Hitachi Device Manager Software 6.4.0-00 Release Notes

About This Document

This document (RN-00HS266 – June.15.2010) provides late-breaking information about the Hitachi Device Manager Software 6.4.0-00. It includes information that was not available at the time the technical documentation for this product was published, as well as a list of known problems and solutions.

Intended Audience

This document is intended for customers and Hitachi Data Systems partners who license and use the Hitachi Device Manager Software.

Getting Help

The Hitachi Data Systems Support Center staff is available 24 hours a day, seven days a week. To reach us, please visit the support Web site for current telephone numbers and other contact information:

http://www.hds.com/services/support/. If you purchased this product from an authorized HDS reseller, contact that reseller for support.

About This Release

- This release is a major release that adds new features and fixes a variety of bugs.

Product Package Contents

Medium	CD-ROM	Revision	Release Type	Prerequisite version of Service Pack
Software	Device Manager Server	6.4.0-00	Full Package	-
	Device Manager Web Client	6.4.0-00	Full Package	-
	Device Manager CLI	6.4.0-00	Full Package	-
	Device Manager CLIEX (*1)	6.4.0-00	Full Package	-
	Device Manager Agent (Windows)	6.4.0-00	Full Package	-
	Device Manager Agent (Solaris)	6.4.0-00	Full Package	-
	Device Manager Agent (HP-UX)	6.4.0-00	Full Package	-
	Device Manager Agent (AIX)	6.4.0-00	Full Package	-
	Device Manager Agent (Linux)	6.4.0-00	Full Package	-
	Device Manager VDS Provider	6.4.0-00	Full Package	-
Documents	Hitachi Device Manager Software Server Configuration and Operation Guide	MK-08HC157-04		
	Hitachi Device Manager Software Command Line Interface (CLI) User's Guide	MK-91HC007-27		
	Hitachi Device Manager Software Error Codes	MK-92HC016-23		
	Hitachi Device Manager Agent Installation Guide	MK-92HC019-22		
	Hitachi Device Manager Software Getting Started Guide	MK-98HC149-03		
	Hitachi Storage Command Suite Software Server Installation Guide Device Manager Provisioning Manager Tiered Storage Manager	MK-98HC150-04		

(*1) CLIEX is bundled with CLI

New Features and Important Enhancements

For 6.4.0-00

#	New Features and Enhancements	Applied products	Applied OS
1	A function to display the correspondence relationships between virtual machines on a virtualization server and volumes on a storage subsystem is now supported.	Device Manager Web Client Device Manager CLI Device Manager server	All (Note)
2	In an IPv6 environment, communication from Hitachi Device Manager to the VMware vSphere Management Assistant (vMA) is now supported.	Device Manager Web Client Device Manager CLI Device Manager server	All (Note)
3	A function to manage Hitachi NAS and High-performance NAS platform is now supported.	Device Manager Web Client Device Manager server	All (Note)
4	The following values can now be selected for hostmode2 when using Hitachi AMS2000 series: Unique Extended COPY Mode Unique Write Same Mode	Device Manager Web Client Device Manager CLI Device Manager server	All (Note)
5	SAS disks in Dense RKA is now supported for Hitachi AMS2000 series.	Device Manager CLI Device Manager server	Windows Solaris (SPARC)
6	When Active Directory is used as an external authentication server, user authentication by using Active Directory group is now supported.	Device Manager Web Client Device Manager CLI Device Manager server	All (Note)
7	Device Manager now supports advanced security settings for encrypting communications.	Device Manager server	All (Note)
8	The following storage subsystem are now supported: Hitachi AMS2100(H/W Rev. 0200) Hitachi AMS2300(H/W Rev. 0200)	Device Manager Web Client Device Manager CLI	Windows Solaris (SPARC)

