HITACHI
Inspire the Next

Hitachi Storage Command Suite

Hitachi Device Manager

Agent Installation Guide

FastFind Links

Hitachi Data Systems

MK-92HC019-22

Contents

Preface

This document describes how to install and work with the Device Manager agent.

This preface includes the following information:

- ☐ Intended Audience
- ☐ Software Version
- ☐ Release Notes
- ☐ Document Revision Level
- ☐ Document Organization
- ☐ Referenced Documents
- ☐ Document Conventions
- ☐ Convention for Storage Capacity Values
- ☐ Getting Help
- ☐ Comments

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

Intended Audience

This guide describes how to install the Device Manager agent software for Hitachi Device Manager software. We assume that our audience has:

- a background in data processing and understands peripheral storage device subsystems and their basic functions,
- read and understands the user guide(s) for the applicable Hitachi storage subsystem(s); for example, *Hitachi Lightning 9900 V Series User and Reference Guide* (MK-92RD100), *Hitachi Thunder 9500 V Series User and Reference Guide* (MK-92DF601),
- familiarity with the host operating system (e.g., the HP-UX OS) on which the agent is installed, and has
- knowledge of Storage Area Networks (SANs).

Software Version

This document revision applies to Hitachi Device Manager software version 6.4.

Release Notes

Release notes can be found on the documentation CD. Release notes contain requirements and more recent product information that may not be fully described in this manual. Be sure to review the release notes before installation.

Document Revision Level

Revision	Date	Description
MK-92HC019-00	November 2002	Initial Release ***Note:*** This document supersedes and replaces *HiCommand Device Manager HiScan Installation Guide* (MK-91HC005-04).
MK-92HC019-01	May 2003	Revision 1, supersedes and replaces MK-92HC019-00
MK-92HC019-02	September 2003	Revision 2, supersedes and replaces MK-92HC019-01
MK-92HC019-03	February 2004	Revision 3, supersedes and replaces MK-92HC019-02
MK-92HC019-04	March 2004	Revision 4, supersedes and replaces MK-92HC019-03
MK-92HC019-05	September 2004	Revision 5, supersedes and replaces MK-92HC019-04
MK-92HC019-06	October 2004	Revision 6, supersedes and replaces MK-92HC019-05
MK-92HC019-07	February 2005	Revision 7, supersedes and replaces MK-92HC019-06
MK-92HC019-08	June 2005	Revision 8, supersedes and replaces MK-92HC019-07
MK-92HC019-09	July 2005	Revision 9, supersedes and replaces MK-92HC019-08
MK-92HC019-10	October 2005	Revision 10, supersedes and replaces MK-92HC019-09
MK-92HC019-11	February 2006	Revision 11, supersedes and replaces MK-92HC019-10

Revision	Date	Description
MK-92HC019-12	June 2006	Revision 12, supersedes and replaces MK-92HC019-11
MK-92HC019-13	October 2006	Revision 13, supersedes and replaces MK-92HC019-12
MK-92HC019-14	January 2007	Revision 14, supersedes and replaces MK-92HC019-13
MK-92HC019-15	June 2007	Revision 15, supersedes and replaces MK-92HC019-14
MK-92HC019-16	October 2007	Revision 16, supersedes and replaces MK-92HC019-15
MK-92HC019-17	January 2008	Revision 17, supersedes and replaces MK-92HC019-16
MK-92HC019-18	May 2008	Revision 18, supersedes and replaces MK-92HC019-17
MK-92HC019-19	February 2009	Revision 19, supersedes and replaces MK-92HC019-18
MK-92HC019-20	July 2009	Revision 20, supersedes and replaces MK-92HC019-19
MK-92HC019-21	December 2009	Revision 21, supersedes and replaces MK-92HC019-20
MK-92HC019-22	June 2010	Revision 22, supersedes and replaces MK-92HC019-21

Document Organization

The following table provides an overview of the contents and organization of this document. Click the chapter title in the left column to go to that chapter. The first page of each chapter provides links to the sections in that chapter.

Chapter	Description
Overview	Gives an overview of the Device Manager agent and describes its system requirements.
Installing the Device Manager Agent	Explains the procedures for installing and setting up the Device Manager agent.
Operating the Device Manager Agent	Provides notes on how to manage host operations and explains how to set up and operate the Device Manager agent.
Troubleshooting	Describes how to troubleshoot problems with the Storage Navigator.
Acronyms and Abbreviations	Defines the acronyms and abbreviations used in this document.
Index	Lists the topics in this document in alphabetical order.

Referenced Documents

The following Hitachi referenced documents can be found on the applicable Hitachi documentation CD:

- Hitachi Storage Command Suite documents:
  - Hitachi Storage Command Suite Server Installation Guide, MK-98HC150
  - Hitachi Device Manager Server Configuration and Operation Guide, MK-08HC157
  - Hitachi Device Manager Command Line Interface (CLI) User's Guide, MK-91HC007
  - Hitachi Device Manager Error Codes, MK-92HC016
  - Hitachi Global Link Manager Installation and Configuration Guide, MK-95HC107
- Hitachi Enterprise Storage Systems documents:
  - Hitachi Lightning 9900 V Series User and Reference Guide, MK-92RD100
  - Hitachi Lightning 9900 User and Reference Guide, MK-90RD008
  - Hitachi Thunder 9500 V Series User and Reference Guide, MK-92RD100
- Hitachi Modular Storage Systems document:
  - Hitachi Thunder 9200 User and Reference Guide, MK-90DF504

Document Conventions

This document uses the following typographic conventions:

Convention	Description
Bold	Indicates text on a window, other than the window title, including menus, menu options, buttons, fields, and labels. Example: Click **OK**.
Italic	Indicates a variable, which is a placeholder for actual text provided by the user or system. Example: copy *source-file target-file* ***Note:*** Angled brackets (< >) are also used to indicate variables.
screen/code	Indicates text that is displayed on screen or entered by the user. Example: # pairdisplay -g oradb
< > angled brackets	Indicates a variable, which is a placeholder for actual text provided by the user or system. Example: # pairdisplay -g <group> ***Note:*** Italic font is also used to indicate variables.
[ ] square brackets	Indicates optional values. Example: [a | b] indicates that you can choose a, b, or nothing.
{ } braces	Indicates required or expected values. Example: { a | b } indicates that you must choose either a or b.
| vertical bar	Indicates that you have a choice between two or more options or arguments. Examples: [a | b] indicates that you can choose a, b, or nothing. { a | b } indicates that you must choose either a or b.

This document uses the following icons to draw attention to information:

Icon	Label	Description
	Note	Calls attention to important and/or additional information.
	Tip	Provides helpful information, guidelines, or suggestions for performing tasks more effectively.
	Caution	Warns the user of adverse conditions and/or consequences (e.g., disruptive operations).
	WARNING	Warns the user of severe conditions and/or consequences (e.g., destructive operations).

Convention for Storage Capacity Values

Physical storage capacity values (e.g., disk drive capacity) are calculated based on the following values:

Physical Capacity Unit	Value
1 KB	1,000 bytes
1 MB	$1,000^2$ bytes
1 GB	$1,000^3$ bytes
1 TB	$1,000^4$ bytes
1 PB	$1,000^5$ bytes
1 EB	$1,000^6$ bytes

Logical storage capacity values (e.g., logical device capacity) are calculated based on the following values:

Logical Capacity Unit	Value
1 KB	1,024 (2^{10}) bytes
1 MB	1,024 KB or $1,024^2$ bytes
1 GB	1,024 MB or $1,024^3$ bytes
1 TB	1,024 GB or $1,024^4$ bytes
1 PB	1,024 TB or $1,024^5$ bytes
1 EB	1,024 PB or $1,024^6$ bytes
1 BLOCK	512 BYTES

Getting Help

The Hitachi Data Systems Support Center staff is available 24 hours a day, seven days a week. To reach us, please visit the support Web site for current telephone numbers and other contact information: http://www.hds.com/services/support/. If you purchased this product from an authorized HDS reseller, contact that reseller for support.

Before calling the Hitachi Data Systems Support Center, please provide as much information about the problem as possible, including:

- The circumstances surrounding the error or failure.
- The exact content of any error message(s) displayed on the host system(s).

Comments

Please send us your comments on this document: doc.comments@hds.com. Include the document title, number, and revision, and refer to specific section(s) and paragraph(s) whenever possible.

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

1

Overview

This chapter gives an overview of the Device Manager agent and its system requirements.

About the Device Manager Agent

The Device Manager agent is a program that runs on a host (an application server) to collect host and storage subsystem information, and report that data to the Device Manager server. Following is the information that is primarily collected:

- Host information (such as host names, IP addresses, HBA WWN, and iSCSI name)
- Information about LDEVs allocated to the host (such as LDEV number, storage subsystem, LUN, and LDEV type)
- Information about file systems allocated to the host (such as file system types, mount points, and usage)
- Copy pair information (such as pair types and statuses)

Although Device Manager agents are not required for Device Manager operations, they enable the following operations when they are installed on a host:

Device Manager management of the storage usage status for each Device Manager host

By installing a Device Manager agent on each host, you can control how the volumes in the storage subsystems are used on each host. Also, if you specify the settings so that information about the hosts that are managed by the Device Manager server is periodically updated, you can use a management client to check the latest information.

- Device Manager management of copy pairs

  By linking with CCI, you will be able to use the Device Manager Web Client to centrally perform operations such as creating copy pairs, and changing configurations and statuses, which previously had to be performed for each server.

When you install a Device Manager agent on a host, the Provisioning Manager agent functionality, Replication Manager agent functionality, and a Global Link Manager agent are installed. Those agents, which are provided as a part of the Device Manager agent functionality, are explained below.

Provisioning Manager agent functionality and Replication Manager agent functionality:

The Provisioning Manager agent functionality or the Replication Manager agent functionality communicates with the Provisioning Manager server or the Replication Manager server respectively, to collect necessary information and configure necessary host settings.

Global Link Manager agent:

If the host OS is Windows®, Solaris 9 (SPARC), or Solaris 10 (SPARC), a Global Link Manager agent is installed. If DMP (the Dynamic Multipathing feature of VxVM) is being used to manage paths between hosts and storage subsystems, the Global Link Manager agent communicates with the Global Link Manager server to report information about paths and configure necessary host settings. For details about the Global Link Manager agent, see the *Hitachi Global Link Manager Installation and Configuration Guide*.

Note: If you use the CIM/WBEM function of Device Manager, you can use the Device Manager agent to obtain performance information about Hitachi USP or Universal Storage Platform V/VM. For details about the required settings for obtaining performance information, see the *Hitachi Device Manager Server Configuration and Operation Guide*.

Host Requirements for the Device Manager Agent

The following explains the system requirements for hosts on which the Device Manager agent is to be installed.

Caution:

- The name of each host on which the Device Manager agent runs must be unique within the notification destination Device Manager server.
- Device Manager agent can connect to Device Manager server of the same version or later. However, if the version of the Device Manager server is later than that of the Device Manager agent, the Device Manager functionality that can be used is limited to that of the Device Manager agent.

Supported Operating Systems

The prerequisite OS for the Device Manager agent depends on whether the agent is used in an IPv4 environment or IPv6 environment. Also, the Device Manager agent service might not start unless the patches required for the Device Manager agent prerequisite OS have been applied.

Operating Systems

The following table lists the supported operating systems for Device Manager agents.

Table 1-1 Supported Operating Systems

OS	Version	Architecture	IPv6 Environment Support	Remarks
Windows Server® 2003[#1]	No SP	x86	--	Not applicable
		IPF	--	Runs under WOW64. We recommend that SP2 be installed.
		x64 Edition (EM64T and AMD64)	--	Runs under WOW64.
	SP1	x86	--	Not applicable
		IPF	--	Runs under WOW64. We recommend that SP2 be installed.
	SP2	x86	Y	Not applicable
		IPF	--	Runs under WOW64.
		x64 Edition (EM64T and AMD64)	Y	
Windows Server 2003 R2[#1]	No SP	x86	--	Not applicable
		x64 Edition (EM64T and AMD64)	--	Runs under WOW64.
	SP2	x86	Y	Not applicable
		x64 Edition (EM64T and AMD64)	Y	Runs under WOW64.
Windows Server 2008[#1]	No SP	x86	Y	Not applicable
		IPF	--	Runs under WOW64.
		x64 Edition (EM64T and AMD64)	Y	
	SP2	x86	Y	Not applicable
		IPF	--	Runs under WOW64.
		x64 Edition (EM64T and AMD64)	Y	

OS	Version	Architecture	IPv6 Environment Support	Remarks
Windows Server 2008 R2[#1]	No SP	IPF	--	Runs under WOW64.
		x64 Edition (EM64T and AMD64)	Y	
Solaris	8	SPARC (32 and 64 bit)	--	We recommend that Solaris Patch Cluster be installed.
	9	SPARC (32 and 64 bit)	--	
	10[#2]	SPARC (32 and 64 bit)	Y	
		x64 Edition (AMD64)[#3]	Y	
AIX®	5.3	32 bit 64 bit	Y	Not applicable
	6.1	64 bit	Y	The Device Manager agent does not support environments where the Secure by Default function is enabled.
Red Hat Enterprise Linux®	Linux AS/ES 3	x86 IPF x64 Edition (EM64T)	--	Only the following versions of Linux AS/ES 3 (x86) are supported for Provisioning Manager: ▪ Update 0 ▪ Update 3 ▪ Update 4 ▪ Update 6

OS	Version	Architecture	IPv6 Environment Support	Remarks
	Linux AS/ES 4 Update 1	x86 IPF x64 Edition (EM64T)	--	Not applicable
	Linux AS/ES 4 Update 3	x86 IPF x64 Edition (EM64T)	--	
	Linux AS/ES 4 Update 4	x86	Y	
		IPF	--	
		x64 Edition (EM64T)	Y	
	Linux AS/ES 4.5	x86	Y	
		IPF	--	
		x64 Edition (EM64T)	Y	
	Linux AS/ES 4.6	x86	Y	
		IPF	--	
		x64 Edition (EM64T)	Y	
	Linux AS/ES 4.7	x86	Y	
		IPF	--	
		x64 Edition (EM64T)	Y	
	Linux AS/ES 4.8	x86	Y	
		IPF	--	
		x64 Edition (EM64T)	Y	
	Linux 5.0	x86	Y	
		IPF	--	
		x64 Edition (EM64T)	Y	
	Linux 5.1	x86	Y	
		IPF	--	
		x64 Edition (EM64T)	Y	
	Linux 5.2	x86	Y	
		IPF	--	
		x64 Edition (EM64T)	Y	

OS	Version	Architecture	IPv6 Environment Support	Remarks
	Linux 5.3	x86	Y	
		IPF	--	
		x64 Edition (EM64T)	Y	
	Linux 5.4	x86	Y	
		IPF	--	
		x64 Edition (EM64T)	Y	
SUSE Linux Enterprise Server 9	SP1 SP2 SP3 SP4	x86	--	Only the default kernel is supported. Not supported for Provisioning Manager.
SUSE Linux Enterprise Server 10	No SP SP1 SP2 SP3	x86 IPF x64 Edition (EM64T)	--	
SUSE Linux Enterprise Server 11	No SP	x86 IPF x64 Edition (EM64T)	--	
HP-UX	11i v1	PA-RISC (32 and 64 bit)	--	Workstation is not supported. 32-bit is not supported for Provisioning Manager.
	11i v2	PA-RISC (64bit) IPF	Y	Workstation is not supported.
	11i v3	PA-RISC (64bit) IPF	Y	

Legend

Y: Supported.

--: Not supported.

Note: Third-party agents are available for other servers. For the latest information about these agents, please contact your Hitachi Data System representative or refer to documentation about a specific agent.

#1: If Windows Firewall has been enabled, the Device Manager agent must be registered as an exception with Windows Firewall when a new installation of the Device Manager agent is performed. For details on how to do this after installing the agent, see When a Firewall Is Enabled.

#2: The Device Manager agent runs in the usual global environment (global zone) only. If a non-global zone has been created, install the Device Manager agent in the global zone.

#3: The Device Manager agent supports only the Sun Fire x64 server family hardware. In addition, only the 64-bit kernel mode is supported.

Caution: The Device Manager agent only supports global addresses. You cannot use link-local addresses or global unique local addresses (site-local addresses).

Required Patches for Operating Systems

When using the Device Manager agent, it is assumed that the OS patches or succeeding patches listed in tables Table 1-2 to Table 1-9 have been applied. The following tables only list the OSs to which patches must be applied.

Table 1-2 Required Patches for Windows

OS	Architecture	Patches
Windows Server 2003 (No SP)	x64 (EM64T and AMD64)	KB922772
Windows Server 2003 (SP1)	x86 IPF	KB922772
Windows Server 2003 R2 (No SP)	x86	KB922772
	x64 (EM64T and AMD64)	KB922772

Table 1-3 Required Patches and Succeeding Patches for Solaris 8

Required patches	Succeeding patches
108434-22 SunOS 5.8: 32-Bit Shared library patch for C++	108434-23, 108434-24, 108434-25
108435-22 SunOS 5.8: 64-Bit Shared library patch for C++	108435-23, 108435-24, 108435-25
108528-29 SunOS 5.8: kernel update and Apache patch	None.
108773-27 SunOS 5.8: IIIM and X Input & Output Method patch	108773-28
108921-25 CDE 1.4: dtwm patch	108921-26, 108921-27
108940-76 Motif 1.2.7 and 2.1.1: Runtime library patch for Solaris 8	None.
108987-19 SunOS 5.8: Patch for patchadd and patchrm	None.
108989-02 SunOS 5.8: /usr/kernel/sys/acctctl and /usr/kernel/sys/exacctsys patch	None.
109147-44 SunOS 5.8: linker patch	None.
109326-20 SunOS 5.8: libresolv.so.2 and in.named patch	109326-21, 109326-22, 109326-23, 109326-24
110386-04 SunOS 5.8: RBAC Feature Patch	None.
110910-11 SunOS 5.8: /usr/lib/fs/ufs utilities patch	110910-12

Required patches	Succeeding patches
111023-03 SunOS 5.8: /kernel/fs/mntfs and /kernel/fs/sparcv9/mntfs patch	None.
111111-07 SunOS 5.8: /usr/bin/nawk patch	None.
111308-05 SunOS 5.8: /usr/lib/libmtmalloc.so.1 patch	None.
111310-01 SunOS 5.8: /usr/lib/libdhcpagent.so.1 patch	None.
111317-07 SunOS 5.8: /sbin/init and /usr/sbin/init patch	None.
112003-03 SunOS 5.8: Unable to load fontset in 64-bit Solaris 8 iso-1 or iso-15	None.
112396-03 SunOS 5.8: /usr/bin/fgrep patch	None.
112438-03 SunOS 5.8: /kernel/drv/random patch	None.
112472-01 SunOS 5.8: Font2DTest2 abort when Lucida Sans Thai Typewriter selected	None.
113648-04 SunOS 5.8: mount patch	113648-05
113886-48 OpenGL 1.3: OpenGL Patch for Solaris (32-bit)	113886-49
113887-48 OpenGL 1.3: OpenGL Patch for Solaris (64-bit)	113887-49
115827-01 SunOS 5.8: /sbin/sulogin and /sbin/netstrategy patch	None.
116602-01 SunOS 5.8: /sbin/uadmin and /sbin/hostconfig patch	None.
117000-05 SunOS 5.8: Kernel Patch	None.
117350-53 SunOS 5.8: kernel patch	117350-54, 117350-55, 117350-56, 117350-57, 117350-58, 117350-59, 117350-60, 117350-61, 117350-62
119067-09 X11 6.4.1: Xsun patch	119067-10, 119067-11
123478-01 SunOS 5.8: fsck patch	None.
128624-04 SunOS 5.8: LDAP2 client, libc, libthread and libnsl libraries patch	128624-05, 128624-06, 128624-07, 128624-08, 128624-09, 128624-10, 128624-11, 128624-12
Note: The architecture is SPARC (32 or 64 bit). You can also install the required patches by applying J2SE Solaris 8 Recommended Patch Cluster. For details on the latest information, see the Sun Microsystems web site.	

Table 1-4 Required Patches and Succeeding Patches for Solaris 9

Required patches	Succeeding patches
111711-16 SunOS 5.9: 32-bit Shared library patch for C++	111711-17, 111711-18, 111711-19, 111711-20, 111711-21, 111711-22
111712-16 SunOS 5.9: 64-Bit Shared library patch for C++	111712-17, 111712-18, 111712-19, 111712-20, 111712-21, 111712-22
112785-63 X11 6.6.1: Xsun patch	112785-64, 112785-65
112963-32 SunOS 5.9: linker Patch	None.

Required patches	Succeeding patches
113096-03 X11 6.6.1: OWconfig patch	None.
113886-48 OpenGL 1.3: OpenGL Patch for Solaris (32-bit)	113886-49
113887-48 OpenGL 1.3: OpenGL Patch for Solaris (64-bit)	113887-49
Note: The architecture is SPARC (32 or 64 bit). You can also install the required patches by applying J2SE Solaris 9 Recommended Patch Cluster. For details on the latest information, see the Sun Microsystems web site.	

Table 1-5 Required Patches and Succeeding Patches for Solaris 10

Architecture	Required patches	Succeeding patches
SPARC (32 and 64 bit)	118833-36 SunOS 5.10: kernel patch	None.
	118918-24 SunOS 5.10: Solaris Crypto Framework patch	None.
	119042-10 SunOS 5.10: svccfg & svcprop patch	119042-11, 138217-01
	119090-26 SunOS 5.10: Sun iSCSI Device Driver and Utilities	None.
	119254-52 SunOS 5.10: Install and Patch Utilities Patch	119254-53, 119254-54, 119254-55, 119254-56, 119254-57, 119254-58, 119254-59, 119254-60, 119254-61, 119254-62, 119254-63, 119254-64, 119254-65, 119254-66
	119578-30 SunOS 5.10: FMA Patch	None.
	120900-04 SunOS 5.10: libzonecfg Patch	None.
	121133-02 SunOS 5.10: zones library and zones utility patch	None.
	138064-03 SunOS 5.10: pkcs11_softtoken patch#	None.

Architecture	Required patches	Succeeding patches
x64 Edition (AMD64) (Version 1.4.2 of the Java™ execution environment)	119091-27 SunOS 5.10_x86: Sun iSCSI Device Driver and Utilities	None.
	138065-03 SunOS 5.10_x86: pkcs11_softtoken patch#	None.
x64 Edition(AMD64) (Version 5.0 of the Java execution environment)	113000-07 SunOS 5.10_x86: SUNWgrub patch	None.
	117435-02 SunOS 5.10_x86: biosdev patch	None.
	118344-14 SunOS 5.10_x86: Fault Manager Patch	None.
	119091-27 SunOS 5.10_x86: Sun iSCSI Device Driver and Utilities	None.
	119255-50 SunOS 5.10_x86: Install and Patch Utilities Patch	119255-51, 119255-52, 119255-53, 119255-54, 119255-55, 119255-56, 119255-57, 119255-58, 119255-59, 119255-60, 119255-61, 119255-62, 119255-63, 119255-64, 119255-65, 119255-66
	119964-08 SunOS 5.10_x86: Shared library patch for C++_x86	119964-09, 119964-10, 119964-11, 119964-12, 119964-13, 119964-14, 119964-15
	120901-03 SunOS 5.10_x86: libzonecfg patch	None.
	121264-01 SunOS 5.10_x86: cadp160 driver patch	None.
	121334-04 SunOS 5.10_x86: zoneadmd, zlogin and zoneadm patch	None.
	126420-01 SunOS 5.10_x86: umountall patch	140797-01
	138065-03 SunOS 5.10_x86: pkcs11_softtoken patch#	None.

Note: You can also install the required patches by applying J2SE Solaris 10 Recommended Patch Cluster. For details on the latest information, see the Sun Microsystems web site.

#: Apply this patch if you use Solaris 10 11/06 (update 3), Solaris 10 8/07 (update 4), Solaris 10 5/08 (update 5), or Solaris 10 10/08 (update 6). Check the update numbers by referencing the /etc/release file. The following shows an example of the /etc/release file for Solaris 10 11/06.

```
Assembled 14 November 2006
Solaris 10 11/06 s10s_u3wos_10 SPARC
Copyright 2006 Sun Microsystems, Inc.  All Rights Reserved.
Use is subject to license terms.
Assembled 14 November 2006
```

Table 1-6 Required Patches and Succeeding Patches for AIX 5.3

Java execution environment	Required patches	Succeeding patches
Version 1.4.2	5300-02 (APAR IY69190)	5300-03, 5300-04, 5300-05, 5300-06, 5300-07, 5300-08, 5300-09, 5300-10, 5300-11
Version 5.0	5300-03 (APAR IY71011)	5300-04, 5300-05, 5300-06, 5300-07, 5300-08, 5300-09, 5300-10, 5300-11
Note: The architecture is 32 or 64 bit. For details on the latest information, see the IBM web site.		

Table 1-7 Required Patches for Linux

OS	Architecture	Patches
Red Hat Enterprise Linux AS/ES 3	x86 x64 Edition (EM64T)	gdb-5.3.90-0.20030710.40.i386.rpm
	IPF	gdb-5.3.90-0.20030710.40.ia64.rpm
Red Hat Enterprise Linux 5.1	x86 IPF x64 Edition (EM64T)	glibc-2.5-18.el5_1.1 or later nscd-2.5-18.el5_1.1 or later
SUSE Linux Enterprise Server 10	x86 IPF x64 Edition (EM64T)	gdb-6.5-21.2 or later

Table 1-8 Required Patches and Succeeding Patches for HP-UX 11i v1

Required patches	Succeeding patches
PHCO_25226 s700_800 11.11 Initialised TLS, Psets, Mutex performance	PHCO_26466, PHCO_27632, PHCO_29109, PHCO_29960, PHCO_30544, PHCO_33282, PHCO_36229, PHCO_38307
PHCO_25452 s700_800 11.11 libc cumulative patch	PHCO_26124, PHCO_27434, PHCO_27740, PHCO_27910, PHCO_28427, PHCO_29029, PHCO_29287, PHCO_29495, PHCO_29955, PHCO_30030, PHCO_30530, PHCO_31061, PHCO_31903, PHCO_32761, PHCO_33360, PHCO_33533, PHCO_33711, PHCO_34275, PHCO_35743, PHCO_36184, PHCO_37369
PHCO_29960 s700_800 11.11 Pthread enhancement and fixes	PHCO_30544, PHCO_33282, PHCO_36229, PHCO_38307
PHKL_24253 s700_800 11.11 thread nostop patch supporting NFS	PHKL_24569, PHKL_25994, PHKL_30216, PHKL_32061, PHKL_34309, PHKL_35879
PHKL_24254 s700_800 11.11 thread nostop patch supporting NFS	PHKL_24568, PHKL_25728, PHKL_25840, PHKL_27092, PHKL_27294, PHKL_27317, PHKL_29707, PHKL_30032, PHKL_30216, PHKL_32061, PHKL_34309, PHKL_35879
PHKL_24255 s700_800 11.11 thread nostop patch supporting NFS	PHKL_25652, PHKL_25993
PHKL_24256 s700_800 11.11 signal race condition patch/threads enh	PHKL_24567, PHKL_25729, PHKL_28122
PHKL_24257 s700_800 11.11 thread nostop patch supporting NFS	PHKL_23665, PHKL_24551, PHKL_25389, PHKL_27091, PHKL_29706, PHKL_30033, PHKL_30587, PHKL_31993, PHKL_33328, PHKL_33336, PHKL_34310, PHKL_35281, PHKL_36948

Required patches	Succeeding patches
PHKL_24751 s700_800 11.11 preserve IPSW W-bit and GR31 lower bits	None.
PHKL_25227 s700_800 11.11 VM/JFS deadlock; mmap performance/defect	PHKL_25614, PHKL_26233, PHKL_27278, PHKL_28267, PHKL_28428, PHKL_28990, PHKL_30158, PHKL_30616, PHKL_31003, PHKL_32578, PHKL_32806, PHKL_33261, PHKL_33270, PHKL_33988, PHKL_35464, PHKL_35564
PHKL_25367 s700_800 11.11 Priority inversion and thread hang	PHKL_26468, PHKL_27316, PHKL_30837, PHKL_34534, PHKL_38299, PHKL_38430
PHKL_25468 s700_800 11.11 eventport (/dev/poll) pseudo driver	PHKL_30542
PHKL_25614 s700_800 11.11 VM-JFS deadlock, mmap, perf thread creation	PHKL_26233, PHKL_27278, PHKL_28267, PHKL_28428, PHKL_28990, PHKL_30158, PHKL_30616, PHKL_31003, PHKL_32578, PHKL_32806, PHKL_33261, PHKL_33270, PHKL_33988, PHKL_35464, PHKL_35564
PHKL_25728 s700_800 11.11 Psets Enablement, thread cumulative	PHKL_25840, PHKL_27092, PHKL_27294, PHKL_27317, PHKL_29707, PHKL_30032, PHKL_30216, PHKL_32061, PHKL_34309, PHKL_35879
PHKL_25729 s700_800 11.11 signals, threads enhancement, Psets Enablement	PHKL_28122
PHKL_25840 s700_800 11.11 Thread NOSTOP, Psets, Thread Abort	PHKL_27092, PHKL_27294, PHKL_27317, PHKL_29707, PHKL_30032, PHKL_30216, PHKL_32061, PHKL_34309, PHKL_35879
PHKL_25842 s700_800 11.11 Thread Abort	PHKL_30288, PHKL_34311
PHKL_25871 s700_800 11.11 eventport syscalls;socket close(2) hang fix	PHKL_25995, PHKL_29826, PHKL_30317, PHKL_30541, PHKL_30557, PHKL_32374, PHKL_32457, PHKL_34024, PHKL_35091, PHKL_37753, PHKL_39133
PHKL_27091 s700_800 11.11 Core PM, vPar, Psets Cumulative, slpq1 perf	PHKL_29706, PHKL_30033, PHKL_30587, PHKL_31993, PHKL_33328, PHKL_33336, PHKL_34310, PHKL_35281, PHKL_36948 PHKL_29706, PHKL_30033, PHKL_30587, PHKL_31993, PHKL_33328, PHKL_33336, PHKL_34310, PHKL_35281, PHKL_36948
PHKL_27092 s700_800 11.11 Thread NOSTOP, Abort; Psets	PHKL_27294, PHKL_27317, PHKL_29707, PHKL_30032, PHKL_30216, PHKL_32061, PHKL_34309, PHKL_35879
PHKL_28489 s700_800 11.11 copyin EFAULT, LDCD access type	None.
PHKL_32457 s700_800 11.11 SPP fragmentation;AIO;EVP;ufalloc;dup2 race	PHKL_34024, PHKL_35091, PHKL_37753
PHKL_32927 s700_800 11.11 PA-8800 Fix Java (64-bit JVM) process hang	PHKL_36763
PHKL_34534 s700_800 11.11 vPar,callout, abstime, sync perf, wakeup	PHKL_38299, PHKL_38430

Required patches	Succeeding patches
PHNE_23502 s700_800 11.11 ONC/NFS General Release/Performance Patch	PHNE_24035, PHNE_24910, PHNE_25625, PHNE_25627, PHNE_26388, PHNE_27218, PHNE_28103, PHNE_28568, PHNE_28983, PHNE_29211, PHNE_29303, PHNE_29783, PHNE_29883, PHNE_30378, PHNE_30380, PHNE_30661, PHNE_31097, PHNE_31929, PHNE_32477, PHNE_32811, PHNE_33315, PHNE_33498, PHNE_33971, PHNE_34293, PHNE_34662, PHNE_34938, PHNE_35418, PHNE_35871, PHNE_36168, PHNE_37110, PHNE_37568
PHNE_25084 s700_800 11.11 Cumulative STREAMS Patch	PHNE_26728, PHNE_27703, PHNE_28476, PHNE_29825, PHNE_30367, PHNE_31091, PHNE_33313, PHNE_33729, PHNE_34131, PHNE_34777, PHNE_35453, PHNE_36576
PHNE_29887 s700_800 11.11 cumulative ARPA Transport patch	PHNE_31247, PHNE_33159, PHNE_33628, PHNE_34135, PHNE_34672, PHNE_35183, PHNE_35351, PHNE_36125, PHNE_37671, PHNE_37898
PHSS_24932 s700_800 11.11 Japanese TrueType font patch	PHSS_26971
PHSS_24934 s700_800 11.11 Korean TrueType font patch	PHSS_26973
PHSS_24936 s700_800 11.11 Chinese-S TrueType font patch for 11.11	PHSS_26975
PHSS_25449 s700_800 11.11 X/Motif Runtime OCT2001 Periodic Patch	PHSS_25881, PHSS_27234, PHSS_27425, PHSS_28370, PHSS_28875, PHSS_29371, PHSS_30262, PHSS_30787, PHSS_31000, PHSS_33130, PHSS_35711, PHSS_37028
PHSS_25881 s700_800 11.11 X/Motif Runtime JAN2002 Periodic Patch	PHSS_27234, PHSS_27425, PHSS_28370, PHSS_28875, PHSS_29371, PHSS_30262, PHSS_30787, PHSS_31000, PHSS_33130, PHSS_35711, PHSS_37028
PHSS_30049 s700_800 11.11 ld(1) and linker tools cumulative patch	PHSS_30966, PHSS_30968, PHSS_30970, PHSS_32864, PHSS_33033, PHSS_33035, PHSS_33037, PHSS_35379, PHSS_35381, PHSS_35383, PHSS_35385, PHSS_37516, PHSS_37517, PHSS_38154, PHSS_39077
Note: The architecture is PA-RISC (32 or 64 bit). Depending on the OS release date, required patches might have been applied at the time of delivery. For details on the latest information, see the HP web site.	

