type new file size [8-4096] (Type '!' to return)

  Current Size(KB): 256
      New Size(KB):
```

4. In the submenu, enter the desired size for the trace log files, and then press **Enter**. If you do not want to change the size, enter `!`, and then press **Enter**.
5. Check the contents you specified, enter `e`, and then press **Enter**.

   A message appears to check if you want to save the changes.

6. Enter `y` to save your changes or enter `n` to exit without saving your changes.

5.4 Ports Used By HiCommand Suite Common Component

5.4.1 Ports Used by Device Manager Server and Common Component

Table 5.3 lists the ports used by the Device Manager Server and the Common Component.

Table 5.3 Device Manager Server and Common Component Ports

Component	Network Port	Description
Device Manager Server	2001/tcp	Used by the Device Manager HTTP (web) Server to communicate with the Web Client and the Device Manager Agent. You can change the port using the `server.http.port` property. For details, see section 8.2.2.

Component	Network Port	Description
	snmptrap:162/udp	Used for receiving SNMP traps from the subsystem(s).
	2443/tcp	Used by the Device Manager Server to use SSL-based communication with the CLI, the Web Client, and the Device Manager Agent. You can change this port by modifying the `server.https.port` property. For details, see section 8.2.3.
Device Manager agent	24041/tcp	Used for the Device Manager agent's daemon process (or service). You can change the port using the `server.agent.port property`. ***Note:*** For more information see *HiCommand Device Manager Agent Installation Guide*.
	24042/tcp	Used for the Device Manager agent HTTP (web) server. You can change this port by modifying the `server.http.port` property file. ***Note:*** For more information see *HiCommand Device Manager Agent Installation Guide*.
	24043/tcp	Used for communication between the Device Manager agent's daemon process and the web server process. You can change the port using the `server.http.localPort` property. ***Note:*** For more information see *HiCommand Device Manager Agent Installation Guide*.
HiCommand Suite Common Component	23015/tcp	Used by the Device Manager server to access non-SSL HBase Storage Mgmt Web Service.
	23016/tcp	Used by web browsers to access SSL HBase Storage Mgmt Web Service. If you want to change this port number after installation, see section 5.4.2. (Device Manager does not use this port).
	23017/tcp	Used by the HBase Storage Mgmt Web Service to access HBase Storage Mgmt Common Service through an AJP connection. If you want to change this port number after installation, see section 5.4.2.
	23018/tcp	Used by HBase Storage Mgmt Common Service and to receive a stop request. If you want to change this port number after installation, see section 5.4.2.
	23032/tcp	Used by HiRDB. If you want to change this port number after installation, see section 5.4.2.
	From 23019/tcp to 23031/tcp, 23033/tcp, and 23034/tcp	Reserved port
	45001/tcp	49000/tcp Used by HiRDB internal communication. Do not use these ports.

Note: If you update the database used by the Device Manager server (version 2.3 to version 3.5) to a database that can be used by the Device Manager server version 4.0, use the port numbers of gds_db:3050/tcp and interserver:3060/tcp.

5.4.2 Changing Ports Used by Common Component

After installing Device Manager, if you want to change the any of the ports used by the Common Component, use the following procedure:

1. If HiCommand Suite products whose versions are earlier than 5.7 are running, stop their services.

   For details about how to stop these services, see the manual for your product version.

2. Stop the services of HiCommand Suite products and HiCommand Suite Common Component.

   For Windows:

   Select **Start**, **Program**, **HiCommand**, **Device Manager**, and then **Stop Server with Common Services**.

   Solaris or Linux:

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

3. Edit the setup file, and change the port number. For details about each port's setup file, see section 5.4.2.1 to 5.4.2.5.

4. Start the service of the Device Manager server, the services of other HiCommand Suite products, and HiCommand Suite Common Component.

   For Windows:

   Select **Start**, **Program**, **HiCommand**, **Device Manager**, and then **Start Server with Common Services**.

   Solaris or Linux:

   # /opt/HiCommand/Base/bin/hcmdssrv -start

5. If HiCommand Suite products whose versions are earlier than 5.7 have been installed, start their services as required.

   For details about how to start these services, see the manual for your product version.

5.4.2.1 23015/tcp (For Accessing Non-SSL HBase Storage Mgmt Web Service)

To change the port used for accessing the non-SSL HBase Storage Mgmt Web Service, you must change the port number written in the following file:

Windows:

- The listen directive in

  <common component installation folder>\httpsd\conf\httpsd.conf

AND

- The port number coded in the listen directive in

  <common component installation folder>\conf\hsso.conf

Solaris or Linux:

- The listen directive in

/opt/HiCommand/Base/httpsd/conf/httpsd.conf

AND

- hsso.hostport in

  /opt/HiCommand/Base/conf/hsso.conf

5.4.2.2 23016/tcp (For Accessing SSL HBase Storage Mgmt Web Service)

To change the port used for accessing SSL HBase Storage Mgmt Web Service, you must change the port number written in the following files:

Windows:

- <VirtualHost host name>:port number in

  <common component installation directory>\httpsd\conf\httpsd.conf

- The port number described in the listen directive in

  <common component installation directory>\httpsd\conf\httpsd.conf

AND

- hsso.sslport in

  <common component installation folder>\conf\hsso.conf

Solaris or Linux:

- <VirtualHost host name>:port number in

  /opt/HiCommand/Base/httpsd/conf/httpsd.conf

- The port number described in the listen directive

  /opt/HiCommand/Base/httpsd/conf/httpsd.conf

AND

- hsso.sslport in

  /opt/HiCommand/Base/conf/hsso.conf

5.4.2.3 23017/tcp (For HBase Storage Mgmt Common Service Through AJP Connection)

To change the port used for the HBase Storage Mgmt Common Service through an AJP connection, you must change the port number written in the following files:

Windows:

- worker.worker1.port in

  <common component installation directory>\cc\web\redirector\workers.properties

  AND

- webserver.connector.ajp13.port in

  <common component installation directory>\cc\web\containers\HiCommand\usrconf\userconf.properties

Solaris or Linux:

- worker.worker1.port in

  /opt/HiCommand/Base/CC/web/redirector/workers.properties

  AND

- webserver.connector.ajp13.port in

  /opt/HiCommand/Base/CC/web/containers/HiCommand/usrconf/usrconf.properties

5.4.2.4 23018/tcp (Used for Stop Requests to HBase Storage Mgmt Common Service)

To change the port through which the HBase Storage Mgmt Common Service Service receives a stop request, you must change the port number written in the following file:

Windows:

- webserver.shutdown.port in

  <common component installation directory>\cc\web\containers\HiCommand\usrconf\userconf.properties

Solaris or Linux:

- webserver.shutdown.port in

  /opt/HiCommand/Base/CC/web/containers/HiCommand/usrconf/usrconf.properties

5.4.2.5 23032/tcp (Used for HiRDB)

To change the port used by HiRDB, you must change the port number written in the following file:

Windows:

- PDNAMEPORT in

  <common component installation folder>\HDB\CONF\emb\HiRDB.ini

- pd_name_port in

  <common component installation folder>\HDB\CONF\pdsys

AND

- pd_name_port in

  <common component installation folder>\database\work\def_pdsys

Solaris or Linux:

- PDNAMEPORT in

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

- pd_name_port in

  /opt/HiCommand/Base/HDB/conf/pdsys

AND

- pd_name_port in

  /opt/HiCommand/Base/database/work/def_pdsys

5.5 Setup for Starting a Web Application from Web Client

5.5.1 Using hcmdslink to Register an Application

When you choose **Go** and then **Links** in the global tasks bar area of Web Client a dialog box is displayed with links for starting applications for which the user is registered. By registering the web applications that you often use or the information that you want to reference (such as a device installation chart) to this window, you can easily call a desired application from Web Client. To register a desired application or cancel the registration, you use the hcmdslink command. This section describes how to use the **hcmdslink** command.

Format:

In Windows:

<common component installation folder>\bin\hcmdslink {/add | /delete } /file user-defined-application-file [/nolog] /user user-identifier /pass password

In Solaris or Linux:

/opt/HiCommand/Base/bin/hcmdslink {-add | -delete } -file user-defined-application-file-name [-nolog] -user user-identifier -pass password

Function:

The **hcmdlink** command registers a web application to allow you to start the desired application from Web Client, or cancels the registration.

In the user-defined application file, you specify a desired application name, URL, and name to be displayed. Then, use the hcmdslink command to register that information. The link to the registered application will be displayed in the link dialog box that appears when you choose **Go** and then **Links** in the global tasks bar area of Web Client.

Note: Once you register a link for starting an application, do not delete the user-defined application file used in the hcmdslink command. If you do, you cannot delete the link for the registered application.

Options:

add: Registers an application.

delete: Deletes an application.

file: Specifies the name of the user-defined application file. In Solaris or Linux, do not specify a path that includes a space.

user: Specifies a user ID used to register or delete the user-defined application link. Specify the user ID of a user who has the Admin permission.

pass: Specifies the password for the user ID used to register or delete the user-defined application link.

nolog: Suppresses outputting messages to the command line. However, even when this option is specified, messages for option errors are displayed.

User-defined application file:

The following shows a coding example in the user-defined application file:

Caution: To code the user-defined application file, use ASCII code only. Also note that you cannot use the control code other than the CR and LF control code.

```
@TOOL-LINK
@NAME SampleApp
@URL http://SampleApp/index.html
@DISPLAYNAME SampleApplication
@DISPLAYORDER 1
@ICONURL http://SampleApp/graphic/icon.gif
@TOOL-END
```

The items to be specified in the user-defined application file are as follows:

@TOOL-LINK: The start key. The information between the start key and the end key is the setting information. This item is required.

@NAME: Information used as the key for registration. Specify a unique name. This item is required. The maximum length of the name is 256 bytes. Use alphanumeric characters only.

@URL: The URL of the target of the link from Web Client. The maximum length of the URL is 256 bytes.

@DISPLAYNAME: The name displayed in the link dialog box that appears when you choose **Go** and then **Links** in the global tasks bar area of Web Client. If no information is specified, the name specified in @NAME is displayed. You can specify a Unicode code point in the range from U+10000 to U+10FFFF. The maximum length of the name is 80 characters.

@DISPLAYORDER: The order of the applications displayed in the link dialog box that appears when you choose **Go** and then **Links** in the global tasks bar area of Web Client. The applications are displayed in ascending order of this value. You can specify a value in the range from -2147483648 to 2147483647.

@ICONURL: The URL of the icon displayed beside the link. The maximum length of the URL is 256 bytes.

@TOOL-END: The end key. This item is required.

Return values:

- 0: Normal termination
- 255: Failure

If you do not specify the nolog option, you can judge whether or not the command was successful from the output message. If you specify the nolog option, no message is output. Therefore, you need to use the return value of the command to judge whether or not the command was successful. For details about errors, see the contents of the log file (hcmdslink[n].log).

Command execution examples:

When adding a link for an application:

C:\Program Files\HiCommand\Base\bin\hcmdslink /add /file C:\SampleLink.txt /user system /pass manager

When deleting a link for an application:

C:\Program Files\HiCommand\Base\bin\hcmdslink /delete /file C:\SampleLink.txt /user system /pass manager

5.5.2 Modifying the URL Information for Starting Web Client

Important: If your Device Manager Server at the recovery site has a different IP address, and you need to switch to that site, then you must change the URL pointers as described in this section. The URL must be fully qualified, e.g., http://192.168.1.100:23015<http://192.168.1.100:23015/>

Once you begin to operate Device Manager, if any of the following changes are made in the configuration, you need to modify the access information (URL information) used to start Web Client:

- Change to the IP address of a host in which the Device Manager Server is installed
- Change to a port used by HBase Storage Mgmt Web Service
- Change to the setting of the Device Manager system in order to use or stop using SSL
- Change to a remote server (for example, in the case of a remote site for disaster recovery)

The access information is stored in the database of Common Component.

To modify information stored in the database, use the hcmdschgurl command described below.

Format:

In Windows:

<common component installation folder>\bin\hcmdschgurl {/print | /change old-URL new-URL }

In Solaris or Linux:

/opt/HiCommand/Base/bin/hcmdschgurl {-print | -change old-URL new-URL }

Function:

The hcmdschgurl command updates the access information (URL information) used to start each application. The access information is stored in the database of Common Component.

Options:

print: Displays a list of URLs and programs that are currently set up

change: Overwrites the information about the currently registered URL with the information about the new URL. Specify the currently registered URL and the new URL. The specified URL must be a complete URL that contains protocols and port number.

Return values:

- 1: Argument error
- 2: URL does not exist
- 253: Restoration failure
- 254: Backup failure
- 255: Abnormal termination

For details about the errors, see the contents of the log file (HcmdsChangeURL[n].log).

Command execution example:

The following shows examples of the hcmdschgurl command execution.

1. First, execute the command with specifying the print option to find the URL information registered in the current database.
2. Next, execute the command with specifying the change option to update the URL information. In the following example, the URL information http://192.168.11.33:23015 is changed to http://192.168.11.55:23015.
3. Finally, execute the command with specifying the print option to confirm the results.

   > C:\Program Files\HiCommand\Base\bin\hcmdschgurl /print
   http://192.168.11.33:23015 DeviceManager

   > C:\Program Files\HiCommand\Base\bin\hcmdschgurl /change
   http://192.168.11.33:23015
   http://192.168.11.55:23015

   The URL was changed from "http://192.168.11.33:23015" to "http://192.168.11.55:23015".

   > C:\Program Files\HiCommand\Base\bin\hcmdschgurl /print
   http://192.168.11.55:23015 DeviceManager

5.6 Settings When Changing the Network Settings for the Management Server or When Performing Maintenance

You first need to edit several settings files when you disconnect the network (to which the management server is connected) in order to change the network settings or to perform maintenance, or when you change the name of the management server. This section describes how to edit the settings files.

5.6.1 When Disconnecting the Management Server Network

When disconnecting the network to change the NIC, performing hub maintenance, or other reasons, you must change the settings files of Device Manager beforehand.

If you disconnect the network without changing the settings files, you will not be able to perform operations on Web Client and CLI because the Device Manager server stops running. To return to the status in which you can perform operation on Web Client and CLI, you need to restart the machine where Device Manager is installed.

The procedure to change the settings file is described in steps 1 through 7 below. You do not need to perform these steps the next time you disconnect the network.

To disconnect the network:

1. If HiCommand Suite products whose versions are earlier than 5.7 are running, stop their services.

   For details about how to stop these services, see the manual for your product version.

2. Stop the services of HiCommand Suite products and HiCommand Suite Common Component.
   - In Windows:

     Select **Start**, **Program**, **HiCommand**, **Device Manager**, and then **Stop Server with Common Services**.
   - In Solaris or Linux:

     Execute the following command:

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

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

   Change the value for the `pdunit` parameter's `-x` option to the loopback address `127.0.0.1`.

   The default installation locations of the `pdsys` file and `def_pdsys` file are as follows:
   - In Windows:

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

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

- In Solaris or Linux:

  /opt/HiCommand/Base/HDB/conf/pdsys

  /opt/HiCommand/Base/database/work/def_pdsys

4. Edit the pdutsys file and the 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 to set a loopback address.

   The default installation locations of the pdutsys file and def_pdutsys file are as follows:

   - In Windows:

     installation-folder-for-HiCommand-Suite-Common-Component\HDB\CONF\pdutsys

     installation-folder-for-HiCommand-Suite-Common-Component\database\work\def_pdutsys

   - In Solaris or Linux:

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

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

5. Edit the HiRDB.ini file.

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

   The default installation locations of the HiRDB.ini file is as follows:

   - In Windows:

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

   - In Solaris or Linux:

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

6. Restart the machine.

7. Execute the following command to make sure that the HiCommand Suite Common Component service is running:

   - In Windows:

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

   - In Solaris or Linux:

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

8. Disconnect the network, and then change the settings or perform maintenance.

9. After the network becomes available, start the service of the Device Manager server, the services of other HiCommand Suite products, and HiCommand Suite Common Component.

   - In Windows:

Select **Start**, **Program**, **HiCommand**, **Device Manager**, and then **Start Server with Common Services**.

– In Solaris or Linux:

Execute the following command:

```
# /opt/HiCommand/Base/bin/hcmdssrv –start
```

10. If HiCommand Suite products have been installed, start their services as required.

For details about how to start these services, see the manual for your product.

5.6.2 When Changing the Host Name of the Management Server

This subsection describes the procedure for changing the host name of the management server.

Caution: The host name must satisfy the following conditions:

- Number of characters: no more than 32 bytes
- Characters that are used: A to Z, a to z, 0 to 9, hyphens (-)

Note that the host name cannot start with and end with a hyphen (-).

Caution: If you change the host name of the management server before you change the host name in the Device Manager settings file, use the `hostname` command to display and write down the changed host name (for Windows, the `ipconfig /ALL` command can also be used to display host names). For the host name in the Device Manager settings file, specify the name you recorded earlier. Note that this name is case-sensitive.

To edit the settings files:

1. If HiCommand Suite products whose versions are earlier than 5.7 are running, stop their services.

   For details about how to stop these services, see the manual for your product version.

2. Stop the Device Manager server and HiCommand suite Common Component.

   For Windows:

   Choose **Start, Program, HiCommand, Device Manager**, and then **Stop Server with Common Services**

   For Solaris or Linux:

   Execute the following command:

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

3. 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 Chapter 7.

4. 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 or Linux:

/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.

Important: Proceed to the next step according to the following cases:

- For a cluster configuration:

  Proceed to step 5.

- For a non-cluster configuration:

  If you performed a new installation of version 5.0 or later, or performed a new installation of version 5.0 or later and then performed a re-installation, skip to step 9. In other cases, proceed to step 5.

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

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

   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

6. 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 loopback address.

   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_pdutsys

   For Solaris:

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

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

7. 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:

   For Windows:

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

   For Solaris:

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

8. Edit the `cluster.conf` file (applicable only for a cluster configuration).

   Change the corresponding logical host name, executing node's host name, and standby node's host name to the host names 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

9. 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, just restart the machine.

10. 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 or Linux:

    opt/HiCommand/Base/bin/hcmdssrv -status

11. Execute the `hcmdschgurl` command to change the host name in the URL for starting Web Client. For details on how to use the `hcmdschgurl` command, see section 5.5.2.

5.7 Security Settings for User Accounts

To prevent users' passwords from being guessed by a third party, HiCommand Device Manager allows password conditions (the minimum number of characters and the combination of characters that can be used) to be specified. You can also have user accounts locked automatically if the wrong password is repeatedly entered for a specific user ID.

Security settings can also be specified from Web Client. However, if the system is in a cluster configuration, the settings from Web Client are only applied to the executing node. To apply the settings to the standby node, switch the nodes, and then specify the same settings. For details on how to operate Web Client, see the *HiCommand Device Manager Web Client User's Guide*.

Caution: When installing version 5.1 or later of HiCommand Suite Common Component, the user account lock function and password complexity check function will be usable. These functions are enabled for users of all HiCommand Suite products, so the following problems might occur in operations of HiCommand Suite products that are version 5.0 or earlier:

- A user is unable to log in even with a correct user ID and password.

  The user account might be locked. Take appropriate action such as unlocking the relevant account or registering a new user account.

- A password is unchangeable, or a user account is not addable.

  The specified password might not follow the password-entry rules. Specify an appropriate password, following the output message.

The password conditions and settings related to account locking are implemented from the `security.conf` file.

In a Windows system, the `security.conf` file is stored in the following folder:

```
installation-folder-for-HiCommand-Suite-Common-Component\conf\sec
```

In a Solaris or Linux system, the `security.conf` file is stored in the following directory:

```
/opt/HiCommand/Base/conf/sec
```

The password conditions that you set in the `security.conf` file are applied when a user account is created or when a password is changed, and are not applied to passwords of existing user accounts. As a result, even if an existing password does not satisfy the password conditions, a user can use the password to log in to the system.

When you change a setting in the `security.conf` file, the change takes effect immediately.

The items you can set in the `security.conf` file are described below.

5.7.1 password.min.length

Specifies the minimum number of characters that can be set as a password. Specify a value in the range from 1 to 256.

Default: `4`

5.7.2 password.min.uppercase

Specifies the minimum number of uppercase letters the password must contain. Specify a value in the range from `0` to 256. If you specify `0`, no restriction applies.

Default: `0` (no restriction)

5.7.3 password.min.lowercase

Specifies the minimum number of lowercase letters the password must contain. Specify a value in the range from `0` to 256. If you specify `0`, no restriction applies.

Default: `0` (no restriction)

5.7.4 password.min.numeric

Specifies the minimum number of numeric characters the password must contain. Specify a value in the range from `0` to `256`. If you specify `0`, no restriction applies.

Default: `0` (no restriction)

5.7.5 password.min.symbol

Specifies the minimum number of symbols the password must contain. Specify a value in the range from `0` to `256`. If you specify `0`, no restriction applies.

Default: `0` (no restriction)

5.7.6 password.check.userID

Specifies whether the password can be the same as the user ID. Specify `true` or `false`. When `true` is specified, passwords cannot be the same as the corresponding user ID. When `false` is specified, passwords can be the same as the corresponding user ID.

Default: `false` (passwords can be the same as user IDs)

5.7.7 account.lock.num

Specifies the number of unsuccessful logon attempts to allow before a user account is automatically locked. If a user makes the specified number of unsuccessful logon attempts, his or her user account will be locked. However, the `System` account cannot be locked. Specify a value in the range from `0` to `10`. If you specify `0`, any number of unsuccessful logon attempts is allowed.

Unsuccessful attempts to log on to other products in the HiCommand Suite that use the Single Sign-On feature count towards the number of unsuccessful logon attempts. For example, if the number of unsuccessful attempts is set to `3`, and a user fails to log on to Device Manager once, fails to log on to Provisioning Manager once, and then fails to log on to Global Link Availability Manager once, his or her user account will be automatically locked.

If the number of unsuccessful logon attempts is changed, the new number will be applied the next time an attempt to log on fails. For example, when you change the number of unsuccessful logon attempts from `5` to `2`, the account of the user who has already failed to log on for three times is still valid. However, the user account will be locked the next time the user fails to log on.

If a user is currently logged on and you attempt to log on using his or her account, but you fail the specified number of times, his or her user account will be locked. However, the user can continue to perform operations while still logged on.

You can unlock user accounts from Web Client. You must have the User Management permission to unlock a user account. For details about unlocking user accounts, see the *HiCommand Device Manager Web Client User's Guide*.

Default: `0` (user accounts will not be locked)

5.8 Warning Banner Settings

In HiCommand Suite Common Component version 5.1 or later, an optional message (warning banner) can be displayed as a security risk measure at login. Issuing a warning beforehand to third parties that might attempt invalid access can help reduce the risk of problems such as data loss or information leakage.

The message displayable on the Login panel must be no more than 1,000 characters. If a message with the same content is registered in a different language for each locale, the message can be automatically switched to match the locale of the web browser.

When setting up a message, you must log on as a user who has the Administrator permissions in Windows, or as the root user in Solaris or Linux.

Warning banner settings can also be specified from Web Client. However, if the system is in a cluster configuration, the settings from Web Client are only applied to the executing node. To apply the settings to the standby node, switch the nodes, and then specify the same settings. For details on how to operate Web Client, see the *HiCommand Device Manager Web Client User's Guide*.

5.8.1 Editing the Message

You edit the message in HTML format. No more than 1,000 characters can be used. In addition to the usual characters, you can use HTML tags to change font attributes or place line breaks in desired locations. (The tag characters are also counted in the number of characters.) Usable characters are from the Unicode UTF-8 encoding.

The following show an example of message editing, and the results (the warning banner) after the message has been registered.

Example of Editing a Message:

Table 5.4 Example of Editing a Message

```
<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.
```

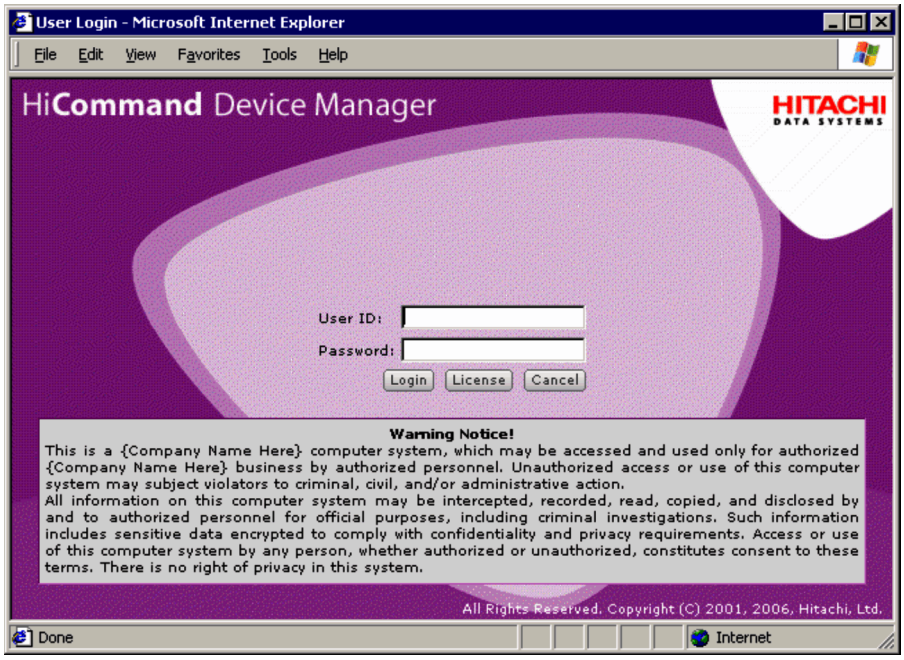

Figure 5.2 Displayed Results After Registering the Message

Caution: When the message is registered, the HTML syntax is neither checked nor corrected. Edit the message correctly in accordance with HTML syntax rules because the edited message will be registered as is. If there is an error in the HTML syntax in the message, the message might not be displayed correctly in the Login panel.

Caution: There are no restrictions on the characters usable in the message, other than that the character encoding must be Unicode (UTF-8). To display a character used in HTML syntax (e.g., <, >, ", ', &), use the HTML escape sequence. For example, to display an ampersand (&) in the Login panel, write `&` in the HTML file.

Caution: To use line breaks to display the message in a desired location, use the HTML tag `<BR>`. Even if there are linefeed characters in the message, they will be ignored when the message is registered.

Note: Sample messages in English (`bannermsg.txt`) and Japanese (`bannermsg_ja.txt`) are provided in the following locations:

- In Windows:

  installation-folder-for-HiCommand-Suite-Common-Component`\sample\resource`

- In Solaris or Linux:

  `/opt/HiCommand/Base/sample/resource`

These sample files are overwritten at installation so, if you wish to use a sample file, copy it and then edit it.

5.8.2 Registering the Message

You use the `hcmdsbanner` command to register an edited message. Execute the following command:

- In Windows:

  installation-folder-for-HiCommand-Suite-Common-Component`\bin\hcmdsbanner /add /file` ***file-name*** `[/locale` ***locale-name***`]`

  The following shows an example of executing the command:

  ```
  C:\Program Files\HiCommand\Base\bin\hcmdsbanner /add /file
  C:\W_Banner\wbfile1 /locale en
  ```

- In Solaris or Linux:

  `# /opt/HiCommand/Base/bin/hcmdsbanner -add -file` ***file-name*** `[-locale` ***locale-name***`]`

file-name

Using an absolute path, specify the file that stores the message. In Solaris or Linux, do not specify a path that includes a space.

local-name

Specify the locale of the language used for the message (e.g., `en` for English, or `ja` for Japanese). If omitted, the default locale will be specified.

When you use Web Client on multiple locales, if you register a message with the same contents in a different language for each locale, the message can be automatically switched to match the locale of the web browser.

The locale for a warning banner displayed in Web Client is set, according to the priority of the language set for the web browser that is used.

If the `locale` option is omitted, you can edit the registered contents from Web Client also. However, available HTML tags are limited when you edit from Web Client.

Return values

0: Normal termination

253: The number of characters in the message exceeds 1,000 characters.

255: Failure

Caution: If a message for the specified locale is already registered, it will be updated by being overwritten.

Note: The execution results of the `hcmdsbanner` command are output to the file `hcmdsbanner`***n***`.log`.

5.8.3 Deleting the Message

You use the `hcmdsbanner` command to delete a registered message. Execute the following command:

- In Windows:

  installation-folder-for-HiCommand-Suite-Common-Component`\bin\hcmdsbanner /delete [/locale` *locale-name*`]`

  The following shows an example of executing the command:

  ```
  C:\Program Files\HiCommand\Base\bin\hcmdsbanner /delete /locale en
  ```

- In Solaris or Linux:

  `# /opt/HiCommand/Base/bin/hcmdsbanner -delete [-locale` *locale-name*`]`

local-name

Specify the locale of the message to be deleted (e.g., `en` for English, or `ja` for Japanese). If omitted, the default locale will be specified.

Return values

0: Normal termination

254: A message of the specified locale has not been registered.

255: Failure

Note: The execution results of the `hcmdsbanner` command are output to the file `hcmdsbannern.log`.

5.9 Generating Audit Logs

Audit logs for Device Manager 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 5.5 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 Lightning/Thunder 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 log files
`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

Categories	Description
Maintenance	Events indicating that a performed maintenance operation succeeded or failed. ▪ 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 section describe the audit log data that can be generated by using Device Manager. For details on the audit log data generated by other products, see the manual for the corresponding product.

5.9.1 Categories of Information Output to Audit Logs in Device Manager

The following table lists the categories of information output to audit logs in Device Manager 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 5.6 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
Authentication	Automatic account lock	Automatic account lock (repeated authentication failure or expiration of account)	4

Category	Type Description	Audit Event	Severity
ConfigurationAccess	User registration	Successful user registration	6
		Failed user registration	3
	User deletion	Successful single user deletion	6
		Failed single user deletion	3
		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 the hcmdsdb command	3
		Successful partial restore using the hcmdsdb command	6
		Failed partial restore using the hcmdsdb command	3
ConfigurationAccess	Database input/output	Successful data output using the hcmdsdbmove command	6

Category	Type Description	Audit Event	Severity
		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
		Failed data output using the hcmdsdbauthmove command	3
		Successful data input using the hcmdsdbauthmove command	6
		Failed data input using the hcmdsdbauthmove command	3
	Device Manager server processing	Request reception (normal)	6
		Request reception (common/abnormal)	3
		Response transmission (normal)	6
		Response transmission (abnormal)	3
	Startup of related products (launch)	Request reception (normal)	6
		Request reception (abnormal)	3
		Response transmission (normal)	6
		Response transmission (abnormal)	3
	Device Manager server (via CIM) processing	Request reception (normal)	6
		Response transmission (normal)	6
		Response transmission (abnormal)	3

5.9.2 Editing Audit Log Environment Settings File

To generate Device Manager 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 the event log files (application log files). For Solaris and Linux, the data is output to the `syslog` file.

Caution: 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:
  installation-folder-for-HiCommand-Suite-Common-Component\conf\sec\auditlog.conf
- For Solaris or Linux:
  /opt/HiCommand/Base/conf/sec/auditlog.conf

The table below shows the items that are set for the `auditlog.conf` file.

Table 5.7 Items 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 5.6), for filtering the output to the `syslog` file. For details about the values that can be specified for `Log.Facility`, see Table 5.8. For details about the correspondence between the severity levels set for audit events and those set in the `syslog.conf` file, see Table 5.9. `Log.Facility` has an effect in Solaris(TM) or Linux 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 5.6. `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 file. For information about the audit events that are output from Device Manager and their severity levels, see Table 5.6. For details about the correspondence between the severity levels of audit events and the types of event log data, see Table 5.9. `Log.Level` has an effect in Windows(R) only. `Log.Level` is ignored in Solaris(TM) and Linux, even if it is specified. Also, if an invalid value or a non-numeric character is specified, the default value is used. Available 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 5.8 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 5.9 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, `Log.Level 6` outputs audit log data corresponding to the Error, Warning, and Information levels. For Solaris(TM) or Linux, `Log.Facility 1` outputs the audit log data to the `syslog` file that is defined as the `user` facility in the `syslog.conf` file.

5.9.3 Format of Output Audit Log Data

This subsection describes the format of output audit log data.

- For Windows:

  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 or Linux:

  The contents of a `syslog` file

  date-time server-name (or *IP-address*) *program-name*[*process-ID*]:*message-portion*

The format and contents of *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- data-type-information*,*application-identification-information*,
reserved-area,*message-text*

Table 5.10 Information Output to message-portion

Item#	Description
uniform-identifier	Fixed to `CELFSS`.
unified-specification-revision-number	Fixed to `1.1`.
serial-number	Serial number of audit log messages.

Item#	Description
message-ID	Message ID. For details, see section 5.9.4
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- data-type-information	Fixed to `BasicLog`.
application-identification-information	Program identification information.
reserved-area	Not output. This is a reserved space.
message-text	The contents vary according to the audit events. Characters that cannot be displayed are output as asterisks (*).

Some items are not output for some audit events.

Example of message-portion output for the Login audit event:

```
CELFSS,1.1,0,KAPM01124-I,2006-05-15T14:08:23.1+09:00,HBase-SSO,management-
host,Authentication,Success,uid=system,,,,,,,,,,,BasicLog,,,"The login process
has completed properly."
```

5.9.4 Audit Log Message ID

The following two types of audit log message IDs are output:

1. KAPM -: Audit events occurring during HiCommand Suite Common Component processing

   For information on the message text corresponding to each message ID, see section 5.9.5.1.

2. KAIC -: Audit events occurring during processing other than 1 above.

   The table below shows the message IDs and their contents.

Table 5.11 Audit Log Message IDs and Their Contents

Message ID	Description	Reference for the Corresponding Message Text
KAIC41000 to KAIC41399	Messages about receiving requests or transmitting responses, related to Device Manager server processing (when processing is normal)	5.9.5.2
KAIC41400 to KAIC41599 KAIC41700 to KAIC41799	Messages about receiving requests or transmitting responses, related to Device Manager server processing (when processing is not normal)	
KAIC43000 to KAIC43199	Messages about receiving requests or transmitting responses, related to startup (launching) of related products (when processing is normal)	5.9.5.3
KAIC43200 to KAIC43399	Messages about receiving requests or transmitting responses, related to startup (launching) of related products (when processing is not normal)	
KAIC44000 to KAIC44399	Messages about receiving requests or transmitting responses, related to Device Manager server processing via CIM (when processing is normal)	5.9.5.4
KAIC44400 to KAIC44799	Messages about receiving requests or transmitting responses, related to Device Manager server processing via CIM (when processing is not normal)	

5.9.5 Message Text Component of Audit Log Data

The format of message text in audit log data varies from one audit event to another. This subsection describes the message text format for each audit event. The item enclosed by square brackets ([ ]) in the message text format might not be output.

5.9.5.1 When Output as Processing Results of HiCommand Suite Common Component

Information on the audit event that has occurred is output in a character string. For more information on the message text, see *HiCommand Device Manager Error Codes*. The following shows an example of message text.

Example of message text output upon login:

```
"The login process has completed properly."
```

5.9.5.2 When Output as Processing Results of Device Manager Server

When a request for server processing, such as changing the configuration or obtaining information, is received or a response is transmitted, information on the request or response is output in the message text. The message text format is described below, followed by a detailed description of the information contained in the message text.

Request reception (normal):

unique-ID detail-message

Response transmission (normal):

unique-ID[*status*] *[request-operation-start-unique-ID]*

Request reception or response transmission (abnormal):

unique-ID error-message-ID

Table 5.12 Information Output When a Device Manager Server Request is Received or a Response is Transmitted

Item	Description
Unique ID	A unique request identifier. For response transmission, the unique ID of the request is output. For processing via the SVP, this ID is also output to the audit log data on the SVP.
Detail message	Detailed information on the request. For details, see section 5.9.6
Status	If the request and the operation are asynchronous, one of the following character strings that indicate the result of polling is output: ▪ `COMPLETED`: The operation was successful. ▪ `PROCESSING`: Now operating ▪ `FAILED`: The operation failed.
Request operation start unique ID	A unique ID that indicates which response (the result of polling the server about the requested operation) corresponds to which request, when a request and the operation are performed asynchronously. This ID corresponds to the message ID that is output as an attribute of the `RequestStatus` element of `GetRequestStatus` (command: `Get`, target: `RequestStatus`). This message ID is output to the detail message when a request is received. For details on detail messages, see section 5.9.6.
Error message ID	The ID of the error message. For more information on the message ID, see *HiCommand Device Manager Error Codes*.

The following examples show message text output when the server receives a request (when no error has occurred) or sends a response (when an error has occurred).

Example of message text output when the server receives a request (when no error has occurred):

```
"123456789 AddLUN<SA info='D700-75010421'><Path info=',,0,4,15,0,'><LDEV
info='D700-75010421-31,,'/><LDEV info='D700-75010421-34,,'/></Path><Path
info=',,1,1,15,0,31'/><Path info=',,16,6,15,0,31'/><Path
info=',,0,4,15,1,35'/></SA>"
```

Example of message text output when the server sends a response (when an error has occurred):

```
"123456789 KAIC01014-E"
```

5.9.5.3 When Output as Startup Information of Related Products

When a request to launch a related product is received or a response is transmitted, information on the request or response is output in the message text. The message text format is described below, followed by a detailed description of the information contained in the message text.

Request reception (normal):

unique-ID [*launch-session-ID*] [*launch-target-identifier*]

Response transmission (normal):

unique-ID [*launch-session-ID*]

Request reception or response transmission (abnormal):

unique-ID [*launch-session-ID*] *error-message-ID*

Table 5.13 Information Output When a Launch Request Is Received or a Response Is Transmitted

Item	Description
Unique ID	A unique request identifier. For response transmission, the unique ID of the request is output. For processing via the SVP, this identifier is also output to the audit log data on the SVP.
Launch session ID	Format: `lsessionID=...` The launch session ID is output. This information is output when a specific application is launched under the condition that request-response exchange between the Web Client and the Device Manager server is performed more than once. For information on the applications for which the launch session ID is output, see Table 5.14. This item is not output when the subsystem to be launched is Universal Storage Platform V.
Launch target identifier	Format: `loid=...` Information that identifies the launch target is output. This information is output only when the first request is received. The information contained in the launch identifier varies depending on the application to be launched. For details, see Table 5.14.
Error message ID	The ID of the error message. For more information on the message ID, see *HiCommand Device Manager Error Codes*.

The table below indicates the relationship between the presence of a launch session ID and the information contained in the launch target identifier for each type of the application to be launched.

Table 5.14 Relationship between the Presence of a Launch Session ID and the Information Contained in the Launch Identifier

Application Type	Presence of Session ID	Information in Launch Identifier
Storage Navigator	Present	Information that identifies the subsystem to be launched. The value is the same as an element identifier#1 in the `StorageArray` element. For more information, see the attribute value output sequence for the `StorageArray` element in Table 5.21.#2
DAMP	Present	
Storage Navigator Modular	Present	
Physical View	Not present	
Resource group assignment	Not present	An ID that indicates the dialog box is used to manage resource groups of the user or used to assign a resource group to the user.launched. Format: ▪ Resource group assignment: `loid=`*UV* ▪ Resource group management: `loid=`*UGV*
Resource group management	Not present	
Dynamic Link Manager	Not present	Information that identifies the host machine to be launched. The value is the same as an element identifier#2 in the `Host` element. For more information, see the attribute value output sequence for the `Host` element in Table 5.21.
Protection Manager	Not present	

#1 An element identifier indicates an attribute.

#2 The IP address is displayed only when Lightning 9900V is launched from Physical View (output example: `loid=10.208.110.110`).

The following examples show message text output when the server receives a launch request (when no error has occurred) or sends a response to a launch request (when no error has occurred).

Example of message text output when the server receives a launch request (when no error has occurred):

```
"123456789 lsessionID=a7e770671b8 loid=R500-14000"
```

Example of message text output when the server sends a response to a launch request (when no error has occurred):

```
"123456789 lsessionID=a7e770671b8"
```

5.9.5.4 When Output as Processing Results of Device Manager Server via CIM

When a CIM service method request is received or a response is transmitted, information on the request or response is output in the message text. The message text format is described below, followed by a detailed description of the information contained in the message text.

Request reception (normal):

unique-ID method-name input-parameter object-path

Response transmission (normal and abnormal):

unique-ID return-code output-parameter

Response transmission (when a job is created through asynchronous processing):

unique-ID `return=4096` *object-path*

Caution: When a job is created through asynchronous processing, no completion notification is output to the audit log data.

Table 5.15 Information Output When a Device Manager Server Request Is Received (via CIM) or a Response Is Transmitted

Item	Description
Unique ID	A unique request identifier. For response transmission, the unique ID of the request is output. For processing via the SVP, this identifier is also output to the audit log data on the SVP.
Method name	The name of the requested method.
Input parameters	Format: `inParams={...}` The input parameters passed to the requested method are output.
Object path	Format: `objectPath=...` The object path passed to the requested method is output.
Return code	Format: `return=...` The return code that indicates the execution result of the requested method is output.
Output parameters	Format: `outParams={...}` The output parameters passed as the execution result of the requested method are output.

The following examples show message text output when the server receives a request for Device Manager server processing (via CIM, when no error has occurred) or sends a response (via CIM, when no error has occurred).

Example of message text output when the server receives a server receives a request for Device Manager server processing (via CIM, when no error has occurred):

```
"123456789 GetSupportedSizeRange
inParams={ElementType=3,Goal=//11.222.33.444/root/hitachi/dm56:HITACHI_StorageSettin
g.InstanceID='RAID5'}
objectPath=/root/hitachi/dm56:HITACHI_StoragePool.InstanceID='AMS500.75010421'"
```

Example of message text output when the server sends a response to a request for Device Manager server processing (via CIM, when no error has occurred):

