

HP StorageWorks Command View XP Advanced Edition software

Device Manager agent installation and configuration
guide

Legal notices

© Copyright 2005, 2007 Hewlett-Packard Development Company, L.P.

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

AIX and IBM are registered trademarks of International Business Machines Corporation.

Emulex is a registered trademark of Emulex Corporation.

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

Itanium is a registered trademark of Intel corporation or its subsidiaries in the United States and other countries.

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

JNI is a registered trademark of Applied Micro Circuits Corporation (formerly JNI Corporation).

Linux is a registered trademark of Linus Torvalds.

Microsoft and Windows are registered trademarks and Windows Server is a trademark of Microsoft Corporation.

QLogic is a registered trademark of QLogic Corporation.

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

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

Red Hat is a registered trademark of Red Hat, Inc.

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

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

UNIX is a registered trademark of The Open Group in the United States and other countries.

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

This product includes software developed by the Apache Software Foundation (<http://www.apache.org/>).

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

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

This product includes software developed by Greg Stein <gstein@lyra.org> for use in the mod_dav module for Apache (http://www.webdav.org/mod_dav/).



HP StorageWorks Command View XP Advanced Edition software includes RSA BSAFE Cryptographic software from RSA Security Inc.

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

This product includes software developed by the University of California, Berkeley and its contributors.

This software contains code derived from the RSA Data Security Inc. MD5 Message-Digest Algorithm, including various modifications by Spyglass Inc., Carnegie Mellon University, and Bell Communications Research, Inc (Bellcore).

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

Part number: T1780-96037

Sixth Edition: February 2007

Contents

About this guide

Revision history.....	7
Intended audience	8
Prerequisites.....	8
Document conventions and symbols.....	8
HP technical support.....	9
Subscription service.....	9
HP web sites	9
Documentation feedback.....	10

1 Overview of the Device Manager agent

1-1 Device Manager agent overview.....	11
--	----

2 Installation requirements and procedures

2-1 Supported OSs and required programs for the Device Manager agent	12
2-1-1 Operating systems supported by the Device Manager agent.....	12
2-1-2 Patches required for operating systems supported by the Device Manager agent.....	13
2-1-3 Java Runtime Environment supplied with the Device Manager agent	17
2-1-4 Device Manager server versions supported by the Device Manager agent.....	17
2-2 File systems supported by the Device Manager agent	17
2-3 Storage subsystems supported by Device Manager agent.....	18
2-4 Requirements for obtaining host WWN information.....	18
2-5 Requirements for using FC-HUB (FC-SWITCH)	19
2-6 When IPv6 is enabled on the host	19
2-7 Volume managers supported by the Device Manager agent	19
2-8 Cluster software supported by the Device Manager agent	20
2-9 Path management software supported by the Device Manager agent.....	21
2-10 Installing the Device Manager agent.....	22
2-10-1 Installing the Device Manager agent on a Windows system.....	23
2-10-2 Installing Device Manager agent on Solaris, AIX, HP-UX®, or Linux	26
2-11 Setting up the Device Manager agent.....	28
2-11-1 Setting server information	28
2-11-2 Setting the execution period for the HiScan command.....	29
2-12 Uninstalling the Device Manager agent.....	31
2-12-1 Uninstalling the Device Manager agent on Windows systems	32
2-12-2 Uninstalling the Device Manager agent in Solaris, AIX, HP-UX, and Linux	32

3 Device Manager agent operations

3-1 Configuring and operating the Device Manager agent	34
3-1-1 Automatic and manual execution of the HiScan command.....	34
3-1-2 Methods of operating the Device Manager agent.....	34
3-2 Notes on Device Manager agent operations.....	35
3-2-1 When a host has multiple network adapters	35
3-2-2 When the storage subsystem configuration changes	35
3-2-3 When an invalid path exists	35
3-2-4 When the host is Windows server 2003 or 2003 x64 edition	35
3-2-5 For multi-path configurations.....	35
3-2-6 Changing the Windows firewall settings manually.....	35
3-2-7 When changing the user executing the Device Manager agent service	36
3-2-8 When the host OS is Solaris, AIX, HP-UX, or Linux.....	36
3-2-9 When the host OS is AIX in a cluster environment	36
3-2-10 When the Device Manager agent is accessed by other Command View XP AE Suite software	36
3-2-11 When the host OS is Windows and a device is assigned a drive letter.....	37
3-2-12 When the host OS is Solaris, and VxVM is used.....	37

3-2-13	When the host OS is Linux.....	37
3-2-14	When the host recognizes 100 or more LUs	37
3-2-15	When the host OS is Solaris	40
3-3	Starting and stopping the Device Manager agent.....	40
3-3-1	Starting the Device Manager agent	40
3-3-2	Stopping the Device Manager agent	41
3-3-3	Checking the operating status of the Device Manager agent.....	41
3-3-4	Restarting the Device Manager agent	42
3-3-5	If the Device Manager agent cannot stop	42
3-4	Modifying server information	42
3-5	Changing the execution period of the HiScan command	42
3-6	Device Manager agent commands	42
3-6-1	hbsasrv command syntax	43
3-6-2	HiScan command syntax.....	43
3-6-3	hldutil command syntax	44
3-6-4	hdvmagt_schedule command syntax	48
3-6-5	hdvmagt_account command syntax	48
3-7	Property files	49
3-7-1	server.properties file	50
3-7-2	logger.properties file	53
3-7-3	programproductinfo.properties file	54
3-7-4	hldutil.properties file	54
3-8	Using a user-created RAID Manager XP configuration definition file.....	55
3-8-1	Requirements for using a user-created RAID Manager XP configuration definition file in Device Manager	55
3-8-2	Reporting the information of the RAID Manager XP configuration definition file to the Device Manager server.....	57
3-8-3	Cautionary notes when Device Manager is used with RAID Manager XP	57
4	Troubleshooting Device Manager agent operations	
4-1	Acquiring error information collectively	59

[Acronyms and abbreviations](#)

[Index](#)

Figures

Figure 4-1 Executing TIC command	60
--	----

Tables

Table 1 Revisions	7
Table 2 Document conventions	8
Table 2-1 Supported operating systems.....	12
Table 2-2 Patches required for the Solaris 7 OS.....	13
Table 2-3 Patches required for the Solaris 8 OS.....	14
Table 2-4 Patches required for the Solaris 9 OS.....	14
Table 2-5 Patches required for the Solaris 10 OS.....	15
Table 2-6 Patches required for the AIX OS	15
Table 2-7 Patches required for the HP-UX 11.0 OS	15
Table 2-8 Patches Required for the HP-UX 11i OS	16
Table 2-9 Patches Required for HP-UX 11i.v2 OS.....	17
Table 2-10 Patches required for the Red Hat Enterprise Linux OSs.....	17
Table 2-11 File systems supported by the Device Manager agent.....	17
Table 2-12 HBA models required to obtain host WWN information	18
Table 2-13 Volume managers supported by the Device Manager agent.....	19
Table 2-14 Cluster software supported by the Device Manager agent.....	20
Table 2-15 Path management software supported by the Device Manager agent	21
Table 2-16 Minimum free hard disk space needed for installation	26
Table 3-1 Items to set when several LUs are recognized by a host	38
Table 3-2 Setting values when a volume manager is not used	39
Table 3-3 Setting values when a volume manager is used (in Windows)	39
Table 3-4 Setting values when a volume manager is used (in Solaris)	39
Table 3-5 Setting values when a volume manager is used (in AIX)	39
Table 3-6 Setting values when a volume manager is used (in HP-UX)	40
Table 3-7 Setting values when a volume manager is used (in Linux).....	40
Table 3-8 hbsasrv command syntax.....	43
Table 3-9 HiScan command syntax	44
Table 3-10 hldutil command syntax	45
Table 3-11 Sort key descriptions	47
Table 3-12 Displayed items.....	47
Table 3-13 Correspondence between RaidID and models	47
Table 3-14 hdvmagt_schedule command syntax	48
Table 3-15 hdvmagt_account command syntax.....	49
Table 3-16 server.properties file (setting up ports used by the daemon process and the Web server function)	50
Table 3-17 server.properties file (setting the host name, IP address, and NIC used by the Web server function)	50
Table 3-18 server.properties file (setting up basic operations of the Web server function).....	51
Table 3-19 server.properties file (security settings for the Web server function).....	51
Table 3-20 server.properties file (information of the Device Manager server)	52
Table 3-21 server.properties file (setting up RAID Manager XP).....	52
Table 3-22 server.properties file (setting up timeout)	53
Table 3-23 logger.properties file.....	54
Table 3-24 programproductinfo.properties file.....	54
Table 3-25 hldutil.properties file	54
Table 3-26 Requirements for a RAID Manager XP configuration definition file used in Device Manager (HORCM_MON parameter).....	56
Table 3-27 Requirements for a RAID Manager XP configuration definition file used in Device Manager (HORCM_CMD parameter).....	56

Table 3-28 Requirements for a RAID Manager XP configuration definition file used in Device Manager (HORCM_DEV parameter).....	56
Table 3-29 Requirements for a RAID Manager XP configuration definition file used in Device Manager (HORCM_LDEV parameter).....	56
Table 3-30 Requirements for a RAID Manager XP configuration definition file used in Device Manager (HORCM_INST parameter).....	57

About this guide

This guide provides information about:

- Installing HP StorageWorks Command View XP Advanced Edition Device Manager agent software.
- Installing Java2 Java™ Runtime Environment (JRE).

Revision history

Table 1 Revisions

Date	Edition	Revision
July 2005	First	Initial release
October 2005	Second	<ul style="list-style-type: none">• Red Hat Enterprise Linux AS 4.0 and Red Hat Enterprise Linux ES 4.0 are now supported.• Addition to the Windows Firewall exceptions list can now be performed during installation.• Java Runtime Environment (JRE) for Windows, Solaris, and HP-UX is now supplied on CD-ROM.• The Windows default installation folder has been changed.
February 2006	Third	<ul style="list-style-type: none">• The following operating systems are now supported for the Device Manager agent.<ul style="list-style-type: none">• Red Hat Enterprise Linux AS 4/ES 4 x86• Red Hat Enterprise Linux AS 3/ES 3 EM64T• Red Hat Enterprise Linux AS 4/ES 4 EM64T• SUSE LINUX Enterprise Server 9• JRE is embedded in the installer of Device Manager agent.
May 2006	Fourth	<ul style="list-style-type: none">• The Windows Server 2003 R2 OS was supported.• AMD64 for Red Hat Enterprise Linux AS/ES3.0 and Red Hat Enterprise Linux AS/ES4.0 were supported.• The <code>-serdec</code> option for the <code>hldutil</code> command was added.• The <code>hdvmagt_account</code> command could specify a host name value in the <code>server.server.serverIPAddress</code> property.
November 2006	Fifth	<ul style="list-style-type: none">• Red Hat Enterprise Linux ES/AS 4.0 Update3 is now supported.• Required patches for Solaris 7, Solaris 10, and AIX have been added.• The patch PHCO_27375 required for HP-UX 11.0 has been deleted and the patch PHCO_31879 has been added.• The cluster software HACMP 5.3 is now supported by AIX 5.3 64 bit version.• Windows MPIO is now supported.• The procedures for installing Device Manager agent on UNIX systems have been integrated.• The number of characters that can be entered for the user ID and password, which are specified when the <code>HiScan</code> command and <code>hdvmagt_account</code> command are executed, has been changed.• The method for setting the memory heap size has been changed.• The <code>server.agent.maxMemorySize</code> property has been added to the <code>server.properties</code> file.

Table 1 Revisions

Date	Edition	Revision
February 2007	Sixth	<ul style="list-style-type: none"> • HP-UX 11i v3 for PA-RISC (64-bit) and IPF is now supported. • Red Hat Enterprise Linux ES/AS 4.0 Update 4 for x86 is now supported. • An explanation has been added for conditions that might prevent acquisition of host WWN information in a host environment that uses a multi-path configuration. • Veritas Volume Manager 5.0 is now supported on Solaris 9 and Solaris 10. • VERITAS Cluster Server 4.1 cluster software is now supported on Solaris 10. • Serviceguard 11.17 cluster software is now supported on HP-UX 11i v2. • Sun StorEdge Traffic Manager path management software is now supported on Solaris 10. • MPIO path management software is now supported on AIX 5.2 and 5.3. • PV-link software and MPIO path management software are now supported on HP-UX 11i v3 PA-RISC (64-bit) and IPF. • Cautionary notes when the host OS is Windows Server 2003 IPF have been changed. • An explanation has been added for conditions that might prevent acquisition of WWN information and LU information for alternate paths in a host environment that use multi-path configurations. • The description of an OS and its host environment, in which the Device Manager server is not notified of correspondence between a file system and a LUN when a device name is based on its enclosure, has been changed. • Notes when the host OS is Windows Server 2003 (IPF) have been added. • Cautionary notes for properly running the Device Manager agent have been added. • Cautionary notes for checking the operating status of the Device Manager agent have been added. • Cautionary notes about installation of the Device Manager agent and service startup when the Device Manager server is not running have been added. • The <code>hldutil.properties</code> file (<code>agent.util.hpux.displayDsf</code> property) has been added to the property files used by the Device Manager agent. • A table for the <code>server.properties</code> file has been divided according to categories. • The default values for the following properties of the <code>server.properties</code> file have been changed: <ul style="list-style-type: none"> • <code>server.agent.maxMemorySize</code> property • <code>server.agent.rm.moduleTimeOut</code> property • An explanation on how to use the RAID Manager XP configuration definition file created by the user has been added. • The RAID Manager XP configuration definition file can now be specified in <code>HORCM_LDEV</code> format.

Intended audience

This guide is intended for customers and HP-authorized service providers who are experienced with the following:

- Data processing and direct-access storage device subsystems
- HP StorageWorks XP Series disk array(s)

Prerequisites

Prerequisites for installing this product include:

- Reading through the user's guide and release notes
- Meeting all the minimum installation requirements
- Reviewing the Release Notes on the CD for any last-minute announcements

Document conventions and symbols

Table 2 Document conventions


Convention Element	Convention Element
Medium blue text: Figure 1	Cross-reference links and e-mail addresses

Table 2 Document conventions

Convention Element	Convention Element
Medium blue, underlined text (http://www.hp.com)	Web site addresses
Bold font	<ul style="list-style-type: none">• Key names• Text typed into a GUI element, such as into a box• GUI elements that are clicked or selected, such as menu and list
<i>italics font</i>	Text emphasis
Monospace font	<ul style="list-style-type: none">• File and directory names• System output• Code• Text typed at the command-line
<i>Monospace, italic font</i>	<ul style="list-style-type: none">• Code variables• Command-line variables
Monospace, bold font	Emphasis of file and directory names, system output, code, and text typed at the command-line

 **CAUTION:** Indicates that failure to follow directions could result in damage to equipment or data.

 **IMPORTANT:** Provides clarifying information or specific instructions.

 **NOTE:** Provides additional information.

 **TIP:** Provides helpful hints and shortcuts.

HP technical support

Telephone numbers for worldwide technical support are listed on the HP support web site:
<http://www.hp.com/support>.

Collect the following information before calling:

- Technical support registration number (if applicable)
- Product serial numbers
- Product model names and numbers
- Error messages
- Operating system type and revision level
- Detailed questions

For continuous quality improvement, calls may be recorded or monitored.

Subscription service

HP recommends that you register your product at the Subscriber's Choice for Business web site:
<http://www.hp.com/go/e-updates>.

After registering, you will receive e-mail notification of product enhancements, new driver versions, firmware updates, and other product resources.

HP web sites

For additional information, see the following HP web sites:

- <http://www.hp.com/>
- <http://www.hp.com/go/storage>
- http://www.hp.com/service_locator
- <http://www.docs.hp.com>

Documentation feedback

HP welcomes your feedback.

To make comments and suggestions about product documentation, please send a message to storagedocs.feedback@hp.com. All submissions become the property of HP.

1 Overview of the Device Manager agent

This chapter contains an overview of the Device Manager agent:

1-1 Device Manager agent overview

HP StorageWorks Command View XP AE Device Manager (called Device Manager in this guide) is another name for HP StorageWorks Command View XP Advanced Edition software. The Device Manager agent collects information about storage devices (logical units on a disk array) that are connected to a host server as well as information about the host server itself. It then transmits this information to the Device Manager server using TCP/IP. The collected information includes the capacity and usage rate for each storage unit, the worldwide name (WWN) of the host bus adapter (HBA), mount points, file system types, and SCSI addresses.