Table 1-9 Required Patches and Succeeding Patches for HP-UX 11i v2

Architecture	Required patches	Succeeding patches
PA-RISC(64bit) (Version 5.0 of the Java execution environment)	PHKL_35029 s700_800 11.23 ksleep cumulative patch	PHKL_36826, PHKL_37121

Architecture	Required patches	Succeeding patches
IPF (Version 1.4.2 of the Java execution environment)	PHCO_30476 s700_800 11.23 Pthread library patch	PHCO_30543, PHCO_31553, PHCO_32489, PHCO_33675, PHCO_34718, PHCO_34944, PHCO_35997, PHCO_36323, PHCO_37543, PHCO_37940, PHCO_38955
	PHKL_30192 s700_800 11.23 Eliminate race at MxN kernel thread creation	PHKL_31500
	PHSS_30015 s700_800 11.23 Aries cumulative patch	PHSS_30237, PHSS_30674, PHSS_30779, PHSS_31816, PHSS_32213, PHSS_32502, PHSS_34201, PHSS_35045, PHSS_35528, PHSS_36519, PHSS_37552, PHSS_38526
	PHSS_34201 s700_800 11.23 Aries cumulative patch	PHSS_35045, PHSS_35528, PHSS_36519, PHSS_37552, PHSS_38526
IPF (Version 5.0 of the Java execution environment)	PHCO_30476 s700_800 11.23 Pthread library patch	PHCO_30543, PHCO_31553, PHCO_32489, PHCO_33675, PHCO_34718, PHCO_34944, PHCO_35997, PHCO_36323, PHCO_37543, PHCO_37940, PHCO_38955
	PHKL_30192 s700_800 11.23 Eliminate race at MxN kernel thread creation	PHKL_31500
	PHKL_35029 s700_800 11.23 ksleep cumulative patch	PHKL_36826, PHKL_37121
	PHSS_30015 s700_800 11.23 Aries cumulative patch	PHSS_30237, PHSS_30674, PHSS_30779, PHSS_31816, PHSS_32213, PHSS_32502, PHSS_34201, PHSS_35045, PHSS_35528, PHSS_36519, PHSS_37552, PHSS_38526
	PHSS_33349 s700_800 11.23 linker + fdp cumulative patch	PHSS_34040, PHSS_34353, PHSS_34440, PHSS_34858, PHSS_34860, PHSS_35979, PHSS_36336, PHSS_36342, PHSS_37201, PHSS_37492, PHSS_37947, PHSS_38134, PHSS_39093
	PHSS_33350 s700_800 11.23 aC++ Runtime	PHSS_34041, PHSS_34441, PHSS_35055, PHSS_35978, PHSS_36343, PHSS_37500, PHSS_38140
	PHSS_34043 s700_800 11.23 Integrity Unwind Library	PHSS_34854, PHSS_34859, PHSS_36345, PHSS_37039, PHSS_37498, PHSS_37953, PHSS_38138, PHSS_39101
	PHSS_34201 s700_800 11.23 Aries cumulative patch	PHSS_35045, PHSS_35528, PHSS_36519, PHSS_37552, PHSS_38526
Note: Depending on the OS release date, required patches might have been applied at the time of delivery. For details on the latest information, see the HP web site.		

Precautions for Using Provisioning Manager

Keep the following in mind for use with Provisioning Manager:

- Host configuration (creation, expansion, and deletion of file systems, and creation and deletion of device files) is supported for host OSs of the following language versions:

  For Windows Server 2003 (x86), or Windows Server 2003 R2

  English, French, German, Italian, Spanish, Simplified Chinese, Traditional Chinese, Korean, Japanese, Portuguese, Brazilian (Portuguese Brazilian), and Swedish

  For Windows Server 2003 (IPF), or Windows Server 2003 (x64)

  English and Japanese

  For Windows Server 2008

  English, French, German, Italian, Spanish, Simplified Chinese, Traditional Chinese, Korean, Japanese, Portuguese, and Brazilian (Portuguese Brazilian)

  For Windows Server 2008 R2

  English, French, German, Italian, Spanish, Simplified Chinese, Korean, Japanese, and Portuguese

  Host configuration cannot be performed in the following two cases even if the OS is one of the above language versions:

  – When the Multilingual User Interface Pack has been applied.

  – When the language settings of the system have been changed.

  Host, file system, and device file settings can be viewed from the server no matter what language version of Windows is on the agent host.

- If the host OS is HP-UX, Provisioning Manager will not support environments containing or allowing mirror volumes.

  For HP-UX 11i v2 or earlier:

  If MirrorDisk/UX is installed on the host, Provisioning Manager functionality cannot be used to view host information and perform host settings.

  For HP-UX 11i v3:

  MirrorDisk/UX is installed on the host by OS default. In this case, Provisioning Manager functionality can be used to view host information and perform host settings.

  Note that software RAIDs using MirrorDisk/UX are not supported.

- When the host OS is HP-UX, in the `/etc/lvmconf` directory, LVM creates a backup file for the configuration information about volume groups. Therefore, to create a volume group by using the host management functionality of Provisioning Manager, a maximum of 500 MB of free disk space (when 255 volume groups are created) is additionally required under `/etc/lvmconf`.

Prerequisite Java Execution Environments

If the host OS is Solaris, AIX, or HP-UX, you need software that provides a Java execution environment on the host before installing the Device Manager agent. Download the software from your OS vendor site, and then install it.

Note: If the host OS is Windows or Linux, use JRE 5.0, which is automatically installed with the Device Manager agent.

The following table shows the prerequisite Java execution environments for Device Manager agents.

Table 1-10 Required Java Execution Environments

OS	Architecture	Java Execution Environment
Solaris	SPARC (32 and 64 bit)	For IPv4 environment operation: JDK™ 1.4.2_*xx* (*xx* is 15 or later) JDK 5.0 (Update 11 or later) For IPv6 environment operation: JDK 5.0 (Update 11 or later)
	AMD64	JDK 5.0 (Update 11 or later)
AIX	32 bit 64 bit	For IPv4 environment operation: JDK 1.4.2 (Update 8 or later) JDK 5.0 (Update 5 or later) For IPv6 environment operation: JDK 5.0 (Update 5 or later)
HP-UX	PA-RISC (32 and 64 bit) IPF	For IPv4 environment operation: JDK 1.4.2_*xx* (*xx* is 17 or later) RTE 1.4.2_*xx* (*xx* is 17 or later) JDK 5.0 (Update 11 or later) JRE 5.0 (Update 11 or later) For IPv6 environment operation: JDK 5.0 (Update 11 or later) JRE 5.0 (Update 11 or later)

Note: Use a package program instead of a self-expanding program. If both version 1.4.2 and version 5.0 are installed, the Device Manager agent uses version 5.0 of the Java execution environment.

Use the following commands to check the versions of the listed software products, which provide a Java execution environment.

Table 1-11 Commands for Checking the Version of the Software that Provides a Java Execution Environment

OS	Software That Provides a Java Execution Environment	Command
Solaris	JDK 1.4.2	`pkginfo -li SUNWj3rt`
	JDK 5.0	`pkginfo -li SUNWj5rt`
AIX	JDK 1.4.2 (32 bit)	`lslpp -l Java14.sdk`
	JDK 1.4.2 (64 bit)	`lslpp -l Java14_64.sdk`
	JDK 5.0 (32 bit)	`lslpp -l Java5.sdk`
	JDK 5.0 (64 bit)	`lslpp -l Java5_64.sdk`
HP-UX	JDK 1.4.2	`swlist T1456AA`
	RTE 1.4.2	`swlist T1457AA`
	JDK 5.0	`swlist Java15JDK`
	JRE 5.0	`swlist Java15JRE`

Caution:

When updating the software that provides a Java execution environment (after installing the Device Manager agent), temporarily stop the Device Manager agent service before proceeding with any updates. Also, when changing the installation path of the software that provides a Java execution environment, you must modify the `server.agent.JRE.location` setting in the `server.properties` file.

For details about stopping and starting the Device Manager agent service, see Managing the Operating Status of the Device Manager Agent Service. For details about the `server.properties` file, see The server.properties File.

Supported Virtualization Software

You can install the Device Manager agent on a guest OS on a virtualization server. Note that the Device Manager agent should be installed on either a virtualization server (host OS) or the virtual machines (guest OS or VIO client).

Virtualization Software

The Device Manager agent can also run on the guest OSs or the VIO clients of the virtualization software in the following table.

Table 1-12 Supported Virtualization Software

Guest OS or VIO Client	Version	Architecture	Virtualization Software
Windows Server 2003	No SP	x86 x64 Edition (EM64T and AMD64)	▪ VMware® ESX 3.*x* ▪ VMware ESX 4.*x* ▪ VMware ESXi 3.*x* ▪ VMware ESXi 4.*x*
	SP1	x86	
	SP2	x86 x64 Edition (EM64T and AMD64)	▪ VMware ESX 3.*x* ▪ VMware ESX 4.*x* ▪ VMware ESXi 3.*x* ▪ VMware ESXi 4.*x* ▪ Windows Server 2008 (Hyper-V™) ▪ Windows Server 2008 R2 (Hyper-V2)
Windows Server 2003 R2	No SP	x86 x64 Edition (EM64T and AMD64)	▪ VMware ESX 3.*x* ▪ VMware ESX 4.*x* ▪ VMware ESXi 3.*x* ▪ VMware ESXi 4.*x*
	SP2	x86 x64 Edition (EM64T and AMD64)	▪ VMware ESX 3.*x* ▪ VMware ESX 4.*x* ▪ VMware ESXi 3.*x* ▪ VMware ESXi 4.*x* ▪ Windows Server 2008 (Hyper-V) ▪ Windows Server 2008 R2 (Hyper-V2)
Windows Server 2008	No SP SP2	x86 x64 Edition (EM64T and AMD64)	▪ VMware ESX 3.*x* ▪ VMware ESX 4.*x* ▪ VMware ESXi 3.*x* ▪ VMware ESXi 4.*x* ▪ Windows Server 2008 (Hyper-V) ▪ Windows Server 2008 R2 (Hyper-V2)
Windows Server 2008 R2	No SP	x64 Edition (EM64T and AMD64)	▪ VMware ESX 3.*x* ▪ VMware ESX 4.*x* ▪ VMware ESXi 3.*x* ▪ VMware ESXi 4.*x* ▪ Windows Server 2008 (Hyper-V) ▪ Windows Server 2008 R2 (Hyper-V2)
Solaris	10	SPARC (32 and 64 bit)	▪ Solaris 10 (SPARC) (Logical Domains 1.2 or 1.3)
AIX	5.3	32 bit 64 bit	▪ AIX 6.1 (VIO 2.1.1)#
	6.1	64 bit	
#: HBAs that support NPIV are required. Use HBAs that support NPIV to assign LUs to the VIO client.			

When running the Device Manager agent on a guest OS or a VIO client, be sure to take into account the number of LUs managed by the virtual machines in order to allocate a sufficient amount of memory to the guest OS or the VIO client. As for the Device Manager agent configuration, follow the configuration recommendations. For details on the amount of memory required for the Device Manager agent, see Specifying Settings When a Host Manages 100 or More LUs.

Virtualization Server Configuration

Install the Device Manager agent either on a virtualization server or a virtual machine running on that server, but not both. You can use the Device Manager agent in the configurations described below. Consider the features of the configurations, and then choose the appropriate one.

Caution:

To use Replication Manager, install the Device Manager agent on a virtualization server or a virtual machine on which CCI will be installed.

- The Device Manager agent is installed on a virtual machine

  To use this configuration, you need to map a RAW device to a virtual machine. Use one of the following configurations based on the configuration of the virtual machine and HBAs.

  – If an HBA is assigned to each virtual machine:

    Install the Device Manager agent on each virtual machine.

    When using this configuration, in the *host-name* subwindow of Device Manager Web Client, if you select a virtual machine, you can view the LDEV information for that virtual machine.

    For example, when using the configuration shown in Figure 1-1, if you select the virtual machine A in Web Client, information for LUN:01 and LUN:02 is displayed. If you select the virtual machine B, information for LUN:03 and LUN:04 is displayed.

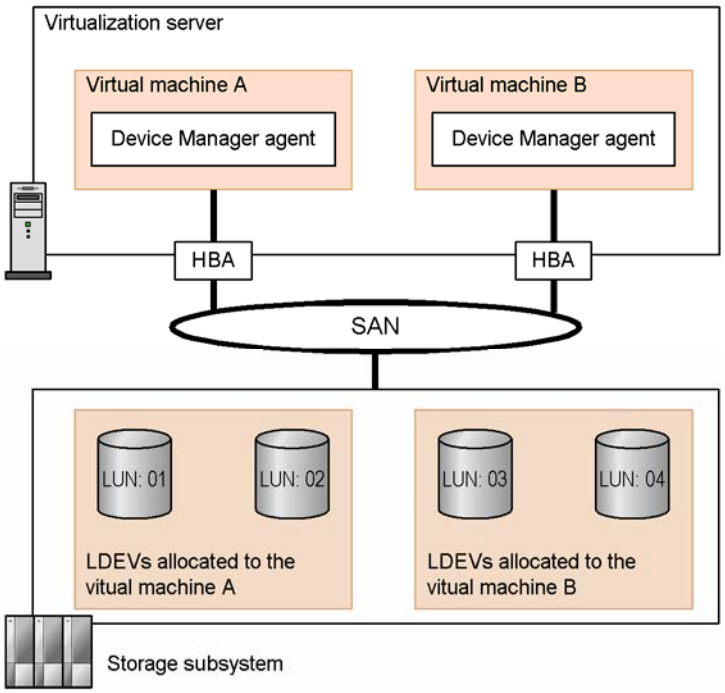

Figure 1-1 Configuration of the Device Manager Agent When an HBA Is Assigned to Each Virtual Machine

– If a virtual HBA or virtual WWN is assigned to each virtual machine:

  If HBAs that support NPIV are used, a virtual HBA or a virtual WWN is assigned to each virtual machine. When you use this configuration, install a Device Manager agent on each virtual machine. In addition, register a virtualization server in the Device Manager server.

  In the *host-name* subwindow of Device Manager Web Client, you can view the LDEV information for each virtual machine to which a virtual HBA has been assigned.

  For example, when you use the configuration shown in Figure 1-2, if you select virtual machine A in Web Client, information for `LUN:01` and `LUN:02` is displayed. If you select virtual machine B, information for `LUN:03` and `LUN:04` is displayed.

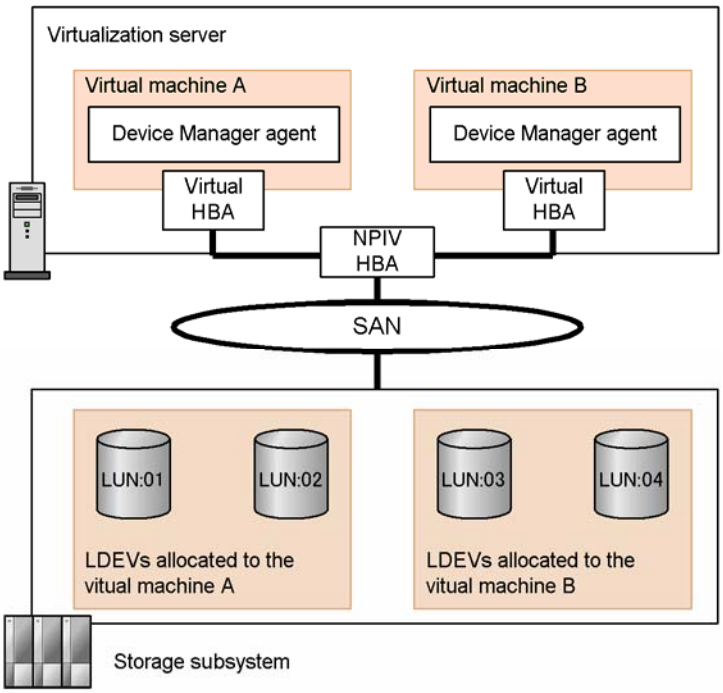

Figure 1-2 Configuration of Device Manager Agent When a Virtual HBA Is Assigned to Each Virtual Machine

– If an HBA is shared by multiple virtual machines:

  Install the Device Manager agent on only one of the virtual machines.

  When using this configuration, in the *host-name* subwindow of Device Manager Web Client, if you select a virtual machine on which the Device Manager agent is installed, you can see information for all LDEVs allocated to the virtualization server. However, information such as the amount of usage and mount point information is displayed in Web Client only for the LDEVs allocated to the virtual machine on which the Device Manager agent is installed.

  For example, when using the configuration shown in Figure 1-3, if you select the virtual machine A in Web Client, LDEV information is displayed for all of LUN:01 through LUN:04, but usage and mount point information is not displayed for LUN:03 and LUN:04.

Notes: If you use this configuration, we recommend that you use Device Manager to assign a label to each LDEV so that in Web Client you can easily determine which LDEV is allocated to which virtual machine.

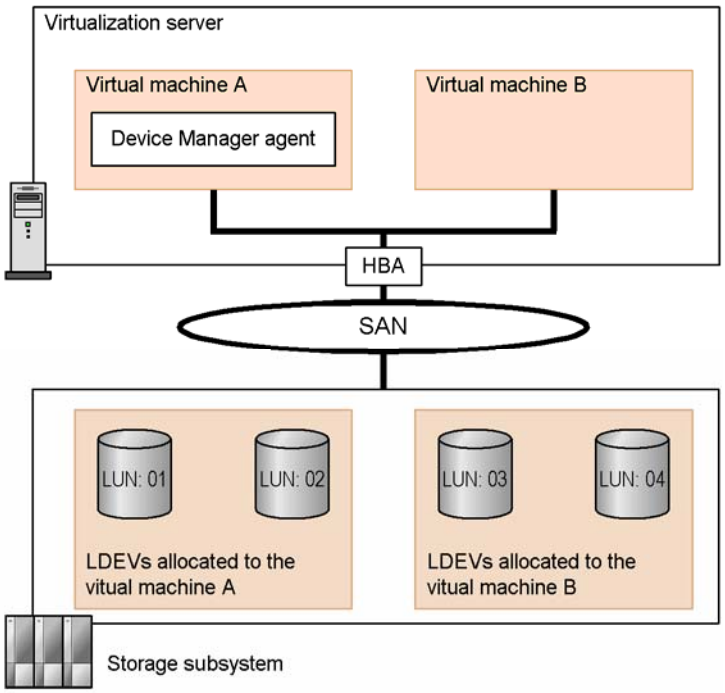

Figure 1-3 Configuration of the Device Manager Agent When an HBA Is Shared by Multiple Virtual Machines

- Device Manager agent is installed on a virtualization server

  When using this configuration, the Device Manager agent manages the virtualization server as if it were a normal application server. Note that, LDEV information such as usage or mount point information is not displayed in Web Client because the Device Manager agent does not recognize virtual machines on a virtualization server.

  For example, when using the configuration shown in Figure 1-4, LDEV information for LUN:01 through LUN:04, which are allocated to the virtual machines, is not displayed in Web Client.

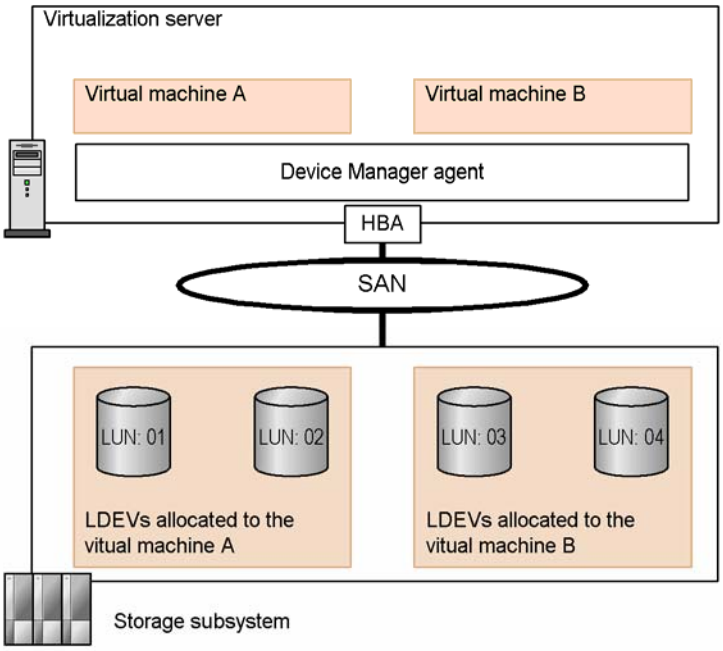

Figure 1-4 Configuration of the Device Manager Agent When an HBA Is Shared by Multiple Virtualization Servers

Note that, if a virtual machine on VMware ESX uses a volume in the storage subsystem, you must define that volume as Mapped Raw LUN. Otherwise, the Device Manager agent does not update the Device Manager server with information about that volume. For details, see the VMware ESX documentation.

Using VMotion™ on a VMware ESX

If you migrate a virtual machine running the Device Manager agent to another computer using VMotion, you must refresh the host information either by executing the `HiScan` command or by refreshing a host from a Web Client. After you have refreshed the host information, use Web Client to delete the WWN or iSCSI names from the computer of which the virtual machine was migrated.

If the WWN or iSCSI name is not deleted, available volume candidates are not displayed in the Web Client when file systems or device files are added or expanded using the Provisioning Manager.

Using Logical Domains

If you export a physical disk of the service domain as a virtual disk of the guest domain, specify the full disk. If you specify a single slice disk instead, information about the virtual disk cannot be acquired correctly.

Supported File Systems

The following table lists the file systems supported by the Device Manager agent. However, depending on the combination of OS and file system, you might not be able to use Provisioning Manager to manage or use these.

Table 1-13 Supported File Systems

OS	File System	Description
Windows	NTFS	Standard OS file system. If you use Provisioning Manager to manage this type of file system, you need to use a dynamic disk or basic disk for the volume manager. However, if you use a basic disk, you cannot expand file systems by using Provisioning Manager. Also, if you use a dynamic disk, you can expand file systems only when they are mounted.
	FAT	Standard OS file system. Provisioning Manager only allows the file system to be displayed.
	FAT32	
Solaris	UFS	Standard OS file system. Provisioning Manager does not allow the file system to be expanded.
	Veritas File System	One of the following versions needs to be used for management by Provisioning Manager: ▪ For Solaris 8: VERITAS File System 3.5 VERITAS File System 4.0 ▪ For Solaris 9: VERITAS File System 3.5 VERITAS File System 4.0 Veritas File System 5.0 ▪ For Solaris 10 (SPARC edition): Veritas File System 5.0 ▪ For Solaris 10 (x64 Edition (AMD64)): VERITAS File System 4.1 Use the same version of Veritas Volume Manager as the Veritas File System used on the volume manager. Note that file systems can only be expanded when mounted.
AIX	JFS	Standard OS file system. Note that file systems can only be expanded when mounted.
Red Hat Enterprise Linux	ext2 ext3	Standard OS file system. Note that file systems can only be expanded when mounted. When the file system is expanded, it is temporarily unmounted. The file system cannot be expanded online. When a file system is expanded, stop all jobs.

OS	File System	Description
SUSE Linux Enterprise Server	ext2 ext3	Standard OS file system. Provisioning Manager is not supported on SUSE Linux Enterprise Server.
HP-UX	Veritas File System (JFS#)	The following versions need to be used for management by Provisioning Manager: ▪ For HP-UX 11i v1: VERITAS File System 3.5. ***Note:*** To enable VERITAS File System 3.5, install a version of Software Pack (Optional HP-UX 11i v1 Core Enhancements) that was released in or after December 2002. ▪ For versions released before the December 2005 version of HP-UX 11i v2: VERITAS File System 3.5 (OS default) ▪ For the December 2005 and later versions of HP-UX 11i v2: VERITAS File System 4.1 (OS default) ▪ For HP-UX 11i v3: VERITAS File System 4.1 (OS default) Note that file systems can only be expanded when mounted.
	HFS	Standard OS file system. Provisioning Manager only allows the file system to be displayed.

#: This includes HP OnlineJFS and HP JFS, which are recognized as Veritas File System on a host.

A file system can be expanded in the online mode by using Provisioning Manager, if a Device Manager agent version 5.1.0 or later and HP OnlineJFS are installed on the host. When you install HP OnlineJFS, make sure you do the following:

- Install a version of HP OnlineJFS that is the same as the version of Veritas File System.

  Provisioning Manager only supports an environment where the versions of Veritas File System and HP OnlineJFS are the same.
- Enable HP OnlineJFS.

  If HP OnlineJFS is disabled, you cannot use Provisioning Manager to expand file systems.

If a Device Manager agent version earlier than 5.1.0 is installed on the host, or HP OnlineJFS is not installed on the host, the file system is unmounted during expansion, so it cannot be expanded in the online mode. When a file system is expanded, stop all jobs.

Note: ZFS, which is a standard OS file system for Solaris 10 Update 2 or later, cannot be managed by Provisioning Manager.

Supported Volume Managers

The following table lists volume managers supported by the Device Manager agent. Note that the table only lists OSs that support volume managers.

Table 1-14 Supported Volume Managers

OS	Version	Architecture	Volume Manager	
			Used with Device Manager	Used with Provisioning Manager
Windows Server 2003	No SP	x86 IPF x64 Edition (EM64T and AMD64)	▪ Basic ▪ Dynamic	▪ Basic[#1] ▪ Dynamic
	SP1	x86	▪ Basic ▪ Dynamic ▪ VERITAS Volume Manager 4.3	▪ Basic[#1] ▪ Dynamic
		IPF	▪ Basic ▪ Dynamic	▪ Basic[#1] ▪ Dynamic
	SP2	x86 IPF x64 Edition (EM64T and AMD64)	▪ Basic ▪ Dynamic	▪ Basic[#1] ▪ Dynamic
Windows Server 2003 R2	No SP SP2	x86 x64 Edition (EM64T and AMD64)	▪ Basic ▪ Dynamic	▪ Basic[#1] ▪ Dynamic
Windows Server 2008	No SP SP2	x86 IPF x64 Edition (EM64T and AMD64)	▪ Basic ▪ Dynamic	▪ Basic[#1] ▪ Dynamic
Windows Server 2008 R2	No SP	IPF x64 Edition (EM64T and AMD64)	▪ Basic ▪ Dynamic	▪ Basic[#1] ▪ Dynamic

OS	Version	Architecture	Volume Manager	
			Used with Device Manager	Used with Provisioning Manager
Solaris	8	SPARC (32 or 64 bit)	▪ SDS 4.2.1 ▪ VERITAS Volume Manager 3.2 ▪ VERITAS Volume Manager 3.5 ▪ VERITAS Volume Manager 4.0	▪ SDS 4.2.1[#2] ▪ VERITAS Volume Manager 3.5[#2] ▪ VERITAS Volume Manager 4.0[#2]
	9	SPARC (32 or 64 bit)	▪ SVM 1.0 ▪ VERITAS Volume Manager 3.5 ▪ VERITAS Volume Manager 4.0 ▪ VERITAS Volume Manager 4.1 ▪ Veritas Volume Manager 5.0	▪ SVM 1.0[#2] ▪ VERITAS Volume Manager 3.5[#2] ▪ VERITAS Volume Manager 4.0[#2] ▪ Veritas Volume Manager 5.0[#2]
	10	SPARC (32 or 64 bit)	▪ SVM 1.0 ▪ VERITAS Volume Manager 4.1 MP2[#3] ▪ Veritas Volume Manager 5.0[#3] ▪ Veritas Volume Manager 5.0 MP1[#3]	▪ SVM 1.0[#2] ▪ VERITAS Volume Manager 4.1 MP2[#2#3] ▪ Veritas Volume Manager 5.0[#2#3] ▪ Veritas Volume Manager 5.0 MP1[#2#3]
		x64 Edition (AMD64)	▪ SVM 1.0 ▪ VERITAS Volume Manager 4.1 ▪ VERITAS Volume Manager 4.1 MP2 ▪ Veritas Volume Manager 5.0 MP1	▪ SVM 1.0[#2] ▪ VERITAS Volume Manager 4.1[#2] ▪ VERITAS Volume Manager 4.1 MP2[#2] ▪ Veritas Volume Manager 5.0 MP1[#2]
AIX	5.3	32 bit 64 bit	LVM	LVM
	6.1	64 bit	LVM	LVM
Red Hat Enterprise Linux	Linux AS/ES 3	x86	LVM	LVM
		IPF x64 Edition (EM64T)	LVM	Unsupported
	Linux AS/ES 4	x86 IPF x64 Edition (EM64T)	LVM2	LVM2
	Linux 5	x86 IPF x64 Edition (EM64T)	LVM2	LVM2

OS	Version	Architecture	Volume Manager	
			Used with Device Manager	Used with Provisioning Manager
SUSE Linux Enterprise Server	9	x86	LVM2	Unsupported
	10	x86 IPF x64 Edition (EM64T)	LVM2	Unsupported
	11	x86 IPF x64 Edition (EM64T)	LVM2	Unsupported
HP-UX	11i v1	PA-RISC (32 or 64 bit)	▪ LVM ▪ VERITAS Volume Manager 3.5	▪ LVM ▪ VERITAS Volume Manager 3.5#4
	11i v2 (for versions earlier than 12/2005)	PA-RISC (64 bit) IPF	▪ LVM ▪ VERITAS Volume Manager 3.5 ▪ VERITAS Volume Manager 4.1	▪ LVM ▪ VERITAS Volume Manager 3.5#4
	11i v2 (for versions later than or equal to 12/2005)	PA-RISC (64 bit) IPF	▪ LVM ▪ VERITAS Volume Manager 3.5 ▪ VERITAS Volume Manager 4.1	▪ LVM ▪ VERITAS Volume Manager 3.5#4 ▪ VERITAS Volume Manager 4.1#4
	11i v3	PA-RISC (64 bit) IPF	▪ LVM ▪ LVM2#5 ▪ LVM2.1#5 ▪ VERITAS Volume Manager 4.1	▪ LVM ▪ LVM2#5 ▪ LVM2.1#5 ▪ VERITAS Volume Manager 4.1#4

Note: To use Provisioning Manager to perform operations on file systems or device files (creation, expansion, or deletion), you must install a volume manager on each host.