```
"123456789 return=0
outParams={MinimumVolumeSize=1024,MaximumVolumeSize=248139692,VolumeSizeDivisor=1024
}"
```

5.9.6 Detail message output for a request to a Device Manager server

This subsection describes the format of and information in the detail message that is output when the Device Manager server receives a request. The item enclosed by square brackets ([ ]) in the output format might not be output.

Detail message output format:

command target [*option*] [*parameter*]

Table 5.16 Information Output in Detail Messages

Item	Description
Command	A character string (3 characters) that indicates the operation (e.g., addition, deletion, modification, or reference) to be performed on the resource. For the meaning of the output character string, see Table 5.18.
Target	Information that identifies the operation to be performed. For information on the target to be output in the message text, see Table 5.19. However, Table 5.19 might not contain some displayed characters.
Option	Format: [...] Information that identifies the operation to be performed. This information is output only when one or more options are specified. For more information on the meanings of output options, see Table 5.20.
Parameters	Information that identifies the operation to be performed and the resource on which the operation is to be performed. (This information is output only when it is specified by request.) This information is output in tagged format.

The format and content of the parameters output in detail messages are described below.

Parameter format 1 (nested):

<*element attribute*>[*parameter-1 parameter-2...parameter-n*]</*element*>

The parameters that depend on the element are output between the start and end tags of the *element*. If no relevant parameters exist, no parameters are output.

Parameter format 2 (non-nested):

<*element attribute*/>

Table 5.17 Information Output in Detail Message Parameters

Item	Description
Element	A character string that indicates the element name. For information on the elements that are output and their meanings, see Table 5.21. However, Table 5.21 might not contain some displayed characters.
Attributes	Format: `info='...'` Attribute values specified for the element are output. When two or more attribute values are output, they are separated by a comma (`,`). Each attribute value is output as a character string or a numeric value. When no corresponding attribute was specified or nothing was specified for the attribute value, no attribute value is output. When all attributes were not specified or nothing was specified for attribute values, this item is not output. If an attribute value contains a single-quotation mark (`'`) or comma (`,`), the quotation mark or comma is replaced with a question mark (`?`). For information on the attribute value output sequence, see Table 5.21.

The table below lists the commands that can be output in detail messages.

Table 5.18 Commands Output in Detail Messages

Output Character String	Full Name	Operation
`Add`	Add	Addition
`Del`	Delete	Deletion
`Get`	Get	Acquisition
`Mod`	Modify	Modification
`Set`	Set	Setting

The table below provides information on the targets to be output in detail messages.

Table 5.19 Targets Output in Detail Messages

Output Character String	Full Name	Operation
`Alerts`	Alerts	Alert information reference or deletion
`ArrGrp`	ArrayGroup	Array group configuration change
`ArrRsrv`	ArrayReservation	Subsystem reservation setting or information acquisition
`CFForRep`	ConfigFileForReplication	CCI configuration file creation
`ConfChange`	ConfigurationChange	Configuration change notification to the Device Manager server
`DataRetentions`	DataRetentions	Data retention information setting or acquisition
`DebugLevel`	DebugLevel	Debug level change or reference
`Host`	Host	Host setting or reference
`HostI`	HostInfo	Host (agent) configuration change or reference

Output Character String	Full Name	Operation
HostRef	HostRefresh	HostInfo update
HSD	HostStorageDomain	Host storage domain configuration change
HostVol	HostVolume	Host volume information notification to the Device Manager server
LDEVForVolMig	LDEVForVolumeMigration	LDEV VolumeMigration attribute setting or information acquisition
ListView	ListView	Listing of information held by the Device Manager server
LogF	LogFile	Log file information acquisition
LGrp	LogicalGroup	Logical group setting or reference
LU	LogicalUnit	Logical unit configuration change
LUFormat	LogicalUnitFormat	Formats of all LDEVs in the logical unit
LUN	LUN	Path configuration change
LUNGrp	LUNGroup	LUN group configuration change
LunScan	LunScan	Assignment of LUNs that do not belong to a logical group
LUSE	LUSE	Expanded LDEV configuration change
Msgs	Messages	Message
ObjForLGrp	ObjectForLogicalGroup	Change to configuration of objects belonging to a logical group
ObjName	ObjectName	Name assignment to objects used in Device Manager
Port	Port	Port configuration change
PortCtrl	PortController	Port controller configuration change
Rep	Replication	Pair configuration change
RepCtrlPair	ReplicationControllerPair	Pair configuration information reference
ReqStatus	RequestStatus	Return of command status
Rule	Rule	ACL rule setting or reference
SrvI	ServerInfo	Device Manager server information acquisition
SpareDrive	SpareDrive	Spare drive configuration change
SA	StorageArray	Subsystem discovery, deletion, and information acquisition
Subscrbr	Subscriber	Event listener addition or deletion
URLLink	URLLink	URL Link information configuration change
User	User	User setting or reference
UGrp	UserGroup	User group (resource group) setting or reference
VolMig	VolumeMigration	Migration plan setting or information acquisition
VolShred	VolumeShredding	Shredding function execution requests or information acquisition
WWN	WorldWideName	WWN deletion

Output Character String	Full Name	Operation
WWNForHSD	WWNForHostStorageDomain	Change to configuration of WWNs belonging to host storage domain
WWNForLUN	WWNForLUN	LUN WWN configuration change
WWNForLUNGrp	WWNForLUNGroup	LUNGroup WWN configuration change
WWNGrp	WWNGroup	WWN group configuration change

The table below provides the contents of options to be output in detail messages.

Table 5.20 List of Options of Detail Messages

Output Character String	Operation
force	Creates an LUSE in the logical unit that already has paths.
suspend	Creates a 3DC pair by using Universal Replicator.
lusekeep	Keeps the LUSE.
noformat	Creates a logical unit without formatting.
split	Splits the pair.
resync	Copies the data of the primary volume to the secondary volume.
restore	Copies the data of the secondary volume to the primary volume.
remainMigraion	Leaves the plan status of the completed plan in the subsystem (SVP).

The table below provides the attribute value output sequence for each element.

Table 5.21 Attribute Output Sequence for Each Element of a Detail Message

Output Character String	Full Name and Content	Attribute Value Output Sequence[#1]
`Alert`	Alert (Information about the error that occurred in Device Manager or the storage subsystem)	alert number
		number
`Alerts`	Alerts (A group of Alert elements)	--
`ArrGrp`	ArrayGroup (Information about the array group of the storage subsystem)	<model name[#2] - serial number - chassis number - array group number>, number of chassis containing the array group, array group RAID level
		<model[#2] - serialnum - chassis - number>, chassis, raidType
`ArrRsrv`	ArrayReservation (Lock information of the storage subsystem)	<model name[#2] - serial number>, <model name[#2] - serial number>
		<model[#2] - serialnum>, <model[#2] - serialnum>
`ChangedItem`	ChangedItem (Information about the data changed in Device Manager)	--
`ChangeI`	ChangeInfo (Version information of the storage subsystem configuration)	LDEV information version, port information version, LU information version, LUSE information version, LUN information version, host mode information version, DCR information version, CVS information version, SSID information version, CHA information version
		versionOfLDEV, versionOfPort, versionOfLogicalUnit, versionOfLUSE, versionOfLUNSecurity, versionOfHostMode, versionOfDCR, versionOfCVS, versionOfSSID, versionOfCHA
`CommandComplete`	CommandComplete (Information required by clients when the `Get Request Status` command is issued)	--
`CommParas`	CommParameters (Information about how to access the storage subsystem)	--
`Comp`	Component (Information about the storage subsystem configuration)	--
`Cond`	Condition (Limits the results of the `Get` command by using the Filter elements at the same time)	LU type, element identifier of LDEV, LDEV type, host storage status, Alert source, host type, CLPR number of journal volume, element identifier of host
		type, childID, volumeKind, host, source, hostType, clprNumber, assocID

Output Character String	Full Name and Content	Attribute Value Output Sequence[#1]
ConfChange	ConfigurationChange (Reports information about the configuration changes of the storage subsystem to the Device Manager server)	user ID, notification type, serial number, product name[#2], occurrence date and time, IP address
		user, type, serialNumber, arrayType[#2], date, ipAddress
ConfigChange	ConfigChange (Information about the data changed in the Device Manager server)	--
ConfigF	ConfigFile (Information about the CCI configuration file)	<host ID - HORCM instance number>
		<hostID - instanceNumber>
DataRetention	DataRetention (Data retention information)	--
DataRetentions	DataRetentions (LDEV data retention information)	--
DebugLevel	DebugLevel (Information about the current debug level of the Device Manager server)	debug level
		value
ErrI	ErrorInfo (Information about the error that occurred in the storage subsystem)	error code of the error detected in the storage subsystem, date and time of the error detected
		errorCode, date
ErrList	ErrorList (A list including the ErrorInfo elements)	number of ErrorInfo elements
		errorCount
ExtPathI	ExternalPathInfo (Access information of the external storage subsystem)	<model name[#2] - serial number - chassis number - array group number - WWN of port for external subsystem - LUN number of external LU - port ID of external port>[#3]
		<model[#2] - serialnum - chassis - number - externalWWN - externalLun - portID>[#3]
F	File (Information about the log file name)	Log file name
		name
Filt	Filter (Limits the results of the Get command)	--
FreeLUN	FreeLUN (Information about availability of the LUN in the host storage domain)	--

Output Character String	Full Name and Content	Attribute Value Output Sequence[#1]
FreeSpace	FreeSpace (Information about the free space in the array group of the storage subsystem)	<model name[#2] - serial number - chassis number - array group number - free space index number within array group>[#3]
		<model[#2] - serialnum - chassis - number - fsControlIndex>[#3]
Host	Host (Host information used by the logical volume)	<host ID>, host name, host IP address, host type, operation target host name
		<hostID>, name, ipAddress, hostType, targetName
HostI	HostInfo (Information about accesses between the LU and host)	<host name - host SCSI bus number - target ID - LU number of volume on host>, type (model[#2]) of storage subsystem connected with host, serial number of storage subsystem connected with host, displayed name of HostInfo object, host IP address, LUN mount point, port ID, domain ID of host storage domain, device number of logical unit[#4], port WWN on HBA, type of file system to be mounted, file system name, LUN capacity, LUN usage
		<name - osScsiBus - osScsiID - osLun>,arrayType[#2], serialNumber, name, ipAddress, mountPoint, portID, domainID, devNum[#4], portWWN, fileSystemType, fileSystemName, sizeInMB, percentUsed
HostVol	HostVolume (Information about the volume recognized by the host to which the storage device is connected)	vendor name, model name[#2], serial number, port number, device number[#4], identification number, host name, IP address, mount point, SCSI bus number, SCSI bus connection identification number, LU number, WWN of HBA, WWN of port for storage device, file system type, file system name, volume size, volume usage, LU pair type, LU pair type (Universal Replicator)
		vendorID, model[#2], serialNumber, port, devNum[#4], hsDeviceID, name, ipAddress, mountPoint, OSscsiBus, OSscsiID, OSlun, portWWN, subsystemPortWWN, fileSystemType, fileSystemName, sizeInMB, percentUsed, pairType, pairTypeTCMirror
HSD	HostStorageDomain (Information about the host storage domain)	<model name[#2] - serial number - port ID - domain ID>, port ID, domain ID, new host connection mode for host storage domain, list of new host connection modes, host connection mode options, host storage domain name, nickname of host storage domain, operation target host storage domain name, operation target host storage domain port ID
		<model[#2] - serialnum - portID - domainID>, portID, domainID, hostMode, hostMode2, hostModeOption, name, nickname, targetNickname, targetPortID
IPAddress	IPAddress (The IP address of the port controller)	--
JrnlPool	JournalPool (Journal group information of Universal Replicator and QuickShadow)	<model name[#2] - serial number - journal pool identifier - pool ID>
		<model#2 - serialnum - poolFunction - poolID>
LDEV	LDEV (Information about the LDEV)	<model name[#2] - serial number - LDEV device number[#4]>, CLPR number, stripe size
		<model[#2] - serialnum - devnum[#4]>, clprNumber, stripeSizeInKB

Output Character String	Full Name and Content	Attribute Value Output Sequence[#1]
LDKC	LogicalDKC (Logical DKC of the storage subsystem)	--
LGrp	LogicalGroup (Groups hosts, host storage domains, or other logical groups)	<logical group ID>, name, description, icon file name, <element identifier of logical group of parent group>,operation target logical group name, parent logical group name
		<groupID>, name, description, icon, <parentID>, targetLogicalPath, parentLogicalPath
LicenseKey	LicenseKey (Key code required to make PP available)	<model name[#2] - serial number - LicenseKeyID>
		<model[#2] - serialnum - PPID>
ListView	ListView (Displays a list of information that the Device Manager server keeps)	grouping unit, name of column to be obtained, name of column to be obtained as unique attribute
		groupBy, requiredAttribute, requiredUniqueAttribute
LU	LogicalUnit (Information that represents the LU)	<model name[#2] - serial number - logical device number[#4]>, number of LDEV contained in a logical unit[#4], volume size, emulation mode, default number of port controllers, whether the LU is used as a command device, whether command device security is set
		<model[#2] - serialnum - devnum[#4]>, devNum[#4], capacityInKB, emulation, defaultPortController, commandDevice, commandDeviceSecurity
LUNGrp	LUNGroup (Groups LUNs or ports)	<model name[#2] - serial - port ID - nickname>, nickname, name
		<model[#2] - serialnum - portID - nickname>, nickname, name
MFVolI	MFVolumeInfo (Access information between the main frame host and LDEV)	--
Msg	Message (Asynchronous message)	--
Msgs	Messages (Groups the Message elements)	Wait time (seconds)
		timeToWait
ObjName	ObjectName (Sets the object name of the Device Manager server)	<target element name - target element identifier>, name ***Caution:*** <target element name> and <target element identifier> indicate the element name and element identifier other than those specified for the ObjectName attribute. For information on the component corresponding to the element identifier, see the attribute value output sequence for <target element name>.
		<target element name - target element identifier>, name
PairedJrnlPool	PairedJournalPool (The journal pool paired with the journal pool of Universal Replicator)	--

Output Character String	Full Name and Content	Attribute Value Output Sequence[#1]
PairedPortController	PairedPortController (CHIP paired on the NAS configuration)	--
PairedVol	PairedVolume (Information about the volume that is paired with HostVolume)	Replication operation type[#5], volume type, serial number of volume device, model of volume device[#2], logical device number of volume[#4], pair status, fence level, MU number of P-VOL corresponding to paired S-VOL
		replicationFunction[#5], otherPairType, otherPairSerialNumber, otherPairArrayType[#2], otherPairDevNum[#4], status, fenceLevel, muNumber
Para	Parameter (A pair of the name and value)	parameter name, parameter value[#2]
		name, value[#2]
Path	Path (Information about the path)	<model name[#2] - serial name - port ID - domain ID - logical device number[#4]>, name, port ID, domain ID of host storage domain, SCSI ID, LUN assigned to path, device number for logical unit identification[#4]
		<model[#2] - serialnum - portID - domainID - devnum[#4]>, name, portID, domainID, scsiID, lun, devNum[#4]
PDEV	PDEV (Information about PDEV)	<model name[#2] - serial number - PDEV ID>
		<model[#2] - serialnum - PDEVID>
Port	Port (Information about the port)	<model name[#2] - serial number - port ID>, Fibre port address, Fibre topology, whether LUN security is enabled or disabled for the port, port options, channel speed
		<model[#2] - serialnum - portID>, fibreAddress, topology, lunSecurityEnabled, portOption, channelSpeed
PortCtrl	PortController (Information about the port controller of the storage subsystem)	<model-name[#2] - serial number - port controller ID>, mode
		<model[#2] - serialnum - controllerID>, mode
RepCtrlPair	ReplicationControllerPair (Information about MCU and RCU)	<serial number of MCU device - CU number of MCU - serial number of RCU device - SSID of RCU>
		<masterSerialNumber - masterControllerID - remoteSerialNumber - remoteSSID>
RepGrp	ReplicationGroup (Information about the HORCM instance group)	<replication group ID>, name of copy group used by CCI, host ID of host that recognizes P-VOL, instance number of HORCM instance that manages P-VOL, port number of HORCM instance that manages P-VOL, host ID of host that identifies S-VOL, instance number of HORCM instance that manages S-VOL, port number of HORCM instance that manages S-VOL, copy type[#5], P-VOL fence level, copy pace
		<replicationGroupID>, groupName, pvolHostID, pvolInstanceNumber, pvolPortNumber, svolHostID, svolInstanceNumber, svolPortNumber, replicationFunction[#5], fenceLevel, copyTrackSize

Output Character String	Full Name and Content	Attribute Value Output Sequence[#1]
RepI	ReplicationInfo (Information about replication)	<PVOL serial number - PVOLLDEV number[#4] - SVOL serial number - SVOLLDEV number[#4]>, name of copy pair used by CCI, type of P-VOL storage subsystem[#2], serial number of storage subsystem containing P-VOL, P-VOL device number[#4], port number in the HORCM configuration file that manages P-VOL paths, ID of pool that contains P-VOL, type of S-VOL storage subsystem[#2], serial number of storage subsystem containing S-VOL, S-VOL device number[#4], port number in the HORCM configuration file that manages S-VOL paths, ID of pool that contains S-VOL, copy type [#5], MU number of P-VOL, P-VOL fence level, copy pace
		<pvolSerialNumber - pvolDevNum[#4] - svolSerialNumber - svolDevNum[#4]>, pairName, pvolArrayType[#2], pvolSerialNumber, pvolDevNum[#4], pvolPortID, pvolPoolID, svolArrayType[#2], svolSerialNumber, svolDevNum[#4], svolPortID, svolPoolID, replicationFunction[#5], muNumber, fenceLevel, copyTrackSize
ReqStatus	RequestStatus (Returns the status of the preceding request)	message ID
		messageID
RSIMI	RSIMInfo (RSIM information of the storage subsystem)	RSIM ID of RSIM information
		RSIMID
RsltObj	ResultObject (A single row in a list displayed by the ListView elements)	--
Rule	Rule (ACL rule of the Device Manager server)	rule ID, rule group name, user logon ID, operation, <LogicalGroup, element identifier of the Host or LDEV element>, type, description
		ruleID, groupName, logonID, operation, <target>, ruleType, description
SA	StorageArray (Storage subsystem information)	<model name[#2] - serial number>
		<model[#2] - serialnum>
SIMI	SIMInfo (SIM information of the storage subsystem)	SIM ID of SIM information
		SIMID
SizeCond	SizeCondition (Conditions for specifying the number within SearchCondition)	number of records to be skipped from the beginning, number of records to be obtained
		offset, size
SlctCond	SelectCondition (Element for which the SelectItem elements were collected)	conditional operator used to concatenate conditions represented by subordinate SelectItem elements
		operator
SlctItem	SelectItem (Filtering conditions within SearchCondition)	filtering condition key value, operator indicating relationship between key attribute and value attribute, filtering condition value[#2]
		key, operator, value[#2]

Output Character String	Full Name and Content	Attribute Value Output Sequence[#1]
SortCond	SortCondition (Element for which SortItems were collected)	--
SortItem	SortItem (Sorting conditions within SearchCondition)	column name used as sort key, sort order, sort priority
		key, order, priority
SrchCond	SearchCondition (Search conditions for obtaining ListView)	--
SrvI	ServerInfo (Obtains information of the Device Manager server)	--
Subscrbr	Subscriber (Report plan topic)	--
Timestamp	Timestamp (Time when the message was created in the Device Manager server)	--
Topic	Topic (Name of the message topic)	report information
		name
UGrp	UserGroup (Groups users according to their permissions)	name, description
		name, description
URLLink	URLLink (Links between a HiCommand object and an application)	<related element identifier - ID>, URL required to launch application or Web page, application name, <linked related element identifier - link ID>, description
		<linkedID - nameID>, url, name, <linkedID – nameID>, description
User	User (Account information of a single user of Device Manager)	user ID, name of group to which the user belongs, permission, user name, description
		loginID, groupName, role, fullName, description
VolCon	VolumeConnection (Information about the assigned LDEV and the corresponding external LU)	<model name of assigned LU[#2] - device serial number of assigned LU - device number of assigned LU[#4]>[#3]
		<mappedArrayType[#2] - mappedSerialNumber - mappedDevNum[#4]>[#3]
VolMig	VolumeMigration (Information about the Volume Migration manual plan)	<model name[#2] - serial number - source LDEV number[#4] - target LDEV number[#4]>, owner ID of the user who performs migration, source device number[#4], target device number[#4]
		<model[#2] - serialnum - sourceDevNum[#4] - targetDevNum[#4]>, ownerID, sourceDevNum[#4], targetDevNum[#4]

Output Character String	Full Name and Content	Attribute Value Output Sequence#1
VolShred	VolumeShredding (Information about the shredding function)	shredding owner ID
		ownerID
WritingPattern	WritingPattern (Writing pattern information for a single writing)	writing pattern used when shredding is specified
		pattern
WritingPatterns	WritingPatterns (All writing pattern information of a single VolumeShredding)	--
WWN	WorldWideName (Host HBA information)	WorldWideName, nickname, targetNickname, operation target host storage domain name
		wwn, nickname, targetNickname
WWNGrp	WWNGroup (Groups WWNs)	<model name#2 - serial number - port ID - nickname of WWN group>, nickname, name
		<model#2 - serialnum - portID - nickname>, nickname, name

Legend:

--: No attribute value is output

<...>: An element identifier that represents an attribute If the contents include multiple elements, they are concatenated by a hyphen (-).

#1 The lower field of each element indicates the output order represented with the names used within Device Manager.

#2 This information is output as the storage subsystem model, and represented by the common output name indicated in the table below. Device Manager versions 5.7 and later do not support T3. However, if a T3 storage subsystem is already registered as a management target of Device Manager in earlier versions and you perform an operation for that T3, this information might be output.

Table 5.22 Common Output Names for Storage Subsystem Models

Common Output Name	Applicable Storage Subsystem Model
D500	Thunder 9200
D600	Thunder 9500V
D700	TagmaStore AMS/WMS series
R400	Lightning 9900
R450	Lightning 9900V
R500	TagmaStore USP
R600	Universal Storage Platform V

Common Output Name	Applicable Storage Subsystem Model
T3	T3

#3 This information is output as the ObjectName element <target element identifier>. The attribute value is not output as a rule.

#4 For Universal Storage Platform V, a numerical value that combines the LDKC number, CU number, and LDEV number (= *LDKC* x 65536 + *CU* x 256 + *LDEV*) is output.For Lightning 9900, Lightning 9900V, or TagmaStore USP, a numerical value that combines the CU and LDEV numbers (= *CU* x 256 + *LDEV*) is output. For Thunder 9200, Thunder 9500V, or TagmaStore AMS/WMS series, the LU number is output.

#5 The replication operation type attribute is represented by the common output name indicated in the table below when it is output.

Table 5.23 Common Output Names for Replication Operation Type Attributes

Common Output Name	Applicable Product
Local Copy	ShadowImage
Remote Copy (Async)	TrueCopy Asynchronous
Remote Copy (Jrnl)	Universal Replicator
Remote Copy (Sync)	TrueCopy
SnapShot	QuickShadow

Chapter 6 Setup for Managing Copy Pairs

This chapter discusses the following setup requirements:

- Server Requirements for Managing Copy Pairs (see section 6.1)
- Host Requirements (see section 6.2)
- Subsystem Requirements (see section 6.3)
- CCI and Protection Manager Requirements (see 6.4)

6.1 Server Requirements for Managing Copy Pairs

- You can use Device Manager to control copy pairs in one of two ways:
  - Local management, with each host managing the copy pair(s) for the LUs recognized by that host.
  - Central management, with a single host managing all of the copy pair(s) for the LUs recognized by multiple hosts. The `server.agent.rm.centralizePairConfiguration` property file for Device Manager Agent must be set to `enable`.
- The subsystems that are candidates for P-VOL or S-VOL must be managed by a single Device Manager Server.
- When local management is used, the Device Manager server must recognize the hosts that manage copy pairs.

6.2 Host Requirements

This section describes the host requirements for operating copy pairs when local management is used and when central management is used. If you have not yet created a copy pair, in the following explanation you must read *P-VOL* as *P-VOL candidate* and *S-VOL* as *S-VOL candidate*:

Figure 6.1 shows a configuration example of operating copy pairs when local management is used.

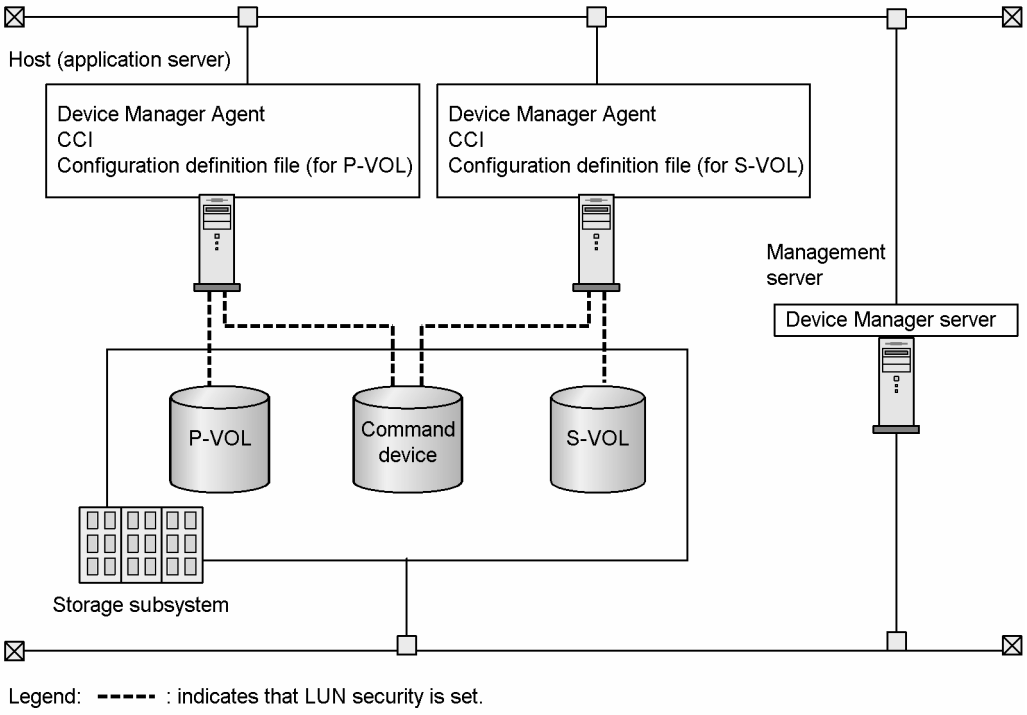

Figure 6.1 Example of Pair Operations When Local Management Is Used

When local management is used:

- From the P-VOL or S-VOL, LUN security must be set for the host.

  LUN security from the P-VOL and S-VOL must be set for at least one host, although the host to which LUN security from the P-VOL is assigned and the host to which LUN security from the S-VOL is assigned do not need to be the same.

- The host must recognize the P-VOL or S-VOL.

  The P-VOL and S-VOL must be recognized by at least one host, although the host that recognizes the P-VOL and the host that recognizes the S-VOL do not need to be the same.

- From a command device, LUN security must be set for the hosts that recognize the P-VOL or S-VOL.

For a host that recognizes the P-VOL, LUN security must be set from the command device on the P-VOL side. For a host that recognizes the S-VOL, LUN security must be set from the command device on the S-VOL side.

- The host that recognizes the P-VOL or S-VOL recognizes a command device.
- Device Manager agent must be installed on the hosts that recognize the P-VOL or S-VOL, and a command device.

  If there are multiple hosts that recognize the P-VOL, a Device Manager agent only needs to be installed on one of the hosts. Similarly, if there are multiple hosts that recognize the S-VOL, a Device Manager agent only needs to be installed on one of the hosts.

  To manage the copy pairs for the TagmaStore AMS/WMS series, Device Manager agent version 4.1 or later is required.

  For details on the correspondence between copy pair operations and required Device Manager agent versions, see Table 6.1.
- CCI must be installed on the hosts that recognize the P-VOL or S-VOL, and a command device.

  If there are multiple hosts that recognize the P-VOL, CCI only needs to be installed on one of the hosts. Similarly, if there are multiple hosts that recognize the S-VOL, CCI only needs to be installed on one of the hosts.

  For details on how to install CCI, see the relevant manual for CCI.
- If there are multiple NICs on the host, the Device Manager agent and CCI must use the same IP address.
- CCI must have fewer than 32 running instances.

Figure 6.2 shows a configuration example of operating copy pairs when central management is used.

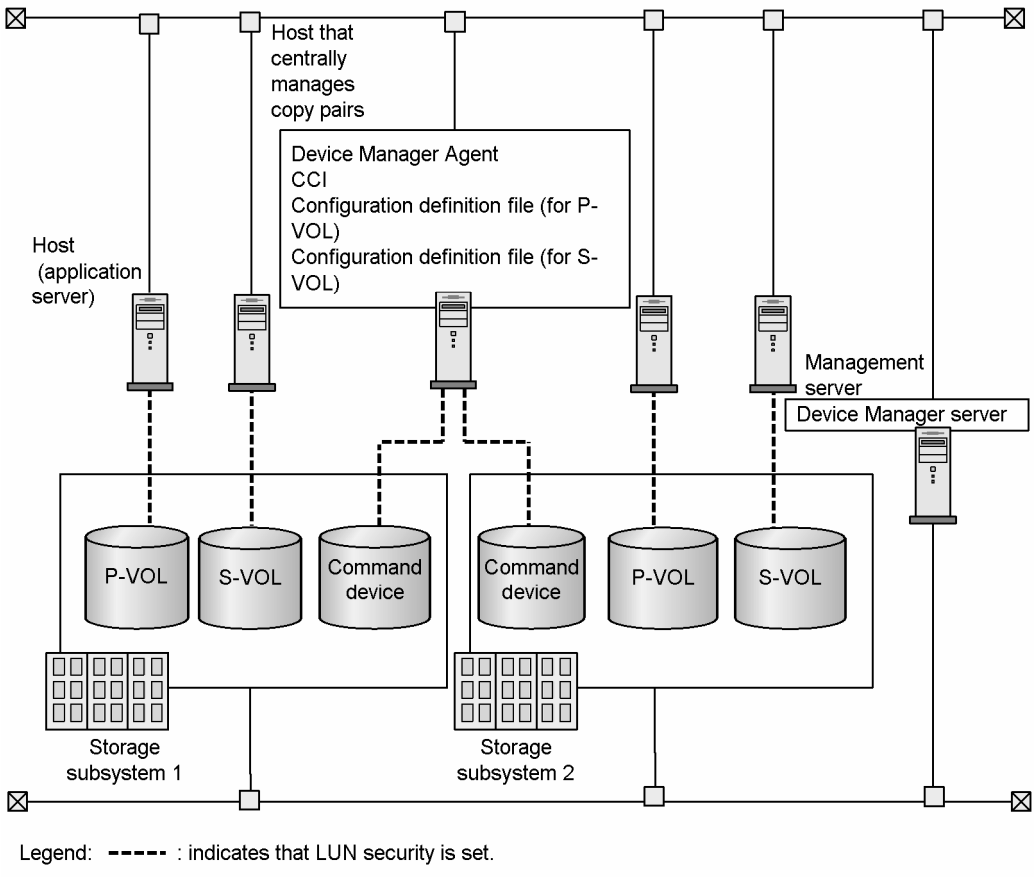

Figure 6.2 Example of Pair Operations When Central Management Is Used

When central management is used:

- From the P-VOL or S-VOL, LUN security must be set for the host.

  The host does not need to recognize the P-VOL or S-VOL.

- From a command device, LUN security must be set for the host that centrally manages copy pairs.

  To manage the copy pairs for TrueCopy or Universal Replicator, LUN security must be set for the host, from the command devices of the storage devices on both the P-VOL and S-VOL.

- The host that centrally manages copy pairs must recognize a command device.

  The command device security must not be used for a command device.

- Device Manager agent version 3.0 or later must be installed on the host that centrally manages copy pairs.

  To manage the copy pairs for the TagmaStore AMS/WMS series, Device Manager agent version 4.1 or later is required.

  For details on the correspondence between copy pair operations and required Device Manager agent versions, see Table 6.1.

- CCI must be installed on the host that centrally manages copy pairs.

  For details on how to install CCI, see the relevant manual for CCI.

- If there are multiple NICs on the host that centrally manages copy pairs, the Device Manager agent and CCI must use the same IP address.
- CCI must have fewer than 32 running instances.

Important: When central management is used, copy pairs of a host that uses a platform on which the Device Manager agent cannot be installed can be recognized.

Table 6.1 shows the copy pair operations and the versions of the Device Manager agent required for performing the operations.

Table 6.1 Copy Pair Operations and Required Versions of Device Manager Agent

Function	Pair Operation	Required Version
ShadowImage and TrueCopy	Displays the status.	2.3 or later
ShadowImage	Display the status (maximum 1:3).	5.5 or later#1
ShadowImage and TrueCopy	Changes the status.	2.4 or later
ShadowImage	Change the status (maximum 1:3).	5.5 or later#1
TrueCopy Extended Distance	Change the status.	5.1 or later
QuickShadow	Changes the status.	3.0 or later
	Change the status (maximum 1:15).	5.5 or later
Universal Replicator	Displays the status.	4.0 or later
	Display the 3DC status.	5.5 or later
	Change the status.	5.6 or later
Copy-on-Write Snapshot	Display the status.	4.1 or later#2
	Change the status.#3	4.1 or later

#1 The version required when TagmaStore AMS/WMS series is used.

#2 The version must be 4.2 or later when Universal Storage Platform V or TagmaStore USP is used.

#3 The status can only be changed on the TagmaStore AMS/WMS series. On Universal Storage Platform V and TagmaStore USP, the status can only be displayed.

Caution: You can use the Remote Console for Lightning 9900, Storage Navigator (for Universal Storage Platform V, TagmaStore USP, and Lightning 9900V), SVP, or CCI library to create or manage a copy pair without using CCI. However, you cannot change the status of or delete such copy pairs from Device Manager, because there is no configuration definition file for operating such a copy pair using CCI. If you have an existing copy pair that was not created using CCI, first release the copy pair (using the same tool that created it), and then use Device Manager(R) to recreate the volume pairs. You can also manually create a configuration definition file to control the existing copy pairs.

6.3 Subsystem Requirements for Managing Copy Pairs

- Command Control Interface (CCI) must be installed and enabled, in the following versions:
  - To use TrueCopy or ShadowImage: 01-10-03, 01-11-03, or 01-12-03/04
  - To use QuickShadow: 01-12-03/04
- Command Device Security must be installed. This requires Resource Manager.
- CCI must have fewer than 32 running instances.
- After the subsystem has been configured as required, the subsystem must be refreshed.
- The subsystem serial numbers managed by Device Manager must all be unique. In the case of TrueCopy, remote subsystems that are not managed by Device Manager must also have unique serial numbers.
- For Thunder 9200, the default serial number of the storage subsystem must not have been changed.

Table 6.2 Subsystem Requirements

Subsystem	Function	Requirements
Universal Storage Platform V TagmaStore USP Lightning 9900V Lightning 9900	Universal Replicator (available for Universal Storage Platform V and TagmaStore USP)	Universal Replicator must be enabled. There must be a fibre-channel connection between the two ports used for an MCU-RCU path.#1 The MCU port for an MCU-RCU path must be an Initiator port, and the RCU port must be an RCU Target port.#1 The RCU and the MCU-RCU path must be registered in the MCU.#1 ***Note:*** To change the port configuration, use the Storage Navigator for Universal Storage Platform V and TagmaStore USP. In the Device Manager server, refresh storage subsystem information after you configure the ports. The subsystem cache or non-volatile storage must be sufficient. For details about Universal Replicator, including how to change the port configuration and a description of the required cache, see the *Hitachi TagmaStore Universal Replicator User's Guide*. ***Note:*** You can use the Storage Navigator for Universal Storage Platform V and TagmaStore USP to check the cache size. Contact your Hitachi Data Systems representative if you need to add to the cache. You must register the journal volumes with the journal group by using the Storage Navigator.

Subsystem	Function	Requirements
	TrueCopy	TrueCopy or TrueCopy Asynchronous must be enabled. There must be a fibre-channel connection between the two ports used for an MCU-RCU path. The MCU port for a MCU-RCU path must be an Initiator port, and the RCU port must be an RCU Target port. The RCU and the MCU-RCU path must be registered in the MCU. ***Note:*** To change the port configuration, use the Storage Navigator for Universal Storage Platform V, TagmaStore USP, and Lightning 9900V, or the Remote Console for Lightning 9900. Refresh the Device Manager server after you configure the ports. The subsystem cache or non-volatile storage must be sufficient. See *Hitachi TagmaStore USP and NSC Universal Storage Platform TrueCopy User and Reference Guide*, *Hitachi Lightning 9900 V Series TrueCopy User and Reference Guide* or *Hitachi Lightning 9900 TrueCopy User and Reference Guide* for more information about TrueCopy, including instructions for changing the port configuration and a description of the required cache. ***Note:*** You can use the Storage Navigator for Universal Storage Platform V, TagmaStore USP, and Lightning 9900V, or the Remote Console for Lightning 9900 to check the cache size. Contact your Hitachi Data Systems representative if you need to add cache.
	ShadowImage	ShadowImage must be enabled. For TagmaStore AMS/WMS series, a DM-LU must be set up. For more information about ShadowImage please see the following *Hitachi TagmaStore USP and NSC ShadowImage User's Guide*, *Hitachi Lightning 9900V Series ShadowImage User's Guide* or *Hitachi Lightning 9900 ShadowImage User's Guide*.
TagmaStore AMS/WMS Series, Thunder 9500V	TrueCopy	TrueCopy Basic or TrueCopy Extended Distance must be enabled. There must be a fibre-channel connection between the two ports used for a path. The TrueCopy path must be configured. The data share mode must be **ON**. The system start attribute must be dual active mode. The SCSI ID/Port ID inheritance mode must be set to **Unused**. For TagmaStore AMS/WMS Series, a DM-LU must be set up. For more information about TrueCopy please see *Hitachi Thunder 9500 V Series TrueCopy User's Guide*.
	ShadowImage	ShadowImage must be enabled. If you have installed TrueCopy Basic, you can also use ShadowImage. The data share mode must be **ON**. The system start attribute must be dual active mode. The SCSI ID/Port ID inheritance mode must be set to **Unused**. For TagmaStore AMS/WMS Series, a DM-LU must be set up. For more information about ShadowImage please see *Hitachi Thunder 9500 V Series ShadowImage User's Guide*.
	QuickShadow[#2]	QuickShadow must be enabled. Restart the subsystem after installation. For QuickShadow, unlike ShadowImage and TrueCopy, you can only specify a V-VOL, which is a special LU prepared in advance, as an S-VOL. To configure QuickShadow or Copy on Write Snapshot:

Subsystem	Function	Requirements
		Create a QuickShadow pool. In the QuickShadow Pool, define the V-VOL. For the TagmaStore AMS/WMS series, a DM-LU must be set up. For more information about QuickShadow, see the *Copy-on-write SnapShot User's Guide*, or the *Hitachi QuickShadow System Construction Guide*.
Thunder 9200	TrueCopy	TrueCopy Synchronous must be enabled. There must be a fibre-channel connection between the two ports used for a path. The Remote Copy path must be configured. The data share mode must be **ON**. The system start attribute must be dual active mode. The SCSI ID/Port ID inheritance mode must be set to **Unused**. Specify the INQUIRY data extended mode in the host mode 2 to all the ports. For more information on TrueCopy please see *Hitachi Thunder 9200 TrueCopy User's Guide*.
	ShadowImage	ShadowImage Lite must be enabled. The stripe size must be configured as 64 KB. The data share mode must be **ON**. The system start attribute must be dual active mode. The SCSI ID/Port ID inheritance mode must be set to **Unused**. Specify the INQUIRY data extended mode in host mode 2 to all ports. For more information on ShadowImage please see *Hitachi Thunder 9200 ShadowImage User's Guide*.

#1 The settings specified in TrueCopy can be shared with Universal Replicator. However, in Universal Replicator, the settings must be specified for both storage subsystems used for the P-VOL and the S-VOL.

#2 In the TagmaStore AMS/WMS series, the product name is Copy-on-Write Snapshot.

6.4 Using Device Manager with CCI or Protection Manager

6.4.1 Using Device Manager when CCI or Protection Manager Manage Existing Copy Pairs

If a copy pair is already managed by CCI, the copy pair can be managed by Device Manager after Device Manager is installed. Similarly, if the copy pair is managed by Protection Manager, the copy pair can be managed by Device Manager after Device Manager is installed.

Caution: If you want to use Device Manager to control copy pairs managed by CCI or Protection Manager, the configuration definition file on the host that manages the P-VOL of the copy pair and the configuration definition file on the host that manages the S-VOL of the copy pair must have the same group name and the same pair name. If different names are specified, Device Manager cannot control that copy pair.

Note: When you install the Device Manager agent, the Device Manager agent properties must be configured if the installation drive of CCI in Windows is different from the installation drive of the Device Manager agent. For details about the Device Manager agent properties to be configured, see the *HiCommand Device Manager Agent Installation Guide*.

To avoid malfunctions and to shorten the processing time of Device Manager, exclude (from Device Manager operations) copy pairs that you do not plan to control from Device Manager. You can do this by performing the following operations:

1. Check the HORCM instance number of CCI managing the copy pair.
2. In the following property in the Device Manager Agent property file, enter the HORCM instance that you want to exclude from Device Manager operations. Separate HORCM instances by commas if you want to enter multiple HORCM instances:
   - Property file name: server.properties.
   - Property name: server.agent.rm.exclusion.instance.

     Example:

     server.agent.rm.exclusion.instance=0,1,2
3. Restart the Device Manager Agent service (daemon).

6.4.2 Using Device Manager Web Client to Create a Configuration Definition File for CCI

Device Manager Web Client allows you to create a configuration definition file. This configuration definition file is used when CCI is used to create copy pairs.

Note: This function is provided for system administrators who use CCI to manage copy pairs.

Caution: You cannot use the configuration definition file created by this function to create a copy pair by using Device Manager.

- You cannot use Device Manager to delete an invalid configuration file if the file was created by this function. Delete this configuration file from or edit on the host.
- An invalid configuration file or a configuration file that is not used for operating copy pairs may affect system performance: for example, when discovering a subsystem or refreshing information. Delete either of these configuration files from the host.

- Requirements for the function for creating the configuration definition file:
  - The storage subsystem and host satisfy the requirements described in section 6.1, 6.2, and 6.3.
  - The version of Device Manager agent installed on the host is 3.1 or later.
- Using the function for creating the configuration definition file:

To create a configuration definition file:

1. Stop the HBase Storage Mgmt Common Service. (For instructions on how to do that, see section 5.2.2.).
2. Set the value of the client.outputhorcmfunction.enabled property in the client.properties file to true. (For details about the client.outputhorcmfunction.enabled property, see section 8.7.3.).
3. Start the HBase Storage Mgmt Common Service. (For instructions on how to start the HiCommand Single Sign On Service, see section 5.2.2.).
4. Start the operation for creating a copy pair. (For instructions on how to create a copy pair, see the HiCommand Device Manager Web Client User's Guide).

   Caution: When managing pairs by each host, Device Manager Agent version 3.1 or later must be installed on the host to be used. When managing pairs by central management, Device Manager Agent version 3.1 or later must be installed on the host that centrally manages the pairs.
5. Perform the operation in the same manner as when creating a copy pair to display the **Step: Summary Of Changes** dialog box.

   Note: In the **Step: Define Pair(s)** dialog box, you do not need to specify the fence level and copy pace. Even if you specify these items, they are not applied in the configuration definition file.

6. In the **Step: Summary Of Changes** dialog box, click **Cancel (Output HORCM)** to stop creating a copy pair, and then start creating the configuration definition file.
7. When creation of the configuration definition file finishes, a dialog box appears notifying you of the completion. Check the display, and then close the dialog box.

In the View Pair Information dialog box, you can view the HORCM instance number, pair group name, and pair name of the created configuration definition file.

Caution: For a Shadow Image copy pair and a QuickShadow or Copy-on-Write Snapshot copy pair, the Device Manager server sets 0 as the MU number in the configuration definition file. (Note that, for TrueCopy, the MU number is not set because this number is not necessary.) The Device Manager server also sets 1 as the MU number in the configuration definition file for Universal Replicator copy pairs. When you use a configuration definition file, created by the Device Manager server, to create a copy pair, make sure that you change these values into appropriate values.

Chapter 7 HiCommand Device Manager Server Security

This chapter provides an overview of Device Manager security and explains procedures for setting up security.

- Overview of HiCommand Device Manager Security (see section 7.1)
- Using HiKeytool to Set Server Security (see section 7.2)
- Configuring the HBase Storage Management Web Service for SSL (see section 7.3)
- Security Settings for CIM/WBEM Functionality (see section 7.4)
- Authenticating File Operations Using a Java Tool (see section 7.5)

7.1 Overview of HiCommand Device Manager Security

This section discusses the following server security procedures:

Note: Screen shots in this section are from Windows, unless otherwise indicated.

7.1.1 About Server and HBase Storage Mgmt Web Service Security

HiCommand Device Manager uses Secure Sockets Layer (SSL) and Transport Layer Security (TLS) to encrypt network transmissions between the Device Manager client and the Device Manager Server or the HBase Storage Mgmt Web Service. SSL and TLS use cryptography, digital signature technology and digital certificates to provide user authentication, data integrity, and privacy. This document includes instructions for configuring Device Manager to securely communicate over the Internet or an Intranet using SSL and TLS.

WARNING: If you are using Internet Explorer, set your options so that encrypted pages are not saved to disk.

Important: If you enable security on Device Manager, you must make sure that the key pair and associated server certificate do not expire. If either the key pair or the server certificate expires, users will be unable to connect to the Device Manager Server or HBase Storage Mgmt Web Service with the Device Manager Web Client. See section 7.2.1 for instructions.

Note: If you use SSL-encrypted communication, you must enter https:// in the browser when sending a request.

This chapter includes the following terms:

- **<host name>** is used to indicate the name of the host that is running the Device Manager Server or HBase Storage Mgmt Web Service, unless otherwise indicated.
- **<Java Web Start>** is used to indicate the default Java Web Start installation directory on a client machine. If a client's Java Web Start directory is not located in the default location, adjust commands or paths accordingly. The default directories are as follows:

  For Windows:

  C:\Program Files\Java*version-of-JRE***\bin**

  For Solaris:

  /usr/j2se/jre/javaws

  For HP-UX:

  /opt/*version-of-JRE***/jre/javaws**

- **<server installation directory>** is used to indicate the default Device Manager Server installation directory. If your directory is not located in the default directory, adjust commands or paths accordingly. The default server installation directories are as follows:

  For Windows:

  C:\Program Files\HiCommand\Device Manager

  For Solaris or Linux:

  /opt/HiCommand/

- **Public Key Infrastructure (PKI)** is a cryptographic technology developed under the guidance of the Internet Engineering Task Force (IETF) to create a secure networking system that can have interoperative characteristics between multiple vendors.
- **Secure Sockets Layer (SSL)** is a protocol first developed by Netscape® to securely transmit data over the Internet. Two SSL-enabled peers use their Private and Public Keys to establish a secure communication session, with each peer encrypting transmitted data with a randomly generated and agreed-upon symmetric key.
- **Transport Layer Security (TLS)** is the successor protocol to SSL. For more information, see the RFC, The TLS Protocol (version 1.0), located on ftp://ftp.isi.edu/in-notes/rfc2246.txt.
- A **keypair** is two mathematically-related cryptographic keys consisting of a Private Key and its associated Public Key.
- A **keystore** is a file that contains the keypair, which is used for TLS/SSL connections and the corresponding server certificate.
- A **keypass** is a password for restoring the keypair used to encrypt TLS/SSL connections and the corresponding server certificate.
- A **truststore** is a file containing a signed and trusted server certificate.

- A **Server Certificate** (sometimes also called a **Digital Certificate**) forms an association between an identity (in this case the Device Manager Server or the HBase Storage Mgmt Web Service) and a specific keypair. A Server Certificate is used to identify the Device Manager Server or HBase Storage Mgmt Web Service to a client so that the server and client can communicate using TLS/SSL. Server Certificates come in two basic types:
  - Self-signed: (see sections 7.2.1 and 7.3.3). This is the case where you generate your own certificate, so that the subject of the certificate is the same as the issuer of the certificate. For example, when you create a keypair with HiKeytool, you will have a keypair and an associated self-signed certificate.
  - Signed and Trusted: (see sections 7.2.3 and 7.3.2). When a Certificate Signing Request (CSR) is generated and sent to a well-known and trusted Certificate Authority (CA) for signing, and is then signed and returned by the Certificate Authority, your certificate is considered signed and trusted. A well-known and trusted Certificate Authority meets the following requirements:
    1) 1. Certificate for that Certificate Authority is located inside the Device Manager Server truststore,
    2) 2. Certificate for that Certificate Authority is located in the database of trusted Certificate Authorities within browsers supported by Device Manager, and
    3) 3. Certificate for that Certificate Authority is located within the truststore distributed with Java Web Start.

Note: The default Device Manager Server truststore is located at **<installation directory>/jre/lib/security/cacerts**. You can modify the default location using the **server.https.security.truststore** property in the server.properties file (see section 8.8.8). The default truststore for Java Web Start is located at **<Java Web Start installation directory>/cacerts**.

7.2 Using HiKeytool to Set Server Security

7.2.1 Creating a Keypair

Throughout this section, use the default values presented unless you are either very familiar with the area of cryptography and Java(TM) security or are otherwise instructed.

Note: If you make a mistake during this process and need to start over, exit by typing Ctrl+C and restart HiKeytool.

Caution: Start HiKeytool as a user with Administrator privileges (in Windows), or as a root user (in Solaris or Linux).

1. Open a command prompt or terminal window, navigate to `<server installation directory>/HiCommandServer` and launch HiKeytool, as follows:
   - For Windows, type **HiKeytool.bat,** and then press **Enter**.
   - For Solaris or Linux, type **HiKeytool.sh**, and then press **Enter**.
2. The HiKeytool main panel (see Figure 7.1) appears Enter 1.
3. The server main panel appears (see Figure 7.2). Enter 1 (**Make Keypair/Self-Signed Certificate**). The Creating a Keypair panel appears (see Figure 7.3).
4. Enter the server name [default=sasol03]. Use the default value unless your machine is visible to the LAN or WAN under a different name, in which case you should use the name by which the Device Manager Server is visible. Any SSL-encrypted communications with the server MUST use this server name, or you will receive an authentication error.
5. Enter the organizational unit [default= *Device Manager Administration*]. The default value is recommended, but you can use anything meaningful, for example, Marketing.
6. Enter your organization name. Ordinarily you would use the default value or your host name, but you can use another name, such as the name of your company.
7. Enter your city or locality. There is no default value for this field.
8. Enter your state or province. Make sure to spell it out instead of using an abbreviation. There is no default provided.
9. Enter your two-character country code [default=*US*].
10. Enter your key alias. [default=sasol03]. This should be the local host name of the Device Manager Server. Make sure to use the same value that you previously used for the server name.
11. Enter your key password (6 characters minimum) [default=passphrase]. This is the value used to access the keypair entry by the Device Manager Server and the default value is taken from the server.https.keystore.keypass property (see section 8.8.6).

12. For security reasons, you will want to change the default value of the key password.

    Important: You should do so by using the process described in section 7.2.7, and you should not simply change it directly from the properties file.

13. Enter the key algorithm [default=RSA]. Currently, only RSA® is supported.

14. Enter the key size (minimum is 512; maximum is 2048, default=2048]. Assuming the RSA® key algorithm is used, any key size from 512 to 2048 is valid, so long as it is a multiple of 64. Larger key sizes are recommended because that will provide greater data security against brute force and factoring attacks.

15. Enter the signature algorithm [default=MD5withRSA]. Currently, only MD5withRSA is supported.

16. Enter the number of days valid [default=365]. This is the period during which the Device Manager Server keypair will be valid:

    - If you have your server certificate signed by a well-known and trusted Certificate Authority, the number of days valid specified by that authority will override the value you place in this field. Make sure to check the web site of your vendor for specific requirements and calendar the need to renew your certificate, because if the key pair and associated server certificate expire, users will be unable to establish a secure connection with the Device Manager Server via SSL/TLS.
    - If you elect not to have your server certificate signed, the value that you place in this field will determine the period during which the keypair and associated server certificate will be valid. The default is 365 days.

17. Enter the keystore password (6 characters minimum) [default=passphrase]. This is the value used to protect and verify the integrity of the keystore, and the default value is taken from the server.https.keystore.passphrase property (see section 8.8.5).

    Important: If you want to change the default value of the keystore password, you should use the process described in section 7.2.7. Do not change it directly from the properties file.

18. Once you have completed these steps, Device Manager will generate the Device Manager Server keypair and associated certificate. The keypair is placed inside the keystore for the Device Manager Server.

    Note: If you create a keypair with a size of 2048 you might have to wait up to a minute for the keypair to generate.

You will need to restart the Device Manager server for the changes to be implemented.

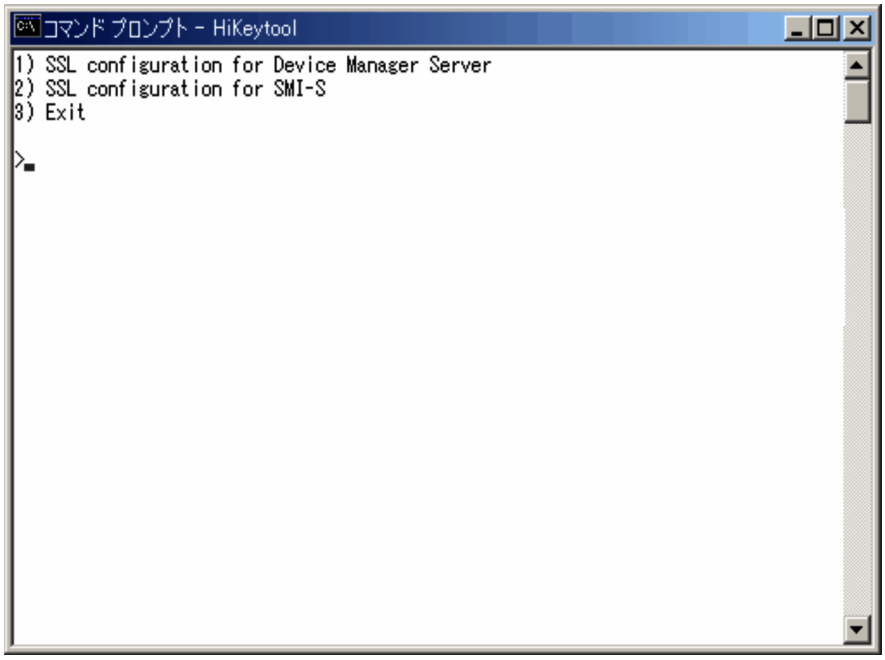

Figure 7.1 HiKeytool Main Panel

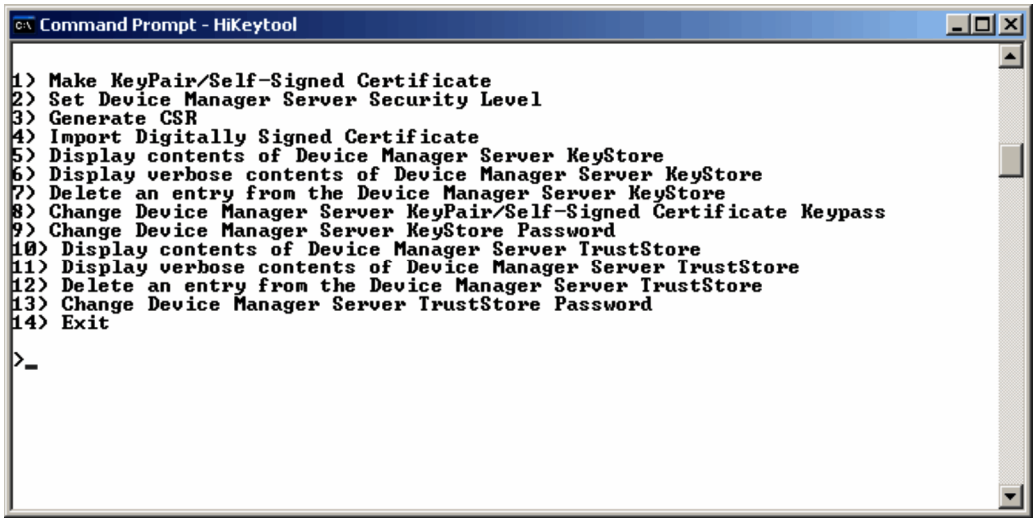

Figure 7.2 Server Main Panel

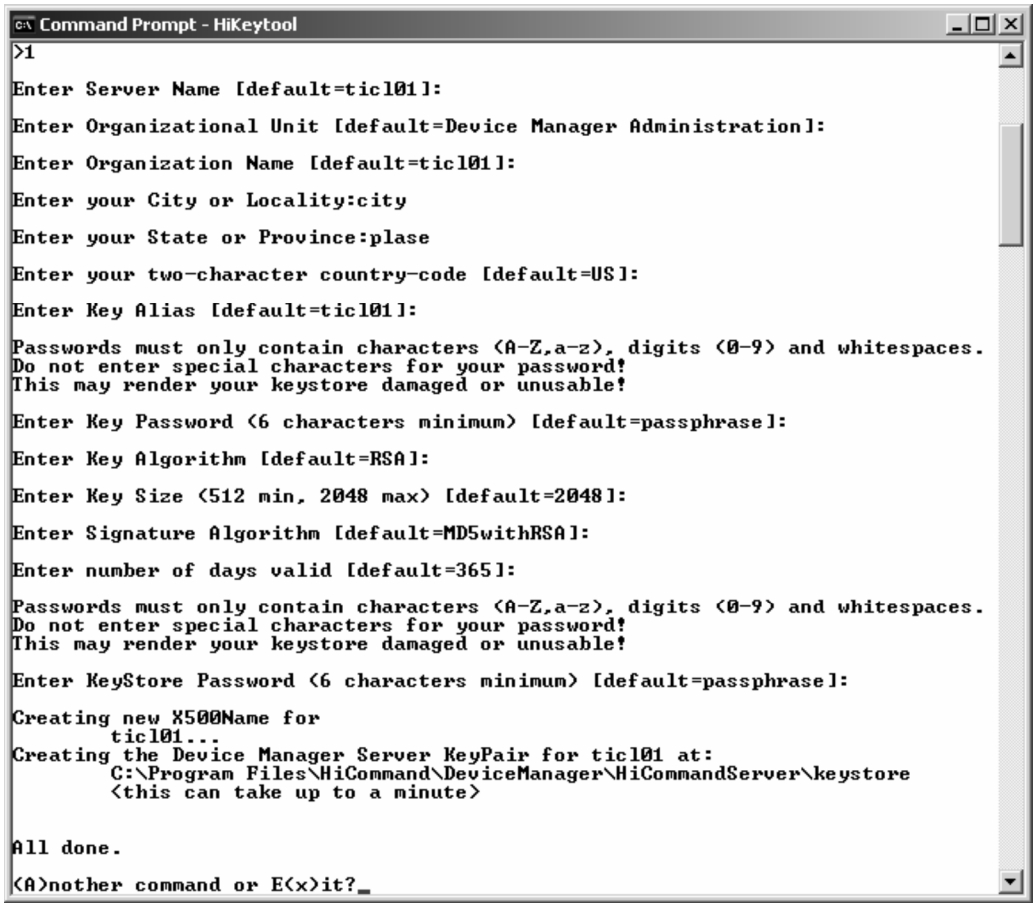

Figure 7.3 Creating a Keypair

7.2.2 Enabling TLS/SSL Server Security

Important: TLS and SSL require Internet Explorer 5.5 or Netscape® 6.0 or higher.

1. Referring to steps 1 and 2 in section 7.2.1, open the server main panel.
2. In the server main panel, enter 2 (**Set Device Manager Server Security Level**).
3. HiKeytool will echo the current security level, display the three available levels of security, and prompt the user for an entry (see Figure 7.4), as follows:
   - 0 Unsecure, no security.
   - 1 Basic authentication, which requires a valid username and password.

     Note: This is the default. Information will be base64 encoded, but it can be easily unencoded and read by anyone listening to the communications being sent on a network.
   - 2 Encrypted using TLS/SSL, which is discussed in this section.
4. To enable TLS/SSL (Secure Sockets), type 2 and press **Enter**. The display will confirm that you have selected TLS/SSL (see Figure 7.5).
5. You will need to restart the Device Manager Server for these changes to take effect.

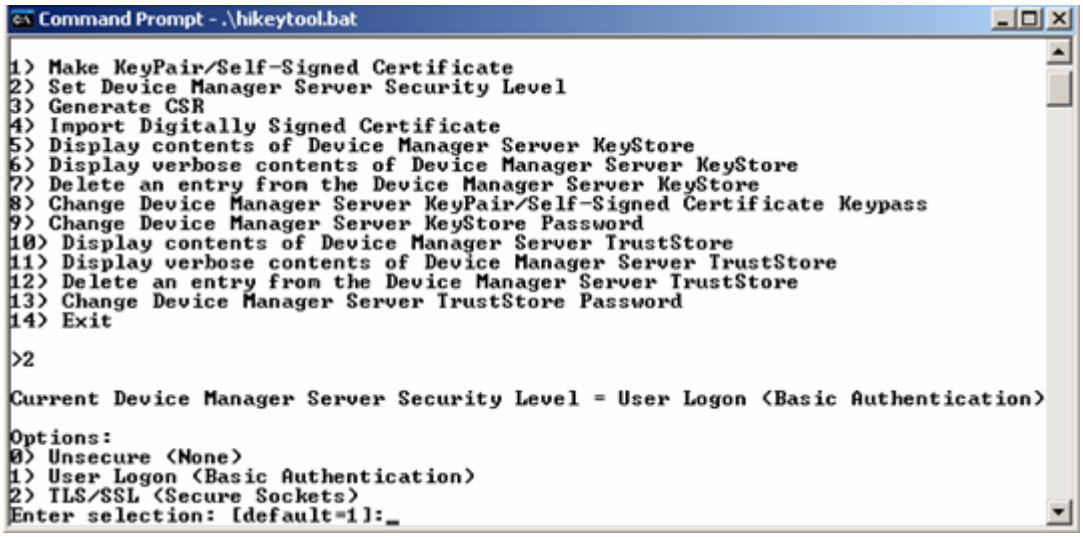

Figure 7.4 Default Device Manager Server Security Level

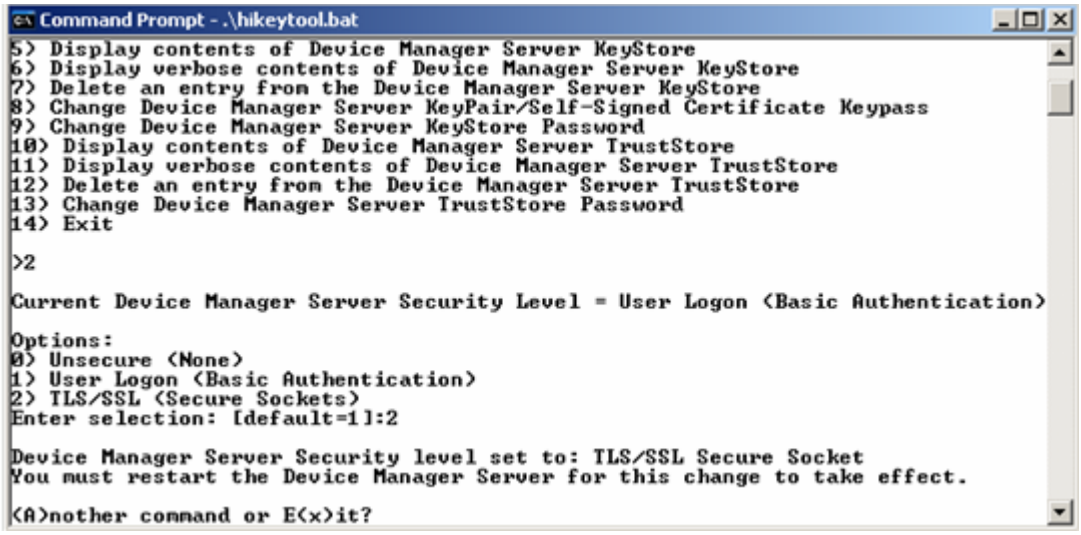

Figure 7.5 Selecting and Confirming Server Security Level Changes

7.2.3 Creating and Importing a Digitally-Signed Certificate

This section contains instructions for obtaining a digitally-signed certificate from a well-known and trusted Certificate Authority. See section 7.1 for a discussion of the merits of using digitally-signed certificates.

7.2.3.1 Creating a Certificate Signing Request (CSR)

To create a Certificate Signing Request:

1. Referring to steps 1 and 2 in section 7.2.1, open the server main panel.
2. In the server main panel, enter 3 (Generate CSR).
3. HiKeytool will inform the user where the Certificate Signing Request has been stored on disk (see Figure 7.6), which will be in a file named <host name>.csr inside the `<server installation directory>/HiCommandServer` directory. The contents of your CSR will look similar to the example in Figure 7.7.

   Important: Your CSR will contain extra carriage returns and line feeds which must be included when it is sent to the Certificate Authority, or it will not be processed correctly.
4. You will then send the CSR to the Certificate Authority of your choice to be digitally signed. The application for digital signing can be done online, and the response is typically returned to you via email from the Certificate Authority.
5. If you intend to have a self-signed certificate digitally signed by a Certificate Authority, you may want to check their web site for specifics. If your Certificate Authority's requirements are sufficiently different, you may want to re-create the Device Manager Server keypair before generating a CSR. To re-create the keypair (see section 7.2.9 for instructions), and then create a new keypair as described in section 7.2.1.

Note: There must be only one entry in the Device Manager Server keystore, or you could have problems when you are running the Device Manager Server in secure mode.

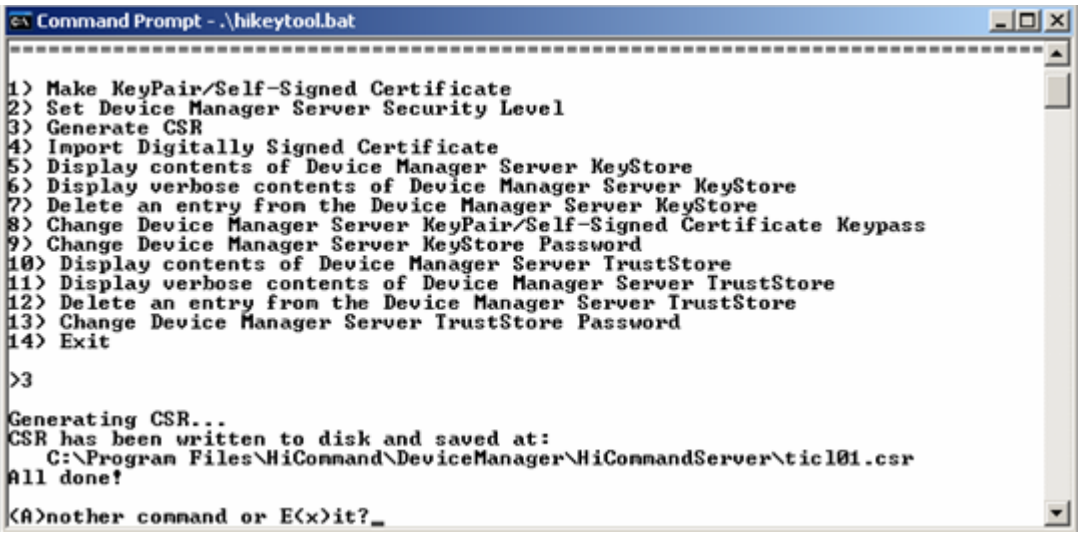

Figure 7.6 Completed CSR

