HITACHI
DATA SYSTEMS

HiCommand® Provisioning Manager Server Installation and Configuration Guide

MK-93HC038-12

Trademarks

Solaris, Solstice DiskSuite, and Sun are trademarks of Sun Microsystems, Inc. in the United States and other countries.

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

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

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

Veritas, and Veritas Storage Foundation are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries.

Windows, Windows Server, and Windows Vista are registered trademarks of Microsoft Corp. in the U.S. and other countries.

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

Notice of Export Controls

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

Document Revision Level

Revision	Date	Description
MK-93HC038-00	September 2004	Initial Release
MK-93HC038-01	October 2004	Revision 1, supersedes and replaces MK-93HC038-00
MK-93HC038-02	March 2005	Revision 2, supersedes and replaces MK-93HC038-01
MK-93HC038-03	June 2005	Revision 3, supersedes and replaces MK-93HC038-02
MK-93HC038-04	July 2005	Revision 4, supersedes and replaces MK-93HC038-03
MK-93HC038-05	December 2005	Revision 5, supersedes and replaces MK-93HC038-04
MK-93HC038-06	February 2006	Revision 6, supersedes and replaces MK-93HC038-05
MK-93HC038-07	June 2006	Revision 7, supersedes and replaces MK-93HC038-06
MK-93HC038-08	November 2006	Revision 8, supersedes and replaces MK-93HC038-07
MK-93HC038-09	February 2007	Revision 9, supersedes and replaces MK-93HC038-08
MK-93HC038-10	June 2007	Revision 10, supersedes and replaces MK-93HC038-09
MK-93HC038-11	October 2007	Revision 11, supersedes and replaces MK-93HC038-10
MK-93HC038-12	January 2008	Revision 12, supersedes and replaces MK-93HC038-11

Preface

This manual describes how to install and configure the environment settings for HiCommand® Provisioning Manager. In this manual, HiCommand Provisioning Manager is abbreviated to Provisioning Manager.

The intended audience is those who use Provisioning Manager to operate or manage a system that uses a storage subsystem (magnetic disk array unit). The readers of this manual should have the following capabilities:

- A basic knowledge of SANs (Storage Area Networks),
- Knowledge of HiCommand Device Manager installation, user setup, resource group setup, volume (LDEV) creation, and logical group creation,
- A basic knowledge of the Windows®, Solaris™ or Linux® operating system on which Provisioning Manager and Device Manager run, and
- A basic knowledge of the Windows, Solaris, AIX®, or Linux operating system on which the Device Manager agent runs.

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

Software Version

This document revision applies to HiCommand Provisioning Manager version 5.9.

Convention for Storage Capacity Values

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

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

Referenced Documents

Manuals related to this manual are listed below. See these manuals when necessary:

- *HiCommand Provisioning Manager Error Codes*, MK-93HC117
- *HiCommand Device Manager Command Line Interface (CLI) User's Guide*, MK-1HC007
- *HiCommand Device Manager Agent Installation Guide*, MK-92HC019
- *HiCommand Device Manager Server Installation and Configuration Guide*, MK-92HC002
- *HiCommand Device Manager Error Codes*, MK-92HC016

When Dynamic Link Manager is installed on the host:

- *HiCommand Dynamic Link Manager for Windows User's Guide*, MK-92DLM129
- *HiCommand Dynamic Link Manager for AIX User's Guide*, MK-92DLM111
- *HiCommand Dynamic Link Manager for Solaris User's Guide*, MK-92DLM114
- *HiCommand Dynamic Link Manager for HP-UX User's Guide*, MK-92DLM112
- *HiCommand Dynamic Link Manager for Linux User's Guide*, MK-92DLM113

Readme and Release Notes Contents

These files can be found on the installation CD. They contain requirements and notes for use of HiCommand Provisioning Manager that may not be fully described in the manual. Be sure to review these files before installing HiCommand Provisioning Manager.

Comments

Please send us your comments on this document. Make sure to include the document title, number, and revision. Please refer to specific section(s) and paragraph(s) whenever possible.

- **E-mail:** doc.comments@hds.com
- **Fax:** 858-695-1186
- **Mail:**
  Technical Writing, M/S 35-10
  Hitachi Data Systems
  10277 Scripps Ranch Blvd.
  San Diego, CA 92131

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

Contents

List of Figures

List of Tables

Chapter 1 Reviewing Components and Requirements for Provisioning Manager

This chapter describes the features and system configuration of Provisioning Manager.

- Provisioning Manager Features (see section 1.1)
- Provisioning Manager Components (see section 1.2)
- System Requirements (see section 1.3)
- Required Programs (see section 1.4)
- Related Program Products (see section 1.5)
- Software Products that Cannot Be Combined (see section 1.6)

1.1 Provisioning Manager Features

Every year, the storage subsystems that support corporate systems and storage service providers (SSPs) increase enormously in size and capability. Additionally, the capacities and numbers of units required by users continue to increase. Consequently, there is a stronger demand to reduce the costs associated with storage management.

In answer to these requirements, Provisioning Manager has been designed to handle a variety of storage subsystems while simplifying storage operation management and reducing associated costs. The features of Provisioning Manager's storage operation management are explained in the following sections.

1.1.1 Managing Various Storage Subsystems as a Storage Pool

Provisioning Manager provides the functionality to integrate and manage various models and types of storage subsystems as a single, logical *storage pool*. In Provisioning Manager, a *storage pool* refers to a managed data storage area that resides on a set of storage subsystems. A storage pool is a collection of volumes (LUs). You can use Device Manager's All Storage and My Storage functionalities to place the storage pools into hierarchies and manage a storage pool for each resource group.

Provisioning Manager presents the volumes associated with each resource group as a single, logical volume, which enables these volumes to be managed without having to be aware where the volumes actually reside. This reduces the user workload required to understand the usage conditions for each volume, and to maintain the various volumes. For details about resource groups and All Storage and My Storage functionality, see the Device Manager online Help.

Figure 1.1 shows a storage pool example.

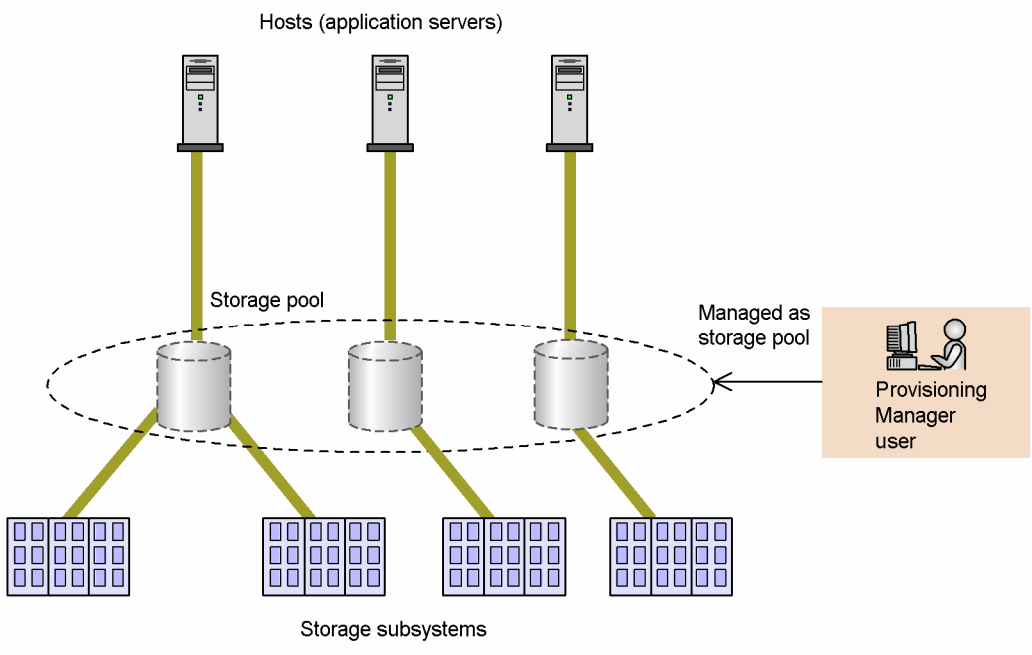

Figure 1.1 Storage Pool Example

To search volumes in a storage pool, you can pre-define search conditions for volume allocation. These pre-defined conditions are called a *provisioning plan*. Specifying a provisioning plan when you analyze a storage pool or display a list of volumes enables you to narrow down and display only those volumes that are relevant when searching a large number of volumes.

1.1.2 Managing Multiple File Systems and Device Files from a Single GUI

Provisioning Manager provides the means to manage different types of hosts by using a single, consistent graphical user interface. This enables you to efficiently manage hosts without having to be aware of functional differences among them.

With Provisioning Manager, you can view the information required to manage storage subsystem operations, including information such as the configuration of the host volumes for file systems and device files, data paths configured from HBA WWNs or iSCSI names, storage subsystem ports, and storage subsystem volumes. Moreover, by using volumes from a storage pool that is allocated to various hosts, you can also create and remove file systems and device files.

Figure 1.2 illustrates the settings for storage subsystems and hosts that use Provisioning Manager.

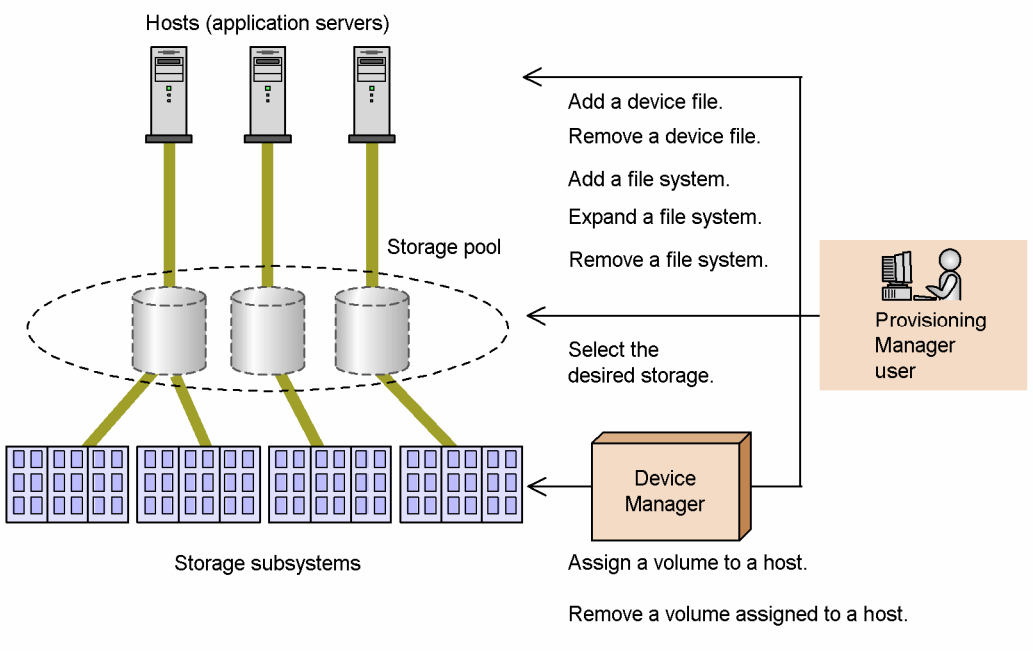

Figure 1.2 Storage Subsystems and Host Setup

1.2 Provisioning Manager Components

Figure 1.3 illustrates the principal components of Provisioning Manager.