#1: File systems cannot be expanded by using Provisioning Manager.

#2: If the host OS is Solaris, you can use Provisioning Manager to display, create and delete file systems and device files, even without a volume manager. However, Provisioning Manager cannot expand file systems created without using Veritas Volume Manager, and can only display file systems and device files that are created by using SDS or SVM. If a host is not the owner of a SDS/SVM diskset, information about the logical volumes and file systems related to that diskset is not displayed.

#3: Logical domains cannot be used.

#4: Provisioning Manager can only display file systems and device files that are created by using Veritas Volume Manager.

#5: Device Manager agent version 6.4 supports volume groups whose version is up to 2.1. Therefore, even if an LVM that supports volume groups whose version is higher than 2.1 is installed on a host, the file systems and device files will be created as volume groups of version 2.1.

Caution: Even if the Device Manager agent is installed on the host, the Web Client LU usage rate will not be displayed in the following cases:

- Windows is the OS on the host using the LUs, and LUs or LU partitions are subject to dynamic disk management.
- Solaris is the OS on the host using the LUs, and LUs are managed by SDS, SVM, or Veritas Volume Manager.
- The OS on the host using the LUs is AIX.
- Linux is the OS on the host using the LUs, and LUs satisfy one of the following conditions:
  - The LUs are managed by LVM or LVM2.
  - The LUs are partitioned, and some of the LU partitions are managed by a volume manager.
- The OS on the host using the LUs is HP-UX, and the LUs are managed by LVM.

Supported Path Management Software

Path management software is required when path redundancy is used between host ports and storage subsystem ports to increase system reliability and availability. The following table lists the path management software supported by the Device Manager agent. Note that the table only lists OSs that support path management software.

Table 1-15 Supported Path Management Software

OS	Version	Architecture	Path Management Software	
			Used with Device Manager	Used with Provisioning Manager
Windows Server 2003	No SP	x86 IPF	Dynamic Link Manager 05-01 to 6.4.0	Dynamic Link Manager 05-02 to 6.4.0
		x64 Edition (EM64T and AMD64)	Dynamic Link Manager 5.7 to 6.4.0	Dynamic Link Manager 5.7 to 6.4.0
	SP1	x86 IPF	Dynamic Link Manager 5.4 to 6.4.0	Dynamic Link Manager 05-60 to 6.4.0
	SP2	x86 IPF x64 Edition (EM64T and AMD64)	Dynamic Link Manager 5.9 to 6.4.0	Dynamic Link Manager 5.9 to 6.4.0
Windows Server 2003 R2	No SP	x86 x64 Edition (EM64T and AMD64)	Dynamic Link Manager 5.8 to 6.4.0	Dynamic Link Manager 5.8 to 6.4.0
	SP2	x86 x64 Edition (EM64T and AMD64)	Dynamic Link Manager 5.9 to 6.4.0	Dynamic Link Manager 5.9 to 6.4.0
Windows Server 2008	No SP	x86 IPF x64 Edition (EM64T and AMD64)	Dynamic Link Manager 5.9.5 to 6.4.0	Dynamic Link Manager 5.9.5 to 6.4.0
	SP2	x86 IPF x64 Edition (EM64T and AMD64)	Dynamic Link Manager 6.1.0 to 6.4.0	Dynamic Link Manager 6.1.0 to 6.4.0
Windows Server 2008 R2	No SP	IPF x64 Edition (EM64T and AMD64)	Dynamic Link Manager 6.2.0 to 6.4.0	Dynamic Link Manager 6.2.0 to 6.4.0

OS	Version	Architecture	Path Management Software	
			Used with Device Manager	Used with Provisioning Manager
Solaris	8	SPARC (32 and 64 bit)	▪ Dynamic Link Manager 03-00 ▪ Dynamic Link Manager 03-02 ▪ Dynamic Link Manager 04-00 to 6.4.0	When VERITAS Volume Manager 3.5 is used: Dynamic Link Manager 04-01-/B Dynamic Link Manager 05-02 to 6.4.0 When VERITAS Volume Manager 4.0 is used: Dynamic Link Manager 05-41 to 6.4.0
	9	SPARC (32 and 64 bit)	▪ VERITAS Volume Manager 4.0 (Dynamic Multi-Pathing) ▪ VERITAS Volume Manager 4.1 (Dynamic Multi-Pathing) ▪ Dynamic Link Manager 04-01 to 6.4.0 ▪ Sun StorEdge Traffic Manager 6.2.6	When VERITAS Volume Manager 3.5 is used: Dynamic Link Manager 04-01-/B Dynamic Link Manager 05-02 to 6.4.0 When VERITAS Volume Manager 4.0 is used: Dynamic Link Manager 05-41 to 6.4.0 When VERITAS Volume Manager 5.0 is used: Dynamic Link Manager 05-62 to 6.4.0
	10	SPARC (32 and 64 bit)	▪ Dynamic Link Manager 5.6.1 to 6.4.0 ▪ Sun StorEdge Traffic Manager	Unsupported
		x64 Edition (AMD64)	Sun StorEdge Traffic Manager	Unsupported
AIX	5.3	32 bit 64 bit	▪ Dynamic Link Manager 05-41 to 6.4.0 ▪ MPIO	Dynamic Link Manager 05-41 to 6.4.0
	6.1	64 bit	Dynamic Link Manager 5.9.4 to 6.4.0	Dynamic Link Manager 5.9.4 to 6.4.0
Red Hat Enterprise Linux	Linux AS/ES 3	x86	Dynamic Link Manager 5.4 to 6.4.0	For update 3 Dynamic Link Manager 5.4.2 to 6.4.0 For update 4 Dynamic Link Manager 5.6 to 6.4.0 For update 6 Dynamic Link Manager 5.7.1 to 6.4.0

OS	Version	Architecture	Path Management Software	
			Used with Device Manager	Used with Provisioning Manager
		IPF	Dynamic Link Manager 5.4 to 6.4.0	Unsupported
		x64 Edition (EM64T)	Dynamic Link Manager 5.6.2 to 6.4.0	Unsupported
	Linux AS/ES 4 Update 1	x86 IPF	Dynamic Link Manager 5.7.0-02 to 6.4.0	Dynamic Link Manager 5.7.0-02 to 6.4.0
		x64 Edition (EM64T)	Dynamic Link Manager 5.7.1 to 6.4.0	Dynamic Link Manager 5.7.1 to 6.4.0
	Linux AS/ES 4 Update 3	x86 IPF x64 Edition (EM64T)	Dynamic Link Manager 5.8.1 to 6.4.0	Dynamic Link Manager 5.8.1 to 6.4.0
	Linux AS/ES 4 Update 4	x86 IPF x64 Edition (EM64T)	Dynamic Link Manager 5.8.1 to 6.4.0	Dynamic Link Manager 5.9.1 to 6.4.0
	Linux AS/ES 4.5	x86 IPF x64 Edition (EM64T)	Dynamic Link Manager 5.9.3 to 6.4.0	Dynamic Link Manager 5.9.3 to 6.4.0
	Linux AS/ES 4.6	x86 IPF x64 Edition (EM64T)	Dynamic Link Manager 5.9.4 to 6.4.0	Dynamic Link Manager 5.9.4 to 6.4.0
	Linux AS/ES 4.7	x86 IPF x64 Edition (EM64T)	Dynamic Link Manager 6.0.0 to 6.4.0	Dynamic Link Manager 6.0.0 to 6.4.0
	Linux AS/ES 4.8	x86 IPF x64 Edition (EM64T)	Dynamic Link Manager 6.0.0 to 6.4.0	Dynamic Link Manager 6.0.0 to 6.4.0
	Linux 5.0	x86 IPF x64 Edition (EM64T)	Dynamic Link Manager 5.9.3 to 6.4.0	Dynamic Link Manager 5.9.3 to 6.4.0
	Linux 5.1	x86 IPF x64 Edition (EM64T)	Dynamic Link Manager 5.9.4 to 6.4.0	Dynamic Link Manager 5.9.4 to 6.4.0

OS	Version	Architecture	Path Management Software	
			Used with Device Manager	Used with Provisioning Manager
	Linux 5.2	x86 IPF x64 Edition (EM64T)	Dynamic Link Manager 5.9.4 to 6.4.0	Dynamic Link Manager 6.0.0 to 6.4.0
	Linux 5.3	x86 IPF x64 Edition (EM64T)	Dynamic Link Manager 6.1.2 to 6.4.0	Dynamic Link Manager 6.1.2 to 6.4.0
	Linux 5.4	x86 IPF x64 Edition (EM64T)	Dynamic Link Manager 6.1.2 to 6.4.0	Dynamic Link Manager 6.1.2 to 6.4.0
SUSE Linux Enterprise Server	9 (SP1, SP2)	x86	Dynamic Link Manager 5.9.0 to 5.9.2	Unsupported
	9 (SP3)	x86	Dynamic Link Manager 5.9.0 to 5.9.4	Unsupported
	9 (SP4)	x86	Dynamic Link Manager 6.0.0 to 6.4.0	Unsupported
	10 (No SP)	x86	Dynamic Link Manager 5.9.0 to 6.4.0	Unsupported
	10 (SP1)	x86	Dynamic Link Manager 5.9.3 to 6.4.0	Unsupported
	10 (SP2)	x86	Dynamic Link Manager 6.0.1 to 6.4.0	Unsupported
	10 (SP3)	x86	Dynamic Link Manager 6.3.0 to 6.4.0	Unsupported
	11 (No SP)	x86	Dynamic Link Manager 6.2.1 to 6.4.0	Unsupported
HP-UX	11i v1	PA-RISC (32bit)	PV-link	▪ PV-link ▪ Dynamic Link Manager 5.6.1 to 6.1.0
		PA-RISC (64bit)	▪ PV-link ▪ Dynamic Link Manager 04-00 to 6.1.0	▪ PV-link ▪ Dynamic Link Manager 5.6.1 to 6.1.0
	11i v2	PA-RISC (64bit) IPF	▪ PV-link ▪ Dynamic Link Manager 5.6.1 to 6.1.0	▪ PV-link ▪ Dynamic Link Manager 5.6.1 to 6.1.0
	11i v3	PA-RISC (64bit) IPF	▪ PV-link ▪ MPIO	▪ PV-link ▪ MPIO

Note: You can use Provisioning Manager to configure host settings for LUs managed by PV-link only if Dynamic Link Manager is not installed. If Dynamic Link Manager is installed, you can view information, but cannot perform host setting operations.

Supported Cluster Software

When cluster software is installed, hosts on which Device Manager agent is also installed can be clustered in an Active-Standby configuration or Active-Active configuration. The Device Manager agent runs in cluster environments configured with the cluster software listed in the table below. Note that the table only lists OSs that support cluster software.

Notes:

Because the Device Manager agent is not compatible with the logical host, the Device Manager agent cannot be registered in cluster resources. The Device Manager agent is activated on the physical hosts that make up the cluster, and collects the data for those hosts.

Cluster software cannot be set up from Provisioning Manager. When you use file systems and device files created by using Provisioning Manager as cluster resources, or when you use a host setting function of Provisioning Manager to operate file systems or device files, set up the cluster software manually.

For details about setting up the cluster software, see the manual for each cluster software product.

Table 1-16 Supported Cluster Software

OS	Version	Architecture	Cluster Software	
			Used with Device Manager	Used with Provisioning Manager
Windows Server 2003	No SP	x86	▪ Microsoft® Cluster Service ▪ VERITAS Cluster Server 4.1	Microsoft Cluster Service
		IPF	Microsoft Cluster Service	Microsoft Cluster Service
		x64 Edition (EM64T and AMD64)	Microsoft Cluster Service	Microsoft Cluster Service
	SP1	x86	▪ Microsoft Cluster Service ▪ VERITAS Cluster Server 4.1 ▪ VERITAS Cluster Server 4.3	Microsoft Cluster Service
		IPF	Microsoft Cluster Service	Microsoft Cluster Service

OS	Version	Architecture	Cluster Software	
			Used with Device Manager	Used with Provisioning Manager
	SP2	x86	Microsoft Cluster Service	Microsoft Cluster Service
		IPF	Microsoft Cluster Service	Microsoft Cluster Service
		x64 Edition (EM64T and AMD64)	Microsoft Cluster Service	Microsoft Cluster Service
Windows Server 2003 R2	No SP SP2	x86	Microsoft Cluster Service	Microsoft Cluster Service
		x64 Edition (EM64T and AMD64)	Microsoft Cluster Service	Microsoft Cluster Service
Windows Server 2008	No SP SP2	x86	Microsoft Failover Cluster	Microsoft Failover Cluster
		IPF	Microsoft Failover Cluster	Microsoft Failover Cluster
		x64 Edition (EM64T and AMD64)	Microsoft Failover Cluster	Microsoft Failover Cluster
Windows Server 2008 R2	No SP	IPF x64 Edition (EM64T and AMD64)	Microsoft Failover Cluster	Microsoft Failover Cluster
Solaris	8	SPARC (32 and 64 bit)	▪ Sun Cluster 3.0 ▪ Sun Cluster 3.1 ▪ VERITAS Cluster Server 1.3 ▪ VERITAS Cluster Server 2.0 ▪ VERITAS Cluster Server 3.5 ▪ PRIMECLUSTER 4.1.4[#1, #2]	VERITAS Cluster Server 3.5
	9	SPARC (32 and 64 bit)	▪ Sun Cluster 3.1 ▪ VERITAS Cluster Server 3.5 ▪ VERITAS Cluster Server 4.0 ▪ VERITAS Cluster Server 4.1 ▪ Cluster Perfect 4.5 R2 ▪ PRIMECLUSTER 4.1.4[#1, #2]	▪ VERITAS Cluster Server 3.5 ▪ VERITAS Cluster Server 4.0

OS	Version	Architecture	Cluster Software	
			Used with Device Manager	Used with Provisioning Manager
	10	SPARC (32 and 64 bit)	▪ Sun Cluster 3.1 ▪ VERITAS Cluster Server 4.1 ▪ VERITAS Cluster Server 4.1 MP2 ▪ Veritas Cluster Server 5.0 ▪ Veritas Cluster Server 5.0 MP1 ▪ PRIMECLUSTER 4.1.4[#1, #2] ▪ PRIMECLUSTER 4.2[#1, #2]	▪ Sun Cluster 3.1 ▪ VERITAS Cluster Server 4.1 ▪ VERITAS Cluster Server 4.1 MP2 ▪ Veritas Cluster Server 5.0 ▪ Veritas Cluster Server 5.0 MP1
		x64 Edition (AMD64)	▪ VERITAS Cluster Server 4.1 MP2 ▪ Veritas Cluster Server 5.0 MP1	▪ VERITAS Cluster Server 4.1 MP2 ▪ Veritas Cluster Server 5.0 MP1
AIX	5.3	32 bit	▪ HACMP 5.2 ▪ PowerHA 5.5 ▪ PowerHA 6.1	▪ HACMP 5.2 ▪ PowerHA 5.5 ▪ PowerHA 6.1
		64 bit	▪ HACMP 5.2 ▪ HACMP 5.3 ▪ PowerHA 5.5 ▪ PowerHA 6.1	▪ HACMP 5.2 ▪ PowerHA 5.5 ▪ PowerHA 6.1
	6.1	64 bit	▪ HACMP 5.4.1 ▪ PowerHA 5.5 ▪ PowerHA 6.1	▪ HACMP 5.4.1 ▪ PowerHA 5.5 ▪ PowerHA 6.1
Red Hat Enterprise Linux	Linux AS/ES 4 Update 1	x86	VERITAS Cluster Server 4.1	Unsupported
	Linux AS/ES 4 Update 4	IPF	PRIMECLUSTER 4.2[#1]	Unsupported
	Linux AS/ES 4.5	IPF	PRIMECLUSTER 4.2[#1]	Unsupported

OS	Version	Architecture	Cluster Software	
			Used with Device Manager	Used with Provisioning Manager
HP-UX	11i v1	PA-RISC (32 bit)	Serviceguard 11.16	Serviceguard 11.16
		PA-RISC (64 bit)	▪ MC/Service Guard 11.15 ▪ Serviceguard 11.16	Serviceguard 11.16
	11i v2	PA-RISC (64 bit) IPF	▪ Serviceguard 11.16 ▪ Serviceguard 11.17	▪ Serviceguard 11.16 ▪ Serviceguard 11.17
	11i v3	PA-RISC (64 bit)	Serviceguard 11.17	Serviceguard 11.17
		IPF	▪ Serviceguard 11.17 ▪ Serviceguard 11.18	▪ Serviceguard 11.17 ▪ Serviceguard 11.18
#1: File systems created with GDS are not supported. ***#2***: Dynamic Link Manager must be already installed.				

Supported SAN Environments

This section explains the system requirements for SAN environments that are supported by Device Manager agents.

Caution:

Before you connect the host with storage subsystems via FC-HUB (or FC-SWITCH), confirm whether FC-HUB (or FC-SWITCH) and its firmware are appropriate for the storage subsystem:

- Check the corresponding HBA model. For details, see Supported Host Bus Adapter Models.
- Check the FC-HUB (and firmware) supported by the target storage subsystems. Refer to the appropriate documentation for your storage subsystem.

Supported Storage Subsystems

The following storage subsystem models are supported by the Device Manager agent:

- Universal Storage Platform V/VM
- Hitachi USP
- Lightning 9900V
- Lightning 9900
- Hitachi AMS 2000
- Hitachi SMS
- Hitachi AMS/WMS
- Thunder 9500V
- Thunder 9200

If a host in which the Device Manager agent is installed is connected to a storage subsystem, all HBA models supported by that storage subsystem are available.

For details, refer to the appropriate Hitachi Data Systems documentation.

Caution:

When using Hitachi AMS 2000, Hitachi SMS, Hitachi AMS/WMS, Thunder 9500V or Thunder 9200, do not change the default settings of the following:

- Vendor ID. Do not change the default setting (`HITACHI`).
- Product ID
  - For Thunder 9200, do not change the default setting (`DF500F`).
  - For Hitachi AMS 2000, Hitachi SMS, Hitachi AMS/WMS and Thunder 9500V, do not change the default setting (`DF600F`).

Note:

- If Lightning 9900 is connected to a Linux host using Fibre Channel, they must be in a one-to-one relation.
- For 9200 LUN attachments, the Device Manager agent requires that the Hitachi Freedom Storage Thunder 9200 array be configured with the Report Inquiry Page 83H option and INQUIRY WWN Mode. For further information, contact your Hitachi Data Systems account team.

Supported Host Bus Adapter Models

To obtain host WWN information, the HBA models shown in the following table and the HBA API library provided by the HBA vendor are required.

Table 1-17 HBA Models Required to Obtain Host WWN Information

OS	Model name	Hitachi type name
Windows	Emulex LP8000	Not applicable
	Emulex LP9002DC	Not applicable
	Emulex LP9002L	Not applicable
	Emulex LP9802	Not applicable
	QLogic QLA23*xx*[#1]	Not applicable
	QLogic QLA24*xx*[#1]	Not applicable
	Hitachi GV-CC62G1	Not applicable
Solaris (SPARC edition)	JNI FCI-1063	A-6516-FCPN
	JNI FC64-1063	A-6716-FCSN
	JNI FCE-6410	Not applicable
	JNI FCE-6460	Not applicable
	QLogic QLA2200	Not applicable
	Sun HBA[#2]	Not applicable
Solaris (x64 Edition (AMD64))	QLogic QLA2310	Not applicable
	Sun HBA	Not applicable

OS	Model name	Hitachi type name
AIX	IBM6227	Not applicable
	IBM6228	Not applicable
Linux	QLogic QLA2200F	Not applicable
	QLogic QLA23*xx*	Not applicable
	QLogic QLA24*xx*	Not applicable
	Hitachi GV-CC62G1	Not applicable
HP-UX	HP A3404A	HT-F3360-FC2
	HP A3591B	HT-F3360-FC3
	HP A3636A	HT-F3360-FC1
	HP A3740A	HT-F3360-PC5
	HP A5158A	HT-F3360-PC5A
	HP A6684A	Not applicable
	HP A6685A	Not applicable
	HP A6795A	HT-F3360-PCFC
	HP A6826A	Not applicable
	HP A9784A	Not applicable
#1: In order to use a QLogic HBA, download and then install Fibre Channel Information Tool (fcinfo) version x86 from the Microsoft web site. Even if the OS of a host where the Device Manager agent is installed is the IPF version or x64 version, the fcinfo x86 version must be used. ***#2***: When using an HBA by Sun Microsystems on Solaris 9, install Sun StorEdge SAN Foundation Software 4.2 or later.		

Note that if either of the following conditions is satisfied, obtaining host WWN information, alternate path WWN information, and LU information (such as file systems, usage, copy types, copy roles, and copy statuses) might not be possible:

- The host on which the Device Manager agent is running does not recognize the LU for the storage subsystem.
- A multi-path configuration is set up in one of the following host environments, where the host OS is:
  - Windows, and Dynamic Link Manager or Windows MPIO is used.
  - Solaris, and Dynamic Link Manager or Sun StorEdge Traffic Manager is used.
  - AIX, and MPIO is used.

Supported iSCSI Connection Configurations

The Device Manager agent supports the iSCSI connection configurations listed below in IPv4 environments only. Note that an instance of Device Manager connected by using iSCSI can only manage storage subsystems that belong to Hitachi AMS 2000, Hitachi SMS and Hitachi AMS/WMS.

Table 1-18 Supported iSCSI Connection Configurations

OS	NIC or HBA	Necessary Drivers
Windows	NIC	Microsoft iSCSI Software Initiator (2.04 or later)
Windows Server 2003 Enterprise Edition SP1 (x86 or x64) Windows Server 2003 R2 Enterprise Edition (x86 or x64)	QLogic QLA4050c QLogic QLA4052c	Microsoft iSCSI Software Initiator (2.04 or later) and QLogic Driver
Solaris	NIC	Included with the OS
AIX	NIC	Included with the OS
Linux	NIC	Included with the OS (Drivers are not installed by default.)
HP-UX	NIC	Included with the OS

Caution:

If you use the Device Manager agent in an iSCSI connection configuration in Solaris, you must apply prerequisite patches. For details on the prerequisite patches, see Required Patches for Operating Systems.

2

Installing the Device Manager Agent

This chapter explains how to install and set up the Device Manager agent.

- ☐ Installing the Device Manager Agent in Windows
- ☐ Installing the Device Manager Agent in UNIX®
- ☐ Performing an Unattended Installation of the Device Manager Agent
- ☐ Uninstalling the Device Manager Agent

Installing the Device Manager Agent in Windows

The following types of Device Manager agent installations can be performed in a Windows environment:

- New installation

  Perform a new installation to install the Device Manager agent on a host for the first time.

- Upgrade installation (updating an earlier version)

  Perform an upgrade installation to upgrade the currently installed Device Manager agent to a new version, revision, or modified version by overwriting it.

- Re-installation (installation for restoration)

  Perform an overwrite installation of the currently installed Device Manager agent with a Device Manager agent whose version, revision, and modified version number are the same as the currently installed Device Manager agent.

Note:

- The Device Manager agent installer can be downloaded from the Device Manager or Replication Manager Web Client. The installer is formatted as an `exe` file, and needs to be decompressed before use.
- To check the version, revision, and modified version numbers of the currently installed Device Manager agent, execute the `hdvm_info` command. For details, see hdvm_info Command Syntax.
- Unattended installation can also be used so that the user does not need to input anything during installation. For details, see Performing an Unattended Installation of the Device Manager Agent.

Before Installing in Windows

When installing the Device Manager agent in a Windows environment, consider the following notes:

- The Device Manager agent does not support environments where only IPv6 addresses can be used. To use the Device Manager agent in an IPv6 environment, set up the OS so both IPv4 and IPv6 addresses can be used.
- The table below indicates the required free space for the installation folder. Also, an additional 100 MB of temporary free space is required for both the system drive and the folder that is specified in the `TMP` environment variable.

Table 2-1 Installation Destinations and Required Disk Space (Windows)

Agent	For 32-bit (x86) architecture	For 64-bit (IPF or x64) architecture	Disk space
Device Manager agent#	*system-drive*\Program Files\HITACHI\HDVM\HBaseAgent	*system-drive*\Program Files (x86)\HITACHI\HDVM\HBaseAgent	180 MB
Global Link Manager agent	*system-drive*\Program Files\HITACHI\HGLMAgent *system-drive*\Program Files\HDVM\HBaseAgent\mod\hglm	*system-drive*\Program Files (x86)\HITACHI\HGLMAgent *system-drive*\Program Files (x86)\HDVM\HBaseAgent\mod\hglm	25 MB

#: If you change the installation destination, the installation folder must satisfy the following conditions:

- The folder name can contain no more than 64 characters.
- The following characters can be used for the installation folder name:

  a-z A-Z 0-9 . _ ( ) space
- A space cannot be used at the beginning or end of the folder name. Also, you cannot use consecutive spaces nor folders or paths that include multi-byte characters.

- If a host environment satisfies both of the following conditions, refreshing the host from Web Client might cause JavaVM to end abnormally and the refresh operation to timeout:
  - The host OS is Windows Server 2003 (IPF), and Service Pack 1 or later has not been installed.
  - The host recognizes a large number of LUs (guideline value is 100 or more).

  To prevent this problem, we recommend that you install Service Pack 1 or later, and then install the Device Manager agent.

  If you install a service pack after installing the Device Manager agent, after you install the service pack, perform an overwrite installation of the Device Manager.

  If 100 or more LUs are recognized by the host, another error might occur. In this case, change the Device Manager agent settings by referring to Specifying Settings When a Host Manages 100 or More LUs.
- If a multi-byte character is included in the Windows logon account name, the TMP environment variable will also include a multi-byte character. If the TMP environment variable includes a multi-byte character, the Device Manager agent cannot be installed. To install the Device Manager agent, specify a folder name that does not include multi-byte characters for the TMP environment variable.
- Do not install a Replication Monitor agent version 5.9 or earlier in an environment where a Device Manager agent version 6.0 or later has already been installed.
- Hitachi Storage Command Suite products for Windows support the Windows Remote Desktop functionality. Note that the Microsoft terms used for this functionality differ depending on the Windows OS. The following terms can refer to the same functionality:
  - Terminal Services in the Remote Administration mode

– Remote Desktop for Administration

– Remote Desktop connection

When using the Remote Desktop functionality to perform a Hitachi Storage Command Suite product operation (including installation or uninstallation), you need to connect to the console session of the target server in advance. However, even if you have successfully connected to the console session, the product might not work properly if another user connects to the console session.

- To log on to Windows from a remote console and then install the Device Manager agent, you must use Terminal Service Client.
- Some of the firewall functions provided by the OS might terminate socket connections in the local host. You cannot install and operate Hitachi Storage Command Suite products in an environment in which socket connections are terminated in the local host. When setting up the firewall provided by the OS, configure the settings so that socket connections cannot be terminated in the local host.
- Before installing the Device Manager agent, stop any programs that are running.
- Check if any security monitoring programs have been installed. If a security monitoring program has been installed, either stop it or change its settings so that it will not interfere with the Device Manager installation.
- Make sure that the setting for automatically generating short file and folder names (8.3 format) is enabled. In addition, when performing installation, use a Windows account that was created when the setting was enabled.

  If the above conditions are not satisfied, installation of the Device Manager agent might fail or the Device Manager agent might not work properly.

  Also, do not change the setting for automatically generating short names even after the installation has completed.

  To check whether a user was created while the setting for automatically generating short file and folder names was disabled, execute the following command:

  ```
  dir /x /a- "Windows-system-drive:\Documents and
  Settings\Windows-account-name" | find "Local Settings"
  ```

  The following examples shows the command execution results when the setting for automatically generating short file and folder names was either enabled or disabled when the specified account was created. If the user was created while this setting was enabled, LOCALS~1 is displayed.

  If the specified user was created while the setting was enabled:

  ```
  2008/01/01  18:26      <DIR>         LOCALS~1       Local Settings
  ```

  If the specified user was created while the setting was disabled:

  ```
  2008/01/01  18:26      <DIR>                        Local Settings
  ```

- The Device Manager agent versions 5.7 and later are compatible with the new Daylight Saving Time (DST) rules implemented in the United States and Canada beginning in 2007. When using the Device Manager agent in an American or Canadian time zone, set the host OS for the new DST rules according to information provided by the OS vendor. If the host OS is not compatible with the new DST rules, the Device Manager agent will also be incompatible with the new rules.

Performing a New Installation in Windows

To perform a new installation of the Device Manager agent:

1. Log on to Windows as a user with Administrator permissions.
2. Insert the Device Manager agent CD-ROM.
3. From the CD-ROM, select and execute `setup.exe`.

   The `setup.exe` file is stored in the following location:

   CD-ROM-drive`\Agent\Windows\`

Caution: If the host OS is Windows Server 2008 or Windows Server 2008 R2, a dialog box asking you to elevate UAC privileges is displayed. Check the contents, and then elevate the privileges.

   The Welcome to the installer for Hitachi Device Manager agent *version-number* (New) window appears.

4. Check the information displayed in the window, and then click the **Next** button.

   The License Agreement window appears.

5. Read the terms, select **I accept the terms in the license agreement**, and then click the **Next** button.

   The Choose Install Folder window appears.

6. Change the installation destination of the Device Manager agent as necessary, and then click the **Next** button.

   If you click the **Next** button, the **Configuration of Windows Firewall** window appears.

Caution:

- If Dynamic Link Manager 5.8.0 or later is installed, the installation destination cannot be changed.
- If the installation path you specify for the Device Manager agent contains a space character, and there is a folder or file whose path matches the specified path (from the beginning until the space character), information cannot be sent to the Device Manager server when the Device Manager agent service is started. For example, this problem occurs if you installed the Device Manager agent in the folder `d:\host agent` and a folder or file whose path is `d:\host` exists. To prevent this problem, do one of the following:
  - Delete the relevant folder or file.
  - Uninstall the Device Manager agent, and then re-install it in another folder.