```
---BEGIN NEW CERTIFICATE REQUEST-----
MIICzDCCAbQCAQAwgYYxCzAJBgNVBAYTAlVTMRMwEQYDVQQIEwpDYWxpZm9ybmlhMRQwEgYDVQQH
EwtMb3MgQW5nZWxlczEQMA4GA1UEChMHaGlzaGFyazEoMCYGA1UECxMfSGlDb21tYW5kIFNlcnZl
ciBBZG1pbmlzdHJhdGlvbjEQMA4GA1UEAxMHaGlzaGFyazCCASIwDQYJKoZIhvcNAQEBBQADggEP
ADCCAQoCggEBALH9cjGweKgcjqcNEBAJyduJkvOkov5UGrEFQXsVBGgq3F30W5PD83EIWfS0+UJU
BHPE7YI5A/yc8IrTbhnb+muXHC/+q1KIIzNTAunt0ta2JuhqK5fR22rJh6wCwvzmOwEZJAINPNUW
SN7w1OLsZ7dPJHAQs4KJBsrG9Gh3+KBU0gFMKO8OlmHPP9e8vfGfQolYdSQpOddQLyHKtQxhMkTQ
l3adMMsXykjS4SCFea1TuLcLRaNHg4Q9mPF+YiVmdcqCEXorhQhcMh3iL/AcOrRAQ9GBFZ1xg2Wn
nA8XawVOeWcdB0Dr9W9TwaKNSAAS5xcF0vxkCZQ01Z+5iTdWdc0CAwEAAaAAMA0GCSqGSIb3DQEB
BAUAA4IBAQBfMbLbYOZJ2JWJohGNk1TY8HYv0DNiU1anuADS7gc0/iLX5/9amexHePxRhIthmih7
C1CoR+IvNlJxhzqVhgl9noLqbqQhTFfIClGA2COvdFN8VPzeLidcH94XaaJfSJ44U29iVgNDSuft
bEk124mimGbDdczRxooDms9pSiI2oCtrWFA7zUXSGO7NquKkPaExO+fM6s5cnTlNew5HE8e6jfoL
e65g9/6hcH7KacbWkRzU9R4iMrcOhW6HnlV0GDeCyhmAEW0dsHSwaBptEM3gGo+ffXhL54tXX771
tnYJU1QAJfrRqTi9eFL4N2Ooo4An8jXYooBjnkno1r+X+V4r
-----END NEW CERTIFICATE REQUEST-----
```

Figure 7.7 Sample Certificate Request

7.2.3.2 Importing a Signed and Trusted Certificate

Once you receive your digitally-signed certificate from the Certificate Authority, you can use HiKeytool to import it. Some Certificate Authorities will return your digitally-signed certificate as an attached file with a .cer extension. Others will return the response as text in the body of an email, in which case you should use a text editor such as Notepad or WordPad to save the response in a new file. A digitally-signed certificate looks something like the example in Figure 7.8.

To import a digitally-signed certificate:

1. Move the file containing the digitally-signed certificate into `<server installation directory>/HiCommandServer`. Name the file <alias>.cer, using the alias that you have chosen for the host.

   Note: Make sure to save the response from your Certificate Authority.

2. Referring to steps 1 and 2 in section 7.2.1, open the server main panel.
3. In the server main panel, enter 4 (Import Digitally Signed Certificate).
4. You will be prompted to enter the location of the digitally-signed certificate. If the certificate is in the default location, press **Enter**. Otherwise, type the complete absolute path, and then press **Enter** (see Figure 7.9).
5. You will be notified when the digitally-signed certificate has been imported (see Figure 7.10).
6. You will need to restart the Device Manager server for the changes to be effective.

   You will use the Web Client to connect to the server and recognize the new digitally-signed certificate.