Device Manager agent commands

The Device Manager agent command `hldutil` collects the preceding information. The agent command `HiScan` transmits the information to the Device Manager server, and a resident program (HBsA) provides the information in response to requests from programs, such as the Device Manager server and Hitachi Dynamic Link Manager.

For more information:

- For details about `hldutil`, see section [3-6-3](#) .
- For information about `HiScan`, see section [3-6-2](#) .
- For details about how to start HBsA, see section [3-3](#) .

Device Manager agent tasks

The Device Manager agent can perform the following tasks in parallel, as necessary:

- Requesting host information (a request from the Device Manager server)
- Requesting creation of a volume pair (a request from the Device Manager server)
- Requesting linkage with other program products

All processes are integrated into a single add-on module, and managed by the Device Manager agent.

Device Manager agent programs

The Device Manager agent incorporates two programs: a daemon (for UNIX® platforms) or a service (for Windows® platforms), and WebServer. When the Device Manager agent receives a request from the Device Manager server, the daemon or service process generates the WebServer process. The WebServer process gathers server-side information and forwards this information to the Device Manager server via TCP/IP. This information includes utilization of LU capacity, host bus adapter (HBA), worldwide names (WWNs), mount points (not currently available for VERITAS), file system types and names, and the operating system's SCSI address.

The Device Manager server presents its view of StorageWorks XP disk array resources to the Device Manager client.

You can display this information by executing the `hldutil` command, and you may send this information by executing the `HiScan` command. The `hldutil` command and `HiScan` command are part of the command line interface (CLI) in the Device Manager agent. Both of these commands are explained further in this guide.

In a standard installation of the Device Manager agent, the operating system task scheduler is configured to execute the `HiScan` command on a periodic basis (for Windows, Solaris™, and HP-UX). The recommended duration for a `HiScan` execution configuration is from 30 minutes to as long as 24 hours, depending upon your operational environment. The Agent (`HiScan`) parameters include the IP address of the Device Manager server.



NOTE: See the release notes for the latest information about the uses of Device Manager.

2 Installation requirements and procedures

This chapter contains the following sections:

- Supported operating systems and required programs for the Device Manager agent (see section 2-1)
- File systems supported by the Device Manager agent (see section 2-2)
- Supported disk arrays (see section 2-3)
- Requirements for Obtaining host WWN information (see section 2-4)
- Requirements for using FC-HUB (FC-SWITCH) (see section 2-5)
- When IPv6 Is enabled on the host (see section 2-6)
- Volume managers supported by the Device Manager agent (see section 2-7)
- Cluster software supported by the Device Manager agent (see section 2-8)
- Path management software supported by the Device Manager agent (see section 2-9)
- Installing the Device Manager agent (see section 2-10)
- Setting up the Device Manager agent (see section 2-11)
- Uninstalling the Device Manager agent (see section 2-12)

2-1 Supported OSs and required programs for the Device Manager agent

The OSs and patches supported by the Device Manager agent and the versions of the Device Manager server that can be connected are described in this section.

2-1-1 Operating systems supported by the Device Manager agent

Table 2-1 lists the OSs supported by the Device Manager agent.

Table 2-1 Supported operating systems

OS	OS Version	Supported Architecture	Remarks
Windows 2000	Not applicable	x86	Service Pack 4 or later is required.
Windows Server™ 2003	Not applicable	x86	Service Pack 1 is supported. ¹
		IPF	The Enterprise and Datacenter Editions of Windows Server 2003 support the IPF version. Runs under Windows on Windows 64 (WOW64). Service Pack 1 is supported. We recommend installing Service Pack 1. ¹
Windows Server 2003 x64 Edition	Not applicable	<ul style="list-style-type: none">• EM64T• AMD64	¹
Windows Server 2003 R2	Not applicable	x86	¹
	x64 Edition	<ul style="list-style-type: none">• EM64T• AMD64	¹
Solaris	7	SPARC (32 and 64 bit)	We recommend installing Solaris Patch Cluster.
	8		
	9		
	10 ²		
AIX®	5.1	32 and 64 bit	Not applicable
	5.2		
	5.3		
HP-UX	11.0	PA-RISC (32 and 64 bit)	Workstation is not supported.

Table 2-1 Supported operating systems

OS	OS Version	Supported Architecture	Remarks
	11i v1		
	11i v2	<ul style="list-style-type: none"> PA-RISC (64 bit) IPF 	
	11i v3		
Red Hat® Enterprise Linux® AS	2.1	x86	Not applicable
	3.0	<ul style="list-style-type: none"> x86 IPF EM64T 	
	4.0 (Update 1, Update 3)	<ul style="list-style-type: none"> x86 IPF EM64T 	
	4.0 (Update 4)	x86	
Red Hat Enterprise Linux ES	3.0	<ul style="list-style-type: none"> x86 IPF EM64T 	Not applicable
	4.0 (Update 1, Update 3)	<ul style="list-style-type: none"> x86 IPF EM64T 	
	4.0 (Update 4)	x86	
SUSE LINUX Enterprise Server	9.0	x86	Not applicable

¹If Windows Firewall is active, you must add the Device Manager agent as an exception to the Windows Firewall exceptions list. For details on how to do this after installing the agent, see section 3-2-6 .

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

2-1-2 Patches required for operating systems supported by the Device Manager agent

Table 2-2 through Table 2-10 list the OS patches that must be applied in order to use the Device Manager agent in Solaris, AIX, HP-UX, and Red Hat Enterprise Linux OSs. If those patches are not applied, the Device Manager agent might not be able to start. The tables list only the OSs that require patches.

2-1-2-1 Patches required for Solaris 7

The table below lists the patches required to use the Device Manager agent with the Solaris 7 OS.

Table 2-2 Patches required for the Solaris 7 OS

Patch No.	Description
107544-03 SunOS 5.7	/usr/lib/fs/ufs/fsck patch
107834-04 SunOS 5.7	dkio.h & commands.h patch
106541-42 SunOS 5.7	Kernel Update Patch
106980-26 SunOS 5.7	libthread patch
106950-24 SunOS 5.7	Linker Patch
106327-23 SunOS 5.7	32-Bit Shared library patch for C++
108376-46 OpenWindows 3.6.1	Xsun Patch
106300-24 SunOS 5.7	64-Bit Shared library patch for C++
107702-12 CDE 1.3	dtsession patch
108374-07 CDE 1.3	libDtWidget Patch
107656-11 OpenWindows 3.6.1	libXt Patch
107081-57 Motif 1.2.7 and 2.1.1	Runtime library patch for Solaris 7
107226-19 CDE 1.3	dtwm patch
107636-10 SunOS 5.7	X Input & Output Method patch

2-1-2-2 Patches required for Solaris 8

The table below lists the patches required to use the Device Manager agent with the Solaris 8 OS.

Table 2-3 Patches required for the Solaris 8 OS

Patch No.	Description
112003-03 SunOS 5.8	Unable to load fontset in 64-bit Solaris 8 iso-1 or iso-15
111310-01 SunOS 5.8	/usr/lib/libdhcpageant.so.1 patch
112472-01 SunOS 5.8	Font2DTest2 abort when Lucida Sans Thai Typewriter selected
109147-32 SunOS 5.8	linker patch
111308-05 SunOS 5.8	/usr/lib/libmtmalloc.so.1 patch
112438-03 SunOS 5.8	/kernel/drv/random patch
108434-18 SunOS 5.8	32-Bit Shared library patch for C++
108435-18 SunOS 5.8	64-Bit Shared library patch for C++
113886-26 OpenGL 1.3	OpenGL Patch for Solaris (32-bit)
113887-26 OpenGL 1.3	OpenGL Patch for Solaris (64-bit)
111111-04 SunOS 5.8	/usr/bin/nawk patch
112396-02 SunOS 5.8	/usr/bin/fgrep patch
110386-03 SunOS 5.8	RBAC Feature Patch
111023-03 SunOS 5.8	/kernel/fs/mntfs and /kernel/fs/sparcv9/mntfs patch
111317-05 SunOS 5.8	/sbin/init and /usr/sbin/init patch
113648-03 SunOS 5.8	/usr/sbin/mount patch
115827-01 SunOS 5.8	/sbin/sulogin and /sbin/netstrategy patch
116602-01 SunOS 5.8	/sbin/uadmin and /sbin/hostconfig patch
108652-88 X11 6.4.1	Xsun patch
108921-23 CDE 1.4	dtwm patch
108940-68 Motif 1.2.7 and 2.1.1	Runtime library patch for Solaris 8
108773-19 SunOS 5.8	IIIM and X Input & Output Method patch
108987-15 SunOS 5.8	Patch for patchadd and patchrm
108528-29 SunOS 5.8	kernel update and Apache patch
108989-02 SunOS 5.8	/usr/kernel/sys/acctctl and /usr/kernel/sys/exacctsyes patch
108993-40 SunOS 5.8	LDAP2 client, libc, libthread and libnsl libraries patch
109326-16 SunOS 5.8	libresolv.so.2 and in.named patch
110615-13 SunOS 5.8	sendmail patch

2-1-2-3 Patches required for Solaris 9

Table 2-4 lists the patches required to use the Device Manager agent with the Solaris 9 OS.

Table 2-4 Patches required for the Solaris 9 OS

Patch No.	Description
113886-26 OpenGL 1.3	OpenGL Patch for Solaris (32-bit)
113887-26 OpenGL 1.3	OpenGL Patch for Solaris (64-bit)
112963-17 SunOS 5.9	linker patch
113096-03 X11 6.6.1	OWconfig patch
112785-45 X11 6.6.1	Xsun patch

2-1-2-4 Patches required for Solaris 10

Table 2-5 lists the patches required to use the Device Manager agent with the Solaris 10 OS.

Table 2-5 Patches required for the Solaris 10 OS

Patch No.	Description
117461-08 SunOS 5.10	ld Patch
119578-18 SunOS 5.10	FMA Patch
118822-30 SunOS 5.10	kernel Patch

2-1-2-5 Patches required for AIX

Table 2-6 lists the patches required to use the Device Manager agent with the AIX OS

Table 2-6 Patches required for the AIX OS

OS	Patch No.
AIX 5L V5.1 (5100_05 RMP or later)	APAR IY71981
AIX 5L V5.2 (5200_02 RMP or later)	APAR IY71978
AIX 5L V5.3	APAR IY70159
	APAR IY71980

2-1-2-6 Patches required for HP-UX 11.0

Table 2-7 lists the patches required to use the Device Manager agent with the HP-UX 11.0* OS.

Table 2-7 Patches required for the HP-UX 11.0 OS

Patch No.	Description
PHCO_26060 s700_800 11.00	Kernel configuration commands patch
PHCO_26089 s700_800 11.00	libpam and libpam_unix cumulative patch
PHCO_26111 s700_800 11.00	libc cumulative header file patch
PHCO_29959 s700_800 11.00	Pthread library cumulative patch
PHCO_31879 s700_800 11.00	cumulative SAM/ObAM patch
PHCO_27731 s700_800 11.00	libc cumulative patch
PHKL_18543 s700_800 11.00	PM/VM/UFS/async/scsi/io/DMAPI/JFS/perf patch
PHKL_23409 s700_800 11.00	NFS, Large Data Space, kernel memory leak
PHKL_24064 s700_800 11.00	eventport (/dev/poll) pseudo driver
PHKL_26008 s700_800 11.00	pstat patch, long command line storage
PHKL_30073 s700_800 11.00	dyn semphores; big data space; msgmn; msgsnd
PHKL_27207 s700_800 11.00	mmap of a java JAR file on CDROM fails
PHKL_27282 s700_800 11.00	signal cumulative patch
PHKL_28172 s700_800 11.00	kmadmin; autoload; DLKM load; MO; eventport
PHKL_28180 s700_800 11.00	Probe, IDDS, PM, VM, PA-8700, AIO, T600, FS, PDC, CLK
PHKL_29434 s700_800 11.00	POSIX AIO;getdirentries;MVFS;rcp;mmap/IDS;
PHNE_23003 s700_800 11.00	r-commands cumulative patch
PHNE_29473 s700_800 11.00	cumulative ARPA Transport patch
PHNE_29785 s700_800 11.00	ONC/NFS General Release/Performance Patch
PHSS_26559 s700_800 11.00	ld(1) and linker tools cumulative patch
PHSS_30181 s700_800 11.00	Xserver cumulative patch

Table 2-7 Patches required for the HP-UX 11.0 OS

Patch No.	Description
PHSS_26945 s700_800 11.X	HP aC++ -AA runtime libraries (aCC A.03.37)
PHSS_26972 s700_800 11.00	Japanese TrueType fonts patch
PHSS_27869 s700_800 11.00	CDE Runtime Periodic Patch
PHSS_30260 s700_800 11.00	X/Motif 32bit Runtime Periodic Patch
PHSS_28368 s700_800 11.00	X/Motif 64bit Runtime Periodic Patch
PHSS_28469 s700_800 11.00	X Font Server Patch

¹PHCO_29108 must not be applied, because it can cause applications to hang. If this patch is already installed, apply PHCO_29959.

2-1-2-7 Patches required for HP-UX 11i

Table 2-8 lists the patches required to use Device Manager agent with the HP-UX 11i^{1,2} OS

Table 2-8 Patches Required for the HP-UX 11i OS

Patch No.	Description
PHCO_24402 s700_800 11.11	libc cumulative header file patch
PHCO_26061 s700_800 11.11	Kernel configuration commands patch
PHCO_29960 s700_800 11.11	Pthread enhancement and fixes
PHCO_27740 s700_800 11.11	libc cumulative patch
PHCO_27958 s700_800 11.11	mountall cumulative patch, Dev IDs enabler
PHKL_24751 s700_800 11.11	preserve IPSW W-bit and GR31 lower bits
PHKL_25233 s700_800 11.11	select(2) and poll(2) hang
PHKL_25468 s700_800 11.11	eventport (/dev/poll) pseudo driver
PHKL_25993 s700_800 11.11	thread noston for NFS, rlimit, Ufalloc fix
PHKL_25994 s700_800 11.11	Thread NOSTOP, Psets Enablement, Ufalloc
PHKL_27091 s700_800 11.11	Core PM, vPar, Psets Cumulative, slpq1 perf
PHKL_27094 s700_800 11.11	Psets Enablement Patch, slpq1 perf
PHKL_27096 s700_800 11.11	VxVM,EMC,Psets&vPar,slpq1,earlyKRS
PHKL_27316 s700_800 11.11	Shared synchronization performance support
PHKL_27317 s700_800 11.11	detach; NOSTOP, Abort; Psets; slpq1 perf
PHKL_27686 s700_800 11.11	MO 4k sector size;FIFO;Event Port;perf;shmem
PHKL_28122 s700_800 11.11	signals, threads enhancement, Psets Enablement
PHKL_26233 s700_800 11.11	VM-JFS ddlock, mmap, thread perf, user limits
PHNE_29887 s700_800 11.11	cumulative ARPA Transport patch
PHNE_29783 s700_800 11.11	ONC/NFS General Release/Performance Patch
PHSS_26560 s700_800 11.11	ld(1) and linker tools cumulative patch
PHSS_26971 s700_800 11.11	Japanese TrueType font patch
PHSS_28370 s700_800 11.11	X/Motif Runtime Periodic Patch
PHSS_28470 s700_800 11.11	X Font Server Patch
PHSS_24638 s700_800 11.11	HP aC++ -AA runtime libraries (aCC A.03.33)
PHSS_29964 s700_800 11.11	HP DCE/9000 1.8 DCE Client IPv6 patch

¹Do not apply PHCO_29109:This patch can cause a applications to hang. If this patch is already installed, apply PHCO_29960.

²Do not apply PHKL_28267. This patch can cause a system panic. If this patch is already installed, delete PHKL_28267 and then apply PHKL_26233 instead.

2-1-2-8 Patches required for HP-UX 11i.v2

Table 2-9 lists the patches required to use Device Manager agent with the HP-UX 11i.v2 OS.