7. Select **Yes**, and then click the **Next** button.

The Setting Up the Agent Service Account window appears.

8. Specify an OS account with Administrator permissions and the password as necessary, and then click the **Next** button.

   To operate the `horcm` instance running on the Device Manager agent, the service permissions need to be changed from LocalSystem to an OS user with Administrator permissions.

   If you click the **Next** button, the **Ready to Install the Program** window appears.

Note:

You can specify a domain user by using the following format:

*domain-name**user-name*

If domain-name is omitted, the Device Manager agent service might not start normally. If the Device Manager agent service does not start normally, set the account information in the Services window on Windows again.

9. Verify that the information is correct, and then click the **Install** button.

   A series of dialog boxes are displayed, indicating the installation status. After a successful installation, a dialog box appears, prompting you to set up the Device Manager agent.

10. To setup the Device Manager agent, select **Yes**. Otherwise, select **No**.

    If **Yes** is selected, the Specifying Server Information window is displayed.

    If **No** is selected, a dialog box is displayed indicating that Device Manager server setup is required. Follow the instructions in the dialog box to perform setup separately after installation.

11. Specify the Device Manager server information, and then click the **Next** button.

    Specify the information for the Device Manager server to which host information is to be reported. These settings are required to use the Device Manager agent.

    To perform these settings separately after installation, select **NO. Setup later**, and then click the **Next** button.

    – IP address or host name

      Specify the IP address or host name for the Device Manager server.

    – Port number

      Specify the port number for the Device Manager server.

    – User ID

      Specify the user ID for logging on to the Device Manager server. In Device Manager, `HaUser` is prepared as a built-in account for use with the Device Manager agent.

    – Password

Specify the password for logging on to the Device Manager server. The default password for HaUser is haset.

If connection with the Device Manager server is successful, the Connection Verification window and then the Specifying the Execution Period of HiScan Command window are displayed.

12. If necessary, specify the execution period for the HiScan command. Then click the **Next** button.

    The HiScan command reports host information to the Device Manager server. Specifying the execution period for the HiScan command registers exeHiScan.bat as a Windows task.

    If you do not specify the execution period, the Device Manager server is not periodically notified of information acquired by the Device Manager agent.

    To specify the execution period for the HiScan command at a later time, or if you do not want the HiScan command to execute automatically, select **NO. Setup later**, and then click the **Next** button.

    – Execution period

      Select **Hourly** to perform automatic execution once every hour, **Daily** to perform automatic execution once every day, or **Weekly** to perform automatic execution once every week.

    – Day of the week

      If you select **Weekly**, specify the day of the week on which automatic execution is to be performed. Select **Sun**, **Mon**, **Tue**, **Wed**, **Thu**, **Fri**, or **Sat**.

    – Execution time

      Specify the execution time for the HiScan command. Specify a value from 0 to 23 for execution time (hour) and 0 to 59 for execution time (minute).

    The Specifying the setup of RAID Manager window appears.

Caution: If the Device Manager agent is installed on multiple hosts, set the HiScan command to execute daily or weekly to reduce the load of the Device Manager server. Also, vary the start times for execution of the HiScan command on each host so that the command will not be executed simultaneously from multiple hosts. For details about how to check the execution time for the HiScan command, see HiScan Command Syntax.

13. If Device Manager is linked with CCI and is managing copy pairs, specify the information needed to use CCI, and then click the **Next** button.

    If you want to set the information for using CCI at a later time, or if you do not use CCI, select **NO. Setup later**, and then click the **Next** button.

    Installation drive

      Specify the drive on which CCI is installed.

Caution: Do not specify a floppy disk drive or CD-ROM drive. If you do so, the Device Manager agent might not operate normally.

Central management method

Select **enable** to batch manage copy pairs on the host on which the Device Manager agent is installed.

14. Click the **OK** button.

    If the following temporary folder created during installation remains, delete it manually:

    *system-drive*_HDVMAgent*version-number*_Install_tmp_\

    If it cannot be deleted, log on to Windows again to delete it.

When you install the Device Manager agent, the folder in which commands are installed is automatically added to the environment variable PATH. After installing the Device Manager agent, you will have to log off from, and then log on to Windows for the changes in the environment variable PATH to be applied.

Caution:

In the following cases, the Device Manager agent service needs to be stopped after installation, and the following Device Manager agent property settings need to be changed.

- If Device Manager is used in an IPv6 environment:

  The following properties in the `server.properties` file need to be set:

  – `server.http.socket.agentAddress`
  – `server.http.socket.bindAddress`

  For details about the `server.properties` file, see The server.properties File.

- If VxVM is installed:

  The version of the installed VxVM needs to be set in the `programproductinfo.properties` file. For details about the `programproductinfo.properties` file, see The programproductinfo.properties File.

- If a version of Dynamic Link Manager earlier than 5.8.0 is installed:

  The port number used by the Device Manager agent needs to be set for the following properties in the `server.properties` file:

  – `server.http.port`
  – `server.agent.port`

  For details about the port number set and the `server.properties` file, see The server.properties File.

For details about stopping and starting the Device Manager agent service, see Managing the Operating Status of the Device Manager Agent Service.

Performing an Upgrade Installation in Windows

This section explains how to perform an upgrade installation of the Device Manager agent. When an upgrade installation is performed, the previously defined information, such as the Device Manager server information or the execution period of the `HiScan` command, will be inherited.

Caution:

- When an overwrite installation of a Device Manager agent whose version is 4.3.0 or earlier is performed in an environment in which Dynamic Link Manager 5.8.0 or later is installed, the installation folder of the Device Manager agent is changed to the following folder:

  If the OS architecture is 32 bits (x86):

  system-drive`\Program Files\HITACHI\HDVM\HBaseAgent\`

  If the OS architecture is 64 bits (IPF or x64):

  system-drive`\Program Files (x86)\HITACHI\HDVM\HBaseAgent\`

  For any other cases, overwrite installation is performed in the installation folder for the previous Device Manager agent.
- Overwrite installations cannot be performed for versions or revisions earlier than the existing version. Make sure that the version of the Device Manager agent for which overwrite installation is to be performed is the same as or later than the existing version. To install an earlier version or revision of a Device Manager agent, first uninstall the existing Device Manager agent.
- The Replication Monitor agent has been integrated with version 6.0 or later Device Manager agents. As such, when an update installation of a version 6.0 or later Device Manager agent is performed in an environment in which a version 5.9 or earlier Replication Monitor agent is installed, the Replication Monitor agent is automatically uninstalled. Note that Replication Monitor package information will no longer be displayed in the Windows Add or Remove Programs window.
- If an overwrite installation of a version is 6.0 or later Device Manager agent is performed in an environment in which a version is 5.9 or earlier Device Manager agent is installed, the Provisioning Manager agent package information will no longer be displayed in the Windows Add or Remove Programs window.
- In Windows Server 2003, if you upgrade the Device Manager agent by overwriting the existing Device Manager agent whose version is 4.1 or earlier, the previously installed VDS provider is deleted, disabling its use. If you want to use VDS functions, you need to re-install the VDS provider separately. For details on VDS installation, see the *Hitachi Device Manager Server Configuration and Operation Guide*.
- Stop the `hdvmagt` service before updating a Device Manager agent whose version is 3.5 or earlier.

- Do not execute any of the commands listed below during an upgrade installation of the Device Manager agent. Also, do not install the Device Manager agent while the following commands are executing:
  - `hbsasrv`
  - `hdvmagt`#
  - `hdvmagt_account`
  - `hdvmagt_schedule`
  - `hdvmagt_setting`
  - `HiScan`
  - `hldutil`
  - `stop_hdvmagt`#
  - `TIC`

  #: These commands are for versions of the Device Manager agent earlier than 5.0.

If you execute the above commands during installation, the upgrade installation might end abnormally. In this case, make sure to restart the computer after installation. The upgrade installation is complete after you have restarted the computer.

To perform an upgrade installation of the Device Manager agent:

1. Log on to Windows as a user with Administrator permissions.
2. Insert the Device Manager agent CD-ROM.
3. From the CD-ROM, select and execute `setup.exe`.

   The `setup.exe` file is stored in the following location:

   CD-ROM-drive`\Agent\Windows\`

Caution: If the host OS is Windows Server 2008 or Windows Server 2008 R2, a dialog box asking you to elevate UAC privileges is displayed. Check the contents, and then elevate the privileges.

   The Welcome to the installer for Hitachi Device Manager agent *version-number* (Upgrade) window appears.

4. Check the information displayed in the window, and then click the **Next** button.

   The Ready to Install the Program window appears.

5. Make sure that the displayed information is correct, and then click the **Install** button.

   Installation starts and a series of dialog boxes indicating the processing status appear. If the installation is successful, a message dialog box appears.

6. Click the **OK** button.

   If the following temporary folder created during installation remains, delete it manually: *system-drive*`\_HDVMAgent`*version-number*`_Install_tmp_\`

If it cannot be deleted, log on to Windows again to delete it.

When you install the Device Manager agent, the folder in which commands are installed is automatically added to the environment variable PATH. After installing the Device Manager agent, you will have to log off from, and then log on to Windows for the changes in the environment variable PATH to be applied.

Caution:

After performing an upgrade installation, the setting specifying the user who executes the Device Manager agent service might return to the Device Manager agent default setting (`LocalSystem`). If you changed the user who executes the Device Manager agent service from `LocalSystem` to another user, respecify the setting as necessary after the upgrade installation of the Device Manager agent finishes. For details about how to change the user who executes the Device Manager agent service, see Changing the User of the Device Manager Agent Service.

Also, in the following cases, the Device Manager agent service needs to be stopped after installation, and the following Device Manager agent property settings need to be changed.

- If Device Manager is used in an IPv6 environment:

  The following properties in the `server.properties` file need to be set:

  – `server.http.socket.agentAddress`
  – `server.http.socket.bindAddress`

  For details about the `server.properties` file, see The server.properties File.

- If VxVM is been installed:

  The version of the installed VxVM needs to be set in the `programproductinfo.properties` file. For details about the `programproductinfo.properties` file, see The programproductinfo.properties File.

- If a version of Dynamic Link Manager earlier than 5.8.0 is installed:

  The port number used by the Device Manager agent needs to be set for the following properties in the `server.properties` file:

  – `server.http.port`
  – `server.agent.port`

  For details about the port number set and the `server.properties` file, see The server.properties File.

For details about stopping and starting the Device Manager agent service, see Managing the Operating Status of the Device Manager Agent Service.

Performing a Restoration Installation in Windows

This section explains how to perform a restoration installation of the Device Manager agent. When a restoration installation is performed, the previously defined information, such as the Device Manager server information or the execution period of the `HiScan` command, will be inherited.

Caution:

Do not execute any of the commands listed below during an upgrade installation of the Device Manager agent. Also, do not install the Device Manager agent while the following commands are executing:

- `hbsasrv`
- `hdvmagt_account`
- `hdvmagt_schedule`
- `hdvmagt_setting`
- `HiScan`
- `hldutil`
- `TIC`

If you execute the above commands during installation, the restoration installation might end abnormally. In this case, restart the computer after installation. The restoration installation is complete after you have restarted the computer.

To complete a restoration installation of the Device Manager agent:

1. Log on to Windows as a user with Administrator permissions.
2. Insert the Device Manager agent CD-ROM.
3. From the CD-ROM, select and execute `setup.exe`. The `setup.exe` file is stored in the following location:

   CD-ROM-drive`\Agent\Windows\`

Caution: If the host OS is Windows Server 2008 or Windows Server 2008 R2, a dialog box asking you to elevate UAC privileges is displayed. Check the contents, and then elevate the privileges.

   The Program Maintenance window appears.

4. Select **Repair**, and then click the **Next** button.

   The Ready to Install the Program window appears.

5. Verify that the displayed information is correct, and then click the **Install** button.

   Installation starts and a series of dialog boxes indicating the processing status appear. If the installation is successful, a message dialog box appears.

6. Click the **OK** button.

   If the following temporary folder created during installation remains, delete it manually:

   *system-drive*_HDVMAgent*version-number*_Install_tmp_\

   If it cannot be deleted, log on to Windows again to delete it.

Caution:

After performing an upgrade installation, the setting specifying the user who executes the Device Manager agent service might return to the Device Manager agent default setting (`LocalSystem`). If you changed the user who executes the Device Manager agent service from `LocalSystem` to another user, respecify the setting as necessary after the upgrade installation of the Device Manager agent finishes. For details about how to change the user who executes the Device Manager agent service, see Changing the User of the Device Manager Agent Service.

Also, in the following cases, the Device Manager agent service needs to be stopped after installation, and the following Device Manager agent property settings need to be changed.

- If VxVM has been installed

  The version of the installed VxVM needs to be set in the `programproductinfo.properties` file. For details about the `programproductinfo.properties` file, see The programproductinfo.properties File.

- If a version of Dynamic Link Manager earlier than 5.8.0 is installed:

  The port number used by the Device Manager agent needs to be set for the following properties in the `server.properties` file:

  – `server.http.port`
  – `server.agent.port`

  For details about the port number set and the `server.properties` file, see The server.properties File.

For details about stopping and starting the Device Manager agent service, see Managing the Operating Status of the Device Manager Agent Service.

Installing the Device Manager Agent in UNIX®

This section describes how to install the Device Manager agent in a UNIX environment.

Note:

- The Device Manager agent installer can be downloaded from the Device Manager or Replication Manager Web Client.

  Before using the downloaded tar file, save it in the `/tmp/Agent` directory.
- To check the version of the currently installed Device Manager agent, execute the `hdvm_info` command. For details, see hdvm_info Command Syntax.
- The Device Manager agent has unattended installation functionality, which does not require any input by the user. For details, see Performing an Unattended Installation of the Device Manager Agent.

Before Installing in UNIX

Keep the following notes in mind when installing the Device Manager agent for UNIX.

- The Device Manager agent does not support environments where only IPv6 addresses can be used. To use the Device Manager agent in an IPv6 environment, set up the OS so both IPv4 and IPv6 addresses can be used.
- The following table indicates the required free space for the installation directory.

Table 2-2 Installation Destinations and Required Disk Space (UNIX)

OS	Device Manager agent		Global Link Manager agent	
	Installation destination	Disk space	Installation destination	Disk space
Solaris	/opt/HDVM/HBaseAgent	20 MB	/opt/HGLMAgent /opt/HDVM/HBaseAgent/mod/hglm	25 MB
AIX	/usr/HDVM/HBaseAgent	35 MB	--	--
Linux (x86 or x64 Edition)	/opt/HDVM/HBaseAgent	100 MB		
Linux (IPF)		140 MB		
HP-UX		20 MB		
Legend: --: Not applicable				

In addition, the log space shown in Table 2-3 and the temporary free space shown in Table 2-4 are also required.

Table 2-3 Required Log Space (UNIX)

OS	Directory	Free space
Solaris	/var/opt	5 MB
AIX	/var	
Linux (x86 or x64 Edition)	/var/opt	
Linux (IPF)		
HP-UX		

Table 2-4 Required Temporary Free Space During Installation (UNIX)

OS	Directory	New installation	Overwrite installation
Solaris	/var/tmp	30 MB	80 MB
AIX		30 MB	80 MB
Linux (x86 or x64 Edition)		125 MB	175 MB
Linux (IPF)		155 MB	205 MB
HP-UX		30 MB	80 MB

- Do not create a symbolic link for any of the directories below. If you have already created a symbolic link by using any of the directories below, do not install the Device Manager agent.

  In Solaris, Linux, or HP-UX:

  /opt

  All subdirectories under /opt/HDVM (including the /opt/HDVM)

  /var

  /var/opt

  All subdirectories under /var/opt/HBaseAgent (including /var/opt/HBaseAgent)

  All subdirectories under /var/opt/HDVM (including /var/opt/HDVM)

  /var/tmp

  In AIX:

  /usr

  All subdirectories under /usr/HDVM (including /usr/HDVM)

  All subdirectories under /var/HDVM (including /var/HDVM)

  /var

  All subdirectories under /var/HBaseAgent (including /var/HBaseAgent)

  /var/tmp

- Overwrite installation cannot be performed for versions or revisions earlier than the existing version. Make sure that the version of the Device Manager agent for which overwrite installation is to be performed is the same as or later than the existing version. To install an earlier version or revision of a Device Manager agent, first uninstall the existing Device Manager agent.
- When an update installation of a version 6.0 or later Device Manager agent is performed in an environment on which a version 5.9 or earlier Replication Monitor agent is installed, the Replication Monitor agent is automatically uninstalled.
- If an overwrite installation of the Device Manager agent is performed in an environment in which version 5.9 or earlier of Device Manager agent is installed, information about the Provisioning Manager agent functionality will no longer be displayed when the package command is executed.
- Before starting the installation of the Device Manager agent, stop any programs that are running.
- Some of the firewall functions provided by the OS might terminate socket connections in the local host. You cannot install and operate Hitachi Storage Command Suite products in an environment in which socket connections are terminated in the local host. When setting up the firewall provided by the OS, configure the settings so that socket connections cannot be terminated in the local host.
- Check if any security monitoring programs have been installed. If a security monitoring program has been installed, either stop it or change its settings so that it will not interfere with the Device Manager installation.
- The Device Manager agent versions 5.7 and later are compatible with the new Daylight Saving Time (DST) rules implemented in the United States and Canada beginning in 2007. When using the Device Manager agent in an American or Canadian time zone, set the host OS for the new DST rules according to information provided by OS vendor. If the host OS is not compatible with the new DST rules, the Device Manager agent will also not be compatible with the new rules.
- Do not execute any of the commands listed below during an upgrade installation of the Device Manager agent. Also, do not install the Device Manager agent while the following commands are executing:
  - `hbsasrv`
  - `hdvmagt`[#]
  - `hdvmagt_account`
  - `hdvmagt_schedule`
  - `hdvmagt_setting`
  - `HiScan`
  - `hldutil`
  - `stop_hdvmagt`[#]

– TIC

#: These commands are for versions of the Device Manager agent earlier than 5.0.

If you execute the above commands during installation, the upgrade installation might end abnormally. In this case, restart the computer after installation. The upgrade installation is complete after you have restarted the computer.

Before Installing in Solaris

Keep the following notes in mind regarding installation of Device Manager agents in a Solaris environment.

- The currently installed HDSHiScan package needs to be deleted before installing the Device Manager agent.

  We recommend that you remove any agent that you will not be using.

Caution: HDSHiScan is the name used for versions earlier than 2.2. HDVMAgent is the name used for version 2.2 and later. The HDSHiScan package is installed in the `/opt/HDVM` directory.

To delete the HDSHiScan package:

a. At the prompt, execute the following commands to check whether a HiScan package is installed:

```
% su
# pkginfo -l HDSHiScan
```

If the HDSHiScan package is installed, confirm the execution period of the `HiScan` command by executing the following commands:

```
% su
# crontab -l
```

For details about how to interpret the execution period of the `HiScan` command, see HiScan Command Syntax.

b. Execute the following commands to remove the existing HiScan package.

```
% su
# pkgrm HDSHiScan
```

Confirmation that the selected program has been deleted is displayed.

Keep the following *notes* in mind regarding installation of Device Manager agents in a Solaris 10 environment.

- When installing the Device Manager agent, do not specify the system's zone settings. If you do this, installation might fail.
- If Device Manager agent version 4.1 to 5.1 was upgraded to version 5.5 or later by an overwrite installation in an environment where the non-global zone is specified, it will be installed in both the global zone and the non-global zone. The Device Manager agent is not required for the non-global zone because the Device Manager agent runs only in the global zone. To uninstall the Device Manager agent from the non-global zone, log in to the non-global zone, and then execute the following command:

```
# pkgrm HDVMAgent
```

Before Installing in AIX

Keep the following notes in mind regarding installation of Device Manager agents in an AIX environment.

- When IBM XL C/C++ Enterprise Edition V8 for AIX Runtime version 8.0.0.3 to 8.0.0.5 has been applied, the overwrite installation of the Device Manager agent will hang if either of the following conditions exists:
  - The installed version of Dynamic Link Manager is from 5.8 to earlier than 5.9.
  - The version of the installed Device Manager agent is from 5.0 to 5.1.03.

  When you use the Device Manager agent, upgrade IBM XL C/C++ Enterprise Edition V8 for AIX Runtime to version 8.0.0.6 or later, or apply the patch (APAR IY87291). For details about the patch, see the IBM Web site.

  Use the following command to check the version of IBM XL C/C++ Enterprise Edition V8 for AIX Runtime:

  ```
  # lslpp -L xlC.aix50.rte
  ```

- AIX has the Stack Execution Disable (SED) function that protects systems from attacks that use a buffer overflow. If the SED mode is set to `all`, you need to change the mode to a mode other than `all` before installing the Device Manager agent. To change the SED mode to a mode other than `all`, execute the following command:

  ```
  # sedmgr -m {select|off|setidfiles}
  ```

  For details about the `sedmgr` command, see the AIX documentation.

  To return the SED mode to `all` after installing the Device Manager agent, exclude the Java process to be used by the Device Manager agent from the SED protection targets. For details, see When the Host OS Is AIX.

- The currently installed HDSHiScan package needs to be deleted before installing the Device Manager agent.

  We recommend that you remove any agent that you will not be using.

Caution: HDSHiScan is the name used for Device Manager agents earlier than version 2.2. HDVMAgent is the name used for version 2.2 and later. The HDSHiScan package is installed in the `/usr/HDVM` directory.

To delete the HDSHiScan package:

a. At the prompt, execute the following commands to check whether a HiScan package is installed:

```
% su
% lslpp -l HDSHiScan.rte
```

If the HDSHiScan package is installed, confirm the execution period of the `HiScan` command before uninstalling by executing the following commands:

```
% su
# crontab -l
```

For details about how to interpret the execution period of the `HiScan` command, see HiScan Command Syntax.

b. Execute the following commands to remove the existing HiScan package.

For a Device Manager agent whose version is 2.4 or earlier:

```
% su
% installp -u HDSHiScan.rte
```

For a Device Manager agent whose version is 3.0 or later:

```
# /usr/HDVM/bin/.uninstall.sh
```

Before Installing in Linux

If a Linux firewall is configured, the Device Manager agent might be unable to communicate with the Device Manager server. In that case, execute the `iptables stop` command on the Linux host to disable `iptables`, and then configure the host to not automatically start `iptables` when the OS starts, or configure `iptables` so that the Device Manager releases the port in use. For the port numbers used, see the *Hitachi Device Manager Server Configuration and Operation Guide*.

Before Installing in HP-UX

Keep the following notes in mind regarding the installation of the Device Manager agent in an HP-UX environment.

- If you perform the installation on a workstation, the following message will be displayed and the installation will fail:

```
ERROR: Could not apply the software selection "HDVMAgent" because there
are no product variations that are compatible with the destination
host(s).
```

- When installing the Device Manager agent, the `swagentd` daemon needs to be running. If the `swagentd` daemon is not running, execute the following command to start it.

```
/usr/sbin/swagentd
```

- Confirm that the file system currently mounted on the host matches the file system defined in `/etc/fstab`, and then install the Device Manager agent.
- Before installing the Device Manager agent, make sure that the network settings such as those in the `hosts` file are correct.
- The currently installed HDSHiScan package needs to be deleted before installing the Device Manager agent.

  We recommend that you remove any agent that you will not be using.

Caution: HDSHiScan is the name used for versions earlier than 2.2. HDVMAgent is the name used for version 2.2 and later. The HDSHiScan package is installed in the `/opt/HDVM` directory.

To delete the HDSHiScan package:

a. At the prompt, execute the following commands to check whether a HiScan package is installed:

```
% su
```

If the HDSHiScan package is installed, check the execution period of the `HiScan` command before uninstalling by executing the following commands:

```
% su
# crontab -l
```

For details about how to interpret the execution period of the `HiScan` command scheduling entry, see HiScan Command Syntax.

b. Execute the following commands to remove the existing HiScan package.

```
% su
# swremove HDSHiScan
```

Performing an Installation in UNIX

This section describes how to install the Device Manager agent in UNIX. The Device Manager agent will be installed to a following location.

After completing a new installation of the Device Manager agent, you can immediately perform the setup procedure.

When an overwrite installation is performed, the previously defined information, such as the Device Manager server information or the execution period of the `HiScan` command, will be inherited.

To perform an installation of the Device Manager agent:

1. Log in as the `root` account.
2. If the host OS is Solaris, AIX, or HP-UX, make sure that the prerequisite software that provides a Java execution environment is installed.

   For details about how to check, see Prerequisite Java Execution Environments.

Caution: When performing an overwrite installation in an environment where the installed version of the Device Manager agent is from 5.0 to 5.9, if the prerequisite software that provides a Java execution environment is not installed on the host, JRE 1.4 bundled with version 5.0 to 5.9 of the Device Manager agent will continue to be used.

After the overwrite installation finishes, install the appropriate software that provides a Java execution environment, and then change the setting of `server.agent.JRE.location` in the `server.properties` file.

3. Insert the Device Manager agent CD-ROM and mount it.

Caution: If the CD-ROM cannot be automatically mounted, mount the CD-ROM to `/mnt/cdrom`.

4. Move to the directory that contains `install.sh`, and then execute the following command: `# ./install.sh`

   After the installation progress is displayed, the software license agreement is displayed.

   If the new installation completes successfully, the following message appears:

   ```
   Would you like to setup the Device Manager agent? (Y)es or (N)o.
   (default:Y)
   ```

Caution: If you do not agree to the user license agreement, uninstall the Device Manager agent after installation is completed.

5. To perform setup, enter Y. Otherwise, enter N.

   If you enter N, a message is displayed indicating that Device Manager server setup is required. Follow the instructions in the message to perform setup separately.

   If you enter Y, the following message is displayed:

   ```
   Do you want to specify the Device Manager server information? (Y)es
   or (N)o. (default:Y)
   ```

6. To set Device Manager server information, enter Y. Otherwise, enter N.

   Input information regarding the Device Manager server that will receive information reported from the host. This setting is required to use the Device Manager agent.

   If N is specified, information about the Device Manager server needs to be set manually after installation.

   If Y is specified, follow the messages to input information about the Device Manager server.

   IP address or host name

   For the message below, enter the IP address or host name for the Device Manager server. The default value is set if the **Enter** key is pressed without anything entered.

   ```
   Enter the IP address or hostname of the Device Manager server.
   (default: 255.255.255.255)
   ```

   Port number

   For the message below, enter the port number for the Device Manager server. The default value is set if the **Enter** key is pressed without anything entered.

   ```
   Enter the port number of the Device Manager server. (default:2001)
   ```

   User ID

   For the message below, enter the user ID for logging on to the Device Manager server. The default value is set if the **Enter** key is pressed without anything entered.

   In Device Manager, HaUser is prepared as a built-in account for use with the Device Manager agent.

   ```
   Enter the user ID for logging on to the Device Manager server.
   (default:HaUser)
   ```

   Password

   For the message below, enter the password for logging on to the Device Manager server.

   The default password for HaUser is haset.

   ```
   Enter the password for logging on to the Device Manager server.
   ```

   The following message is displayed if the connection with the Device Manager server is successful:

```
The connection to the server has been verified.
Do you want to specify the execution period of the HiScan command? (Y)es
or (N)o. (default:Y)
```

7. Enter `Y` to set an execution period for the `HiScan` command. Otherwise, enter `N`.

   Specify the execution period for the command for reporting host information to the Device Manager server (`HiScan` command).

   This setting is optional. If you do not specify the execution period, the Device Manager server is not periodically notified of information acquired by the Device Manager agent. To specify the execution period for the `HiScan` command at a later time, or if you do not want the `HiScan` command to execute automatically, enter `N`.

   If `Y` is specified, set the `HiScan` command execution period as instructed in the messages.

   Execution period

   For the following message, enter `H` for automatic hourly execution, `D` for automatic daily execution, or `W` for automatic weekly execution.

   ```
   Enter execution period: (H)ourly, (D)aily, (W)eekly (default:D)
   ```

Caution: When the Device Manager agent is installed on multiple hosts, set the `HiScan` command to execute daily or weekly to reduce the load of the Device Manager server. Also, vary the start times for execution of the `HiScan` command on each host so that the command is not executed simultaneously from multiple hosts. For details about how to check the execution period for the `HiScan` command, see HiScan Command Syntax.

Day of the week

If you enter `W`, specify the day of the week when automatic execution will be performed.

```
Enter a day of the week:
(0)Sun,(1)Mon,(2)Tue,(3)Wed,(4)Thu,(5)Fri,(6)Sat
```

Execution time

Specify the execution time for the `HiScan` command. Enter `Y` to use the default setting. To change the execution time, enter `N`.

```
Do you want to set the default time (2:30) to the execution time?
(Y)es or (N)o. (default:N)
```

To change the execution time, enter the time according to the prompts.

```
Enter time (hour): (0-23)
Enter time (minute): (0-59)
```

After entry for the `HiScan` command execution period is complete, the following message is displayed.

```
This will set the HiScan automatic execution schedule.
Are you sure? (Y)es or (N)o. (default:Y)
```

If you enter Y:

The execution period is set in the Device Manager agent, and the following message is displayed:

```
Configuration of the HiScan automatic execution schedule has completed.

Do you want to specify the RAID Manager installation directory? (Y)es or (N)o. (default:Y)
```

If you enter N:

Setting of the execution period for the Device Manager agent is canceled, and the following message is displayed:

```
Do you want to specify the RAID Manager installation directory? (Y)es or (N)o. (default:Y)
```

Caution: If the host OS is Red Hat Enterprise Linux AS/ES 3, do not specify the execution period for the `HiScan` command. If you have already specified the execution period, clear the setting. For details about how to clear this setting, see hdvmagt_schedule Command Syntax. If system operation requires that the `HiScan` command be executed automatically, do not execute any OS commands or the `dlmcfgmgr` command while the `HiScan` command is automatically executing.

8. To set the installation directory of CCI, enter `Y`. Otherwise, enter `N`.

   This setting is optional. Set this if linkage with CCI is used so that copy pairs can be managed in Device Manager. To specify this setting later, or if you do not want to use Device Manager to manage copy pairs, enter `N`.

   If you enter `Y`, follow the messages to specify the installation directory of CCI .

   Installation directory

   Enter the installation directory of CCI.

   ```
   Enter the RAID Manager installation directory. (default: /HORCM)
   ```

   Central management method

   Specify whether copy pairs will be centrally managed on hosts on which the Device Manager agent is installed. To perform central management, enter `Y`. Otherwise, enter `N`.

   ```
   Enter (Y)es when a single host centrally manages the creation, status change, and deletion of copy pairs.

   Do you want to be enable centrally manage pair configuration? (Y)es or (N)o. (default:N)
   ```

   After installation directory entry is completed, the following message is displayed indicating that Device Manager agent setup is complete.

   ```
   The Device Manager agent setup has completed successfully.
   ```

Caution:

- Write `localhost` and your host (host name) into the `/etc/hosts` file. When the host OS is Linux, write your host on the line above the `localhost` line. After this, restart the Device Manager agent service. For details about stopping and starting the Device Manager agent service, see Managing the Operating Status of the Device Manager Agent Service.
- In the following cases, the Device Manager agent service needs to be stopped after installation, and the following Device Manager agent property settings need to be changed.
  - If Device Manager is used in an IPv6 environment

    The following properties in the `server.properties` file need to be set:
    `server.http.socket.agentAddress`
    `server.http.socket.bindAddress`
  - If Dynamic Link Manager earlier than 5.8.0 is installed

    The port number used by the Device Manager agent needs to be set for the following properties in the `server.properties` file:
    `server.http.port`
    `server.agent.port`

  For details about stopping and starting the Device Manager agent service, see Managing the Operating Status of the Device Manager Agent Service. For details about the `server.properties` file, see The server.properties File.