```
-----BEGIN CERTIFICATE-----
MIIDMDCCApmgAwIBAgIDOBcYMA0GCSqGSIb3DQEBBAUAMIGHMQswCQYDVQQGEwJa
QTEiMCAGA1UECBMZRk9SIFRFU1RJTkcgUFVSUE9TRVMgT05MWTEdMBsGA1UEChMU
VGhhd3RlIENlcnRpZmljYXRpb24xFzAVBgNVBAsTDlRFU1QgVEVTVCBURVNUMRww
GgYDVQQDExNUaGF3dGUgVGVzdCBDQSBSb290MB4XDTAxMDkxMTAyMDMzNFoXDTAx
MTAwMjAyMDMzNFowgYYxCzAJBgNVBAYTAlVTMRMwEQYDVQQIEwpDYWxpZm9ybmlh
MRQwEgYDVQQHEwtMb3MgQW5nZWxlczEQMA4GA1UEChMHaGlzaGFyazEoMCYGA1UE
CxMfSGlDb21tYW5kIFNlcnZlciBBZG1pbmlzdHJhdGlvbjEQMA4GA1UEAxMHaGlz
aGFyazCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALH9cjGweKgcjqcN
EBAJyduJkvOkov5UGrEFQXsVBGgq3F30W5PD83EIWfS0+UJUBHPE7YI5A/yc8IrT
bhnb+muXHC/+q1KIIzNTAunt0ta2JuhqK5fR22rJh6wCwvzmOwEZJAINPNUWSN7w
1OLsZ7dPJHAQs4KJBsrG9Gh3+KBU0gFMKO8OlmHPP9e8vfGfQolYdSQpOddQLyHK
tQxhMkTQl3adMMsXykjS4SCFea1TuLcLRaNHg4Q9mPF+YiVmdcqCEXorhQhcMh3i
L/AcOrRAQ9GBFZ1xg2WnnA8XawVOeWcdB0Dr9W9TwaKNSAAS5xcF0vxkCZQ01Z+5
iTdWdc0CAwEAAaMlMCMwEwYDVR0lBAwwCgYIKwYBBQUHAwEwDAYDVR0TAQH/BAIw
ADANBgkqhkiG9w0BAQQFAAOBgQBtzeFG4IfvpPnA7G/khD4rrT1TvjbK4Y1pcROM
cel43uUfKgNYgY35UukoNtd120XOoudLwKvJu5JK7846zWIbEJmCr5BYlmywZuao
MQdXMyPOUnqucgg44/JG2F27xqP4atWEZsNlj5R7XGGXi4RPAO5Y0YbbbvMJD0QR
yV0Oxw==
-----END CERTIFICATE-----
```

Figure 7.8 Sample Digitally-Signed Certificate

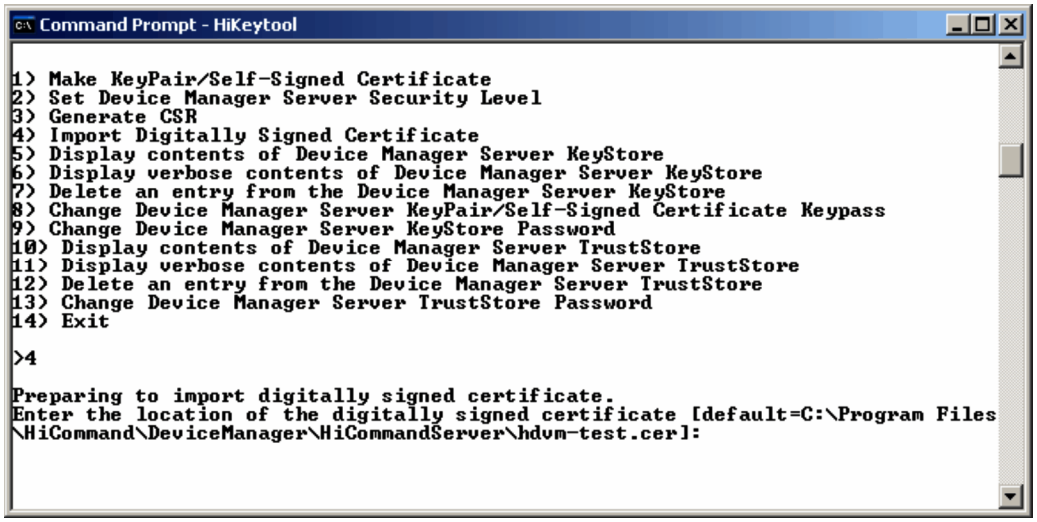

Figure 7.9 Entering the Location of the Digitally-Signed Certificate (Windows)

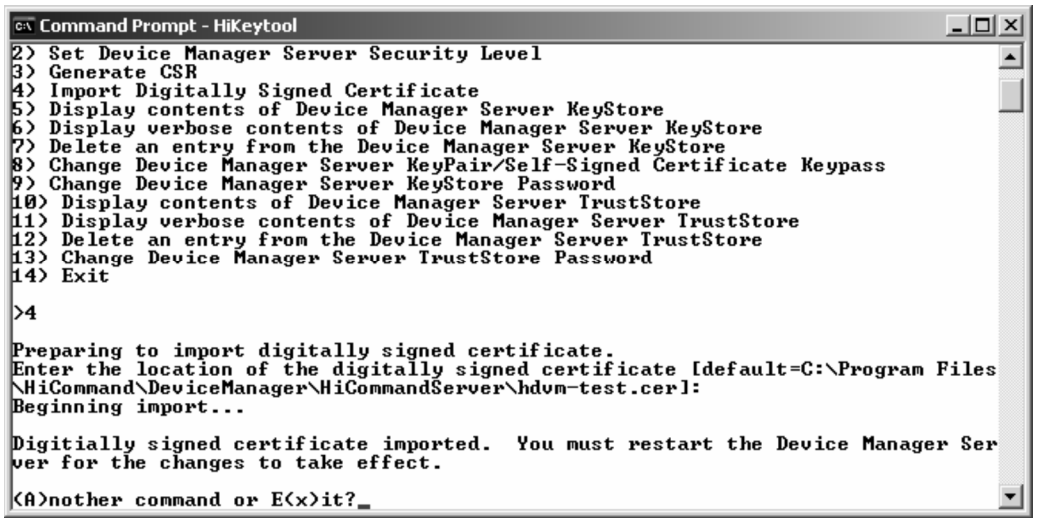

Figure 7.10 Notification of Successful Import of Digitally-Signed Certificate

7.2.4 Displaying Contents of the HiCommand Device Manager Keystore

7.2.4.1 Regular Mode

1. Referring to steps 1 and 2 in section 7.2.1, open the server main panel.
2. In the server main panel, enter 5 (Display Contents of Device Manager Server Keystore).
3. HiKeytool will display information similar to that in Figure 7.11, including the alias for the keystore entry, the date the entry was created, and the MD5 Fingerprints for the entry, as follows:

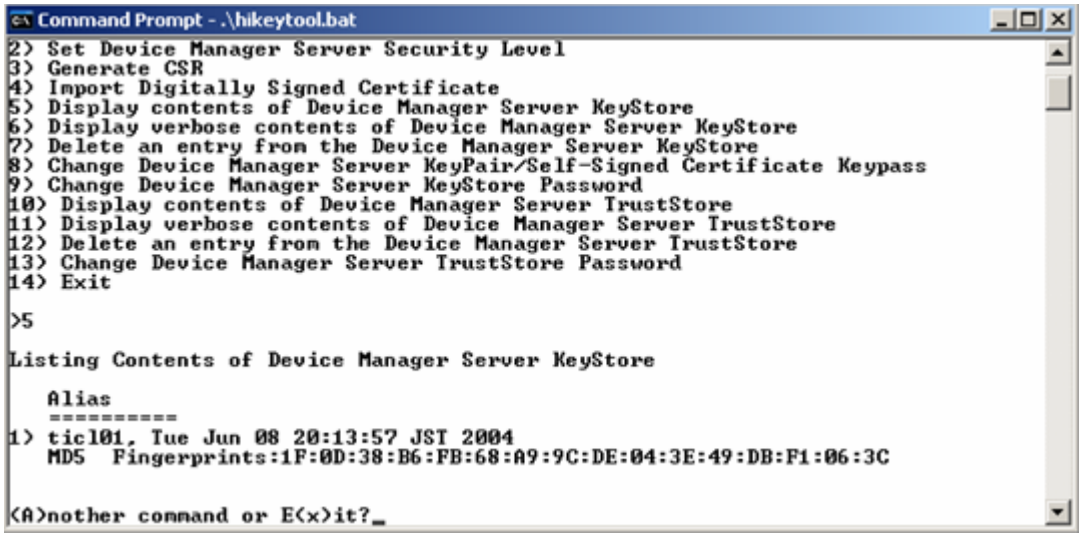

Figure 7.11 Sample Contents of Device Manager Server Keystore

7.2.4.2 Verbose Mode

1. Referring to steps 1 and 2 in section 7.2.1, open the server main panel.
2. In the server main panel, enter 6 (Display Verbose Contents of Device Manager Server Keystore).
3. HiKeytool will display the verbose contents of the Device Manager Server keystore (see Figure 7.12 for a sample).

Figure 7.12 Sample Verbose Contents of Device Manager Server Keystore

7.2.5 Deleting an Entry from HiCommand Device Manager Server Keystore

1. Referring to steps 1 and 2 in section 7.2.1, open the server main panel.
2. In the server main panel, enter 7 (Delete an Entry from the Device Manager Server Keystore).
3. This will display information about the contents of the Device Manager Server keystore, and prompt you to enter the number of the Device Manager Server keypair to be deleted (see Figure 7.13).
4. HiKeytool will request confirmation of the delete (see Figure 7.14). Enter Y to confirm the delete.
5. HiKeytool will display the contents of the Device Manager Server keystore after the deletion.

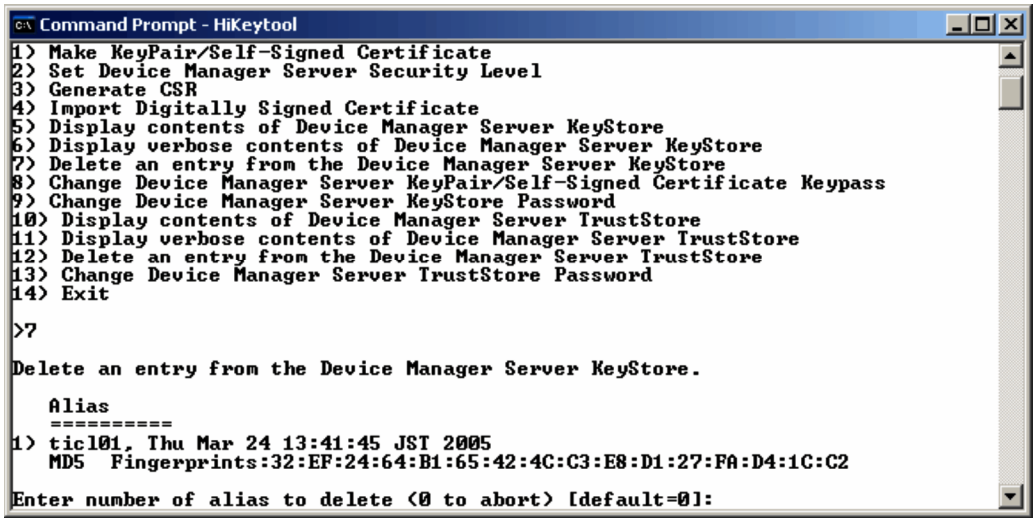

Figure 7.13 Entering the Number of Alias to be Deleted

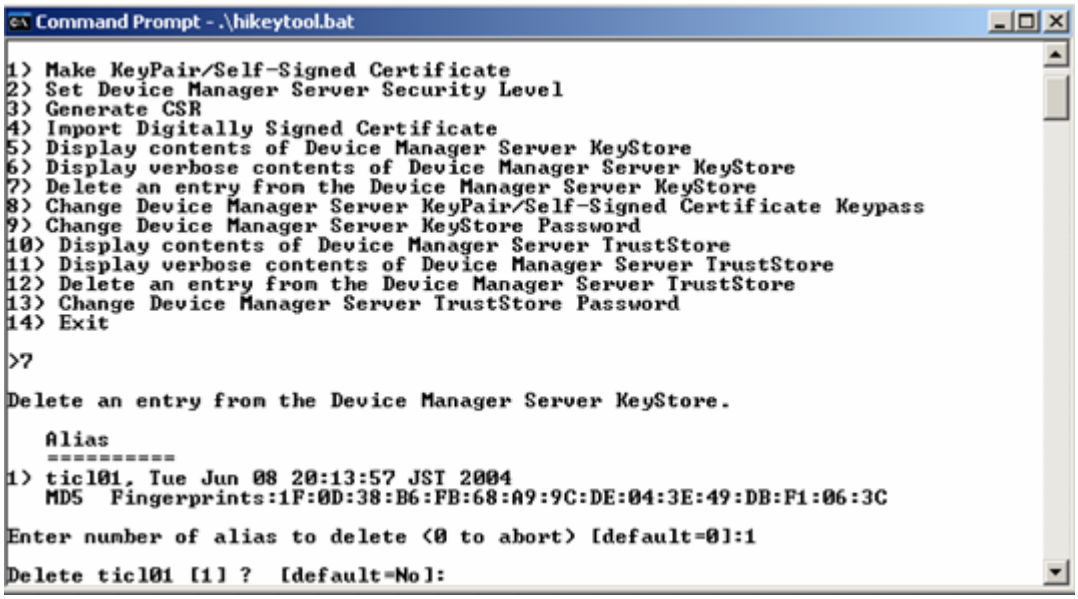

Figure 7.14 Confirming Deletion of an Alias

7.2.6 Changing the Device Manager Server Keypass

1. Referring to steps 1 and 2 in section 7.2.1, open the server main panel.
2. In the server main panel, enter 8 (**Change Device Manager Server Keypair/Self-Signed Certificate Keypass**).
3. Enter the existing HiCommand Device Manager server keystore password (see Figure 7.15).
4. Type the existing keypass and press **Enter** (see Figure 7.16).
5. Type the new keypass and press **Enter** (see Figure 7.17). This is case sensitive.

   WARNING: Make sure to enter only characters (A-Z, a-z), numbers (0-9) or white space, or you can render your keystore unusable.
6. You will be prompted for a confirmation of the new Keypass. Type the new Keypass again and press **Enter** (see Figure 7.17).
7. You must restart the Device Manager server for the changes to be effective.

Figure 7.15 Entering the Current Keystore Password

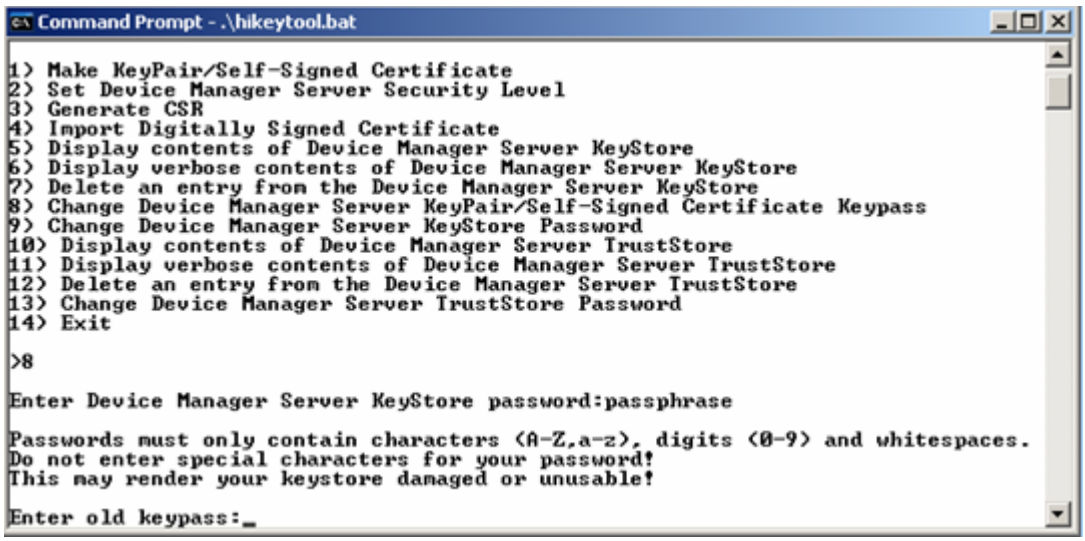

Figure 7.16 Entering the Old Keypass

Figure 7.17 Entering and Confirming the New Keypass

7.2.7 Changing the Device Manager Server Keystore Password

1. Referring to steps 1 and 2 in section 7.2.1, open the server main panel.
2. In the server main panel, enter 9 (**Change Device Manager Server Keystore Password**).
3. Type the current keystore password, then press **Enter** (see Figure 7.18).

   You will be prompted for your new password. (see Figure 7.19).
4. Type the new password and press **Enter** (see Figure 7.20).

   This password is case-sensitive.

   WARNING: Make sure to enter only characters (A-Z, a-z), numbers (0-9) or white space, or you can render your keystore unusable.
5. Confirm the new password (see Figure 7.20).
6. You will have to restart the Device Manager server for the changes to be effective.

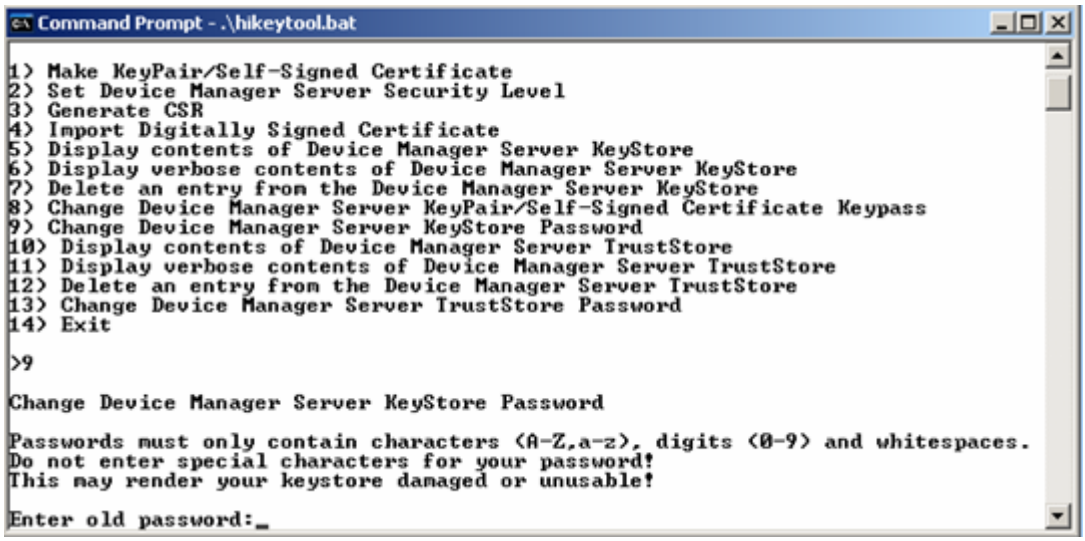

Figure 7.18 Entering Old Keystore Password

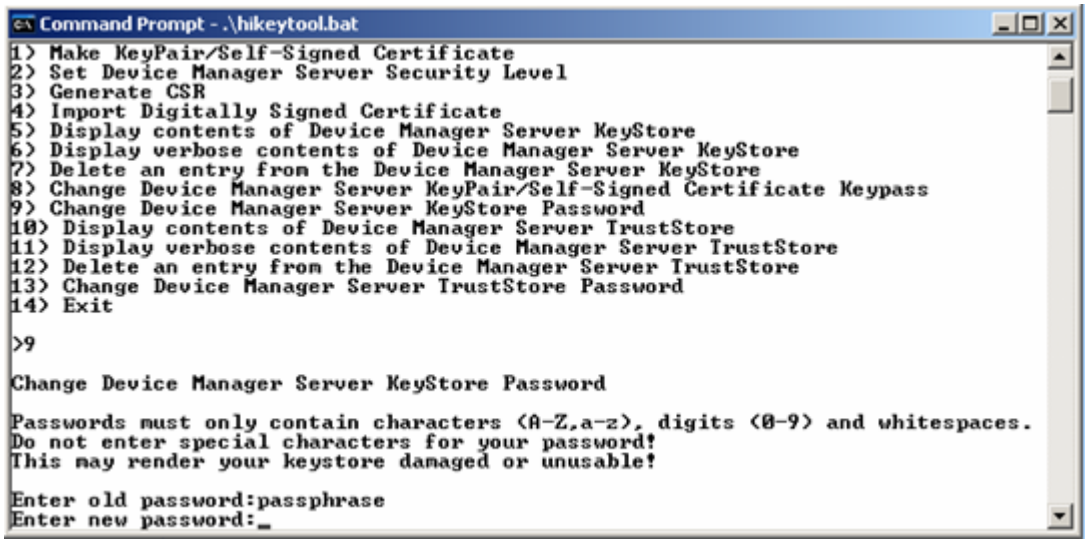

Figure 7.19 Entering New Keystore Password

Figure 7.20 Confirming New Keystore Password

7.2.8 Displaying Contents of HiCommand Device Manager Server Truststore

7.2.8.1 Regular Mode

1. Referring to steps 1 and 2 in section 7.2.1, open the server main panel.
2. In the server main panel, enter 10 (**Display Contents of Device Manager Server Truststore**).
3. The display will include the entry alias, the date the certificate was created, and the MD5 Fingerprints for that entry (see Figure 7.21).

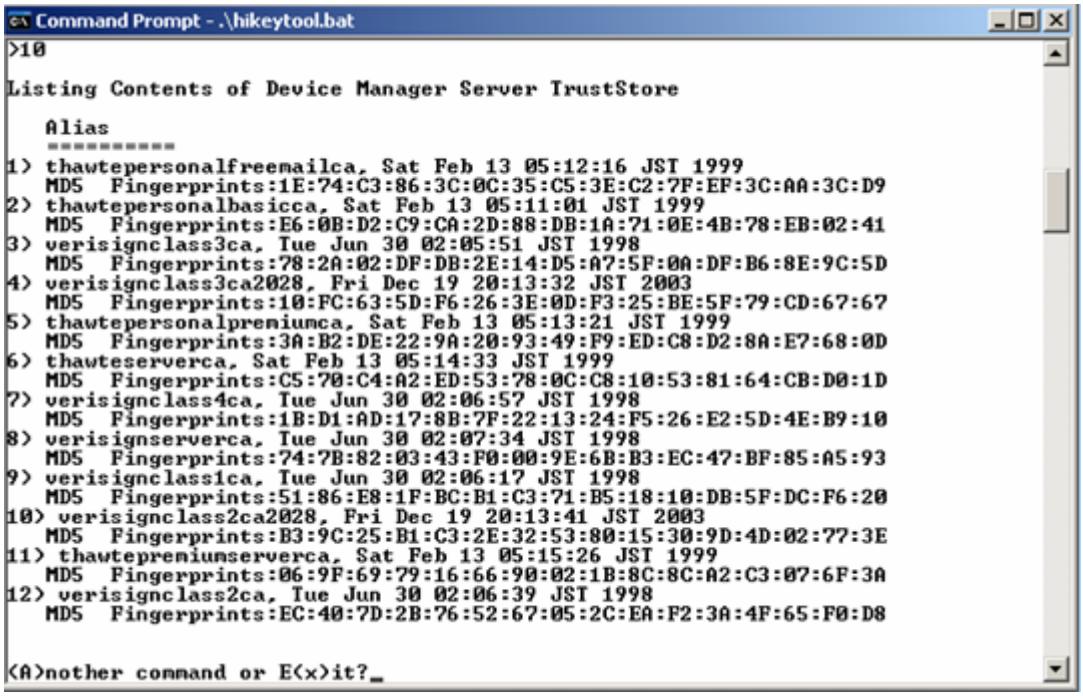

Figure 7.21 Contents of Device Manager Server Truststore

7.2.8.2 Verbose Mode

1. Referring to steps 1 and 2 in section 7.2.1, open the server main panel.
2. In the server main panel, enter 11 (**Display Verbose Contents of Device Manager Server Truststore**).
3. This will display the verbose information for each entry in the Device Manager Server truststore (see Figure 7.22).

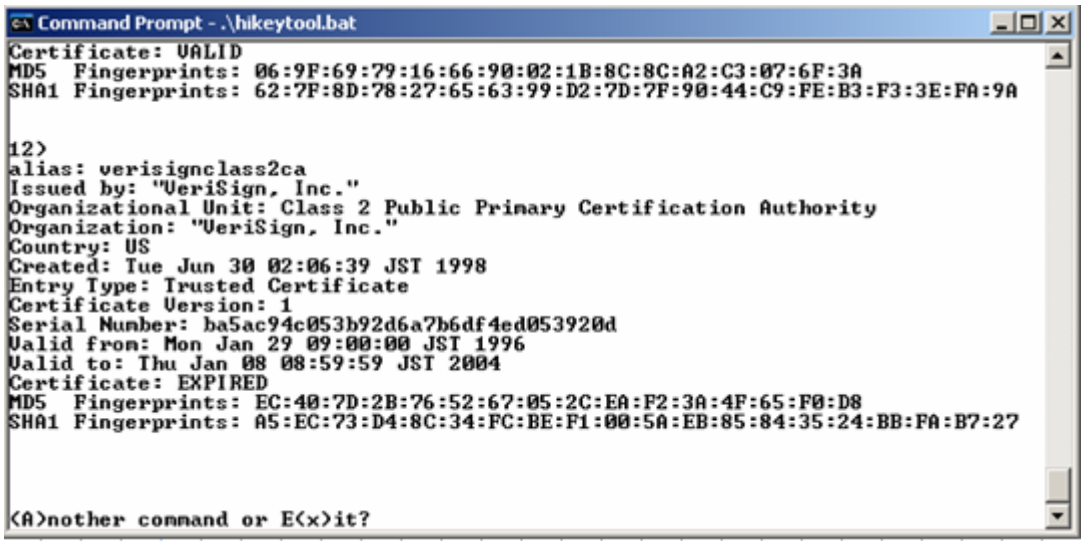

Figure 7.22 Displaying Verbose Information for Device Manager Truststore

7.2.9 Deleting an Entry from HiCommand Device Manager Server Truststore

1. Referring to steps 1 and 2 in section 7.2.1, open the server main panel.
2. In the server main panel, enter 12 (Delete an Entry from the Device Manager Server Truststore).
3. HiKeytool will display a list of all entries in the Device Manager Server truststore.
4. Type the number of the alias to be deleted from the Device Manager Server truststore, and press **Enter** (see Figure 7.23).
5. HiKeytool will request confirmation from the user to delete the designated entry. Enter Y to delete the entry (see Figure 7.24).
6. HiKeytool will delete the nominated entry, re-list the contents of the Device Manager Server truststore, and note that the deletion has been completed.

Figure 7.23 Entering the Alias to be Deleted from Truststore

Figure 7.24 Confirming the Alias to be Deleted From Truststore

7.2.10 Changing the HiCommand Device Manager Server Truststore Password

1. Referring to steps 1 and 2 in section 7.2.1, open the server main panel.
2. In the server main panel, enter 13 (Change Device Manager Server Truststore Password).
3. Type the existing truststore password and press **Enter** (see Figure 7.25).

   The truststore password will be set in the `server.https.truststore.passphrase` property of the Device Manager server properties file. (For details, see section 8.8.9.)
4. Type the new truststore password and press **Enter** (see Figure 7.26). This password is case sensitive.

   WARNING: Make sure to enter only characters (A-Z, a-z), numbers (0-9) or white space, or you can render your keystore unusable.
5. Type the new password in again, and press **Enter** (see Figure 7.26).
6. You will need to restart the Device Manager server for the changes to take effect.

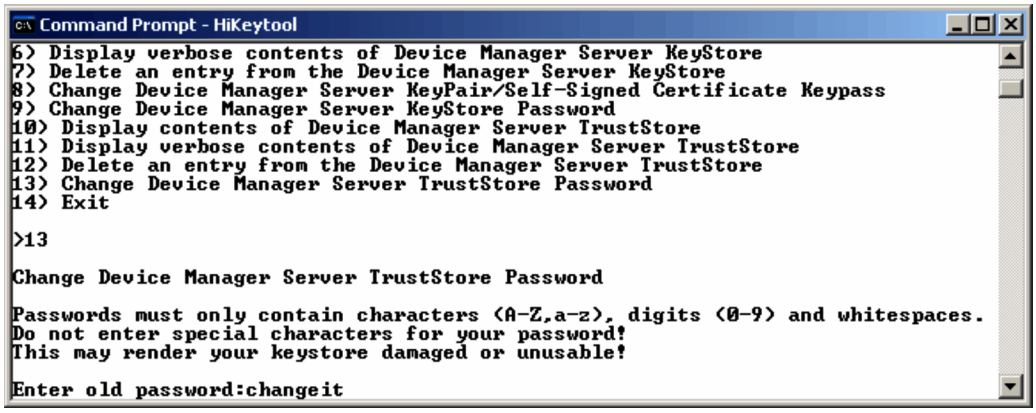

Figure 7.25 Entering the Current Truststore Password

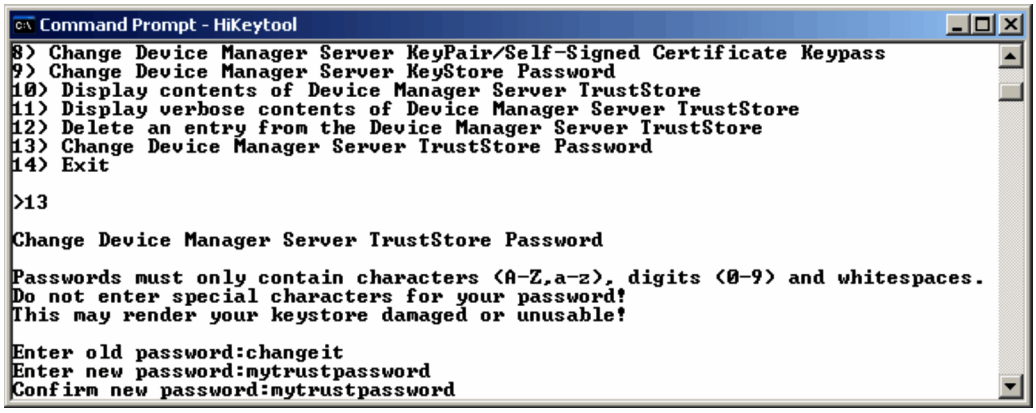

Figure 7.26 Entering and Confirming New Truststore Password

7.3 Configuring the HBase Storage Management Web Service for SSL

The HBase Storage Mgmt Web Service supports versions 3 of SSL, and version 1 of TLS.

This section discusses the following security procedures:

- Generating a Private Key (see section 7.3.1)
- Creating a Certificate Signing Request (CSR) (see section 7.3.2)
- Creating a Self-Signed Certificate (see section 7.3.3)
- Enabling SSL (see section 7.3.4.1)
- Disabling SSL (see section 7.3.4.2)
- Changing a Port Assigned to SSL (see section 7.3.4.3)

This section gives notes on setting SSL (see section 7.3.5).

7.3.1 Generating a Private Key Using SSLC

To create a private key, you will use the sslc utility. You can either use the private key as the basis for a certificate signing request (see section 7.3.2), or you can use it as a self-signed certificate to test the web server. The default location of the sslc utility is as follows:

Windows:

C:\Program Files\HiCommand\Base\httpsd\sslc\bin

Solaris or Linux:

/opt/HiCommand/Base/httpsd/sslc/bin

The sslc utility has the following format:

sslc genrsa -out key-file [512 | 1024 | 2048]

- **-out key-file** specifies the file that will contain the private key.
- **[512** | **1024** | **2048**] specifies the bit length of the private key.

For example, to output a 1024-bit private key to the httpsdkey.pem file, you would execute the command as shown below. In this example, you first move to the directory for storing the sslc utility, and then execute the command.

- **# .\sslc genrsa -out demoCA/httpsdkey.pem** 1024 (Windows)
- **# ./sslc genrsa -out demoCA/httpsdkey.pem** 1024 (Solaris or Linux)

This would generate the following output:

```
 1160 semi-random bytes loaded
Generating RSA private key, 1024 bit long modulus
.........+++++
.........+++++
e is 65537 (0x10001)
```

Figure 7.27 Output of # ./sslc genrsa -out demoCA/httpsdkey.pem 1024 Command

7.3.2 Creating a Certificate Signing Request (CSR)

Use the sslc req utility to create a Certificate Signing Request (CSR), which you will send to a Certificate Authority (CA). After you send a CSR to a CA, the CA will send you a signed certificate in the format of *.pem. The received certificate is used to enable SSL. The exact format of the CSR will vary depending on which CA you use.

If Device Manager has been installed in the default directory, the sslc.cnf file to be specified by the sslc req utility is in the following location:

Windows:

C:\Program Files\HiCommand\Base\httpsd\sslc\bin\demoCA

Solaris or Linux:

/opt/HiCommand/Base/httpsd/sslc/bin/demoCA

The sslc req utility has the following format:

sslc req -config configuration-file -new -key key-file -out CSR-file

- **-config configuration-file** specifies the sslc.cnf file that contains the information you want the utility to access. When you define information in the sslc.cnf file in advance, you do not need to enter information such as Country Name and Locality Name on the command line. If you want to use information that is different than previously defined, you need to specify it when prompted.
- **-new** indicates a new CSR (required).
- **-key key-file** indicates the file containing the private key.
- **-out CSR-file** indicates the file that will contain the Certificate Signing Request (CSR).

For example, to output a CSR when the configuration file is demoCA/sslc.cnf, the key file is demoCA/httpsdkey.pem, and the name of the CSR file is demoCA/httpsd.csr, you would execute the command as shown below. In this example, you first move to the directory for storing the sslc utility, and then execute the command.

- **# .\sslc req -config demoCA\sslc.cnf -new -key demoCA\httpsdkey.pem -out demoCA\httpsd.csr** (Windows)
- **# ./sslc req -config demoCA/sslc.cnf -new -key demoCA/httpsdkey.pem -out demoCA/httpsd.csr** (Solaris or Linux)

The utility would prompt you to enter certain information, including the country name and locality. If you want to leave a field blank, enter a period (.). If you want to select the default, press **Enter**.

Note: For Common Name, specify the host name of the web server. The prompts appear generally as follows:

```
Using configuration from demoCA/sslc.cnf
You will be prompted to enter information to incorporate into the certificate request.
This information is called a Distinguished Name or a DN.
There are many fields however some can remain blank.
Some fields have default values.
Enter '.', to leave the field blank.
-----
Country Name (2 letter code) []:US
State or Province Name (full name) []:Washington
Locality Name (eg, city) []:New York
Organization Name (eg, company) []:HITACHI
Organizational Unit Name (eg, section) []:WebSite
Common Name (eg, YOUR name) []:www.example.com
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

Figure 7.28 sslc req Utility Prompts

7.3.3 Creating a Self-Signed Certificate

If you do not have a signed and trusted certificate, you can create a self-signed certificate using the sslc x509 utility. This is useful if you want to test the web server.

The sslc x509 utility has the following format:

sslc x509 -in CSR-file -out certificate-file -req -signkey key-file -days valid-period.

- **-in CSR-file** specifies the Certificate Signing Request (CSR) file to be passed to the utility.
- **-out certificate-file** specifies the file for containing the created self-signed certificate.
- **-req** indicates the request (required).
- **-signkey key-file** specifies the file that contains the private key.
- **-days valid-period** specifies the number of days during which the self-signed certificate is valid.

For example, to create a self-signed certificate when the CSR file is demoCA/httpsd.csr, the key file is demoCA/httpsdkey.pem, and the name of the file that will contain the self-signed certificate is demoCA/newcert.pem, you would execute the command as shown below. In this example, you first move to the directory for storing the sslc utility, and then execute the command.

- **# .\sslc x509 -in demoCA\httpsd.csr -out demoCA\newcert.pem -req -signkey demoCA\httpsdkey.pem -days 365** (Windows).
- **# ./sslc x509 -in demoCA/httpsd.csr -out demoCA/newcert.pem -req -signkey demoCA/httpsdkey.pem -days 365** (Solaris or Linux).

This would create the following output:

```
Signature OK
subject=/C=US/ST=Washington/L=New York/O=HITACHI/OU=WebSite/CN=www.example.com
```

Figure 7.29 Sample Output of a sslc x509 Command

7.3.4 Configuring SSL

To enable or disable SSL, or to change the port for SSL, you must edit the httpsd.conf file. The following describes the storage destination for the httpsd.conf file.

- For Windows:

  installation-folder-for-HiCommand-Suite-Common-Component\httpsd\conf\

- For Solaris or Linux:

  /opt/HiCommand/Base/httpsd/conf/

7.3.4.1 Enabling SSL

To enable SSL:

1. If HiCommand Suite products whose versions are earlier than 5.7 have been installed, stop their services.

   For details about how to stop these services, see the manual for your product version.

2. Stop the HiCommand Suite product services and HiCommand Suite Common Component.
   - In Windows

     From **Start,** choose **Programs, HiCommand**, **Device Manager**, and then **Stop Server with Common Services**
   - In Solaris or Linux

     Execute the following command:

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

3. Copy the private key file and the signed certificate file received from the Certificate Authority to an appropriate directory.

   We recommend that you copy these files into the following directory:
   - In Windows

     c:\Program Files\HiCommand\Base\httpsd\conf\ssl\server
   - In Solaris or Linux

     /opt/HiCommand/Base/httpsd/conf/ssl/server

4. Open the httpsd.conf file.

5. Make the directives for the SSL port and logical host effective by deleting the pound sign (#) at the beginning of the corresponding lines.

6. Specify the full path name of the certificate file received from the Certificate Authority in SSLCertificateFile.

   Important: If you use a certificate issued by a chained Certificate Authority, specify the full path name in SSLCACertificateFile.

7. Specify the full path name of the private key file for the web server in SSLCertificateKeyFile.

8. Start the HiCommand Suite product services and HiCommand Suite Common Component.
   - In Windows

     From **Start,** choose **Programs, HiCommand**, **Device Manager**, and then **Stop Server with Common Services**
   - In Solaris or Linux

     Execute the following command:

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

9. If HiCommand Suite products whose versions are earlier than 5.7 have been installed, restart their services as required.

   For details about how to start these services, see the manual for your product version.

In this example, the signed certificate received from the Certificate Authority is httpsd.pem, and the private key is httpsdkey.pem.

Note: The line that begins with a pound sign (#) is a comment line.

```
Listen 23015
SSLDisable

Listen 23016
<VirtualHost www.example.com:23016>
  ServerName www.example.com
  SSLEnable
  SSLRequireSSL
  SSLCertificateFile "c:/Program Files/HiCommand/Base/httpsd/conf/ssl/server/httpsd.pem"
  SSLCertificateKeyFile "c:/Program
Files/HiCommand/Base/httpsd/conf/ssl/server/httpsdkey.pem"
#  SSLCACertificateFile "c:/Program Files/HiCommand/Base/httpsd/conf/ssl/cacert
/anycert.pem"
  SSLSessionCacheTimeout 3600
</VirtualHost>
```

Figure 7.30 Enabling SSL (Windows)

In this example, the signed certificate received from the Certificate Authority is httpsd.pem, and the private key is httpsdkey.pem.

Note: The line that begins with a pound sign (#) is a comment line.

```
Listen 23015
SSLDisable

Listen 23016
<VirtualHost www.example.com:23016>
  ServerName www.example.com
  SSLEnable
  SSLRequireSSL
  SSLCertificateFile    /opt/HiCommand/Base/httpsd/conf/ssl/server/httpsd.pem
  SSLCertificateKeyFile /opt/HiCommand/Base/httpsd/conf/ssl/server/httpsdkey.pem
# SSLCACertificateFile  /opt/HiCommand/Base/httpsd/conf/ssl/cacert/anycert.pem
  SSLSessionCacheTimeout 3600
</VirtualHost>
SSLCacheServerPort   /opt/HiCommand/Base/httpsd/logs/gcache_port
SSLCacheServerPath   /opt/HiCommand/Base/httpsd/sbin/gcache
SSLCacheServerRunDir /opt/HiCommand/Base/httpsd/logs
```

Figure 7.31 Enabling SSL (Solaris or Linux)

7.3.4.2 Disabling SSL

To disable SSL, comment out the directives for the SSL port and ***logical*** host in the httpsd.conf file.

Caution: Stop the Device Manager and HiCommand Suite Common Component, and then edit the httpsd.conf file. After editing the file, start the Device Manager and HiCommand Suite Common Component to apply the changes.

Figure 7.32 is an example of disabling SSL in Windows.

Note: The line that begins with a pound sign (#) is a comment line.

```
Listen 23015
SSLDisable

#Listen 23016
#<VirtualHost www.example.com:23016>
# ServerName www.example.com
# SSLEnable
# SSLRequireSSL
# SSLCertificateFile "c:/Program Files/HiCommand/Base/httpsd/conf/ssl/server/httpsd.pem"
# SSLCertificateKeyFile "c:/Program
Files/HiCommand/Base/httpsd/conf/ssl/server/httpsdkey.pem"
# SSLCACertificateFile "c:/Program Files/HiCommand/Base/httpsd/conf/ssl/cacert
/anycert.pem"
# SSLSessionCacheTimeout 3600
#</VirtualHost>
```

Figure 7.32 Disabling SSL (Windows)

Figure 7.33 is an example of disabling SSL in Solaris or Linux.

Note: The line that begins with a pound sign (#) is a comment line.

```
Listen 23015
SSLDisable

#Listen 23016
#<VirtualHost www.hws.hitachi.co.jp:23016>
#  ServerName www.hws.hitachi.co.jp
#  SSLEnable
#  SSLRequireSSL
#  SSLCertificateFile    /opt/HiCommand/Base/httpsd/conf/ssl/server/httpsd.pem
#  SSLCertificateKeyFile /opt/HiCommand/Base/httpsd/conf/ssl/server/httpsdkey.pem
#  SSLCACertificateFile  /opt/HiCommand/Base/httpsd/conf/ssl/cacert/anycert.pem
#  SSLSessionCacheTimeout 3600
#</VirtualHost>
# SSLCacheServerPort   /opt/HiCommand/Base/httpsd/logs/gcache_port
# SSLCacheServerPath   /opt/HiCommand/Base/httpsd/sbin/gcache
# SSLCacheServerRunDir /opt/HiCommand/Base/httpsd/logs
```

Figure 7.33 Disabling SSL (Solaris or Linux)

7.3.4.3 Changing a Port Assigned to SSL

The default port of SSL for HBase Storage Mgmt Web Service is 23016. To change the port, edit the httpsd.conf file and hsso.conf file.

Stop the Device Manager and HiCommand Suite Common Component, and then edit the httpsd.conf file and hsso.conf file. After editing these files, start the Device Manager and HiCommand Suite Common Component to apply the changes.

7.3.5 About Setting SSL

When SSL communication is set for Device Manager, it can be used between the HBase Storage Mgmt Web Service and the Device Manager server, and between the Device Manager server and the Web Client. For details about SSL settings for linked applications, see the appropriate documentation.

When you set SSL, you will need to specify a logical host name for the cluster manager IP address. That IP address must be enabled and accessible. If that IP address was specified during Device Manager installation, execute the following command:

Windows:

c:\Program Files\HiCommand\Base\bin\hcmdschgurl /change http://<cluster manager IP address>:port number http://<host name for the cluster manager IP address>:port number

Solaris or Linux:

/opt/HiCommand/Base/bin/hcmdschgurl -change http:// <cluster manager IP address>:port number http:// <host name for the cluster manager IP address>:port number

7.3.5.1 Security Settings for HiCommand Device Manager Server

If you are creating a keypair by using HiKeytool, specify a logical host name in **Enter Server Name[default=HDM_Server]:** (see Figure 7.3).

7.3.5.2 SSL Settings for HBase Storage Mgmt Web Service

When creating a Certificate Signing Request (CSR), specify a logical host name in Common Name (eg, YOUR name). That IP address must be enabled and accessible.

If you are editing the `httpsd.conf` file, stop the Device Manager and HiCommand(R) Suite Common Component, and then edit the `httpsd.conf` file.

For the items shown below, among the host names displayed by using the `hostname` command, specify the host names that are used by the Device Manager server. In Windows, host names can also be displayed by using the `ipconfig /ALL` command. Note that host names are case sensitive.

- `ServerName` at the beginning of the `httpsd.conf` file
- `<VirtualHost>`
- `ServerName` enclosed by `<VirtualHost>` and `</VirtualHost>`

Figure 7.34 shows the editing format for the `httpsd.conf` file.

```
ServerName logical-host-name
 :
Listen 23015
SSLDisable
 :
SSLSessionCacheSize 0
Listen 23016
<VirtualHost logical-host-name:port-number>
 ServerName logical-host-name
 SSLEnable
 SSLRequireSSL
 SSLCertificateFile signed-certificate-file
 SSLCertificateKeyFile private-key-file-for-the-web-server
 SSLCACertificateFile certificate-file-of-chained-authorized-body
 SSLSessionCacheTimeout 3600
</VirtualHost>
```

Figure 7.34 Editing Format for the httpsd.conf File

After editing the `httpsd.conf` file, start the Device Manager and HiCommand Suite Common Component to apply the changes.

7.4 Security Settings for CIM/WBEM Functionality

CIM/WBEM functionality supports SSL communication for the following functions:

- Object operations

  In the object operation feature, a CIM client acts as an SSL client and the Device Manager server acts as an SSL server.

  By default, you can perform SSL communication in object operations. If you want to modify a keystore file used for SSL, see section 7.4.1.

- Event indication

  In the event indication feature, the Device Manager server acts as an SSL client and a CIM client (Indication Listener) acts as an SSL server.

  By default, the Device Manager server can use SSL communication to receive event indications by following the CIM client requests. In this case, settings must be specified beforehand to enable SSL communication between the CIM clients.

In addition, you can strengthen security by applying two-way authentication for object operations and event indication. Two-way authentication enables communications between pre-specified trusted users. In this way, users can accept object operations from specific CIM clients only, and send event indications to specific CIM clients only. For details on the setting procedures, see section 7.4.2 and 7.4.3.

Caution: You must enable CIM/WBEM functionality to perform SSL communication. For details on setting up CIM/WBEM features, see Chapter 11.

Note: Use Java™ commands to set up SSL, as described in section 7.5.

7.4.1 Modifying the Keystore File for Object Operations

The keystore file used for CIMOM object operations (the keystore password is `wbemssl`) is by default stored in the following location and can be used without any modification:

In Windows:

installation-folder-for-the-Device-Manager-Server\HiCommandServer\wsi\server\jserver\bin\.keystore

In Solaris or Linux:

/opt/HiCommand/HiCommandServer/wsi/server/jserver/bin/.keystore

To modify the keystore file:

1. Create a keystore file. Name the file `.keystore` and use it to replace the default keystore file. For details on how to create a keystore file, see section 7.5.1.
2. Encrypt the keystore password.

   Use `WSIEncryptString.jar` to encrypt the keystore password that was specified during creation of the keystore file in step 1. `WSIEncryptString.jar` is stored in the following location:

   – In Windows:

   installation-folder-for-the-Device-Manager-Server\HiCommandServer\wsi\no-redist

   – In Solaris or Linux:

   /opt/HiCommand/HiCommandServer/wsi/no-redist/

   Example of executing the command:

   > java -jar WSIEncryptString.jar keystore-password

   When the command is executed, the encrypted character string of the keystore password is displayed. This character string is used in a later step.
3. Stop the Device Manager server.

   – In Windows:

   Select **Start**, **Programs**, **HiCommand**, **Device Manager**, and then **Stop Server**.

   – In Solaris or Linux:

   Execute the following command:

   # /opt/HiCommand/suitesrvcntl -stop_hdvm
4. Modify the MOF file (`WBEMSolutions_CIMXMLCPA.mof`).

   Specify in the MOF file the keystore password that was encrypted in step 2 of this procedure. The MOF file is stored in the following location:

   – In Windows:

   installation-folder-for-the-Device-Manager-Server\HiCommandServer\wsi\server\jserver\mof

   – In Solaris or Linux:

   /opt/HiCommand/HiCommandServer/wsi/server/jserver/mof

```
instance of WBEMSolutions_HttpsCPASettingData as $d {
InstanceID = "WBEMSolutions:WBEMSolutions_HttpsCPASettingData:001";
ElementName = "WBEM Solutions HTTPS Client Adapter Settings";
ClientAuthenticationEnabled = false;
ServerKeyStorePassword = "xxxxxx";
};
```

Figure 7.35 MOF File Example

The xxxxxx part of ServerKeyStorePassword contains the character string that encrypted the keystore password used by the default keystore file. In xxxxxx, specify the keystore password that you encrypted in step 2.

5. Compile the MOF file.

   Use the mofcomp command to compile the MOF file. The mofcomp command is stored in the following location:

   - In Windows:

     installation-folder-for-the-Device-Manager-Server\HiCommandServer\wsi\bin\mofcomp.bat

   - In Solaris or Linux:

     /opt/HiCommand/HiCommandServer/wsi/bin/mofcomp

   Example of executing the command:

```
> mofcomp -s http://localhost/interop -SI -o ..\server\jserver\logr
..\server\jserver\mof\WBEMSolutions_CIMXMLCPA.mof
```

6. Start the Device Manager Server.

   Start the Device Manager server as follows:

   - In Windows:

     Select **Start**, **Programs**, **HiCommand**, **Device Manager**, and then **Start Server**.

   - In Solaris or Linux:

     Execute the following command:

     # /opt/HiCommand/suitesrvcntl -start_hdvm

7.4.2 Specifying Two-Way Authentication for Object Operations

This section describes how to set up two-way authentication for object operations. Use HiKeytool for this task.

7.4.2.1 First Setup Procedure Performed in a CIM client

Create a keystore file for the CIM, and export the client authentication file.

For details on creating a keystore file, see section 7.5.1. For details on exporting an authentication file, see section 7.5.2.

7.4.2.2 Setup Procedure Performed in the Device Manager Server

The following describes the procedure for setting up two-way authentication, importing the client authentication file, and exporting the server authentication file.

1. Open a command prompt or terminal window, navigate to `<server installation directory>/HiCommandServer`, and run HiKeytool.
   - For Windows, type **HiKeytool.bat,** and then press the **Enter** key.
   - For Solaris or Linux, type **HiKeytool.sh**, and then press the **Enter** key.
2. The HiKeytool main panel appears (see Figure 7.1). Enter `2`.

   The SMI-S main panel appears as in the example shown below.

```
1) Set Security Level for Object Operations
(Current setting:SSL without two-way authentication)
2) Set Security Level for Event Indications
(Current setting:SSL without two-way authentication)
3) Import Client's Certificate to TrustStore for Object Operations
4) Import Client's Certificate to TrustStore for Event Indications
5) Export Server's Certificate from KeyStore for Object Operations
6) Export Server's Certificate from KeyStore for Event Indications
7) Exit

>
```

3. If `(Current setting:SSL without two-way authentication)` appears at item 1 in the SMI-S main panel, type `1`.

   If `(Current setting:SSL with two-way authentication)` appears in the SMI-S main panel, skip to step `6`.

   When you type `1` in the SMI-S main panel, a submenu appears as in the example shown below.

```
You must stop the Device Manager Server before specifying this setting.
1) SSL without two-way authentication
2) SSL with two-way authentication

>
```

4. Stop the Device Manager server as indicated in the displayed message.

   Stop the Device Manager server as follows:

   – In Windows:

     Select **Start**, **Programs**, **HiCommand**, **Device Manager**, and then **Stop Server**.

   – In Solaris or Linux:

     Execute the following command:

     # /opt/HiCommand/suitesrvcntl -stop_hdvm

5. Type `2` in the submenu.

   The `mofcomp` command is executed and the MOF file is compiled.

   You are returned to the SMI-S main panel when the `mofcomp` command has completed execution.

   Caution: If you type the same number as the current setting, you are immediately returned to the SMI-S main panel.

   Caution: If `mofcomp` command execution fails, the following message appears: `The compilation of the MOF file failed.` In this case, collect all files in the following directory, and then contact maintenance personnel.

   – In Windows:

     installation-folder-for-the-Device-Manager-Server`\HiCommandServer\wsi\server\jserver\mof`

   – In Solaris or Linux:

     `/opt/HiCommand/HiCommandServer/wsi/server/jserver/mof`

6. In the SMI-S main panel, enter `3`.

   This option starts processing to import the client authentication file to the truststore file for object operations.

   Note: The truststore file for object operations (the truststore password is `trustssl`) is stored in the following location:

   – In Windows:

     installation-folder-for-the-Device-Manager-Server`\HiCommandServer\wsi\server\jserver\bin\.truststore`

   – In Solaris or Linux:

     `/opt/HiCommand/HiCommandServer/wsi/server/jserver/bin/.truststore`

7. Enter the alias, the truststore password, and the client authentication file name.

   Enter the client authentication file name by absolute path.

   An input example is shown below.

```
Enter alias:foocorpclient
Enter truststore-password:trustssl
Enter authentication-filename(absolute path):c:\tmp\client.cer
```

   At completion of processing, you are returned to the SMI-S main panel.

8. In the SMI-S main panel, enter `5`.

   This option starts processing to export the server authentication file from the keystore file for object operations.

9. Enter the keystore password, the alias, and the server authentication file name.

   Enter the server authentication file name by absolute path.

   An input example is shown below.

```
Enter keystore-password:serverssl
Enter alias:foocorpserver
Enter authentication-filename(absolute path):c:\tmp\server.cer
```

   At completion of processing, you are returned to the SMI-S main panel.

10. Start the Device Manager server if stopped.

    Start the Device Manager server as follows:

    - In Windows:

      Select **Start**, **Programs**, **HiCommand**, **Device Manager**, and then **Start Server**.

    - In Solaris or Linux:

      Execute the following command:

      # /opt/HiCommand/suitesrvcntl -start_hdvm

7.4.2.3 Second Setup Procedure Performed in a CIM Client

Import the server authentication file for object operation into the truststore file for the CIM client.

For details on creating a truststore file and importing the authentication file, see section 7.5.3.

7.4.3 Procedure for Specifying Two-way Authentication for Event Indications

This section describes how to set up two-way authentication for event indications.

7.4.3.1 First Setup Procedure Performed in a CIM Client

Create a keystore file for the CIM and export the client authentication file.

For details on creating a keystore file, see section 7.5.1. For details on exporting an authentication file, see section 7.5.2.

7.4.3.2 Setup Procedure Performed in the Device Manager Server

The following describes the procedure for creating a keystore file and setting up two-way authentication for event indications, importing the client authentication file, and exporting the server authentication file.

1. Create a new keystore file for the event indication.

   The default keystore file for the event indication (the keystore password is `indssl`) is stored in the following location:

   – In Windows:

     installation-folder-for-the-Device-Manager-Server\HiCommandServer\wsi\server\jserver\bin\.ind.keystore

   – In Solaris or Linux:

     /opt/HiCommand/HiCommandServer/wsi/server/jserver/bin/.ind.keystore

   The default keystore file can be used without any modification. If you want to use the default keystore file, skip to step 6.