Table 2-9 Patches Required for HP-UX 11i.v2 OS

OS	Patch No.	Description
HP-UX 11i v2 (PA-RISC)	PHKL_31500 s700_800 11.23	Sept04 base patch*
HP-UX 11i v2 (IPF)	PHKL_31500 s700_800 11.23	Sept04 base patch*
	PHKL_32264 s700_800 11.23	mmap(2) MAP_NORESERVE signal correction
	PHSS_30231 s700_800 11.23	Integrity aC++ Runtime (A.05.56)
	PHSS_30232 s700_800 11.23	Integrity Unwind Library
	PHSS_32765 s700_800 11.23	linker + fdp cumulative patch

*Do not install PHKL_31500 alone. Instead, apply HP-UX 11i v2 (B.11.23) released in September 2004, which includes this patch. However, if this patch contains a warning patch, apply the related patch that addresses the problem.

2-1-2-9 Patches required for Red Hat Enterprise Linux

Table 2-10 lists the patches required to use Device Manager agent with the Red Hat Enterprise Linux OSs.

Table 2-10 Patches required for the Red Hat Enterprise Linux OSs

OS	Patch No.
Red Hat Enterprise Linux AS/ES 3.0	gdb-5.3.90-0.20030710.40.i386.rpm
Red Hat Enterprise Linux AS3 (IPF)	gdb-5.3.90-0.20030710.40.ia64.rpm

2-1-3 Java Runtime Environment supplied with the Device Manager agent

The Device Manager agent is shipped with the J2SE Java Runtime Environment (JRE) 1.4. During installation of the Device Manager agent, the JRE is automatically installed in the installation directory of the Device Manager agent.

2-1-4 Device Manager server versions supported by the Device Manager agent

A Device Manager server v5.6 or later can be used with the Device Manager agent. Even if the version of the Device Manager server is newer than the version of the Device Manager agent, you will be able to use the functions supported by the installed version of the Device Manager agent.

2-2 File systems supported by the Device Manager agent

Table 2-11 lists, by OS, the file systems supported by the Device Manager agent.

Table 2-11 File systems supported by the Device Manager agent

OS	File System
Windows 2000	• NTFS
Windows Server 2003	• FAT
Windows Server 2003 x64 Edition	• FAT32
Windows Server 2003 R2	
Solaris	• VERITAS File System • UFS
AIX	JFS
HP-UX	• HFS • VERITAS File System (JFS)
Red Hat Enterprise Linux AS 2.1	• ext2

Table 2-11 File systems supported by the Device Manager agent

OS	File System
Red Hat Enterprise Linux AS/ES 3.0	• ext3
Red Hat Enterprise Linux AS/ES 4.0	
SUSE LINUX Enterprise Server 9	

2-3 Storage subsystems supported by Device Manager agent

The following disk array models are supported by the Device Manager agent:

- XP10000
- XP12000
- SVS200
- XP48
- XP128
- XP512
- XP1024

All HBA models supported by the disk array are available.



IMPORTANT: If an HP XP Disk Array 512/48 is connected to a Linux host via fiber, they must be in a one-to-one relationship.

2-4 Requirements for obtaining host WWN information

You might not be able to obtain host WWN information when one of the following conditions is satisfied:

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

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 2-12 HBA models required to obtain host WWN information

OS	Model Name
Windows	Emulex LP8000
	Emulex LP9002DC
	Emulex LP9002L
	Emulex LP9802
	QLogic QLA23xx ¹
Solaris ²	JNI FCI-1063
	JNI FC64-1063
	JNI FCE-6410
	JNI FCE-6460
	QLogic QLA2200
AIX	IBM6227
	IBM6228
HP-UX	HP A3404A

Table 2-12 HBA models required to obtain host WWN information

OS	Model Name
	HP A3591B
	HP A3636A
	HP A3740A
	HP A5158A
	HP A6684A
	HP A6685A
	HP A6795A
	HP A6826A
	HP A9784A
Linux	QLogic QLA2200F
¹ In order to use a QLogic HBA, download and then install the Fibre Channel Information Tool (fcinfo) x86 version from the Microsoft web site. Even if the OS of a host machine 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.	

2-5 Requirements for using FC-HUB (FC-SWITCH)

Before connecting a host with disk arrays via FC-HUB (or FC-SWITCH), confirm whether FC-HUB (or FC-SWITCH) and its firmware are available for the disk array:

- Depending on the storage subsystem, see section 2-4 and check the corresponding HBA.
- Check the FC-HUB and related firmware supported by the target disk arrays.

For more information, see the documentation for your disk array.

2-6 When IPv6 is enabled on the host

When the IPv6 function is enabled, the Device Manager agent cannot start. Disable IPv6. For details on how to do this, see the OS documentation.

2-7 Volume managers supported by the Device Manager agent

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

Table 2-13 Volume managers supported by the Device Manager agent

OS	OS Version or Architecture	Volume Manager
Windows 2000 SP4	--	<ul style="list-style-type: none"> • Basic • Dynamic • VERITAS Volume Manager 2.7, 3.0 and 3.5
Windows Server 2003 without SP	--	<ul style="list-style-type: none"> • Basic • Dynamic
Windows Server 2003 SP1	x86	<ul style="list-style-type: none"> • Basic • Dynamic • VERITAS Volume Manager 4.3
	IPF	<ul style="list-style-type: none"> • Basic • Dynamic
Windows Server 2003 X64 Edition	--	<ul style="list-style-type: none"> • Basic • Dynamic
Windows Server 2003 R2	--	<ul style="list-style-type: none"> • Basic • Dynamic

Table 2-13 Volume managers supported by the Device Manager agent

OS	OS Version or Architecture	Volume Manager
Solaris	7	VERITAS Volume Manager 3.2
	8	<ul style="list-style-type: none"> • SDS 4.2.1 • VERITAS Volume Manager 3.2, 3.5 and 4.0
	9	<ul style="list-style-type: none"> • SVM 1.0 • VERITAS Volume Manager 3.5, 4.0 and 4.1 • Veritas Volume Manager 5.0 ¹
	10	<ul style="list-style-type: none"> • SVM 1.0 • Veritas Volume Manager 5.0 ¹
AIX	--	LVM
HP-UX	11.0	LVM
	11i v1	<ul style="list-style-type: none"> • LVM • VERITAS Volume Manager 3.5
	11i v2	<ul style="list-style-type: none"> • LVM • VERITAS Volume Manager 3.5 and 4.1
Linux	Red Hat Enterprise Linux AS2.1	LVM 1.0.1 rc4
	Red Hat Enterprise Linux AS/ES 3.0	LVM
	Red Hat Enterprise Linux AS/ES4.0	LVM2
	SUSE LINUX Enterprise Server 9	LVM2

NOTE: ¹ Veritas Volume Manager 5.0 is included in Veritas Storage Foundation.

2-8 Cluster software supported by the Device Manager agent

The Device Manager agent runs in cluster environments configured with the cluster software listed in [Table 2-14](#). The Device Manager agent runs in both Active-Standby and Active-Active configurations. The table lists only OSs that support cluster software.



NOTE: The the Device Manager agent is incompatible with the logical host and cannot be registered in cluster resources. It is activated instead on the physical hosts that make up the cluster, and it then collects the data for those hosts.

Table 2-14 Cluster software supported by the Device Manager agent

OS	Supported Cluster Software	Remarks
Windows 2000 SP4	<ul style="list-style-type: none"> • Microsoft Cluster Server (MSCS) 	Only Windows 2000 with service pack (SP)4 supports MSCS
Windows Server 2003	<ul style="list-style-type: none"> • MSCS • VERITAS Cluster Server (VCS) 4.1 • VCS 4.3 (Only supports Windows Server 2003 x86 version with SP1) 	Only x86 version without SP supports VCS 4.1 x86 version with SP1 supports VCS 4.1 and VCS 4.3
Windows Server 2003 x64 Edition	<ul style="list-style-type: none"> • MSCS 	
Windows Server 2003 R2	<ul style="list-style-type: none"> • MSCS 	
Solaris 7	<ul style="list-style-type: none"> • VCS 1.3 and 2.0 	
Solaris 8	<ul style="list-style-type: none"> • Sun Cluster 3.0 and 3.1 • VCS 1.3, 2.0 and 3.5 	

Table 2-14 Cluster software supported by the Device Manager agent

OS	Supported Cluster Software	Remarks
Solaris 9	<ul style="list-style-type: none"> • Sun Cluster 3.1 • VCS 3.5, 4.0 and 4.1 • Cluster Perfect 4.1 	
Solaris 10	<ul style="list-style-type: none"> • VCS 4.1 	
AIX 5.1	<ul style="list-style-type: none"> • HACMP 4.4.1, 4.5 and 5.1 	
AIX 5.2	<ul style="list-style-type: none"> • HACMP 5.1 	
AIX 5.3	<ul style="list-style-type: none"> • HACMP 5.2 • HACMP 5.3 (Only supports AIX 5.3 64 bit version) 	
HP-UX 11i v1	<ul style="list-style-type: none"> • MC/Service Guard 11.15 (Only supports HP-UX 11i v1 64 bit version) • Serviceguard 11.16 	64 bit version supports MC/Service Guard 11.15 as well
HP-UX 11i v2	<ul style="list-style-type: none"> • Serviceguard 11.16 and 11.17 	
Red Hat Enterprise Linux AS 2.1 (x86)	<ul style="list-style-type: none"> • VCS 2.2 	Only supports x86 version
Red Hat Enterprise Linux AS/ES 4.0 Update 1 (x86)	<ul style="list-style-type: none"> • VCS 4.1 	

2-9 Path management software supported by the Device Manager agent

Path management software supported by the Device Manager agent is listed in the following table. The table lists only the OSs that support path management software.

Table 2-15 Path management software supported by the Device Manager agent

OS	Architecture	Path Management Software Name	Path Management Software Version
Windows Server 2003 SP1	--	Windows MPIO (MPIO DSM: HP MPIO DSM v1.00)	Versions supported by DSM described to the left
Windows Server 2003 x64 Edition	--	Windows MPIO (MPIO DSM: HP MPIO DSM v1.00)	Versions supported by DSM described to the left
Windows Server 2003 R2	--	Windows MPIO (MPIO DSM: HP MPIO DSM v1.00)	Versions supported by DSM described to the left
Solaris 7 and 8	--	Hitachi Dynamic Link Manager	05-00 or later
Solaris 9	--	VERITAS Volume Manager (Dynamic Multi-Pathing)	4.1
		Hitachi Dynamic Link Manager	05-00 or later
		Sun StorEdge Traffic Manager	6.2.6
Solaris 10	--	Hitachi Dynamic Link Manager	5.6.1 or later
		Sun StorEdge Traffic Manager	--
AIX 5.1	--	Hitachi Dynamic Link Manager	04-00 or later
AIX 5.2	--	Hitachi Dynamic Link Manager	05-00 or later
		MPIO	--
AIX 5.3	--	Hitachi Dynamic Link Manager	5.4.1 or later

Table 2-15 Path management software supported by the Device Manager agent

OS	Architecture	Path Management Software Name	Path Management Software Version
		MPIO	-
HP-UX 11.0	-	PV-link	-
HP-UX 11i v1	-	PV-link	-
HP-UX 11i	PA-RISC (64 bit) and IPF	PV-link	-
HP-UX 11i v3	PA-RISC (64 bit) and IPF	PV-link	-
		MPIO	-

2-10 Installing the Device Manager agent

This section describes how to install the Device Manager agent for each supported program (Windows, Solaris, AIX, HP-UX, and Linux). The section includes the following topics:

- Installing the Device Manager agent on a Windows system, section [2-10-1](#)
- Installing the Device Manager agent on a Solaris system, see section [2-10-2](#)
- Installing the Device Manager agent on an AIX system, see section [2-10-2](#)
- Installing the Device Manager agent on an HP-UX system, see section [2-10-2](#)
- Installing the Device Manager agent on a Linux system, see section [2-10-2](#)

When you install the Device Manager agent for the first time, the default installation location is as follows.

In Windows:

- On a 32-bit (x86) Windows system, the default installation location is:
`system-drive\Program Files\HDVM\HBaseAgent`
- On a 64-bit Windows system (IPF, EM64T or AMD64), the default installation location is:
`system-drive\Program Files (x86)\HDVM\HBaseAgent`

In Solaris, HP-UX, or Linux, the default installation location is:

```
/opt/HDVM/HBaseAgent
```

In AIX, the default installation location is:

```
/usr/HDVM/HBaseAgent
```

CAUTION: When the installation destination is a Windows system, and if Hitachi Dynamic Link Manager (version 5.8 or later) or Device Manager agent (version 1.1 or earlier) is already installed in the Windows system, the installation destination folders for the Device Manager agent are determined in the order shown below.

- 1 If Hitachi Dynamic Link Manager version 5.8 or later has already been installed, the Device Manager agent is installed on the drive that contains Hitachi Dynamic Link Manager.
- 2 If Device Manager agent version 1.1 or earlier has already been installed, the Device Manager agent is installed in the following location:
`installation-folder-for-an-older-version-of-Device-Manager-agent\HBaseAgent`

If the Device Manager agent version 1.1 or earlier has already been installed, the Device Manager agent is installed by overwriting the folder in which the existing Device Manager agent software is installed.

If the Device Manager agent has already been installed, check the version of the installed Device Manager agent by executing the following command:

In Windows:

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

In Solaris, HP-UX or Linux:

```
# /opt/HDVM/HBaseAgent/bin/hdvm_info
```

In AIX:

```
# /usr/HDVM/HBaseAgent/bin/hdvm_info
```

CAUTION: Do not execute any of the following commands during an upgrade installation of the Device Manager agent. Also, do not install the Device Manager agent while the following commands are executing: `hbsasrv`, `HiScan`, `hdvmagt_account`, `hdvmagt_schedule`, `hlautil`, `TIC` (Trouble Information Collector), `hdvmagt`, or `stop_hdvmagt`

If you execute these commands during installation, the upgrade installation can end abnormally. Be sure to restart the system after installation.

CAUTION: If a version of Hitachi Dynamic Link Manager earlier than 5.8 is installed, you must install the Device Manager agent, and then set the port number used by the Device Manager agent. For details, see subsection [3-2-10](#).

NOTE: Make sure beforehand that there is enough space in the default directory for installing the Device Manager agent.

NOTE: The Device Manager agent can be downloaded from the Device Manager server using the web client. Decompress the downloaded file and then install the decompressed files. For details on the downloading, see the *HP StorageWorks Command View XP Advanced Edition software Device Manager web client user guide*.

2-10-1 Installing the Device Manager agent on a Windows system

This section contains the following topics:

- New installation in Windows see section [2-10-1-1](#)
Use this method to install the Device Manager agent on a host where it does not already exist.
- Upgrade installation in Windows, see section [2-10-1-2 \(updating an earlier version\)](#)
Perform this to upgrade the Device Manager agent on a host that already contains a version earlier than 5.6.
- Reinstallation in Windows, see section [2-10-1-3 \(installation for restoration\)](#)
Use this method to install the Device Manager agent on a host that already contains the Device Manager agent version 5.6.

Before installing the Device Manager agent in a Windows system:

- See [Table 2-1](#) for supported operating systems and a list of required programs for your operating system.
- Make sure beforehand that there is enough space in the default directory to install the Device Manager agent.
- You must be a member of the Administrator group.
- At least 70 MB of free space is required on the hard disk. An additional 70 MB of free space is required on the system drive to create temporary files during installation.
- If the Device Manager agent version 5.6 has already been installed, do not perform an overwrite installation with an earlier version. To install an earlier version, make sure to uninstall the existing version first.
- Before starting the installation of the Device Manager agent, cancel any programs that may be running.
- If you log in to Windows from a remote console and install the Device Manager agent after logging in, you must use Terminal Service Client.
- 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 has not been installed.
 - The host recognizes many LUs (guideline value is 100 or more).

To avoid the above problems, HP recommends that you install Service Pack 1, 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.

NOTE: If 100 or more LUs are recognized by the host, another error might occur. See section [3-2-14](#), and change the settings for the Device Manager agent.

If you install a Service Pack after installing the Device Manager agent version 5.6, reinstall (overwrite) the Device Manager agent version 5.6.

- When installing the Device Manager agent on a host in which Windows Server 2003 was installed in the following order, you cannot add the Device Manager agent to the Windows Firewall exceptions list during the installation.
 1. Install Windows Server 2003 (no Service Pack).
 2. Install Service Pack 1.

For such hosts, manually add the Device Manager agent to the Windows Firewall exceptions list after installing it. For details on how to do this, see subsection [3-2-6](#) .

When you install the Device Manager agent on a host on which Windows Server 2003 with Service Pack 1 was installed, you can add the Device Manager agent to the Windows Firewall exceptions list during the installation.