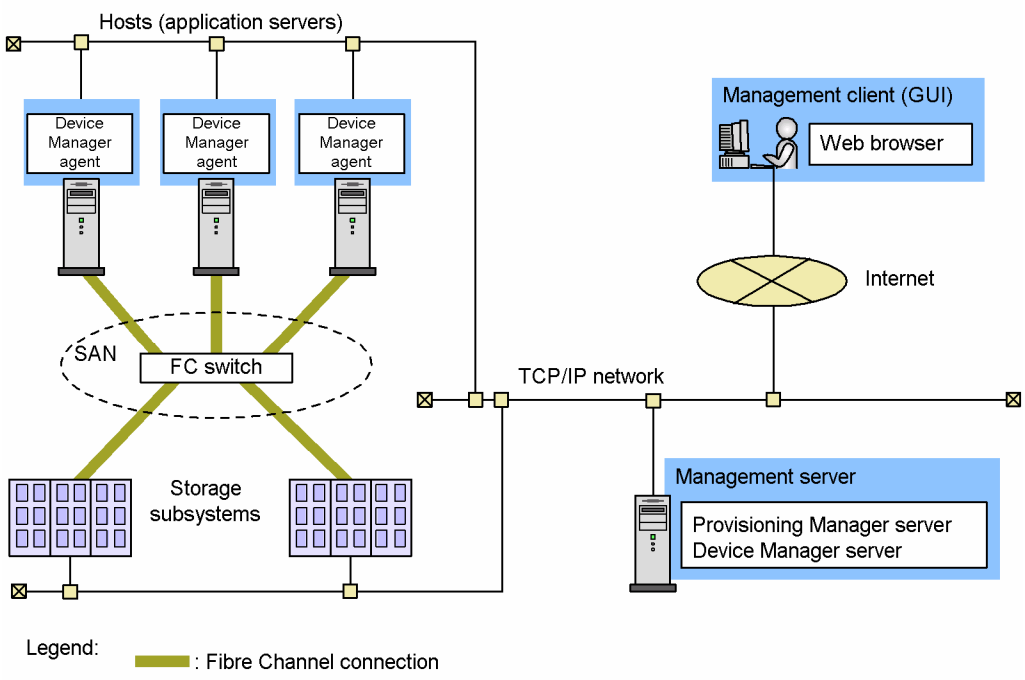

Figure 1.3 Provisioning Manager Components

- The Provisioning Manager Server forms storage pools from storage subsystems and allocates volumes to hosts. It issues instructions to the Device Manager agent installed on each host, allowing the user to create or delete file systems and device files, and to expand file systems. For more information about Device Manager agent, see the *HiCommand Device Manager Agent User's Guide*.
- The Provisioning Manager client allows users to access the server using a Web browser. For details about using the graphical user interface (GUI), see the Provisioning Manager online Help.

1.3 System Requirements

This section describes the components that are required for Provisioning Manager.

1.3.1 Hardware Configuration

You will need the following components:

- Host (application server)
- Storage subsystem
- Management server
- Management client

The subsystem requirements are the same as for Device Manager, which is required to operate Provisioning Manager. For details, see the *HiCommand Device Manager Server Installation and Configuration Guide*.

Note: Setting and reference operations for mainframe volumes are not supported.

Figure 1.4 illustrates a configuration where the management server also acts as the management client.

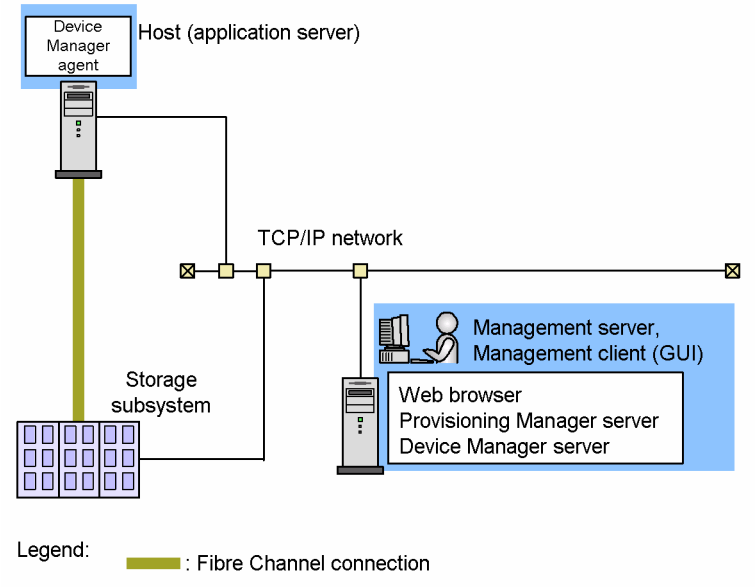

Figure 1.4 Minimum Hardware Configuration (Example 1)

Figure 1.5 illustrates a configuration where the management client is set up in another system. The management client can connect either to a TCP/IP network (intranet) or via the Internet.

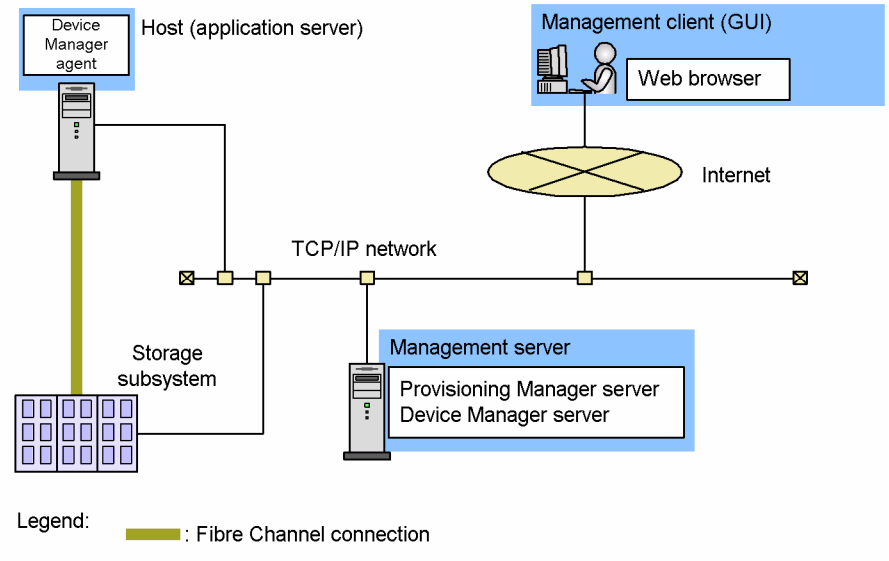

Figure 1.5 Minimum Hardware Configuration (Example 2)

Figure 1.6 illustrates a configuration with multiple storage subsystems and hosts. Note that there is no need to connect hosts in which no Device Manager agent is installed on a TCP/IP network.

Important: If your configuration includes multiple storage subsystems, be sure to assign a unique name to each storage subsystem. Duplicate subsystem names are not supported.

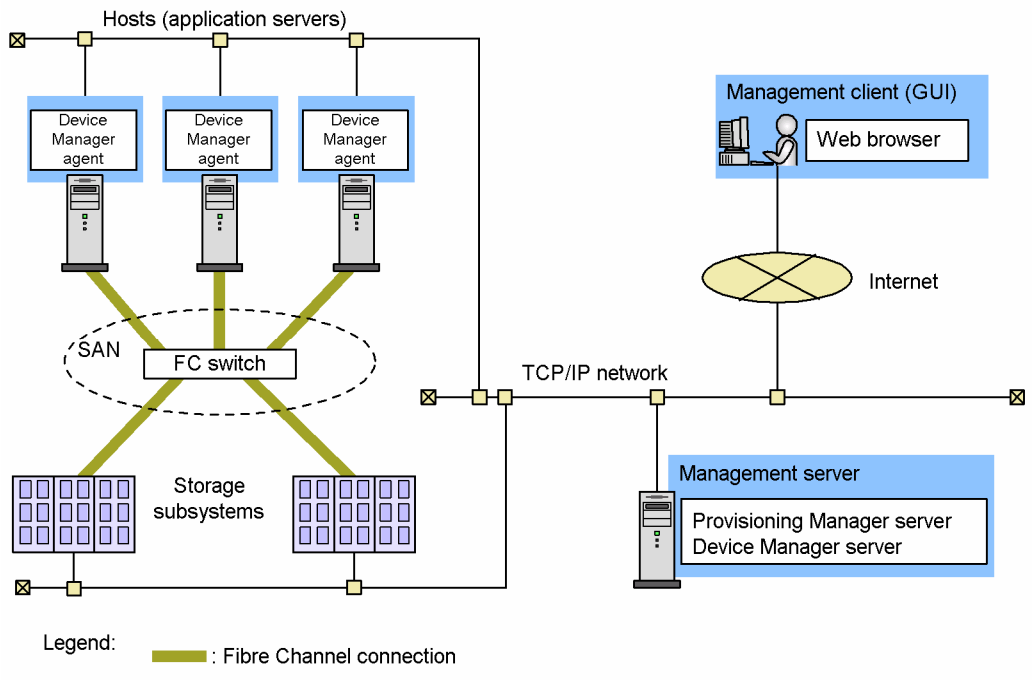

Figure 1.6 Hardware Configuration with Multiple Subsystems and Multiple Hosts

Caution: Make sure that you specify a unique port address for each port of the storage devices in the same zone. If the same port addresses exist in the same zone, the OS cannot recognize the ports and may not recognize the device files. In such a state, if you add a device file, add a file system, or expand a file system from Provisioning Manager, the device file cannot be recognized and an error occurs.

1.3.2 Server Operating System Requirements

Provisioning Manager's management server shares the same machine as Device Manager's management server. For details about the OS requirements for management servers, see the *HiCommand Device Manager Server Installation and Configuration Guide*.

1.3.3 Operating Systems Supported for Hosts

Table 1.1 lists the host OSs that are required for Provisioning Manager.

Table 1.1 Required Host OSs

OS	Version
Windows 2000[#1, #2]	Windows 2000 Professional SP4 Windows 2000 Server SP4 Windows 2000 Advanced Server SP4 Windows 2000 Datacenter Server SP4
Windows Server 2003 (x86)[#1]	Windows Server 2003, Standard Edition Windows Server 2003, Standard Edition SP1 Windows Server 2003, Standard Edition SP2 Windows Server 2003, Enterprise Edition Windows Server 2003, Enterprise Edition SP1 Windows Server 2003, Enterprise Edition SP2 Windows Server 2003, Datacenter Edition Windows Server 2003, Datacenter Edition SP1 Windows Server 2003, Datacenter Edition SP2
Windows Server 2003 (IPF)[#1]	Windows Server 2003, Enterprise Edition for Itanium-based Systems Windows Server 2003, Enterprise Edition for Itanium-based Systems SP1 Windows Server 2003, Enterprise Edition for Itanium-based Systems SP2 Windows Server 2003, Datacenter Edition for Itanium-based Systems Windows Server 2003, Datacenter Edition for Itanium-based Systems SP1 Windows Server 2003, Datacenter Edition for Itanium-based Systems SP2
Windows Server 2003 x64 Edition[#1]	Windows Server 2003, Standard x64 Edition Windows Server 2003, Standard x64 Edition SP2 Windows Server 2003, Enterprise x64 Edition Windows Server 2003, Enterprise x64 Edition SP2 Windows Server 2003, Datacenter x64 Edition Windows Server 2003, Datacenter x64 Edition SP2
Windows Server 2003 R2 (x86)[#1]	Windows Server 2003 R2, Standard Edition Windows Server 2003 R2, Standard Edition SP2 Windows Server 2003 R2, Enterprise Edition Windows Server 2003 R2, Enterprise Edition SP2 Windows Server 2003 R2, Datacenter Edition Windows Server 2003 R2, Datacenter Edition SP2
Windows Server 2003 R2 x64 Edition[#1]	Windows Server 2003 R2, Standard x64 Edition Windows Server 2003 R2, Standard x64 Edition SP2 Windows Server 2003 R2, Enterprise x64 Edition Windows Server 2003 R2, Enterprise x64 Edition SP2 Windows Server 2003 R2, Datacenter x64 Edition Windows Server 2003 R2, Datacenter x64 Edition SP2