   If you want to create a new keystore file, name the file `.ind.keystore` and use it to replace the default keystore file.

   For details on how to create a keystore file, see section 7.5.1.

2. Encrypt the keystore password.

   Use `WSIEncryptString.jar` to encrypt the keystore password that was specified during creation of the keystore file in step 1. `WSIEncryptString.jar` is stored in the following location:

   – In Windows:

     installation-folder-for-the-Device-Manager-Server\HiCommandServer\wsi\no-redist

   – In Solaris or Linux:

     /opt/HiCommand/HiCommandServer/wsi/no-redist/

   Example of executing the command:

   > java -jar WSIEncryptString.jar *keystore-password*

   When the command is executed, the encrypted character string of the keystore password is displayed. This character string is used in a later step.

3. Stop the Device Manager Server.

   Stop the Device Manager server as follows:

   – In Windows:

     Select **Start**, **Programs**, **HiCommand**, **Device Manager**, and then **Stop Server**.

   – In Solaris or Linux:

     Execute the following command:

     # /opt/HiCommand/suitesrvcntl -stop_hdvm

4. Modify the MOF file.

   Specify, in the MOF file, the encrypted keystore password that was obtained in step 2 of this procedure. The MOF file is stored in the following location:

   – In Windows:

     installation-folder-for-the-Device-Manager-Server\HiCommandServer\wsi\server\jserver\mof

   – In Solaris or Linux:

     /opt/HiCommand/HiCommandServer/wsi/server/jserver/mof

   See Figure 7.35 for an example of a MOF file.

5. In the MOF file, change **IndicationAuthenticationEnabled** to **true**. Compile the MOF file.

   Use the `mofcomp` command to compile the file. The `mofcomp` command is stored in the following location:

   – In Windows:

     installation-folder-for-the-Device-Manager-Server\HiCommandServer\wsi\bin\mofcomp.bat

   – In Solaris or Linux:

     /opt/HiCommand/HiCommandServer/wsi/bin/mofcomp

6. Open a command prompt or terminal window, navigate to `<server installation directory>/HiCommandServer`, and run HiKeytool.
   - For Windows, type **HiKeytool.bat,** and then press the **Enter** key.
   - For Solaris or Linux, type **HiKeytool.sh**, and then press the **Enter** key.
7. The HiKeytool main panel appears (see Figure 7.1). Enter `2`.

   The SMI-S main panel appears.

```
1) Set Security Level for Object Operations
(Current setting:SSL without two-way authentication)
2) Set Security Level for Event Indications
(Current setting:SSL without two-way authentication)
3) Import Client's Certificate to TrustStore for Object Operations
4) Import Client's Certificate to TrustStore for Event Indications
5) Export Server's Certificate from KeyStore for Object Operations
6) Export Server's Certificate from KeyStore for Event Indications
7) Exit

>
```

8. If `(Current setting:SSL without two-way authentication)` appears at item `2` in the SMI-S main panel, type `2`.

   If `(Current setting:SSL with two-way authentication)` appears in the SMI-S main panel, skip to step 11.

   When you type `2` in the SMI-S main panel, a submenu appears as in the example shown below.

```
You must stop the Device Manager Server before specifying this setting.
1) SSL without two-way authentication
2) SSL with two-way authentication

>
```

9. Stop the Device Manager server, if running, as indicated in the displayed message.

   Stop the Device Manager server as follows:
   - In Windows:

     Select **Start**, **Programs**, **HiCommand**, **Device Manager**, and then **Stop Server**.
   - In Solaris or Linux:

     Execute the following command:

     # /opt/HiCommand/suitesrvcntl -stop_hdvm

10. Type `2` in the submenu.

    The `mofcomp` command is executed and the MOF file is compiled.

    You are returned to the SMI-S main panel when the `mofcomp` command has completed execution.

    Caution: If you type the same number as the current setting, you are immediately returned to the SMI-S main panel.

    Caution: If `mofcomp` command execution fails, the following message appears: `The compilation of the MOF file failed.` In this case, collect all files in the following directory, and then contact maintenance personnel.

    - In Windows:

      installation-folder-for-the-Device-Manager-Server`\HiCommandServer\wsi\server\jserver\mof`

    - In Solaris or Linux:

      `/opt/HiCommand/HiCommandServer/wsi/server/jserver/mof`

11. In the SMI-S main panel, enter `4`.

    This option starts processing to import the client authentication file to the truststore file for event indications.

    Important: The truststore file for the event indication (the truststore password is `indtrust`) is stored in the following location:

    - In Windows:

      nstallation-folder-for-the-Device-Manager-Server`\HiCommandServer\wsi\server\jserver\bin\.ind.truststore`

    - In Solaris or Linux:

      `/opt/HiCommand/HiCommandServer/wsi/server/jserver/bin/.ind.truststore`

12. Enter the alias, the truststore password, and the client authentication file name.

    Enter the client authentication file name by absolute path.

    An input example is shown below.

```
Enter alias:foocorpindclient
Enter truststore-password:indtrust
Enter authentication-filename(absolute path):c:\tmp\clientind.cer
```

    At completion of processing, you are returned to the SMI-S main panel.

13. In the SMI-S main panel, enter `6`.

    This option starts processing to export the server authentication file from the keystore file for event indications.

14. Enter the keystore password, the alias, and the server authentication file name.

    Enter the server authentication file name by absolute path.

    An input example is shown below.

```
Enter keystore-password:serverindtrust
Enter alias:foocorpindserver
Enter authentication-filename(absolute path):c:\tmp\serverind.cer
```

    At completion of processing, you are returned to the SMI-S main panel.

15. Start the Device Manager server if stopped.
    - In Windows:

      Select **Start**, **Programs**, **HiCommand**, **Device Manager**, and then **Start Server**.
    - In Solaris or Linux:

      Execute the following command:

      # /opt/HiCommand/suitesrvcntl -start_hdvm

7.4.3.3 Second Setup Procedure Performed in a CIM Client

Import the server authentication file for object operation into the truststore file for the CIM client.

For details on creating a truststore file and importing the authentication file, see section 7.5.3.

7.4.4 Procedure for Disabling Two-way Authentication

The procedure for disabling two-way authentication for object operations or event indications is described below. Use HiKeytool for this task.

1. Open a command prompt or terminal window, navigate to

   <*Device-Manager-server-installation-directory*>/HiCommandServer and run HiKeytool.

   - For Windows, type **HiKeytool.bat,** and then press the **Enter** key.
   - For Solaris or Linux, type **HiKeytool.sh**, and then press the **Enter** key.

2. The HiKeytool main panel appears (see Figure 7.1). Enter 2.

   The SMI-S main panel appears as in the example shown below.

```
1) Set Security Level for Object Operations
(Current setting:SSL with two-way authentication)
2) Set Security Level for Event Indications
(Current setting:SSL with two-way authentication)
3) Import Client's Certificate to TrustStore for Object Operations
4) Import Client's Certificate to TrustStore for Event Indications
5) Export Server's Certificate from KeyStore for Object Operations
6) Export Server's Certificate from KeyStore for Event Indications
7) Exit

>
```

3. To disable two-way authentication for object operations, enter 1 in the SMI-S main panel. To disable two-way authentication for event indications, enter 2 in the SMI-S main panel.

   A panel appears as in the example below.

```
You must stop the Device Manager Server before specifying this setting.
1) SSL without two-way authentication
2) SSL with two-way authentication

>
```

4. Stop the Device Manager server as indicated in the displayed message.

   Stop the Device Manager server as follows:

   - In Windows:

     Select **Start**, **Programs**, **HiCommand**, **Device Manager**, and then **Stop Server**.

   - In Solaris or Linux:

     Execute the following command:

     # /opt/HiCommand/suitesrvcntl -stop_hdvm

5. Enter `1`.

   The `mofcomp` command is executed and the MOF file is compiled.

   You are returned to the SMI-S main panel when the `mofcomp` command has completed execution.

   Caution: If you type the same number as the current setting, you are immediately returned to the SMI-S main panel.

   Caution: If `mofcomp` command execution fails, the following message appears: `The compilation of the MOF file failed.` In this case, collect all files in the following directory and contact maintenance personnel.

   – In Windows:

     nstallation-folder-for-the-Device-Manager-Server`\HiCommandServer\wsi\server\jserver\mof`

   – In Solaris or Linux:

     `/opt/HiCommand/HiCommandServer/wsi/server/jserver/mof`

6. Start the Device Manager Server.

   Start the Device Manager server as follows:

   – In Windows:

     Select **Start**, **Programs**, **HiCommand**, **Device Manager**, and then **Start Server**.

   – In Solaris or Linux:

     Execute the following command:

     # /opt/HiCommand/suitesrvcntl -start_hdvm

7.5 Authenticating File Operations Using a Java Tool

This section describes the following operations required for SSL-encrypted communication between the Device Manager server and the CIM client using CIM/WBEM functionality:

- Creating a keystore file
- Exporting authentication files from a keystore file
- Creating a truststore file and importing authentication files

These operations use the Java `keytool` command (equivalent to JDK1.4.0). The `keytool` command is installed in the following location when Device Manager is installed:

In Windows:

installation-folder-for-HiCommand-Suite-Common-Component\jdk\bin\keytool.exe

In Solaris or Linux:

/opt/HiCommand/Base/jdk/bin/keytool

In the `keytool` command, specify the file name, alias, and password for the keystore file or the truststore file. Note the following when specifying these items:

- Do not use the following symbols in the file name:

  : , ; * ? " < > |

- Specify the file name as a character string of no more than 255 bytes.
- Do not include double quotation marks (") in the alias or password.

Note: This section assumes that a path to the `keytool` command has been added to the environment variable `PATH`.

7.5.1 Creating a Keystore File

To create a keystore file:

1. Execute the following command:

```
keytool -genkey -keystore keystore-filename -storepass keystore-password -alias alias -
dname entity-distinguished-name -validity validity-of-certificate -keypass keypass -
keyalg RSA
```

Note: Specify the same password for `-storepass` and `-keypass`.

Example of executing the command:

```
> keytool -genkey -keystore .keystore -storepass sanssl -alias san3gssl -dname
"CN=san3g, OU=SSL, O=hitachi, L=yokohama, S=kanagawa, C=JP" -validity 720 -keypass
sanssl -keyalg RSA
```

2. Check the created keystore file.

   Execute the following command:

   `keytool -list -keystore` *`keystore-filename`* `-storepass` *`keystore-password`*

7.5.2 Exporting an Authentication File from a Keystore File

To expoert an authentication file from a keystore file:

1. Execute the following command:

   keytool -export -keystore keystore-filename -storepass keystore-password -alias alias -file authentication-file-name

2. Check the exported authentication file using the following command:

   keytool -printcert -v -file authentication-file-name

7.5.3 Creating a Truststore File and Importing an Authentication File

To create a truststore file and import the authentication file:

1. Execute the following command:

   keytool -import -alias alias -keystore truststore-filename -storepass truststore-password -trustcacerts -file authentication-filename

2. Check the created keystore file:

   keytool -list -keystore truststore-filename -storepass truststore-password

Chapter 8 HiCommand Device Manager Server Properties

- Overview of HiCommand Device Manager Server Properties (see section 8.1)
- Server Configuration Properties (see section 8.2)
- Database Properties (see section 8.3)
- Logger Properties (see section 8.4)
- Dispatcher Properties (see section 8.5)
- MIME Properties (see section 8.6)
- Client Properties (see section 8.7)
- Security Properties (see section 8.8)
- SNMP Trap Log Output Function Properties (see section 8.9)
- Launchable Applications Properties (see section 8.10)
- Mainframe Host Agent Properties (see section 8.11)
- Report Function Properties(see section 8.12)
- Restrictions on Web Clients Connected to the Device Manager Server (see section 8.13)

8.1 Overview of HiCommand Device Manager Server Properties

In Windows systems, the default directory for the configuration definition file is:

```
c:\Program Files\DeviceManager\HiCommandServer\config
```

In Solaris or Linux systems, the default directory for the configuration definition file is:

```
/opt/HiCommand/HiCommandServer/config
```

Important: If you make a change to any property file, that change will not take effect until the server is rebooted. If you make changes to any server properties, you will need to restart the Device Manager Agent.

- Server properties include web configuration properties and performance properties (see section 8.2). Web configuration properties include the IP address and port of the HTTP listener(s), the location of the server's document directory, and the name of the default index page. They also include performance-tuning properties, such as the size of input/output buffers, various TCP/IP stack and socket settings, server file-cache parameters, connection thread priorities, and properties related to the email notification function.

  WARNING: You should not undertake the task of optimizing these attributes unless you are an expert, because even minor changes could severely impact the performance of the Device Manager Server.

- Database properties (see section 8.3) include DBMS parameters, such as drivers and logon ID.

  WARNING: You should not undertake the task of optimizing these attributes unless you are an expert, since minor changes could severely impact the performance of the Device Manager Server.

- Logger properties (see section 8.3.2) include directives that configure Device Manager Server's logging module, including the names, locations and verbosity level of operational and error logging of the various log files.

- Dispatcher properties (see section 8.5) include properties that allow the fine-tuning of various background processes (daemons) and the optimization of the thread-priority for service agents.

- MIME properties (see section 8.6) include the translation/lookup table for all Multipurpose Internet Mail Extensions (MIME) file types recognized by the Device Manager Server.

- Client properties (see section 8.7) include properties that configure the Device Manager Web Client.

- Server security properties (see section 8.8) include whether secure-socket encryption is being utilized, the location and passwords for the Server Certificate TrustStore, a list of permitted client IP addresses, and properties that support the hardening of the Device Manager Server against certain kinds of denial-of-service attacks.

- SNMP trap *log output function* properties (see section 8.9) include whether to enable Device Manager to use the SNMP trap function and whether to customize the trap list.

- Launchable application properties (see section 8.10) include the necessary information for launching related applications.
- Mainframe Host Agent Properties (see section 8.11) include the settings for communication between the Device Manager server and mainframe hosts.

These files are in Java property file format, and except for the security properties file can be modified using any text editor. Each property directive consists of a name-value pair separated by the equal sign (for example, foo.bar=12345). The appropriate end-of-line terminator, as defined by the operating system, delineates individual properties.

Comments in Device Manager property files are tagged using the "#" character at the start of a line. Literals (text strings or numeric values) do not need to be quoted. Boolean values can be either true or false (case-insensitive). Any other setting (for example, yes) is interpreted as false.

The backslash is a reserved character in Java property files, and is used for escaping various control characters such as tabs, line-feeds, etc. On Windows platforms absolute pathnames typically contain backslash characters, and must be backslash-escaped, for example, the file pathname c:\HiCommand\docroot\foo.bar should be entered as c:\\HiCommand\\docroot\\foo.bar. There is generally no need to backslash-escape any other characters in the property directives.

WARNING: As a general rule, server properties should not need to be modified. Use extreme caution when you are modifying the configuration properties, because you can cause the server to fail or to function incorrectly. Do not modify server properties unless you have sufficient expertise to understand the potential consequences of your actions.

Table 8.1 summarizes the various Device Manager property files.

Table 8.1 Summary of Device Manager Property Files

Property	Description	Location
Server Configuration Properties	**These files relate to server performance properties, including the size of input/output buffers, various TCP/IP stack and socket settings, server file-cache parameters, and connection thread priorities.**	**Section 8.2**
server.http.host	Designates either the host name or the dotted-decimal IP address for the Device Manager web server.	Section 8.2.1
server.http.port	Assigns the port used for the Device Manager HTTP server.	Section 8.2.2
server.https.port	Assigns the port used for the Device Manager secure HTTP server.	Section 8.2.3
server.http.default	Sets the name of the default index page for the Device Manager web server.	Section 8.2.4
server.http.request.timeout	Sets the read-blocking timeout of the HTTP socket connection.	Section 8.2.5
server.http.connection.priority	Sets the priority for all client-connection threads spawned by HTTP requests made against the Device Manager Server.	Section 8.2.6
server.http.connection.bufSize	Sets the size (in bytes) for the server's input/output (I/O) buffers.	Section 8.2.7

Property	Description	Location
server.http.socket.backlog	Assigns the maximum queue length for incoming connection indications.	Section 8.2.8
server.http.socket.maxThreads	Sets the maximum number of concurrent connections accepted by the Device Manager Server.	Section 8.2.9
server.http.socket.linger	Toggles whether the SO_LINGER socket attribute is enabled for client connections with the Device Manager Server.	Section 8.2.10
server.http.socket.noDelay	Toggles whether the TCP_NODELAY socket attribute is enabled for connections to the Device Manager Server.	Section 8.2.11
server.http.headers.maxNumber	Sets the maximum number of HTTP headers permitted for any request submitted to the Device Manager web server.	Section 8.2.12
server.http.headers.maxLength	Sets the maximum length permitted for any HTTP header.	Section 8.2.13
server.http.entity.maxLength	Sets the maximum length of an HTTP request entity.	Section 8.2.14
server.http.log.reverseDNS	Flags whether the Device Manager Server performs reverse-DNS (Domain Name Server) lookup for its access logging.	Section 8.2.15
server.http.cache.size	Sets the upper-limit size of the Device Manager Server's internal file cache.	Section 8.2.16
server.http.cache.maxFileSize	Sets the maximum file size for server-side caching.	Section 8.2.17
server.http.fileTypes.noLog	Contains a comma-delimited list of the file types that are not logged in the Device Manager Server's access log when being transferred via HTTP.	Section 8.2.18
server.http.mode	This property sets whether the server is running in real mode or simulation mode.	Section 8.2.19
server.installTime	This property contains the install date of Device Manager.	Section 8.2.20
server.base.home	This property contains the installation directory of the Common Component.	Section 8.2.21
server.horcmconfigfile.hostname	This property allows you to specify whether to use the host name (hostname) or the IP address (ipaddress) when Device Manager edits the configuration definition file.	Section 8.2.22
server.base.initialsynchro	This property allows you to specify whether to synchronize the management information database and the displayed information (HiCommand Suite Common Repository) when you start Device Manager.	Section 8.2.23
server.cim.support	Determines whether CIM support is enabled.	Section 8.2.24
server.cim.support.protocol	Specifies whether to open or close the ports used by the CIM function.	Section 8.2.25
server.cim.http.port	Specifies the port for non- SSL transmission, for the CIM function.	Section 8.2.26
server.cim.https.port	Specifies the port for CIM SSL transmission.	Section 8.2.27
server.configchange.enabled	Determines whether to enable the automatic refresh function.	Section 8.2.28
server.configchange.autorefresh.lastrefreshed	Specifies whether to update the time of the last refresh, during automatic refreshing.	section 8.2.29
server.mail.enabled	Determines whether to enable the email notification function.	section 8.2.30

Property	Description	Location
server.mail.from	Changes the email sender's name when using the email notification function.	section 8.2.31
server.mail.smtp.host	Specifies the host name or IP address of the SMTP server to be accessed when an email is sent by the email notification function.	section 8.2.32
server.mail.smtp.port	Specifies the port number of the SMTP server to be accessed when an email is sent by the email notification function.	section 8.2.33
server.mail.smtp.auth	Specifies whether to use SMTP authentication when an email is sent by the email notification function.	section 8.2.34
server.mail.alert.type	Specifies the type of alerts to be reported by the email notification function.	section 8.2.35
server.mail.alert.status	Specifies the severity of alerts to be reported by the email notification function.	section 8.2.36
Database Properties	**These files contain the set of directives that pertain to establishing a connection with the Device Manager Server's database.**	**Section 8.3**
dbm.traceSQL	Designates whether output SQL to trace.log or not	Section 8.3.1
dbm.startingCheck.retryCount	Specifies the number of times the Device Manager Server retries the checking whether DBMS has started.	Section 8.3.2
dbm.startingCheck.retryPeriod	Specifies the interval (in seconds) at which the Device Manager Server retries the checking whether DBMS has started.	Section 8.3.3
Logger Properties	**These files contain a set of directives that configure Device Manager Server's logging module, including the names, locations and verbosity level of operational and error logging of the various log files.**	**Section 8.4**
logger.loglevel	Determines the verbosity level of operational (trace) and error logging.	Section 8.4.1
logger.MaxBackupIndex	Sets the number of rolling backups to keep of each log file before the oldest is erased.	Section 8.4.2
logger.MaxFileSize	Allows you to specify the maximum size for each log file.	Section 8.4.3
logger.hicommandbase.loglevel	Determines the verbosity level of operational (trace) and error logging which writes into HDvMtrace1.log by the Common Component	Section 8.4.4
logger.hicommandbase.sysloglevel	This property determines the verbosity level of operational (trace) and error logging which writes into the EventLog (for Windows) or the syslog (In Solaris or Linux systems) by the Common Component.	Section 8.4.5
logger.hicommandbase.MaxBackup Index	This property sets the number of rolling backups to keep of HDvMtrace1 log file before the oldest is deleted.	Section 8.4.6
logger.hicommandbase.MaxFileSize	This property sets the number of rolling backups to keep of HDvMtrace1 log file before the oldest is deleted.	Section 8.4.7
Dispatcher properties	**These files contain a set of configurable directives pertaining to the operation of Device Manager Server's dispatcher layer, including properties that allow the fine-tuning of various background processes (daemons) and the optimization of the thread-priority for service agents.**	**Section 8.5**

Property	Description	Location
server.dispatcher.agent.priority	Assigns the priority for Device Manager service agent threads.	Section 8.5.1
server.dispatcher.message.timeout	Sets the timeout for pending response messages before they are expired (purged).	Section 8.5.2
server.dispatcher.message.timeout.in.processing	Sets the timeout for processing messages (in minutes) that are not completed by some reason.	Section 8.5.3
server.dispatcher.daemon.pollingPeriod	Defines the polling interval for the background agents responsible for checking component status and configuration version.	Section 8.5.4
server.dispatcher.traps.purgePeriod	Defines the purging interval for stale SNMP traps or alerts.	Section 8.5.5
server.dispatcher.startTimeOfIgnoring ConnectionAlert	Defines the start time of the interval for stopping SNMP communication alert.	Section 8.5.6
server.dispatcher.endTimeOfIgnoring ConnectionAlert	Defines the end time of the interval for stopping SNMP communication alert.	Section 8.5.7
server.dispatcher.daemon.receiveTrap	Determines whether or not port 162 is used as an SNMP trap.	Section 8.5.8
MIME Properties	**These files contain the translation/lookup table for all Multipurpose Internet Mail Extensions (MIME) file types recognized by the Device Manager web server.**	**Section 8.6**
Client Properties	**These files affect the configuration of Device Manager Web Client.**	**Section 8.7**
client.logger.trace	Defines whether or not to output trace log information.	Section 8.7.1
client.message.timeout	Defines the maximum wait time for the Device Manager Server response (timeout of connection) in seconds.	Section 8.7.2
client.outputhorcmfunction.enabled	Specifies whether to enable Web Client to use CCI to create a configuration definition file.	Section 8.7.3
table.ldev.rowsperpage	Specifies the values displayed in the drop-down list used for setting the number of lines displayed per page on a window using a Web Client sortable table.	Section 8.7.4
client.assignlun.upperlimit.enabled	Enables you to make the upper limit check enabled or disabled for the number of LUNs that are assigned when storage is added.	Section 8.7.5
client.report.csv.format.escaped	Enables you to switch the format of the CSV report for information of the storages and users that are managed by Device Manager.	Section 8.7.6
Security Properties	**These files include whether secure-socket encryption is being utilized, the location and passwords for the Server Certificate TrustStore, and a list of permitted client IP addresses. This group also contains a number of properties that support the hardening of the Device Manager Server.** ***WARNING:*** **Do not use a text editor to change these properties. See Chapter 7 for more information on modifying security properties.**	**Section 8.8**
server.http.secure	Sets the security level of the Device Manager Server.	Section 8.8.1
server.http.security.realm	Sets the security realm message for the Device Manager Server's authentication challenge.	Section 8.8.2
server.http.security.clientIP	Implements an IP address filter.	Section 8.8.3

Property	Description	Location
server.https.security.keystore	Assigns the name of the Keystore file that contains a Server Certificate used for establishing an encrypted communication via Secure Sockets Layer (SSL) and Transport Layer Security (TLS).	Section 8.8.4
server.https.keystore.passphrase	Contains the logon password for the Keystore file that contains a keypair and associated Server Certificate used for SSL/TLS connections.	Section 8.8.5
server.https.keystore.keypass	Contains the password for recovering the keypair and associated Server Certificate used for encrypting SSL/TLS connections from the Device Manager Server's Keystore.	Section 8.8.6
server.http.security.unprotected	Designates a comma-delimited list of any non-protected file resources under the server's document root.	Section 8.8.7
server.https.security.truststore	Assigns the name and location of the truststore file that contains the Server Certificates.	Section 8.8.8
server.https.truststore.passphrase	Contains the password used to access the default truststore distributed with the Java Runtime Environment.	Section 8.8.9
SNMP Trap log output function properties	**These files include whether to allow Device Manager to use SNMP traps, and whether the trap list will be customized.**	**Section 8.9**
customizedsnmptrap.customized SNMPTrapEnable	This property allows you to enable the SNMP trap log output function.	Section 8.9.2
customizedsnmptrap.customizelist	This property allows you to specify how to customize the SNMP trap log output.	Section 8.9.3
Link and Launch Properties	**These properties include server information about applications that can be launched from the GUI.**	**Section 8.10**
launchapp.damp.url	This property specifies a URL for accessing the DAMP installation directory from a client web browser.	Section 8.10.1
Mainframe host agent properties	These properties include settings for communication between the Device Manager server and mainframe hosts.	Section 8.11
host.mf.agent.connection.timeout	Specifies the timeout for communication processing with a host agent.	Section 8.11.1

8.2 Server Configuration Properties

The server configuration properties are contained in the server.properties file. This is normally located in the HiCommandServer/config directory, under the installation directory.

The default directory for the configuration properties on Windows systems is:

```
c:\Program Files\Device Manager\HiCommand\HiCommandServer\config
```

The default directory for the configuration properties on Solaris or Linux systems is:

```
/opt/HiCommand/HiCommandServer/config
```

8.2.1 server.http.host

This property specifies either the host name or dotted-decimal IP address for the host that operates the web server functionality of Device Manager:

- If you specify a host name, make sure to use a value that a DNS can resolve on the Web Client, CLI, and the subsystem.
- If you specify an IP address, specify a value to which Web Client, CLI, and the subsystem can connect.
- In a cluster environment, specify the IP address of the cluster manager.
- When multiple NICs (Network Interface Cards) are installed on the server, specify an IP address corresponding to an NIC to which Web Client, CLI, and the subsystem can connect.

Default: localhost

8.2.2 server.http.port

This property assigns the port used for the Device Manager HTTP (web) server. The conventional port number used for a standard web server is 80, but there may already be an Intranet server running on this port. Moreover, you should avoid low-numbered ports because these could conflict with other services installed on the server. As a general rule, you can pick any port between 1024 and 49151.

Caution: Use 80 for the port number when this property is set to a space character.

Default: 2001

8.2.3 server.https.port

This property assigns the port used for the Device Manager secure HTTP web server. The conventional port number for a secure web server is 443, but there may already be a secure Intranet server running on this port. As noted above, it is better practice to utilize a port number between 1024 and 49151 for a specialized (middleware) HTTP server. Make sure that it has a different value than the port designated for the HTTP listener.

Default: 2443

8.2.4 server.http.default

This property sets the name of the default index page for the Device Manager web server. If an HTTP request is made against a directory (for example, https://hic.domain.com:2443/foo/, where foo is a folder under the server's document root), the web server attempts to find and transfer the named file to the client. If none exists, a directory listing is returned to the client browser. Under normal conditions, you should not need to change the default value of this property.

Default: index.html

8.2.5 server.http.request.timeout

This property sets the read-blocking timeout of the HTTP socket connection (in milliseconds). It can be used to enable or disable the SO_TIMEOUT setting for client-connection sockets. Reading from the input stream associated with a socket will block for only this amount of time before the socket expires. Its default value is 5000 (5 seconds). A value of zero is interpreted as an infinite timeout, meaning that SO_TIMEOUT is disabled for client connections. You should only modify this property if you are an expert System Administrator seeking to fine-tune the server's performance.

Default: 5000 (5 seconds)

8.2.6 server.http.connection.priority

This property sets the priority for all client-connection threads spawned by HTTP requests made against the Device Manager Server. Valid values are between 1 and 10 (1 = minimum priority; 5 = normal priority; 10 = maximum priority). You should only modify this property if you are an expert System Administrator seeking to fine-tune the server's performance. Recommended values are between 5 and 8.

Note: If the connection thread priority is set to 10 (maximum), any simultaneous request connections are queued for sequential processing, which defeats the purpose of a multi-threaded server. This setting would actually adversely affect server performance, particularly when you are loading complex HTML pages (for example, those containing many images).

Default: 7

8.2.7 server.http.connection.bufSize

This property sets the size (in bytes) for all of the server's input/output (I/O) buffers. Increased buffer size may improve request/response network performance for high-volume connections, while decreasing it can help reduce the backlog of incoming data. Do not set the default value smaller than 1024 bytes, or it can cause failure. You should only modify this property if you are an expert System Administrator seeking to fine-tune the server's performance.

Default: 8192 bytes

8.2.8 server.http.socket.backlog

This property assigns the maximum queue length for incoming connection indications (a request to connect), such as setting the SO_MAX_CONN attribute of the server socket. If a connection indication arrives when the queue is already full, the Device Manager Server will refuse the new connection. You should only modify this property if you are an expert System Administrator seeking to fine-tune the server's performance.

Default: 50

8.2.9 server.http.socket.maxThreads

When a request has been issued and is being processed on the Device Manager Server, a client has an active connection on the server. This property specifies the number of active requests that can be processed at one time on Device Manager Server, not the maximum number of clients. Once this limit is reached, the next request will be dropped. You should only modify this property if you are an expert System Administrator seeking to fine-tune the server's performance.

Default: 50

8.2.10 server.http.socket.linger

This Boolean property toggles whether the SO_LINGER socket attribute is enabled for client connections with the Device Manager Server. Setting this flag to its default value means a linger-On-close timeout of 60 seconds is applied to socket connections. You should only modify this property if you are an expert System Administrator seeking to fine-tune the server's performance.

Default: true

8.2.11 server.http.socket.noDelay

This Boolean property toggles whether the TCP_NODELAY socket attribute is enabled for connections to the Device Manager Server. Setting this flag at its default value disables the Nagle algorithm for TCP/IP packets. You should only modify this property if you are an expert System Administrator seeking to fine-tune the server's performance.

Default: true

8.2.12 server.http.headers.maxNumber

This property sets the maximum number of HTTP headers permitted for any request submitted to the Device Manager web server, and helps prevent certain types of denial of service and attempted buffer overflow attacks by restricting the effect of malicious requests containing a large number of headers. You should not need to change this setting under normal circumstances. The Device Manager Server silently ignores any HTTP headers in excess of this number. Runtime errors are not automatically generated under such circumstances.

Default: 20

8.2.13 server.http.headers.maxLength

This property sets the maximum length permitted for any HTTP header (in bytes). You should not need to change this setting under normal circumstances. It helps prevent certain types of denial of service and attempted buffer-overflow attacks by restricting the effect of malicious requests that contain unusually large header fields. Headers longer than the specified length will be truncated by the Device Manager Server without automatically generating runtime errors.

Default: 1024

8.2.14 server.http.entity.maxLength

This property sets the maximum length of an HTTP request entity (in bytes). You should not need to change this setting under normal circumstances. It helps prevent certain types of denial of service and attempted buffer overflow attacks by restricting the effect of malicious requests that contain unusually large payload entities. If the server detects a posted request longer than this value, it sends an error response to the client and logs details of the attempted request.

Default: 131072

8.2.15 server.http.log.reverseDNS

This Boolean property flags whether the Device Manager Server performs reverse-DNS (Domain Name Server) lookup for its access logging. When set, this property the server attempts to resolve the name of a client from the IP address for incoming connections. If the client's IP address can be resolved, the domain name is also written into the server's access log (for example, http://www.hds.com/193.36.36.6). Not all IP addresses on the Internet have an assigned domain name, so some logged requests might still be recorded as a numeric IP address, even with this flag turned on.

Note: While translation of the IP address to a domain name can assist analysis of the server's access logs, reverse-DNS lookups are expensive in terms of resources, and this feature may significantly degrade the server's performance, especially on a slow network. You should keep the setting at the default value for better performance.

Default: false

8.2.16 server.http.cache.size

This property sets the upper-limit size of the Device Manager Server's internal file cache (in bytes). A value of zero turns file caching off, which may adversely affect server performance when delivering complex static files (HTML pages containing images, etc).

This setting could be increased on a host machine with sufficient RAM installed. However, since the number of static files being served by Device Manager is only in the order of a few pages, performance gains would most likely be quite trivial.

Default: 10000000 bytes

8.2.17 server.http.cache.maxFileSize

This property sets the maximum file size for server-side caching. Static files larger than this limit (for example, the GUI application JAR file) are read from disk instead of being cached. There is no significant difference in response time whether these files are cached in memory or read directly from disk. A zero value for this property turns file caching off, which may adversely affect the web server's performance.

Default: 100000 bytes

8.2.18 server.http.fileTypes.noLog

This property contains a comma-delimited list of the file types that are not logged in the Device Manager Server's access log when being transferred via HTTP. Generally, logging should be performed only for the HTML pages being requested by a browser or other client, or the server's access log quickly becomes filled with entries for files such as graphics files, JavaScript, or cascading style sheets.

The default value for this property eliminates logging for the majority of the resource-type files likely to be requested from the Device Manager web server. White space in the list is ignored. If you want access logging for all files, set this property to empty.

Default: gif,jpg,jpeg,png,css,js

8.2.19 server.http.mode

This property sets whether the server is running in real mode or simulation mode. This property is only used for development of the application that is connected to Device Manager. You should not change this property for normal operation.

Default: real

8.2.20 server.installTime

This property contains the Device Manager installation date.

Format: dd/mm/yyyy:HH:MM:SS ZZZZ (dd:day, mm:month, yyyy:year, HH:hour, MM:minute, SS:second ZZZZ (TimeZone).

Default: dd/mm/yyyy:HH:MM:SS ZZZZ (Install date).

8.2.21 server.base.home

This property contains the installation directory of the Common Component, which is set by the Device Manager installer. You should not change this property under normal circumstances.

Default: (Value set by the installer)

8.2.22 server.horcmconfigfile.hostname

This property allows you to specify whether to use the host name (hostname) or the IP address (ipaddress) when Device Manager edits the configuration definition file.

Caution: Deleting a host name or an IP address that was specified when a copy pair was created disables operations on the copy pair. In such a case, refresh the subsystem information.

Default: ipaddress

8.2.23 server.base.initialsynchro

This property allows you to specify whether to synchronize the management information database and the displayed information (HiCommand Suite Common Repository) when you start Device Manager. A setting of true will synchronize the information. A setting of false will not synchronize the information.

Caution: If this property is set to **true**, synchronization of the information will take several minutes. If you change the property and then log in to Device Manager right away, an error may occur. If that occurs, wait until the synchronization is finished, and then log in.

Default: false

8.2.24 server.cim.support

This property determines whether CIM support is enabled. If you want to use a VDS service provider or execute CIM, you must set this property to **true**.

The installer sets this property to **true** if you enable the CIM/WBEM features for the SMI-S Provider service setting during installation.

Default: false

8.2.25 server.cim.support.protocol

This property sets whether to open or close the ports used by the CIM function. A value of `1` to `3` can be specified. When `1` is specified, the port for non-SSL transmission is opened and the port for SSL transmission is closed. When `2` is specified, the port for non-SSL transmission is closed and the port for SSL transmission is opened. When `3` is specified, both ports are opened.

If you decide not to use SSL when Device Manager is newly installed, `1` is set. If you select to use SSL, `3` is set.

Default: 3

8.2.26 server.cim.http.port

This property specifies the port for non- SSL transmission for the CIM function. If the SSL of the CIM function is disabled, `HITACHI_ObjectManager.Name` (a property of the CIM function) is set as this port.

For details on the `HITACHI_ObjectManager.Name` property, see the manual *HiCommand Device Manager CIM/WBEM User's Guide*.

Default: `5988`

8.2.27 server.cim.https.port

This property specifies **HITACHI_ObjectManager.Name** as the port for the CIM function if SSL is enabled. For more information, see Hitachi Device Manager

Default: 5989

8.2.28 server.configchange.enabled

This property determines whether to enable the automatic refresh function. This function automatically performs a refresh when the Device Manager Server detects that the system configuration has been changed by the launched subsystem management tool (Storage Navigator or Storage Navigator Modular (for Web)). To enable this function, set this property to true.

Default: `true`

8.2.29 server.configchange.autorefresh.lastrefreshed

This property specifies whether the time of the last update is to be updated during an automatic refresh. (The time of the last refresh is always updated during a manual refresh, but this is an optional setting for an automatic refresh.) To specify that the time of the last update is to be updated during an automatic refresh, set this property to `true`.

Default: `true`

8.2.30 server.mail.enabled

This property determines whether to report an alert that has occurred in a storage subsystem to the user by email. To enable the email notification function, set this property to `true`.

Default: `true`

8.2.31 server.mail.from

This property changes the mail address of the notification source (sender). If no value is specified or the specified value is invalid, the default value is set.

Default: `hdvmserver`

8.2.32 server.mail.smtp.host

This property specifies the host name or IP address of the SMTP server to be accessed when an email is sent by the email notification function of the Device Manager server. You must specify this property.

Caution: If you do not specify this property, the email notification function will not be enabled even if you specify `true` for the `server.mail.enabled` property.

Default: None

8.2.33 server.mail.smtp.port

This property specifies the port number of the SMTP server to be accessed when an email is sent by the email notification function of the Device Manager server. You must specify this property.

Specifiable range: `0` to `65535`.

Default: `25`

8.2.34 server.mail.smtp.auth

This property specifies whether to use SMTP authentication when an email is sent by the email notification function of the Device Manager server. To use SMTP authentication, set this property to `true`. To not use SMTP authentication, set this property to `false`. Specifying this property is optional.

Default: `false`

8.2.35 server.mail.alert.type

This property specifies the type of alerts to be reported by the email notification function of the Device Manager server. The following values can be specified:

`Trap`: Reports only SNMP trap alerts.

`Server`: Reports only the alerts detected by the background threads responsible for checking component status and the configuration version.

`All`: Reports both SNMP trap alerts and the alerts detected by the background threads responsible for checking component status and the configuration version.

Note: If `All` is set, alerts are reported from both SNMP and the server even if these alerts refer to the same error information.

Default: `Trap`

8.2.36 server.mail.alert.status

This property specifies the severity of alerts to be reported by the email notification function of the Device Manager server. The Device Manager server reports alerts whose severity is higher than the severity specified for this property. The following values (listed in ascending order of importance) can be specified:

`Normal`, `Service`, `Moderate`, `Serious`, `Acute`

Default: `Moderate`

8.3 Database Properties

Database properties are contained in the database.properties file.

The database properties configuration file contains the set of directives that pertain to establishing a connection with the Device Manager Server's database. Before the Device Manager Server will run you need to correctly enter these settings and start the Database Management System (DBMS). If the server cannot connect to its DBMS, an entry is written to the error log (the default location is in the logs directory). This information can help considerably when you are troubleshooting a new installation.

This file also holds debugging and optimization property settings for the Java Database Connectivity (JDBC) layer in Device Manager Server. You should only modify these properties if you need detailed diagnostic information or if you are an expert System Administrator seeking to fine-tune certain aspects of performance and/or memory utilization.

The default directory for the Windows database properties file is:

c:\Program Files\DeviceManager\HiCommandServer\config

The default directory for Solaris or Linux logger properties file is:

/opt/HiCommand/HiCommandServer/config

8.3.1 dbm.traceSQL

This property designates whether the output to trace.log is SQL. Set true to output to SQL. Set false not to output SQL.

Default: false

8.3.2 dbm.startingCheck.retryCount

This property specifies the number of times the Device Manager Server will retry whether DMBS has started when the server is launched. The specifiable value ranges form 0 to 100. As a general rule, you do not need to change this setting.

Default: 18

8.3.3 dbm.startingCheck.retryPeriod

This property specifies the interval (in seconds) the Device Manager Server will retry whether DMBS has started when the server is launched. The specifiable value ranges form 0 to 100. As a general rule, you do not need to change this setting.

Default: 10 seconds

8.4 Logger Properties

Logger properties are contained in the logger.properties file.

This properties file contains a set of directives that configure Device Manager Server's logging module, including the names, locations and verbosity level of operational and error logging of the various log files. You can also use this file to configure trace logging for debugging and diagnostic purposes. The applicable file names are access.log, error.log, service.log, and trace.log.

The default directory for the Windows logger properties file is:

```
c:\Program Files\HiCommand\DeviceManager\HiCommandServer\config
```

The Windows event log is located in the event viewer.

The default directory for Solaris or Linux logger properties file is:

```
/opt/HiCommand/HiCommandServer/config
```

The default syslog is specified in `/etc/syslog.conf`

8.4.1 logger.loglevel

This property determines the verbosity level of operational (trace) and error logging. The values accepted in this field are (in decreasing order of detail): DEBUG, INFO, WARN, ERROR, and FATAL. The default logging level for production systems is INFO, which means that debugging or informational entries as well as warnings and error messages are written into the trace and error logs.

Default: INFO

8.4.2 logger.MaxBackupIndex

This property sets the number of rolling backups to keep of each log file before the oldest is deleted. If this property is set to zero, no rolling backups are created, and log files are simply truncated when their maximum file size is reached. When a log file reaches its maximum length its filename is modified by appending a counter, for example, access.log.1. As more backup log files are created, their counter or version suffix is incremented (for example, access.log.1 becomes access.log.2), until the specified number of rolling backups have been created. After that, the oldest backup log file is deleted each time a new backup is created. You can specify a range of 1 to 20.

Default: 10

8.4.3 logger.MaxFileSize

This property allows you to specify the maximum size for each log file. Unless KB is specified for kilobytes or MB for megabytes, bytes is assumed. In this property, the term KB is interpreted as 1024 bytes, and MB as 1024 kilobytes.