2-10-1-1 New installation in Windows

To install the Device Manager agent:

1. Log on to Windows using a User ID in the Administrators Group.
2. Insert the Device Manager agent CD-ROM.
3. Select **Start, Run, Browse**, and then select and execute `install.exe` in the `\Agent\Windows` folder of the CD-ROM.

Installation of the Device Manager agent starts, and the Welcome to the InstallShield Wizard for Device Manager - Agent dialog box is displayed.

4. Select **Next**.
The Agent License Agreement window appears.
5. Select **Yes**.
The Choose Destination Location window appears. Specify or select the folder in which you want to install the Device Manager agent.



NOTE:

If the Device Manager or the version 5.8 or later of Hitachi Dynamic Link Manager has already been installed, this window does not appear.

You can use `a-z` `A-Z` `0-9` `.` `_` `()` and spaces for the path name. Do not use a space at the beginning or end of a path name, and do not use two or more space characters consecutively.

6. Select **Next**.
If the target OS is Windows Server 2003 SP1 or Windows Server 2003 x64 Edition, a confirmation message appears, asking whether you want to add the Device Manager agent as an exception to the Windows Firewall exception list.
7. Select **Yes**, then select **Next**.
The Start Copying Files window appears.





NOTE: If you select the **Next** button in this panel, you cannot cancel the installation of the Device Manager agent.

8. Select **Next** to continue.
The software is installed and the Setup Status window appears.

In Windows 2000 or Windows Server 2003 (32-bit processor version), the Installing Add-on panel appears. Add-on functionality is installed together with the Device Manager agent. Upon completion of the installation process, the Install Complete window appears.
9. Select **OK**, and then check the `system-drive` folder:
 - If the `system-drive_HDVMAgent0560_Install_tmp_` file remains, delete it manually (it is a temporary file created during installation).
 - If the file cannot be deleted, log on to Windows again to delete it

After the installation successfully finishes, set up the Device Manager agent. For details about how to set it up, see section [2-11](#) .

 **NOTE:** When you install version 5.6 of the Device Manager agent, the folder in which commands are installed is automatically added to the environment variable `PATH`. Therefore, when you execute a command, you do not need to change the current folder to the folder that contains commands. After installing the Device Manager agent, you will have to log off and log on again to Windows for the changes in the environment variable `PATH` to be applied.

 **CAUTION:** If VxVM is installed, specify the version of the installed VxVM in the `programproductinfo.properties` file. For details about the setting, see subsection [3-7-3](#) .

2-10-1-2 Upgrade installation in Windows

To perform an upgrade **in Windows**:

1. Log on to Windows using an Administrators-group user ID.
2. Insert the Device Manager agent CD-ROM.
3. Select **Start**, **Run**, and **Browse**, and then select and execute `install.exe` in the `\Agent\Windows` folder of the CD-ROM.

A confirmation message appears, asking whether you want to continue the upgrade.


4. Select **Yes**.


A window displays the message that add-on modules are being installed.


Add-on functionality is installed together with the Device Manager agent. Upon completion of the installation process, an Install Complete window appears.

5. Select **OK**.


6. Check the `system-drive` folder. If `system-drive_HDVMAgent0560_Install_tmp_file` (a temporary file created during installation) remains, delete it manually. If it cannot be deleted, log on to Windows again to delete it.

 **NOTE:** In upgrade (overwrite) installations, predefined settings for Device Manager server information and the execution period of the HiScan command are inherited. To modify information about the Device Manager server, see section [3-4](#) . For details about how to change the execution period, see section [3-5](#) .

 **NOTE:** When you install version 5.6 of the Device Manager agent, the folder in which commands are installed is automatically added to the environment variable `PATH`. Therefore, when you execute a command, you do not need to change the current folder to the folder that contains commands. After installing the Device Manager agent, you will have to log off and then log on again to Windows for the changes in the environment variable `PATH` to be applied.

 **CAUTION:** If VxVM is installed, specify the version of the installed VxVM in the `programproductinfo.properties` file. For details about the setting, see subsection [3-7-3](#) .

2-10-1-3 Reinstallation in Windows

 **CAUTION:** When reinstalling the Device Manager agent, do not execute the following commands during installation: `HiScan`, `hdvmagt_account`, `hdvmagt_schedule`, `hbsasrv start`, and `TIC`. If you execute any of these commands, the reinstallation may not complete properly. In this case, retry the reinstallation.

To reinstall Device Manager agent in Windows:

1. Log on to Windows using a user ID in the Administrators group.
2. Insert the Device Manager agent CD-ROM.
3. From the **Start** menu, select **Run** and then **Browse**. Execute `install.exe` in the `\Agent\Windows\` folder on the CD-ROM.

The Welcome: Modify, Repair, or Remove the Program window appears.

4. Select **Repair**, and then **Next**.

A window appears, confirming the reinstallation.

5. Select **OK**.

A window appears, indicating that add-on modules are being installed.

Add-on functionality is installed. Upon completion of the installation process, an Install Complete window appears.

6. Select **OK**.
7. Check the system-drive folder. If the `system-drive_HDVMAgent0560_Install_tmp_` remains, delete it manually; it is a temporary folder created during installation.
If the folder cannot be deleted, log on to Windows again to delete it.

⚠ CAUTION: If VxVM is installed, specify the version of the installed VxVM in the `programproductinfo.properties` file. For details about the setting, see section 3-7-3 .

2-10-2 Installing Device Manager agent on Solaris, AIX, HP-UX®, or Linux

This subsection explains how to install Device Manager agent on a Solaris, AIX, HP-UX, or Linux system.

Installation requirements

The requirements for installing Device Manager agent on a Solaris, AIX, HP-UX, or Linux system are as follows.

- You must log in with `root` permissions.
- The hard disk has the amount of free space shown in the following table.

Table 2-16 Minimum free hard disk space needed for installation

OS name	Amount of hard disk free space (Unit: MB)
Solaris	100
AIX	120
HP-UX	220
Linux	140

Installation directory

When you install the Device Manager agent for the first time, the default installation location is as follows:

In Solaris, HP-UX, or Linux:

`/opt/HDVM/HBaseAgent`

In AIX:

`/usr/HDVM/HBaseAgent`

2-10-2-1 Preparing for installation

Before starting the installation of the Device Manager agent, cancel any programs that are running. Also, keep the following in mind.

Notes about symbolic link

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, HP-UX, or Linux:

- `/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

Precautions for installation on Solaris 10

- When installing the Device Manager agent, do not specify the system's zone settings. If you do this, installation might fail.
- When a Device Manager agent version earlier than 5.6 is installed in an environment where the local zone is set, it will be installed in both the global zone and the local zone. In this environment, if you perform an upgrade installation of Device Manager agent version 5.6, only the Device Manager agent in the global zone will be upgraded. Log in to the local zone to execute the following command, and then delete the Device Manager agent in the local zone.

```
# pkgrm HDVMAgent
```

Precautions for installation on HP-UX

- 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 Device Manager agent, make sure that the network settings such as those in the `hosts` file are correct.

Precautions for installation on 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 *HP StorageWorks Command View XP Advanced Edition software Device Manager server installation and configuration guide*.

Precautions for overwrite installation

If Device Manager agent version 5.6 has already been installed, do not perform an overwrite installation with an earlier version. To install an earlier version, make sure to uninstall the existing version first.

2-10-2-2 Installation procedures

To install the Device Manager agent:

1. 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`.

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

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

Executing `install.sh` starts installation of the Device Manager agent (Installation of add-on functionality is also performed).


3. At this point, software licensing agreement information will appear. If you do not accept the licensing agreement, uninstall the Device Manager agent after installation finishes.
4. The following message appears when installation finishes:

```
Device Manager - Agent installed successfully.
```

5. When performing a new installation of the Device Manager agent, the following message appears, prompting you to execute the `hdvmagt_account` command and the `hdvmagt_schedule` command.

```
Please execute hdvmagt_account command and hdvmagt_schedule command to setup Device Manager - Agent.
```


```
Execute the hdvmagt_account command and the hdvmagt_schedule command, and then set up the Device Manager agent. For details on this procedure, see section 2-11 .
```

 **NOTE:** For upgrade (overwrite) installations, predefined settings for Device Manager server information and the execution period of the `HiScan` command are inherited. To modify information about the Device Manager server, see section 3-4 . For details about how to change the execution period, see section 3-5 .

2-11 Setting up the Device Manager agent


After the installation of the Device Manager agent finishes, you must set the operational parameters for the Device Manager agent. Refer to the following sections for further information:

- Setting server information, see section 2-11-1
- Setting the execution period of the `HiScan` command, see section 2-11-2

 **NOTE:** You can set any execution period for the `HiScan` command. If you do not set up the execution period, the Device Manager server is not periodically notified of information acquired by the Device Manager agent.

2-11-1 Setting server information

Set the IP address or host name, port number, user ID, and password of the Device Manager server interactively using the `hdvmagt_account` command.

 **CAUTION:** Before starting to set the server information, be sure the values you are planning to input are valid. Operations will end abnormally if you enter three consecutive invalid values.

To set the server information:

1. From the command prompt, execute the `hdvmagt_account` command.
The `hdvmagt_account` command is stored in the following location:
 - In Windows:
`installation-folder-for-Device-Manager-agent\bin\hdvmagt_account.bat`
 - In Solaris, HP-UX, or Linux:
`/opt/HDVM/HBaseAgent/bin/hdvmagt_account`
 - In AIX:
`/usr/HDVM/HBaseAgent/bin/hdvmagt_account`
2. A message asks whether to change the Device Manager server information. Type `y`.
 - Would you like to change the Device Manager Server information? (Y)es or (N)o. (default:N)
3. The following message prompts you to enter the IP address or host name of the Device Manager server. Enter the IP address (in the `xxx.xxx.xxx.xxx` format) or host name.

- Enter the IP address or host name of the Device Manager Server. (default: 255.255.255.255)

If you do not enter a value and press the **Enter** key, the default IP address 255.255.255.255 is set.



NOTE: To specify a host name, use a character string of 50 bytes or less. You can use the following characters: 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.

4. The following message prompts you to enter the port number of the Device Manager server. Enter the port number. The default value is 2001:

- Enter the port for the Device Manager Server. (default:2001)

If you do not enter a value and press the **Enter** key, the default port number 2001 is set. If the entered value is invalid, you will be prompted to re-enter it.

5. The following message prompts you to enter the user ID for logging on to the Device Manager server. Enter the user ID:

- Enter the Device Manager Server user ID.

The default user ID is HaUser.

Specification of the user ID

You can use a character string of 1 to 256 bytes to specify a user ID. The following characters can be used:

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

If you do not enter anything or enter an invalid character and press the **Enter** key, you will be prompted to re-enter the user ID.

6. The following message prompts you to enter the password for logging on to the Device Manager server. Enter the password:

- Enter the Device Manager Server password.

The default password for the HaUser user ID is haset. When you have changed the password for HaUser by using web client, use the new password.

Specification of the password

You can use a character string of 1 to 256 bytes to specify a password. The following characters can be used:

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

If you do not enter anything or enter an invalid character and press the **Enter** key, you will be prompted to re-enter the password.



IMPORTANT: For security reasons, HP recommends always using this procedure when changing the password in Device Manager agent.

7. A message is displayed confirming whether the settings are to be saved. Type y:
 - Would you like to save to server.properties? (Y)es or (N)o. (default:N)



IMPORTANT: For Windows, be sure you restart the Device Manager agent service after executing the `hdvmagt_account` command. For details on starting and stopping the Device Manager agent, see section 3-3 .

2-11-2 Setting the execution period for the HiScan command

You must set the execution period for notifying the Device Manager server of the information obtained by the Device Manager agent. In a new installation, the information obtained by the Device Manager agent is not sent regularly to the Device Manager server unless you set the execution period for the HiScan Command.

Precautions when the host operating system is Linux:

These precautions apply to the following versions:

- Linux AS 2.1

- Versions earlier than Linux AS 3.0 Update 6
- Versions earlier than Linux ES 3.0 Update 6

Do not set the execution period of the `HiScan` command. If the execution period of the `HiScan` command is set, clear the setting. For details about how to clear this setting, see subsection [3-6-4](#) .

If system operation requires that the `HiScan` command be executed automatically, do not perform any operations on the host while the `HiScan` command is automatically executing.

To set the execution period:

1. Execute the `hdvmagt_schedule` command from the command prompt.

The `hdvmagt_schedule` command is stored in the following location:

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

2. A message asks whether to change the execution period. Type `y` or `n`:

If the schedule for performing automatic execution is already registered, the registered contents are also displayed.

- Do you want to set the execution period of the HiScan command? (Y)es or (N)o. (default:N)

3. A message prompts you to specify the execution period. Enter `h` for automatic hourly execution, `d` for automatic daily execution, or `w` for automatic weekly execution. If you do not want to perform automatic execution (or if you want to cancel the set automatic execution), enter `c`.

- Enter execution period: (H)ourly, (D)aily, (W)eekly or (C)lear (default:D)

When you enter a character other than `c`, go to the next step.

When you enter `c`, the message "This program removes all of current HiScan automatic execution schedule. Are you sure? (Y)es or (N)o. (default:N)" is displayed. Also, the registered contents are displayed. When you enter `y`, the message "Configuration of the HiScan automatic execution schedule is completed." appears, and then the setting of the execution period finishes.

4. If you enter `w` for Step 3, the following message prompts you to specify the day of the week when automatic execution is performed. Specify the day of the week.

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

5. If you specify the day of the week for Step 4, or enter `h` or `d` for Step 3, the following message prompts you to specify when automatic execution is performed. To accept the default time, enter `y`. If you want to specify the time for automatic execution, enter `n`.

When you specify the day of the week or enter `d`:

- Do you want to set the default time (2:47) to the execution time? (Y)es or (N)o. (default:N)

When you enter `h`:

- Do you want to set the default time (*:47) to the execution time? (Y)es or (N)o. (default:N)

The default automatic execution times are as follows:

- For hourly execution: 47th minute of every hour
- For daily or weekly execution: 2:47

When you enter `n`, the following message appears; specify the execution time.

Enter time(hour) : (0-23)

Enter time(minute) : (0-59)

6. A message asks you whether you want to apply the settings. Enter `y` or `n`.

The new settings are also displayed along with the message.

When setting the execution period for the first time:

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

When updating the execution period:

- This program updates all of current HiScan automatic execution schedule. Are you sure? (Y)es or (N)o. (default:N)

7. When you enter *y*, the following message appears, and the setting of the execution period finishes.
 - Configuration of the HiScan automatic execution schedule is completed.
8. For Windows, start the Device Manager agent service.

For details about how to start the service of the Device Manager agent, see section 3-3 .

For details about how to change the execution period of the HiScan command, see section 3-5 .

Precautions when installing Device Manager agent on multiple hosts

⚠ CAUTION: When the Device Manager agent is installed on multiple hosts, set the HiScan command to execute daily or weekly at different start times for each host so that the command will not be executed simultaneously from multiple hosts. When changing a start time, make sure that you set a time that does not overlap the HiScan command execution period (command start time to end time) set for any other hosts.

To check the HiScan command execution period refer to the following messages output to the HiScan.log file:

- KAIC22805-I (output when the HiScan command starts.)
- KAIC22804-I (output when the HiScan command ends.)

The HiScan.log file is stored in the following location:

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

2-12 Uninstalling the Device Manager agent

This section contains the procedure for uninstalling the Device Manager agent.

-
- 📝 NOTE:** When uninstalling the Device Manager agent, the Device Manager agent and add-on modules stop automatically. If attempts to stop fail, see subsection 3-3-5 .
 - 📝 NOTE:** You cannot perform uninstallation while the Device Manager agent is processing a job. Wait until the Device Manager agent completes the job, and then uninstall again.
 - 📝 NOTE:** Do not execute any of the following commands during the uninstallation. Also, do not uninstall while the following commands are executing: *hbsasrv*, *HiScan*, *hdvmagt_account*, *hdvmagt_schedule*, *hldutil*, or *TIC*
 - 📝 NOTE:** If you execute the above commands during uninstallation, uninstallation might fail.
 - 📝 NOTE:** If you attempt to uninstall while the HiScan command is executing, uninstallation will stop. So wait for the execution to finish, and then uninstall again.
 - 📝 NOTE:** If you attempt to uninstall while a command other than HiScan is executing, the uninstallation might end abnormally. In such a case, reboot the system.
 - 📝 NOTE:** If Hitachi Dynamic Link Manager version 5.8 or later has been installed, some folders, files, and detailed information will not be deleted even if the Device Manager agent is uninstalled. However, these folders, files, and detailed information will be deleted when Hitachi Dynamic Link Manager is uninstalled.
 - 📝 NOTE:** Files created by using HiScan, RAID Manager XP configuration definition files, and error information files created from the results of TIC commands cannot be deleted.
-

2-12-1 Uninstalling the Device Manager agent on Windows systems

The procedures for uninstalling the Device Manager agent and deleting tasks that run the HiScan command in Windows are described in this section.