OS	Version
Windows Server 2008	Windows Server 2008 Standard 32-bit Windows Server 2008 Enterprise 32-bit Windows Server 2008 Datacenter 32-bit Windows Server 2008 Standard Windows Server 2008 Enterprise Windows Server 2008 Datacenter Windows Server 2008 for Itanium-based Systems
Solaris	Solaris 8 (SPARC edition) [#3] Solaris 9 (SPARC edition) [#4] Solaris 10 (SPARC edition) [#5] Solaris 10 (x64 edition)[#6]
AIX	AIX 5.2 AIX 5.3 AIX 6.1[#7]
Linux (x86)	Red Hat Enterprise Linux AS 3 Update 0[#8] Red Hat Enterprise Linux ES 3 Update 0[#8] Red Hat Enterprise Linux AS 3 Update 3[#8] Red Hat Enterprise Linux ES 3 Update 3[#8] Red Hat Enterprise Linux AS 3 Update 4[#8] Red Hat Enterprise Linux ES 3 Update 4[#8] Red Hat Enterprise Linux AS 3 Update 6 Red Hat Enterprise Linux ES 3 Update 6 Red Hat Enterprise Linux AS 4 Update 1 Red Hat Enterprise Linux ES 4 Update 1 Red Hat Enterprise Linux AS 4 Update 3 Red Hat Enterprise Linux ES 4 Update 3 Red Hat Enterprise Linux AS 4 Update 4 Red Hat Enterprise Linux ES 4 Update 4 Red Hat Enterprise Linux AS 4.5 Red Hat Enterprise Linux ES 4.5 Red Hat Enterprise Linux 5 Advanced Platform Red Hat Enterprise Linux 5 server
Linux (x64)	Red Hat Enterprise Linux AS 4 Update 1 Red Hat Enterprise Linux ES 4 Update 1 Red Hat Enterprise Linux AS 4 Update 3 Red Hat Enterprise Linux ES 4 Update 3 Red Hat Enterprise Linux AS 4 Update 4 Red Hat Enterprise Linux ES 4 Update 4 Red Hat Enterprise Linux AS 4.5 Red Hat Enterprise Linux ES 4.5 Red Hat Enterprise Linux 5 Advanced Platform Red Hat Enterprise Linux 5 server

OS	Version
Linux (IPF)	Red Hat Enterprise Linux AS 4 Update 1 Red Hat Enterprise Linux ES 4 Update 1 Red Hat Enterprise Linux AS 4 Update 3 Red Hat Enterprise Linux ES 4 Update 3 Red Hat Enterprise Linux AS 4 Update 4 Red Hat Enterprise Linux ES 4 Update 4 Red Hat Enterprise Linux AS 4.5 Red Hat Enterprise Linux ES 4.5 Red Hat Enterprise Linux 5 Advanced Platform Red Hat Enterprise Linux 5 server
HP-UX	HP-UX 11i v1 (PA-RISC 64 bits) September 2004 version or later of HP-UX 11i v2 (PA-RISC and IPF) HP-UX 11i v3 (PA-RISC and IPF)

OS	Version

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

- For Windows 2000: English, French, German, Italian, Spanish, Simplified Chinese, Traditional Chinese, Korean, Japanese, Portuguese, Brazilian (Portuguese Brazilian), Danish, and Swedish
- For Windows Server 2003 (x86) , or Windows Server 2003 R2 : English, French, German, Italian, Spanish, Simplified Chinese, Traditional Chinese, Korean, Japanese, Portuguese, Brazilian (Portuguese Brazilian), and Swedish
- For Windows Server 2003 (IPF), or Windows Server 2003 x64 Edition : English and Japanese

Host configuration cannot be executed in the following two cases even if the operating system is one of the above language versions:

- When the Multilingual User Interface Pack has been applied.
- When the language settings of the system have been changed. Host, file system, and device file settings can be viewed from the server no matter what language version of Windows is on the agent host.

#2 If the host OS is Windows 2000, you must install the `diskpart.exe` command line utility provided by Microsoft in the following folder: *system-installation-directory*`\system32`

#3 If the host OS is Solaris 8 (SPARC edition), you must apply the following OS patch: 121972-04

#4 If the host OS is Solaris 9 (SPARC edition), you must apply the following OS patch: 118335-08

#5 If the host OS is Solaris 10 (SPARC edition), do not apply the following OS patches:

- 127111-02
- 127111-03

#6 If the host OS is Solaris 10 (x64 edition), do not apply the following OS patches:

- 127112-02
- 127112-03

Note that only the Sun Fire x64 server family is supported by the host. Set the kernel mode to the 64-bit kernel mode.

#7 The environments where the Secure by Default function is enabled are not supported.

#8 The following limitations apply when the host OS is Red Hat Enterprise Linux AS/ES 3 Update 0, Update 3, or Update 4:

- Do not perform the following operations while performing a host setting operation (creating or deleting a device file; or creating, expanding, or deleting a file system) by using the Provisioning Manager client:

  Updating host information in the Provisioning Manager client

  Updating host information in the Device Manager client

  Starting the Device Manager agent

  Executing the Device Manager agent `HiScan` command or `hldutil` command

  Executing disk control-related commands (such as `blockdev`)
- Do not perform the following operations while updating host information in the Provisioning Manager client:

  Setting up a host by using the Provisioning Manager client

  Executing the Dynamic Link Manager `dlmcfgmgr` command

  Executing disk control-related commands (such as `blockdev`)
- Do not perform the following operations while starting the Device Manager agent:

  Setting up a host using the Provisioning Manager client

  Executing the Dynamic Link Manager `dlmcfgmgr` command

  Executing disk control-related commands (such as `blockdev`)
- Do not perform the following operations concurrently with the Device Manager agent `HiScan` command or `hldutil` command:

  Setting up a host using the Provisioning Manager client.

  Executing the Dynamic Link Manager `dlmcfgmgr` command

  Executing disk control-related commands (such as `blockdev`)
- Do not perform automatic execution of the Device Manager agent `HiScan` command:

  If automatic execution of the `HiScan` command has been specified, clear the setting. For details about how to do this, see the *HiCommand Device Manager Agent Installation Guide*.

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

1.3.4 Supported Host File Systems

The type of file systems that can be used differs depending on the host operating system. Table 1.2 shows the supported host file system types.

Table 1.2 Supported File System Types

Host OS	File system that can be used	Expandable or not	Remarks
Windows	NTFS	Yes[#1, #2]	Standard OS file system
	FAT[#3]	No	Standard OS file system
	FAT32[#3]	No	Standard OS file system
Solaris	UFS	No	Standard OS file system
	Veritas File System	Yes[#1, #4]	▪ For Solaris 8: VERITAS File System 3.5 VERITAS File System 4.0 ▪ For Solaris 9: VERITAS File System 3.5 VERITAS File System 4.0 Veritas File System 5.0 ▪ For Solaris 10 (SPARC edition): Veritas File System 5.0 ▪ For Solaris 10 (x64 edition): VERITAS File System 4.1
AIX	JFS	Yes[#1]	Standard OS file system
Linux	ext2, ext3	Yes[#1, #5]	Standard OS file system
HP-UX	Veritas File System[#6]	Yes[#1, #7]	▪ For HP-UX 11i v1: VERITAS File System 3.5 is supported. To enable VERITAS File System 3.5, install a version of Software Pack (Optional HP-UX 11i v1 Core Enhancements) that was released in or after December 2002. ▪ For versions released before the December 2005 version of HP-UX 11i v2: VERITAS File System 3.5, which comes standard with the OS, is supported. ▪ For the December 2005 and later versions of HP-UX 11i v2: VERITAS File System 4.1, which comes standard with the OS, is supported. ▪ For HP-UX 11i v3: VERITAS File System 4.1, which comes standard with the OS, is supported.

Host OS	File system that can be used	Expandable or not	Remarks
	HFS#3	No	Standard OS file system

Legend:

Yes: Expandable

No: Not expandable

#1 Operations for expanding a file system can be performed only when the file system is mounted.

#2 A dynamic disk is required.

#3 File systems can only be displayed.

#4 Veritas Volume Manager is required. Veritas File System is supported only when the Veritas Volume Manager version is the same as the Veritas File System version.

#5 A file system cannot be expanded in the online mode because it is unmounted during expansion. When a file system is expanded, stop jobs.

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

#7 A file system can be expanded in the online mode if a Device Manager agent version 5.1 or later and HP OnlineJFS are installed on the host. When you install HP OnlineJFS, make sure you do the following:

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

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

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

If a Device Manager agent version earlier than 5.1 is installed on the host, or HP OnlineJFS is not installed on the host, the file system is unmounted during expansion, so it cannot be expanded in the online mode. When a file system is expanded, stop all jobs.

1.3.5 Supported OSs and Web Browsers for Management Clients

The Provisioning Manager graphical user interface (GUI) is available with a Web browser of a management client. For details about the OSs and web browsers required for management clients, see the Provisioning Manager online Help

1.3.6 Memory and Disk Space Requirements

Table 1.3 lists the memory and disk space requirements for Provisioning Manager.

Table 1.3 Memory and Disk Space Requirements

Machine	Program	Memory Requirements	Disk Space Requirements	Remarks
Management server	Provisioning Manager	500 MB	350 MB The value, when about 10 storage subsystems are connected.	Extra space is required for running the Device Manager server, which is a prerequisite program for the Provisioning Manager server.
Host	The Device Manager agent (The host management functionality of Provisioning Manager is contained in the Device Manager agent.)	See the Device Manager release notes.		When the host OS is HP-UX, in the `/etc/lvmconf` directory, LVM creates a backup file for the configuration information about volume groups. Therefore, to create a volume group by using the host management functionality of Provisioning Manager, a maximum of 500 MB of free disk space (when 255 volume groups are created) is additionally required under `/etc/lvmconf`.
Management client	The GUI of Provisioning Manager	50 MB per browser	N/A (The GUI does not need to be installed.)	N/A

1.4 Required Programs

Table 1.4 lists the Device Manager agent versions that Provisioning Manager requires for each host OS.

Table 1.4 lists required versions of the Device Manager agent for each host OS

Table 1.4 Required Versions of the Device Manager Agent.

OS	Version of OS	Version of the Device Manager agent
Windows 2000	Windows 2000 Professional SP4 Windows 2000 Server SP4 Windows 2000 Advanced Server SP4 Windows 2000 Datacenter Server SP4	4.0.0-05 or later
Windows Server 2003 (x86)	Windows Server 2003, Standard Edition Windows Server 2003, Enterprise Edition Windows Server 2003, Datacenter Edition	4.0.0-05 or later
	Windows Server 2003, Standard Edition SP1 Windows Server 2003, Enterprise Edition SP1 Windows Server 2003, Datacenter Edition SP1	4.1.0-01 or later
	Windows Server 2003, Standard Edition SP2 Windows Server 2003, Enterprise Edition SP2 Windows Server 2003, Datacenter Edition SP2	5.6.0-00 or later
Windows Server 2003 (IPF)	Windows Server 2003, Enterprise Edition for Itanium-based Systems Windows Server 2003, Enterprise Edition for Itanium-based Systems SP1 Windows Server 2003, Datacenter Edition for Itanium-based Systems Windows Server 2003, Datacenter Edition for Itanium-based Systems SP1	5.0.0-00 or later
	Windows Server 2003, Enterprise Edition for Itanium-based Systems SP2 Windows Server 2003, Datacenter Edition for Itanium-based Systems SP2	5.6.0-00 or later
Windows Server 2003 x64 Edition	Windows Server 2003, Standard x64 Edition Windows Server 2003, Enterprise x64 Edition Windows Server 2003, Datacenter x64 Edition	4.3.0-01 or later
	Windows Server 2003, Standard x64 Edition SP2 Windows Server 2003, Enterprise x64 Edition SP2 Windows Server 2003, Datacenter x64 Edition SP2	5.6.0-00 or later

OS	Version of OS	Version of the Device Manager agent
Windows Server 2003 R2	Windows Server 2003 R2, Standard Edition Windows Server 2003 R2, Enterprise Edition Windows Server 2003 R2, Datacenter Edition Windows Server 2003 R2, Standard x64 Edition Windows Server 2003 R2, Enterprise x64 Edition Windows Server 2003 R2, Datacenter x64 Edition	5.1.0-00 or later
	Windows Server 2003 R2, Standard Edition SP2 Windows Server 2003 R2, Enterprise Edition SP2 Windows Server 2003 R2, Datacenter Edition SP2 Windows Server 2003 R2, Standard x64 Edition SP2 Windows Server 2003 R2, Enterprise x64 Edition SP2 Windows Server 2003 R2, Datacenter x64 Edition SP2	5.6.0-00 or later
Windows Server 2008	Windows Server 2008 Standard 32-bit Windows Server 2008 Enterprise 32-bit Windows Server 2008 Datacenter 32-bit Windows Server 2008 Standard Windows Server 2008 Enterprise Windows Server 2008 Datacenter Windows Server 2008 for Itanium-based Systems	5.9.0-00 or later
Solaris	Solaris 8 Solaris 9	4.0.0-05 or later
	Solaris 10 (SPARC edition)	4.1.0-01 or later
	Solaris 10 (x64 edition)	5.8.0-00 or later
AIX	AIX 5.2 AIX 5.3	4.0.0-05 or later
	AIX 6.1	5.9.0-00 or later
Linux (x86)	Red Hat Enterprise Linux AS/ES 3 Update 0 Red Hat Enterprise Linux AS/ES 3 Update 3 Red Hat Enterprise Linux AS/ES 3 Update 4	4.1.0-01 or later
	Red Hat Enterprise Linux AS/ES 3 Update 6 Red Hat Enterprise Linux AS/ES 4 Update 1	5.1.0-00 or later
	Red Hat Enterprise Linux AS/ES 4 Update 3	5.5.0-00 or later
	Red Hat Enterprise Linux AS/ES 4 Update 4 Red Hat Enterprise Linux AS/ES 4.5 Red Hat Enterprise Linux 5	5.9.0-00 or later
Linux (x64)	Red Hat Enterprise Linux AS/ES 4 Update 1 Red Hat Enterprise Linux AS/ES 4 Update 3 Red Hat Enterprise Linux AS/ES 4 Update 4 Red Hat Enterprise Linux AS/ES 4.5 Red Hat Enterprise Linux 5	5.9.0-00 or later

OS	Version of OS	Version of the Device Manager agent
Linux (IPF)	Red Hat Enterprise Linux AS/ES 4 Update 1	5.0.0-00 or later
	Red Hat Enterprise Linux AS/ES 4 Update 3	5.5.0-00 or later
	Red Hat Enterprise Linux AS/ES 4 Update 4	5.7.0-00 or later
	Red Hat Enterprise Linux AS/ES 4.5 Red Hat Enterprise Linux 5	5.9.0-00 or later
HP-UX	HP-UX 11i v1 HP-UX 11i v2	4.3.0-01 or later
	HP-UX 11i v3	5.6.0-00 or later

For more information on the Device Manager agent, see the *HiCommand Device Manager Agent Installation Guide*.