Specifiable range: from 512 KB to 32 MB

Default: 1 MB

8.4.4 logger.hicommandbase.loglevel

This property determines the verbosity level of operational (trace) and error logging which writes into HDvMtrace1.log by the Common Component. Each logging event has its own importance level independent from its type (error, warning, and information). The levels, in increasing order of importance, are: 30, 20, 10, and 0. The default logging level for production systems is 20, which means that messages for logging event levels 20, 10, and 0 are written into the HDvMtrace1.log, but messages for logging event level 30 are not.

Default: 20

8.4.5 logger.hicommandbase.sysloglevel

This property determines the verbosity level of operational (trace) and error logging which writes into the EventLog (Windows) or the syslog (Solaris or Linux) by the Common Component. Each logging event has its own importance level independent from its type (error, warning, and information). The levels, in increasing order of importance, are: 30, 20, 10 and 0. The default logging level for production systems is 0, which means that messages for only the logging event leveled 0 are written into the EventLog (Windows) or the syslog (Solaris or Linux), but messages for the logging event leveled 30, 20, and 10 are not. The default value is recommended.

Default: 0

8.4.6 logger.hicommandbase.MaxBackupIndex

This property sets the maximum number of files to keep of the HDvMtrace1 log file before the oldest is deleted. Valid values are between 1 and 16. When a log file reaches its maximum length, its filename is modified by increasing a counter (e.g., for example, HDvMtrace2). As more backup log files are created, their counter or version suffix is incremented (e.g., HDvMtrace2.log becomes HDvMtrace3.log), until the specified number of rolling backups have been created. After that, the oldest backup log file is deleted each time a new backup is created.

Default: 10

8.4.7 logger.hicommandbase.MaxFileSize

This property sets the maximum size of each of the rolling backup Device Manager trace log files. The specified size is assumed to be in bytes unless you specify kB for kilobytes, MB for megabytes or GB for gigabytes. Valid values are between 4096 and 2147483647. Even if this directive is not found in the properties file, an internal default value of 1 MB will be used.

Default: 1 MB

8.5 Dispatcher Properties

Dispatcher properties are contained in the dispatcher.properties file.

This properties file contains a set of configurable directives pertaining to the operation of Device Manager Server's dispatcher layer, including properties that allow the fine-tuning of various background processes (daemons) and the optimization of the thread-priority for service agents.

The default directory for the Windows dispatcher properties file is:

```
c:\Program Files\HiCommand\DeviceManager\HiCommandServer\config
```

The default directory for Solaris or Linux logger properties file is:

```
/opt/HiCommand/HiCommandServer/config
```

8.5.1 server.dispatcher.agent.priority

This property assigns the priority for Device Manager Agent threads. Valid values are between 1 and 10 (1 = minimum priority; 5 = normal priority; 10 = maximum priority). You should change the default value only if you need to fine-tune the agent dispatcher's performance. The recommended values are between 5 and 8, and you should not set it to the maximum thread priority (9-10), because while that may cause individual requests to execute faster, it is likely to cause an overall degradation in performance when multiple users are sending concurrent requests.

Default: 5

8.5.2 server.dispatcher.message.timeout

This property sets the timeout for pending response messages (in minutes) before they are expired (purged). A pending message consists of a response from a long-running process (for example, discovery of a storage array) that has not yet been either polled by the client or sent to the client via the Device Manager notification service.

Default: 15 minutes

8.5.3 server.dispatcher.message.timeout.in.processing

This property sets the timeout for processing messages (in minutes) that are not completed by some reason.

Default: 720 minutes

8.5.4 server.dispatcher.daemon.pollingPeriod

This property defines the polling interval (in minutes) for the background agents responsible for checking component status and configuration version. A value of zero will disable these polling agents.

Default: 5 minutes

8.5.5 server.dispatcher.traps.purgePeriod

This property defines the purging interval for stale SNMP traps or alerts (in minutes). A value of zero will disable the purging of traps from the server.

Default: 5 minutes

8.5.6 server.dispatcher.startTimeOfIgnoringConnectionAlert

This property defines the start time of the interval for stopping SNMP communication alert. Accessing the subsystem that is in regular reboot will incur this alert.

Default: 2:45

8.5.7 server.dispatcher.endTimeOfIgnoringConnectionAlert

This property defines the end time of the interval for stopping SNMP communication alert. If you access a subsystem that is in regular reboot, that will cause this alert.

Default: 3:15

8.5.8 server.dispatcher.daemon.receiveTrap

This property determines whether or not port 162 is used as an SNMP Trap listener. Device Manager can use SNMP to detect command completion and hardware issues. If port 162 is in use, Device Manager can use polling to determine these issues, but using SNMP is preferred.

If the SNMP trap is set, then Device Manager Server is started and port 162 is in use, the server will output an error message and stop. During installation, the SNMP Trap Note panel is displayed to warn the user of this potential outcome.

The default value of this property is **true**, which enables the SNMP Trap reception function. If you set this property to **false**, the function is disabled. If you choose to disable the function during a new installation, the installer automatically sets this property to **false**.

Default: True

8.6 MIME Properties

MIME properties are contained in the mime.properties file.

This file contains the translation/lookup table for all Multipurpose Internet Mail Extensions (MIME) file types recognized by the Device Manager web server. Each property in this lookup table maps a particular extension suffix to the MIME type for that file. You should not need to modify this setting under normal circumstances, and in any event only expert System Administrators should make any additions to this file.

The default directory for the Windows MIME properties file is:

```
c:\Program Files\HiCommand\DeviceManager\HiCommandServer\config
```

The default directory for Solaris or Linux logger properties file is:

```
/opt/HiCommand/HiCommandServer/config
```

8.7 Client Properties

Client properties are contained in the client.properties file. This properties file contains the configuration information for the Device Manager Web Client.

In Windows, the default directory for the client properties file is as follows:

c:\Program Files\HiCommand\DeviceManager\HiCommandServer\config

In Solaris or Linux, the default directory for the client properties file is as follows:

/opt/HiCommand/HiCommandServer/config

8.7.1 client.logger.trace

This property defines whether output the trace information or not by applying Java Web Start's log output function. Set this property to true to output trace information. Set this property to false to not output trace information.

Note: In order to output trace information, Java Web Start's log output function must be activated. See *HiCommand Device Manager Web Client User's Guide* for more information about the Java Web Start log output function.

Default: false

8.7.2 client.message.timeout

This property defines the maximum wait time for the Device Manager Server response (timeout of connection) in seconds. Web Client sends the notification messages to the server, and the server sends the notification of the task complete or the alert in response. The connection between the client and the server is on while waiting the response of the notification from the server. This property sets the timeout of this waiting time. The client sends the notification message again after the timeout. This timeout will be applied each time Web Client accesses the server.

Note: When the client is accessing the server through a proxy server and the connection timeout of the proxy is shorter than the timeout of this property, the notification message may be lost, because the timeout of the proxy server cuts the connection before the Device Manager Server can send the response to the Web Client. If this is the case, please set the timeout for this property to a time shorter than the timeout of the proxy.

Default: 300 seconds

8.7.3 client.outputhorcmfunction.enabled

This property enables Web Client to use CCI to create a configuration definition file. Set this property to true to enable the use of this function.

Before changing this property, stop HBase Storage Mgmt Common Service. After changing this property, restart HBase Storage Mgmt Common Service. For details about how to start and stop HBase Storage Mgmt Common Service, see section 5.2.

Default: false

8.7.4 table.ldev.rowsperpage

Specifies the values displayed in the drop-down list used for setting the number of lines displayed per page on a window using a Web Client sortable table. The values set by this property appear in a Web Client drop-down list. Up to two choices for the number of lines can be included in the drop-down list. To set two choices, specify the two values separated by a comma. The minimum number of lines that can be specified is `1`. The maximum number of lines that can be specified depends on the environment, such as the web browser the client uses and the CPU performance and memory capacity of the client machine. The maximum number of lines (standard) for each web browser is as follows:

- Internet Explorer 6.0: 1000
- Mozilla 1.4: 2000
- Mozilla 1.7: 300

If you specify a value larger than the maximum value (standard), a warning dialog box may appear indicating that the machine may be unable to respond. If this occurs, decrease the value of the property and restart HBase Storage Mgmt Common Service. For details about how to start and stop HBase Storage Mgmt Common Service, see section 5.2.

8.7.5 client.assignlun.upperlimit.enabled

This property enables you to make the upper limit check enabled or disabled for the number of LUNs that are assigned when storage is added.

When *LUN assignment*, which is a step of the storage addition function, is performed in a state where many volume paths have already been determined, HBase Storage Mgmt Common Service might stop running. This problem occurs when the size of the memory required to keep the display information for *LUN assignment* and the log output information exceeds the upper limit of the JAVA heap size for HBase Storage Mgmt Common Service. Therefore, to prevent HBase Storage Mgmt Common Service from stopping, set and check the upper limit for the number of LUNs that can be assigned in a single operation. The upper limit of the number of LUNs, which is used for the check, is 100. To enable the check, specify `true`, and to disable the check, specify `false`.

Before changing this property, stop HBase Storage Mgmt Common Service. After changing this property, restart HBase Storage Mgmt Common Service. For details about how to start and stop HBase Storage Mgmt Common Service, see section 5.2.

Default: `true`

8.7.6 client.report.csv.format.escaped

This property enables you to switch the format of the CSV report for information of the storages and users that are managed by Device Manager. If this property is set to `true`, each value is output enclosed by double quotation marks ("). For details on the report function, see the *HiCommand Device Manager Web Client User's Guide*.

Default: `true`

8.8 Security Properties

Server security properties are contained in the server.properties and security.properties files. These files include whether secure-socket encryption is being utilized, the location and passwords for the Server Certificate TrustStore, and a list of permitted client IP addresses. This group also contains a number of properties that support the hardening of the Device Manager Server.

In Windows or Linux, the default directory for the security properties file is as follows:

```
c:\Program Files\HiCommand\DeviceManager\HiCommandServer\config
```

In Solaris, the default directory for the security properties file is as follows:

```
/opt/HiCommand/HiCommandServer/config
```

WARNING: Do not use a text editor to edit these properties. See Chapter 7 for more information on changing security properties.

8.8.1 server.http.secure

This property sets the security level of the Device Manager Server. See section 7.2.2 for instructions on how to use HiKeytool to set the security level, as follows:

- 0 = Unsecure. Any client application can obtain access to the server. No logon authentication is required from the client. This setting is intended for use only on highly secure LANs and/or private networks, and even in those environments more robust server security is highly recommended.
- 1 = Basic Authentication. The Device Manager Server is operating in protected mode, and client applications attempting to connect with the server must submit an authorized user's logon ID and password and be authenticated against the Access Control List (ACL).

  Note: These requirements do not apply to requests for files that are intentionally designated as being excluded from ACL security protection (see the server.http.security.unprotected property in section 8.8.7).
- 2 = Secure Socket (TLS/SSL). In this security mode, the server opens an additional secure HTTP listener on a port designated by the server.https.port property. All communications via this port are strongly encrypted using Secure Socket Layer (SSL) or Transport Layer Security (TLS). Refer to Chapter 7 for further information on SSL and TLS. In order for a server to use the secure HTTP protocol, a keypair and associated Server Certificate must be present in the Device Manager Server Keystore. This setting is strongly recommended if a Device Manager Server is exposed to any public network or Internet.

  Default: 1

8.8.2 server.http.security.realm

This property sets the security realm message for the Device Manager Server's authentication challenge. This text is usually displayed in a browser's logon dialog.

Default: `Device Manager Security`

8.8.3 server.http.security.clientIP

This property implements an IP address filter, which helps harden a server against malicious attacks. The default value is *.*.*.* which means that an HTTP connection from any client IP address will be accepted. You can restrict the Device Manager Server access to designated clients and/or to subnets such as a Local Area Network (LAN) or Wide Area Network (WAN), by using asterisks as a wildcard character. For example, a Device Manager Server would only accept connections from the host machine itself and other client users on a LAN if this directive was set as:

server.http.security.clientIP=127.0.0.1,192.168.*.*

White space (the space following the comma delimiter) is ignored, as are any invalid dotted-decimal IP entries, so that no runtime error is raised if an invalid or incorrectly formatted network address is detected in this list.

Client machines that are not on the access list will be denied access to the server, however access from the Web Client cannot be restricted. No HTTP response message (stating a reason for the failure to establish a connection) will be returned to the intruder, in order to reduce vulnerability to certain denial of service attacks that attempt to overload a server by flooding it with a large number of simultaneous (bogus) requests.

Caution: You do not need to specify the IP address (the local loop-back address) of a machine on which the Device Manager server is installed. In this property, it is assumed that the Device Manager server can always be connected to the local loop-back address.

Caution: If the version of the Device Manager server is version 3.0 or later, you must also register the IP addresses to the environment definition file **httpsd.conf** for HiCommand Suite Common Component. For details, see section 8.13.

Default: *.*.*.*

8.8.4 server.https.security.keystore

This property assigns the name of the Keystore file that contains the keypair and associated Server Certificate used for establishing an encrypted communication via Secure Sockets Layer(SSL) or Transport Layer Security. The default setting is keystore.

The Keystore file shipped with a Device Manager Server is an empty placeholder file that does not contain the required keypair and associated Server Certificate needed to run the Device Manager Server in secure mode. If you attempt to start the server in secure mode with an empty Keystore file, the server will log a fatal exception and fail. A keypair and associated self-signed or trusted certificate must first be installed into the Keystore before encrypted communications can be started. see section 7.2.3 for more information about Server Certificates.

Default: keystore

8.8.5 server.https.keystore.passphrase

This property contains the logon password for the Keystore file that contains a keypair and associated Server Certificate used for SSL/TLS connections. The logon password is used to check the integrity of the Keystore data. See section 7.2.6 for instructions on using HiKeytool to change the password.

Default: passphrase

8.8.6 server.https.keystore.keypass

This file contains the password for recovering the keypair and associated Server Certificate used for encrypting SSL/TLS connections from the Device Manager Server's Keystore (refer also to the server.https.security.keystore property in section 8.8.4). See section 7.2.7 for instructions on how to use HiKeytool to change the Keystore password.

Default: passphrase

8.8.7 server.http.security.unprotected

This property designates a comma-delimited list of any non-protected file resources under the server's document root. When files or directories are designated as unprotected, they are not subject to Access Control List checks (user authentication), regardless of the security mode setting for the server. Entire directories (including nested sub-directories) can be flagged as unprotected by using an asterisk as a wildcard character. If this directive is empty all resources are protected, so that every request to the Device Manager Server will require user authentication.

This property allows anyone to view the index.html front page via a browser, without user authentication being required. More importantly, it allows the Java Web Start application to update its JAR file and deploy (via the HiCommand.jnlp file) to the end-user's system without raising a series of logon dialogs. Similarly, the GUI's help files (and certain client installation information) can be viewed via a web browser without separate authentication being required at each step. The default should not require modification under normal circumstances.

Default: index.html, HiCommand/*, webstart/*, images/*, style/*, docs/*, favicon/ico

8.8.8 server.https.security.truststore

This property assigns the name and location of the truststore file that contains the Server Certificates. The Device Manager Server uses the default truststore distributed with the JRE named "cacerts".

Note: This property cannot be modified with HiKeytool. If you want to change the value, you must do so by editing the value in the server.properties file.

Default: **{java.home}/lib/security/cacerts**

8.8.9 server.https.truststore.passphrase

This property contains the password used to access the default truststore distributed with the Java Runtime Environment. For instructions on how to use HiKeytool to change the truststore password, see section 7.2.10.

Default: changeit.

8.9 SNMP Trap Log Output Function Properties

SNMP trap log output function properties are contained in the customizedsnmptrap.properties file.

In Windows, the default directory for the SNMP trap log output function properties file is:

```
C:\Program Files\HiCommand\DeviceManager\HiCommandServer\config
```

In Solaris or Linux, the default directory for the SNMP trap log output function properties file is:

```
/opt/HiCommand/HiCommandServer/config
```

Device Manager can be configured to output the SNMP Traps as a log file, which allows you to centrally monitor devices within a storage area and applications.

The SNMP trap log has the following features:

- A log message contains information about the events related to a trap and the information that can identify where those events occurred.
- The trap to be logged is not limited to the trap related to storage devices. The traps related to the desired devices and applications can be output to logs uniformly.
- Each element of the acquired SNMP Trap is output to the log output message. The items to be output and their order can be customized.

The scope of the log output is as follows:

- Notification of an error or command completion (Universal Storage Platform V, TagmaStore USP, Lightning 9900V, and Lightning 9900 only)
- Other SNMP traps (Universal Storage Platform V, TagmaStore USP, Lightning 9900V, and Lightning 9900 only)
- SNMP traps for other devices (SNMP version 1 trap only)

The log message outputs the following information:

- Message ID indicating that a trap was received
- Sender (agent)
- Enterprise ID (enterprise)
- Generic trap number (generic)
- Specific trap number (specific)

Log messages are output to the following destinations:

- The output destinations for HiCommand Suite Common Component log messages (for details, see section 5.4):
  - Device Manager trace log file
  - HiCommand Suite common trace log file
  - Event log / syslog file
- The output destinations for log messages related to system startup processes:
  - Trace log file
  - Error log file#

  # This file is output only when the severity is Error, Critical, or Alert. For details on the severity, see Table 8.2.

8.9.1 Log output customization

By setting the `customizedsnmptrap.customizedSNMPTrapEnable` property to true, the SNMP Trap information can be output to log messages. You can customize the output information in the `customizedsnmptrap.customizelist` property. A customization definition for output log consists of five items separated by colons. You can omit some items, but may not omit the colon delimiter. To specify more than one customization definition, use a comma as a delimiter, but make sure not to enter a comma at the end of the last entry. To change the line in the middle of a customization list, enter a back slash (\) at the end of that line. The line feed following the back slash (\) is ignored.

The following shows the definition for log customization:

```
customizedsnmptrap.customizelist = \
enterprise-ID-1:generic-trap-number-1:specific-trap-number-1:severity-1:message-1, \
enterprise-ID-2:generic-trap-number-2:specific-trap-number-2:severity-2:message-2, \
...
enterprise-ID-n:generic-trap-number-n:specific-trap-number-n:severity-n:message-n
```

The following table lists and describes the format of each item used during customization definition.

Table 8.2 Format of Each Item Used for Customization Definition

Item	Format	Remarks
Enterprise ID	Specify by using a dot (e.g., .1.3.6.1.4.116.3.11.1.2)	Required
Generic trap number	Numeric value, from 0 to 6	Required
Specific trap number	Numeric value	Required
Severity	Information: -I WARNING: -W Error: -E Critical:-E Alert: -E Null: no output	Not required. When this is omitted, Null is used.

Item	Format	Remarks
Message	Use the following character strings (variable) to specify message information to be output: $a Agent address (dotted decimal format) $e Enterprise ID (dotted format) $g Generic trap number $s Specific trap number $n (where n indicates an integer, which is 1 or larger): The value of the nth variable is binding	Not required. When this is omitted, aegs is used.

The following shows an example of a customized log configuration:

```
customizedsnmptrap.customizelist = \
.1.2.3:6:1:Information:$a$e$g$s$1$2, \
.1.3.6.1.4.1.2854:6:1:Warning:$e$a$s$3$2$1$g, \
.1.3.6.1.4.1.116.3.11.4.1.1:6:1:ERROR:$a$s, \
.1.3.6.1.4.1.116.3.11.4.1.1:6:100:Information:$a$s
```

Figure 8.1 Sample Log Customization (1)

8.9.2 customizedsnmptrap.customizedSNMPTrapEnable

This property allows you to enable the SNMP trap log output function. Specify true to use the log output function, or false to not to use the function.

Default: false

8.9.3 customizedsnmptrap.customizelist

This property allows you to specify how to customize the SNMP trap log output. See section 8.9.1 for details.

Default: None

8.10 Launchable Applications Properties

This file contains information on launchable applications.

This properties file contains information for the server that contains the applications that can be launched.

In Windows, the default directory for the launchable application properties file is as follows:

c:\Program Files\HiCommand\DeviceManager\HiCommandServer\config

In Solaris, the default directory for the launchable application properties file is as follows:

/opt/HiCommand/HiCommandServer/config

8.10.1 Launchapp.damp.url

This property specifies the URL of the web server for Storage Navigator Modular (for Web) or Damp (for Web) to be launched from the web browser in a client.

Note: Even if this was previously set in the previous version, you must re-set it. If you change the value, restart the server and then refresh the subsystems.

The following shows an example of specifying the URL of the web server for Storage Navigator Modular (for Web):

launchapp.damp.url=http://192.168.17.235:23015/program/DeviceManager/snm

Important: Setting up alias information is necessary in order to use Storage Navigator Modular (for Web). For details on setting the environment information in one operation, see section 9.1.2.

The following shows an example of specifying the URL of the web server for DAMP (for Web):

launchapp.damp.url=http://192.168.17.235:23015/program/DeviceManager/damp

Important: Setting up alias information is necessary in order to use DAMP (for Web). For details on setting the environment information in one operation, see section 9.2.2

Default: Not applicable

8.10.2 launchapp.snm.rmi.port

When you have changed the port number used for RMI communication in Storage Navigator Modular (for Web), you need to specify the new port number in this property. If you do not do this, Device Manager cannot link with Storage Navigator Modular (for Web). Valid values are from 1 to 65535.

If you have not changed the port number used for communication, do not specify this property. For details on how to view and change the port number used for communication that is specified in Storage Navigator Modular (for Web), see the *Storage Navigator Modular (for Web) User's Guide*.

Default: None

8.11 Mainframe Host Agent Properties

Properties of the mainframe host agent are contained in the `host.properties` file.

This properties file contains settings for communication between the Device Manager server and mainframe hosts.

In Windows, the default directory for the mainframe host agent properties file is:

```
C:\Program Files\HiCommand\DeviceManager\HiCommandServer\config
```

In Solaris or Linux, the default directory for the mainframe host agent properties file is:

```
/opt/HiCommand/HiCommandServer/config
```

8.11.1 host.mf.agent.connection.timeout

This property specifies the timeout (in seconds) for communication processing between the Device Manager server and a mainframe host agent. Valid values are `0` and from `30` to `3600`. If you specify `0`, no timeout applies. You should only modify this property if you are an expert System Administrator seeking to fine-tune performance of the mainframe host agent.

Default: `300`

8.12 Report Function Properties

Report function properties are contained in the `DvMReport.properties` file.

In Windows, the default directory for the report function properties file is:

```
C:\Program Files\HiCommand\DeviceManager\HiCommandServer\config
```

In Solaris or Linux, the default directory for the report function properties file is:

```
/opt/HiCommand/HiCommandServer/config
```

8.12.1 DetailedArrayReport.outputPath

This property specifies the storage location of the CSV file that is generated from the Detailed Array Reports window in Web Client.

Important: The value specified for the storage location of the CSV file is enabled when the Detailed Array Reports - Reports subwindow is first displayed on Web Client after the Device Manager server service is restarted.

Default: *Device-Manager-server-installation-directory*`/DvMReport/CSV`

8.13 Restrictions on Web Clients Connected to the Device Manager Server

If the version of the Device Manager server is version 3.0 or later, restrict Web Clients that can connect to the Device Manager server by performing the following procedure. If the version is earlier than 3.0, perform only step 4 to restrict the Web Clients.

To restrict Web Clients that can connect to the Device Manager server:

1. If HiCommand Suite products whose versions are earlier than 5.7 are installed, stop their services.

   For details about how to stop these services, see the manual for your product version.

2. Stop the HiCommand Suite product services and HiCommand Suite Common Component.
   - For Windows, select **Start**, **Program**, **HiCommand**, **Device Manager**, and then **Stop Server with Common Services**.
   - For Solaris or Linux, execute the following command:

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

3. Open the `httpsd.conf` file, located in the following directory:
   - For Windows:

```
Installation-folder-for-HiCommand-Suite-Common-
Component\httpsd\conf\httpsd.conf
```

   - For Solaris or Linux:

     `/opt/HiCommand/Base/httpsd/conf/httpsd.conf`

4. Register hosts that can be connected to the Device Manager Server in the last line of the `httpsd.conf` file.

   The following shows the format for registering hosts in the `httpsd.conf` file:

```
<Location /DeviceManager>
        order allow,deny
        allow from host [host....]
</Location>
```

   Figure 8.2 Format for Registering Hosts in the `httpsd.conf` File

   Hosts can be written in the following formats:
   - The domain name (***example:*** `hitachi.datasystem.com`)
   - Part of the domain name (***example:*** `hitachi`)
   - The whole IP address (***example:*** `10.1.2.3 127.0.0.1`)
   - Part of the IP address (***example:*** `10.1` which, in this case, means `10.1.0.0/16`)
   - Network/Netmask format (dot notation) (***example:*** `10.1.0.0/255.255.0.0`)
   - Network/*n* (CIDR notation: *n* is the number of bits for identifying a network) (***example:*** `10.1.0.0/16`)

   If you want to specify two or more hosts in a command line for `allow from`, delimit the hosts with a space.

Multiple lines can be used to specify hosts for `allow from`.

If you attempt to connect from a machine which has Device Manager installed, you must also specify the local loop-back address (`127.0.0.1` or `localhost`).

Be sure to specify `order` in accordance with the specified format. If extra spaces or tabs are inserted, the operation will fail.

The following shows an example of registering hosts in the `httpsd.conf` file:

```
<Location /DeviceManager>
        order allow,deny
        allow from 127.0.0.1 10.0.0.1
        allow from 10.0.0.0/26
</Location>
```

Figure 8.3 Example of Registering Hosts to the `httpsd.conf` File

5. Register hosts to the `server.http.security.clientIP` property. For details on how to set the `server.http.security.clientIP` property, see section 8.8.3
6. Restart the HiCommand Suite product services and HiCommand Suite Common Component.
   - For Windows, select **Start-Programs-HiCommand-Device Manager-Start Server**.
   - For Solaris or Linux, execute the following command:

     ```
     # /opt/HiCommand/Base/bin/hcmdssrv -start
     ```
7. If HiCommand Suite products whose versions are earlier than 5.7 is installed, restart their services as required.

   For details about how to start these services, see the manual for your product version.

Caution: If you log on to a HiCommand Suite product from a host that is not registered in the `httpsd.conf` file, the Device Manager server cannot be started from that HiCommand Suite product.

Chapter 9 Linking Device Manager With Other Products

This chapter describes the settings for linking Device Manager with related products.

- Linking With Storage Navigator Modular (for Web) (see section 9.1)
- Linking With DAMP (for Web) (see section 9.2)
- Starting HSSM From the Dashboard (see section 9.3)

9.1 Linking With Storage Navigator Modular (for Web)

This section describes prerequisites and environment setup for linking with Storage Navigator Modular (for Web).

Caution: The Linux version does not support linkage with Storage Navigator Modular (for Web).

9.1.1 Prerequisites for Using Storage Navigator Modular (for Web)

The prerequisites for using Storage Navigator Modular (for Web) are as follows:

- For details about the environment setup required for operating Storage Navigator Modular (for Web), see the *Storage Navigator Modular (for Web) User's Guide*.
- Install Storage Navigator Modular (for Web) on the machine where the Device Manager server is installed.
- To use Storage Navigator Modular (for Web), you must set up a web server to run it.
- Use HiCommand Suite Common Component for the web server that runs Storage Navigator Modular (for Web). HiCommand Suite Component is installed during installation of the HiCommand Device Manager server.
- Storage Navigator Modular (for Web) cannot be used together with DAMP (for Web).
- Multiple Storage Navigator Modular (for Web) clients cannot concurrently access the same storage subsystem.

Caution: The web server for Storage Navigator Modular (for Web) can be accessed via only one NIC even if multiple NICs are installed on the machine. To link with Storage Navigator Modular (for Web) in a machine environment where multiple NICs are installed, you need to specify the NIC to be used to access the web server for Storage Navigator Modular (for Web). The IP address specified for this setting must be the same as that specified during installation of the Device Manager server. For details on how to specify the settings, see the *Storage Navigator Modular (for Web) User's Guide*.

Caution: To link with Storage Navigator Modular (for Web) in a cluster environment, the host you specify for accessing the web server of Storage Navigator Modular must be identical to the logical host name you specified when installing the Device Manager server. For details on setting the host name, see the Storage Navigator Modular (for Web) User's Guide.

9.1.2 Setting the Launch Environment for Storage Navigator Modular (for Web)

Set the launch environment for Storage Navigator Modular (for Web) using the simple setup tool `launchapptool`.

The following conditions apply when setting the launch environment:

- The `launchapp.properties` file and `httpsd.conf` file must exist in the installation folder and must be write-enabled.
- HiRDB must be running.

Note: For details on the `launchapp.properties` file, see section 8.10.

Note: The `httpsd.conf` file is stored in the following location:

- In Windows:

  installation-folder-for-HiCommand-Suite-Common-Component`\httpsd\conf`

- In Solaris:

  `/opt/HiCommand/Base/httpsd/conf`

Note: For details on how to check the HiRDB operating status and start the HiRDB service, see section 5.3.1.

To specify the launch environment settings for Storage Navigator Modular (for Web):

1. Install Storage Navigator Modular (for Web).

   For details on how to install Storage Navigator Modular (for Web), see the *Storage Navigator Modular (for Web) User's Guide*.

2. Execute the following command from the command prompt or terminal window:
   - In Windows:

     installation-folder-for-the-Device-Manager-server`\HiCommandServer\tools\launchapptool.bat`

     The following shows an example of executing the command:

     ```
     C:\Program Files\HiCommand\DeviceManager\HiCommandServer\tools\launchapptool.bat
     ```

   - In Solaris:

     ```
     # /opt/HiCommand/HiCommandServer/tools/launchapptool.sh
     ```

3. The main menu appears. Select **1**.

```
================================================================================
launchapptool
================================================================================

1) Storage Navigator Modular (for Web) launch setup
2) Disk Array Management Program (for Web) launch setup
3) Delete launch settings
4) Exit

>1

Launch Settings for Storage Navigator Modular (for Web) will now Start.
```

4. If the launch environment settings for Storage Navigator Modular (for Web) have already been specified, a confirmation message asks if you want to change the current settings. Select **y** to change the settings, or **n** to leave the settings unchanged.

5. Specify the protocol to be used in the web server URL. Select **1** to use http protocol, or **2** to use https protocol.

```
Specify the URL protocol.
 1) http
 2) https
    Caution: To use https, settings to enable SSL communication
             with the web server must be specified in advance.

Enter Value [default=1]
>1
```

Caution: For option **2,** the web server must be set up for SSL communication.

6. Enter the IP address or host name to be used in the web server's URL.

   Specify an IP address or host name that can be accessed from the client machine on which the Web Client program is running.

```
Specify the IP address or hostname of the web server.
Enter Value [default=10.208.64.134]
>10.208.64.134
```

Note: To use a local host, specify its IP address rather than the host name.

7. Enter the port number to be used in the web server's URL.

```
Specify the port number of the web server.
Enter Value [default=23015]
>23015
```

8. If you changed the port number for RMI communication in Storage Navigator Modular (for Web), enter the new port number.

```
Specify the port number for RMI communications.
Enter Value [default=1099]
>1099
```

Caution: Do not enter anything if you did not change the communication port number.

9. Enter the installation directory of Storage Navigator Modular (for Web).

```
Specify the installation directory path name of Storage Navigator Modular (for Web).
    Caution: Make sure that the specified installation directory
             path name ends with a forward slash (/).
    Caution: Replace backslashes (\) with forward slashes (/)
             in the specified installation directory path name.

Enter Value [default=C:/Program Files/Storage Navigator Modular Web/]
>D:/Storage Navigator Modular Web/
```

Caution: Make sure that the path ends with a forward slash (/).

Caution: In Windows, replace \ with / in the path name.

```
Example: "C:/Program Files/Storage Navigator Modular Web/"
```

10. Restart the Device Manager server and HiCommand Suite Common Component.

    The changes to the launch environment settings now apply.

```
Launch setup has successfully completed.

You must restart the Device Manager Server and Common Component Services
for this these changes to take effect.

Exit - Default is n?(y, n):
```

11. Check whether Storage Navigator Modular (for Web) runs on HiCommand Suite Common Component.

    Specify the following URL in the browser, and then make sure that the Storage Navigator Modular (for Web) window appears.

```
http://host-name-or-IP-address:portID/program/DeviceManager/snm/default.htm
```

12. Refresh the storage subsystems to be operated on by Storage Navigator Modular (for Web).

    Note: If you set up the launch environment by using the simple setup tool, the URL associated with Storage Navigator Modular (for Web) is set as alias information in HiCommand Suite Common Component. This alias information remains if you subsequently uninstall Device Manager or Storage Navigator Modular (for Web). To delete the alias information and other launch settings, see section 9.1.3.

Table 9.1 launchapptool Input Example (When Setting Storage Navigator Modular (for Web))

```
1) Storage Navigator Modular (for Web) launch setup
2) Disk Array Management Program (for Web) launch setup
3) Delete launch settings
4) Exit

>1

Launch Settings for Storage Navigator Modular (for Web) will now Start.

Specify the URL protocol.
 1) http
 2) https
    Caution: To use https, settings to enable SSL communication
             with the web server must be specified in advance.

Enter Value [default=1]
>1

Specify the IP address or hostname of the web server.
Enter Value [default=10.208.64.134]
>10.208.64.134

Specify the port number of the web sever.
Enter Value [default=23015]
>23015

Specify the port number for RMI communications.
Enter Value [default=1099]
>1099

Specify the installation directory path name of Storage Navigator Modular (for Web).
    Caution: Make sure that the specified installation directory
             path name ends with a forward slash (/).
    Caution: Replace backslashes (\) with forward slashes (/)
             in the specified installation directory path name.

Enter Value [default=C:/Program Files/Storage Navigator Modular Web/]
>D:/Storage Navigator Modular Web/

Launch setup has successfully completed.

You must restart the Device Manager Server and Common Component Services for this
these changes to take effect.

Exit - Default is n?(y, n):
```

9.1.3 Deleting Launch Settings

Delete the launch environment settings by using the simple setup tool `launchapptool`.

You can delete the launch settings if the `launchapp.properties` file and `httpsd.conf` file reside in the installation folder and are write-enabled.

Note: For details on the `launchapp.properties` file, see section 8.10.

Note: The `httpsd.conf` file is stored in the following location:

- In Windows:

  installation-folder-for-HiCommand-Suite-Common-Component`\httpsd\conf`

- In Solaris or Linux:

  `/opt/HiCommand/Base/httpsd/conf`

1. To delete the launch environment settings, execute the following command from the command prompt or terminal window:
   - In Windows:

     installation-folder-for-the-Device-Manager-server`\HiCommandServer\tools\launchapptool.bat`

     The following shows an example of executing the command:

     ```
     C:\Program
     Files\HiCommand\DeviceManager\HiCommandServer\tools\launchappto
     ol.bat
     ```

   - In Solaris or Linux:

     ```
     # /opt/HiCommand/HiCommandServer/tools/launchapptool.sh
     ```

2. The main menu appears. Select **3**.

   A deletion confirmation message appears.

```
================================================================================
launchapptool
================================================================================

1) Storage Navigator Modular (for Web) launch setup
2) Disk Array Management Program (for Web) launch setup
3) Delete launch settings
4) Exit

>3

Launch settings will now be deleted.

Would you like to delete launch settings?(y, n):y
```

3. Select **y** if you are sure you want to delete the launch environment settings; select **n** to cancel deletion.
4. Restart the Device Manager server and HiCommand Suite Common Component.

   The launch environment settings are now deleted.

```
Launch settings have successfully been deleted.

You must restart the Device Manager Server and Common Component Services
for this these changes to take effect.

Exit - Default is n?(y, n):
```

9.1.4 Accessing a Storage Subsystem with Password Protection or Account Authentication Enabled

For storage subsystems whose Password Protection or Account Authentication is enabled, do not use a user ID that starts with "HDvM".

When Password Protection or Account Authentication is enabled, if you launch the Storage Navigator Modular (for Web), the system creates a temporary user account for the Storage Navigator Modular (for Web) to access the storage subsystem. This user account is automatically registered into the system with a user ID that starts with "HDvM", and automatically deleted after you exit the Storage Navigator Modular (for Web). Therefore, manual registration of a user account that starts with "HDvM" or making changes of the registration details might cause the launch to fail.

For details on Account Authentication, see *Hitachi TagmaStore(R) Adaptable Modular Storage and Workgroup Modular Storage Account Authentication User's Guide*.

9.2 Linking With DAMP (for Web)

This section describes prerequisites and environment setup for linking with DAMP (for Web). This section also describes storage subsystem information to be registered into DAMP (for Web).

Caution: The Linux version does not support linkage with DAMP (for Web).

9.2.1 Prerequisites for Using DAMP (for Web)

The prerequisites for using DAMP (for Web) are as follows:

- To perform DAMP launching, the DAMP (for Web) version must be 10.00 or later.
- For details on the environment requirements for running DAMP (for Web), see the *Disk Array Management Program 2 (for Web) User's Guide* or *Disk Array Management Program 3 (for Web) User's Guide*.
- Install DAMP (for Web) on the machine where the HiCommand Device Manager server is installed.
- To use DAMP (for Web), the settings for the web server for running DAMP (for Web) are required.
- Use HiCommand Suite Common Component for a web server for running DAMP (for Web). HiCommand Suite Common Component is installed during installation of the Device Manager server.
- DAMP (for Web) cannot be used together with Storage Navigator Modular (for Web), and cannot be used while the TagmaStore AMS/WMS series is in use.

Caution: The web server for DAMP (for Web) can be accessed via only one NIC even if multiple NICs are installed on the machine. To link with DAMP (for Web) in a machine environment where multiple NICs are installed, you need to specify the NIC to be used to access the web server for DAMP (for Web). The IP address specified for this setting must be the same as that specified during installation of the Device Manager server. For details on how to specify the settings, see the *Disk Array Management Program 2 (for Web) User's Guide* or *Disk Array Management Program 3 (for Web) User's Guide*.

Caution: To link with DAMP (for Web) in a cluster environment, the host you specify for accessing DAMP's web server must be identical to the logical host name you specified when installing the Device Manager server. For details on setting the host name, see the *Disk Array Management Program 2 (for Web) User's Guide* or *Disk Array Management Program 3 (for Web) User's Guide*.

Caution: When the Password Protection functionality is enabled on Thunder 9200 or Thunder 9500V Series, DAMP (for Web) operations launched from Physical View, Web Client operations#, or CLI operations#, might fail. The following are ways to avoid this problem:

- Change the application you use from DAMP (for Web) to Storage Navigator Modular (for Web).
- Use DAMP (for Web) by directly connecting to it from the browser.

  When you connect to DAMP (for Web), you must use a user ID different from the one you used when you registered Thunder 9200 or Thunder 9500V in Device Manager.

  In this case, you cannot perform DAMP (for Web) operations and operations for Web Client or CLI# at the same time for the same storage subsystem (Thunder 9200 or Thunder 9500V). This however is the normal situation when the Password Protection functionality is enabled.
- Stop the polling of the Device Manager server, and try not to perform DAMP (for Web) operations and operations for Web Client or CLI# at the same time for the same storage subsystem (Thunder 9200 or Thunder 9500V).

To stop the polling of the Device Manager server:

1. Specify `0` for `server.dispatcher.daemon.pollingPeriod property` in the `dispatcher.properties` file. For details about the `server.dispatcher.daemon.pollingPeriod` property, see section 8.5.4.
2. To enable the property settings, restart the Device Manager server.

   This operation disables the alert detection performed by polling. However, for the following storage subsystems, you can use alert detection by using the SNMP trap:

   - Universal Storage Platform V
   - TagmaStore USP
   - Lightning 9900V Series
   - Lightning 9900 Series

#: Includes such operations as changing the configuration of, or refreshing the storage subsystem, by using Web Client or CLI.

9.2.2 Setting the Launch Environment When Using DAMP (for Web)

Set the launch environment for DAMP (for Web) using the simple setup tool `launchapptool`.

The following conditions apply when setting the launch environment:

- The `launchapp.properties` file and `httpsd.conf` file must exist in the installation folder and must be write-enabled.
- HiRDB must be running.

Note: For details on the `launchapp.properties` file , see section 8.10.

Note: The `httpsd.conf` file is stored in the following location:

- In Windows:

  installation-folder-for-HiCommand-Suite-Common-Component\httpsd\conf

- In Solaris:

  /opt/HiCommand/Base/httpsd/conf

Note: For details on how to check the HiRDB operating status and start the HiRDB service, see section 5.2.1.

To specify launch environment settings for DAMP (for Web):

1. Install DAMP (for Web).

   For details on how to install DAMP (for Web), see the *Disk Array Management Program 2 (for Web) User's Guide* or *Disk Array Management Program 3 (for Web) User's Guide*.

2. Execute the following command from the command prompt or terminal window:

   – In Windows:

     installation-folder-for-the-Device-Manager-server\HiCommandServer\tools\launchapptool.bat

     The following shows an example of executing the command:

     ```
     C:\Program
     Files\HiCommand\DeviceManager\HiCommandServer\tools\launchappto
     ol.bat
     ```

   – In Solaris:

     ```
     # /opt/HiCommand/HiCommandServer/tools/launchapptool.sh
     ```

3. The main menu appears. Select **2**.

```
================================================================================
launchapptool
================================================================================

1) Storage Navigator Modular (for Web) launch setup
2) Disk Array Management Program (for Web) launch setup
3) Delete launch settings
4) Exit

>3

Launch settings will now be deleted.

Would you like to delete launch settings?(y, n):y
```

4. If launch environment settings already exist for DAMP (for Web), a confirmation message asks if you want to change the current settings. Select **y** to change the settings, or **n** to leave the settings unchanged.

5. Specify the protocol to be used in the web server URL. Select **1** to use http protocol, or **2** to use https protocol.

```
Specify the URL protocol.
 1) http
 2) https
    Caution: To use https, settings to enable SSL communication
             with the web server must be specified in advance.

Enter Value [default=1]
>1
```

Caution: For option **2,** the web server must be set up for SSL communication.

6. Enter the IP address or host name to be used in the web server's URL.

   Specify an IP address or host name that can be accessed from the client machine on which the Web Client program is running.

```
Specify the IP address or hostname of the web server.
Enter Value [default=10.208.64.134]
>10.208.64.134
```

Note: To use a local host, specify its IP address rather than the host name.