NOTE: Once uninstallation is started, you cannot use the **Cancel** button to stop the processing. After the uninstallation finishes, install the Device Manager agent again.



NOTE: If the Device Manager agent is registered in the Windows Firewall exceptions list, you must release the Windows Firewall settings after uninstalling the Device Manager agent. For details on how to release these settings, see step 3 of subsection [3-2-6](#).

2-12-1-1 Uninstalling the Device Manager agent in Windows

To uninstall the Device Manager agent in Windows:

1. Select **Start, Settings, Control Panel, and Add/Remove Programs**.
2. Click the **Change/Remove** button for the Device Manager agent.
The Device Manager agent Maintenance menu opens
3. Select **Remove**.



NOTE: Although both Repair and Remove are selectable in the maintenance menu, do not select **Repair**. When reinstalling the Device Manager agent, follow the procedures described in the procedure for reinstalling the Device Manager agent in Windows, in subsection [2-10-1](#).

2-12-1-2 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. Delete these tasks from Scheduled Tasks in the Control Panel.

- Tasks that execute `exeHiScan.bat` if the task schedule was modified by a user using Scheduled Tasks in the Control Panel
- Tasks that execute `exeHiScan.bat` in Windows Server 2003 or Windows Server 2003 x64 Edition

2-12-2 Uninstalling the Device Manager agent in Solaris, AIX, HP-UX, and Linux

This subsection describes how to uninstall the Device Manager agent.



CAUTION: When the host OS is Solaris 10, observe following cautions:

When uninstalling the Device Manager agent, do not specify the system's zone settings. If you do this, uninstallation might fail.



CAUTION: When the host OS is HP-UX, observe following cautions:

- When uninstalling the Device Manager agent, the `swagentd` daemon must 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 uninstall the Device Manager agent.

To uninstall the Device Manager agent on a Solaris, AIX, HP-UX, or Linux:

1. Execute the following command from the command line:
 - In Solaris, HP-UX, and Linux:
 - `# /opt/HDVM/HBaseAgent/bin/.uninstall.sh`
 - In AIX:
 - `# /usr/HDVM/HBaseAgent/bin/.uninstall.sh`

The following message appears:

- Are you sure to UNINSTALL Device Manager-Agent? (Y/N)
2. Type `y`.

The following confirmation message appears:

- Uninstallation of Device Manager - Agent was successful.

3 Device Manager agent operations

This chapter describes how to specify commands used for Device Manager agent operations, and provides details on Device Manager agent properties.

This chapter contains the following topics:

- Configuring and operating the Device Manager agent (see section 3-1)
- Notes on Device Manager agent operations (see section 3-2)
- Starting and stopping the Device Manager agent (see section 3-3)
- Modifying server information (see section 3-4)
- Changing the execution period of the HiScan command (see section 3-5)
- Device Manager agent commands (see section 3-6)
- Property files (see section 3-7)
- Using a User-created RAID Manager XP Configuration Definition File (see section 3-8)

3-1 Configuring and operating the Device Manager agent

This section describes Device Manager agent operations and operating methods.

The Device Manager agent collects information about storage devices (logical units on a disk array) that are connected to the host server as well as information about the host server itself. It then transmits this information to the Device Manager server using TCP/IP. This collected information includes the capacity and usage rate for each storage unit, the WWN of the HBA, mount points, file system types, and SCSI addresses.

The Device Manager agent command `hldutil` collects this information and the `HiScan` command transmits the information to the Device Manager server and to a resident program that provides responses to requests from programs such as the Device Manager server and Hitachi Dynamic Link Manager.

When the Device Manager agent is started, the `HiScan` command is automatically executed one time, and the information is reported to the Device Manager server. After that first execution, the `HiScan` command is executed according to the schedule selected during setup, and then the information is reported to the Device Manager server.

CAUTION:

When installing the Device Manager agent on multiple hosts, set a different execution time for each host to prevent the `HiScan` command from being executed simultaneously by multiple hosts.

When the Device Manager agent is installed, the resident program (HBsA) is automatically started, and the `HiScan` command is periodically executed by the task management function of the system.

The name of the host running the Device Manager agent must be unique for each Device Manager server to which information is to be reported

For details about `HiScan`, see section 3-6-2 . For details about how to start HBsA, see section 3-3 . For details about `hldutil`, see section 3-6-3 .

3-1-1 Automatic and manual execution of the HiScan command

The `HiScan` command can be executed either manually or using auto-execution.

- When set to auto execution, the `HiScan` command runs according to the specified execution period.
For details on how to set up the execution period, see subsection 2-11-2 . For details about how to change the specified execution period, see section 3-5 .
- Under manual execution, the user runs programs as necessary. With the Device Manager agent, the user runs the `HiScan` command, and starts and stops the Device Manager agent.
- Under manual execution, the user runs the `HiScan` command as necessary.

3-1-2 Methods of operating the Device Manager agent

You can operate the Device Manager agent using the following methods:

- **Modify server information:** You can modify the server information you set up. For details on modifying the server information, see section 3-4 .
- **Change the execution period:** You can change the execution period for the HiScan command. For details about how to change the execution period, see section 3-5 .

3-2 Notes on Device Manager agent operations

This section provides additional notes on Device Manager agent operations and the settings required to manage Device Manager agent operations.

3-2-1 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.

3-2-2 When the storage subsystem configuration changes

The OS may not immediately recognize the latest updates after the disk array configuration is changed (for example, if an LU is registered or deleted). In this case, the Device Manager agent reports old information to the Device Manager server. If the changes in the disk array configuration are not reflected in the Device Manager server, execute the `hldutil` command to ensure that the host recognizes the configuration changes, and then execute the `HiScan` command. For details about the `hldutil` command, see section 3-6-3 . For details about the `HiScan` command, see section 3-6-2 .

3-2-3 When an invalid path exists

Sometimes a path for an LU managed by a Device Manager is invalid due to some problem such as a disconnection. If the `HiScan` command is executed in this situation, the error message `KAIC22019-E` is output to the console where the command is executed or to the error log file. In this a case, the system may be unable to register the host information in the Device Manager server.

If this should happen, restore the invalid path, or change the OS settings so that the OS cannot recognize the invalid path.

3-2-4 When the host is Windows server 2003 or 2003 x64 edition

The Device Manager agent runs on WOW64 when the host is Windows Server 2003 or Windows Server 2003 x64 Edition. Execute Device Manager agent commands from the command prompt for WOW64. The following command is an example:

- `C:\WINDOWS\SysWOW64\cmd.exe`

When other programs linked with the Device Manager frequently access the Device Manager agent running on the Windows Server 2003 or Windows Server 2003 x64 Edition host, JavaVM can end abnormally. If this happens, 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 add `-Djava.compiler=NONE` to the Java startup option. The following shows an example of editing the `server.cmd` file:

```
..java -Dalet.msclang -Djava.compiler=NONE %1 %2 -classpath ...
```

3-2-5 For multi-path configurations

When multi-path configurations are used in the following host environments, WWN information and LU information (including file systems, volume usage, copy types, copy roles, and copy statuses) might not be obtainable for alternate paths:

- The host OS is Windows, and Windows MPIO is used.
- The host OS is Solaris, and Hitachi Dynamic Link Manager or Sun StorEdge Traffic Manager is used.
- The host OS is AIX, and MPIO is used.

For details about obtaining WWN information for alternate paths, see section 2-4 .

3-2-6 Changing the Windows firewall settings manually

To run a Device Manager agent on a host with an active Windows Firewall, you must 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 Device Manager agent as an exception:
 - > netsh firewall add allowedprogram program="installation-folder-for-the-Device-Manager-agent\agent\bin\hbsa_service.exe" name="HBase Agent" mode=ENABLE
 - > netsh firewall add allowedprogram program="installation-folder-for-the-Device-Manager-agent\agent\JRE1.4\bin\java.exe" name="HBase Agent" mode=ENABLE
2. If Windows Firewall is being turned on for the first time, restart the machine.
3. Execute the following command to check the registered contents:
 - > netsh firewall show allVerify that the execution of the command produces the following results:
 - That HBase Agent is displayed.
 - That Mode is Enable.
 - The paths to hbsa_service.exe and java.exe are correct.



NOTE: To reverse the setting executed in step 1, execute the following command :

- 1 > netsh firewall delete allowedprogram "installation-folder-for-Device-Manager-agent\agent\bin\hbsa_service.exe"
- 2 > netsh firewall delete allowedprogram "installation-folder-for-Device-Manager-agent\agent\JRE1.4\bin\java.exe"

3-2-7 When changing the user executing the Device Manager agent service

For Windows, the LocalSystem privilege is set up for the user that executes the service of the Device Manager agent. Follow the steps below to change the HBsA Service execution user to a user with Administrator privilege.

To change the HBsA Service execution user:

1. Stop the Device Manager agent.
For details on this procedure, see subsection 3-3-2 .
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 select **Account**.
5. Set up the user and password and click **OK**.
6. From the Services window, select HBsA Service and start the service.
The HBsA Service starts running.

3-2-8 When the host OS is Solaris, AIX, HP-UX, or Linux

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.

3-2-9 When the host OS is AIX in a cluster environment

When the execution period for the HiScan command of the Device Manager agent is set to the same period in both the active node and standby node, if the I/O load on the shared disk increases, occasionally SC_DISK_ERR2 (Device Busy) can be output to the error log in the standby node. In this case, the shared disk is correctly reserved by the active node, so the system is not affected by this error. In addition, because the information about the shared disk is obtained from the Device Manager agent operating in the active node, there is no problem in the operation.

3-2-10 When the Device Manager agent is accessed by other Command View XP AE Suite software

If the Device Manager agent is accessed by another product in the Command View XP AE Suite (a collective name for HP StorageWorks Command View XP Advanced Edition software and plug-in products) either

immediately after installation or immediately after the service starts up, a transmission error occurs and the other Command View XP AE Suite software can stop running. If the product stops running, wait a few minutes and then restart it.

If a version of Hitachi Dynamic Link Manager earlier than 5.8 is installed, you must set the port number used by the Device Manager agent agent by setting the following values in the `server.properties` file:

- `Server.http.port`: 23011
- `Server.agent.port`: 23013

3-2-11 When the host OS is Windows and a device is assigned a drive letter

When assigning a drive letter to a device on a Windows host, use a letter from C through Z. The Device Manager agent does not acquire data from a devices assigned drive letter A or B.

3-2-12 When the host OS is Solaris, and VxVM is used

If the host OS is Solaris and a VxVM version earlier than 4.0 is used, when a device is named based on its enclosure, the Device Manager agent does not notify the Device Manager server of correspondence between a file system and a LUN.

3-2-13 When the host OS is Linux

If the host OS is Linux AS 2.1 or an earlier version of Linux AS3.0 (Update 6) or Linux ES 3.0 (Update 6), the following rules apply:

- 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) using the HP StorageWorks XP Provisioning Manager software client
 - Executing the Hitachi Dynamic Link Manager `dlnmcfgmgr` command
 - Executing disk control commands (such as `blockdev`)
- Do not perform the following operations while starting the Device Manager agent:
 - Setting up a host using the XP Provisioning Manager client
 - Executing the Hitachi Dynamic Link Manager `dlnmcfgmgr` 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 using the XP Provisioning Manager client
 - Executing the Hitachi Dynamic Link Manager `dlnmcfgmgr` command
 - Executing disk control commands (such as `blockdev`)
- Do not automatically execute 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 section [3-6-2](#) .

If the `HiScan` command must be executed automatically for system-operational reasons, do not perform any operation on the host during the execution of the command.

3-2-14 When the host recognizes 100 or more LUs

If the number of LUs managed by Device Manager and recognized by a single host is 100 or more, the following problems can occur:

- When the `HiScan` command is executed, the `KAIC22014-E`, or `KAIC22019-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 does not respond even after waiting for a while.

To avoid the above, change the values shown in the following table.

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 <code>server.http.entity.maxLength</code> property in the <code>server.properties</code> property file of the Device Manager server. For details about the <code>server.http.entity.maxLength</code> property, see the <i>HP StorageWorks Command View XP Advanced Edition software Device Manager server installation and configuration guide</i> .
The timeout value for the processing to register information in a server	Set the following properties in the <code>server.properties</code> property file for the Device Manager agent: <ul style="list-style-type: none">• <code>server.http.server.timeOut</code>• <code>server.util.processTimeOut</code> For details about the properties, see subsection 3-7-1 .
The memory heap size	Set the value for the <code>server.agent.maxMemorySize</code> property in the <code>server.properties</code> property file of the Device Manager agent. For details about the <code>server.agent.maxMemorySize</code> property, see subsection 3-7-1 .

The values set for the above items differ depending on whether the host is using a volume manager. For details when no volume manager is used, see subsection 3-2-14-1 . For details when a volume manager is used, see subsection 3-2-14-2 .

CAUTION: Depending on the load status of the Device Manager server, an `OutOfMemory` error might also 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 *HP StorageWorks Command View XP Advanced Edition software Device Manager server installation and configuration 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>
```

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.

NOTE: Depending on the environment, this issue may not be solved by setting the guide values. Make sure that you adjust the values to suit your environment.

NOTE: 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.

NOTE: If the host OS is Windows Server 2003 (IPF), make sure that Service Pack 1 has been installed.

3-2-14-1 Setting values when a volume manager is not used

Tables 3-1 through 3-6 provides estimates for setting values values in the following environments

Depending on your environment, the estimated values described here may be insufficient. Make sure that you adjust the values to suit your environment.

In the following cases, specify values that are two to three times larger than the values described below:

- 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

When a volume manager is not used

Table 3-2 lists approximate standards for setting values.

Table 3-2 Setting values when a volume manager is not used

Number of LUs managed by Device Manager, and recognized by the host	<code>server.http.entity.maxLength</code> (units: bytes)	<code>server.http.server.timeOut</code> (units: seconds)	<code>server.util.processTimeOut</code> (units: milliseconds)
100	Default value (131072)	Default value (600)	Default value (600000)
256	153600	600	600000
512	307200	600	600000
1024	614400	1200	1200000

3-2-14-2 Setting values when a volume manager is used

The following table lists the setting values when the execution of the `HiScan` command finishes within an hour, for each host OS. Using a configuration where the number of LUs or logical volumes is more than the number shown in the following table is not recommended because, in such a configuration, it will take more than one hour to execute the `HiScan` command, and the `HiScan` command 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	<code>server.http.entity.maxLength</code> (units: bytes)	<code>server.http.server.timeOut</code> (units: seconds)	<code>server.util.processTimeOut</code> (units: milliseconds)	<code>server.agent.maxMemorySize</code> (units: MB)
88/10	230000	Default value (600)	Default value (600000)	64
88/20	750000	600	600000	64
100/200	12000000	600	600000	128
100/500	30000000	600	600000	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	<code>server.http.entity.maxLength</code> (units: bytes)	<code>server.http.server.timeOut</code> (units: seconds)	<code>server.util.processTimeOut</code> (units: milliseconds)	<code>server.agent.maxMemorySize</code> (units: MB)
100/200	3100000	Default value (600)	Default value (600000)	128
100/500	7200000	600	600000	384
150/500	12000000	600	600000	512
250/500	18000000	600	600000	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	<code>server.http.entity.maxLength</code> (units: bytes)	<code>server.http.server.timeOut</code> (units: seconds)	<code>server.util.processTimeOut</code> (units: milliseconds)	<code>server.agent.maxMemorySize</code> (units: MB)
100/200	2500000	Default value (600)	Default value (600000)	128
100/500	6000000	600	600000	384
175/500	11000000	600	670000	640
250/500	15000000	600	1200000	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.processTimeout (units: milliseconds)	server.agent.maxMemorySize (units: MB)
100/50	745000	Default value (600)	Default value (600000)	64
100/100	1400000	600	600000	64
100/256	3500000	600	600000	192
200/256	7000000	600	600000	512

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.processTimeout (units: milliseconds)	server.agent.maxMemorySize (units: MB)
100/50	748000	Default value (600)	Default value (600000)	64
100/100	1420000	600	600000	64
100/256	3600000	600	600000	192
200/256	7100000	600	600000	512

3-2-15 When the host OS is Solaris

You cannot obtain partition information of LUs that do not have a label. Therefore, XP Provisioning Manager displays the partition size of such LUs as `Unknown`.

3-3 Starting and stopping the Device Manager agent

This section contains information about starting and stopping the Device Manager agent. It includes the following topics:

- Starting the Device Manager agent, see section 3-3-1
- Stopping the Device Manager agent, see section 3-3-2
- Checking the operating status of the Device Manager, see section 3-3-3



NOTE: In Solaris, AIX, HP-UX, or Linux, if setup is performed after the Device Manager agent installation finishes, the Device Manager agent service or daemon process starts automatically.

3-3-1 Starting the Device Manager agent

This subsection describes how to start the Device Manager agent. This operation requires Administrator or superuser privileges.



CAUTION: To run the Device Manager agent properly, setup for the Device Manager agent must be completed beforehand. For details about the setup procedure, see section 2-11 .

In Windows:

There are two ways to start the Device Manager agent:

- From the Services window, select HBsA Service to start the service.
- From the command line, execute the `hbsasrv` command:


```
> installation-folder-for-Device-Manager-agent\bin\hbsasrv.exe start
```

In Solaris, HP-UX, or Linux:

Execute the following command from the command line:


```
# /opt/HDVM/HBaseAgent/bin/hbsasrv start
```

In AIX:

Execute the following command from the command line:

```
# /usr/HDVM/HBaseAgent/bin/hbsasrv start
```


3-3-2 Stopping the Device Manager agent

This subsection describes how to stop the Device Manager agent. This operation requires Administrator or superuser privileges.

In Windows:

There are two ways to stop the Device Manager agent:

- From the Services window, select **HBsA Service**.
- From the command line, execute the `hbsasrv` command:
> *installation-folder-for-Device-Manager-agent*\bin\hbsasrv.exe stop

 **CAUTION:** If you are working in a Windows Server 2003 or Windows Server 2003 x64 Edition environments, use the `hbsasrv` command to stop the service.

In Solaris, HP-UX, or Linux:

Execute the `hbsasrv` command from the command line:

```
# /opt/HDVM/HBaseAgent/bin/hbsasrv stop
```


In AIX:

Execute the `hbsasrv` command from the command line:

```
# /usr/HDVM/HBaseAgent/bin/hbsasrv stop
```

3-3-3 Checking the operating status of the Device Manager agent

This subsection describes how to check the operating status of the Device Manager agent. This operation requires Administrator or superuser privileges.

 **CAUTION:** The checking methods shown below are used to check whether the Device Manager agent service or daemon process is running. To run the Device Manager agent properly, setup for the Device Manager agent must be completed beforehand. For details about the setup procedure, see section [2-11](#) .

In Windows:

The following methods can be used to check the operating status:

- From the Services window, check the HBsA Service status.
- From the command line execute the following command.
> *installation-folder-for-Device-Manager-agent*\bin\hbsasrv.exe status

In Solaris, HP-UX, or Linux:

Execute the following command from the command line:


```
# /opt/HDVM/HBaseAgent/bin/hbsasrv status
```

In AIX:

Execute the following command from the command line:

```
# /usr/HDVM/HBaseAgent/bin/hbsasrv status
```

If the result of the command displays `Status` as `Running`, the Device Manager agent service or daemon process is operating. If the result displays `Status` as `Stop`, the service or daemon process has stopped.

 **NOTE:** The version displayed when you execute the `hbsasrv` command is not the Device Manager agent version. Use one of the following commands to check the Device Manager agent version.

In Windows:

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

In Solaris, HP-UX, or Linux:

```
# /opt/HDVM/HBaseAgent/bin/hdvm_info
```

In AIX:

```
# /usr/HDVM/HBaseAgent/bin/hdvm_info
```

3-3-4 Restarting the Device Manager agent

The service or daemon process of the Device Manager agent must be restarted in the following cases:

- When the IP address of a host on which the Device Manager agent is installed changes.
- When the HBA driver or HBA API library was installed on a host in which the Device Manager agent is installed.
- When a host on which the Device Manager agent is running is deleted in the web client host management window.
- When the contents of the property files (`logger.properties` and `server.properties`) of the Device Manager agent are modified.
- When RAID Manager XP is installed or uninstalled.
- When execution of the `hdvmagt_account` command is interrupted.
- When the `hdvmagt_account` command is executed in Windows.

△ CAUTION: If the Device Manager server is not running, information will not be 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, make sure that the Device Manager server service is running, and then install a Device Manager agent or start a Device Manager agent service.

3-3-5 If the Device Manager agent cannot stop

A Device Manager agent may be unable to stop when an add-on module or version 05-80 or later of Hitachi Dynamic Link Manager is running. In this case, the error message `KAIE62604-E` appears. To stop the Device Manager agent, wait until processing is complete for the add-on module and Hitachi Dynamic Link Manager, and then attempt to stop the Device Manager agent again.

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 this case, all processing by the Device Manager agent terminates and ongoing processing of jobs is not guaranteed.

3-4 Modifying server information

You can use the `hdvmagt_account` command to change the Device Manager server to which the Device Manager agent transmits information.

This command provides an interactive user interface for setting the following property values in the `server.properties` file:

- `server.server.serverIPAddress`
- `server.server.serverPort`
- `server.server.authorization`

For details about the `hdvmagt_account` command, see section [3-6-5](#) .

3-5 Changing the execution period of the HiScan command

To change the execution period of the `HiScan` command, use the `hdvmagt_schedule` command. For details about this command, see section [3-6-4](#) .

3-6 Device Manager agent commands

With the Device Manager agent, you can use the following commands:

- `hbsasrv` command
This is a command for starting and stopping the Device Manager agent and for displaying the operating status. For details about the `hbsasrv` command, see subsection 3-6-1 .
- `HiScan` command
This is a command for sending information to the Device Manager server. For details about the `HiScan` command, see section 3-6-2 .
- `hldutil` command
This is a command for displaying device information and managing execution results log files. For details about the `hldutil` command, see section 3-6-3 .
- `hdvmagt_schedule` command
This is a command for changing the execution period of the `HiScan` command. For details about the `hdvmagt_schedule` command, see section 3-6-4 .
- `hdvmagt_account` command
This is a command for changing the information about the Device Manager server. For details about the `hdvmagt_account` command, see section 3-6-5 .



NOTE: In Windows, the folder in which the Device Manager agent 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 apply the changes in the environment variable `PATH`. Thereafter, you can execute commands from any directory.

3-6-1 `hbsasrv` command syntax

The `hbsasrv` command is used to start and stop the Device Manager agent and to display the operating status.

The `hbsasrv` command is stored in the following location:

In Windows:

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

In Solaris, HP-UX, or Linux:

```
/opt/HDVM/HBaseAgent/bin/hbsasrv
```

In AIX:

```
/usr/HDVM/HBaseAgent/bin/hbsasrv
```

The syntax of the `hbsasrv` command is described below.

Table 3-8 `hbsasrv` command syntax

Item	Description
Synopsis	<code>hbsasrv [start stop [-f] status]</code>
Description	Starts or stops the service or daemon process of the Device Manager agent. This command also displays the status of the service or daemon process.
Options	<p><code>start</code>: Starts the service or daemon process.</p> <p><code>stop [-f]</code>: Stops the service or daemon process.</p> <p>If any add-on module or the version 5.8 or later of Hitachi Dynamic Link Manager is running, you may not be able to stop the Device Manager agent. In this case, the error message <code>KAIE62604-E</code> appears. Wait until the add-on module or Hitachi Dynamic Link Manager completes its operation, and then execute the command again.</p> <p>If you urgently need to stop the Device Manager agent, you can force the Device Manager agent to shut down by executing the <code>hbsasrv</code> command with the <code>stop -f</code> option. In this case, all processing terminates and ongoing processing of jobs is not guaranteed.</p> <p><code>status</code>: Displays the operating status of the <code>service</code> or <code>daemon</code> process.</p> <p>Note: If you execute the command without specifying an argument, the command usage information is displayed.</p>

3-6-2 `HiScan` command syntax

The `HiScan` command is stored in the following locations.

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

The syntax of the `HiScan` command is described below.

Table 3-9 HiScan command syntax

Item	Description
Synopsis	<code>HiScan { -s server [-u userid -p password] [{ -c sec -t output-file }] -t output-file }</code>
Description	<p>Reports information about attached StorageWorks XP disk arrays. <code>HiScan</code> scans system information and constructs associations among file systems, volumes, partitions and disk drives. From these results it creates an HTTP/XML message. Depending upon parameters, <code>HiScan</code> can transmit this message to a Device Manager server so that host, file system, disk adapter, and utilization information can be associated with StorageWorks XP disk arrays.</p> <p>This command requires superuser or Administrator privileges.</p>
Option	<p>-s server: <i>server</i> specifies the network address for the transfer destination of the HTTP/XML message generated by the Device Manager agent. <i>server</i> can be specified in the following format: <code>{IP-address[:port-number] host-name[:port-number] localhost[:port-number] }</code> An IP address, a host name, or <code>localhost</code> can be specified as a network address. In addition, a port number can be attached to the address in an <code>address:port-number</code> format. If no port number is provided, the default port number is 2001; For example: 192.168.1.102:2001. You can 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 - . @ _ -s is an optional parameter. If -s is omitted, the -t option must be supplied.</p> <p>-u userid The user identifier is used by the Device Manager server to validate <code>HiScan</code> database update requests. If the -s option is supplied and u option is omitted, <code>HiScan</code> uses the userid and password stored in <code>server.server.authorization</code> of the <code>server.properties</code> file (see Table 3-20). You can use a character string of 1 to 256 bytes to specify this option. The following characters can be used: a-z A-Z 0-9 # + - . @ _</p> <p>-p password The password is used by the Device Manager server to validate the userid supplied in the -u option. The -p option is required if the -u option is supplied. If the -s option is supplied and the -p option is omitted, <code>HiScan</code> uses the userid and password that are stored in <code>server.server.authorization</code> of the <code>server.properties</code> file (see Table 3-20). You can use a character string of 1 to 256 bytes to specify this option. You can use the following characters: a-z A-Z 0-9 ! " # \$ % & () * + - . = @ \ ^ _ ' </p> <p>-c sec Pauses for xx seconds between successive scan/report cycles. Continue to iterate until a termination signal is encountered. Values of less than ten seconds are recognized as invalid. If -t is supplied, -c must not be used.</p> <p>-t output-file Sends the output messages to the indicated output file. Note: This option is intended for diagnostic purposes only. It can be supplied in addition to the -s option. If both are supplied, the output request message and input response message (from the Device Manager server) are both included in the output file. If -t is supplied, -c must not be used.</p>
Exit Status	None.

3-6-3 hldutil command syntax

The `hldutil` command displays device information and manages the execution results log file.

- In Windows:

Installation-folder-for-Device-Manager-agent\util\bin\
hldutil.exe

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

Table 3-10 on the following pages lists and describes the hldutil command syntax.

Table 3-10 hldutil command syntax

Item	Description
Synopsis	<p>For the device information display function: hldutil [-d <i>device-file</i>] [-g <i>disk-group</i>] [-l <i>ldev#.ser#</i>] [-p] [-q] [-nolog] [-s <i>sort-key.</i>] [-serdec] [-k] [-hf <i>log-file</i>] [-h <i>log-number</i>]</p> <p>For the execution-result log file management function: hldutil -h <i>log-number</i> -hb <i>log-file</i> -hrm [<i>log-number all</i>] -history <i>number</i></p>
Description	<p>Displays device information and manages the execution results log file. If you do not specify an option, the command outputs information about all currently recognized logical devices. This command requires superuser or Administrator privileges. If you execute the hldutil command immediately after the host environment is changed (for example, when a logical unit is added or deleted), the command may not be able to recognize the changed contents of the host.</p>
Options	<p>-d [device-file]: If you want to view information about a specific logical device, specify the device special file name (in Solaris, AIX, HP-UX, or Linux) or disk number (in Windows) of the logical device. If you omit this option, the command displays information about all currently recognized logical devices. You cannot specify the -d option and the -g or -l option at the same time.</p> <p>-g [disk-group]: 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.</p> <p>-l ldev# ser#: If you want to view information about a specific logical device, specify the logical device number (<i>ldev#</i>) and serial number (<i>ser#</i>) of the logical device in the order indicated. If you omit either the logical device number or serial number, the command does not provide information about the logical device. You cannot specify the -l option and the -d or -g option at the same time. If you specify the -l option, the display items output by the command with this option specified is limited to <i>ldev#</i> (logical device number). If you specify the -l option, the command displays only the following items: <i>ldev#</i> (logical device number), <i>ser#</i> (storage subsystem serial number), <i>Device</i> (device special file or disk number), <i>Dg name</i> (disk group name), <i>fs</i> (file system)</p> <p>-p: Specify this option to add the P-VOL and S-VOL information (that you set up by using Business Copy XP, Continuous Access XP, Snapshot XP, or Continuous Access XP Journal) to the logical device information to be output. If no P-VOL or S-VOL information is assigned to a logical device, a command with this option specified does not output P-VOL or S-VOL information.</p> <p>-q: Specify this option to output command execution results only to the execution result log file. If you specify this option, the command does not send its execution results to the standard output (quiet mode). Typically, you would specify this option to run a background job and supply the latest logical device information to the execution result log file. However, error messages are output to the standard error output.</p> <p>-nolog: Specify this option to output command execution results only to the standard output. If you specify this option, the execution result log file is not updated.</p> <p>-s sort-key: Specify this option when sorting logical device information in ascending order of ASCII codes. This option includes one or more sort keys. When specifying multiple sort keys, place a one-byte space between adjacent sort keys.</p> <ul style="list-style-type: none"> • 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 logical device 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, you receive an error message. • If you do not specify the -s option, the command outputs logical device information in the order in which it processes the information. See Table 3-11 for the sort key descriptions.

Table 3-10 hldutil command syntax

Item	Description
Options	<p><code>-k</code> Specify this option when outputting the latest execution result log file to the standard output. This processing involves no hardware access. Since the command skips processing for obtaining logical device information, its execution does not affect device input or output. However, if the execution result log file contains no record, the command acquires logical device information and outputs the results to the standard output and the execution result log file. You cannot specify the <code>-k</code> option and the <code>-h</code> or <code>-hf</code> option at the same time.</p> <p><code>-hf [log-file]</code> This command outputs the contents of the specified execution result log file to the standard output. The command does not access any disk array device. If you omit the file name, the command waits for the entry of a file name. If the specified file name does not identify an execution result log file, the command outputs an error message and ends. You cannot specify the <code>-hf</code> option and the <code>-k</code> or <code>-h</code> option at the same time.</p> <p><code>-h [log-number]</code> If you use the device information display function, this command outputs the contents of the execution result log file identified by the specified log number to the standard output. The command does not access any disk array device. If you use the execution result log file management function, the command copies an execution-result log file. Assign the copy source execution result log file name to a log number and specify the <code>-hb</code> option to designate the copy destination.</p> <ul style="list-style-type: none"> • 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 the specified log number does not identify an execution result log file, the command outputs an error message and terminates. You cannot specify the <code>-h</code> option and the <code>-k</code> or <code>-hf</code> option at the same time. <p><code>-hb [log-file]</code> Specify this option when copying an execution result log file that is the result of using the device information display function. The command copies the execution result log file specified by the <code>-h</code> option to the file specified by the <code>-hb</code> option. Use the full path name (including directories) or relative path name for the file. 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 whether to overwrite the file and waits for your reply. You must specify this option together with the <code>-h</code> option. You cannot specify the <code>-hb</code> option together with any option other than <code>-h</code>.</p> <p><code>-hrm [log-number all]</code> Specify this option when deleting an execution result log file that was created when the device information display function was used. Specify the log number that identifies the execution result log file to be deleted.</p> <ul style="list-style-type: none"> • If you specify <code>all</code> instead of a log number, the command deletes all execution result log files from the default log storage directory. • If you omit the log number, 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 terminates. <p>You cannot specify the <code>-hrm</code> option together with any other option.</p> <p><code>-history number</code> Specify the number of generations of execution result log files to be retained. The execution result log files are created when the device information display function is used. You can specify a number between 1 and 64. The default value is 32. The specified number becomes effective the next time the device information display function is used to create an execution result log file. You cannot specify the <code>-history number</code> option together with any other option.</p> <p><code>-serdec</code> Specify this option to display the serial number of the storage subsystem in the decimal format when displaying device information.</p>
Exit Status	None.

Table 3-11 describes the sort keys for the `hldutil` command.

Table 3-11 Sort key descriptions

Sort Key	Descriptions
dg	Disk group name.
fs	File system name.
ldev	Logical device number
lun	Logical unit number
port	Port number
prod	Product name
rg	RAID Group number
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

Table 3-12 describes the items displayed by the device information display function. The items displayed differ depending on the OS and the specified options.

Table 3-12 Displayed items

Item	Description
Dg name	Disk group name
Device	Device special file name (for Solaris, AIX, HP-UX, or Linux) Disk number (for Windows)
fs	File system name
P/S	Identification of the primary volume or secondary volume
Vend.	Vendor name
Prod.	Product name
Port#	Port number (on the DKC)
Tid#	Target ID (SCSI interface on the host)
Lun#	Logical unit number (SCSI interface on the host)
Ldev#	Logical device 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	PortWWN
NodeWWN	NodeWWN

Table 3-13 describes the correspondence between the character string for RaidID and HP storage systems.

Table 3-13 Correspondence between RaidID and models

RaidID	Model
R401	XP48
R400	XP512
R451	XP128
R450	XP1024

Table 3-13 Correspondence between RaidID and models

RaidID	Model
R500	XP12000
R501	XP10000
R502	SVS200

3-6-4 hdvmagt_schedule command syntax

The `hdvmagt_schedule` command specifies information for the Device Manager server to which the Device Manager agent sends information.

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

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

The `hdvmagt_schedule` command syntax is described below.

Table 3-14 `hdvmagt_schedule` command syntax

Item	Description
Synopsis	<code>hdvmagt_schedule</code>
Description	Provides an interactive interface to setup the automatic execution period of the <code>HiScan</code> command. You must have superuser/Administrator authority to execute the <code>hdvmagt_schedule</code> command. When you execute this command, you can choose one of four automatic execution periods for the <code>HiScan</code> command: <ul style="list-style-type: none">• Hourly• Daily• Weekly• No automatic execution(or cancel the set schedule) You can specify any execution time. If you do not specify the execution time for the hourly execution period, the <code>HiScan</code> command is executed at the 47th minute of every hour. For the daily or weekly period, the command is executed at 2:47 AM.
Options	None.

3-6-5 hdvmagt_account command syntax

The `hdvmagt_account` command specifies information for the Device Manager server to which the Device Manager agent sends host information.

When you change an account used in the Device Manager agent, use the web client to create or change the user ID. For this work, set the user privileges to Peer. For details about how to create or change a user ID, see the *HP StorageWorks Command View XP Advanced Edition software Device Manager web client user guide*.

CAUTION: For Solaris, AIX, HP-UX or Linux, if you execute the `hdvmagt_account` command, the Device Manager agent is restarted of whether or not the server information is changed. For details on how to start and stop the Device Manager agent, see section 3-3 .

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

- In Windows:
Installation-folder-for-Device-Manager-agent\bin\hdvmagt_account.bat
- In Solaris, HP-UX, or Linux:
/opt/HDVM/HBaseAgent/bin/hdvmagt_account

- *Installation-folder-for-Device-Manager-agent\agent\config\logger.properties*
- *Installation-folder-for-Device-Manager-agent\agent\config\programproductinfo.properties*
- *installation-folder-for-Device-Manager-agent\util\bin\hldutil.properties*
- In Solaris, HP-UX, or Linux:
 - /opt/HDVM/HBaseAgent/agent/config/server.properties*
 - /opt/HDVM/HBaseAgent/agent/config/logger.properties*
 - /opt/HDVM/HBaseAgent/util/bin/hldutil.properties*
- In AIX:
 - /usr/HDVM/HBaseAgent/agent/config/server.properties*
 - /usr/HDVM/HBaseAgent/agent/config/logger.properties*
 - /usr/HDVM/HBaseAgent/util/bin/hldutil.properties*

3-7-1 server.properties file

The `server.properties` file contains network configuration properties. [Table 3-16](#) to [Table 3-22](#) list and describe the HTTP communication function properties for the Device Manager agent.

Table 3-16 `server.properties` file (setting up ports used by the daemon process and the Web server function)

Property	Description
<code>server.agent.port</code>	<p>Specifies the port number to be used for the Device Manager agent's daemon process (or service).</p> <p>Normal range is 1024 to 49151. Too small a number may conflict with other applications. If a version of Hitachi Dynamic Link Manager earlier than 5.8 is installed, set the port number 23013.</p> <p>Default: 24041</p>
<code>server.http.localPort</code>	<p>Specifies the port number for communication between the Device Manager agent's daemon process and the WebServer process.</p> <p>Normal range is 1024 to 49151. Too small a number conflicts with other applications.</p> <p>Default: 24043</p>
<code>server.http.port</code>	<p>Specifies the port number that the Device Manager agent's WebServer uses.</p> <p>Avoid using low port numbers, because they might conflict with other applications. Normal range is 1024 to 49151. If a version of Hitachi Dynamic Link Manager earlier than 5.8 is installed, set the port number 23011.</p> <p>Default: 24042</p>

Table 3-17 `server.properties` file (setting the host name, IP address, and NIC used by the Web server function)

Property	Description
<code>server.http.host</code>	<p>Specify the host that executes the Device Manager agent's WebServer.</p> <p>Default: localhost</p>
<code>server.http.socket.agentAddress</code>	<p>Specify the IP address at which the Device Manager agent transmits notifications to a Device Manager server. To limit the IP address, specify the desired IP address as a dotted decimal number. The default is the IP address acquired by the Device Manager agent. For multiple IP addresses, the first IP address acquired by the Device Manager agent via API is used.</p> <p>Default: IP address acquired by the Device Manager agent</p>

Table 3-17 server.properties file (setting the host name, IP address, and NIC used by the Web server function)

Property	Description
server.http.socket.bindAddress	<p>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 the property is left blank (which is the default), the Device Manager agent can accept requests through all NICs. When restricting the NIC to be accepted, enter the dotted decimal IP addresses that the Device Manager agent accepts.</p> <p>Default: None. (The Device Manager agent listens to all NICs.)</p>

Table 3-18 server.properties file (setting up basic operations of the Web server function)

Property	Description
server.agent.maxMemorySize	<p>Specify the maximum memory heap size for Web server function processes of the Device Manager agent, in MB.</p> <p>Specifiable range (MB): 32 to 4096.</p> <p>Default: None (the heap runs in a 64-megabyte memory area).</p>
server.agent.shutdownTime	<p>Specify the period (in milliseconds) the Device Manager agent's WebServer should wait after it receives or sends the last http message. If a value of zero or less is specified, the waiting period is unlimited.</p> <p>Do not edit this property without knowing the current status of the Device Manager agent's performance.</p> <p>Default: 600000[msec]</p>

Table 3-19 server.properties file (security settings for the Web server function)

Property	Description
server.http.entity.maxLength	<p>Specify the maximum size (in bytes) of HTTP request entities permitted by the Web server function of the Device Manager agent. By limiting the impact of malicious requests with an entity with an unusually large amount of data, this setting can be useful in repelling attacks intended to impair services or cause a buffer overflow. When it detects a request larger than the specified limit, the Device Manager agent sends a remote error response and records details of the request in the log.</p> <p>Normally, the default value of this property need not be changed.</p> <p>Default:1024</p>
server.http.security.clientIP	<p>Specify that the remote host or subnet can send a request to the Device Manager agent.</p> <p>This setting limits the IP addresses permitted for connection, preventing denial-of-service attacks or other attacks that intend to overflow buffers.</p> <p>For example, server.http.security clientIP=191.0.0.2, 192.168.*.*, will permit 191.0.0.2 and 192.168.0.0 to 192.168.255.255 to connect to the Device Manager agent</p> <p>You can use an asterisk (*) as a wildcard character to specify multiple connections from a single IP address. When specifying multiple IP addresses, separate them by commas (.). Invalid specifications for dotted decimal IP addresses and spaces are ignored and do not cause an error.</p> <p>Default: *.*.*.*.(Any host can access the Device Manager agent)</p>

Table 3-20 server.properties file (information of the Device Manager server)

Property	Description
server.server.authorization	<p>A stored user-id and password, authorized by the Device Manager server. This property is encoded data, so you cannot edit it using a text editor. To edit this property, use the <code>hevdmagt_account</code> command (see section 3-6-5).</p> <p>Default: None.</p>
server.server.serverIPAddresses	<p>Enter the IP address or host name of the Device Manager server.</p> <p>When specifying an IP address use the dotted-decimal format.</p> <p>When specifying a host name:</p> <p>Use a character string of 50 bytes or fewer.</p> <p>You can use the following characters:</p> <p>a-z A-Z 0-9 - . @ _</p> <p>To specify this property use the text editor, or execute the <code>hdvdmagt_account</code> command (see section 3-6-5).</p> <p>Default: 255.255.255.255</p>
server.server.serverPort	<p>Specifies the port number of the Device Manager server to which the Device Manager agent will be connected. You can specify a value from 1024 to 49151. You must specify the same value specified for the <code>server.http.port</code> property of the Device Manager server.</p> <p>Note: The value of this property equals the value of the port number of the Device Manager server. Specify this property using a text editor, or by executing the <code>hdvdmagt_account</code> command (see section 3-6-5).</p> <p>Default: 2001</p>

Table 3-21 server.properties file (setting up RAID Manager XP)

Property	Description
server.agent.rm.centralizePairConfiguration	<p>When a specific host is used to centrally manage pair configurations of Business Copy XP, Continuous Access XP, Snapshot XP or Continuous Access XP Journal for the storage subsystems managed by a Device Manager server, set this property to <code>enable</code> for that host. If the host recognizes the command device in each disk array, the LUs not recognized by the host can also be used for a pair setting.</p> <p>The default value of this property is <code>disable</code> only LUs that are recognized by the host can be used for a pair setting).</p> <p>Default: <code>disable</code></p>
server.agent.rm.exclusion.instance	<p>When a volume pair on the host installing the Device Manager agent is already managed by RAID Manager XP and you want to exclude the volume pair from Device Manager operations, you can exclude that volume pair by specifying the instance number of RAID Manager XP. To specify multiple instance numbers, separate the individual numbers with commas (,). From the Device Manager agent, you cannot operate a RAID Manager XP with the instance number specified in this property.</p> <p>Default: None</p>
server.agent.rm.location	<p>You can specify the install directory of RAID Manager XP. For Windows systems, you cannot specify <code>\</code> as a delimiter. Use <code>\\</code> or <code>/</code> instead. To view copy pair information or operate copy pairs, it is necessary to specify the correct directory where RAID Manager XP is installed.</p> <p>The default for Windows is: <code>drive-where-Device-Manager-agent-is-installed/RAIDManager</code></p> <p>The default for Solaris, AIX, HP-UX, and Linux is: <code>/RAIDManager</code></p>

Table 3-21 server.properties file (setting up RAID Manager XP)

Property	Description
server.agent.r m.optimization .userHorcmFile	<p>Specifies whether the user-created RAID Manager XP configuration definition file will be optimized. To optimize the file, specify <code>true</code>. 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:</p> <ul style="list-style-type: none"> • A serial number is added to a command device as a comment. • If that command device becomes unavailable due to, for example, a change to the volume name, the file information that defines the configuration 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 that are not being used are deleted. • The control unit (CU) and LDEV numbers of a command device and pair volume are added as a comment in the <code>cu:ldev</code> format. <p>Default: <code>false</code></p>

Table 3-22 server.properties file (setting up timeout)

Property	Description
server.agent.r m.moduleTimeOu t	<p>Sets a timeout value (in seconds) for the return of the result when the Device Manager agent executes a RAID Manager XP command.</p> <p>When a command takes longer to execute than the setting in this property, the Device Manager agent concludes that an error occurred during the command execution.</p> <p>This setting should only be modified by a system administrator with expert knowledge to fine tune the performance of the Device Manager agent's pair configuration facility.</p> <p>Default: <code>600(seconds)</code></p>
server.http.se rver.timeOut	<p>Specifies a timeout value (in seconds) for receiving a response from the Device Manager server when registering host information using the <code>HiScan</code> command. If no response is received from the Device Manager server by the time specified in this property, the Device Manager agent concludes that an error has occurred and the <code>HiScan</code> command terminates abnormally. You can specify a minimum value of 100 and a maximum value of 3600 in this property. When the specified value is outside these bounds, the timeout is assumed to be 100 if the specified value is less than the minimum, or 3600 if the specified value exceeds the maximum.</p> <p>Default: <code>600</code></p>
server.util.pr ocessTimeOut	<p>Specifies the period (in milliseconds) that is considered as the Device Manager agent's normal execution time for external programs.</p> <p>If an external program takes longer to execute than the time period specified in this property, the Device Manager agent considers the program abnormal and terminates it. If you specify too short a time period, the Device Manager agent may stop executing regular external programs. Do not edit this property without knowing the Device Manager agent's current status.</p> <p>Default: <code>600000[msec]</code> (= 10 minutes)</p>

3-7-2 logger.properties file

The `logger.properties` file contains the logging functions of the Device Manager agent. To configure the `daemon/service` and `WebServer` processes of the Device Manager agent, see [Table 3-23](#).

Table 3-23 logger.properties file

Property	Description
logger.loglevel	Specifies the level of log that the Device Manager agent outputs to the files <code>error.log</code> and <code>trace.log</code> . Log levels: DEBUG, INFO, WARN, ERROR, and FATAL. Default: INFO
logger.MaxBackupIndex	Specifies the maximum number of log file backups. 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, when <code>access.log</code> becomes <code>access.log.1</code> . If additional backup log files are created, the counter increases until the specified number of backup log files is generated (for example, <code>access.log.1</code> becomes <code>access.log.2</code>). After the specified number of backup log files is created, each time a new backup file is created, the oldest backup file is deleted. Specifiable range: 1 through 20. Default: 10
logger.MaxFileSize	Specifies the maximum size of each log file. If a log file becomes larger than specified here, the Device Manager agent creates a new file and writes to it. Unless KB is specified for kilobytes or MB for megabytes, the specified size is interpreted to mean bytes. In this property, the term KB is interpreted as 1024 bytes, and MB as 1024 kilobytes. Specifiable range: From 512KB to 32MB. Default: 1 MB.

3-7-3 programproductinfo.properties file

Table 3-24 contains the program product information properties of the Device Manager agent.

Table 3-24 programproductinfo.properties file

Property	Description
veritas.volume.manager.version	Indicates the version of VxVM installed in Windows. If VxVM is installed in a Windows environment, specify the VxVM version in this property, in the <code>x.x</code> format. Default: None

3-7-4 hldutil.properties file

Table 3-25 lists and describes the properties used to specify the action of the `hldutil` command.

Table 3-25 hldutil.properties file

Property	Description
agent.util.hpux.displayDsf	Specifies the format of the device file name displayed when the <code>hldutil</code> command is executed on a host on which HP-UX 11i v3 is running as the OS. If <code>disk</code> is specified: The disk device files are displayed. If <code>ctd</code> is specified: The ctd device files are displayed. If <code>mix</code> is specified: Both the disk device files and ctd device files are displayed. If any value other than the above is specified, <code>mix</code> is assumed. This property cannot be specified in an OS other than HP-UX 11i v3 and later. Default: <code>mix</code>

3-8 Using a user-created RAID Manager XP configuration definition file

In Device Manager, you can use a user-created RAID Manager XP configuration definition file to manage copy pairs. This section describes requirements for using a user-created RAID Manager XP configuration definition file in Device Manager, how to report the information of the RAID Manager XP configuration definition file to Device Manager, and cautionary notes.

3-8-1 Requirements for using a user-created RAID Manager XP configuration definition file in Device Manager

This subsection describes requirements for using a user-created RAID Manager XP configuration definition file in Device Manager, referring to the following three items:

- Installation and setup for the Device Manager agent
- Storage location for a RAID Manager XP configuration definition file
- Contents of a RAID Manager XP configuration definition file

3-8-1-1 Installation and setup for the Device Manager agent

When you use a RAID Manager XP configuration definition file in Device Manager, the following setup is required in the Device Manager agent:

Installation and setup for the Device Manager agent

- The Device Manager agent must be installed on a host on which RAID Manager XP has been installed.
- The Device Manager server information must be registered after the setup has been completed.

Setup for the Device Manager agent

- If you are using centralized management, you need to specify `enable` for the `server.agent.rm.centralizePairConfiguration` property in the `server.properties` file.
- If one of the following conditions is satisfied, you need to specify the installation directory of RAID Manager XP for the `server.agent.rm.location` property of the `server.properties` file.
 - RAID Manager XP have been installed in a directory other than the default installation directory.
 - In Windows, the installation drive for RAID Manager XP, and the installation drive for the Device Manager agent are different.

3-8-1-2 Storage location for a RAID Manager XP configuration definition file

When you use a user-created RAID Manager XP configuration definition file in Device Manager, the configuration definition file must be stored in the following location:

In Windows:

System folder (which is indicated by the environment variable `%windir%`)

In UNIX:

`/etc` directory

3-8-1-3 Contents of a RAID Manager XP configuration definition file

When you use a RAID Manager XP configuration definition file in Device Manager, there are some limitations on the format and contents of the RAID Manager XP configuration definition file. The requirements for a RAID Manager XP configuration definition file for each parameter are shown below.

Common to all parameters

The following are limits common to all parameters:

- A line that consists only of space characters cannot be included.
- 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_MON` parameter

The following table describes the limitations for the `HORCM_MON` parameter.

Table 3-26 Requirements for a RAID Manager XP configuration definition file used in Device Manager (`HORCM_MON` parameter)

Item	Requirements
<code>ip_address</code>	Specify the IP address or name of the host. The following values are not allowed because the Device Manager server cannot resolve the host with those values: <ul style="list-style-type: none"> • Loopback IP address (127.0.0.1) • Loopback host name (localhost) • Cluster virtual IP address • Cluster virtual host name • NONE
<code>service</code>	Specify the service number by using numerical value.

`HORCM_CMD` parameter

The following table describes the limitations for the `HORCM_CMD` parameter.

Table 3-27 Requirements for a RAID Manager XP configuration definition file used in Device Manager (`HORCM_CMD` parameter)

Item	Requirements
<code>dev_name</code>	Specify this item in one of the following formats: <ul style="list-style-type: none"> • <code>\\.\PhysicalDrive#</code> (# can be any numeral) For the Device Manager agent 4.3 or earlier, this item is case sensitive. • <code>\\.\Volume{GUID}</code> The version of the Device Manager agent must be 5.0 or later. • <code>\\.\CMD-Serial#-LDEV#-Port#</code> (# can be any numeral) The version of the Device Manager agent must be 5.1 or later. The specified command device must be recognized by the host.

`HORCM_DEV` parameter

The following table describes the limitations for the `HORCM_DEV` parameter.

Table 3-28 Requirements for a RAID Manager XP configuration definition file used in Device Manager (`HORCM_DEV` parameter)

Item	Requirements
<code>dev_group</code>	Specify this item by using no more than 31 single-byte characters. A hyphen (-) cannot be specified at the beginning of a character string.
<code>dev_name</code>	Specify this item by using no more than 31 single-byte characters. A hyphen (-) cannot be specified at the beginning of a character string.
<code>MU#</code>	Specify a value from 0 to 63, or from h1 to h3. You cannot specify h0.

Character combination of `dev_group` and `dev_name` must not be duplicated.

`HORCM_LDEV` parameter

You can specify the `HORCM_LDEV` parameter when version 5.6 or later of the Device Manager agent has been installed.

⚠ CAUTION: If you use the `HORCM_LDEV` parameter to set up copy pair volumes, you can only view or delete the RAID Manager XP configuration definition file.

The following table describes the limitations for the `HORCM_LDEV` parameter.

Table 3-29 Requirements for a RAID Manager XP configuration definition file used in Device Manager (`HORCM_LDEV` parameter)

Item	Requirements
<code>dev_group</code>	Specify this item by using no more than 31 single-byte characters. A hyphen (-) cannot be specified at the beginning of a character string.
<code>dev_name</code>	Specify this item by using no more than 31 single-byte characters. A hyphen (-) cannot be specified at the beginning of a character string.
<code>Serial#</code>	Specify this item by using 10-base numbers. Hexadecimal numbers cannot be

Table 3-29 Requirements for a RAID Manager XP configuration definition file used in Device Manager (`HORCM_LDEV` parameter)

	used.
LDEV#	Specify this item by using hexadecimal numbers in <code>CU:LDEV</code> format, hexadecimal numbers, or 10-base numbers. Example: 01:04 (Hexadecimal numbers in <code>CU:LDEV</code> format) Example: 0x104 (Hexadecimal numbers) Example: 260 (10-base numbers)
MU#	Specify this item by using a value from 0 to 63, or from h1 to h3. You cannot specify h0.

Character combination of `dev_group` and `dev_name` must not be duplicated.

`HORCM_INST` parameter

The following table describes the limitations for the `HORCM_INST` parameter.

Table 3-30 Requirements for a RAID Manager XP configuration definition file used in Device Manager (`HORCM_INST` parameter)

Item	Requirements
<code>dev_group</code>	Specify this item by using no more than 31 single-byte characters. A hyphen (-) cannot be specified at the beginning of a character string.
<code>ip_address</code>	Specify the IP address or name of the host. The following values are not allowed because the Device Manager server cannot resolve the host with those values: <ul style="list-style-type: none"> • Loopback IP address (127.0.0.1) • Loopback host name (localhost) • Cluster virtual IP address • Cluster virtual host name • NONE You cannot specify this item more than once for a string specified in <code>dev_group</code> .
<code>service</code>	Specify the service number by using numerical value.

3-8-2 Reporting the information of the RAID Manager XP configuration definition file to the Device Manager server

If you created or changed a RAID Manager XP configuration definition file, you must report the information of the configuration definition file to the Device Manager server. To report the information of the configuration definition file, refresh the storage subsystem. You can refresh any of the storage subsystems whose LUs are assigned to the host that stores the configuration definition file.

3-8-3 Cautionary notes when Device Manager is used with RAID Manager XP

This subsection gives cautionary notes when Device Manager is used with RAID Manager XP.

3-8-3-1 Notes when you delete copy pairs

When you perform a delete operation of copy pairs from a client, if all the definitions of the copy pairs in a configuration definition file is deleted, that configuration definition file will be deleted. If you do not want the configuration definition file to be deleted, make a backup of the configuration definition file before you perform a delete operation.

3-8-3-2 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 RAID Manager XP configuration definition file. In this case, note the following points:

Notes on backing up the configuration definition file

In the optimization processing, the original configuration definition file `horcmXX.conf` is backed up as `horcmXX.conf.bk`. If the optimization processing is performed twice or more, the original user-created configuration definition file will be lost, because only one generation of backup file can be made. Therefore, make a backup as necessary.

Notes on a comment added to the command device definition

When the RAID Manager XP configuration definition file is optimized, the serial number of a command device is added as a comment on the line on which the command device is defined. In this case, be careful about the following:

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

3-8-3-3 Instance number and service number of RAID Manager XP used by Device Manager

When acquiring copy pair information, Device Manager creates a temporary configuration definition file in the installation destination of RAID Manager XP. This configuration definition file uses the following instance number and service number:

- Instance number: 900 to 998
- Service number: 53232 to 53330

If a number shown above is used in a user-created configuration definition file, RAID Manager XP error information might be output to the system log or event log. HP recommends that you change the number in the user-created configuration definition file to a number other than the numbers above.

4 Troubleshooting Device Manager agent operations

4-1 Acquiring error information collectively

If an error occurs in the Device Manager agent, you can acquire error information from both the Device Manager agent and the Device Manager server. In the Device Manager agent, you can use Trouble Information Collector (TIC). TIC acquires the log files and other information necessary to determine the cause of the error collectively from the Device Manager agent environment. For details about how to acquire error information in the Device Manager server, see the *HP StorageWorks Command View XP Advanced Edition software Device Manager server installation and configuration guide*.



NOTE: To use TIC, you must be a member of the Administrator group or a superuser.

The location of the TIC command differs depending upon the operating system.

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

Format

- In Windows:
`TIC.bat [-outdir location-of-resultDir-directory [-f]]`
- In Solaris, AIX, HP-UX, or Linux:
`TIC.sh [-outdir location-of-resultDir-directory [-f]]`

Arguments

- `-outdir location-of-resultDir-directory`
Specifies the location of the `resultDir` directory for storing the acquired error information. Specify the relative path from the execution directory or the absolute path. If another `resultDir` directory already exists in the specified location, a confirmation message is displayed, asking whether to delete that directory.



NOTE: If you do not specify this argument, the `resultDir` directory is created in the directory that contains the TIC command.

- `-f`
When this argument is specified and another `resultDir` directory already exists in the location specified in `-outdir`, the TIC command deletes the existing directory without displaying a confirmation message. The acquired error information files are stored in a new `resultDir` directory.



CAUTION: This argument can be specified only when the location of the directory is specified in `-outdir`.

To acquire error information collectively using TIC:

1. In the Command Prompt window, execute the TIC command.
If the `resultDir` directory already exists, the following confirmation message is displayed:

```
Output Directory [location-of-resultDir-directory\resultDir] already exists.
This program will delete [location-of-resultDir-directory\resultDir] before
working.
Continue ?
(Y)es or (N)o :
```
2. Enter `y` or `n`.
 - When you enter `y`, the command deletes the `resultDir` directory, and stores the acquired error information files in a new `resultDir` directory.

- When you enter *n*, processing is canceled.



NOTE: Even if you enter *y*, the `resultDir` directory may not be deleted. If the `resultDir` directory remains undeleted, the command creates a new directory in the specified location. The directory name is `resultDir` with an index (for example, `resultDir_1`).

A listing of acquired error information is displayed:

- Completed collection of *name-of-acquired-file: last-update-time*
...

The following termination message is displayed once the command successfully acquired error information:

- Finished successfully.

When the command terminated abnormally, the following message is displayed:

- Finished abnormally. *Message*

Figure 4-1 shows an example in which the TIC command is executed:

```

Command Prompt - TIC.bat
C:\Program Files\HDUM\HBaseAgent\bin>TIC.bat
KAIC27809-I Log collection started.
KAIC27801-I Completed collection of C:\Program Files\HDUM\HBaseAgent\bin\resultDir\HDvMFileInfo.txt. : Mon Mar 20 12:30:03 PST 2006
KAIC27801-I Completed collection of C:\Program Files\HDUM\HBaseAgent\agent\bin\Server.cmd. : Mon Mar 20 12:27:18 PST 2006
KAIC27801-I Completed collection of C:\Program Files\HDUM\HBaseAgent\agent\config\logger.properties. : Thu Jan 19 15:50:36 PST 2006
KAIC27801-I Completed collection of C:\Program Files\HDUM\HBaseAgent\agent\config\mime.properties. : Mon Oct 24 15:30:36 PDT 2005
KAIC27801-I Completed collection of C:\Program Files\HDUM\HBaseAgent\agent\config\programproductinfo.properties. : Fri Sep 17 11:09:16
KAIC27801-I Completed collection of C:\Program Files\HDUM\HBaseAgent\agent\config\server.properties. : Mon Mar 20 12:26:37 PST 2006
KAIC27801-I Completed collection of C:\Program Files\HDUM\HBaseAgent\agent\config\TIC.properties. : Sat Nov 05 00:56:30 PST 2005
KAIC27801-I Completed collection of C:\Program Files\HDUM\HBaseAgent\bin\HiScan.bat. : Mon Mar 20 12:26:35 PST 2006
KAIC27801-I Completed collection of C:\Program Files\HDUM\HBaseAgent\bin\logs\hbsaservice.log. : Mon Mar 20 12:28:12 PST 2006
KAIC27801-I Completed collection of C:\Program Files\HDUM\HBaseAgent\bin\logs\HiScan.err. : Thu Sep 02 21:11:40 PDT 2004
KAIC27801-I Completed collection of C:\Program Files\HDUM\HBaseAgent\bin\logs\HiScan.log. : Thu Sep 02 21:11:44 PDT 2004
KAIC27801-I Completed collection of C:\Program Files\HDUM\HBaseAgent\bin\logs\HiScan.msg. : Thu Sep 02 21:11:50 PDT 2004
KAIC27801-I Completed collection of C:\Program Files\HDUM\HBaseAgent\util\logs\hldu_err.log. : Thu Sep 02 21:13:48 PDT 2004
KAIC27801-I Completed collection of C:\Program Files\HDUM\HBaseAgent\mod\hdum\config\resource.properties. : Tue Nov 08 12:00:06 PST 200
KAIC27801-I Completed collection of C:\HDUM\agent_install.log. : Mon Mar 20 12:28:10 PST 2006
KAIC27801-I Completed collection of C:\hpvm\mainst.log. : Mon Mar 20 12:27:48 PST 2006
KAIC27801-I Completed collection of C:\hpvm\auit.log. : Mon Mar 20 12:24:18 PST 2006
KAIC27802-I Completed collection of OS Information to C:\Program Files\HDUM\HBaseAgent\bin\resultDir\OsInfo.txt. : Mon Mar 20 12:30:05
KAIC27802-I Completed collection of NetWork Information to C:\Program Files\HDUM\HBaseAgent\bin\resultDir\NetWorkInfo.txt. : Mon Mar 20
006
KAIC27802-I Completed collection of Version Information to C:\Program Files\HDUM\HBaseAgent\bin\resultDir\AgentVersionInfo.txt. : Mon M
PST 2006
KAIC27807-I Collection of HPVM information was started. : Mon Mar 20 12:30:05 PST 2006
KAIC27808-I Completed collection of HPVM information. : Mon Mar 20 12:30:06 PST 2006
KAIC27810-I Collection of HBaseAgent information was started. : Mon Mar 20 12:30:06 PST 2006
KAIC27811-I Completed collection of HBaseAgent information. : Mon Mar 20 12:30:08 PST 2006
KAIC27803-I Finished successfully.
Press any key to continue . . .

```

Figure 4-1 Executing TIC command

Acronyms and abbreviations

API	application programming interface
ASCII	American Standard Code for Information Interchange
CIM	Common Information Model
CLI	command line interface
CU	control unit
DNS	Domain Name Server
DSM	Device Specific Module
HBA	host bus adapter
HTML	hypertext markup language
HTTP	hypertext transfer protocol
JFS	Journaled File System
JRE	Java Runtime Environment or Java 2 Runtime Environment
LU	logical unit
LUN	logical unit number, logical unit
LVM	Logical Volume Manager
MPIO	MultiPath I/O
NIC	network interface card
NTFS	NT File System
OS	operating system
RTE	run time environment
SCSI	small computer systems interface
SDK	software development kit
SNIA	Storage Networking Industry Association
SP	service pack
TCP/IP	transmission control protocol/internet protocol
UFS	UNIX File System
TIC	trouble information collector
VCS	VERITAS Cluster Server
VxVM	VERITAS Volume Manager
WOW64	Windows on Windows 64
WWN	worldwide name
XML	extensible markup language

Index

C

Commands
hldutil, 11

D

Device Manager agent
supported storage subsystem, 18
document
providing feedback, 10

H

hbsasrv
restarting, 42
help
obtaining, 9
HiScan
hldutil command syntax, 45
hldutil command, 11
HP
Subscriber's choice for business web site, 9
technical support, 9
web sites, 9

M

MPIO, 21

O

Overview
Device Manager agent, 11
Webserver, 11

P

property file
hldutil.properties file, 54
logger.properties file, 53
programproductinfo.properties file, 54

server.properties file, 50

S

server.agent.maxMemorySize, 51
setting up, 28
execution period for the HiScan command, 29
server information, 28
Subscriber's choice
HP, 9
Sun StorEdge Traffic Manager, 21

T

technical support
HP, 9
TIC, 59
troubleshooting
hldutil.properties file, 54
logger.properties file, 54
programproductinfo.properties file, 54
server.properties file, 50, 51, 52, 53

U

Uninstalling Device Manager agent, 31
for AIX, 32
for HP-UX, 32
for Linux, 32
for Solaris, 32
for Windows, 32

V

VxVM, 54

W

web sites
HP, 9
Windows
changing execution user, 36