Note: To create, expand, and delete file systems and device files on the host, and to use host management functions (including file system and device file management), you must install the Device Manager agent, which is a component of Device Manager, on each host. Installing the Device Manager agent onto a host also installs the Provisioning Manager agent.

Caution: Do not uninstall the Provisioning Manager agent by itself, because Device Manager and Provisioning Manager share a common agent. If you do, reinstall the Device Manager agent. After the Device Manager agent is installed on a Windows host, **HiCommand Provisioning Manager-agent** is displayed in **Add/Remove Programs** in the **Control Panel**.

1.5 Related Program Products

This section describes programs related to Provisioning Manager.

1.5.1 Path Manager

Path redundancy between a host port and storage subsystem port improves system reliability and availability. Path redundancy requires a path manager. Provisioning Manager supports the following path managers:

- Dynamic Link Manager
- PV-link (when the host OS is HP-UX)
- MPIO (when the host OS is HP-UX 11i v3)

For LUs managed by another path manager, Provisioning Manager cannot be used to perform a host setting operation, and there are GUI-based display limitations. For details, see the Provisioning Manager online Help.

1.5.1.1 Dynamic Link Manager

HDLM must be installed on each host but the version to be installed differs depending on the host operating system. Table 1.5 shows the versions of Dynamic Link Manager that are supported by Provisioning Manager. Note that Table 1.5 includes only OSs that support Dynamic Link Manager.

Table 1.5 Product Names and Versions of Dynamic Link Manager

OS	Program product name and version
Windows 2000	For Windows 2000 SP4: Dynamic Link Manager 05-02 to 5.9.4
Windows Server 2003	For Windows Server 2003: Dynamic Link Manager 05-02 to 5.9.4 For Windows Server 2003 SP1: Dynamic Link Manager 5.6 to 5.9.4 For Windows Server 2003 SP2 Dynamic Link Manager 5.9.1 to 5.9.4
Windows Server 2003 x64 Edition	For Windows Server 2003 x64 Edition Dynamic Link Manager 5.7 to 5.9.4 For Windows Server 2003 x64 Edition SP2 Dynamic Link Manager 5.9.1 to 5.9.4

OS	Program product name and version
Windows Server 2003 (IPF)	For Windows Server 2003 (IPF): Dynamic Link Manager 05-02 to 5.9.4 For Windows Server 2003 (IPF) SP1: Dynamic Link Manager 5.6 to 5.9.4 For Windows Server 2003 (IPF) SP2 Dynamic Link Manager 5.9.1 to 5.9.4
Windows Server 2003 R2	For Windows Server 2003 R2 Dynamic Link Manager 5.8 to 5.9.4 For Windows Server 2003 R2 SP2 Dynamic Link Manager 5.9.1 to 5.9.4
Windows Server 2003 R2 x64 Edition	For Windows Server 2003 R2 x64 Edition Dynamic Link Manager 5.8 to 5.9.4 For Windows Server 2003 R2 x64 Edition SP2 Dynamic Link Manager 5.9.1 to 5.9.4
Windows Server 2008	For Windows Server 2008 Dynamic Link Manager 5.9.4
Solaris	For VERITAS Volume Manager 3.5 on Solaris 8 or Solaris 9: Dynamic Link Manager 04-01-/B Dynamic Link Manager 05-02 to 5.9.4 For VERITAS Volume Manager 4.0 on Solaris 8 or Solaris 9: Dynamic Link Manager 5.4.1 to 5.9.4
AIX	For AIX 5.2: Dynamic Link Manager 05-02 to 5.9.4 For AIX 5.3: Dynamic Link Manager 5.4.1 to 5.9.4 For AIX 6.1: Dynamic Link Manager 5.9.4
Linux	For Red Hat Enterprise Linux AS/ES 3 Update 3: Dynamic Link Manager 5.4.2 to 5.9.4 For Red Hat Enterprise Linux AS/ES 3 Update 4: Dynamic Link Manager 5.6 to 5.9.4 For Red Hat Enterprise Linux AS/ES 3 Update 6: Dynamic Link Manager 5.7.1 to 5.9.4 For Red Hat Enterprise Linux AS/ES 4 Update 1: Dynamic Link Manager 5.7.0-02 to 5.9.4 For Red Hat Enterprise Linux AS/ES 4 Update 3: Dynamic Link Manager 5.8.1 to 5.9.4 For Red Hat Enterprise Linux AS/ES 4 Update 4: Dynamic Link Manager 5.9.1 to 5.9.4 For Red Hat Enterprise Linux AS/ES 4.5: Dynamic Link Manager 5.9.3 to 5.9.4 For Red Hat Enterprise Linux 5: Dynamic Link Manager 5.9.3 to 5.9.4

OS	Program product name and version
HP-UX	For HP-UX 11i v1 or HP-UX 11i v2: Dynamic Link Manager 5.6.1 to 5.9.4

For details about the Dynamic Link Manager, see the *HiCommand Dynamic Link Manager User's Guide*.

1.5.1.2 PV-link

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

1.5.1.3 MPIO

In HP-UX 11i v3 you can use Provisioning Manager to perform a host setting operation for LUs managed by MPIO.

1.5.2 Volume Manager

To use Provisioning Manager to perform operations on file systems or device files (create, expand, or delete), you must have volume management software (a volume manager). A Volume Manager is required on each host. However, if the host OS is Solaris, you can use Provisioning Manager to create and delete file systems and device files, even without a volume manager.

Table 1.6 shows the product names and versions of supported volume managers.

Table 1.6 Supported Volume Managers

Host OS	Volume Manager
Windows	Dynamic (comes standard with the OS) Basic (comes standard with the OS) #1

Host OS	Volume Manager
Solaris	For Solaris 8: VERITAS Volume Manager 3.5#2 VERITAS Volume Manager 4.0#2 SDS#3 For Solaris 9: VERITAS Volume Manager 3.5#2 VERITAS Volume Manager 4.0#2 Veritas Volume Manager 5.0#2 SVM#4 For Solaris 10 (SPARC edition): Veritas Volume Manager 5.0#2 SVM#4 For Solaris 10 (x64 edition): VERITAS Volume Manager 4.1#2 SVM#4
AIX	LVM (comes standard with the OS)
Linux	For Red Hat Enterprise Linux AS/ES 3: LVM (comes standard with the OS) For Red Hat Enterprise Linux AS/ES 4: LVM2 (comes standard with the OS) For Red Hat Enterprise Linux AS/ES 4.5: LVM2 (comes standard with the OS) For Red Hat Enterprise Linux 5: LVM2 (comes standard with the OS)
HP-UX	For HP-UX 11i v1 and versions released before the December 2005 version of HP-UX 11v2: LVM (comes standard with the OS) VERITAS Volume Manager 3.5 (comes standard with the OS) #5 For the December 2005 and later versions of HP-UX 11i v2: LVM (comes standard with the OS) VERITAS Volume Manager 4.1 (comes standard with the OS)#5 For HP-UX 11i v3: LVM (comes standard with the OS) VERITAS Volume Manager 4.1 (comes standard with the OS)#5
#1 File systems cannot be expanded. #2 File systems created without using Veritas Volume Manager cannot be expanded. #3 Provisioning Manager can only display file systems and device files that are created by using SDS. #4 Provisioning Manager can only display file systems and device files that are created by using SVM. #5 Provisioning Manager can only display file systems and device files that are created by using Veritas Volume Manager.	

1.5.3 Cluster Software

Table 1.7 lists the cluster software supported by hosts. Note that Table 1.7 includes only OSs that support cluster software.

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

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

Table 1.7 Supported Cluster Software Versions

Host OS	Cluster Software
Windows	For Windows 2000 (SP4), Windows Server 2003 (either without any SP or with SP1), Windows Server 2003 x64 Edition (without any SP) or Windows Server 2003 R2 (without any SP): Microsoft Cluster Service (MSCS)
Solaris	Solaris 8: VERITAS Cluster Server 3.5 Solaris 9: VERITAS Cluster Server 3.5 or VERITAS Cluster Server 4.0 Solaris 10 (SPARC edition): VERITAS Cluster Server 4.1 Sun Cluster 3.1
AIX	For AIX 5.3: HACMP 5.2
HP-UX	For HP-UX 11i v1: ServiceGuard 11.16 For HP-UX 11i v2: ServiceGuard 11.16 or ServiceGuard 11.17 For HP-UX 11i v3: ServiceGuard 11.17

1.6 Software Products that Cannot Be Combined

This section describes software products that cannot be used with Provisioning Manager.

- When the host OS is HP-UX:

  Provisioning Manager does not support an environment in which a mirror volume exists or can exist.

  - When the OS is HP-UX 11i v2 or earlier

    If MirrorDisk/UX is installed on the host, you cannot use the Provisioning Manager functionality to view the host information and configure the host.

  - When the OS is HP-UX 11i v3

    MirrorDisk/UX is installed on the host during a standard OS installation.

    You can use the Provisioning Manager functionality to view the host information and configure the host.

    However, a software RAID product that uses MirrorDisk/UX is not supported.

- When the host OS is Windows:

  If Veritas Volume Manager is installed on the host, you cannot use the host management functionality of Provisioning Manager

Chapter 2 Setting Up Provisioning Manager

This chapter describes how to set up, start, and stop Provisioning Manager and database operations.

- Setting Up Provisioning Manager on a Management Server (see section 2.1)
- Setting Up Provisioning Manager on a Host (see section 2.2)
- Starting and stopping Provisioning Manager and Device Manager (see section 2.3)
- Operating a Database on a Provisioning Manager Server (see section 2.4)

2.1 Setting Up Provisioning Manager on a Management Server

To set up Provisioning Manager on a management server:

1. Install the Device Manager server.

   When you install the Device Manager server, the Provisioning Manager server is automatically installed in the `ProvisioningManager` at the same level as the Device Manager server's installation target. For example, if you install the Device Manager server in the default path, the Provisioning Manager server is installed in the following path:

   - For Windows

     `C:\Program Files\HiCommand\ProvisioningManager\`

   - For Solaris or Linux

     `/opt/HiCommand/ProvisioningManager/`

     In Solaris 8, Solaris 9, and Solaris 10 (SPARC), this installation path is fixed.

   Provisioning Manager shares databases with Device Manager. During installation, the minimum database capacity for Provisioning Manager is 0.1 MB. You can estimate the total capacity required for the management server by finding the sum of the capacities used by Device Manager, Provisioning Manager, and HiCommand Suite Common Component.

   Important:

   The path on which a Provisioning Manager server of version 05-08 or earlier is installed is at the same level as the HiCommand Suite Common Component installation target. However, the path on which a Provisioning Manager server of version 5.9 or later is installed is at the same level as the Device Manager server installation target.