7. Enter the port number to be used in the web server's URL.

```
Specify the port number of the web server.
Enter Value [default=23015]
>23015
```

8. Enter the installation directory of DAMP (for Web).

```
Specify the installation directory path name of Disk Array Management Program (for
Web).
    Caution: Make sure that the specified installation directory
             path name ends with a forward slash (/).
    Caution: Replace backslashes (\) with forward slashes (/)
             in the specified installation directory path name.

Enter Value [default=C:/Program Files/DA Manager Web/]
>C:/Program Files/DA Manager Web/
```

Caution: Make sure that the path ends with a forward slash (/).

Caution: In Windows, replace \ with / in the path name.

```
Example: "C:/Program Files/DA Manager Web/"
```

9. Restart the Device Manager server and HiCommand Suite Common Component.

   The changes to the launch environment settings now apply.

```
Launch setup has successfully completed.

You must restart the Device Manager Server and Common Component Services
for this these changes to take effect.

Exit - Default is n?(y, n):
```

10. Check whether DAMP (for Web) runs on HiCommand Suite Common Component. Specify the following URL in the browser, and then make sure that the DAMP (for Web) window appears.

```
http://host-name-or-IP-address:portID/program/DeviceManager/damp/default.htm
```

11. Refresh the storage subsystems to be operated on by DAMP (for Web).

Note: If you set up the launch environment by using the simple setup tool, the URL associated with DAMP (for Web) is set as alias information in HiCommand Suite Common Component. This alias information remains if you subsequently uninstall Device Manager or DAMP (for Web). To delete the alias information and other launch settings, see section 9.1.3.

9.2.3 Storage Subsystem Information to be Registered by Using DAMP (for Web)

- To operate storage subsystems by launching DAMP (for Web) from the HiCommand Device Manager server, the storage subsystem information must be registered in advance by using DAMP (for Web). For details on how to register this information, see the *Disk Array Management Program 2 (for Web) User's Guide* or *Disk Array Management Program 3 (for Web) User's Guide*.
- To register a unit name of the storage subsystem by using DAMP (for Web), use an IP address with an `H` added as a prefix. (Example: If the IP address is `192.168.108.123`, the unit name will be `H192.168.108.123`.)
- The IP address used for a unit name is *IP-address-1* or *IP-address-2* with which the storage subsystem was registered in HiCommand Device Manager.
- When DAMP (for Web) is directly used without launching DAMP (for Web) after the launch settings for DAMP (for Web) are configured, specify the following URL in the browser.

  ```
  http://host-name-or-IP-address:portID/program/DeviceManager/damp/default.htm
  ```

  This way, you can also register information about storage subsystems.

9.3 Starting HSSM From the Dashboard

To link with HSSM and start HSSM from the **Dashboard** menu, create the `StorageServicesManager.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 or a Linux system:

```
/opt/HiCommand/Base/common
```

In the `StorageServicesManager.conf` file, specify the `LaunchURL` parameter in the format shown as follows:

Format of the StorageServicesManager.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 `StorageServicesManager.conf` as follows:

For Secure Connections:

```
LaunchURL=https://machinename
```

For Nonsecure Connections:

```
LaunchURL=http://machinename
```

Chapter 10 Troubleshooting

- Problems and Solutions (see section 10.1)
- Collecting Maintenance Information (see section 10.2)
- Obtaining Alert Information by Using the Email Notification Function (see section 10.3)
- Contacting the Hitachi Data Systems Support Center (see section 10.4)

10.1 Problems and Solutions

Table 10.1 lists the common problems and solutions after installing Device Manager on a Windows, Solaris, or Linux platform. For a listing of Device Manager Error Codes, see *Hitachi HiCommand Device Manager Error Codes* (MK-92HC016).

Table 10.1 General Troubleshooting Information

No.	Problem	Solution
1	DESCRIPTION: Inconsistencies in LUNs and Logical Group information. LUNs disappear or logical group information is inconsistent between Device Manager Servers. CAUSE: Multiple Device Manager Servers are managing the storage subsystems	SOLUTION: Never have more than one active Device Manager Server managing a single storage array at a time. Device Manager was designed to manage multiple storage arrays, but not to cooperate with other instances of Device Manager Server to manage the same storage subsystems. More than one active Device Manager client is not a problem.
2	DESCRIPTION: Not enough disk space for installation in a Windows environment. CAUSE: The InstallAnywhere installer needs sufficient space to unpack the compressed installation files. InstallAnywhere uses the Windows TEMP environment variable to locate the temporary directory for extracting the files. You should have at least 100 MB of free space available, preferably more, on this drive.	SOLUTION: Choose a different drive and directory, or delete files from the Windows TEMP directory to clear enough space for InstallAnywhere.

No.	Problem	Solution
3	DESCRIPTION: The InterBase Server service stops and then the HiCommandServer service stops when an attempt is made to start the HiCommand Device Manager server on a machine managed by the Microsoft Systems Management Server (SMS). CAUSE: The InterBase Server and SMS are not set to coexist in the current configuration.	SOLUTION: To prevent the InterBase Server service from stopping, change the following SMS settings file: *SMS-installation-directory*\Inboxes\Clifiles.src\Hinv\Sms_def.mof Change the settings (change TRUE to FALSE) as follows: Before change: `[SMS_Report(TRUE),` `SMS_Group_Name("Services"),` `ResID(5000),ResDLL("SMS_RXPL.dll"),` `SMS_Class_ID("MICROSOFT|SERVICE|1.0")]` `class Win32_Service :` `SMS_Class_Template ` After change: `[SMS_Report(FALSE),` `SMS_Group_Name("Services"),` `ResID(5000),ResDLL("SMS_RXPL.dll"),` `SMS_Class_ID("MICROSOFT|SERVICE|1.0")]` `class Win32_Service :` `SMS_Class_Template ` For details, see WORKAROUND in the following Microsoftknowledge base article: *Microsoft Knowledge Base Article - 257509 SMS: Hardware Inventory May Cause Third-Party Win32 Services to Stop* (http://support.microsoft.com/default.aspx?scid=kb;EN-US;257509)

4	DESCRIPTION: The following message was displayed during Device Manager server installation on a Linux environment:
	`[yyyy/mm/dd hh:mm:ss] main() Invoke: /opt/HiCommand/HiCommandServer/inst/GetDBInfo.sh`
	..
	`An error occurred during loading of a library.`
	...
	CAUSE: The prerequisite library `compat-libstdc++-33-3.2.3-47.3` is not installed.
		SOLUTION: Perform the following operations in order:
		1. Install `compat-libstdc++-33-3.2.3-47.3`.
		2. Uninstall the Device Manager server (see section 4.8).
		3. Perform a new installation of the Device Manager server (see section 4.2.3).

No.	Problem	Solution

5	DESCRIPTION: An error occurs during Device Manager server installation.
	CAUSE: There is an error in the environment or settings on the installation destination machine.
		SOLUTION: If an error occurs during the Device Manager server installation, take one or more of the following actions. If you cannot resolve the problem, contact maintenance personnel.
		1. Use the `hcmdsgetlogs` command to collect maintenance information#1.
		2. Back up the database and property files if they have not been backed up already#2. If other HiCommand Suite products are installed, refer to the documentation of the appropriate product when performing backup.
		3. In the **Applications** tab of the Windows Task Manager, terminate the **InstallAnywhere** task. If other applications are currently being installed, wait until installation of all applications has been completed before terminating the **InstallAnywhere** task.Reboot the system.
		4. In Windows, delete the following folders if they exist:
		The folder set for the `temp` environment variable of the installation user:
		`{1345FCD1-713E-4449-8F76-3F6503941040}`
		Example: `C:\Documents and Settings\Administrator\Local Settings\Temp\{1345FCD1-713E-4449-8F76-3F6503941040}`
		The following folder directly under the startup drive:
		`_HDBInstallerTemp`
		Example: `C:\_HDBInstallerTemp`
		Folders within the installation folder of the Device Manager server:
		`installation-folder-for-the-Device-Manager-server``\_InstallerFilesTemp`
		5. Perform one of the following, based on the type of installation:
		When an attempt to perform a new installation fails:
		Perform uninstallation. Reboot the system, and then install again.
		When an attempt to perform an upgrade installation fails:
		Perform uninstallation. Reboot the system, and then perform a new installation again. Then, restore any backed-up data #3.
		When an attempt to update the database fails during an upgrade installation from version 3.5 or earlier:
		Perform the recovery procedures that follow the troubleshooting information.

No.	Problem	Solution
		#1 For details about collecting maintenance information, see section 10.2. #2 For details about performing backup manually, see section 3.2.4 for Windows, or section 4.2.5 for Solaris or Linux. For details about using commands to back up a database, see section 3.6.1 for Windows, or section 4.6.1 for Solaris or Linux. #3 For details about using commands to restore a database, see section 3.6.2 for Windows, or section 4.6.2 for Solaris or Linux.
6	DESCRIPTION: In an upgrade operation of the Device Manager Server 3.5 or earlier to 4.0 or later, an error occurred while a database is being converted. CAUSE: The free disk space used to store the database is less then 100 MB, or a required service is not running.	SOLUTION: Make sure the following: 100 MB of free disk space is available for the Device Manager Server database. The Common Component is running. Both InterBase and InterClient are running. If no problem was found, execute the database convert command (`migrateFmIB`). For details about the database convert command, see section 3.7 for Windows, or section 4.7 for Solaris.

No.	Problem	Solution
7	DESCRIPTION: In an operation to upgrade the HiCommand Device Manager server version 3.5 or earlier to version 4.0 or later, an error occurred before the database was converted. CAUSE: Installation was interrupted due to service interruption, or other failures.	SOLUTION: Perform the following operations in sequence and then retry the installation: 1. Copy the following files to a location other than the installation folder: In Windows: *installation-folder-for-the-Device-Manager-server*\migrateFmIB.bat *installation-folder-for-the-Device-Manager-server*\HiCommandServer\ext\interclient.jar *installation-folder-for-the-Device-Manager-server*\HiCommandServer\database\interbase\HICOMMAND.GDB Among the property files below, copy only those in which a value other than the default value is specified for a property: *installation-folder-for-the-Device-Manager-server*\HiCommandServer\config*.properties *installation-folder-for-the-Device-Manager-server*\SupportTools\CollectTool\TIA.properties *installation-folder-for-the-Device-Manager-server*\HiCommandCLI\legacy\R2.1\HiCommandCLI.properties *installation-folder-for-the-Device-Manager-server*\HiCommandCLI\legacy\R2.0\HiCommandCLI.properties *installation-folder-for-the-Device-Manager-server*\HiCommandCLI\HiCommandCLI.properties In Solaris /opt/HiCommand/migrateFmIB.sh /opt/HiCommand/HiCommandServer/ext/interclient.jar /opt/HiCommand/HiCommandServer/database/interbase/HiCommand.gdb

No.	Problem	Solution

		Among the property files below, copy only those in which a value other than the default value is specified for a property:
		`/opt/HiCommand/HiCommandServer/config/*.properties`
		`/opt/HiCommand/SupportTools/CollectTool/TIA.properties`
		`/opt/HiCommand/HiCommandCLI/legacy/R2.1/HiCommandCLI.properties`
		`/opt/HiCommand/HiCommandCLI/legacy/R2.0/HiCommandCLI.properties`
		`/opt/HiCommand/HiCommandCLI/HiCommandCLI.properties`
		2. Uninstall the HiCommand Device Manager server.
		3. Perform a new installation of the HiCommand Device Manager server (for details, see section 3.2.2 for Windows, or section 4.2.3 for Solaris).
		Note: For Windows, choose the same directory as the original installation directory.Copy the files `migrateFmIB.bat(sh)`, `interclient.jar`, and `hicommand.gdb`, copied in the first step, back to the original location.
		4. Also copy `interclient.jar` to the following directory:
		In Windows:
		`installation-folder-for-HiCommand-Suite-Common-Component``\database\interclient.jar`
		In Solaris:
		`/var/opt/HiCommand/Base/database/interclient.jar`
		5. Apply the same settings specified in the property files that were copied in the first step to the relevant property files (if `*.properties.old` have already been created, simply copy them).
		6. Use the following procedure to start HiCommand Suite Common Component.
		In Windows:
		Execute the following command from the command prompt:
		`installation-folder-for-HiCommand-Suite-Common-Component``\bin\hcmdssrv /start /server HBase`
		The following shows an example of executing the command:
		`C:\Program Files\HiCommand\Base\bin\hcmdssrv /start /server HBase`
		In Solaris:
		Execute the following command from the terminal window:
		`# /opt/HiCommand/Base/bin/hcmdssrv –start /server HBase`

No.	Problem	Solution
		7. Execute the database convert command (`migrateFmIB`) 8. Set the `server.base.initialsynchro` property to true. 9. Use the following procedure to start the HiCommand Device Manager server. In Windows: Select **Start**, **Programs**, **HiCommand**, **Device Manager**, and then **Start Server**. In Solaris: Execute the following command from the terminal window: `# /opt/HiCommand/suitesrvcntl -start_hdvm` 10. If Tuning Manager has been installed in a different server and the Single Sign On function is used, configure the settings for Single Sign On again (see the Tuning Manager manual). 11. If the port for HiCommand Suite Common Component has been changed, return the setting to that state.

No.	Problem	Solution
8	DESCRIPTION: As a result of a Device Manager server upgrade, the user ID or password is no longer usable. CAUSE: The user ID or password contains a character that cannot be used in version 3.5 later.	SOLUTION: Perform the following operations in sequence and create a new user ID or password. 1. Back up `oldDbBackup.gbk`. `oldDbBackup.gbk` in the following location: In Windows: *`installation-folder-for-the-Device-Manager-server`*`\HiCommandServer\database\interbase\oldDbBackup.gbk` In Solaris: `/opt/HiCommand/HiCommandServer/database/interbase/oldDbBackup.gbk` 2. Uninstall the HiCommand Device Manager server). 3. Re-install the HiCommand Device Manager server used before the upgrade (see the manual of the installed version). 4. Restore `oldDbBackup.gbk` (which was backed up in the first step). 5. Create a new user by using the appropriate characters for user IDs in version 3.5 or later. The following characters are usable: User ID: A-Z a-z 0-9 - _ . @ + # Password: A-Z a-z 0-9 ! # $ % & ( ) * + - . = @ \ ^ _ | ' 6. Upgrade the HiCommand Device Manager server (for details see section 3.2.4 for Windows, or section 4.2.5 for Solaris). 7. Clear the cache in Java Web Start. For details about how to clear the cache in Java Web Start, see the *HiCommand Device Manager Web Client User's Guide*.

No.	Problem	Solution
9	DESCRIPTION: In Windows, reports are not displayed when the **HTML** button is clicked in the Storage Utilization by Host - Reports subwindow or Storage Utilization by Logical Group - Reports subwindow in the Web Client. CAUSE: Either too many storage subsystems have been selected, or the size of the memory heap used by the Device Manager server is too small.	SOLUTION: Decrease the number of storage subsystems selected in the Storage Utilization by Host - Reports subwindow or Storage Utilization by Logical Group - Reports subwindow, and then display a report. Alternatively, increase the size of the memory heap used by the Device Manager server to allow reports to be displayed. The size of the memory heap can be changed as follows. 1. Edit the `HiCommandServer.lax` file in the following folder to change the memory heap size: *`Installation-folder-for-the-Device-Manager-server`*`\HiCommandServer` 2. Open the `HiCommandServer.lax` file in a text editor, and change the value for `lax.nl.java.option.java.heap.size.max` to the value calculated below, in bytes. The default value is 268,435,456 (256 MB). If the result of the following formula is already smaller than 256 MB, then no changes are needed. (15000 x *number-of-LUNs-displayed* + 1700 x *number-of-WWNs-displayed*) x *number-of-users* *number-of-LUNs-displayed*: Total number of LUNs displayed per host (not the number of LUNs set for the storage subsystem) *number-of-WWNs-displayed*: Total number of WWNs displayed per LUN *number-of-users*: Number of users using the report feature concurrently. 3. After the `HiCommandServer.lax` file is changed, perform the following to restart the Device Manager server. Select **Start**, **Programs**, **HiCommand**, **Device Manager**, and then **Stop Server**. After the Device Manager server has been stopped, select **Start**, **Programs**, **HiCommand**, **Device Manager**, and then **Start Server**.

No.	Problem	Solution

10	DESCRIPTION: In Solaris or Linux:, reports are not displayed when the **HTML** button is clicked in the Storage Utilization by Host - Reports subwindow or the Storage Utilization by Logical Group - Reports subwindow in the Web Client.
	CAUSE: Either too many storage subsystems have been selected, or the size of the memory heap used by the Device Manager server is too small.
		SOLUTION: Decrease the number of storage subsystems selected in the Storage Utilization by Host - Reports subwindow or Storage Utilization by Logical Group - Reports subwindow, and then display a report. Alternatively, increase the size of the memory heap used by the Device Manager server to allow reports to be displayed.
		The size of the memory heap can be changed as follows.
		1. Edit the `hicommand.sh` file in the following folder to change the memory heap size:
		`/opt/HiCommand`
		2. Open the `hicommand.sh` file in a text editor, and change the value of the `-Xmx` option of the `java` command specified in the `start` option script to the value calculated below, in MB. The default value is 256 MB. If the result of the following formula is already smaller than 256 MB, then no changes are needed.
		(0.0145 x *number-of-LUNs-displayed* + 0.00165 x *number-of-WWNs-displayed*) x *number-of-users*
		number-of-LUNs-displayed: Total number of LUNs displayed per host (not the number of LUNs set for the storage subsystem)
		number-of-WWNs-displayed: Total number of WWNs displayed per host
		number-of-users: Number of users using the report feature concurrently.
		The following shows how to change the value for a value of 512 MB as calculated above.
		Before: `java -Xmx256m -classpath ...`
		After: `java -Xmx512m -classpath ...`
		3. After the `hicommand.sh` file is changed, perform the following to restart the Device Manager server.
		Execute the following command:
		`# /opt/HiCommand/suitesrvcntl -stop_hdvm`
		After the Device Manager server has been stopped, execute the following command:
		`# /opt/HiCommand/suitesrvcntl -start_hdvm`

No.	Problem	Solution
11	DESCRIPTION: Database registration attempts fail when the Device Manager server is installed in a Windows cluster environment. CAUSE: The termination code of the `hcmdsdbclustersetup` command is `250` (data import processing has failed).	SOLUTION: Perform the following procedures in the order given to restore the system. If the database has been backed up: 1. Perform recovery from the database backup.To restart setting of the cluster environment, first perform the procedures to stop the Device Manager server and HiCommand Suite Common Component. 2. If you want to continue the cluster environment settings, first perform the procedure for executing the `hcmdsdbclustersetup` command to migrate the database to the shared disk. If a HiCommand Suite product whose version is earlier than 5.7 has been installed, stop the service of that product, and then migrate the database. If the database has not been backed up: 1. Execute the following two commands to restore the state of Device Manager. *installation-folder-for-HiCommand-Suite-Common-Component*\HDB\BIN\pdntcmd.bat *installation-folder-for-HiCommand-Suite-Common-Component*\HDB\BIN\pdrels -r HDVM_RD The following shows examples of executing the commands: C:\Program Files\HiCommand\Base\HDB\BIN\pdntcmd.bat C:\Program Files\HiCommand\Base\HDB\BIN\pdrels -r HDVM_RD 2. Uninstall the Device Manager server. 3. Install the Device Manager server. 4. To continue the cluster environment settings, first perform the appropriate step listed below: If database registration failed while performing the installation procedure in section 3.3.3, perform the operations from step 2 in section 3.3.3.1. If database registration failed while performing the installation procedure in section 3.3.4, first stop services of HiCommand Suite Common Component and all HiCommand Suite products. Then, perform the operations from step 9 in section 3.3.4.1. If database registration failed while performing the installation procedure in section 3.3.6, perform the operations from step 3.

No.	Problem	Solution

12	DESCRIPTION: Database registration attempts fail when the Device Manager server is installed In Solaris or Linux: cluster environment.
	CAUSE: The termination code of the `hcmdsdbclustersetup` command is `250` (data import processing has failed).
		SOLUTION: Perform the following procedures in the order given to restore the system.
		If the database has been backed up:
		1. Perform recovery from the database backup.To restart setting of the cluster environment, first perform the procedures to stop the Device Manager server and HiCommand Suite Common Component.
		2. To continue the cluster environment settings, first perform the procedure for executing the `hcmdsdbclustersetup` command to migrate the database to the shared disk.
		If a HiCommand Suite product whose version is earlier than 5.7 has been installed, stop the service of that product, and then migrate the database
		If the database has not been backed up:
		1. Execute the following two commands to restore the state of Device Manager.
		`# /opt/HiCommand/Base/HDB/bin/pduxenv`
		`# /opt/HiCommand/Base/HDB/bin/pdrels -r HDVM_RD`
		2. Uninstall the Device Manager server.
		3. Install the Device Manager server. For details about how to perform the installation, see section 4.2.3.
		4. To continue the cluster environment settings, first perform the appropriate step listed below:
		If database registration failed while performing the installation procedure in section 4.3.3, perform the operations from step 2 in section 4.3.3.1.
		If database registration failed while performing the installation procedure in section 4.3.4, first stop services of HiCommand Suite Common Component and all HiCommand Suite products. Then, perform the operations from step 8 in section 4.3.4.2.
		If database registration failed while performing the installation procedure in section 4.3.6, perform the operations from step 3.

13	DESCRIPTION: SSL communication with SMI-S Provider is disabled because SSL configuration for SMI-S failed during Device Manager server installation. CAUSE: An unexpected error occurred while configuring SSL for SMI-S.	SOLUTION: Use the `HiKeytool` command to configure SSL for SMI-S. For details about how to do this, see section 7.4.
14	DESCRIPTION: The service discovery feature is not available, because the SLP service (or the SLP daemon) failed to start during Device Manager server installation. CAUSE: An unexpected error occurred during the SLP service (or the SLP daemon) startup.	SOLUTION: Set the service discovery feature. For details about how to do this, see section 11.5.

No.	Problem	Solution
15	DESCRIPTION: Canceling the SLP service (or the SLP daemon) failed during Device Manager server uninstallation. CAUSE: This problem happens in either of the following cases: When performing uninstallation while the SLP service (or the SLP daemon) is running When performing uninstallation while the SLP service is stopped, but is registered as a Windows service.	SOLUTION: Stop or clear the SLP service (or the SLP daemon). For details about how to do this, see section 11.5. If you use Windows, the OpenSLP file might be deleted during uninstallation. In that case, perform the following operations in order, and then clear the SLP service: 1. In the Services panel, disable the Service Location Protocol service. 2. Restart Windows.
16	DESCRIPTION: Even though the port number of SMI-S was entered during Device Manager server installation, after installation, the Device Manager server does not start or communication with SMI-S Provider is disabled. CAUSE: The port number entered during installation is incorrect.	SOLUTION: Change the port number used by the CIM/WBEM features, and then restart the Device Manager server. For details about how to change port numbers, see section 11.3.2.2. When you change a port number, do not specify the port numbers described in section 5.5.1.
17	DESCRIPTION: Device Manager output the message `KAIC00114-E An attempt to start the HTTP server on port "2001" failed.` or `KAIC00115-E An attempt to start HTTPS server on port "2443" failed.` to the event log file for Windows, or the `syslog` file for Solaris or Linux, and then could not be started. CAUSE: The port number is already used by another program.	SOLUTION: Change the port number used by the Device Manager web server (2001) or the port number used for secure HTTP communication by the Device Manager web server (2443), and then restart the Device Manager server. For details on how to change a port number, see section 8.2.2 and 8.2.3. When changing a port number, do not specify the port numbers listed in section 5.4.1.
18	DESCRIPTION: Incompatibility between Graph-Track 4.06 and Device Manager, such that installing one over the other can cause failures. CAUSE: Device Manager requires InterBase (`GDS32.dll`) at core rev level 6.0.1.0 and Graph-Track 4.06 uses core rev level 5.6.0.29.	SOLUTION: Upgrade to Graph-Track 5.0 or higher. If you are running Graph-Track 4.06, please see Graph-Track Alert # 21 for installation instructions.

10.2 Collecting Maintenance Information

When an error occurs in a Device Manager Server, you can use the **hcmdsgetlogs** command to obtain the maintenance information required for analyzing the Device Manager Server error.

10.2.1 Using the hcmdsgetlogs Command to Acquire Maintenance Information

When you execute the **hcmdsgetlogs** command, maintenance information (log files and database files) is acquired, and four archive files (`.jar`, `.hdb.jar`, `.db.jar`, and `.csv.jar`) are created. To execute this command, you must log on as a user who has Administrator permissions in Windows, or as the root user in Solaris or Linux.

Note: Do not execute more than one **hcmdsgetlogs** command simultaneously.

The **hcmdsgetlogs** command has the following format:

For Windows:

installation-directory-for-Common-Component\Base\bin\hcmdsgetlogs /dir directory-name [/type application-name] [/arc archive-file-name]

The following shows an example of executing the command:

C:\Program Files\HiCommand\Base\bin\hcmdsgetlogs /dir C:\hcmds_logs /type DeviceManager /arc dvm_log1

For Solaris or Linux:

 # /opt/HiCommand/Base/bin/hcmdsgetlogs -dir directory-name [-type application-name] [-arc archive-file-name]

You can specify the following options for the **hcmdsgetlogs** command:

`dir`

Specify the name of the directory on a local disk that stores maintenance information. If the directory has already been created, empty the directory. The maximum length of a path name that can be specified is as follows:

- When the `type` option is not specified: 71 bytes
- When `DeviceManager` is specified for the `type` option: 45 bytes

For details about the maximum length of a path name when an application name other than `DeviceManager` is specified in the `type` option, see the manual for each product.

You can specify any printable ASCII character excluding certain special characters. You cannot specify the following characters:

`\ / : , ; * ? " < > | $ % & ' ` `

However, you can specify `\`, `:`, and `/` (in Windows), or `/` (in Solaris or Linux) as a path delimiter. Do not specify a path delimiter at the end of a path name.

In Windows, to specify a space character in a path name, enclose the path name in double quotation marks ("). In Solaris or Linux, you cannot specify a space character in a path name.

`type`

Specify the name of the application from which maintenance information will be collected. To collect maintenance information for Device Manager, specify `DeviceManager` as the application name. If you do not specify this option, maintenance information for all of the web applications registered in HiCommand(R) Suite Common Component is collected.

`arc`

Specify the name of the archive files to be created. If you do not specify this option, the default file name is `HiCommand_log`. When the archive files are output, each of them will have an extension corresponding to the type of each archive file (`.jar`, `.hdb.jar`, `.db.jar`, or `.csv.jar`). The archive files are output under the directory specified in the dir option.

For the file name, you can specify any printable ASCII character excluding certain special characters. You cannot specify the following characters:

`\ / : , ; * ? " < > | $ % & ' ` `

In Solaris or Linux, you cannot specify a space character in a file name.

Return values

`0`: Normal termination

`1`: Parameter error

`2`: Abnormal termination

An example of collecting maintenance information for Device Manager only is shown below. In this example, the archive file named `HiCommand_log` is created under the `logs_work` directory.

In Windows:

```
installation-directory-for-Common-Component\bin\hcmdsgetlogs /dir
C:\logs_work /type DeviceManager
```

In Solaris or Linux:

```
# /opt/HiCommand/Base/bin/hcmdsgetlogs -dir /opt/logs_work -type
DeviceManager
```

An example of collecting maintenance information for HiCommand Suite products is shown below. In this example, the archive file named hicmd_log is created under the logs_work directory.

In Windows:

```
installation-directory-for-Common-Component\bin\hcmdsgetlogs /dir
C:\logs_work /arc hicmd_log
```

In Solaris or Linux:

```
# /opt/HiCommand/Base/bin/hcmdsgetlogs -dir /opt/logs_work -arc
hicmd_log
```

10.2.2 Obtaining a Thread Dump

If Device Manager uses the HBase Storage Mgmt Common Service function, collect a Java VM thread dump to check the cause of the problem if one of the following events occurs:

- The Device Manager log on window is not displayed when you start Web Client.
- The Device Manager main window is not displayed after logging on to Device Manager.
- The Device Manager main window is not displayed when you start a Device Manager Server from Tuning Manager.

To acquire a Java VM thread dump:

Windows:

1. In **<installation directory>\cc\web\containers\HiCommand**, create a file called **dump**.
2. Access the **Services** panel.
3. Stop the HBase Storage Mgmt Common Service. see section 5.2.2 if you need instructions.
4. The javacorexxx.xxxx.txt file is output to **<installation directory>\cc\web\containers\HiCommand**.
5. From the **Services** panel, start the HBase Storage Mgmt Common Service.

Solaris or Linux:

1. Execute **kill -3** PID. PID is a process ID written in the **/var/opt/HiCommand/Base/CC/web/containers/HiCommand/logs/cjstdout.log** file.
2. The **javacorexxx.xxxx.txt** file is output to **/opt/HiCommand/Base/CC/web/containers/HiCommand**.
3. Stop the HBase Storage Mgmt Common Service using the following command:

   # /opt/HiCommand/Base/bin/hcmdssrv -stop -server HBase
4. Start the HBase Storage Mgmt Common Service using the following command:

   # /opt/HiCommand/Base/bin/hcmdssrv -start -server HBase

10.3 Obtaining Alert Information by Using the Email Notification Function

The email notification function notifies users, by email, of the contents of alerts that occurred in the storage subsystem and were detected by the Device Manager server.

To use this function, you need to configure the SMTP server, a Device Manager user, and the Device Manager server.

For the email notification function, the Device Manager server notifies users of an alert only once when the Device Manager server detects the alert. If the Device Manager server fails to send an email, the same email will not be sent again. Information on an alert for which the Device Manager server fails to send an email, as well as the email address of the intended destination of this email, are output to the Device Manager trace log file. For details about the Device Manager trace log file, see section 5.3.1. Also, if the Device Manager server service is stopped before the Device Manager server sends an email about an alert, the email will not be sent. In this case, even if the Device Manager server service is started again, the Device Manager server will not send the email that has not been sent. Start the Device Manager server service, and then execute the `GetAlerts` command from the CLI or use the alert management function of Web Client, to make sure that actions have been taken for every alert.

If you set up an environment or perform maintenance tasks for the storage subsystem that was discovered by the Device Manager server, many alerts might be generated in that storage subsystem. Therefore, we recommend that you disable the email notification function.

The users who receive emails need to use email software that supports Unicode (UTF-8) encoding because when sending an email, the Device Manager server sets the character encoding of the email to Unicode (UTF-8).

10.3.1 Configuring the SMTP Server

Follow the setting procedure of the SMTP server so that the Device Manager server can connect the SMTP server.

The Device Manager server supports the following SMTP authentication methods: LOGIN or PLAIN. Make sure that you specify one of these authentication methods in the SMTP server that you use.

10.3.2 Specifying Settings for a User Who Receives Emails

When using the email notification function, use Web Client to specify the settings below for a Device Manager user who receives emails. For details on how to specify settings, see the *HiCommand Device Manager Web Client User's Guide*.

An email that contains the same contents will be sent to the users for whom the settings below are specified. Each email is addressed to one recipient, and is sent to the users individually.

- Set the Modify permission of Device Manager.
- Assign `All Resources` as a resource group.
- Edit the profile, and then specify an email address.

10.3.3 Configuring the Device Manager Server

To configure the Device Manager server when using the email notification function:

1. Stop the Device Manager server service.

   For details about how to stop the Device Manager server service, see secion 3.5 for Windows, or section 4.5 for Solaris or Linux.

2. Set the Device Manager server properties related to the email notification function. The following shows the properties related to the email notification function:

   - `server.mail.enabled`(see section 8.2.30)
   - `server.mail.from` (see section 8.2.31)
   - `server.mail.smtp.host` (see section 8.2.32)
   - `server.mail.smtp.port` (see section 8.2.33)
   - `server.mail.smtp.auth` (see section 8.2.34)
   - `server.mail.alert.type` (see section 8.2.35)
   - `server.mail.alert.status` (see section 8.2.36)

   Note: When the SMTP authentication setting is enabled on the Device Manager server and there are multiple SMTP authentication methods that the SMTP server specifies, the Device Manager server selects an authentication method (LOGIN or PLAIN in that priority order), and then sends an email. If LOGIN or PLAIN is not specified, the Device Manager server will send an email without using the SMTP authentication.

   Note: If the SMTP authentication setting is disabled on the SMTP server, even if the setting is enabled on the Device Manager server, the Device Manager server will send an email without using the SMTP authentication.

3. If you want to use SMTP authentication for the SMTP server, set the SMTP authentication user information.

   To set SMTP authentication user information, execute the SMTP authentication user information setting command. Even if SMTP authentication is enabled in the Device Manager server, if SMTP authentication user information is not registered, the Device Manager server will send emails without using SMTP authentication.

   For details about the SMTP authentication user information setting command, see section 10.3.4.

4. If necessary, edit the template file of the email used by the email notification function.

   For details about the template file used by the email notification function, see section 10.3.5.

5. Start the Device Manager server service.

For details about how to start the Device Manager server service, see section 3.5, or section 4.5.

10.3.4 SMTP Authentication User Information Setting Command

To use the email notification function, you need to connect to the SMTP server. To use SMTP authentication for the SMTP server, you need to set the SMTP authentication user information on the Device Manager server.

To register or modify the SMTP authentication user information on the Device Manager server, execute the `hdvmmodmailuser` command. The set information will be applied when you start the Device Manager server service after executing this command.

You can set only one piece of SMTP authentication user information on the Device Manager server. The set SMTP authentication user information will be updated each time you execute the command. If the currently set SMTP authentication user information is unknown, re-execute the command to set SMTP authentication user information.

Note: Even if the SMTP authentication setting is enabled on the Device Manager server, the Device Manager server sends an email without using SMTP authentication if the connection target SMTP server has not enabled the SMTP authentication setting.

Note: You cannot delete the SMTP authentication user information that you set on the Device Manager server.

To execute the `hdvmmodmailuser` command, the following conditions must be satisfied:

- A user who executes the `hdvmmodmailuser` command has the Administrator permission for Windows, or the root permission for Solaris or Linux
- A user who is specified when executing the `hdvmmodmailuser` command has the Admin permission of Device Manager
- The Device Manager server service is stopped.
- The HiCommand Suite Common Component services are running.

The following shows the installation location and format of the `hdvmmodmailuser` command:

In Windows:

installation-folder-for-the-Device-Manager-server`\HiCommandServer\tools\hdvmmodmailuser.bat -u` *Device-Manager-user-ID* `-p` *Device-Manager-password SMTP-authentication-user-ID* `[`*SMTP-authentication-password*`]`

The following is an example of executing the command:

```
C:\Program
Files\HiCommand\DeviceManager\HiCommandServer\tools\hdvmmodmailuse
r -u dvmuser1 -p sys0305 dvmuser1_mail dvmuser1_sys
```

In Solaris or Linux:

```
# /opt/HiCommand/HiCommandServer/tools/hdvmmodmailuser.sh –u Device-Manager-user-ID –p Device-Manager-password SMTP-authentication-user-ID [SMTP-authentication-password]
```

You can specify the following options in the `hdvmmodmailuser` command:

`–u` *Device-Manager-user-ID*

Specify a user ID that has the Admin permission of Device Manager.

You can use the following characters in the range from 1 to 256 bytes:

`A - Z, a - z, 0 - 9, #, +, –, ., @, _`

`–p` *Device-Manager-password*

Specify the password used to log in to Device Manager by the user *Device-Manager-user-ID* specified using the `–u` option.

You can use the following characters in the range from 1 to 256 bytes:

`A - Z, a - z, 0 - 9, !, #, $, %, &, ', (, ), *, +, –, ., =, @, \, ^, _, |`

SMTP-authentication-user-ID

Specify a user ID used for SMTP authentication.

You can use the following characters in the range from 1 to 64 bytes:

`A - Z, a - z, 0 - 9, !, #, $, %, &, ', (, ), *, +, , ,–, ., =, @, \, ^, _, |`

SMTP-authentication-password

Specify the password used to log in to the SMTP server by the user *SMTP-authentication-user-ID*. You can specify the following characters in the range from 0 to 64 bytes:

`A - Z, a - z, 0 - 9, !, #, $, %, &, ', (, ), *, +, , , –, ., =, @, \, ^, _, |`

You can omit this option.

10.3.5 The Template File Used by the Email Notification Function

The contents of the email sent to users by the email notification function are set in the template file `mail–alert–detection.txt`. If necessary, you can edit this file to customize the contents of the email.

The `mail–alert–detection.txt` file is stored in the following location:

For Windows:

installation-folder-for-the-Device-Manager-server`\HiCommandServer\config`

For Solaris or Linux:

`/opt/HiCommand/HiCommandServer/config`

The following shows the settings of the default file (the `mail-alert-detection.txt` file):

```
Subject:[DVM] Alert Notification

The following alert occurred.

MessageID: ${messageID}
Alert Type: ${alertType}
Source: ${source}
Status: ${status}
Component: ${component}
Description: ${description}
Recommended Action: ${recommendedAction}
Additional Info: ${additionalInfo}
Occurrence Time: ${occurrenceTime}

This message was sent automatically by the Device Manager server.
```

The `mail-alert-detection.txt` file consists of a header (by default, `Subject:[DVM] Alert Notification`) and the body of the email.

You can specify parameters for the header and body of the email. When the email is sent, the specified parameters will be replaced with the alert information collected by the Device Manager server. The following table shows the specifiable parameters:

Table 10.2 Parameters that Can Be Set in the Template File

Parameter Name	Description
messageID	Alert ID
alertType	Alert type
source	Storage subsystem name
status	Severity of an alert
component	Location of the storage device in which an alert occurred
description	Description of the problem
recommendedAction	Action that has to be taken for the problem
additionalInfo	Supplementary information
occurrenceTime	Time at which the Device Manager server obtained alert information Display format: `yyyy/mm/dd hh:mm:ss` `hh` is displayed by using 24-hour display.

Set the `mail-alert-detection.txt` file so that all of the conditions shown below are satisfied. If at least one condition is not satisfied, the Device Manager server will create an email by using the default settings instead of using the settings of the template file that you edited.

- The file name is `mail-alert-detection.txt`.
- The file is stored in the same location when the Device Manager server is installed.
- The file size is no more than 64 KB.

- Unicode (UTF-8) can be used as the character encoding.
- Each line of the template file is no more than 1024 bytes in length, excluding a line feed character.
- In the top line, the header is specified in the following format.

  `Subject:`*email-title*

  Only a single header is specified.
- In the second line from the top, specify a blank line.
- In the third line from the top until the bottom line, specify the contents.
- Parameters are specified in the following format:

  `${`*parameter-name*`}`

  The parameter name is case sensitive.

Note: The settings of this template file will be applied when the Device Manager service starts.

10.4 Contacting the Hitachi Data Systems Support Center

If you need to contact the Hitachi Data Systems Support Center, make sure that you provide as much information as possible about the problem, 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

Chapter 11 Overview and Setup of CIM/WBEM

This chapter gives an overview of CIM/WBEM (Web-Based Enterprise Management) provided by Device Manager, and explains how to set up CIM/WBEM.

- Device Manager and CIM/WBEM (see section 11.1)
- CIM/WBEM Features of Device Manager (see section 11.2)
- Preparations for Operating the CIM/WBEM Features (see section 11.3)
- Properties File Settings When Executing CIM (see section 11.4)
- Setting the Service Discovery Feature (see section 11.5)
- User Permissions for Using CIM/WBEM Features (see section 11.6)

11.1 Device Manager and CIM/WBEM

Device Manager supports WBEM defined by the standards-setting organization DMTF. WBEM is a standard proposed by the DMTF for managing networked devices, including hosts and storage subsystems, over the Internet. WBEM enables you to share data about devices in different environments (such as environments with different vendors, operating systems, or protocols) without considering the differences. WBEM is based on CIM, an object-oriented information model.

CIM, defined by DMTF, is a standardized approach for managing systems in network environments. CIM provides a framework for expressing the data to be managed. Applying CIM to storage subsystems enables you to use standardized methods to manage the configuration and status of storage subsystems in networks.

The CIM models provided by Device Manager conform to the SMI-S specifications (SNIA-CTP) endorsed by SNIA. The CIM models of the Device Manager server are defined in MOF (Managed Object Format) files provided by Device Manager. The MOF namespace provided by Device Manager.

CIM clients can access Device Manager by using the CIM XML/HTTP interface defined by WBEM.

Figure 11.1 shows the CIM components for Device Manager.

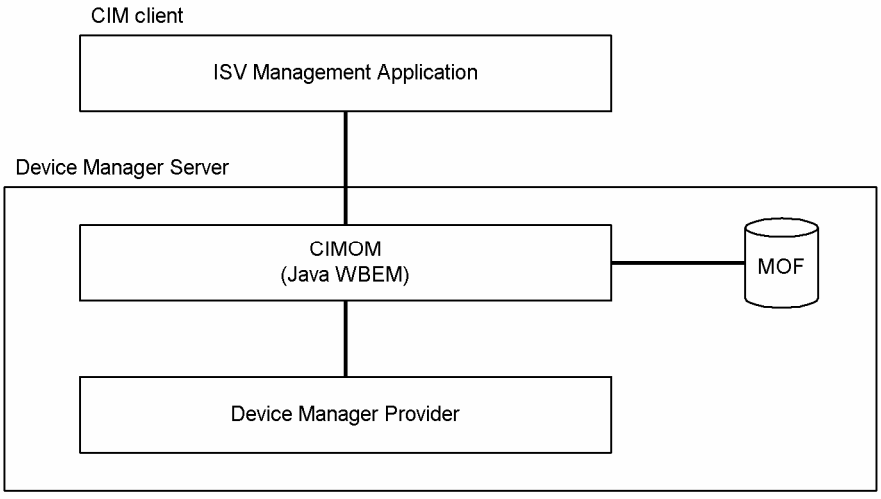

Figure 11.1 CIM Components for Device Manager

From a CIM client, you can specify a namespace by using the follow procedure:

- Specify the SMI-S version.

  Specify `root/smis/smis`***xx*** (***xx*** is an abbreviation for the version number).