Performing an Unattended Installation of the Device Manager Agent

The Device Manager agent has unattended installation capability, which does not require any user input. Users can automatically install a Device Manager agent on multiple hosts by creating and executing a script file. This section describes how to perform an unattended installation of the Device Manager agent.

Overview of an Unattended Installation

There are two ways to execute an unattended installation:

- Automatically install, and then manually specify the settings after the installation

  After a Device Manager agent is automatically installed, manually specify the settings for communicating with the Device Manager server, the settings for the execution period of the `HiScan` command, and the settings for using CCI.

- Automatically install, and automatically specify the settings after the installation

  The following operations are performed automatically: installation of a Device Manager agent, the settings for communicating with the Device Manager server, and the settings for the execution period of the `HiScan` command. Before an installation, you need to create an auto-setting file that contains the data to be specified when the installation is completed.

Caution: After an installation, the Device Manager agent will check whether it can connect to the Device Manager server. If the agent fails to connect to the server, settings will not be specified after the installation. In such a case, you need to manually specify the settings.

Note: When using unattended installation, observe the following critical points:

- For an overwrite installation, version 4.1 or later of the Device Manager agent must already be installed.
- The Device Manager agent cannot be automatically registered as an exception to the Windows firewall.

Unattended Installation Procedure

This subsection describes how to perform an installation without needing to respond to displayed prompts during installation. Before installation, check the free disk space and the installation status of other programs, as is performed in a normal installation. For details about how to check these items, see Before Installing in Windows for Windows, or Before Installing in UNIX for UNIX.

To install the Device Manager agent:

1. If you want the post-installation setup performed automatically, edit the `HDVMAgent.conf` file. If you want to perform post-installation setup manually, go to step 2.

   Refer to Properties to Specify for Automatic Post-installation Setup and set up `HDVMAgent.conf`.

Caution: If `HDVMAgent.conf` is stored on unwritable storage media, such as the installation CD, copy the directory that stores `HDVMAgent.conf` to writable media, and then edit `HDVMAgent.conf`.

2. Open the command prompt in Windows, or open the shell in UNIX.

   For Windows Server 2008 or Windows Server 2008 R2, open the elevated command prompt.

3. Move to the directory that stores the installer execution file (`setup.exe` in Windows, or `install.sh` in UNIX).

Caution: If the installer execution file is in a location where the permission cannot be changed, move it to a location where the permission can be changed.

4. Execute the installer execution file in the format shown below. Installation will start.

   The format for executing unattended installation is shown below.

   – In Windows:

     `start /WAIT setup.exe /s [`*Device-Manager-agent-installation-folder*`] [/u]`

     The Device Manager agent installation folder is enabled only for a new installation. If this setting is not made, the Device Manager agent will be installed in the default installation folder. For details about the default installation folder and the number and type of characters that can be specified for it, see Performing a New Installation in Windows.

   – In UNIX:

     `install.sh -s [-u]`

   The command options for executing unattended installation are shown below:

   `/s` or `-s`

   Specify this option when executing an unattended installation.

   `/u` or `-u`

   Specify this option if you want the settings to be automatically specified after installation.

Caution:

- If `HDVMAgent.conf` is stored on read-only media such as the installation CD, copy `HDVMAgent.conf` from the installation CD to a writable media and edit the file.
- Do not specify two or more sets of data to a single item. Make sure that you specify `serverIP`, `serverPort`, and `HiScanPeriod`.

No error messages are displayed during an unattended installation, even if the installation fails. Refer to the values returned in the execution results to resolve any problems that occur. To check the values returned in the execution results, execute the following command in the directory that stores the installer execution file:

In Windows:

```
> echo %ERRORLEVEL%
```

In UNIX:

```
# echo $?
```

Table 2-5 describes the return values of the unattended installation results.

5. If you want to perform post-installation setup manually, execute the `hdvm_account`, `hdvmagt_schedule`, or `hdvmagt_setting` command.

   For details about each command, see hdvmagt_account Command Syntax, hdvmagt_schedule Command Syntax, or hdvmagt_setting Command Syntax.

Table 2-5 Return Values of the Unattended Installation Results

Return value[#]	Description	Action
0x00	Ended normally.	None.
0x90	A failure occurred during the installation of the Device Manager agent.	The following are likely causes: ▪ There is insufficient free disk space. Secure sufficient disk space, and then perform the installation again. ▪ The OS where the installation is being performed is not supported. Check the OS. ▪ An installation or uninstallation underway for a program other than the Device Manager agent. Wait for the current installation or uninstallation to finish, and then perform the Device Manager agent installation again. In UNIX, the following causes are also possible: ▪ The software that provides the Java execution environment cannot run. Make sure that the patches required for the Device Manager agent have been applied to the host OS. Also, make sure that the software that provides the Java execution environment is installed in the location indicated by the installation path specified in the property `server.agent.JRE.location` of the `server.properties` file. ▪ The software that provides a Java execution environment, which is prerequisite software for the Device Manager agent, is not installed. Install the software, and then retry the installation of the Device Manager agent. ▪ The permission for the installer execution file could not be changed. Move all files and subdirectories in the directory where the installer execution file exists to a location where the permission can be changed, and then execute the installation again.
0x91	The installation command contains a syntax error.	The syntax of the installation command argument is incorrect. Correct the syntax, and then perform the installation again.
	The specified value for the installation directory is not correct.	The installation directory has been specified using characters that cannot be used, or exceeds 64 bytes. Correct the setting, and then perform the installation again. Space character and the following characters can be in for the installation directory: `a-z A-Z 0-9 . _ ( )` Note that a space character cannot be specified for the first character or the last character of the directory name. Additionally, two or more space characters cannot be specified consecutively.

Return value#	Description	Action
0x92	HDVMAgent.conf is not stored in the directory in which the installer execution file is stored, or HDVMAgent.conf contains some setting errors.	Installation failed. Perform the following depending on the cause of the error: ▪ HDVMAgent.conf is not stored in the directory in which the installer execution file is stored. Store HDVMAgent.conf in the directory in which the installer execution file is stored and execute the installation again. ▪ HDVMAgent.conf contains some setting errors. Correct the errors and execute the installation again.
0x93	The Device Manager agent was successfully installed, but the settings for linking to other program products could not be applied.	For an environment in which Protection Manager Console has been installed, execute either hptmguiinst.exe or hptmguiinst.sh. Check the error message, take the appropriate action to correct the error, and then perform the installation again. For an environment in which the GUI for Dynamic Link Manager has been installed, contact maintenance personnel for assistance. If the OS is Solaris, the installation of the Global Link Manager agent might have failed. Execute the installation again. If the error still persists, contact maintenance personnel for assistance.
0x95	Setup of the Device Manager agent functionality succeeded. However, an error might have occurred while setting up Provisioning Manager agent functionality or Replication Manager agent functionality.	Make sure that the OS is supported and the required patches have been applied, and then perform installation again. If you cannot solve the problem, contact maintenance personnel for assistance.
0x96	The user attempting this operation does not have Administrator permissions.	Retry the operation by using a user ID that has Administrator permissions.
0x98	You cannot downgrade the Device Manager agent because a newer version of the Device Manager agent is installed.	None
0x99	The Device Manager agent or a related program is running.	Take action by following the KAIC25111-W to KAIC25113-W messages. For details about the action to be taken when each message is output, see the *Hitachi Device Manager Error Codes*.
0x9A	setup.exe might not have started correctly, or a user might have executed an internal command manually.	Take action by following the KAIC25156-E message. For details about the action to be taken when the KAIC25156-E message is output, see the *Hitachi Device Manager Error Codes*.

Return value#	Description	Action
0x9D	A failure occurred while connecting to the Device Manager server specified in HDVMAgent.conf.	Use the hdvmagt_account command or hdvmagt_setting command to specify the IP address or host name of the Device Manager server again.
#: Return values are output in hexadecimal.		

Properties to Specify for Automatic Post-installation Setup

This subsection describes the properties to be specified in the HDVMAgent.conf file when you want the post-installation setup performed automatically.

The following table describes property names, data to be set, specification examples of the properties, and the default values for when the properties are not specified. Open HDVMAgent.conf with a text editor and specify the settings for the properties.

Caution: Do not specify the same property more than once.

Table 2-6 Data to Be Set in HDVMAgent.conf

Property	Data to be set	Specification example	Default value
serverIP (required)	Specify the IP address or host name of the Device Manager server. You can specify an IPv6 address as the IP address. When you specify an IPv6 address, make sure that you specify a global address. Specify a character string of 50 bytes or less for the host name. You can use the following characters as the host name: A to Z, a to z, 0 to 9, hyphen (-), underscore (_), period (.), at mark (@)	▪ When specifying an IP address in IPv4 format: serverIP=129.144.52.38 ▪ When specifying an IP address in IPv6 format: serverIP=2001:0:0:0:8:800:200C:417A ▪ When specifying hdvmlocalhost as a host name: serverIP=hdvmlocalhost	None

Property	Data to be set	Specification example	Default value
serverPort (required)	Specify the port number of the Device Manager server. Specify a number between 0 and 65535.	▪ When specifying 2001 as a port number: serverPort=2001	2001
HiScanPeriod (required)	Specify the interval of HiScan. Specify one of the following according to your needs. This property is not case sensitive. ▪ H: Once an hour ▪ D: Once a day ▪ W,SUN: Once every Sunday ▪ W,MON: Once every Monday ▪ W,TUE: Once every Tuesday ▪ W,WED: Once every Wednesday ▪ W,THU: Once every Thursday ▪ W,FRI: Once every Friday ▪ W,SAT: Once every Saturday ▪ N: No interval	▪ When specifying the execution period of the HiScan command as once a day: HiScanPeriod=D ▪ When specifying the execution period of the HiScan command as once every Monday: HiScanPeriod=W,MON	D

Property	Data to be set	Specification example	Default value
HiScanSchedule (optional)	Specify the timing for executing the HiScan command. To specify this timing, you can use one of the following methods: When specifying the execution time of the HiScan command at a scheduled time: Specify this option to periodically execute the HiScan command at the predefined time. Select one of the following execution periods of the HiScan command: - Once an hour at a specified time. - Once a day at a specified time. - Once a week at a specified time. When specifying execution of the HiScan command at random times: Specify this option, in an environment where multiple hosts are connecting to the Device Manager server, to execute the HiScan command at random times on multiple hosts during the predefined period of time. By specifying execution of the HiScan command at random times, the load on the Device Manager server when the HiScan command is executed can be decreased because the execution time of the HiScan command on each host is unlikely to be the same. Select one of the following execution periods of the HiScan command: - Once an hour, at a random time during the specified period of time. - Once a day, at a random time during the specified period of time. - Once a week, at a random time during the specified period of time. Specify the value as follows. *hh* should be from 0 to 23 and *mm* should be from 0 to 59. If the value is a one-digit number, you can specify the value as a one-digit number or two-digit number. For example, when specifying 1 for *hh*, you can specify 1 or 01. When specifying a scheduled time for the execution: Specify a value as follows: ▪ When the execution period is once a day or once a week: *hh*:*mm* ▪ When the execution period is once an hour. *mm*	▪ When specifying the execution time of the HiScan command as 2:30: HiScanSchedule=2:30 ▪ When specifying random execution of the HiScan command between 2:30 and 5:30: ▪ HiScanSchedule=2:30-5:30	2:30

Property	Data to be set	Specification example	Default value
	When specifying execution at random times: Specify a value as follows: ▪ When the execution period is once a day or once a week: *hh*:*mm*-*hh*:*mm* (start-time to end-time) ▪ When the execution period is once an hour. *mm*-*mm* If the start time is later than the end time, the end time is set for the next day or hour (example: 23:00-1:00 or 45-15). If the start time and the end time are set to the same time, the HiScan command executes as if you had specified a scheduled time for the command to execute. ***Caution:*** ▪ If H is specified for HiScanPeriod, be sure to change the format of this property value from the *hh*:*mm* format to the *mm* format. If you do not change the format of the property value, installation will fail ▪ If N is specified for HiScanPeriod, this property value is ignored.		
configOverwrite (optional)	Specify whether to overwrite the settings during an overwrite installation. enable: Overwrite the settings disable: Do not overwrite the settings This property is not case sensitive. ***Caution:*** If you specify enable to perform an overwrite installation of the Device Manager agent, the user ID and password used for communication with the Device Manager server are set to the default. The default user ID and password are HaUser and haset respectively. If you want to specify the user ID and the password again, see hdvmagt_account Command Syntax or hdvmagt_setting Command Syntax to change the user ID and the password.	▪ When overwriting the settings: configOverwrite=enable ▪ When not overwriting the settings: configOverwrite=disable	disable

Uninstalling the Device Manager Agent

This section explains how to uninstall Device Manager agents.

Caution:

- When Device Manager agent uninstallation is started, Device Manager agents and add-on modules are automatically stopped. If stop processing fails, follow the instructions in Managing the Operating Status of the Device Manager Agent Service.
- Do not execute any of the following commands during uninstallation. Also, do not perform uninstallation while the following commands are executing:
  - `hbsasrv`
  - `hdvmagt_account`
  - `hdvmagt_schedule`
  - `hdvmagt_setting`
  - `HiScan`
  - `hldutil`
  - `TIC`

  If you attempt uninstallation while the `HiScan` command is executing, uninstallation will stop. Therefore, wait for the execution to finish, and then perform the uninstallation again.

  If you attempt to perform uninstallation while a command other than the `HiScan` command is executing, the uninstallation might end abnormally. In this case, reboot the computer.
- If Dynamic Link Manager version 5.8 or later or a Global Link Manager agent version 6.2 or later is installed, the following data remains even after the Device Manager agent has been uninstalled:
  - Data in the Device Manager agent installation folder
  - Data in the Java execution environment installation folder

  This data is deleted when all of the installed Dynamic Link Manager and Global Link Manager agents are uninstalled.
- Files created by using the `HiScan` command, CCI configuration definition files, and error information files created from the results of TIC commands cannot be deleted.

Uninstalling the Device Manager Agent in Windows

After you uninstall the Device Manager agent in a Windows environment, you must manually delete tasks that execute the `HiScan` command.

Uninstalling in Windows

To uninstall the Device Manager agent:

1. Log on to Windows as a user with Administrator permissions.
2. Perform one of the following:
   - Display the Windows Add or Remove Programs window, select **Hitachi Device Manager agent**, and then click the **Change or Remove Programs** button.
   - Execute `agent_uninstShortcut.bat`.

     `agent_uninstShortcut.bat` is stored in the following location:

     Device-Manager-agent-installation-folder`\bin\`

Caution:

- If the host OS is Windows Server 2008 or Windows Server 2008 R2, execute the batch file at a command prompt that was started by a user with administrator permissions.
- For a Windows Server 2008 or Windows Server 2008 R2 Server Core environment, execute `agent_uninstShortcut.bat`.

   The Remove the Program window is displayed.
3. Click the **Remove** button.

   Uninstallation processing starts. Once uninstallation processing has started, it cannot be canceled midway.

Caution: If an empty folder remains under the installation folder after uninstalling the Device Manager agent, log on to Windows again and delete it manually.

Even if the Device Manager agent is uninstalled, the following folder and files for the Global Link Manager agent might remain. The folder and files are automatically deleted when the machine is restarted.

For a 32-bit architecture (x86) OS:

system-drive\Program Files\HITACHI\HGLMAgent\uninst\
system-drive\Program Files\HITACHI\HGLMAgent\uninst\setup.exe
system-drive\Program Files\HITACHI\HGLMAgent\uninst\setup.iss
system-drive\Program Files\HITACHI\HGLMAgent\uninst\setup.log

For a 64-bit architecture (IPF or x64) OS:

system-drive\Program Files (x86)\HITACHI\HGLMAgent\uninst\
system-drive\Program Files (x86)\HITACHI\HGLMAgent\uninst\setup.exe
system-drive\Program Files (x86)\HITACHI\HGLMAgent\uninst\setup.iss
system-drive\Program Files (x86)\HITACHI\HGLMAgent\uninst\setup.log

Deleting Tasks that Execute the HiScan Command

The following tasks that execute the HiScan command are not deleted when the Device Manager agent is uninstalled.

- Tasks that execute exeHiScan.bat whose task schedule was modified by a user using **Scheduled Tasks** in the Control Panel
- Tasks that execute exeHiScan.bat in Windows Server 2003, Windows Server 2003 R2, Windows Server 2008 or Windows Server 2008 R2

Delete these tasks from **Scheduled Tasks** in the control panel.

Uninstalling the Device Manager Agent in UNIX

This section explains how to uninstall the Device Manager agent in a UNIX environment.

Caution:

- If the host OS is Solaris 10, do not perform any system zone settings while the Device Manager agent is being uninstalled, or uninstallation might fail.
- If the host OS is HP-UX, the swagentd daemon needs to be running when the Device Manager agent is uninstalled. If the daemon is not running, execute the following command to start it: /usr/sbin/swagentd
- If the host OS is HP-UX, make sure that the file system currently mounted on the host matches the file system defined in /etc/fstab before uninstalling the Device Manager agent.

To uninstall the Device Manager agent:

1. Log in as the `root` account.
2. Execute the following command from the command line:

   Solaris, Linux and HP-UX:

   ```
   # /opt/HDVM/HBaseAgent/bin/.uninstall.sh
   ```

   AIX:

   ```
   # /usr/HDVM/HBaseAgent/bin/.uninstall.sh
   ```

   The following message appears:

   ```
   Are you sure to UNINSTALL Device Manager - Agent? (Y)es or (N)o:
   ```

3. Enter `Y`.

   When uninstallation finishes, the following message appears:

   ```
   Device Manager - Agent removed successfully.
   ```

Performing an Unattended Uninstallation of Device Manager Agent

The Device Manager agent has the unattended uninstallation function, which does not require any input from the user. By creating and executing script files, the Device Manager agent can be automatically uninstalled from multiple hosts.

Unattended Uninstallation in a Windows Environment

To perform an unattended uninstallation in a Windows environment:

1. Log on to Windows as a user with Administrator permissions.
2. Copy the following file to a desired location:

   Device-Manager-agent-installation-folder`\bin\agent_uninstShortcut.bat`
3. At the command prompt, execute the following batch file:

   copy-destination-folder`\agent_uninstShortcut.bat /s`

   When this batch file is executed, the progress of the unattended uninstallation is displayed.

Caution:

If the host OS is Windows Server 2008 or Windows Server 2008 R2, execute the batch file at a command prompt that was started by a user with administrator permissions.

No error messages are displayed during the execution of unattended uninstallation, even if the uninstallation fails. To resolve any problems that occur, refer to the values returned in the execution results.

After finishing unattended uninstallation, delete the copied file `agent_uninstShortcut.bat`.

Unattended Uninstallation in a UNIX Environment

To perform an unattended uninstallation in a UNIX environment:

1. Log in as the root account.
2. Execute the following command from the command line:

   In Solaris, Linux, or HP-UX:

   ```
   /opt/HDVM/HBaseAgent/bin/.uninstall.sh -s
   ```

   In AIX:

   ```
   /usr/HDVM/HBaseAgent/bin/.uninstall.sh -s
   ```

No error messages are displayed if unattended uninstallation fails. For this reason, always check the return value of the execution results and remove the cause of the problem.

Return Values in the Execution Results of Unattended Uninstallation

The following table lists and describes the return values of the execution results of unattended uninstallation.

Table 2-7 Return Values of the Execution Results of Unattended Uninstallation

Return value#	Description	Action
0x00	Normal termination	-
0x90	Uninstallation of Device Manager agent failed.	The following are likely causes: ▪ An installation or uninstallation underway for a program other than the Device Manager agent. Wait for the current installation or uninstallation to finish, and then perform the Device Manager agent installation again. In Solaris, AIX, Linux, or HP-UX, the following causes are also possible: ▪ Uninstallation of a related program failed. Contact maintenance personnel. ▪ The software that provides the Java execution environment cannot run. Make sure that the patches required for the Device Manager agent have been applied to the host OS. Also, make sure that the software that provides the Java execution environment is installed in the location indicated by the installation path specified in the property server.agent.JRE.location of the server.properties file.
0x91	The uninstallation command contains a syntax error.	The syntax of the uninstallation command argument is not correct. Correct the syntax, and then perform the uninstallation again.
0x93	A failure occurred while uninstalling another program product.	Uninstallation of the Global Link Manager agent might have failed. Execute the uninstallation again. If the error still persists, contact maintenance personnel for assistance.

Return value#	Description	Action
0x96	The user attempting this operation does not have Administrator permissions.	Retry the operation by using a user ID that has Administrator permissions.
0x99	The Device Manager agent or a related program is running.	Follow the KAIC25111-W to KAIC25113-W messages and act accordingly. For details about what to do when each message is displayed, see the *Hitachi Device Manager Error Codes*.
0x9B	The current directory is in the Device Manager agent installation directory. This return value may be displayed in UNIX.	Move the current directory to another directory, such as the root directory, and then perform uninstallation again.
#: Return values are displayed in hexadecimal.		

3

Operating the Device Manager Agent

This chapter provides notes on managing host operations and explains Device Manager agent settings and operations.

Before Operating the Device Manager Agent

This section provides notes on Device Manager agent operations and the settings required before using Device Manager agent.

Operations that Require Restarting the Device Manager Agent Service

The Device Manager agent service needs to be restarted when:

- The IP address of a host in which the Device Manager agent is installed is changed
- The HBA driver or HBA API library is installed on a host in which the Device Manager agent is installed
- A host in which the Device Manager agent is running is deleted in the Web Client host management window
- The contents of the property files of the Device Manager agent are modified
- A new installation of the Device Manager server is performed after the OS is re-installed on the management server
- CCI is installed or uninstalled
- Dynamic Link Manager is installed or uninstalled on AIX or Linux
- Execution of the `hdvmagt_account` command is interrupted
- The `hdvmagt_account` command is executed in Windows
- Execution of the `hdvmagt_setting` command is interrupted

For details about stopping and starting the Device Manager agent service, see Managing the Operating Status of the Device Manager Agent Service.

If the Device Manager server service is not running, information is not reported to the server even if a Device Manager agent is installed or a Device Manager agent service starts. For information to be reported to the Device Manager server, verify that the Device Manager server service is running, and then install a Device Manager agent or start the Device Manager agent service.

When a Host Has Multiple Network Adapters

When the Device Manager agent runs on a host that has multiple network adapters, specify the IP address of the network adapter used by the Device Manager agent in the `server.http.socket.agentAddress` property in the `server.properties` file. For details about this file, see The server.properties File.

Changing the Storage Subsystem Configuration

The OS might not recognize the modified contents immediately after the storage subsystem configuration is changed (for example, when an LU is registered or deleted). In this case, the Device Manager agent reports the old information to the Device Manager server. If the changes to the storage subsystem configuration have not been applied to the Device Manager server, execute the `hldutil` command to obtain the latest information, and then execute the `HiScan` command.

For details about the `hldutil` command, see hldutil Command Syntax. For details about the `HiScan` command, see HiScan Command Syntax.

Upgrading the Host OS

If you have installed the Device Manager agent and then upgraded the host OS under any of the following conditions, perform an overwrite installation of the Device Manager agent:

- Upgrading Solaris from a version earlier than 9 to version 9 or later
- Upgrading AIX from a version earlier than 5.2 to version 5.3 or later
- Upgrading HP-UX from a version earlier than 11i v2 to version 11i v2 or later

When the Host OS Is Windows

This section provides notes that are specific to hosts using Windows.

Allocation Device Drives

The Device Manager agent will not acquire data from devices assigned drive letter A or B. Assign a drive letter from C to Z for a device managed by the Device Manager agent.

When a Firewall Is Enabled

To run a Device Manager agent on a computer on which Windows Firewall is active, you need to add the Device Manager agent to the Windows Firewall exceptions list.

To register Device Manager as an exception:

1. Execute the following commands to register the exception:

```
> netsh firewall add allowedprogram
program="installation-folder-for-the-Device-Manager-agent\agent\bi
n\hbsa_service.exe" name="HBase Agent" mode=ENABLE

> netsh firewall add allowedprogram
program="installation-folder-for-the-Device-Manager-agent\agent\JR
E1.5\bin\java.exe" name="HBase Agent" mode=ENABLE
```

Note: If Windows Firewall has been turned on for the first time, restart the computer.

2. Execute the following command to check the registered contents:

   ```
   > netsh firewall show all
   ```

   Confirm the following in the command execution results:

   – That `HBase Agent` is displayed.

   – That `Mode` is `Enable`.

   – That the paths to `hbsa_service.exe` and `java.exe` are correct.

Notes: Execute the following command to deactivate this setting:

```
> netsh firewall delete allowedprogram
"installation-folder-for-Device-Manager-agent\agent\bin\hbsa_service.exe"
> netsh firewall delete allowedprogram
"installation-folder-for-Device-Manager-agent\agent\JRE1.5\bin\java.exe"
```

When the Host OS Is AIX

To change the SED mode to `all`, follow the procedures below to register the Java process to be used by the Device Manager agent as an SED exception.

To register the Java process as an SED exception:

1. Execute the following command to register the Java process to be used by the Device Manager agent as an SED exception:

   ```
   # sedmgr -c exempt
   installation-path-of-the-software-that-provides-a-Java-execution-environment-and-is-used-by-the-Device-Manager-agent/bin/java
   ```

   If this command execution succeeds, no execution results are output.

2. Execute the following command to ensure that the Java process to be used by the Device Manager agent has been registered as an SED exception:

   ```
   # sedmgr -d
   installation-path-of-the-software-that-provides-a-Java-execution-environment-and-is-used-by-the-Device-Manager-agent/bin/java
   ```

   If the Java process has been registered as an SED exception, the following information will be displayed:

   ```
   installation-path-of-the-software-that-provides-a-Java-execution-environment-and-is-used-by-the-Device-Manager-agent/bin/java : exempt
   ```

3. Restart the host.

You can use the `server.agent.JRE.location` property in the `server.properties` file to check the installation path of the software that provides a Java execution environment and is used by the Device Manager agent. For details about the properties, see The server.properties File.

When the Host OS Is Linux

The following are notes for when the host OS is Linux.

When the Host OS Is Red Hat Enterprise Linux AS/ES 3

If the host OS is Red Hat Enterprise Linux AS/ES 3, note the following:

- Do not perform the following operations while updating host information in the Device Manager client:
  - Setting up a host (creating or deleting a device file; or creating, expanding, or deleting a file system) by using the Provisioning Manager client
  - Executing the Dynamic Link Manager `dlmcfgmgr` command
  - Executing disk control-related commands (such as `blockdev`)

- Do not perform the following operations while starting the Device Manager agent:
  - Setting up a host (creating or deleting a device file; or creating, expanding, or deleting a file system) by using the Provisioning Manager client
  - Executing the Dynamic Link Manager `dlmcfgmgr` command
  - Executing disk control-related commands (such as `blockdev`)
- Do not perform the following operations concurrently with the Device Manager agent `HiScan` command or `hldutil` command:
  - Setting up a host (creating or deleting a device file; or creating, expanding, or deleting a file system) by using the Provisioning Manager client
  - Executing the Dynamic Link Manager `dlmcfgmgr` command
  - Executing disk control-related commands (such as `blockdev`)
- Do not perform automatic execution of the Device Manager agent `HiScan` command.

  If the `HiScan` command has been set for automatic execution, cancel this setting. For details about the procedure, see hdvmagt_schedule Command Syntax.

  If the `HiScan` command needs to be automatically executed for system-operational reasons, do not execute any OS commands or the `dlmcfgmgr` command during automatic execution of the `HiScan` command.

Using the rpm Command

If you attempt to display the Device Manager agent package information using the `rpm -V` command, the command will fail. This does not affect Device Manager agent operations.

Setting up the Device Manager Agent

This section explains the settings required to start Device Manager agent operations.

If the following settings were not specified during a new installation of the Device Manager agent, execute the `hdvmagt_setting` command to specify the required settings. For details about the `hdvmagt_setting` command, see hdvmagt_setting Command Syntax.

- Settings for Device Manager server information (required)
- Settings for the interval for reporting host information to the Device Manager server (optional)
- Settings for managing copy pairs in Device Manager (optional)

In addition, specify the following settings as necessary:

- Settings for changing the user of the Device Manager agent service (optional)

  For details, see Changing the User of the Device Manager Agent Service.
- Settings required when 100 or more LUs are managed for a host (optional)

  For details, see Specifying Settings When a Host Manages 100 or More LUs.
- Settings for managing copy pairs in Replication Manager (optional)

  For details, see Specifying Settings for Managing Copy Pairs in Replication Manager.

Setting Device Manager Server Information

When the Device Manager server to be notified is changed, or the IP address or host name of the Device Manager server to be notified is changed, execute the `hdvmagt_account` command to set the Device Manager server information in the Device Manager agent. For details about the command, see hdvmagt_account Command Syntax.

For Windows, restart the Device Manager agent service after executing the `hdvmagt_account` command. For details on starting and stopping the Device Manager agent service, see Managing the Operating Status of the Device Manager Agent Service.

Setting the Cycle of Reporting Host Information to the Device Manager Server

To automatically send host information from a Device Manager agent to the Device Manager server, use the `hdvmagt_schedule` command. It sets the notification interval (`HiScan` command execution period). For details about the command, see hdvmagt_schedule Command Syntax.

- If the host OS is Red Hat Enterprise Linux AS/ES 3, do not set the notification interval. If regular notification is set, clear the setting.

  If host information needs to be reported regularly due to the system operations, avoid executing OS commands or the `dlmcfgmgr` command during the notification time interval.

- If Device Manager agents are installed on multiple hosts, set the notification intervals to daily or weekly to reduce the load on the Device Manager server. Adjust the execution time so that multiple hosts are not notifying the Device Manager server at the same time.

  The currently set execution time can be checked from `KAIC22805-I` messages and `KAIC22804-I` messages in the `HiScan.log` file, which is stored in the following locations:

  In Windows:

  `installation-folder-for-Device-Manager-agent``\bin\logs\HiScan.log`

  In Solaris, Linux, or HP-UX:

  `/opt/HDVM/HBaseAgent/bin/logs/HiScan.log`

  In AIX:

  `/usr/HDVM/HBaseAgent/bin/logs/HiScan.log`

Specifying Settings for Managing Copy Pairs in Device Manager

To link with CCI and manage copy pairs in Device Manager, you need to specify the properties in the `server.properties` file as necessary. Specify these properties if any of the following conditions is met:

- When CCI is installed in a location other than the default location, or when the host OS is Windows and the CCI installation drive is different from the Device Manager agent installation drive:

  `server.agent.rm.location`

- When you want to centrally manage copy pairs in the storage subsystem managed by the Device Manager server from the management target host:

  `server.agent.rm.centralizePairConfiguration`

- When you want to unify the coding format of pair volume information into the `HORCM_DEV` or `HORCM_LDEV` format when creating pairs:

  `server.agent.rm.pairDefinitionForm`

Note: If you use Hitachi AMS 2000, Hitachi SMS, Hitachi AMS/WMS, Thunder 9500V series, or Thunder 9200 storage to manage copy pairs, and if pair volume information is written in HORCM_DEV format, we recommend that you change to the HORCM_LDEV format. Note that before you change to the HORCM_LDEV format, CCI 01-17-03/04 or later needs to be installed.