   As a result of this change, if the installation environment of HiCommand Suite Common Component is different from that of the Device Manager server, and if an upgrade installation is performed with a Device Manager server of version 5.9 or later, the Provisioning Manager server installation target is changed to the Device Manager server installation target.

   For details about installation procedures and the disk capacity required for the management server, see the *HiCommand Device Manager Server Installation and Configuration Guide*.

2. Set up an environment for the Device Manager and Provisioning Manager servers.

   For details about setting up the environment for the Device Manager server, see the *HiCommand Device Manager Server Installation and Configuration Guide*.

   For details about setting up the environment for the Provisioning Manager server, see Chapter 3

3. Register the license key.

   To use Provisioning Manager, you must register a license key at the Provisioning Manager's management client. For details about how to register license keys, see the Provisioning Manager online Help.

2.2 Setting Up Provisioning Manager on a Host

To set up Provisioning Manager on a host:

1. Install a volume manager and Dynamic Link Manager and set up their environments.
2. If you plan to use Provisioning Manager to set up and operate the host, you must first install the Device Manager agent and set up its environment.

   The Provisioning Manager agent's functions are automatically installed when a Device Manager agent is installed.

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

   For details about the Provisioning Manager-related settings in the Device Manager agent property files, see Chapter 3.

2.3 Starting and Stopping Provisioning Manager Server and Device Manager Agent

The following applies to starting and stopping Provisioning Manager and Device Manager and the agents they share.

- The Provisioning Manager server is automatically started when you start the Device Manager server and is automatically stopped when you stop the Device Manager server. You can check the event log or the syslog to verify that the Provisioning Manager server is running. For details about how to start and stop the Device Manager server, see the *HiCommand Device Manager Server Installation and Configuration Guide*.
- Device Manager and Provisioning Manager share an agent, so launching the Device Manager agent is all that is necessary. For details about how to start and stop the Device Manager agent, see the *HiCommand Device Manager Agent Installation Guide*.

2.4 Operating a Database on a Provisioning Manager Server

Provisioning Manager and Device Manager share databases. If you back up, restore, update, or migrate the Device Manager server's database, the Provisioning Manager server's data is also backed up, restored, updated, or migrated. For details about the database operations, see the *HiCommand Device Manager Server Installation and Configuration Guide*.

Chapter 3 Configuring a Provisioning Manager Environment

This chapter describes Provisioning Manager properties, Device Manager agent properties, and the audit logs.

- Provisioning Manager Server Properties (see section 3.1)
- Device Manager Agent Properties (see section 3.2)
- Settings to Use When 100 or More LUs Are Recognized by the Host (see section 3.3)
- Generating Audit Logs (see section 3.4)

3.1 Provisioning Manager Server Properties

The Provisioning Manager server has the following two types of properties:

- Server configuration properties are located in the `server.properties` file.
- Server log properties are located in the `logger.properties` file.

The `server.properties` and `logger.properties` files are stored in the following locations:

- In Windows:
  installation-folder-for-Provisioning-Manager-server\conf\
- In Solaris or Linux:
  installation-folder-for-Provisioning-Manager-server/conf/

These files are formatted as Java™ properties files, which means you can use a text editor to update the properties. A property is specified by connecting its property name and the appropriate value with an equals sign, as in `foo.bar=12345`. Each such specification of a name and a value is delimited by the appropriate end-of-line character as defined by the OS.

Any line in a Provisioning Manager properties file that begins with a hash mark (#) is handled as a comment. You do not need to enclose a literal (character string or numerics) in double quotation marks. The Boolean values are `true` and `false` (not case-sensitive). Any other specification (for example, `yes`) is interpreted as `false`.

In a Java properties files, the backslash (\) is a reserved character that represents the escape character. The backslash is used to indicate that the character immediately following it is a control character, such as a tab or linefeed. Because absolute path names on the Windows platform generally contain backslashes (\), you must insert the escape character (\) before these backslashes. For example, enter `c:\\HiCommand\\docroot\\foo.bar` for the path name `c:\HiCommand\docroot\foo.bar`. In general, you do not need the backslash escape character for any other characters in property specifications.

If you modified the `server.properties` file, you must restart the Device Manager server to apply the changes. If you modified the `logger.properties` file, you must restart the Device Manager server and the HiCommand Suite Common Component services to apply the changes. For details about restarting the Device Manager server and the HiCommand Suite Common Component services, see the *HiCommand Device Manager Server Installation and Configuration Guide*.

If you do not specify properties, or if a specified value for a property exceeds the valid range, the Provisioning Manager server operates using default values.

Table 3.1 lists the Provisioning Manager server properties.

Table 3.1 Summary of Provisioning Manager Server Properties

Classification	File Name	Property	See Section
Properties related to server configuration information.	server.properties	server.operation.abortTimeout	3.1.1.1
		server.operation.eventTimeout	3.1.1.2
		server.rmiapi.port	3.1.1.3
		server.history.maxNumber	3.1.1.4
		server.history.maxDays	3.1.1.5
		server.installTime	3.1.1.6
Properties related to server log functionality.	logger.properties	Logger.loglevel	3.1.2.1
		Logger.sysloglevel	3.1.2.2
		Logger.MaxBackupIndex	3.1.2.3
		Logger.MaxFileSize	3.1.2.4

3.1.1 Server Configuration Information Properties

This section describes the server configuration properties.

3.1.1.1 server.operation.abortTimeout

This property sets the timeout period for host operations, starting from the time when suspension of a host operation begins, and ending when that operation is to be stopped automatically.

Specify a value (in hours) from 0 to 10,000. If 0 is specified, a suspended operation will not be stopped automatically. The default is 24.

3.1.1.2 server.operation.eventTimeout

This property sets the timeout period for transaction logs, starting from the time when Provisioning Manager begins holding the transaction logs, and ending when those logs are purged automatically.

Specify a value (in hours) from 0 to 10,000. If 0 is specified, the operation history is not purged automatically. The default is 24.

3.1.1.3 server.rmiapi.port

This property specifies the management server port number. The default is 20333.

3.1.1.4 server.history.maxNumber

This property sets the maximum number of items to be recorded in the transaction logs. Specify a value from 1 to 100,000. The default is 10,000.

3.1.1.5 server.history.maxDays

This property sets the number of days to retain transaction logs. Any log older than the specified number of days is deleted.

Specify a value from 1 to 100,000 (days). There is no default value.

3.1.1.6 server.installTime

The date, time, and time zone in which installation was completed are written into this property.

3.1.2 Server Log Properties

This section describes the server log properties.

3.1.2.1 Logger.loglevel

This property sets the output level threshold for trace logs and message logs.

The following trace and message logs are affected (* indicates a file number):

- `HPvMGuiTrace*.log`
- `HPvMGuiMessage*.log`
- `HPvMServerTrace*.log`
- `HPvMServerMessage*.log`

Provisioning Manager specifies 0, 10, 20, or 30 as the output level for each log output message according to its content, regardless of whether the message type is error, warning, or information. Only messages with an output level that is less than or equal to the value set in this field are output to the trace log or message log.

Although this field will accept 0, 10, 20, and 30 as values, the default output level of 20 is recommended.

3.1.2.2 Logger.sysloglevel

This property sets the output level threshold for the Common Component logs that are output to the OS (event log in Windows, syslog in Solaris or Linux).

Provisioning Manager specifies 0, 10, 20, or 30 as the output level for each log output message according to its content, regardless of whether the message type is error, warning, or information. Only messages with an output level that is less than or equal to the value set in this field are output to the event log or syslog.

Although this field will accept 0, 10, 20, and 30 as values, use of the default output level of 0 is recommended. The default is 0.

3.1.2.3 Logger.MaxBackupIndex

This property sets the maximum number of trace log files and message log files that can be output.

Caution: This property affects the Provisioning Manager server and GUI trace log files and message log files.

A log file is created with a size as specified in the `Logger.MaxFileSize` property (see section 3.1.2.4), and is assigned a file name with a version number added (e.g., `HPvMServerTrace1.log` and `HPvMServerTrace2.log`). Log files are used in the order of their numbers, and trace information is written into them. When the last file becomes full, the first file is overwritten.

Specify a value from 1 to 16. The default is 10.

3.1.2.4 Logger.MaxFileSize

This property sets the maximum size of a trace log file or message log file. If you do not specify KB (for kilobytes), MB (for megabytes), or GB (for gigabytes), the specified value is assumed to be in bytes. This property is applied to the Provisioning Manager server, GUI trace log files, and message log files.

You can specify a value from 4,096 bytes to 2,147,483,647 bytes (up to but not including 2 GB). The default is 1 MB.

3.2 Device Manager Agent Properties

The Device Manager agent has the following three types of properties:

- Properties related to an agent's HTTP communication function, located in the `server.properties` file.
- Properties related to the log function of an agent, located in the `logger.properties` file.
- Property related to the device files that are used to configure a host running HP-UX 11i v3

  `hldutil.properties` file

The `server.properties` and `logger.properties` files are stored in the following locations:

- For Windows

  installation-folder-for-Device-Manager-agent`\HBaseAgent\agent\config\`
- For Solaris, Linux, or HP-UX

  `/opt/HDVM/HBaseAgent/agent/config/`
- For AIX

  `/usr/HDVM/HBaseAgent/agent/config/`

The `hldutil.properties` file is stored in the following locations:

- For Windows

  installation-folder-for-Device-Manager-agent`\util\bin\`
- For Solaris, Linux, or HP-UX

  `/opt/HDVM/HBaseAgent/util/bin/`
- For AIX

  `/usr/HDVM/HBaseAgent/util/bin/`

If you modify the `logger.properties` or `server.properties` file, you must restart the Device Manager agent to apply the changes. For details on how to restart the Device Manager agent, see the *HiCommand Device Manager Agent Installation Guide*.

If you do not specify the properties, or if a specified value for a property exceeds the valid range, the Device Manager agent uses the default value.

Table 3.2 lists and describes the properties of the Device Manager agent.

Table 3.2 Device Manager Agent Properties

Classification	File Name	Property	See Section
Properties related to an agent's HTTP communication function.	Server.properties	server.agent.fs.moduleTimeOut	3.2.1.1
		server.agent.vm.moduleTimeOut	3.2.1.2
		server.agent.os.moduleTimeOut	3.2.1.3
Properties related to an agent's log function.	logger.properties	logger.loglevel See ***Note***	*HiCommand Device Manager Agent Installation Guide*
		logger.MaxBackupIndex See ***Note***	
		logger.MaxFileSize See ***Note***	
Properties related to the device files used to configure an HP-UX 11i v3 host	hldutil.properties	agent.util.hpux.displayDsf	3.2.2

Note: The log files that are targeted by these properties are `trace.log` and `error.log`.

3.2.1 Properties Related to Agent HTTP Communication Functions

This section describes the properties related to the agent's HTTP communication functions.

3.2.1.1 server.agent.fs.moduleTimeOut

This property is used to set the timeout value from when a file system operation command is executed, until the command execution result is to be returned. You can specify a value from 1 to 2,147,483,647 seconds. The default is 1,200.

3.2.1.2 server.agent.vm.moduleTimeOut

This property is used to set the timeout value from when a volume manager operation command is executed, until the command execution result is to be returned. You can specify a value from 1 to 2,147,483,647 seconds. The default is 1,200.

3.2.1.3 server.agent.os.moduleTimeOut

You use this property to set the timeout value from when a host setup command (such as a device recognition command) is executed, until the command execution result is to be returned. You can specify a value from 1 to 2,147,483,647 seconds. The default is 180.

3.2.2 Properties Related to the Device Files Used to Configure an HP-UX 11i v3 Host

When the host OS is HP-UX 11i v3, you can use the `agent.util.hpux.displayDsf` property to specify the device files used for Provisioning Manager host settings.

When `disk` is specified:

The setting operation is performed for the `disk` device files.

When `ctd` is specified:

The setting operation is performed for the `ctd` device files.

When `mix` is specified:

The setting operation is performed for both the `disk` device files and `ctd` device files.

The default is `mix`.

3.3 Settings to Use When 100 or More LUs Are Recognized by the Host

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

- When the `HiScan` command is executed, the `KAIC22009-E`, `KAIC22014-E`, `KAIC22019-E`, or `KAIC22048-E` error message is output, and the host information cannot be registered in the Provisioning Manager server.
- When the host is refreshed, an OutOfMemory error occurs on the host, and the host does not respond even after waiting.