  For example, to specify version 1.1.0, enter `root/smis/smis11`.

  The latest namespaces that complies with the specified SMI-S version is selected.

- Specify the condition `current`.

Enter `root/smis/current`.

The current namespace is selected.

- Specify the Device Manager version.

  Specify `root/hitachi/dm`***xx*** (***xx*** is an abbreviation for the version number)

The following table lists and describes the correspondence between the namespaces supported by Device Manager and SMI-S versions.

Table 11.1 Correspondence Between Namespaces and SMI-S Versions

Namespace[#1]			**SMI-S**
dm*xx*[#2]	**smis*xx***	**current**	
dm35	--	--	1.0.2
dm40	--	--	
dm41	--	--	
dm42	smis10	--	
dm43	--	--	1.1.0
dm50	--	--	
dm51	--	--	
dm55	--	--	
dm56	--	--	
dm57	smis11	current	

Legend: --: N/A

#1: We recommend that you specify a namespace by entering `root /smis/smis10`, `root/smis/smis11`, or `root/smis/current`.

#2: If you need to specify the namespaces (`dm24` and `dm30`) that were supported by versions of Device Manager earlier than 5.5, contact the maintenance personnel.

You can obtain information about CIM at:

http://www.dmtf.org/home/

You can obtain information about SMI-S at:

http://www.snia.org/smi/home/

11.2 CIM/WBEM Features of Device Manager

CIM/WBEM of Device Manager provides the three features specified in SMI-S:

- Objection operation feature
- Indication feature
- Service discovery feature

These features are described below:

Object operation feature

The SMI-S specifications, which Device Manager conforms to, define the interfaces for devices that make up a storage network, such as storage subsystems, virtual storage systems, switches, and hosts. The features that need to be provided by the management service to manage the devices are grouped in a profile for each device.

The profiles used by the CIM/WBEM features of Device Manager are the Array profile and its subprofiles. The Array profile defines the interfaces for storage subsystems.

Indication feature

The *indication* feature is the event notification feature defined by CIM. When an event occurs in a CIM server, the CIM server reports the indication instance, which shows the information about the event (such as generation or deletion of a CIM instance), to CIM clients. For a CIM client to receive indications, its location and transmission conditions for indications must be registered in the CIM server beforehand. For details on how to register, see the SNIA website.

Device Manager reports the occurrence of the following events:

- Generation of a volume
- Deletion of a volume
- Allocation of a path
- Cancellation of a path

Service discovery feature

Device Manager provides the service discovery feature based on the Service Location Protocol (SLP).

The SLP is undergoing standardization by IETF and provides a way to discover desired services available in a network. For details on the SLP, see RFC2608.

Just by specifying the type of service, SLP clients can obtain information (such as URLs) about how to access the available services, and information about service attributes.

In Device Manager, the Device Manager server uses the SLP to report information about the WBEM Service.

11.3 Preparations for Operating the CIM/WBEM Features

CIM/WBEM features are disabled by default in the Device Manager settings. To use the CIM/WBEM features, you must specify the following settings after installation:

- Basic settings required to use the CIM/WBEM features
- Setting the port used by CIM/WBEM features
- Settings required to use SSL (Secure Sockets Layer) in the CIM/WBEM features

11.3.1 Basic Settings Required to Use the CIM/WBEM Features

To use the CIM/WBEM features, you must first enable them.

To enable the CIM/WBEM features:

1. Change the setting in the Device Manager server property file.

   Change the setting of the `server.cim.support` property in the property file `server.properties` from `false` to `true`. The `server.properties` file is stored in the following location:

   In Windows:

   installation-folder-for-the-Device-Manager-server`\HiCommandServer\config\`

   Note: The default installation folder for Device Manager server is as follows:

   ```
   C:\Program Files\HiCommand\DeviceManager
   ```

   In Solaris or Linux:

   ```
   /opt/HiCommand/HiCommandServer/config
   ```

2. Stop any service that uses a port having a port number used by the CIM/WBEM service.

   The table below shows the port used by each CIM/WEB feature.

Table 11.2 Port Number Used by CIM/WBEM Features

Feature	Port Number Used
Objection operation feature	For non-SSL communication: 5988 (default) For SSL communication: 5989 (default)
Service discovery feature	427

Execute the following command to determine if any service program running is using the same port to be used by each CIM/WBEM feature:

- In Windows: `netstat -anp TCP`
- In Solaris: `netstat -an -P tcp`
- In Linux: `netstat -tan`

If any service program using the same port is running, change the port number for the service program.

If any service program is running (normally, another WBEM service program) that is using the same port to be used by an object operation feature, the object operation feature is not available.

If any service program is running (normally, another SLP service (or SLP daemon)) that uses the same port (427) to be used by the service discovery feature, an attempt to start the SLP service (or SLP daemon) for Device Manager will fail.

In Solaris:

In Solaris, CIMOM is incorporated in the system during installation. If CIMOM is running, an attempt to start CIM/WBEM might fail.

Use the following command to stop CIMOM:

```
# /etc/init.d/init.wbem stop
```

Also, delete CIMOM from `inittab` to prevent CIMOM from automatically starting.

3. Set up and start the SLP service (or SLP daemon).

   Set up the SLP service (or SLP daemon) to enable the service discovery feature. For details about how to set up this feature, see section 11.5.

   Note: In the SLP service (or SLP daemon), register the port used by CIM/WBEM features by default. For the ports used by CIM/WBEM features, see section 11.3.2.

4. Restart the HiCommand Device Manager server.

   In Windows:

   Select **Start**, **Programs**, **HiCommand**, **Device Manager**, and then **Stop Server.**

   When the Device Manager server has stopped, select **Start**, **Programs**, **HiCommand**, **Device Manager**, and then **Start Server**.

In Solaris or Linux:

Execute the following command:

/opt/HiCommand/suitesrvcntl -stop_hdvm

When the Device Manager server has stopped, execute the following command:

/opt/HiCommand/suitesrvcntl -start_hdvm

Note: When upgrading Device Manager from version 4.2 or earlier to 4.3 or later, check the `httpsd.conf` file. If this file contains coding that enables SSL functionality in the CIM/WBEM features, remove or comment out the coding before performing the upgrade. For details on how to disable SSL functionality, see section 7.3.4.2.

The `httpsd.conf` file is stored in the following folder or directory:

In Windows:

installation-folder-for-HiCommand-Suite-Common-Component`\httpsd\conf\httpsd.conf`

In Solaris or Linux:

`/opt/HiCommand/Base/httpsd/conf/httpsd.conf`

The following shows the coding contained in the `httpsd.conf` file that enables SSL functionality when the Device Manager version is 4.2 or earlier:

```
LoadModule proxy_module complete-path-name-for-the-proxy-module

Listen port-number-for-SSL-in-CIM/WBEM-features
<VirtualHost host-name:port-number-for-SSL-in-CIM/WBEM-features>
  ServerName host-name
  SSLEnable
  SSLRequireSSL
  SSLCertificateFile complete-path-name-for-the-certificate-file-from-CA
  SSLCertificateKeyFile complete-path-name-for-the-private-key-file
  ProxyPass / http://127.0.0.1:5988/
  ProxyPassReverse / http://127.0.0.1:5988/
</VirtualHost>
```

11.3.2 Setting up the Ports Used by CIM/WBEM Features

11.3.2.1 Opening and Closing Ports According to the Communication Type

Ports can be opened or closed according to the communication type used by CIM/WBEM features. Security can be enhanced by closing unused ports.

To open or close the port:

1. Using the `server.cim.support.protocol` property in the property file (`server.properties`) of the Device Manager server, set up whether to open or close each port according to the communication type.

   The setting values for `server.cim.support.protocol` are shown in the table below.

Table 11.3 Setting Values for server.cim.support.protocol

Setting Value	Port Status		Applicable Communication Type
	HTTP Port	HTTPS Port	
1	Open	Close	Non-SSL communication
2	Close	Open	SSL communication
3	Open	Open	SSL communication and non-SSL communication

2. Restart the Device Manager server.

   In Windows:

   Select **Start**, **Programs**, **HiCommand**, **Device Manager**, and then **Stop Server**.

   When the Device Manager server has stopped, select **Start**, **Programs**, **HiCommand**, **Device Manager**, and then **Start Server**.

   In Solaris or Linux:

   Execute the following command:

   # /opt/HiCommand/suitesrvcntl -stop_hdvm

   When the Device Manager server has stopped, execute the following command:

   # /opt/HiCommand/suitesrvcntl -start_hdvm

11.3.2.2 Changing the Port Number

In the initial state, the port numbers used by the CIM/WBEM features are as follows:

- HTTP port number: 5988
- HTTPS port number: 5989

To specify the port number, follow the steps below:

1. Change the port number set in the Device Manager server property file (`server.properties`). For details on the Device Manager server property file, see section 11.4.1.

   To change the HTTP port number:

   Change the port number set in `server.cim.http.port`.

   To change the HTTPS port number:

   Change the port number set in `server.cim.https.port`.

2. Restart the HiCommand Device Manager server.

   In Windows:

   Select **Start**, **Programs**, **HiCommand**, **Device Manager**, and then **Stop Server.**

   When the Device Manager server has stopped, select **Start**, **Programs**, **HiCommand**, **Device Manager**, and then **Start Server**.

   In Solaris or Linux:

   Execute the following command:

   # /opt/HiCommand/suitesrvcntl -stop_hdvm

   When the Device Manager server has stopped, execute the following command:

   # /opt/HiCommand/suitesrvcntl -start_hdvm

11.4 Properties File Settings When Executing CIM

When executing CIM, you must set up the properties files for the Device Manager server and restart Device Manager. The following table lists the Device Manager server properties you must set.

Table 11.4 Properties You Must Set for Device Manager Server When Executing CIM

Settings Required	File Name	Property
Enable CIM, and specify ports used in CIM	server.properties	server.cim.support
		server.cim.support.protocol
		server.cim.http.port
		server.cim.https.port
Set up the operating environment for the WBEM Service.	wbemservices.properties	classpath
		BaseDir
		propdir
		logdir
Set the authentication class for Device Manager.	cimom.properties	org.wbemservices.wbem.cimom.pswdprov

11.4.1 The server.properties File

When executing CIM, set up the following properties in addition to the regular settings.

11.4.1.1 server.cim.support

This property specifies whether to use the CIM interface. Set the `server.cim.support` property to `true`. The default is `false`, which specifies that the CIM interface is not used.

```
# whether the server supports CIM interface or not
server.cim.support={true | false}
```

11.4.1.2 server.cim.support.protocol

Specify whether to open or close the port used by the CIM interface.

Default: `3` (opens both the port for SSL communication and port for non-SSL communication.)

11.4.1.3 server.cim.http.port

To use non-SSL for the CIM interface, specify the HTTP port number.

Default: `5988`

11.4.1.4 server.cim.https.port

To use SSL for the CIM interface, specify the port number of HTTPS.

Default: `5989`

11.4.2 The jserver.properties File

This properties file sets up the operating environment for the WBEM Service. This file is stored in the following directory when Device Manager is installed:

In Windows:

```
installation-folder-for-the-Device-Manager-server\HiCommandServer\config
```

Note: The default installation folder for Device Manager server is as follows:

```
C:\Program Files\HiCommand\DeviceManager
```

In Solaris or Linux:

```
/opt/HiCommand/HiCommandServer/config
```

The contents of the `wbemservices.properties` file are as follows.

11.4.2.1 classpath

This property sets `classpath` required for operating the WBEM Service. Do not change the value of this property.

11.4.2.2 BaseDir

This property specifies the name of the base directory of `classpath` required for operating the WBEM Service. Do not change the value of this property.

11.4.2.3 propdir

This property specifies the directory containing the `cimom.properties` file. Do not change the value of this property.

11.4.2.4 logdir

This property specifies the directory containing the repository (compilation results of the MOF file: `store`). Do not change the value of this property.

11.4.3 Saving the cimom.properties File

Save the `cimom.properties` file in the directory specified by the `propdir` property in the `wbemservices.properties` file.

11.4.3.1 org.wbemservices.wbem.cimom.pswdprov

This property specifies the authentication class for Device Manager. Do not change the value of this property.

11.5 Setting the Service Discovery Feature

This section describes how to set the service discovery feature of Device Manager. To use the service discovery feature of Device Manager, you need the following prerequisite software:

In Windows or Linux:

OpenSLP 1.0.11

OpenSLP is attached to Device Manager. When you install Device Manager, the required file is copied. For details on OpenSLP, see the OpenSLP website (http://www.openslp.org/).

In Solaris:

SUNWslpr package and SUNWslpu package

These packages are attached to the Solaris system. For details on the SUNWslpr package and the SUNWslpu package, see the Sun Microsystems website (http://docs.sun.com/).

OpenSLP, the SUNWslpr package, and the SUNWslpu package need to be set up separately. For the setup procedure, see section 11.5.1.

When starting the CIM client, set the language tag (locale) for the service discovery feature to English (en).

11.5.1 Setting Up the Service Discovery Feature

11.5.1.1 In Windows

When you install Device Manager, the OpenSLP file is copied simultaneously. To use the service discovery feature, you need to register the SLP service (service name: `slpd`, display name: `Service Location Protocol`) as a Windows service. Perform the following procedure to register the SLP service as a Windows service.

To register the SLP service:

1. Install Device Manager, and then log on as a member of the Administrator group.
2. Display the command prompt and move to the folder containing the OpenSLP executable file.

   OpenSLP is installed in the following folder:

   ```
   installation-folder-for-the-Device-Manager-server\HiCommandServer\wsi\bin\windows
   ```

   Note: The default installation folder for Device Manager server is as follows:

   ```
   C:\Program Files\HiCommand\DeviceManager
   ```

3. Register the SLP service as a Windows service.

   Execute the following command:

```
> slpd -install
```

   To automatically start the service when Windows starts, execute the command with the `auto` option.

```
> slpd -install auto
```

   This operation is required only once. Even if you restart the Windows system, you do not need to re-register the daemon. If you execute the command without the `auto` option, you need to manually start the SLP service.

If the following message is displayed when Device Manager is uninstalled, release the SLP service manually from the Windows services.

```
An attempt to release the SLP service has failed. After uninstallation, release
the SLP service manually. Uninstallation continues.
```

To release the SLP service:

1. Log on as a member of the Administrator group.
2. Show the command prompt and move to the folder containing the OpenSLP executable file.
3. Release the SLP service from Windows services.

   Execute the following command:

```
> slpd -remove
```

11.5.1.2 In Solaris

In Solaris, the SLP daemon is installed in the standard configuration. However, the SLP daemon does not become active with the default settings. Perform the following procedure to automatically start the SLP daemon when the system starts.

To automatically start the SLP daemon:

1. Log on as the root user.
2. Check that the SLP daemon is installed.

   Use the `pkginfo` command or the graphical user interface of Solaris to check that the SUNWslpr package and the SUNWslpu package are installed. If they are not installed, install them.

3. Change the name of the configuration file of the SLP daemon.

   Change the file name as follows:

   Before change: `/etc/inet/slp.conf.example`

   After change: `/etc/inet/slp.conf`

4. Start the SLP daemon.

   Restart Solaris or execute the following command:

```
# /etc/init.d/slpd start
```

If Device Manager is uninstalled, stop or cancel the SLP daemon, as required. You can cancel the SLP daemon by using either of the following methods:

- Delete /etc/init.d/slpd or rename it.
- Delete /etc/inet/slp.conf or rename it.

11.5.1.3 In Linux

When Device Manager is installed, the OpenSLP file is copied at the same time. Settings do not need to be specified after installation, and the service discovery feature can be used as is.

If the following message is displayed when Device Manager is uninstalled, release the SLP daemon manually from the Linux daemons manually.

```
WARNING: An attempt to release the SLP daemon has failed. After uninstallation,
release the SLP daemon manually. Uninstallation continues.
```

To release the SLP daemon:

1. Log on as the root user.
2. Stop the SLP daemon.

   Execute the following command:

```
/opt/HiCommand/HiCommandServer/wsi/bin/slpd.sh stop
```

3. If `/etc/init.d/slpd` exists, delete it.

   Execute the following command:

```
chkconfig --level 01345 slpd off
chkconfig --del slpd
rm -f /etc/init.d/slpd
```

11.5.2 Starting and Stopping the Service Discovery Feature

11.5.2.1 In Windows

To manually start the SLP service, perform either of the following procedures:

- From **Administrative Tools**, choose **Services** and then **Service Location Protocol** to start the SLP service.
- Show the command prompt, move to the folder containing the OpenSLP executable file, and execute the following command:

```
> slpd -start
```

To stop the SLP service, perform either of the following:

- From **Administrative Tools**, choose **Services** and then **Service Location Protocol**.
- Display the command prompt, move to the folder containing the OpenSLP executable file, and execute the following command:

```
> slpd -stop
```

11.5.2.2 In Solaris

To manually start the SLP daemon, execute the following command:

```
# /etc/init.d/slpd start
```

To stop the SLP daemon, execute the following command:

```
# /etc/init.d/slpd stop
```

Note:

Sometimes, the `/etc/init.d/slpd stop` command may not successfully stop the SLP daemon. In that case, perform the following procedure to stop the SLP daemon:

- Return the name of the `/etc/inet/slp.conf` file to `/etc/inet/slp.conf.example`.

  You must delete the `/etc/inet/slp.conf` file at this point.
- Restart Solaris.

11.5.2.3 In Linux

To manually start the SLP daemon, execute the following command:

```
# /opt/HiCommand/HiCommandServer/wsi/bin/slpd.sh start
```

To stop the SLP daemon, execute the following command:

```
# /opt/HiCommand/HiCommandServer/wsi/bin/slpd.sh stop
```

11.5.3 Notes on Using OpenSLP

The SLP service (or SLP daemon) of OpenSLP outputs operation logs to the following file:

In Windows:

```
%WINDIR%slpd.log#
```

#%WINDIR% is replaced by the value of the environment variable WINDIR in Windows. Normally, the value is C:\WINNT\.

In Linux:

```
/opt/HiCommand/HiCommandServer/wsi/cfg/slp.log
```

By default, only the start message at SLP service startup is output to the log file. Since the SLP service log output (or SLP daemon) accumulates as time elapses, if you use the SLP service (or SLP daemon) for an extended period of time, the log output may eventually use up a lot of disk space. To prevent this, you need to periodically back up the log file and clear the disk space.

11.6 User Permissions for Using CIM/WBEM Features

The following table shows the user permissions for using CIM/WBEM features, based on the Device Manager permissions and executable CIM methods.

Table 11.5 User Permissions for Using CIM/WBEM Features

#	Resource Group	Device Manager Permissions				Executable CIM Methods	
		Admin	Modify	View	Peer#	Service Methods	CIM Operations
1	All Resources	Yes	Yes	Yes	--	Permitted	Permitted
2		--	Yes	Yes	--	Permitted	Permitted
3		--	--	Yes	--	Not permitted	Permitted
4		--	--	--	Yes	Not permitted	Permitted
5	User-defined resource groups	Yes	Yes	Yes	--	Not permitted	Not permitted
6		--	Yes	Yes	--	Not permitted	Not permitted
7		--	--	Yes	--	Not permitted	Not permitted
8		--	--	--	Yes	Not permitted	Permitted

Legend:

Yes: Has corresponding Device Manager permissions

--: Does not have corresponding Device Manager permissions

Permitted: Execution of corresponding CIM methods is permitted

Not permitted: Execution of corresponding CIM methods is not permitted

#: For *Peer* Device Manager permissions, users are treated as All Resources users, even when they belong to a user-defined resource group, due to Device Manager server processing.

Chapter 12 Overview and Setup of VDS

This chapter provides an overview of Device Manager VDS Provider, and explains the setup procedure.

- About Device Manager VDS Provider (see section 12.1)
- Installation Requirements and Procedures (see section 12.2)
- Operating Device Manager VDS Provider (see section 12.3)

12.1 About Device Manager VDS Provider

12.1.1 Overview of Device Manager VDS Provider

Windows Server 2003 provides Virtual Disk Service (VDS), which is a virtual disk system designed to manage storage subsystem devices via standardized interfaces.

Device Manager VDS Provider is a Device Manager software product that provides and configures storage subsystem information for VDS.

Device Manager VDS Provider supports the following OSs:

- Windows Server 2003 (SP1 or SP2)
- Windows Server 2003 x64 Edition (no SP or SP2)
- Windows Server 2003 R2 (no SP or SP2)

12.1.2 Functions of Device Manager VDS Provider

Device Manager VDS Provider is a hardware provider that is resident on a Windows host and replies to VDS requests. Device Manager VDS Provider provides functions for:

- Obtaining the following storage subsystem related configuration information:
  - Subsystem
  - LUN
  - LUN replication information
  - Path information
  - Port information

  If you specify a user assigned to a user-defined resource group as a user account used by VDS Provider, only the resources that have been defined in the resource group can be displayed when configuration information is acquired. This is called the *filtering function*.
- Performing the following storage subsystem related configuration tasks:
  - LUN creation
  - LUN expansion
  - LUN deletion
  - LUN mapping
  - LUN masking

Before you can use the DISKRAID command provided by Microsoft, you must perform the following installation tasks:

- Install Device Manager VDS Provider.

  Important: To use Device Manager VDS Provider, you need to change the value of the Device Manager server property `server.cim.support` to `true` in the `server.properties` file, and then restart the Device Manager server.

- If your host computer OS is not Windows Server 2003 R2, download VDS SDK from the Microsoft web page (http://www.microsoftstoragepartners.com/) and then install it.

12.1.3 Available Functions in Storage Manager for SANs for Windows Server 2003 R2

You can operate a storage subsystem via the VDS Provider function of Device Manager by using Storage Manager for SANs provided by Windows Server 2003 R2.

The following functions are available:

- Create LUN
- Delete LUN
- Extend LUN
- Rename LUN
- Assign LUN
- Unassign LUN
- Manage Server Connections
- Rename Subsystem
- Refresh

The following functions are not available:

- Blink Drive Light
- Manage iSCSI Targets
- Manage iSCSI Security
- Log On to iSCSI Targets

12.2 Installation Requirements and Procedures

12.2.1 Installing Device Manager VDS Provider

There are three methods for installing Device Manager VDS Provider in Windows.

- New installation

  Use this installation method to install Device Manager VDS Provider in a host in which Device Manager VDS Provider does not exist.

- Upgrade installation (to update an earlier version)

  Use this installation method to install Device Manager VDS Provider on a host in which an older version of Device Manager VDS Provider has been installed.

- Re-installation (to correct the same version)

  Use this installation method to install Device Manager VDS Provider on a host in which the same version of Device Manager VDS Provider has been installed.

You can obtain the version of an installed Device Manager VDS Provider by executing the following command:

```
installation-folder-for-Device-Manager-VDS-Provider\bin\hdvminfo.exe
```

The following shows an example of executing the command:

```
C:\Program Files\HITACHI\HDvM_VDS\bin\hdvminfo.exe
```

Notes: Note the following when installing Device Manager VDS Provider:

- At least 5 MB of free space is required on the hard disk. Also, an additional 5 MB of free space is required on the system drive to create temporary files during installation.
- After installation, you will need to set up access permission for the Device Manager VDS Provider installation folder. Since access permission cannot be set for FAT or FAT32 formatted drives, be sure to install Device Manager VDS Provider installation on an NTFS formatted drive.
- Do not execute the Microsoft-provided DISKRAID or `hdvmconfig` command during an upgrade installation of Device Manager VDS Provider. Also, do not install Device Manager VDS Provider when the Microsoft-provided DISKRAID or `hdvmconfig` command is being executed. If you execute the above command during an upgrade installation, the installation might end before completion. Make sure that you restart the system after installation
- Version 4.1 or earlier of Device Manager VDS Provider is automatically installed or uninstalled when Device Manager Agent is installed. If you want to use version 4.1 or earlier of Device Manager VDS Provider, install Device Manager Agent. For details on how to install Device Manager Agent, see the *HiCommand Device Manager Agent Installation Guide*.

- Version 4.1 or earlier of Device Manager VDS Provider cannot be used at the same time as version 4.2 or later. Stop the service of the version that will not be unused. For details on how to stop the service, see section 12.3.1. The service names are:
  - In version 4.1 or earlier: **Hitachi RAID Provider**
  - In version 4.2 or later: **Device Manager VDS Provider**
- If the Hitachi RAID Provider service is running, version 4.3 or later of Device Manager VDS Provider cannot be installed. If you attempt to install it, the following message appears.

```
Hitachi RAID Provider is running. Re-install after stopping this service.
```

- Overwrite installation (an update installation or a fixed version) may fail, in which case cancellation of the overwrite installation is reported. Overwrite installation (update or fixed) may also fail when the startup status of the Device Manager VDS Provider service is disabled. In this case, reboot the system, and then perform installation again.

12.2.1.1 New installation

To perform a new installation:

1. Log on to Windows using an Administrators-group user ID.
2. Insert the Device Manager VDS Provider CD-ROM.

   Note: Before starting the installation, cancel any programs that may be running.
3. From the **Start** menu, select **Run**. In the displayed panel, click **Browse**. In the displayed tree view, select `setup.exe` (in the \VDS folder on the CD-ROM). Then, click **OK**.

   The Welcome to the InstallShield Wizard for Device Manager VDS Provider panel appears.
4. Select **Next**.

   The Device Manager VDS Provider License Agreement panel appears.
5. Select **Next**.

   The Choose Destination Location panel appears. Select the folder in which you want Device Manager VDS Provider to be installed.

   Note: Do not select the installation folder for Device Manager VDS Provider version 4.1 or earlier.

   Note: The installation folder displayed by default differs for x86, and IPF or EM64T.
   - For x86

     `\Program Files\HITACHI\HDvM_VDS`
   - For IPF and EM64T

     `\Program Files (x86)\HITACHI\HDvM_VDS`
6. Select **Next**.

   The IP Address of the Device Manager server panel appears.

   Enter the IP address of the Device Manager server.

7. Select **Next**.

   The Installation Confirmation panel appears.

   Note: In this and previous steps, you can select **Cancel** to cancel installing Device Manager VDS Provider.

8. Select **Install**.

   The Progress Panel appears.

   When installation is complete, a panel indicating the completion of installation appears.

9. Select **Finish**.

10. Set up access permissions for the Device Manager VDS Provider installation folder.

    Using the appropriate OS function, set up read/write access permissions for the Administrators group and SYSTEM group.

    Do not set up access permissions for groups other than the Administrators group and SYSTEM group.

If your installation has ended normally, specify your user ID and password for connection to the Device Manager server. For details on how to specify your user ID and password, see section 12.3.3.

12.2.1.2 Upgrade Installation (To Update an Earlier Version)

To perform an upgrade installation:

1. Log on to Windows using an Administrators-group user ID.

2. Insert the Device Manager VDS Provider CD-ROM.

   Note: Before starting the installation, cancel any programs that may be running.

3. From the **Start** menu, select **Run**. In the displayed panel, click **Browse**. In the displayed tree view, select `setup.exe` (in the \VDS folder on the CD-ROM). Then, click **OK**.

   The Welcome to the InstallShield Wizard for Device Manager VDS Provider panel appears.

4. Select **Next**.

   Note: In this and previous steps, you can select **Cancel** to cancel installing Device Manager VDS Provider.

   The Progress Panel appears.

   When installation is complete, a panel indicating the completion of installation appears.

5. Select **Finish**.

6. Set up access permissions for the Device Manager VDS Provider installation folder.

   Using the appropriate OS function, set up read/write access permissions for the Administrators group and SYSTEM group.

   Do not set up access permissions for groups other than the Administrators group and SYSTEM group.

Note: Upgrade installation relies on the already specified Device Manager server IP address, user ID, and password as they are inherited from the original system. If you want to change the IP address, user ID, or password, see section 12.3.3.

12.2.1.3 Re-installation (To Correct the Same Version)

To perform an upgrade installation:

1. Log on to Windows using an Administrators-group user ID.
2. Insert the Device Manager VDS Provider CD-ROM. Then, from the **Start** menu, select **Run**. In the displayed panel, click **Browse**. In the displayed tree view, select `setup.exe` (in the \VDS folder on the CD-ROM), and then click **OK**.

   A window is displayed in which Repair or Remove can be selected.

   Note: You can also perform the above operation by choosing **Start**, **Settings**, **Control Panel**, and **Add or Remove Programs**. In the displayed panel, select **Device Manager - VDS Provider** and then click the **Change/Remove** button.
3. Select **Repair** and choose **Next**.

   The setup dialog box is displayed.
4. Select **Next**.

   A dialog box indicating that preparations for setup have finished is displayed.

   Note: Up until this step, you can select **Cancel** to cancel installation of Device Manager VDS Provider.
5. Select **Next**.

   A dialog box appears, indicating that Device Manager VDS Provider is being installed, and then a panel indicating the completion of installation appears.
6. Select **Finish**.
7. Set up access permissions for the Device Manager VDS Provider installation folder.

   Using the appropriate OS function, set up the read/write access permissions for the Administrators group and SYSTEM group.

   Do not set up access permissions for groups other than the Administrators group and SYSTEM group.

12.2.2 Uninstalling Device Manager VDS Provider

This section describes how to uninstall Device Manager VDS Provider.

Note: When you perform an uninstallation under the following conditions, a message that prompts you to restart the system is displayed after the uninstallation. Even though this message appears, you do not have to restart the system. Take the appropriate action by following the relevant instructions.

- If the exe file or bat file corresponding to Device Manager VDS Provider is being executed:

  Stop the exe file or bat file (or both) that is being executed.

- If the command prompt window is open and its current folder is the same as the installation folder for Device Manager VDS Provider:

  Close the command prompt window.

Uninstalling Device Manager VDS Provider stops service programs and deletes all the folders, files, and registry information that were registered during installation. The system returns to the status before installation.

Note: Once uninstallation is started, you cannot use the **Cancel** button to stop the processing. After the uninstallation finishes, install Device Manager VDS Provider again.

To uninstall Device Manager VDS Provider (method 1):

1. Select **Start**, **Settings**, **Control Panel**, and **Add/Remove Programs**.
2. Click the **Remove** button for Device Manager VDS Provider.

To uninstall Device Manager VDS Provider (method 2):

1. Select **Start**, **Settings**, **Control Panel**, and **Add/Remove Programs**.
2. Click the **Change** button for Device Manager VDS Provider.

   The Device Manager - VDS Provider maintenance menu is displayed.
3. Click the **Remove** button.

Caution: When changes or deletions are performed from **Add/Remove Programs**, an error might occur, in which case the following message is displayed. If an error occurs, use `setup.exe` in the `\VDS` folder on the CD-ROM to perform any changes or deletions.

```
An error occurred during reading C:\Program Files\Common
Files\InstallShield\Professional\RunTime\10\50\Intel32\Ctor.dll. The specified module
cannot be found.
```

12.3 Operating Device Manager VDS Provider

12.3.1 Starting and Stopping Device Manager VDS Provider

The following describes how to start and stop Device Manager VDS Provider.

12.3.1.1 Starting the Service

Open the Services window by choosing **Start**, **Settings**, **Control Panel**, **Management Tools**, and then **Services**. Then, start the **Device Manager VDS Provider** service.

Note: After the service starts, the message `KAIC24804-I` is output to the log file:

```
KAIC24804-I Inquiring storage information from Device Manager Server has been completed.
```

The log file is:

```
installation-folder-for-Device-Manager-VDS-Provider\logs\hdvmcomm.log
```

Caution: Do not connect from the VDS client to the VDS Provider until the Device Manager VDS Provider service starts.

12.3.1.2 Stopping the Service

Open the Services window by choosing **Start**, **Settings**, **Control Panel**, **Management Tools**, and then **Services**. Then, stop the **Device Manager VDS Provider** service.

12.3.1.3 Notes on Starting and Stopping the Service

After stopping or restarting Device Manager VDS Provider while the DISKRAID command is running, if the subcommand of the DISKRAID command is executed, an error occurs. In this case, finish the DISKRAID command by executing the `QUIT` command, and then restart the DISKRAID command.

Device Manager VDS Provider acquires information about the storage subsystems from the Device Manager server when Device Manager VDS Provider starts, or the `REFRESH` subcommand of the DISKRAID command is executed.

It might take a long time to acquire this information, so follow the directions below:

- Notes on restarting Device Manager VDS Provider

  Until Device Manager VDS Provider completes processing to acquire configuration information about the storage subsystems, note that:

  - If you execute a DISKRAID command to display information about the storage subsystems, the information is not displayed.
  - If you execute the `REFRESH` subcommand of the DISKRAID command, an error occurs.

- Notes on executing the `REFRESH` subcommand of the DISKRAID command

  Until Device Manager VDS Provider completes processing to acquire configuration information about the storage subsystem, note that:

  - If you execute a DISKRAID command to display information about the storage subsystems, the information before the refresh operation is displayed.
  - If you re-execute the `REFRESH` subcommand of the DISKRAID command, an error occurs.

  WARNING: If the `REFRESH` subcommand is executed, while the storage subsystem deleted from the Device Manager server is selected by executing the `SELECT` subcommand, the `LIST` subcommand might display incorrect information. In such a case, select another storage subsystem by executing the `SELECT` subcommand, and then re-execute the `REFRESH` subcommand, or restart the `DISKRAID` command.

12.3.2 Device Manager VDS Provider Property Files

Device Manager VDS Provider uses two property files:

- `vds.properties` file

  This file is used to configure the Device Manager VDS Provider environment.

- `logger.properties` file

  This file is used to configure the Device Manager VDS Provider logging function.

These files are stored in the following locations:

`vds.properties` file:

installation-folder-for-Device-Manager-VDS-Provider\config\vds.properties

`logger.properties` file:

installation-folder-for-Device-Manager-VDS-Provider\config\logger.properties

WARNING: If you change the contents of the Device Manager VDS Provider property files (`vds.properties` and `logger.properties`), you must restart the service.

12.3.2.1 vds.properties file

The `vds.properties` file contains the following information:

- IP address of the Device Manager server
- Port number of the Device Manager server
- Account (user name and password) used for Device Manager VDS Provider
- Device Manager VDS Provider account (user name and password) used for the filtering function

  Note: This information will be specified in the `vds.properties` file only when the filtering function is used.

  Note: Because the data of the Device Manager VDS Provider user account is encrypted, execute the `hdvmconfig` command to edit the data.

You can change the above information after installing Device Manager VDS Provider. For details on how to change the information, see section 12.3.3.

12.3.2.2 logger.properties File

The `logger.properties` file is used to configure the logging function of Device Manager VDS Provider. Table 12.1 contains the logging function properties of Device Manager VDS Provider.

Table 12.1 logger.properties File

Property	Description
logger.loglevel	You can specify the log level for data that Device Manager VDS Provider outputs to the files `hdvmcomm.log` and `hdvmprov.log`. Log levels: DEBUG, INFO, WARN, ERROR, and FATAL. If you use the default value, entries of INFO, WARN, ERROR, and FATAL are output to the log files, but the entries of DEBUG are not output. Default: `INFO`
logger.MaxBackupIndex	You can specify the maximum number of log file backups. If more log files are generated than specified, Device Manager VDS Provider writes over the oldest one. If a log file reaches the maximum size, the file is renamed by adding a counter (which represents the version) to the file name. For example, `hdvmcomm.log` becomes `hdvmcomm.log.1`. If additional backup log files are created, the counter increases until the specified number of backup log files is generated (for example, `hdvmcomm.log.1` becomes `hdvmcomm.log.2`). After the specified number of backup log files are created, each time a new backup file is created, the oldest backup file is deleted. Specifiable range: `1` through `20`. Default: `10`
logger.MaxFileSize	You can specify the maximum size of each log file. If a log file becomes larger than the specified maximum, Device Manager VDS Provider creates a new file and writes logs to it. Unless `KB` is specified for kilobytes or `MB` for megabytes, a specified size is interpreted to mean bytes. Specifiable range: from `512KB` to `32MB` Default: `1 MB`

Caution: If you changed the logger.properties file, restart Device Manager VDS Provider.

12.3.3 Setting up Device Manager VDS Provider

To set up Device Manager VDS Provider, use Web Client to create a user account for Device Manager VDS Provider, and then execute the `hdvmconfig` command.

12.3.3.1 Creating a user account used by Device Manager VDS Provider

Create a user account that Device Manager VDS Provider uses to access the Device Manager server. Both user accounts must have the Admin permission.

- A user to which All Resources is assigned

  This user is required for creating or deleting a volume.

- A user to which a user-defined resource group is assigned

This user is required for using the filtering function. Assign the resource to be acquired for Device Manager VDS Provider to the resource group. For details on how to create a user ID and how to assign a resource group, see the *HiCommand Device Manager Web Client User's Guide*.

12.3.3.2 Specifying information in the vds.properties file of Device Manager VDS Provider

Use the `hdvmconfig` command to change the information about Device Manager VDS Provider specified in the `vds.properties` file.

This command enables you to interactively specify each property stored in the `vds.properties` file. To execute this command, the Administrator permission is required. If you execute this command with a permission other than the Administrator permission, an error message will be output.

The `hdvmconfig` command is stored in the following location:

```
installation-folder-for-Device-Manager-VDS-Provider\bin\hdvmconfig.exe
```

To specify information in the `vds.properties` file:

1. Execute the following command:

   installation-folder-for-Device-Manager-VDS-Provider`\bin\hdvmconfig.exe`

2. A message asking if you want to change the settings appears.

   Enter `y` to change the settings, or `n` to leave the settings unchanged.

3. Enter the IP address of the Device Manager server.

   Enter the IP address of the Device Manager server in dotted decimal format. The specified IP address is assigned to `server.ipaddress` in the property file.

4. Enter the port number of the Device Manager server.

   If you do not enter a port number, the default `5988` is specified. The specified port number is assigned to `server.port` in the property file.

Caution: Specify the port number assigned to the `server.cim.http.port` in the property file (`server.properties`) used in the Device Manager server.

5. Enter the type of user to be registered.

   When `1` is entered:

   > You need to specify a user to which All Resources is assigned. This user acquires configuration information of all resources. This user can create and delete a volume.

   When `2` is entered:

   > You need to specify a user to which a user-defined resource group is assigned. This user acquires configuration information within the resource group that is assigned to this user. This user cannot create or delete a volume.

   When `3` is entered:

   > This user acquires configuration information within the resource group that is assigned to this user. This user can create and delete a volume.

   To use the filtering function, enter `2` or `3`.

6. By following the selection in step 5, enter the user ID and password.

   You can use the following characters for the user ID:

   `a-z, A-Z, 0-9, #, +, ., -, _, @`

   Note: For overwrite installations, if you do not enter a user ID, the currently set user ID will be inherited.

   You can use the following characters for the password:

   `a-z, A-Z, 0-9, !, #, $, %, &, (, ), *, +, -, ., =, @, \, ^, _, |, '`

   The user ID and password are encrypted by the `hdvmconfig` command and assigned to `server.authorization` and `server.authorizationforresourcegroup` in the property file.

7. A message appears asking if you want to save the entered information in the `vds.properties` file.

   Enter `y` to save the information, or `n` to leave the information unchanged.

8. Restart Device Manager VDS Provider.

12.3.4 Device Manager VDS Provider Log Files

Problems that occur during Device Manager VDS Provider installation, uninstallation, or execution of its services are recorded in the log file.

See Table 12.2 for the log filenames, locations, and descriptions.

Table 12.2 Log Files

Log File Name and Location	Description
installation-folder-for-Device-Manager-VDS-Provider\logs\hdvmcomm.log	Information about communication between Device Manager VDS Provider and the Device Manager server is recorded in this file.
installation-folder-for-Device-Manager-VDS-Provider\logs\hdvmprov.log	Information about the starting and stopping of Device Manager VDS Provider is recorded in this file.
Windows-system-drive:\DeviceManager_5_1_VDS_Install.log	Information about the installation execution for Device Manager VDS Provider is recorded in this file.
Windows-system-drive:\DeviceManager_VDS_UninstallLog.log	Information about the uninstallation execution for Device Manager VDS Provider is recorded in this file.

If a problem occurs in Device Manager VDS Provider, you can use the error information batch collection tool (`hdvmgetlogs.bat`). This tool collects the log files and property files required for error analysis from the Device Manager VDS Provider environment in a single operation. To execute this tool, you must have Administrator privileges.

`hdvmgetlogs.bat` is stored in the following location:

```
installation-folder-for-Device-Manager-VDS-Provider\bin
```

The format of `hdvmgetlogs.bat` is: `hdvmgetlogs.bat` (no arguments)

When you execute `hdvmgetlogs.bat`, a `resultDir` folder is created under *installation-folder-for-Device-Manager-VDS-Provider*. This folder stores the collected log files and property files.

Caution: If the `resultDir` folder already exists, the following confirmation message appears:

```
Output Directory "resultDir" already exists.
This program will delete "resultDir" before working. continue?
(Y)es or (N)o :
```

When you enter `y`, the command deletes the `resultDir` folder, and stores the acquired error information files in a new `resultDir` folder. When you enter `n`, processing is canceled.

Acronyms and Abbreviations

ACL	Access Control List
AMS	Adaptable Modular Storage
API	application program interfaces
CCI	Command Control Interface
CLI	Command Line Interface
COW	Copy on Write
CSR	Certificate Signing Request
DAMP	Java Web Start
DASD	direct access storage device
DHCP	Dynamic Host Configuration Protocol
DST	Daylight Saving Time
GB	gigabyte(s)
GUI	Graphical User Interface
HDP	Hitachi Dynamic Provisioning
IETF	Internet Engineering Task Force
JDK	Java Development Kit
JRE	Java Runtime Environment
JWS	Java WE
Kb	kilobyte(s)
LAN	local-area network
LDEV	logical device
LUN	Logical unit number
MOF	Managed Object Format
MSCS	Microsoft Cluster Service
NSC	Network Storage Controller
PKI	Public Key Infrastructure
SNMP	Simple network management protocol (part of the TCP/IP protocol suite).
SSL	Secure Sockets Layer
SVP	Service Processor
TCP/IP	transmission control protocol/internet protocol
TLS	Transport Layer Secuirty
USP	Universal Storage Platform

VDS	Virtual Disk Service
WMS	Workgroup Modular Storage
WWN	Worldwide name

Index

K

L