If pair volume information is written in HORCM_DEV format for these storage subsystems, it might take a long time to perform the following operations:

- Refreshing hosts
- Refreshing subsystems

- When you want to exclude a volume pair that is already managed by CCI from Device Manager operations

  `server.agent.rm.exclusion.instance`

- When you want to optimize a user-created CCI configuration definition file so that it can be used in Device Manager

  `server.agent.rm.optimization.userHorcmFile`

For details about the properties, see The server.properties File. For details about how to use a user-created CCI configuration definition file in Device Manager, see Using a Configuration Definition File.

Changing the User of the Device Manager Agent Service

A LocalSystem account is established for the user who executes the Device Manager agent service. After installing the Device Manager agent, you can change the user who has Administrator permissions by completing the following steps.

To change the user who executes the Device Manager agent service:

1. Stop the Device Manager agent service.

   For details on this procedure, see Managing the Operating Status of the Device Manager Agent Service.
2. Open the Services window by selecting **Management Tools**, and then **Services**.
3. Select **HBsA Service**, **Operations**, and then **Properties**.

   The HBsA Service property window opens.
4. Click the **Logon** tab, and then select **Account**.
5. Set up the user and password, and then click **OK**.
6. From the Services window, select **HBsA Service**, and then start it.

Specifying Settings When a Host Manages 100 or More LUs

If 100 or more LUs are managed by Device Manager and are recognized by a single host, the following problems might occur:

- When the HiScan command is executed, the KAIC22009-E, KAIC22014-E, KAIC22019-E, or KAIC22048-E error message is output, and the host information cannot be registered in the Device Manager server.
- When performing operations such as refreshing the host, an OutOfMemory error occurs on the host and the host stops responding.

To prevent these issues, change the values shown as the following table. Note that the values set for these items differ depending on whether the host is using a volume manager. For more information, see Setting Values When a Volume Manager Is Not Used and Setting Values When a Volume Manager Is Used.

Table 3-1 Items to Set When Several LUs Are Recognized by a Host

Setting item	Description
The maximum length of data that can be received by the Device Manager server	Set the value for the server.http.entity.maxLength property in the server.properties file of the Device Manager server. For details about the server.properties file, see the *Hitachi Device Manager Server Configuration and Operation Guide*.
The timeout value for the processing to register information in a server	Set the value for the following property in the server.properties file of the Device Manager agent. ▪ server.http.server.timeOut ▪ server.util.processTimeOut For details about the server.properties file, see The server.properties File.
The memory heap size	Set the value for the server.agent.maxMemorySize property in the server.properties property file of the Device Manager agent. For details about the server.properties file, see The server.properties File.

Caution:

- Depending on the load status of the Device Manager server, an OutOfMemory error might occur. If the following error message is output to the log file specified for the `-t` option of the `HiScan` command or the `HiScan.msg` file, change the memory heap size of the Device Manager server by following the procedure described in the *Hitachi Device Manager Server Configuration and Operation Guide*.

```
<html><head><title>400 Bad request</title>
<meta http-equiv="Content-Type" content="text/html; charset=ISO-8859-1">
</head><body>
<h1>400 Bad request</h1>
<p><strong>ServiceConnection#0: java.lang.OutOfMemoryError</strong>
</body></html>
```

- The `HiScan.msg` file is stored in the following locations:
  - In Windows:
    installation-folder-for-the-Device-Manager-agent`\bin\logs\`
  - In Solaris, Linux, or HP-UX:
    `/opt/HDVM/HBaseAgent/bin/logs/`
  - In AIX:
    `/usr/HDVM/HBaseAgent/bin/logs/`

  In addition, to reduce the load of the Device Manager server, use the `hdvmagt_schedule` command to set the execution period of the `HiScan` command so that multiple hosts do not execute the `HiScan` command at the same time.

Notes:

- Depending on the environment, this issue might not be solved by setting the guide values. Make sure that you adjust the values to suit your environment.
- In the following cases, set a value two to three times larger than the guide value.
  - When executing the `HiScan` command shortly after restarting the Device Manager agent.
  - When executing the `hldutil` command and `HiScan` command at the same time.
  - When executing multiple `HiScan` commands at the same time.
- If the host OS is Windows Server 2003 (IPF), verify that Service Pack 1 or later has been installed.

Setting Values When a Volume Manager Is Not Used

The following table lists the recommended setting values when a volume manager is not used.

Table 3-2 Setting Values When a Volume Manager Is Not Used

Number of LUs managed by Device Manager, and recognized by the host	server.http.entity.maxLength (units: bytes)	server.http.server.timeOut (units: seconds)	server.util.processTimeOut (units: milliseconds)
100	131,072 or more	600 (Default value)	600,000 (Default value)
256	153,600 or more	600	600,000
512	307,200 or more	When managed in Device Manager: 600 When managed in Device Manager and Provisioning Manager: 1,000	600,000
1,024	614,400 or more	When managed in Device Manager: 1,200 When managed in Device Manager and Provisioning Manager: 1,800	1,200,000

Setting Values When a Volume Manager Is Used

Table 3-3 to Table 3-7 list, for each host OS, the general setting values when using a volume manager. These tables also list the setting values when the execution of the HiScan command finishes within an hour. Using a configuration where the number of LUs or logical volumes is more than the number shown in the tables is not recommended: It will take more than one hour for the HiScan operation to complete, and the operation might fail.

Table 3-3 Setting Values When a Volume Manager Is Used (in Windows)

Number of LUs and logical volumes managed by Device Manager and recognized by the host	server.http.entity.maxLength (units: bytes)	server.http.server.timeOut (units: seconds)	server.util.process TimeOut (units: milliseconds)	server.agent.max MemorySize (units: MB)
88/10	230,000 or more	600 (Default value)	600,000 (Default value)	64
88/20	750,000 or more	600	600,000	64
100/200	12,000,000 or more	600	600,000	128
100/500	30,000,000 or more	When managed in Device Manager 600 When managed in Device Manager and Provisioning Manager 1,000	600,000	384

Table 3-4 Setting Values When a Volume Manager Is Used (in Solaris)

Number of LUs and logical volumes managed by Device Manager and recognized by the host	server.http.entity.maxLength (units: bytes)	server.http.server.timeOut (units: seconds)	server.util.process TimeOut (units: milliseconds)	server.agent.max MemorySize (units: MB)
100/200	3,100,000 or more	600 (Default value)	600,000 (Default value)	128
100/500	7,200,000 or more	When managed in Device Manager 600 When managed in Device Manager and Provisioning Manager 1,000	600,000	384
150/500	12,000,000 or more	When managed in Device Manager 600 When managed in Device Manager and Provisioning Manager 1,000	600,000	512

Number of LUs and logical volumes managed by Device Manager and recognized by the host	server.http.entity.maxLength (units: bytes)	server.http.server.timeOut (units: seconds)	server.util.process TimeOut (units: milliseconds)	server.agent.max MemorySize (units: MB)
250/500	18,000,000 or more	When managed in Device Manager 600 When managed in Device Manager and Provisioning Manager 1,000	600,000	768
500/1,000	36,000,000 or more	When managed in Device Manager 600 When managed in Device Manager and Provisioning Manager 1,000	600,000	768
1,000/1,000	72,000,000 or more	1,200	600,000	768

Table 3-5 Setting Values When a Volume Manager Is Used (in AIX)

Number of LUs and logical volumes managed by Device Manager and recognized by the host	server.http.entity.maxLength (units: bytes)	server.http.server.timeOut (units: seconds)	server.util.process TimeOut (units: milliseconds)	server.agent.max MemorySize (units: MB)
100/200	2,500,000 or more	600 (Default value)	600,000 (Default value)	128
100/500	6,000,000 or more	When managed in Device Manager 600 When managed in Device Manager and Provisioning Manager 1,000	600,000	384
175/500	11,000,000 or more	When managed in Device Manager 600 When managed in Device Manager and Provisioning Manager 1,000	600,000	640

Number of LUs and logical volumes managed by Device Manager and recognized by the host	server.http.entity.maxLength (units: bytes)	server.http.server.timeOut (units: seconds)	server.util.process TimeOut (units: milliseconds)	server.agent.max MemorySize (units: MB)
250/500	15,000,000 or more	When managed in Device Manager 600 When managed in Device Manager and Provisioning Manager 1,000	600,000	768
500/1,000	19,000,000 or more	When managed in Device Manager 600 When managed in Device Manager and Provisioning Manager 1,000	600,000	768
1,000/1,000	38,000,000 or more	When managed in Device Manager 600 When managed in Device Manager and Provisioning Manager 1,000	600,000	768

Table 3-6 Setting Values When a Volume Manager Is Used (in HP-UX)

Number of LUs and logical volumes managed by Device Manager and recognized by the host	server.http.entity.maxLength (units: bytes)	server.http.server.timeOut (units: seconds)	server.util.process TimeOut (units: milliseconds)	server.agent.max MemorySize (units: MB)
100/50	745,000 or more	600 (Default value)	600,000 (Default value)	64
100/100	1,400,000 or more	When managed in Device Manager 600 When managed in Device Manager and Provisioning Manager 1,000	600,000	64
100/256	3,500,000 or more	When managed in Device Manager 600 When managed in Device Manager and Provisioning Manager 1,000	600,000	192
200/256	7,000,000 or more	When managed in Device Manager 600 When managed in Device Manager and Provisioning Manager 1,000	600,000	512
500/1,000	40,000,000 or more	When managed in Device Manager 600 When managed in Device Manager and Provisioning Manager 1,000	600,000	896
1,000/100	8,000,000 or more	When managed in Device Manager 600 When managed in Device Manager and Provisioning Manager 1,000	600,000	192

Number of LUs and logical volumes managed by Device Manager and recognized by the host	server.http.entity.maxLength (units: bytes)	server.http.server.timeOut (units: seconds)	server.util.process TimeOut (units: milliseconds)	server.agent.max MemorySize (units: MB)
1,000/500	42,000,000 or more	When managed in Device Manager 600 When managed in Device Manager and Provisioning Manager 1,000	1,200,000	896

Table 3-7 Setting Values When a Volume Manager Is Used (in Linux)

Number of LUs and logical volumes managed by Device Manager and recognized by the host	server.http.entity.maxLength (units: bytes)	server.http.server.timeOut (units: seconds)	server.util.process TimeOut (units: milliseconds)	server.agent.max MemorySize (units: MB)
100/50	748,000 or more	600 (Default value)	600,000 (Default value)	64
100/100	1,420,000 or more	When managed in Device Manager 600 When managed in Device Manager and Provisioning Manager 1,000	600,000	64
100/256	3,600,000 or more	When managed in Device Manager 600 When managed in Device Manager and Provisioning Manager 1,000	600,000	192
200/256	7,100,000 or more	When managed in Device Manager 600 When managed in Device Manager and Provisioning Manager 1,000	600,000	512

Specifying Settings for Managing Copy Pairs in Replication Manager

To use Replication Manager to manage copy pairs, you need to specify the properties below. If the properties are not set to appropriate values, the memory heap size might be insufficient or a timeout might occur during the Replication Manager processing.

- `agent.rm.TimeOut` property in the `agent.properties` file

  Adjust this value as necessary, while running Replication Manager and checking for timeouts during processing. For details about the `agent.rm.TimeOut` property, see The agent.properties File.

- `server.agent.maxMemorySize` property in the `server.properties` file

  Specify a value based on the number of pairs managed by a host (pair management server). By default, the heap runs in a 64-megabyte memory area. If the number of managed pairs exceeds 5,000, increase the memory heap size by 64 MB, and increase by another 64 MB for every 2,500 pairs above that. For example, if a host manages 6,000 pairs, set the `server.agent.maxMemorySize` property to 128. Also, if a host manages the configuration definition files for both a primary and secondary site, specify a value based on having twice as many managed pairs. For details about the `server.agent.maxMemorySize` property, see The server.properties File.

Operating the Device Manager Agent

This section explains Device Manager agent operations.

Managing the Operating Status of the Device Manager Agent Service

Immediately after Device Manager agent installation is completed, the Device Manager agent service is enabled. If you change settings in a properties file or execute a command, restart the Device Manager agent service as necessary.

Execute the `hbsasrv` command to start, stop, or check the operating status of the Device Manager agent service. For details about the `hbsasrv` command, see hbsasrv Command Syntax.

Caution:

- If you urgently need to stop the Device Manager agent, you can force the Device Manager agent to shut down by executing the `hbsasrv` command with the stop `-f` option. In such a case, all processing by the Device Manager agent service is forced to terminate, thus ongoing processing of jobs is not guaranteed.

Notes:

When the Device Manager agent service is started, the following service or daemon process will be started (dependent on the OS):

In Windows:

`hbsa_service.exe` (Service name: HBsA Service)

In UNIX:

`hbsa_service`

Reporting Host Information to the Device Manager Server

When the configuration of a storage subsystem connected to a host or the configuration of a file system on a host is changed, you can reflect the changes to the Device Manager server by manually executing the `HiScan` command. For details about the command, see HiScan Command Syntax.

Note: Information about the host on which a Device Manager agent is installed is automatically reflected to the Device Manager server when:

- The `HiScan` command is automatically executed
- The host machine is started
- Host information is updated from the Web Client

Checking the Version of the Device Manager Agent

Before you upgrade or restore the Device Manager agent, or when you want to find out which functions are supported in the Device Manager server, execute the `hdvm_info` command and confirm the version of the Device Manager agent installed on the host. For details about this command, see hdvm_info Command Syntax.

Using a Configuration Definition File

In Device Manager, you can use a user-created CCI configuration definition file to manage copy pairs.

Before Using Configuration Definition File in Device Manager

Before you create a configuration definition file, refer to Editing a Configuration Definition File so that you create a file that uses items supported by Device Manager. Store the created configuration definition file in the location shown in Configuration Definition File Storage Location.

In addition, to use the configuration definition file, the Device Manager agent must be installed on the host on which CCI is installed, and the settings for Device Manager server information and for managing copy pairs with Device Manager must be specified. For detailed settings information, see Setting Device Manager Server Information and Specifying Settings for Managing Copy Pairs in Device Manager.

Editing a Configuration Definition File

This subsection explains the required information, when you create a configuration definition file that can be used by Device Manager, or when you change a previously created configuration definition file.

Parameters Supported by Device Manager

Device Manager supports the following parameters:

- HORCM_MON
- HORCM_CMD
- HORCM_DEV
- HORCM_LDEV
- HORCM_INST
- HORCM_INSTP#
- HORCM_CTQM#

#

These parameters are supported by Device Manager agent version 6.2 or later. Note that when you create or use a copy pair, even if HORCM_INSTP or HORCM_CTQM information is defined in the configuration definition file, the Device Manager agent will operate while ignoring the definition. The Device Manager agent does not add the HORCM_INSTP or HORCM_CTQM definitions to the configuration definition file, nor does it add a pair group to the existing definitions. However, when you delete a pair, any definitions of that pair group that exist in the HORCM_INSTP or HORCM_CTQM definitions will also be deleted.

If a parameter not supported by Device Manager is used, the configuration definition file is assumed to be invalid and the system does not execute normal processing. Even though a parameter is supported, Device Manager might not support certain description formats. Note that the configuration definition file is assumed to be invalid if an item is specified using an unsupported format. The following tables show the support status of description formats:

Note: For details about description rules related to the entire configuration definition file and the specification contents for each parameter, see Overview of Description Rules for a Configuration Definition File. Furthermore, for detailed rules related to the contents that can be specified for each parameter, see Detailed Description Rules for Configuration Definition File.

Table 3-8 Support Status of HORCM_MON Parameter Description Format

Version	Item			
	ip_address	service	poll	timeout
6.1 or later	Yes	Yes	Yes	Yes
5.9 to 6.0	Yes	Only supports port number specification.	Yes	Yes
5.8	Supports IP address, host name, and NONE.	Only supports port number specification.	Yes	Yes
Earlier than 5.7	Supports IP address and host name.	Only supports port number specification.	Yes	Yes

Legend:

Yes: Supports all description formats.

Table 3-9 Support Status of HORCM_CMD Parameter Description Format

Version		Item
		dev_name
05-10 or later	Windows	Yes
	UNIX	Only supports specification using a special file.
05-00	Windows	Supports description formats other than CMD format.
	UNIX	Only supports specification using a special file.
Earlier than 04-30	Windows	Supports description formats other than CMD and GUID formats.
	UNIX	Only supports specification using a special file.

Legend:

Yes: Supports all description formats.

Table 3-10 Support Status of HORCM_DEV Parameter Description Format

Version	Item					
	dev_group	dev_name	port#	targetID	LU#	MU#
04-00 or later	Yes	Yes	Yes	Yes	Yes	Yes
Earlier than 03-50	Yes	Yes	Yes	Yes	Yes	Supports specification using mirror descriptors, omissions (blank), and numeric values.

Legend:

Yes: Supports all description formats.

Table 3-11 Support Status of HORCM_LDEV Parameter Description Format

Version	Item				
	dev_group	dev_name	Serial#	CU:LDEV(LDEV#)	MU#
6.2 or later	Yes	Yes	Yes	Yes	Yes
6.1 to 05-60	Yes	Yes	Yes	Supports description formats other than the *serial-number*:*journal-ID* format.	Yes
Earlier than 05-50	No	No	No	No	No
Legend: Yes: Supports all description formats. No: Does not support any description formats.					

Table 3-12 Support Status of HORCM_INST Parameter Description Format

Version	Item		
	dev_group	ip_address	service
6.1 or later	Yes	Yes	Yes
Earlier than 6.0	Yes	Yes	Only supports port number specification.
Legend: Yes: Supports all description formats.			

Overview of Description Rules for a Configuration Definition File

A configuration definition file cannot include a line that consists only of space characters. In addition, if the version of Device Manager agent is 5.5 or earlier, a line that starts with `H` and includes any of the following character strings cannot be included (except in the starting line of the parameter):

`HORCM_MON`, `HORCM_CMD`, `HORCM_DEV`, `HORCM_INST`, `HORCM_INSTP`, `HORCM_CTQM`

The following tables show the contents and specified items in a configuration definition file for each parameter. For details about description rules for the content that can be specified, see Detailed Description Rules for Configuration Definition File.

Table 3-13 HORCM_MON Parameter Items and Descriptions

Item	Description
ip_address	Specify the IP address (the Device Manager agent whose version is 5.9 or later supports the IPv6 protocol), host name, NONE, or NONE6. Note that NONE cannot be specified if the version of the Device Manager agent is 5.7 or earlier. Also, NONE6 cannot be specified if the version of the Device Manager agent is 5.8 or earlier. Note that if you use Replication Manager to generate a configuration definition file, this item will always be specified for the host name (Replication Manager uses a Device Manager agent to view the configuration definition file).
service	Specify the port name or port number. Note that the port name cannot be specified if the version of the Device Manager agent is 5.9 or earlier.
poll(10ms)	Specify a value (in ten millisecond units) or -1.
timeout(10ms)	Specify the timeout period in ten millisecond units.

Table 3-14 HORCM_CMD Parameter Items and Descriptions

Item	Description
dev_name	In Windows: Specify the command device using the PhysicalDrive format, GUID format, or CMD format. Note that the GUID format cannot be used if the version of the Device Manager agent is 04-30 or earlier. Also, the CMD format cannot be used if the version of the Device Manager agent is 05-00 or earlier. In UNIX: Specify the command device using a special file. You cannot specify a serial number, LDEV number, or port number. You can specify more than one command device in the same system, and you can specify a command device in more than one system.

Table 3-15 HORCM_DEV Parameter Items and Descriptions

Item	Description
dev_group	Specify the group name.
dev_name	Specify the name of the pair volume.
port#	Specify the port name.
targetID	Specify the target ID of SCSI/Fibre.
LU#	Specify the LU number of SCSI/Fibre.
MU#	Specify the mirror descriptor using a numeric value or the h addition. You can omit this by leaving it blank. Note that the h addition cannot be used if the version of the Device Manager agent is 03-50 or earlier.

Table 3-16 HORCM_LDEV Parameter Items and Descriptions

Item	Description
dev_group	Specify the group name.
dev_name	Specify the name of the pair volume.
Serial#	Specify the system number of the storage subsystem using the decimal number or *serial-number*:*journal-ID* format. Note that the *serial-number*:*journal-ID* format cannot be used if the version of the Device Manager agent is 6.1 or earlier.
CU:LDEV(LDEV#)	Specify the LDEV number using the decimal number, hexadecimal number, or *CU*:*LDEV* format.
MU#	Specify the mirror descriptor using a numeric value or h addition. You can omit this by leaving it blank. Note that the h addition cannot be used if the version of the Device Manager agent is 03-50 or earlier.
Note: This parameter cannot be specified if the version of the Device Manager agent is 05-50 or earlier.	

Table 3-17 HORCM_INST Parameter Items and Descriptions

Item	Description
dev_group	Specify the contents specified for dev_group of the HORCM_DEV parameter or HORCM_LDEV parameter.
ip_address	Specify the IP address (the Device Manager agent whose version is 5.9 or later supports the IPv6 protocol) or host name. If you use Replication Manager to add a new group to the existing configuration definition file, this item will always be specified using the host name.
service	Specify the port name or port number. Note that the port name cannot be specified if the version of the Device Manager agent is 6.0 or earlier.

Detailed Description Rules for Configuration Definition File

This subsection explains the description rules for configuration definition files for each parameter.

Description Rules for the HORCM_MON Parameter

The following explains the description rules related to ip_address and service.

- For ip_address, specify the information for the host managed by the Device Manager server.
- The host name specified for ip_address is case sensitive.
- Match the IP address version (IPv6 or IPv4) specified for ip_address to the one specified for HORCM_INST.
- If an IPv6 environment is being used, specify an IP address for ip_address. If you specify a host name, an IPv4 environment is used.

- If the OS is Windows Server 2003 or Windows Server 2003 R2, you cannot specify an IPv6 address. When an IPv6 environment is used with Windows Server 2003 or Windows Server 2003 R2, you must specify `NONE6`.
- The following values are not allowed for `ip_address` because the Device Manager server cannot resolve a host with those values.

  When the version of the Device Manager agent is 5.9 or later:
  - Cluster virtual IP address
  - Cluster virtual machine name
  - `__NONE__`
  - `__NONE6__`

  When the version of the Device Manager agent is 5.8
  - Cluster virtual IP address
  - Cluster virtual machine name
  - `NONE6`
  - `__NONE__`

  When the version of the Device Manager agent is 5.7 or earlier:
  - Loopback IP address (from 127.0.0.1 to 127.255.255.254)
  - Loopback host name (`localhost`)
  - Cluster virtual IP address
  - Cluster virtual machine name
  - `NONE`
  - `NONE6`
- For `service`, specify the port name using 1 to 15 single-byte characters. The environment must support the conversion of port names to port numbers.
- For `service`, specify the port number as a numeric value from 0 to 65535.

Description Rules for the HORCM_CMD Parameter

The following explains the description rules related to `dev_name`. For `dev_name`, you must specify a command device that is recognized by the host. The description rules differ depending on the specification format:

PhysicalDrive format

`\\.\PhysicalDrive`*disc-number-defined-by-Windows*

For the Device Manager agent 4.3 or earlier, this item is case sensitive.

GUID format

`\\.\Volume{`*GUID*`}`

The version of the Device Manager agent must be 5.0 or later.

CMD format

\\.\CMD-*serial-number*[-*logical-device-number*[-*port-name*[-*host-group-number*]]]

The version of the Device Manager agent must be 5.1 or later. You must use base-10 numbers to specify the serial number and logical device number. For the host group number, if the version of the Device Manager agent is 5.6 or later, specify a value from 0 to 254. If the version of the Device Manager agent is 5.5 or earlier, specify a value from 0 to 127.

Description Rules for the HORCM_DEV Parameter

The following explains the description rules related to dev_group, dev_name, port#, and MU#.

- Specify dev_group and dev_name using no more than 31 single-byte characters. A hyphen (-) cannot be specified at the beginning of the character string.
- The same dev_name value must not be duplicated in a configuration definition file.
- The combination of the dev_group and dev_name values must not be duplicated in the configuration definition file for a host.
- If you specify the host group number immediately after specifying the port name for port#, the range of values that you can specify differs depending on the version of the Device Manager agent. When the version of the Device Manager agent is 5.6 or later, specify a value from 0 to 254. When the version of the Device Manager agent is 5.5 or earlier, specify a value from 0 to 127.
- The value that can be specified for MU# differs depending on the Device Manager agent version being used and the copy type.

  When the version of the Device Manager agent is 6.3 or later:

  ShadowImage: 0 to 2

  Copy-on-Write Snapshot: 0 to 63

  TrueCopy: Not specified

  Universal Replicator: Not specified#, 0#, h1, h2, or h3

  #:

  When specified, multi-target configuration pairs cannot be created with TrueCopy.

  When the version of the Device Manager agent is from 04-20 to 6.2:

  ShadowImage: 0 to 2

  Copy-on-Write Snapshot: 0 to 63

  TrueCopy: Not specified

  Universal Replicator: h1, h2, or h3

  When the version of the Device Manager agent is 4.0 or 4.1

  ShadowImage: 0 to 2

Copy-on-Write Snapshot: 0 to 13

TrueCopy: Not specified

Universal Replicator: h1, h2, or h3

When the version of the Device Manager agent is 3.5 or earlier

ShadowImage: 0 to 2

Copy-on-Write Snapshot: 0 to 13

TrueCopy: Not specified

Description Rules for the HORCM_LDEV Parameter

The following explains the description rules related to dev_group, dev_name, LDEV#, and MU#.

- Specify dev_group and dev_name using no more than 31 single-byte characters. A hyphen (-) cannot be specified at the beginning of the character string.
- The same dev_name value must not be duplicated in a configuration definition file.
- The combination of the dev_group and dev_name values must not be duplicated in the configuration definition file for a host.
- The following are examples of LDEV#:

  Base-10 numbers

  260

  Hexadecimal numbers

  0x104

  CU:LDEV format

  01:04

- The value that can be specified for MU# differs depending on the version and copy type of the Device Manager agent, as shown below.

  When the version of the Device Manager agent is 6.3 or later:

  ShadowImage: 0 to 2

  Copy-on-Write Snapshot: 0 to 63

  TrueCopy: Not specified

  Universal Replicator: Not specified#, 0#, h1, h2, or h3

  #:

  When specified, multi-target configuration pairs cannot be created with TrueCopy.

  When the version of the Device Manager agent is 6.2 or earlier:

  ShadowImage: 0 to 2

Copy-on-Write Snapshot: `0` to `63`

TrueCopy: Not specified

Universal Replicator: `h1`, `h2`, or `h3`

Description Rules for the HORCM_INST Parameter

The following explains the description rules related to `dev_group`, `ip_address`, and `service`.

- Specify `dev_group` using no more than 31 single-byte characters. A hyphen (`-`) cannot be specified at the beginning of the character string.
- You cannot specify `ip_address` more than once for the same host for a single `dev_group`.
- For `ip_address`, specify the information for the host managed by the Device Manager server.
- The host name specified for `ip_address` is case sensitive.
- Match the IP address version (IPv6 or IPv4) specified for `ip_address` to the one specified for `HORCM_MON`.
- When an IPv6 environment is being used, you cannot specify a host name. If you specify a host name, an IPv4 environment is used.
- The following values are not allowed for `ip_address` because the Device Manager server cannot resolve a host with those values.

  When the version of the Device Manager agent is 5.8 or later:
  - Cluster virtual IP address
  - Cluster virtual machine name

  When the version of the Device Manager agent is 5.7 or earlier:
  - Loopback IP address (from 127.0.0.1 to 127.255.255.254)
  - Loopback host name (`localhost`)
  - Cluster virtual IP address
  - Cluster virtual machine name
- For `service`, specify the port name using 1 to 15 single-byte characters. The environment must support the conversion of port names to port numbers.
- For `service`, specify the port number as a numeric value from 0 to 65535.

Notes About Creating a Configuration Definition File

The following are important notes that are applicable when CCI is used with Device Manager.

Instance Number and Service Number of a Configuration Definition File

The instance number of the configuration definition file must be from 0 to 4094 (if Device Manager is used to obtain and operate copy pair information). A value from 900 to 998 might be used to temporarily obtain and operate copy pair information. Therefore, we recommend that you use a value other than these numbers.

In addition, when CCI is used with Device Manager, we recommend that you do not use service numbers `53232` to `53330`. If these service numbers are used, CCI error information might be output to the system log or event log.

Notes on Optimization Processing of the Configuration Definition File

If `true` is specified for the `server.agent.rm.optimization.userHorcmFile` property of the `server.properties` file, when the Device Manager agent service starts, or when you operate copy pairs, the Device Manager agent optimizes the contents of the CCI configuration definition file. In this case, note the following:

Notes on backing up the configuration definition file

In the optimization processing, the original configuration definition file `horcm`*`XX`*`.conf` is backed up as `horcm`*`XX`*`.conf.bk`. If the optimization is performed more than once, the original user-created configuration definition file will be lost because only one generation of backup file is made. Therefore, back up as necessary.

Notes on a comment added to the command device definition

When the CCI configuration definition file is optimized, the unit ID, logical device number, and serial number for the command device are added as comments on the line before the line on which the command device is defined. In this case, note the following:

- Do not change the contents of the comment because the Device Manager agent references it.
- When you copy the CCI configuration definition file that the Device Manager agent is already managing, and then create a new CCI configuration definition file, delete this comment.

For details about `server.properties` file, see The server.properties File.

Configuration Definition File Storage Location

Save the configuration definition file in the following folder or directory.

In Windows:

System folder (represented by the environment variable `%windir%`)

In UNIX:

`/etc` directory

Operations Required When Creating or Changing a Configuration Definition File

When you use Device Manager to create or change a configuration definition file, the information that is defined in the file is automatically reported to the Device Manager server. However, if you create or change a configuration definition file without using the Device Manager, for example, by using the Replication Manager instead or by directly editing the file, you need to manually report the file information to the Device Manager server. To manually report file information to the Device Manager server, you need to refresh the storage subsystem from a management client. Refresh all storage subsystems associated with copy pair volumes that are specified in the configuration definition file.

For details about refreshing storage subsystems, see the Device Manager online Help, or the *Hitachi Device Manager Command Line Interface (CLI) User's Guide*.

Notes About Operating the Configuration Definition File

When you delete copy pairs from a management client, if all the definitions of the copy pairs in a configuration definition file are deleted, that configuration definition file will also be deleted. If you do not want the configuration definition file to be deleted, back up of the configuration definition file before you delete the copy pairs.

Using Device Manager Agent Commands

This section explains the syntax of Device Manager agent commands.

Notes:

- When using one of the following OSs on the host, execute Device Manager agent commands from the WOW64 command prompt:
  - Windows Server 2003 (x64 and IPF)
  - Windows Server 2003 R2 (x64)
  - Windows Server 2008 (x64 and IPF)
  - Windows Server 2008 R2 (x64 and IPF)

  Following is an example of executing from the command prompt:
  `C:\WINDOWS\SysWOW64\cmd.exe`
- In Windows, the folder in which the Device Manager agent commands are installed is automatically added to the environment variable PATH. When you execute a command, you do not need to change the current folder to the folder that contains commands.