To avoid these problems, change the following values using the appropriate values listed in the tables in sections 3.3.1 and 3.3.2:

- The maximum length of data that can be received by the Device Manager server: Set this value for the `server.http.entity.maxLength` property in the `server.properties` property file of the Device Manager server. For details on the `server.http.entity.maxLength` property, see the *HiCommand Device Manager Server Installation and Configuration Guide*.
- The timeout value for the processing to register information in a server: Set this value for the `server.http.server.timeOut` property and `server.util.processTimeOut` property in the `server.properties` property file of the Device Manager agent. For details on the `server.http.server.timeOut` property and `server.util.processTimeOut` property, see the *HiCommand Device Manager Agent Installation Guide*.
- The memory heap size

  Set this value for the `server.agent.maxMemorySize` property in the `server.properties` property file of the Device Manager agent.

  For details about the `server.agent.maxMemorySize` property, see the *HiCommand Device Manager Agent Installation Guide*.

This section provides estimates for the setting values depending on whether or not a volume manager is used.

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

3.3.1 When a Volume Manager Is Not Used

Table 3.3 shows the guidelines for the settings when a volume manager is not used.

Table 3.3 Setting Values When a Volume Manager Is Not Used

Number of LUs Managed by Provisioning Manager, and Recognized by the Host	server.http.entity.maxLength (Units: Bytes)	server.http.server.timeOut (Units: Seconds)	server.util.processTimeOut (Units: Milliseconds)
100	131,072 (Default value)	600 (Default value)	600,000 (Default value)
256	153,600	600	600,000
512	307,200	1,000	600,000
1024	614,400	1,800	1,200,000

3.3.2 When a Volume Manager Is Used

Table 3.4 through Table 3.8 show the guidelines for the settings for each host OS when a volume manager is used.

Table 3.4 Setting Values When a Volume Manager Is Used (in Windows)

Number of LUs and Logical Volumes Managed by Provisioning Manager and Recognized by the Host	server.http.entity. maxLength (Units: Bytes)	server.http.server.time Out (Units: Seconds)	server.util.processTime Out (Units: Milliseconds)	server.agent. maxMemory Size (Units: MB)
88/10	230,000	600 (Default value)	600,000 (Default value)	64
88/20	750,000	600	600,000	64
100/200	12,000,000	600	600,000	128
100/500	30,000,000	1,000	600,000	384

Table 3.5 Setting Values When a Volume Manager Is Used (in Solaris)

Number of LUs and Logical Volumes Managed by Provisioning Manager and Recognized by the Host	server.http.entity. maxLength (Units: Bytes)	server.http.server.time Out (Units: Seconds)	server.util.processTime Out (Units: Milliseconds)	server.agent. maxMemory Size (Units: MB)
100/200	3,100,000	600 (Default value)	600,000 (Default value)	128

Number of LUs and Logical Volumes Managed by Provisioning 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)
100/500	7,200,000	1,000	600,000	384
150/500	12,000,000	1,000	600,000	512
250/500	18,000,000	1,000	600,000	768
500/1,000	36,000,000	1,000	600,000	768
1,000/1,000	72,000,000	1,200	600,000	768

Table 3.6 Setting Values When a Volume Manager Is Used (in AIX)

Number of LUs and Logical Volumes Managed by Provisioning 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)
100/200	2,500,000	600 (Default value)	600,000 (Default value)	128
100/500	6,000,000	1,000	600,000	384
175/500	11,000,000	1,000	600,000	640
250/500	15,000,000	1,000	600,000	768
500/1000	19,000,000	1,000	600,000	768
1,000/1,000	38,000,000	1,000	600,000	768

Table 3.7 Setting Values When a Volume Manager Is Used (in Linux)

Number of LUs and Logical Volumes Managed by Provisioning 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	748,000	600 (Default value)	600,000 (Default value)	64
100/100	1,420,000	1,000	600,000	64
100/256	3,600,000	1,000	600,000	192
200/256	7,100,000	1,000	600,000	512

Table 3.8 Setting Values When a Volume Manager Is Used (in HP-UX)

Number of LUs and Logical Volumes Managed by Provisioning 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	745,000	600 (Default value)	600,000 (Default value)	64
100/100	1,400,000	1,000	600,000	64
100/256	3,500,000	1,000	600,000	192
200/256	7,000,000	1,000	600,000	512
500/1,000	40,000,000	1,000	600,000	896
1,000/100	80,000,00	1,000	600,000	192
1,000/500	42,000,000	1,000	1,200,000	896

3.4 Generating Audit Logs

Audit logs for Provisioning Manager and other Hitachi storage-related products can be generated in order to prove to auditors and evaluators the compliance with regulations, security evaluation standards, and other business standards. The Table 3.9 lists and describes the categories of audit log data that can be generated from Hitachi storage-related products.

Table 3.9 Categories and Descriptions

Categories	Description
`StartStop`	Events indicating starting or stopping of hardware or software. ▪ Starting or shutting down an OS ▪ Starting or stopping a hardware component (including micro components) ▪ Starting or stopping software on the storage subsystem, SVP, and HiCommand Suite products
`Failure`	Events indicating hardware or software failures. ▪ Hardware failures ▪ Software failures (memory error, etc.)
`LinkStatus`	Events indicating link status among devices. ▪ Whether a link is up or down
`ExternalService`	Events indicating communication results between Hitachi storage-related products and external services. ▪ Communication with a RADIUS, LDAP, NTP, and DNS server ▪ Communication with a management server (SNMP)
`Authentication`	Events indicating that a device, administrator, or end user succeeded or failed in connection or authentication. ▪ FC login ▪ Device authentication (FC-SP authentication, iSCSI login authentication, SSL server/client authentication) ▪ Administrator or end user authentication
`AccessControl`	Events indicating that a device, administrator, or end user succeeded or failed in gaining access to resources. ▪ Access control for devices ▪ Access control for the administrator or end users
`ContentAccess`	Events indicating that attempts to access important data succeeded or failed. ▪ Access to important files on NAS or to contents when HTTP is supported ▪ Access to audit log files
`ConfigurationAccess`	Events indicating that the administrator succeeded or failed in performing an allowed operation. ▪ Reference or update of the configuration information ▪ Update of account settings including addition or deletion of accounts ▪ Security configuration ▪ Reference or update of audit log settings

Categories	Description
Maintenance	Events indicating that a performed maintenance operation succeeded or failed. ▪ Addition or deletion of hardware components ▪ Addition or deletion of software components
AnomalyEvent	Events indicating that anomalies such as a threshold excess occurred. ▪ Excess over network traffic threshold ▪ Excess over CPU load threshold ▪ Over-limit pre-notification or wraparound of audit logs temporarily saved inside
	Events indicating that abnormal communication occurred. ▪ SYN flood attacks to a regularly used port, or protocol violations ▪ Access to an unused port (port scanning, etc.)

The audit log types that can be generated vary according to products. The following sections describe the audit logs that can be generated by using Provisioning Manager. For details on the audit logs for other products, see their respective manuals.

3.4.1 Categories of Information Output to Audit Logs in Provisioning Manager

The following table lists the categories of information output to audit logs in Provisioning Manager and the audit events. Each audit event is assigned a severity level. You can filter audit log data to be output according to their the severity levels of events.

Table 3.10 Categories of Information Output to Audit Logs, and Audit Events

Category	Description	Audit Event	Severity
StartStop	Start and stop of software	Successful SSO server start	6
		Failed SSO server start	3
		SSO server stop	6
Authentication	Administrator or end user authentication	Successful login	6
		Failed login (wrong user ID or password)	4
		Failed login (logged in as a locked user)	4
		Failed login (logged in as a non-existing user)	4
		Failed login (no permission)	3
		Failed login (authentication failure)	4
		Successful logout	6
	Automatic account lock	Automatic account lock (repeated authentication failure or expiration of account)	4

Category	Description	Audit Event	Severity
ConfigurationAccess	User registration	Successful user registration	6
		Failed user registration	3
	User deletion	Successful single user deletion	6
		Failed single user deletion	3
		Successful multiple user deletion	6
		Failed multiple user deletion	3
	Password change (from the administrator panel)	Successful password change by the administrator	6
		Failed password change by the administrator	3
	Password change (from the user's own panel)	Failed in authentication processing for verifying old password	3
		Successful change of login user's own password (from the user's own panel)	6
		Failed change of login user's own password (from the user's own panel)	3
	Profile change	Successful profile change	6
		Failed profile change	3
	Permission change	Successful permission change	6
		Failed permission change	3
	Account lock	Successful account lock	6
		Failed account lock	3
	Account lock release	Successful account lock release	6
		Failed account lock release	3
	Database backup or restore	Successful backup using the hcmdsdb command	6
		Failed backup using the hcmdsdb command	3
		Successful full restore using the hcmdsdb command	6
		Failed full restore using the hcmdsdb command	3
		Successful partial restore using the hcmdsdb command	6
		Failed partial restore using the hcmdsdb command	3
	Database input/output	Successful data output using the hcmdsdbmove command	6

Category	Description	Audit Event	Severity
		Failed data output using the `hcmdsdbmove` command	3
		Successful data input using the `hcmdsdbmove` command	6
		Failed data input using the `hcmdsdbmove` command	3
	Database area creation or deletion	Successful database area creation using the `hcmdsdbsetup` command	6
		Failed database area creation using the `hcmdsdbsetup` command	3
		Successful database area deletion using the `hcmdsdbsetup` command	6
		Failed database area deletion using the `hcmdsdbsetup` command	3
	Authentication data input/output	Successful data output using the `hcmdsdbauthmove` command	6
		Failed data output using the `hcmdsdbauthmove` command	3
		Successful data input using the `hcmdsdbauthmove` command	6
		Failed data input using the `hcmdsdbauthmove` command	3
	Reception of a request to the Provisioning Manager server and transmission of response	Reception of request (during normal processing)	6
		Reception of request (common, in the event of an error)	3
		Transmission of response (during normal processing)	6
		Transmission of response (in the event of an error)	3

3.4.2 Editing Audit Log Environment Settings File

To generate the Provisioning Manager audit logs, you must edit the environment settings file (`auditlog.conf`). The audit logs can be generated by setting audit event categories, in `Log.Event.Category` of the environment settings file, to be generated. For Windows, the audit logs are output to the event log files (application log files). For Solaris™ and Linux, they are output to the `syslog` file.

Caution: A large volume of audit log data might be output. Change the log size and back up or archive the generated logs accordingly.

The following describes the storage destination for the `auditlog.conf` file.

- For Windows:

```
installation-folder-for-HiCommand-Suite-Common-Component\conf\sec\auditlog.conf
```

- For Solaris or Linux:

```
installation-directory-for-HiCommand-Suite-Common-Component/conf/sec/auditlog.conf
```

The table below shows the items that are set for the `auditlog.conf` file.

Table 3.11 Items Set for auditlog.conf

Item	Description
`Log.Facility`	Specify (by using a number) the facility to be used when the audit log messages are output to the `syslog` file. `Log.Facility` is used, in combination with the severity levels set for each audit event (see Table 3.10), for filtering the output to the `syslog` file. For details about the values that can be specified for `Log.Facility`, see Table 3.12. For details about the correspondence between the severity levels set for audit events and those set in the `syslog.conf` file, see Table 3.13. `Log.Facility` has an effect in Solaris or Linux only. `Log.Facility` is ignored in Windows, even if it is specified. Also, if an invalid value or a non-numeric character is specified, the default value is used. Default value: `1`
`Log.Event.Category`	Specify the audit event categories to be generated. When specifying multiple categories, use commas (`,`) to separate them. If `Log.Event.Category` is not specified, audit log data is not output. For information about the available categories, see Table 3.10. `Log.Event.Category` is not case-sensitive. If an invalid category name is specified, the specified file name is ignored. Default value: (not specified)
`Log.Level`	Specify the severity level of audit events to be generated. Events with the specified severity level or lower will be output to the event log file. For information about the audit events that are output from Provisioning Manager and their severity levels, see Table 3.10. For details about the correspondence between the severity levels of audit events and the types of event log data, see Table 3.13. `Log.Level` has an effect in Windows® only. `Log.Level` is ignored in Solaris and Linux, even if it is specified. Also, if an invalid value or a non-numeric character is specified, the default value is used. Specifiable values: `0` to `7` (severity level) Default value: `6`

The table below shows the values that can be set for `Log.Facility` and the corresponding values specified in the `syslog.conf` file.