  Note that after installing the Device Manager agent, you will have to log off from, and then log on to Windows for the changes in the environment variable PATH to be applied.

hbsa_modinfo Command Syntax

The `hbsa_modinfo` checks the available agent functions (add-on modules). It is stored in the following locations:

In Windows:

`installation-folder-for-Device-Manager-agent``\bin\hbsa_modinfo.bat`

In Solaris, Linux, or HP-UX:

`/opt/HDVM/HBaseAgent/bin/hbsa_modinfo`

In AIX:

`/usr/HDVM/HBaseAgent/bin/hbsa_modinfo`

The following table describes the `hbsa_modinfo` command syntax.

Table 3-18 hbsa_modinfo Command Syntax

Item	Details
Synopsis	hbsa_modinfo [*name-of-the-addon-module*]

Item	Details
Description	Uses *V*.*R1*.*R2*-*MM* (*V*: version number, *R1* and *R2*: revision numbers, *MM*: modification version number) to display all add-on module names and versions that are ready for use. You can also specify an add-on module to check whether the module is ready for use. This operation requires Administrator or superuser privileges. If the OS is Windows Server 2008 or Windows Server 2008 R2, the command must be executed from a command prompt started as an Administrator. If applicable add-on modules are not found, a message appears indicating that the system was unable to find the add-on modules. However, the `hbsa_modinfo` command completes normally. Note that if the version of Global Link Manager agent is 6.2, `HGLM Agent` is displayed for the add-on module name in the command execution results. Also note that `hdlm` is displayed for the add-on module name only if the OS is Windows and the version of Dynamic Link Manager agent is 6.0 or later.
Options	*name-of-the-addon-module* Specifies the following abbreviations for add-on modules whose availability you wish to check: `hdlm`: Dynamic Link Manager agent `hdvm`: Device Manager agent `hglm`: Global Link Manager agent `hptm`: Protection Manager agent `hpvm`: Provisioning Manager agent `hrpm`: Replication Manager agent `hrpmap`: Replication Manager Application agent

The following describes add-on modules that can be checked by the `hbsa_modinfo` command and provides a functional overview.

- Dynamic Link Manager agent

  Monitors and adjusts the access route between the host and storage subsystems. For details see the *Hitachi Dynamic Link Manager User's Guide*.

- Device Manager agent

  Collects host and storage subsystem usage. For details, see About the Device Manager Agent.

- Global Link Manager agent

  Monitors the DMP path route between the host and storage subsystems. For details, see the *Hitachi Global Link Manager Installation and Configuration Guide*.

- Protection Manager agent

  Simplifies backup operations using the high-speed copy function of the storage subsystem. For details, see the *Hitachi Protection Manager Console User's Guide*.

- Provisioning Manager agent

  Creates or deletes the file system or a device file. For details, see the Provisioning Manager online Help.

- Replication Manager agent

Monitors the status of storage subsystem replication. For details, see the *Hitachi Replication Manager Installation and Configuration Guide*.

- Replication Manager Application agent

  Centrally manages backup operations on a unit basis using the high-speed copy function of the storage subsystem. For details, see the *Hitachi Replication Manager Installation and Configuration Guide*.

hbsa_util Command Syntax

The `hbsa_util` command deletes the files and registry entries of the Device Manager agent when the host OS is Windows. The command is stored in the following location:

`installation-folder-for-Device-Manager-agent``\bin\hbsa_util.exe`

Notes: The `hbsa_util.exe` file is stored in the following folder of the Device Manager agent CD-ROM.

`CD-ROM-drive``\Agent\Windows\`

The following table describes the `hbsa_util` command syntax.

Table 3-19 hbsa_util Command Syntax

Item	Details
Synopsis	`hbsa_util [-cleanup]`
Description	Deletes the files and registry entries of the Device Manager agent in a Windows environment. This operation requires Administrator privileges. If the OS is Windows Server 2008 or Windows Server 2008 R2, the command must be executed from a command prompt started as an Administrator.
Options	`-cleanup` Delete the files and registry entries of the Device Manager agent.

hbsasrv Command Syntax

The `hbsasrv` command starts and stops the Device Manager agent service and displays the status of the service. It is stored in the following locations:

- In Windows:
  `installation-folder-for-Device-Manager-agent``\bin\hbsasrv.exe`
- In Solaris, Linux, or HP-UX:
  `/opt/HDVM/HBaseAgent/bin/hbsasrv`
- In AIX:
  `/usr/HDVM/HBaseAgent/bin/hbsasrv`

The following table describes the `hbsasrv` command syntax.

Table 3-20 hbsasrv Command Syntax

Item	Details
Synopsis	`hbsasrv [start|stop [-f]|status]`
Description	Starts or stops the service or daemon process of the Device Manager agent. Also, this command displays the status of the service or daemon process. This operation requires Administrator or superuser privileges. If the OS is Windows Server 2008 or Windows Server 2008 R2, the command must be executed from a command prompt started as an Administrator.

Options	`start`
	Starts the service or daemon process.
	`stop [-f]`
	Stops the service or daemon process.
	If any add-on module or version 5.8 or later of Dynamic Link Manager is still running, you might not be able to stop the Device Manager agent service. In such a case, the error message KAIE62604-E is output. Wait until the add-on module or Dynamic Link Manager completes its operation, and then execute the command again.
	If you urgently need to stop the Device Manager agent, you can force the Device Manager agent service to shut down by executing the hbsasrv command with the stop `-f` option. In such a case, all processing is forced to terminate, thus ongoing processing of jobs is not guaranteed.
	`status`:
	Displays the service or daemon process operating status.
	If the command execution result displays Status as Running, the Device Manager agent service or daemon process is running. If the result displays Status as Stop, the service or daemon process has stopped.
	Caution: The version displayed when you execute the hbsasrv command is not the Device Manager agent version. You must use hdvm_info commands to check the Device Manager agent version.

hdvm_info Command Syntax

The `hdvm_info` command displays the version of the Device Manager agent. It is stored in the following locations:

- In Windows:
  `installation-folder-for-Device-Manager-agent``\bin\hdvm_info.exe`
- In Solaris, Linux, or HP-UX:
  `/opt/HDVM/HBaseAgent/bin/hdvm_info`
- In AIX:
  `/usr/HDVM/HBaseAgent/bin/hdvm_info`

The following table describes the `hdvm_info` command syntax.

Table 3-21 hdvm_info Command Syntax

Item	Details
Synopsis	`hdvm_info`

Item	Details
Description	The hdvm_info command displays the version of the Device Manager agent in *V.R1.R2-MM* format, where *V* is the version number, *R1.R2* is the revision number, *MM* is the modified version.
Options	None

hdvmagt_account Command Syntax

The hdvmagt_account command provides an interactive interface for setting Device Manager server information used to communicate with Device Manager agents. It is stored in the following locations:

- In Windows:

  installation-folder-for-Device-Manager-agent\bin\hdvmagt_account.bat

- In Solaris, Linux, or HP-UX:

  /opt/HDVM/HBaseAgent/bin/hdvmagt_account

- In AIX:

  /usr/HDVM/HBaseAgent/bin/hdvmagt_account

Caution:

For Windows, after you change the Device Manager server information, restart the Device Manager agent service. For details, see Managing the Operating Status of the Device Manager Agent Service.

For UNIX, if you execute the hdvmagt_account command, the Device Manager agent service is restarted, regardless of whether the server information has changed.

The following table describes the hdvmagt_account command syntax.

Table 3-22 hdvmagt_account Command Syntax

Item	Details
Synopsis	hdvmagt_account

Item	Details
Description	This command allows you to set Device Manager server information for communication with Device Manager agents. If Device Manager server information is already set, the settings are displayed when the hdvmagt_account command is executed. This operation requires Administrator or superuser privileges. If the OS is Windows Server 2008 or Windows Server 2008 R2, the command must be executed from a command prompt started as an Administrator. Enter the following information when requested. Note that when prompted for each item, operations will end abnormally if you enter three invalid values consecutively. *IP-address* or *host-name* Enter the IP address or host name of the Device Manager server. When specifying an IP address: For IPv4, specify the IP address in the dotted-decimal format. For IPv6, specify the IP address by using hexadecimal numbers with colons. Abbreviation can be used. When specifying a host name: Use a character string of 50 bytes or less to specify a host name. The following characters can be used: a-z A-Z 0-9 - . @ _ If the entered value is not in the specified format, or the host name cannot be resolved to an IP address, you will be prompted to re-enter it. The specified value is set in the server.server.serverIPAddress property of the server.properties file (see Table 3-39). *Port-number* Enter the port number of the Device Manager server to which the Device Manager agent connects. Specify a number from 0 to 65535. The specified value is set in the server.server.serverPort property of the server.properties file (see Table 3-39). *User-id* and *password* Enter the user ID and password for the Device Manager agent registered with the Device Manager server. For a built-in account for use with the Device Manager agent, the user ID is HaUser and the default password is haset. To change the account used in the Device Manager agent, a user ID with Peer privileges must already be created by using the Web Client. For details on how to create a user ID, see the Device Manager online Help. The specified values of the user ID and password are encrypted and then set in server.server.authorization in the server.properties file (see Table 3-39).
Options	None

hdvmagt_schedule Command Syntax

The hdvmagt_schedule command provides an interactive interface for setting the automatic execution period of the HiScan command. It is stored in the following locations:

- In Windows:

  installation-folder-for-Device-Manager-agent\bin\hdvmagt_Schedule.bat

- In Solaris, Linux, or HP-UX:
  `/opt/HDVM/HBaseAgent/bin/hdvmagt_schedule`
- In AIX:
  `/usr/HDVM/HBaseAgent/bin/hdvmagt_schedule`

Caution: For Windows, after you execute this command, restart the Device Manager agent service. For details, see Managing the Operating Status of the Device Manager Agent Service.

The following table describes the `hdvmagt_schedule` command syntax.

Table 3-23 hdvmagt_schedule Command Syntax

Item	Details
Synopsis	hdvmagt_schedule
Description	This command allows you to set the automatic execution period for the HiScan command. If an execution period is already registered, the registered interval is displayed when the hdvmagt_schedule command is executed. This operation requires Administrator or superuser privileges. If the OS is Windows Server 2008 or Windows Server 2008 R2, the command must be executed from a command prompt started as an Administrator. You can select one of the following four automatic execution periods for the HiScan command: ▪ Hourly ▪ Daily ▪ Weekly ▪ No automatic execution (or cancel the set schedule)# #: This can be selected only if an automatic execution period has already been set. Note that any execution time can be specified. If you do not specify the execution time, for the hourly execution period, the HiScan command is executed at the 30th minute of every hour. For the daily or weekly period, the command is executed at 2:30 AM. In Windows, specifying an execution period registers exeHiScan.bat as a Windows task.
Options	None

hdvmagt_setting Command Syntax

The `hdvmagt_setting` command provides an interactive interface for specifying the following information in one operation:

- Information for the Device Manager server
- Execution period for the `HiScan` command
- Information for using CCI

The `hdvmagt_setting` command is stored in the following locations:

- In Windows:
  installation-folder-for-Device-Manager-agent\bin\hdvmagt_setting.exe
- In Solaris, Linux, or HP-UX:
  /opt/HDVM/HBaseAgent/bin/hdvmagt_setting
- In AIX:
  /usr/HDVM/HBaseAgent/bin/hdvmagt_setting

The following table describes the hdvmagt_setting command syntax.

Table 3-24 hdvmagt_setting Command Syntax

Item	Details
Synopsis	hdvmagt_setting
Description	The hdvmagt_setting command sets the following items in order: 1. Information for the Device Manager server Specify the same settings as for the hdvmagt_account command. For details about these settings, see hdvmagt_account Command Syntax. 2. Execution period for the HiScan command Specify the same settings as for the hdvmagt_schedule command. For details about these settings, see hdvmagt_schedule Command Syntax. In Windows, specifying an execution period registers exeHiScan.bat as a Windows task. 3. Information for using CCI Specify the following items: Installation location - Specify the drive or directory where CCI is installed. Do not specify a floppy disk drive or CD-ROM drive. Central management method - Specify whether to perform central management of copy pairs on the target hosts. This operation requires Administrator or superuser privileges. If the OS is Windows Server 2008 or Windows Server 2008 R2, the command must be executed from a command prompt started as an Administrator.
Options	None

HiScan Command Syntax

The HiScan command is used to send host information to the Device Manager server. The HiScan command is stored in the following locations:

- In Windows:
  installation-folder-for-Device-Manager-agent\bin\HiScan.bat
- In Solaris, Linux, or HP-UX:
  /opt/HDVM/HBaseAgent/bin/HiScan
- In AIX:
  /usr/HDVM/HBaseAgent/bin/HiScan

The following table describes the HiScan command syntax.

Table 3-25 HiScan Command Syntax

Item	Details
Synopsis	HiScan {-s *server-destination* [-u *user-id* -p *password*] [{-c *sec*|-t *output-file-name*}]|-t *output-file-name*}
Description	This command allows you to send host information such as the host name, HBA WWN, file system, mount point, and information on the LU connected to the host to the Device Manager server. This operation requires Administrator or superuser privileges. If the OS is Windows Server 2008 or Windows Server 2008 R2, the command must be executed from a command prompt started as an Administrator.
Options	-s *server-destination* Specify the Device Manager server destination. *server-destination* can be specified in the following format: *IP-address*[:*port-number*] *host-name*[:*port-number*] localhost[:*port-number*] If the port number is omitted, the port number set in the server.server.serverPort property of the server.properties file is used (For example; 192.168.1.102: 2001). In addition, when you specify an IPv6 format IP address and port number at the same time, enclose the IPv6 address in square brackets ([]) (for example, [2001::1234:5678]:2001). Use a character string that is 50 bytes or fewer to specify the host name. The following characters can be used: a-z A-Z 0-9 - . @ _ This parameter is optional. If -s is omitted, the -t option must be specified. -u *user-id* Specify the user ID of an account with Peer permissions that is registered in the transmission destination Device Manager server. If the -s option is specified, but the -u and -p options are omitted, HiScan uses the user ID that is stored in server.server.authorization of the server.properties file (see Table 3-39). -p *password* Specify the password of an account with Peer permissions that is registered in the transmission destination Device Manager server. The -p option is required if the -u option is specified. If the -s option is specified but the -u and -p options are omitted, HiScan uses the password that is stored in server.server.authorization of the server.properties file (see Table 3-39). -c *sec* Specifies the interval (in seconds) at which host information is sent to the Device Manager server. Host information is continuously sent to the Device Manager server at the specified interval, until a forced termination occurs. Values of less than ten seconds are recognized as invalid. Specify a value in the range from 10 to 2147483647. If -t is specified, -c cannot be used. -t *output-file-name* Specify a file name if you want to output host information sent to the Device Manager server to an XML file. The file is output to the current directory. ***Caution:*** The -t option can be specified in addition to the -s option. If both options are specified, the information sent from the Device Manager agent and the messages received from the Device Manager server are output to the file. If -t is specified, -c cannot be used.

hldutil Command Syntax

The `hldutil` command is used to obtain information on storage subsystem LDEVs, file systems, and other devices. It also allows you to output the obtained information to an execution log file and to view past execution log files. The `hldutil` command is stored in the following locations:

- In Windows:
  installation-folder-for-Device-Manager-agent`\util\bin\hldutil.exe`
- In Solaris, Linux, or HP-UX:
  `/opt/HDVM/HBaseAgent/util/bin/hldutil`
- In AIX:
  `/usr/HDVM/HBaseAgent/util/bin/hldutil`

The following table describes the `hldutil` command syntax.

Table 3-26 hldutil Command Syntax

Item	Details
Synopsis	`hldutil [-d [`*device-number-or-device-file-name*`]|-g [`*disk-group-name*`]|-l` *ldev-number*`.`*serial-number*`] [-p] [-q] [-nolog] [-s` *sort-key*`...] [-serdec] [-k|-hf [`*log-file-name*`]|-h [`*log-number*`]]` `hldutil -h [`*log-number*`] -hb [`*log-file-name*`]|-hrm [`*log-number*`|all]|-history` *number-of-log-file-generations*
Description	The `hldutil` command is used to obtain information on storage subsystem LDEVs, file systems, and other devices. It also allows you to output the obtained information to an execution log file and to view past execution log files. If all options are omitted, information is output about all LDEVs recognized by the host. This operation requires Administrator or superuser privileges. If the OS is Windows Server 2008 or Windows Server 2008 R2, the command must be executed from a command prompt started as an Administrator. ***Caution:*** If you execute the `hldutil` command immediately after the host environment is changed (for example, after an LU is added or deleted), the command might not be able to recognize the changed contents of the host. In this case, wait a while, and then re-execute the `hldutil` command.

Item	Details
Options	-d [*device-number-or-device-file-name*] To view information about a specific LDEV, specify the disk number (in Windows) or device special file name (in UNIX) of the LDEV. If you omit this option, the command displays information about all currently recognized LDEVs. You cannot specify the -d option and the -g or -l option at the same time. -g [*disk-group-name*] If you want to view information about a specific disk group, specify the name of the disk group. If you omit the disk group name, the command outputs information about all currently defined disk groups. You cannot specify the -g option and the -d or -l option at the same time. -l *ldev-number*.*serial-number* If you want to view information about a specific LDEV, specify the LDEV number (*LDEV#*) and serial number (*serial#*) of the LDEV. The LDEV number and serial number must be specified in the indicated order. If you omit the LDEV number or serial number, the command does not output information about the LDEV. You cannot specify the -l option and the -d or -g option at the same time. If you specify the -l option, only the following items are output: Ldev# (LDEV number) Ser# (storage subsystem serial number) Device (device special file name or disk number) Dg name (disk group name) fs (file system) -p Specify this option to add the P-VOL and S-VOL information (that you set up by using ShadowImage, TrueCopy, Copy-on-Write Snapshot, QuickShadow or Universal Replicator) to the disk information to be output. When this option specified, if no P-VOL or S-VOL information is assigned to an LDEV, nothing is output. -q Specify this option to output the command execution results only to the execution log file without sending them to the standard output (quiet mode). Typically, you specify this option when you want to run a background job to output the latest LDEV information to the execution-result log file. However, error messages are sent to the standard error output. -nolog Specify this option to send the command execution results only to the standard output without updating the execution log file. -s *sort-key* Specify this option to sort LDEV information in ascending order of ASCII codes. This option must include one or more sort keys. When specifying multiple sort keys, place a one-byte space between sort keys. If you specify multiple sort keys, the command sorts information using the sort keys in the order in which they are specified. If you specify the file system name as the sort key, the command sorts LDEV information using the file system name that is included in each logical device and assigned the lowest ASCII code. If you do not specify a sort key or if you specify the same sort key more than once, an error message is output. If you do not specify the -s option, the command outputs LDEV information in the order in which it has processed the information. Table 3-27 lists and describes the sort key. -serdec Specify this option to display the serial number of the storage subsystem in decimal format. -k Specify this option to send the contents of the latest execution log file to the standard output. This processing involves no hardware access. Note that if no disk information is recorded in an execution log file, the disk information is obtained and then output to the standard output and an execution log file. You cannot specify the -k option and the -h or -hf option at the same time.

Item	Details
Options	-hf [*log-file-name*] Specify this option to output the contents of a specific execution log file to the standard output. This processing involves no hardware access. If you omit the file name, the command waits for the entry of a file name. If the specified execution-result log file cannot be found, the command outputs an error message and then ends. You cannot specify the -hf option and the -k or -h option at the same time. -h [*log-number*] Specify this option to output the contents of the execution log file identified by a specific log number to the standard output. This processing involves no hardware access. Also specify this option when you want to create a copy of an execution log file. Use the -h option to specify the log number of the copy source execution log file, and the -hb option to specify the copy destination. If you omit the log number, the command displays a list of the existing execution-result log files and waits for the entry of a log number. If an execution-result log file with the specified log number cannot be found, the command outputs an error message and then ends. You cannot specify the -h option and the -k or -hf option at the same time. -hb [*log-file-name*] Specify this option to create a copy of an execution log file. Use the -h option to specify the log number of the copy source execution log file, and the -hb option to specify the copy destination. Use the absolute path or relative path to specify the copy destination file name. If you omit the log file, the command waits for the specification of a file name. If the specified file already exists, the command displays a prompt asking you whether you want to overwrite the file and waits for your reply. You must specify this option together with the -h option. You cannot specify the -hb option together with any option other than -h. -hrm [*log-number*|all] Specify this option to delete an execution-result log file. Specify the log number that identifies the execution-result log file to be deleted. If you specify all instead of a log number, the command deletes all execution-result log files from the default log storage directory. If you specify nothing, the command displays a list of execution-result log files and waits for the specification of a log number. If the specified log number does not identify any execution-result log file, the command displays an error message and then ends. You cannot specify the -hrm option together with any other option. -history *number-of-log-file-generations* Specify this option to change the number of generations of execution log files to be kept. The execution-result log files are created when the device information display function is used. Specify a number from 1 to 64. The default value is 32. The specified value takes effect when the next execution log file is created. You cannot specify the -history option together with any other option.

Table 3-27 hldutil Sort Keys That Can be Specified for the hldutil Command

Sort Key	Descriptions
dg	Disk group name
fs	File system name
iscsin	iSCSI name for the iSCSI initiator
ldev	LDEV number
lun	LU number
port	Port number
prod	Product name
rg	RAID Group number

Sort Key	Descriptions
rid	Character string representing a storage subsystem model
ser	Serial number of a storage subsystem
tid	Target ID
vend	Vendor name
wwnn	Node WWN name
wwnp	Port WWN name

The following table lists and describes the information output when you execute the `hldutil` command. The information items are output in the order shown in the table. The items displayed differ depending on the OS and the specified options.

Table 3-28 Information Displayed When the hldutil Command is Executed

Item	Description
Dg name	Disk group name
Device	Disk number (for Windows)
	Device special file name (for UNIX)
fs	File system name
P/S	Identification of the P-VOL or S-VOL
Vend.	Vendor name
Prod.	Product name
Port#	Port number (on the DKC)
Tid#[#]	Target ID (SCSI interface on the host)
Lun#[#]	LU number (SCSI interface on the host)
Ldev#	LDEV number (on the DKC)
Ser#	Serial number of the storage subsystem
RaidID	Character string indicating the model of the storage subsystem
RG#	RAID Group number
PortWWN	Port WWN
NodeWWN	Node WWN
iSCSIName	iSCSI name for the iSCSI initiator
#: In the case of HP-UX 11i v3, this item is not displayed for a persistent special device (persistent device special file).	

The following table lists the correspondence between the string output for `RaidID` and the storage subsystem model.

Table 3-29 Correspondence between RaidID and Storage Subsystem Models

RaidID	Model
71	Hitachi WMS 100
73	Hitachi AMS 200
75	Hitachi AMS 500
77	Hitachi AMS 1000
81	Hitachi SMS 100
83	Hitachi AMS 2100
85	Hitachi AMS 2300
87	Hitachi AMS 2500
D500	Thunder 9200
D50L	Thunder 9200
D600	Thunder 9570V, Thunder 9520V
D60H	Thunder 9580V
D60J	Thunder 9530V
R400	Lightning 9960
R401	Lightning 9910V
R450	Lightning 9980V
R451	Lightning 9970V
R500	Hitachi USP 100, Hitachi USP 600 or Hitachi USP 1100
R501	Hitachi NSC 55
R600	Universal Storage Platform V
R601	Universal Storage Platform VM

TIC Command Syntax

The `TIC` command is used to collect error information on Device Manager agents. The `TIC` command is stored in the following locations:

- In Windows:
  `installation-folder-for-Device-Manager-agent``\bin\TIC.bat`
- In Solaris, Linux, or HP-UX:
  `/opt/HDVM/HBaseAgent/bin/TIC.sh`
- In AIX:
  `/usr/HDVM/HBaseAgent/bin/TIC.sh`

The following table describes the `TIC` command syntax.

Table 3-30 TIC Command Syntax

Item	Details
Synopsis	In Windows: TIC.bat [-outdir *location-of-resultDir-directory* [-f] [-d [*addon-module-name, addon-module-name*]]] In Solaris: TIC.bat [-outdir *location-of-resultDir-directory* [-f] [-d [*addon-module-name*]]] In AIX, Linux, or HP-UX: TIC.sh [-outdir *location-of-resultDir-directory* [-f]]
Description	This command lets you obtain Device Manager agent log files and system information for error analysis. This operation requires Administrator or superuser privileges. If the OS is Windows Server 2008 or Windows Server 2008 R2, the command must be executed from a command prompt started as an Administrator.
Options	-outdir *location-of-resultDir-directory* Specify the location of the resultDir directory for storing the acquired error information. Specify a relative path from the execution directory or the absolute path. If another resultDir directory exists in the specified location, a message asking whether you want to delete that directory appears. If you do not specify this option, the resultDir directory is created in the directory that contains the TIC command. If the resultDir directory already exists, then it is deleted during command execution, and error information files are stored in a newly created resultDir directory. If the resultDir directory cannot be deleted, a directory named with an index appended to resultDir is created in the specified destination (example: resultDir_1). -f Specify this option to forcibly delete any resultDir directory already existing in the location specified by the -outdir option. The acquired error information files will be stored in a new resultDir directory. You can specify this option only when the location of the directory is specified in -outdir. -d [*addon-module-name, addon-module-name*] Specify the following abbreviations for add-on modules whose error information you wish to remove from the acquisition target: hglm: Global Link Manager agent hrpmap: Replication Manager Application agent (Windows only) If you specify multiple parameters, separate them with commas (,). If the name of the add-on module is omitted, the error information for the Global Link Manager agent and Replication Manager Application agent is not acquired.

Working with Agent Property Files

This section explains the property files used by the Device Manager agent.

Caution: If you change the contents of a Device Manager agent properties file, the Device Manager agent service needs to be restarted. For details, see Managing the Operating Status of the Device Manager Agent Service.

The agent.properties File

The `agent.properties` file is used to specify the operation settings used when a Device Manager agent is linked with a Replication Manager server. The file is stored in the following locations:

- In Windows:

  installation-folder-for-Device-Manager-agent`\mod\hrpm\config\agent.properties`

- In Solaris, Linux, or HP-UX:

  `/opt/HDVM/HBaseAgent/mod/hrpm/config/agent.properties`

- In AIX:

  `/usr/HDVM/HBaseAgent/mod/hrpm/config/agent.properties`

The following table lists the properties for specifying operation settings when a Device Manager agent is linked with a Replication Manager server.

Table 3-31 agent.properties File

Property	Setting details
`agent.rm.TimeOut`[#1]	Specify the time limit for a response from the CCI command used by the Device Manager agent (in seconds). Specify a value from 0 to 86,400. Specify `0` for no time-out. Default: `600`
`agent.rm.everytimeShutdown`[#1]	Specify whether to stop the HORCM instance for monitoring[#2] every time. Specify `true` or `false`. If `true` is specified, the instance stops every time. If `false` is specified, the instance does not stop. Default: `false`
`agent.rm.shutdownWait`	Specify the wait time when stopping the HORCM instance for monitoring[#2] (in seconds). Specify a value from 1 to 60. Default: 5

Property	Setting details
agent.rm.horcmInstance	Specify the instance number of the HORCM file for monitoring[#2]. Specify a value from 0 to 4,094. This value must be different from the instance number of other CCI configuration definition files. Do not specify a value from 990 to 998 because Device Manager agent uses these values. Default: 4094
agent.rm.horcmService	Specify the UDP port number of the HORCM file for monitoring[#2]. Specify a value from 0 to 65,535. This value must be different from the port number of other applications. Do not set a value from 53,232 to 53,330 because Device Manager agent uses these values. Default: 54323
agent.rm.horcmSource[#1]	Specify the location (directory or folder) of the existing CCI configuration definition file. Use ASCII characters to specify a file location. Use the forward slash (/) as the folder separator instead of the back slash (\), even in Windows. Default value for Windows: System folder (represented by the environment variable %windir%) Default value for UNIX: /etc
agent.logger.loglevel	Specify the output level of the log file for the Replication Manager agent functionality. Log data that has a level equal to or higher than the specified value is output. Specify one of the following values (listed in ascending order of importance): DEBUG, INFO, WARN, ERROR, FATAL Default: INFO
agent.logger.MaxBackupIndex[#3]	Specify the maximum number of log files for the Replication Manager agent functionality. Specify a value from 1 to 20. When the number of log files generated reaches this value, the log files are reused, beginning with the oldest file. Default: 5

Property	Setting details
agent.logger.MaxFileSize[#3]	Specify the maximum size of log files for the Replication Manager agent functionality. Specify a value from 512 KB to 32 MB. You can specify the value in bytes, kilobytes, or megabytes. If KB or MB is not specified for the number, bytes is assumed. Default: 5 MB
#1: Normally, the values set for these parameters do not need to be changed. To change their values, you need expert knowledge of the Device Manager agent. ***#2***: The Device Manager agent uniquely creates and manages the configuration definition files and instances for monitoring to monitor the statuses of copy pairs in Replication Manager. The *HORCM instance for monitoring* is the instance of CCI used by the Device Manager agent. The *HORCM file for monitoring* is the CCI configuration definition file of that instance. ***#3:*** The size of an output log file depends on the number of copy pairs managed by Replication Manager. You can use the following formula to determine the log file output size: *amount-of-information-output-to-log-file* (MB/week) = 0.75 **x** *number-of-copy-pairs* + 4 Set the values of agent.logger.MaxBackupIndex and agent.logger.MaxFileSize taking into account the amount of information that is output and the retention period. To check the number of copy pairs managed by the target host (pair management server), use Replication Manager's *copy-group-name* subwindow.	

The hldutil.properties File

The hldutil.properties file is used to specify the action of the hldutil command. The file is stored in the following locations:

- In Windows:
  installation-folder-for-Device-Manager-agent\util\bin\hldutil.properties
- In Solaris, Linux, or HP-UX:
  /opt/HDVM/HBaseAgent/util/bin/hldutil.properties
- In AIX:
  /usr/HDVM/HBaseAgent/util/bin/hldutil.properties

The following table lists and describes the properties used to specify the action of the hldutil command.

Table 3-32 hldutil.properties File

Property	Description
agent.util.hpux.displayDsf	Specify the format of the device file name displayed when the hldutil command is executed on a host on whose OS is HP-UX 11i v3. If you are also using Provisioning Manager, the value set in this property determines the format of device file names used for host settings. If you are using Provisioning Manager and PV-link, specify ctd. ▪ If disk is specified: When the hldutil command is executed, disk device file names are displayed. In Provisioning Manager, the setting operation applies to disk device files. ▪ If ctd is specified: When the hldutil command is executed, ctd device file names are displayed. In Provisioning Manager, the setting operation applies to ctd device files. ▪ If mix is specified: When the hldutil command is executed, both disk and ctd device file are displayed. In Provisioning Manager, the setting operation applies to both disk and ctd device files. If any value other than the above is specified, mix is assumed. This property cannot be specified in an OS other than HP-UX 11i v3. Default: mix

The logger.properties File

The logger.properties file is used to configure the logging function of the Device Manager agent. The file is stored in the following locations:

- In Windows:
  installation-folder-for-Device-Manager-agent\agent\config\logger.properties
- In Solaris, Linux, or HP-UX:
  /opt/HDVM/HBaseAgent/agent/config/logger.properties
- In AIX:
  /usr/HDVM/HBaseAgent/agent/config/logger.properties

The following table lists and describes the logging function properties of the Device Manager agent.