Table 3.12 Log.Facility Values and the Corresponding Values in syslog.conf

Facility	Corresponding Values in syslog.conf
1	`user`
2	`mail*`
3	`daemon`

Facility	Corresponding Values in syslog.conf
4	auth*
6	lpr*
16	local0
17	local1
18	local2
19	local3
20	local4
21	local5
22	local6
23	local7

* Although you can specify this value, we do not recommend that you specify it.

The table below shows the correspondence between the severity levels of audit events, the values indicating severity that are specified in the `syslog.conf` file, and the types of event log data.

Table 3.13 Correspondence Between the Severity Levels of Audit Events, the Severity Levels in syslog.conf, and the Types of Event Log Data

Severity of Audit Events	Severity in syslog.conf	Type of Event Log Data
0	emerg	Error
1	alert	
2	crit	
3	err	
4	warning	Warning
5	notice	Information
6	info	
7	debug	

The following shows an example of the `auditlog.conf` file:

```
Log.Facility  1
Log.Event.Category Authentication,ConfigurationAccess
Log.Level 6
```

In the example above, the audit events related to `Authentication` or `ConfigurationAccess` are output. For Windows, `Log.Level 6` outputs audit log data corresponding to the Error, Warning, and Information levels. For Solaris or Linux, `Log.Facility 1` outputs the audit log data to the `syslog` file that is defined as the `user` facility in the `syslog.conf` file.

3.4.3 Format of Output Audit Log Data

This section describes the format of output audit log data.

- For Windows:

  When you open an event by choosing **Event Viewer** and then **Application**, the following is displayed in the **Description** area in the **Event Properties**.

  ```
  program-name [process-ID]: message-portion
  ```

- For Solaris or Linux:

  The contents of a `syslog` file

  ```
  date-time server-name (or IP-address) program-name[process-ID]: message-portion
  ```

The format and contents of *message-portion* are described below.

The output format of message-portion:

uniform-identifier,*unified-specification-revision-number*,
serial-number,*message-ID*,*date-and-time*,*detected-entity*,*detected-location*,*audit-event-type*,
audit-event-result,*audit-event-result-subject-identification-information*,
hardware-identification-information,*location-information*,*location-identification-information*,
FQDN,*redundancy-identification-information*,*agent-information*,*request-source-host*,
request-source-port-number,*request-destination-host*,*request-destination-port-number*,
batch-operation-identifier,*log-data-type-information*,*application-identification-information*,
reserved-area,*message-text*

Table 3.14 Information Output to message-portion

Item*	Description
uniform-identifier	Fixed to `CELFSS`.
unified-specification-revision-number	Fixed to `1.1`.
serial-number	Serial number of audit log messages.
message-ID	Message ID. For details, see section 3.4.4.
date-and-time	The date and time when the message was output. This item is output in the format of *yyyy*`-`*mm*`-`*dd*`T`*hh*`:mm:`*ss*`.s`*time-zone*.
detected-entity	Component or process name.
detected-location	Host name.
audit-event-type	Event type.
audit-event-result	Event result.
audit-event-result-subject-identification-information	Account ID, process ID, or IP address corresponding to the event.
hardware- identification-information	Hardware model or serial number.
location-information	Identification information for the hardware component.
location-identification-information	Location identification information.
FQDN	Fully qualified domain name.
redundancy-identification-information	Redundancy identification information.
agent-information	Agent information.
request-source-host	Host name of the request sender.
request-source-port-number	Port number of the request sender.
request-destination-host	Host name of the request destination.
request-destination-port-number	Port number of the request destination.
batch-operation-identifier	Serial number of operations through the program.
log-data-type-information	Fixed to `BasicLog`.
application-identification-information	Program identification information.
reserved-area	Not output. This is a reserved space.
message-text	The contents vary according to the audit events. Characters that cannot be displayed are output as asterisks (`*`). For details, see section 3.4.5.

* Some items are not output for some audit events.

Example of message-portion output for the Login audit event:

```
CELFSS,1.1,0,KAPM01124-I,2006-05-15T14:08:23.1+09:00,HBase-SSO,management-host,
Authentication,Success,uid=system,,,,,,,,,,,BasicLog,,,"The login process has
completed properly."
```

Example of audit log data output when a request to the Provisioning Manager server is received:

```
CELFSS,1.1,0,KARF91200-I,2006-11-10T18:21:17.9+09:00,PvM,CZA92G,Configuration
Access,Success,uid=System,,,,,,,from=10.208.64.128,,,,,BasicLog,PvM,,
"PvM123456789 GetSPoolSum info='All Resources' CID=Pv1163150475209G"
```

3.4.4 Audit Log Message ID

The following two types of audit log message IDs are output:

1. KAPM: Audit events occurring during HiCommand Suite Common Component processing

   For information on the message text corresponding to each message ID, see section 3.4.5.1.

2. KARF: Audit events occurring during processing other than 1 above.

   The table below shows the message IDs and their contents.

Table 3.15 Audit Log Message IDs and Their Contents

Message ID	Description	Section for the corresponding message format
KARF91000 to KARF91399	When a request to the Provisioning Manager server is received and when a response is sent (during normal processing)	3.4.5.2
KARF91400 to KARF91799	When a request to the Provisioning Manager server is received and when a response is sent (during error handling processing)	

3.4.5 Message Text Component of Audit Log Data

The format of message text in audit log data varies from one audit event to another. This section describes the message text format for each audit event. The item enclosed by square brackets ([ ]) in the message text format might not be output.

3.4.5.1 When Output as Processing Results of HiCommand Suite Common Component

Information on the audit event that has occurred is output in a character string. For more information on the message text, see the *HiCommand Device Manager Error Codes*. The following shows an example of message text.

Example of message text output upon login:

```
"The login process has completed properly."
```

3.4.5.2 When Output as Processing Results of Provisioning Manager Server

This section describes the format of messages that are output to the message text, and the information displayed when a request to the Provisioning Manager server is received or a response is sent.

Format of messages output when a request is received (during normal processing):

unique-ID details-of-request parameter command-ID

Format of messages output when a request is received (in the event of an error):

unique-ID details-of-request parameter command-ID error-code

Format of messages output when a response is sent (during normal processing of a view or setting operation or when processing for either of those operations is suspended):

unique-ID command-ID operation-ID

Format of messages output when a response is sent (during abnormal processing of a view or setting operation):

unique-ID command-ID error-code

Format of messages output when a response is sent (during normal polling processing):

unique-ID command-ID status operation-ID

Format of messages output when a response is sent (during abnormal polling processing):

unique-ID command-ID error-code operation-ID

Table 3.16 Information That Is Displayed in the Message Text When a Request to the Provisioning Manager Server Is Received or a Response Is Sent

Item	Description
unique-ID	Displays a unique value as the ID that identifies a request or response.
details-of-request	Displays a character string as the details of a request to the Provisioning Manager server. For the meaning of the character string that is displayed as the details of a request, see 3.4.6
parameter	Displays the parameter information for identifying the target resource, from among the parameters that are passed when a request is issued. If there are no parameters, this information is not displayed. For details about the parameters that are displayed, see 3.4.6 The format for output parameters is as follows: ▪ A parameter is displayed in the format: `info='...'`. If there are multiple parameters, each parameter is separated by a comma (`,`). Such as: `info='X,Y,Z'`. ▪ If a parameter is an array, each value in the array is separated by a space and the entire array is enclosed in square brackets, such as: `[a1 a2 a3]`. ▪ If a parameter value contains a single quotation mark (`'`), comma (`,`), or square brackets (`[]`), the relevant symbol is replaced with a question mark (`?`).
command-ID	Displays the ID that is assigned to an operation so that the logs related to the operation can be identified. The format for output command-IDs is as follows: ▪ A command ID is displayed in the format `CID=...`. ▪ A command ID is not displayed when you register or view a license. ▪ Except for the above case, if a command ID cannot be obtained, the character string `Unknown` is displayed.
status	Displays a character string that indicates the polling results. Some Provisioning Manager operations take a long time to finish after a request is issued. In this case, the processing status is checked by a polling operation. One of the following character strings is displayed: ▪ COMPLETED: The processing was completed. ▪ FAILED: The processing failed. ▪ SUSPENDED: The processing was suspended.
error-code	Displays the message ID.
operation-ID	Output character string that shows that the log before the operation was interrupted is related to the log after the operation resumes. This item is displayed in the following situations: ▪ When a response for a setting operation is sent (during normal processing) ▪ When a response for polling is sent (during normal processing) ▪ When a response for polling is sent (during abnormal processing)

The following shows an example of the displayed message text:

Example of message text that is displayed for the audit event *reception of request (during normal processing)*:

```
"PvM123456789 GetAlloc info='32' CID=Pv243488034G"
```

Example of message text that is displayed for the audit event *transmission of response (in the event of an error)*:

```
"PvM123456789 CID=Pv243488034G KARF15000-E"
```

3.4.6 Details of Requests, and Parameters that Are Output to the Audit Log

The following table lists and describes the details of requests, their descriptions, and parameters that are output by Provisioning Manager to the audit log.

Table 3.17 Details of Requests to the Provisioning Manager Server and the Parameters That Are Output

Details of Request	Description	Parameter that is Output
AddLicense	Adds a license by using a single license key.	Fixed to * * * * *
	Adds a license by using a license key file.	Size of the license key file
CreateAllocPl	Creates a new allocation plan.	Information about the allocation plan#1
DelAllocPl	Deletes an allocation plan.	Resource identifier of the allocation plan that is to be deleted#2
GetAllocVols	Acquires a list of volumes to be displayed in the list of allocated LDEVs.	▪ Names of the resource groups in a storage pool from which the volumes are acquired ▪ Resource identifier of the storage subsystem to which the acquired volumes belong#2 ▪ Information about the allocation plan (if specified)#1
GetAllocVolInfos	Acquires a list of volumes to be displayed in the list of allocated LDEVs, and additional information that indicates the non-conforming status of the storage subsystem.	▪ Names of the resource groups in a storage pool from which the volumes are acquired ▪ Resource identifier of the storage subsystem to which the acquired volumes belong#2 ▪ Information about the allocation plan (if specified)#1
GetAllocPls	Acquires all allocation plans that can be referenced by the logon user.	--
GetAllocPl	Acquires the allocation plan that has the specified resource identifier.	Resource identifier of the allocation plan#2

Details of Request	Description	Parameter that is Output
GetAllocPlByName	Acquires the allocation plan that has the specified name.	Allocation plan name
GetConPortInfoByDevF	Acquires the port connection information that has been set between the specified device file and the volume.	▪ Resource identifier of the volume#2 ▪ Resource identifier of the device file#2
GetConPortInfoByHost	Acquires the port connection information that has been set between the specified host and the volume	▪ Resource identifier of the volume#2 ▪ Resource identifier of the host#2
GetDevF	Acquires the device file that has the specified resource identifier.	Resource identifier of the device file#2
GetDevFByName	Acquires the device file that has the specified name.	▪ Resource identifier of the host#2 ▪ Device file name
GetDevFHost	Acquires the device file of the specified host.	Resource identifier of the host#2
GetDevFsSumByHost	Acquires the device file of the specified host.	Resource identifier of the host#2
GetDevOprLogDtl	Acquires the details of the device operation log information that has the specified device operation log ID.	Log ID
GetDevOprLogs	Acquires device operation log information.	--
GetFSys	Acquires the file system that has the specified resource identifier.	Resource identifier of the file system#2
GetFSysMP	Acquires, on the specified host, the file system at the mount point.	▪ Resource identifier of the host#2 ▪ Mount point
GetFSysByHost	Acquires the file system of the specified host.	Resource identifier of the host#2
GetFSysSumHost	Acquires the file system of the specified host.	Resource identifier of the host#2
GetFiltSPoolDtl	Acquires storage pool information for the specified resource group and the resource groups immediately below it.	▪ Target resource group name ▪ Information about the allocation plan (if specified)#1
GetFiltSPoolSum	Acquires the storage pool information for the specified resource group	▪ Target resource group name ▪ Information about the allocation plan (if specified)#1
GetHost	Acquires the host information that has the specified resource identifier.	Resource identifier of the host#2
GetHostByIPAddress	Acquires the host information that has the specified IP address.	IP address
GetHostByName	Acquires the host information that has the specified name.	Host name
GetHosts	Acquires the host information for all management-target hosts.	--

Details of Request	Description	Parameter that is Output
GetHostSum	Acquires the host information for all management-target hosts.	--
GetLicenseInfo	Acquires the license information.	--
GetLogLevel	Dynamically acquires the log output level.	--
GetOprEvent	Acquires a host setting event.	Operation ID of the host setting processing that was acquired as the return value of the host setting operation API
GetProvInfo	Acquires provisioning settings.	Operation ID of the host setting processing that was acquired as the return value of the host setting operation API
GetSA	Acquires storage subsystem information that has the specified resource identifier.	Resource identifier of the storage subsystem to which the acquired volumes belong[#2]
GetSAByTypeSrlNum	Acquires storage subsystem information specified by the model and serial number.	▪ Model name of the storage subsystem ▪ Serial number of the storage subsystem
GetSAs	Acquires storage subsystem information for all management targets.	--
GetSAByName	Acquires storage subsystem information that has the specified name.	Storage subsystem name
GetSPoolDtl	Acquires an array whose elements are the storage pool information for the specified resource group and the resource groups immediately below it.	Target resource group name
GetSPoolDispArrFamDtl	Acquires an array whose elements are the storage pool information for the specified resource group and the resource groups immediately below it.	Target resource group name
GetSPoolDispArrFamSum	Acquires storage pool information for the specified resource group for each series.	Target resource group name
GetSPoolDispArrTypeDtl	Acquires an array whose elements are the storage pool information for the specified resource group and the resource groups immediately below it.	Target resource group name
GetSPoolDispArrDypeSum	Acquires storage pool information for the specified resource group for each model.	Target resource group name
GetSPoolRaidTypeDtl	Acquires an array whose elements are the storage pool information for the specified resource group and the resource groups immediately below it.	Target resource group name

Details of Request	Description	Parameter that is Output
GetSPoolRaidTypeSum	Acquires storage pool information for the specified resource group for each RAID type.	Target resource group name
GetSPoolSANameDtl	Acquires an array whose elements are the storage pool information for the specified resource group and the resource groups immediately below it.	▪ Target resource group name ▪ Information about the allocation plan#1
GetSPoolSANameSum	Acquires storage pool information for the specified resource group for each device.	▪ Target resource group name ▪ Information about the allocation plan#1
GetSPoolSum	Acquires storage pool information for the specified resource group.	Target resource group name
GetSprtSAFams	Acquires a list of supported series.	--
GetSprtSATypes	Acquires a list of supported models.	--
GetUnAllocVols	Acquires a list of volumes to be displayed in the list of unallocated LDEVs.	▪ Names of the resource groups in a storage pool from which the volumes are acquired ▪ Resource identifier of the storage subsystem to which the acquired volumes belong#2 ▪ Information about the allocation plan#1
GetUnAllocVolInfos	Acquires a list of volumes to be displayed in the list of unallocated LDEVs, and additional information that indicates the non-conforming status of the storage subsystem.	▪ Names of the resource groups in a storage pool from which the volumes are acquired ▪ Resource identifier of the storage subsystem to which the acquired volumes belong#2 ▪ Information about the allocation plan#1
GetUGrp	Acquires the resource group to which the logon user belongs.	--
GetUGrpByName	Acquires the resource group that has the specified name.	Resource group name
GetUGrpForVol	Acquires an array of resource groups to which the specified volume belongs.	Array of the resource identifiers of the volume#2
GetUGrps	Acquires an array that indicates the parent-child relationship of the resource groups to which the logon user belongs and the resource groups immediately below it.	--
GetVer	Acquires the version information.	--
GetVolSADevNum	Acquires the volume in the specified storage subsystem and device number.	▪ Resource identifier of the storage subsystem#2 ▪ Device number
GetVolSA	Acquires the volume in the specified storage subsystem.	Resource identifier of the storage subsystem#2

Details of Request	Description	Parameter that is Output
GetVolForAddDevF	Acquires a list of volumes for creating a device file.	▪ Resource identifier of the target host to which the volumes being acquired are to be allocated#2 ▪ Resource identifier of the storage subsystem to which the acquired volumes belong#2
GetVolInfosForAddDevF	Acquires a list of volumes for creating a device file, and additional information that indicates the non-conforming status of the storage subsystem.	▪ Resource identifier of the target host to which the volumes being acquired are to be allocated#2 ▪ Resource identifier of the storage subsystem to which the acquired volumes belong#2
GetVolForAddFSys	Acquires a list of volumes for creating a file system.	▪ Resource identifier of the target host to which the volumes being acquired are to be allocated#2 ▪ Resource identifier of the storage subsystem to which the acquired volumes belong#2
GetVolInfosForAddFSys	Acquires a list of volumes for creating a file system, and additional information that indicates the non-conforming status of the storage subsystem.	▪ Resource identifier of the target host to which the volumes being acquired are to be allocated#2 ▪ Resource identifier of the storage subsystem to which the acquired volumes belong#2
GetVolForExpFSys	Acquires a list of volumes for expanding a file system.	▪ Resource identifier of the file system to be expanded#2 ▪ Resource identifier of the target host to which the volumes being acquired are to be allocated#2 ▪ Resource identifier of the storage subsystem to which the acquired volumes belong#2
GetVolInfosForExpFSys	Acquires a list of volumes for expanding a file system, and additional information that indicates the non-conforming status of the storage subsystem.	▪ Resource identifier of the file system to be expanded#2 ▪ Resource identifier of the target host to which the volumes being acquired are to be allocated#2 ▪ Resource identifier of the storage subsystem to which the acquired volumes belong#2
GetVolForModPool	Acquires a list of volumes for displaying the storage pool change window.	▪ Names of the resource groups in a storage pool from which the volumes are acquired ▪ Resource identifier of the storage subsystem to which the acquired volumes belong#2 ▪ Information about the allocation plan#1

Details of Request	Description	Parameter that is Output
GetVolSumForAllocPool	Acquires summary information for volumes to display a list of allocated LDEVs.	▪ Names of the resource groups in a storage pool from which the volumes are acquired ▪ Resource identifier of the storage subsystem to which the acquired volumes belong#2 ▪ Information about the allocation plan#1
GetVolSumForModPool	Acquires summary information for volumes to display the storage pool change window.	▪ Names of the resource groups in a storage pool from which the volumes are acquired ▪ Resource identifier of the storage subsystem to which the acquired volumes belong#2 ▪ Information about the allocation plan#1
GetVolSumForUnAllocPool	Acquires summary information for volumes to display a list of unallocated LDEVs.	▪ Names of the resource groups in a storage pool from which the volumes are acquired ▪ Resource identifier of the storage subsystem to which the acquired volumes belong#2 ▪ Information about the allocation plan#1
IsUsedLogicVolName	Checks whether the logical volume name is already in use.	▪ Resource identifier of the host#2 ▪ Logical volume name
IsUsedVolGrpName	Checks whether the volume group name is already in use.	▪ Resource identifier of the host#2 ▪ Volume group name
ModAllocPl	Edits an existing allocation plan.	Information about the allocation plan#1
ModPool	Changes the storage pool that owns the specified volume as OWN.	▪ Resource group name to which the volume belonged before the move ▪ Resource group name after the move ▪ Array of the resource identifiers of the volume to be moved#2
RefreshHostInfo	Refreshes host information.	Resource identifier of the host to be refreshed#2
ResumeOpr	Restarts the host setting operation that has been suspended.	Operation ID acquired as the return value of the host setting operation API when the host setting operation was suspended
SetLogLevel	Dynamically changes the log output level.	Log output level
SetStatus	Changes the status (public or private) of the provisioning plan.	▪ Resource identifier of the provisioning plan#2 ▪ Status after change (public or private)

Details of Request	Description	Parameter that is Output
StartAddDevF	Creates a device file.	▪ Resource identifier of the target host#2 ▪ Resource identifier of the target volume#2 ▪ Type of the volume manager to be used ▪ Volume group name ▪ Logical volume name ***Caution***: Volume group name and logical volume name are displayed only when they are specified.
StartAddFSys	Creates a file system.	▪ Resource identifier of the target host#2 ▪ Resource identifier of the target volume#2 ▪ Type of the file system to be created ▪ Mount point of the file system to be created ▪ Type of the volume manager to be used ▪ Volume group name ▪ Logical volume name ***Caution***: Volume group name and logical volume name are displayed only when they are specified.
StartDelDevF	Deletes a specified device file.	Resource identifier of the device file to be deleted#2
StartDelFSys	Deletes a specified file system.	Resource identifier of the file system to be deleted#2
StartExpandFSys	Expands a file system.	▪ Resource identifier of the file system to be expanded#2 ▪ Resource identifier of the target volume#2

#1 For details about the parameters that are output as information about the allocation plan, see Table 3.18. The allocation plan information is displayed enclosed in square brackets ([]), and values are separated by a semicolon (;).

#2 The resource identifier consists of several elements. For details about the elements of each resource identifier, see Table 3.19. The elements of each resource identifier are output, separated by a hyphen (-).

Table 3.18 Parameters That Are Output as Information About the Allocation Plan

Information about the allocation plan	Output	
	ModAllocPl	Other than ModAllocPl
Plan name	Y	Y
Model name of storage subsystem	Y	Y
RAID level	Y	Y
Plan creation date	Y	--
Plan owner resource group	Y	--
User who created the plan	Y	--
Plan creation resource group	Y	--
Plan update date and time	Y	--
User who updated the plan	Y	--
Plan update resource group	Y	--
Plan status (public or private)	Y	--

Legend: Y: Output, --: Not output

Table 3.19 Elements of the Resource Identifier

Resource Type	Element of Resource Identifier
File system	File system ID, host ID
Device file	Device file ID, host ID
Plan	Plan ID
Volume	Model name of storage subsystem, serial number, LDEV number
Storage subsystem	Model name of storage subsystem, serial number
Host	Host ID

For the correspondence between the storage subsystem name that is displayed in the audit log and the actual model name, see Table 3.20. Note that Device Manager versions 5.7 or later do not support T3. However, if a T3 storage subsystem is already registered as a management target of Device Manager in earlier versions and you perform an operation for that storage subsystem, information about T3 might be output to the audit log.

Table 3.20 Correspondence Between the Storage Subsystem Name That Is Displayed in the Audit Log and the Actual Model Name

Name Output to the Audit Log	Model
D500	Thunder 9200
D600	Thunder 9500V
D700	TagmaStore AMS/WMS series
D800	Hitachi AMS series
R400	Lightning 2000
R450	Lightning 9900V series
R500	TagmaStore USP
R600	Universal Storage Platform V/VM
T3	Sun StorEdge T3

Acronyms and Abbreviations

AMS	Adaptable Modular Storage
API	Application Programming Interface
ASCII	American Standard Code for Information Interchange
CLI	Common Line Interface
CPU	Central Processing Unit
DNS	Domain Name System
FC-SP	Fibre Channel Security Protocol
FQDN	Fully Qualified Domain Name
FTP	File Transfer Protocol
GUI	graphical user interface
HA	High Availability
HBA	host bus adapter
HDLM	HiCommand Dynamic Link Manager and Hitachi Dynamic Link Manager
HTTP	HyperText Transfer Protocol
ID	IDentifier
IP	Internet Protocol
IPF	Itanium Processor Family
iSCSI	Internet Small Computer System Interface
JFS	Journaled file system
LDAP	Lightweight Directory Access Protocol
LDEV	logical device
LVM	logical volume manager
NAS	Network Attached Storage
NSC	TagmaStore Network Storage Controller
NTFS	NT file system
NTP	Network Time Protocol
OS	Operating system
RADIUS	Remote Authentication Dial In User Service
RAID	Redundant Arrays of Inexpensive Disks
SAN	storage area network
SDS	Solstice DiskSuite
SNMP	Simple Network Management Protocol
SSL	secure socket Layer
SSO	Single Sign-On
SSP	Storage Service Provider
SVP	Service Processor

TCP/IP	transmission control protocol/internet Protocol
UFS	UNIX file system
URL	Uniform Resource Locator
USP	Universal Storage Platform
WMS	Workgroup Modular Storage
WWN	World Wide Name

Index