Table 3-33 logger.properties File

Property	Description
logger.loglevel	Specify the minimum level of log data that the Device Manager agent outputs to the files error.log and trace.log. The values can be specified (in increasing order of importance) are DEBUG, INFO, WARN, ERROR, and FATAL. For example, if the default value is specified, INFO, WARN, ERROR, and FATAL data is output to the log files, but DEBUG data is not output. Default: INFO
logger.MaxBackupIndex#	Specify the maximum number of backup files for the files access.log, error.log, service.log, and trace.log. Specify the maximum number of log files. If more log files are generated than specified, the Device Manager agent 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, access.log becomes access.log.1. If additional backup log files are created, the counter increases until the specified number of backup log files is generated (for example, access.log.1 becomes access.log.2). After the specified number of backup log files is created, each time a new backup file is created, the oldest backup file is deleted. Specify a value from 1 to 20. Default: 10
logger.MaxFileSize#	Specify the maximum number of backup files for the files access.log, error.log, service.log, and trace.log. Specify the maximum size of each log file. If a log file becomes larger than this value, the Device Manager agent creates a new file and writes log data to it. Unless KB is specified for kilobytes or MB for megabytes, the specified size is interpreted to mean bytes. Specify a value from 512 KB to 32 MB. Default: 5 MB
#: The size of an output log file depends on the number of copy pairs managed by Replication Manager. You can use the following formula to determine the log file output size: *amount-of-information-output-to-log-file* (MB/week) = 0.8 **x** *number-of-copy-pairs* + 25 Set the values of logger.MaxBackupIndex and logger.MaxFileSize taking into account the amount of information that is output and the retention period. To check the number of copy pairs managed by the target host (pair management server), use Replication Manager's *copy-group-name* subwindow.	

Notes: The files access.log, error.log, service.log, and trace.log are output to the following locations:

In Windows:

installation-folder-for-the-Device-Manager-agent\agent\logs\

In Solaris, Linux, or HP-UX:

/opt/HDVM/HBaseAgent/agent/logs/

In AIX:

/usr/HDVM/HBaseAgent/agent/logs/

The programproductinfo.properties File

The programproductinfo.properties file is used to specify program product information. This file exists only when the host OS is Windows, and it is stored in the following location:

installation-folder-for-Device-Manager-agent\agent\config\programproductinfo.properties

The following table lists and describes the program product information properties of the Device Manager agent.

Table 3-34 programproductinfo.properties File

Property	Description
veritas.volume.manager.version	Specify the version of VxVM installed in Windows. If VxVM is installed in a Windows environment, specify the VxVM version in this property, in the format *x.x*. Default: None

The server.properties File

The server.properties file is used to configure the operations of the Device Manager agent. The file is stored in the following locations:

- In Windows:
  installation-folder-for-Device-Manager-agent\agent\config\server.properties
- In Solaris, Linux, or HP-UX:
  /opt/HDVM/HBaseAgent/agent/config/server.properties
- In AIX:
  /usr/HDVM/HBaseAgent/agent/config/server.properties

The following tables describe the properties of the server.properties file.

Table 3-35 server.properties File (Setting Up Ports Used by the Daemon Process and the Web Server Function)

Property	Description
server.agent.port	Specify the port number for the Device Manager agent's daemon process (or service). Avoid specifying small port numbers because such numbers might conflict with other applications. The normal range is 1024 to 49151. If a version of Dynamic Link Manager earlier than 5.8 is installed, specify 23013. Default: 24041

Property	Description
server.http.localPort	Specify the port number for communication between the Device Manager agent's daemon process and the Web server process. Avoid specifying small port numbers because such numbers might conflict with other applications. The normal range is 1024 to 49151. Default: 24043
server.http.port	Specify the port number that the Device Manager agent's Web server uses. Avoid specifying small port numbers because such numbers might conflict with other applications. The normal range is 1024 to 49151. If a version of Dynamic Link Manager earlier than 5.8 is installed, specify 23011. Default: 24042

Table 3-36 server.properties File (Setting the Host Name, IP Address, and NIC Used by the Web Server Function)

Property	Description
server.http.host	Specify the host that executes the Device Manager agent's Web server. Default: localhost
server.http.socket.agentAddress	Specify the IP address at which the Device Manager agent transmits notifications to the Device Manager server. In order to limit the IP addresses notified to the Device Manager server from the Device Manager agent, specify the IP address to be notified. For operation in an IPv6 environment, specify a global address. If you specify a site-local address or link-local address, the IPv4 address will be used. It is necessary to match the IP address version to the one specified in server.http.socket.bindAddress. The IP address that you specified in this property can also be used when creating or editing the CCI configuration definition file. If CCI is used with the Device Manager agent, make sure that communication between CCI instances is possible using the specified IP address. Default: None# # If no IP address is specified, the IP address acquired by the Device Manager agent will be used. If there are multiple IP addresses, the first IP address acquired by the Device Manager agent via API will be used.)
server.http.socket.bindAddress	In situations in which the Device Manager agent runs on a platform on which two or more network interface cards (NICs) are installed, this property allows you to specify the NIC through which the Device Manager agent can accept requests. If you want to restrict the interface to be accepted, specify the IP address to be accepted with the Device Manager agent. For operation in an IPv6 environment, specify a global address. If you specify a site-local address or link-local address, the default value will be used. It is necessary to match the IP address version to the one specified in server.http.socket.agentAddress. Default: None. (The Device Manager agent accepts all NIC requests.)

Table 3-37 server.properties File (Setting Up Basic Operations of the Web Server Function)

Property	Description
server.agent.maxMemorySize	Specify the maximum memory heap size for the Web server function processes of the Device Manager agent (in MB). Specifiable range (MB): 32 to 4,096. Default: None # #: The heap runs in a 64 MB memory area. In Solaris 10 (x64 Edition (AMD64)), the heap runs in a memory area that is 1/4 of the physical memory area or a 1 GB memory area, whichever is smaller. ***Caution:*** If you are using both Device Manager and Replication Manager, for each product, specify the required memory size. For details on the required memory size for Device Manager, see Specifying Settings When a Host Manages 100 or More LUs. For details on the required memory size for Replication Manager, see Specifying Settings for Managing Copy Pairs in Replication Manager.
server.agent.shutDownTime	Specify the period to shutdown the Device Manager agent's Web server after it receives or sends the last HTTP/XML message (in milliseconds). If a value of zero or less is specified, the waiting period is unlimited. Do not edit this property without current knowledge of the Device Manager agent's performance. Default :600000
server.agent.JRE.location	Specify the installation destination of the software that provides the Java execution environment for the Device Manager agent. You can specify this property when the host OS is UNIX. Default for Windows or Linux: None Default for Solaris, AIX, or HP-UX Installation path for the software that provides a Java execution environment and was installed on the host when you installed the Device Manager agent ***Caution:*** If the host OS is Windows, this property is ignored even if you specify a value, and the software that provides a Java execution environment and is bundled with the Device Manager agent is used.

Table 3-38 server.properties File (Security Settings for the Web Server Function)

Property	Description
server.http.entity.maxLength	Specify the maximum size of HTTP request entities permitted by the Web server function of the Device Manager agent (in bytes). Normally, the default value of this property need not be changed. By limiting the impact of malicious requests with an entity that has an abnormally large data size, this setting can be useful in repelling attacks that are intended to impair services or cause a buffer overflow. When detecting a post request larger than the specified limit, the Device Manager agent sends a remote error response and records details of the request in the log. Default: 32768
server.http.security.clientIP	Specify an IPv4 or IPv6 address that can be used to connect to the Device Manager agent. This setting limits the IP addresses permitted for connection, thus preventing denial-of-service attacks or other attacks that intend to overflow buffers. You can use an asterisk (*) as a wildcard character when you use IPv4 addresses. To specify multiple IP addresses, separate them with commas (,). In the following example, the specification permits the address 191.0.0.2 and addresses from 192.168.0.0 to 192.168.255.255 to connect to the Device Manager agent: server.http.security.clientIP=191.0.0.2, 192.168.*.* In the following example, the specification permits the addresses 2001::203:baff:fe36:109a and 2001::203:baff:fe5b:7bac to connect to the Device Manager agent: server.http.security.clientIP=2001::203:baff:fe36:109a, 2001::203:baff:fe5b:7bac Default: None (All IP addresses can connect to the Device Manager agent.)

Table 3-39 server.properties File (Information of the Device Manager Server)

Property	Description
server.server.authorization	This property stores the ID and password of the user for Device Manager server authorization. This property is encoded, so you cannot edit it using a text editor. To edit this property, use the hdvmagt_account command (see hdvmagt_account Command Syntax). Default: None
server.server.serverIPAddress	Enter the IP address or host name of the Device Manager server. When specifying an IP address: For IPv4, specify the IP address in dotted-decimal format. For IPv6, specify the IP address using hexadecimal numbers with colons. Abbreviation can be used. The following example shows how to specify an IPv6 address: server.server.serverIPAddress=2001::214:85ff:fe02:e53b When specifying a host name: Use a character string of 50 bytes or fewer to specify the host name. The following characters can be used: a-z A-Z 0-9 - . @ _ Default: 255.255.255.255
server.server.serverPort	Specify the port number of the Device Manager server to which the Device Manager agent is going to connect. As a general rule, you can specify a value from 1024 to 49151. You must specify the same value specified for the server.http.port property of Device Manager server. Default: 2001 ***Caution:*** The value of this property equals the value of the port number of the Device Manager server (see hdvmagt_account Command Syntax).

Table 3-40 server.properties File (CCI Settings)

Property	Description
server.agent.rm.centralizePairConfiguration	disable Specify this value to manage copy pairs for each host when the system uses the local management method. To use the local management method, you need to install the Device Manager agent and CCI on each host. When the local management method is used, if you specify LUs as a copy pair that has different hosts, make sure that each LU is recognized by each host. enable When the system uses the central management method, specify this value to manage all copy pairs with a single host (pair management server). To use the central management method, you must install the Device Manager agent and CCI only in the pair management server, and the Device Manager agent only in other hosts. When the central management method is used, if the pair management server recognizes the command device in each storage subsystem, the server can use all LUs, including LUs that are not recognized by the hosts of each storage subsystem, to create copy pairs. For details about the local management method and central management method, see the *Hitachi Device Manager Server Configuration and Operation Guide*. Default: disable
server.agent.rm.cuLdevForm	Specify the output format for LDEV numbers when pair volume information is written in HORCM_LDEV format in the configuration definition file when creating pairs. DECIMAL Specify to output in decimal format. CULDEV Specify to output in *CU:LDEV* format. HEXA Specify to output in hexadecimal format. This property is enabled only when creating copy pairs for Universal Storage Platform V/VM, Hitachi USP, Lightning 9900V, or Lightning 9900. Default value: None (output in decimal format)
server.agent.rm.exclusion.instance	On the host where the Device Manager agent is installed, to exclude volume pairs already managed by CCI from Device Manager operations, specify the applicable CCI instance numbers. The volume pairs excluded from Device Manager operations are also excluded from Replication Manager operations. To specify multiple instance numbers, separate the individual numbers with commas (,). From the Device Manager agent, you cannot operate a CCI whose instance number is specified in this property. Default: None

Property	Description
server.agent.rm.location	Specify the CCI installation directory in the following cases: ▪ CCI is installed in a location other than the default location ▪ The host OS is Windows, and the CCI installation drive is different from the Device Manager agent installation drive For Windows, you cannot specify \ as a delimiter. Use \\ or / instead. Default for Windows: *drive-where-Device-Manager-agent-is-installed*/HORCM Default for UNIX: /HORCM
server.agent.rm.optimization.userHorcmFile	Specify whether to optimize the user-created CCI configuration definition files. To optimize the file, specify true. If you do this, the file is updated so that Device Manager can use it. Also, when the Device Manager agent starts or when the configuration definition file is updated by pair operations, the following optimizations are performed: ▪ The unit ID, LDEV number, and serial number of a command device are added as comments. ▪ If the above command device becomes unavailable due to, for example, a change to the volume name, the configuration definition file information is updated so that the command device can be used. ▪ If the host is connected to multiple command devices in a storage subsystem and only some of those command devices are specified, the rest of the command devices are specified as reserved command devices. ▪ Command devices that are not being used are deleted. ▪ The CU and LDEV numbers of a command device and pair volume are added as a comment in the format *cu*:*ldev*. Default: false
server.agent.rm.pairDefinitionForm	Specify which format should be used to specify pair volume information in the configuration definition file when creating a pair: HORCM_DEV format or HORCM_LDEV format. If you want to unify the format into the HORCM_DEV format, specify HORCM_DEV. If you want to unify the format into the HORCM_LDEV format, specify HORCM_LDEV. We recommend that you use the HORCM_LDEV format. The Device Manager agent decides which format should be used in the configuration definition file when creating a pair according to the following conditions: ▪ Which format is used in the existing configuration definition file: HORCM_DEV format or HORCM_LDEV format. ▪ A pair is created for a new copy group or existing copy group. Table 3-41 lists the conditions that the Device Manager agent uses to decide whether to apply the HORCM_DEV or the HORCM_LDEV format. ***Caution:*** Do not specify HORCM_LDEV in an environment where CCI 01-17-03/04 or later is not installed. If you do this, the message An attempt to create a pair has failed. Error detail, host "*host-name*" : "*error-detail*" is displayed, and the attempt to create pairs fails. Default: None

Table 3-41 Conditions on Which the Device Manager Agent Decides Which Format Should be Used in the Configuration Definition File

Which format is used in the existing configuration definition file	Pair operation	Format to be used in the configuration definition file
No format is used.	Creating a pair for a new copy group.	If a format is specified in the property: The format specified in the property If a format is not specified in the property: The format HORCM_DEV
HORCM_DEV format is used.	Adding a pair to an existing copy group.	HORCM_DEV format, regardless of the format specified in the property
	Creating a pair for a new copy group.	If a format is specified in the property: The format specified in the property If a format is not specified in the property: The format HORCM_DEV
HORCM_LDEV format is used.	Adding a pair to an existing copy group.	HORCM_LDEV format, regardless of the format specified in the property
	Creating a pair for a new copy group.	If a format is specified in the property: The format specified in the property If a format is not specified in the property: The format HORCM_LDEV
Both HORCM_DEV format and HORCM_LDEV format are used.	Adding a pair to an existing copy group that uses HORCM_DEV format.	HORCM_DEV format, regardless of the format specified in the property
	Adding a pair to an existing copy group that uses HORCM_LDEV format.	HORCM_LDEV format, regardless of the format specified in the property
	Adding a pair to an existing copy group that uses both HORCM_DEV format and HORCM_LDEV format.	If a format is specified in the property: The format specified in the property If a format is not specified in the property: The format HORCM_DEV
	Creating a pair for a new copy group.	If a format is specified in the property: The format specified in the property If a format is not specified in the property: The format HORCM_DEV

Table 3-42 server.properties File (Setting Up Timeout)

Property	Description
server.agent.rm.moduleTimeOut	Specify a timeout value for receiving command execution results when the Device Manager agent executes a CCI command (in seconds). When a command takes longer to execute than the specified value, the Device Manager agent concludes that an error occurred during command execution. This property should be changed only by a system administrator who has expert knowledge, when performance of the Device Manager agent's pair configuration functionality needs to be fine-tuned. Default: 600 (seconds)
server.http.server.timeOut	Specify a timeout value for receiving a response from the Device Manager server, for example, when registering host information by executing the HiScan command, restarting the service, refreshing the host (in seconds). If no response is received from the Device Manager server within the specified time, the Device Manager agent concludes that an error has occurred and the HiScan command terminates abnormally. Specify a value from 100 to 3,600. If the specified value is less than 100, the timeout is assumed to be 100. If the specified value is more than 3,600, the timeout is assumed to be 3,600. Default: 600
server.util.processTimeOut	Specify the Device Manager agent's normal execution time for external programs (in milliseconds). If an external program takes longer than the specified time, the Device Manager agent concludes that an error has occurred and terminates the program. If you specify too short a time period, the Device Manager agent might stop execution of external programs that are running regularly. Do not edit this property without current knowledge of the Device Manager agent's performance. Default:600000
server.agent.fs.moduleTimeOut	Specify a timeout value for receiving command execution results when a file-system-related operation is executed in Provisioning Manager (in seconds). Specify a value from 1 to 2,147,483,647. Default: 1200
server.agent.vm.moduleTimeOut	Specify a timeout value for receiving command execution results when a volume-manager-related operation is executed in Provisioning Manager (in seconds). Specify a value from 1 to 2,147,483,647. Default: 1200
server.agent.os.moduleTimeOut	Specify a timeout value for receiving command execution results when a host setting, such as device recognition, is performed in Provisioning Manager (in seconds). Specify a value from 1 to 2,147,483,647. Default: 180

4

Troubleshooting

This chapter describes how to troubleshoot problems with the Storage Navigator:

- Troubleshooting
- Calling the Hitachi Data Systems Support Center

Troubleshooting

This section describes how to troubleshoot the Device Manager agent.

Obtaining Error Information

If an error occurs in the Device Manager agent, acquire error information from both the Device Manager agent and the Device Manager server.

- To acquire error information from the Device Manager agent, execute the `TIC` command (the Trouble Information Collector tool). For details, see TIC Command Syntax.
- To acquire error information from the Device Manager server, see the *Hitachi Device Manager Server Configuration and Operation Guide*.

Common Problems and Solutions

The following table lists common problems that occur on the Device Manager agent and describes how to resolve them.

Table 4-1 Common Problems and Solutions

No.	Problem	Solution
1	The following message was output to the event log or the system log: `[HORCM_005] Could not create endpoint for remote connection.`	This message is output when multiple HiScan commands are executed at the same time. No action is required.
2	The following message was output to the event log or the system log: `[HORCM_007] Illegal parameter values in HORCM configuration file.`	
3	When executing the HiScan command, the KAIC22019-E error message is output, and host information cannot be registered on the Device Manager server.	The path to the LU managed by the Device Manager recognized by the host has been disabled, possibly due to a lost connection. Either restore the disabled path, or change the OS settings so that the disabled path is no longer recognized.
4	A communication error occurs, and the processing of other Hitachi Storage Command Suite products stops.	Another Hitachi Storage Command Suite product might have attempted to access the Device Manager agent either immediately after the installation of the Device Manager agent was complete, or immediately after the Device Manager agent services started. Wait a few minutes, and then retry the operation.
5	Protection Manager - Console cannot be started from the Device Manager Web Client.	Use an OS supported by Protection Manager in the management client. If the host OS is Windows Server 2003 (no SP), Protection Manager - Console cannot be started from the Device Manager Web Client.
6	In a Windows environment, two copies of **HBase Agent** are displayed in the Add or Remove programs window of the computer on which the Device Manager agent or Dynamic Link Manager is installed.	Execute the hbsa_util command to delete the files and registry entries of the Device Manager agent. To execute the hbsa_util command: 1. Log on to Windows as a user with Administrator permissions. 2. Execute the command hbsa_util.exe. For details on the command, see hbsa_util Command Syntax.
7	In a Windows environment, **HBase Agent** is displayed in the Add or Remove programs window even after you uninstall both the Device Manager agent and Dynamic Link Manager.	

No.	Problem	Solution
8	JavaVM ends abnormally in the following environments: Windows Server 2003 (x64 and IPF), Windows Server 2003 R2 (x64), Windows Server 2008 (x64 and IPF), and Windows Server 2008 R2 (x64 and IPF).	Another program linked with Device Manager might be frequently accessing the Device Manager agent that is running. If JavaVM ends abnormally, edit the following file: *installation-folder-for-Device-Manager-agent*\agent\bin\Server.cmd Use a text editor to open the Server.cmd file, and then add -Djava.compiler=NONE to the Java startup options. The following shows an example of editing the Server.cmd file: ..java -Dalet.msglang -Djava.compiler=NONE %1 %2 -classpath "C:\Program Files\HITACHI\HDVM\HBaseAgent\agent\jar\agent4.jar;C:\Program Files\HITACHI\HDVM\HBaseAgent\agent\jar\jdom.jar;C:\Program Files\HITACHI\HDVM\HBaseAgent\agent\jar\xerces.jar;C:\Program Files\HITACHI\HDVM\HBaseAgent\agent\jar\servlet.jar;C:\Program Files\HITACHI\HDVM\HBaseAgent\agent\jar\log4j-1.2.3.jar" com.Hitachi.soft.HiCommand.DVM.agent4.as.export.Server %* exit /b %ERRORLEVEL%
9	The following messages are output to Event ID: 51 or Event ID: 57 in the Windows event log: ▪ Event ID: 51 An error was detected on device \Device\Harddisk*nn*\DR*n* during a paging operation. (where *n* is a number.) ▪ Event ID: 57 The system failed to flush data to the transaction log. Corruption may occur.	These messages are output when a paired S-VOL is mounted. No action is required.

No.	Problem	Solution
10	When executing the HiScan command in a Windows Server 2008 or Windows Server 2008 R2 environment, the KAIC22009-E, KAIC22014-E, KAIC22019-E, or KAIC22048-E error message is output, and host information cannot be registered on the Device Manager server.	This occurs if there are 100 or more LUs managed by Device Manager recognized by a single host, and the Device Manager agent is upgraded from version 6.0.0-00 - 6.2.0-02 to version 6.4 or later via an overwrite installation. To avoid this, follow the procedure in Specifying Settings When a Host Manages 100 or More LUs.
11	When a host refresh is performed in a Windows Server 2008 or Windows Server 2008 R2 environment, an OutOfMemory error occurs on the host, and there is no response for a while.	
12	When using a version of VxVM earlier than 4.0 in a Solaris environment, file system names are not shown in the Device Manager Web Client.	To check the correspondence between the file system and LUN, use VxVM version 4.0 or later. When using a version of VxVM earlier than 4.0, the Device Manager agent does not notify the Device Manager server of correspondence between the file system and LUN if device names are set based on the enclosure.
13	In a Solaris environment, Unknown is displayed as the LU partition size in Provisioning Manager.	Partition information cannot be acquired for LUs that do not have a label. Set a label for the LU.
14	In an AIX environment, SC_DISK_ERR2 (Device Busy) is output in the error log of the standby node. In addition, HSDRV_RSV_CONFLICT is output to the error log.	The active node is providing disk reserve normally for the shared disk, and therefore there is no problem with the system. Shared disk information is acquired from the Device Manager agent running on the active node, and therefore there is no problem with the operation of Device Manager. This problem is listed because it might occur rarely if the execution frequency of the HiScan command for the Device Manager agent is set to the same time in both the active node and the standby node and if there is a high I/O load on the shared disk.

Calling the Hitachi Data Systems Support Center

If you need to call the Hitachi Data Systems Support Center, please provide as much of the following information about the problem as possible:

- Circumstances surrounding the error or failure
- The platform (OS and version)
- Host agent version and build
- HBA make, model, firmware, and driver
- Device Manager server version and build
- Device Manager server OS and version (including build)
- All applicable configuration and log files of the Device Manager agent and the `HiScan` command (see Table 4-2 through Table 4-6)
- The exact content of any error messages displayed on the Device Manager server, Device Manager client, the Device Manager agent, and/or host system

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 of the United States: (858) 547-4526

Table 4-2 Required Logs for Troubleshooting Windows Hosts

File to Collect	File Location	Explanation
access.log	*Installation-directory-for-Device-Manager-agent*/agent/logs/	Access log for the communication control function
error.log	*Installation-directory-for-Device-Manager-agent*/agent/logs/	Communication control function error log
service.log	*Installation-directory-for-Device-Manager-agent*/agent/logs/	Servlet function operation log
trace.log	*Installation-directory-for-Device-Manager-agent*/agent/logs/	Warnings of communication control function, internal trace data log
HiScan.msg	*Installation-directory-for-Device-Manager-agent*/bin/logs/	Directory where HiScan output messages are stored
HiScan.log	*Installation-directory-for-Device-Manager-agent*/bin/logs/	HiScan output log
HiScan.err	*Installation-directory-for-Device-Manager-agent*/bin/logs/	HiScan output error log
hdvmagterr.log	*Installation-directory-for-Device-Manager-agent*/bin/logs/	hdvmagt log file
hldu_err.log	*Installation-directory-for-Device-Manager-agent*/util/logs/	hldutil.exe error log
timestamp.log	*Installation-directory-for-Device-Manager-agent*/util/logs/	Volume information extracted by HLDUTIL
Device_Manager_VERSION NO._InstallLog.log	*Installation-directory-for-Device-Manager-agent*	An information output log file when the Device Manager agent is installed.

Table 4-3 Required Logs for Troubleshooting Solaris Hosts

File to Collect	File Location	Explanation
access.log	/opt/HDVM/agent/logs/	Access log for the communication control function
error.log	/opt/HDVM/agent/logs/	Communication control function error log
service.log	/opt/HDVM/agent/logs/	Servlet function operation log
trace.log	/opt/HDVM/agent/logs/	Warnings of communication control function, internal trace data log
HiScan.msg	/var/opt/HDVM/logs/	Directory where HiScan output messages are stored
HiScan.log	/var/opt/HDVM/logs/	HiScan output log
HiScan.err	/var/opt/HDVM/logs/	HiScan output error log
hdvmagterr.log	/var/opt/HDVM/logs/	Hdvmagt log file
hldn_err.log	/var/opt/HDVM/logs/	HLDUTIL log file
timestamp.log	/var/opt/HDVM/logs/	Volume information extracted by HLDUTIL
messages	/var/adm/	OS output log

Table 4-4 Required Logs for Troubleshooting HP-UX Hosts

File to Collect	File Location	Explanation
access.log	/opt/HDVM/agent/logs/	Access log for the communication control function
Error.log	/opt/HDVM/agent/logs/	Communication control function error log
service.log	/opt/HDVM/agent/logs/	Servlet function operation log
Trace.log	/opt/HDVM/agent/logs/	Warnings of communication control function, internal trace data log
HiScan.msg	/var/opt/HDVM/logs/	Directory where HiScan output messages are stored
HiScan.log	/var/opt/HDVM/logs/	HiScan output log
HiScan.err	/var/opt/HDVM/logs/	HiScan output error log
hdvmagterr.log	/var/opt/HDVM/logs/	Hdvmagt log file
hldn_err.log	/var/opt/HDVM/logs/	HLDUTIL log file
timestamp.log	/var/opt/HDVM/logs/	Volume information extracted by HLDUTIL
syslog.log	/var/adm/syslog/	OS output log
swagent.log	/var/adm/sw/	Device Manager agent install log
swinstall.log	/var/adm/sw/	Device Manager agent install log

Table 4-5 Required Logs for Troubleshooting AIX Hosts

File to Collect	File Location	Explanation
access.log	/usr/HDVM/agent/logs/	Access log for the communication control function
Error.log	/usr/HDVM/agent/logs/	Communication control function error log
service.log	/usr/HDVM/agent/logs/	Servlet function operation log
Trace.log	/usr/HDVM/agent/logs/	Warnings of communication control function, internal trace data log
HiScan.msg	/var/HDVM/logs/	Directory where HiScan output messages are stored
HiScan.log	/var/HDVM/logs/	HiScan output error log
HiScan.err	/var/HDVM/logs/	HiScan output error log
hdvmagterr.log	/var/HDVM/logs/	hdvmagt log file
hldu_err.log	/var/HDVM/logs/	HLDUTIL log file
timestamp.log	/var/HDVM/logs/	Volume information extracted by HLDUTIL
syslog.log	/var/adm/syslog/	OS output log

Table 4-6 Required Logs for Troubleshooting Linux Hosts

File to Collect	Location where File is Stored	Explanation
access.log	/opt/HDVM/agent/logs/	Access log for the communication control function
error.log	/opt/HDVM/agent/logs/	Communication control function error log
service.log	/opt/HDVM/agent/logs/	Servlet function operation log
trace.log	/opt/HDVM/agent/logs/	Warnings of communication control function, internal trace data log
HiScan.msg	/var/opt/HDVM/logs/	Directory where HiScan output messages are stored
HiScan.log	/var/opt/HDVM/logs/	HiScan output log
HiScan.err	/var/opt/HDVM/logs/	HiScan output error log
hdvmagterr.log	/var/opt/HDVM/logs/	Hdvmagt log file
hldu_err.log	/var/opt/HDVM/logs/	HLDUTIL log file
timestamp.log	/var/HDVM/logs/	Volume information extracted by HLDUTIL

Acronyms and Abbreviations

API	Application Programming Interface
ASCII	American Standard Code for Information Interchange
CD-ROM	Compact Disk - Read-Only Memory
CIM	Common Information Model
CU	Control Unit
CVS	Custom Volume Size
DKC	Disk Controller
DMP	Dynamic MultiPathing
DNS	Domain Name Server
DSM	Device Specific Module
DST	Daylight Saving Time
EM64T	Extended Memory 64 Technology
FAT	File Allocation Table
FC	Fibre Channel
GUI	Graphical User Interface
I/O	Input/Output
ID	Identifier
HBA	Host Bus Adapter
HFS	Hierarchical File System
HTTP	Hypertext Transfer Protocol
IP	Internet Protocol
IPF	Itanium® Processor Family
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
iSCSI	Internet Small Computer System Interface
JFS	Journaled File System
JNI	Java Native Interface
LDEV	Logical Device
LU	Logical Unit
LUN	Logical Unit Number
LVM	Logical Volume Manager

MPIO	Multipath I/O
MRCF-Lite	Multiple RAID Coupling Feature - Lite
NIC	Network Interface Card
NPIV	N_Port ID Virtualization
NTFS	New Technology File System
OS	Operating System
P-VOL	Primary Volume
PA-RISC	Precision Architecture - Reduced Instruction Set Computer
RAID	Redundant Array of Independent Disks
RTE	RunTime Environment
S-VOL	Secondary Volume
SAN	Storage Area Network
SCSI	Small Computer System Interface
SDS	Solstice DiskSuite
SED	Stack Execution Disable
SNMP	Simple Network Management Protocol
SSL	Secure Sockets Layer
SP	Service Pack
SPARC	Scalable Processor Architecture
SVM	Solaris Volume Manager
TCP	Transmission Control Protocol
UAC	User Account Control
UDP	User Datagram Protocol
UFS	UNIX File System
VDS	Virtual Disk Service
WBEM	Web-Based Enterprise Management
WOW64	Windows On Windows 64-bit
WWN	World Wide Name
XML	Extensible Markup Language
ZFS	Zettabyte File System

Index

U

V

Hitachi Data Systems

Corporate Headquarters
750 Central Expressway
Santa Clara, California 95050-2627
U.S.A.
Phone: 1 408 970 1000
www.hds.com
info@hds.com

Asia Pacific and Americas
750 Central Expressway
Santa Clara, California 95050-2627
U.S.A.
Phone: 1 408 970 1000
info@hds.com

Europe Headquarters
Sefton Park
Stoke Poges
Buckinghamshire SL2 4HD
United Kingdom
Phone: + 44 (0)1753 618000
info.eu@hds.com

MK-92HC019-22