	Hitachi AMS2500(H/W Rev. 0200)	Device Manager server	
9	Device Manager server, Web Client and CLI now support the following Linux OS versions: SUSE Linux Enterprise Server 10 Service Pack3 SUSE Linux Enterprise Server 11	Device Manager Web Client Device Manager CLI Device Manager server	Linux
10	Device Manager server, Web Client and CLI now support the following Linux OS versions: Red Hat Enterprise Linux Advanced Platform 5.4 Red Hat Enterprise Linux 5.4	Device Manager Web Client Device Manager CLI Device Manager server	Linux
11	Device Manager server now supports the following OS as a guest OS of virtual server product VMWare ESX/ESXi Server 3.x or 4.x. Windows 7 Windows Server 2008 R2	Device Manager server	Windows
12	Device Manager server now supports the virtual server product Solaris LDoms 1.3.	Device Manager server	Solaris
13	The -d option has been added to the Device Manager agent TIC command. Specifying this option will suppress the acquisition of error information.	Device Manager agent	All (Note)
14	The property server.agent.rm.cuLdevForm has been added. This property makes it possible to specify the output format of LDEV numbers when the HORCM_LDEV format is used to write pair volume information to the CCI configuration file during the creation of pairs.	Device Manager agent	All (Note)
15	The Device Manager agent can now collect performance information for storage subsystems that contain SLPRs.	Device Manager agent	All (Note)
16	PowerHA 6.1 is now supported when the host OS is AIX 6.1.	Device Manager agent	All (Note)
17	The refreshing of both hosts and subsystems has been improved when pair definitions are written in HORCM_DEV format and the pairs are created in Hitachi AMS2000, Hitachi SMS, Hitachi AMS/WMS, Thunder 9500V, and Thunder 9200 subsystems.	Device Manager agent	Windows Solaris (SPARC)
18	The refreshing of subsystems has been improved when pair definitions are written in HORCM_LDEV format.	Device Manager agent	All (Note)
19	Device Manager agent now support the following virtualization software: Solaris Logical Domains 1.3	Device Manager agent	All (Note)
20	Device Manager has been improved so that the Device Manager server does not stop when a product other than a Hitachi Storage Command Suite product or related product uses a port from 45001/tcp to 49000/tcp. The related products are as follows:	Device Manager server	All (Note)

	- Hitachi Storage Navigator Modular2 - Hitachi Network Attached Storage/Management		

***Note**:* Applies to all supported operating systems in Device Manager server.

System Requirements

Operating System Requirements

- Server Machine

  See System and Media Requirements in the *Hitachi Device Manager Software Server Configuration and Operation Guide*.

  (1) Web Client
  See the online help.

  (2) CLI
  See Requirements for CLI Operations in the *Hitachi Device Manager Software Command Line Interface (CLI) User's Guide*.

  (3) CLIEX
  See System Requirements in the *Hitachi Device Manager Software Command Line Interface (CLI) User's Guide*.

- Host Agent Machine

  (1) Operating Systems Requirements for a Host Agent Machine
  See Supported OSs in the *Hitachi Device Manager Agent Installation Guide*.

  (2) Patch Requirements for Operating Systems Supported by a Host Agent
  See Applicable OS Patches in the *Hitachi Device Manager Agent Installation Guide*.

- VDS Host Machine
  See Overview of Device Manager VDS Provider in the *Hitachi Device Manager Software Server Configuration and Operation Guide*.

- Mainframe Agent Host Machine
  See the documentation for the *Hitachi Mainframe Agent Software.*

Firmware Levels

- Storage System Firmware version:

  See Required Products for the Storage Subsystem in the *Hitachi Device Manager Software Server Configuration and Operation Guide*.

Prerequisite Programs

- Server Machine

  See System and Media Requirements in the *Hitachi Device Manager Software Server Configuration and Operation Guide*.

- Client Machine

  (1) Web Client
  See the online help.

  (2) CLI
  See Requirements for CLI Operations in the *Hitachi Device Manager Software Command Line Interface (CLI) User's Guide*.

  (3) CLIEX
  See System Requirements in the *Hitachi Device Manager Software Command Line Interface (CLI) User's Guide*.

- Host Agent Machine

  See Applicable OS Patches and Applicable Java Programs in the *Hitachi Device Manager Agent Installation Guide*.

- VDS Host Machine

  None

Memory and Disk Space Requirements

Program name	Machine	Memory	Disk space
Device Manager Server (Windows)	Server	1 GB	3.4 GB (*1)
Device Manager Server (Solaris)	Server	1.5 GB	3.3 GB (*2)
Device Manager Server (Linux)	Server	1.5 GB	3.3 GB (*2)
Web Client (on Windows)	Client	120 MB	30 MB
Web Client (on Solaris)	Client	150 MB	40 MB
Web Client (on HP-UX)	Client	150 MB	40 MB
Device Manager Agent (Windows)	Host	(*4)	(*3)
Device Manager Agent (Solaris)	Host	(*4)	(*3)
Device Manager Agent (HP-UX)	Host	(*4)	(*3)
Device Manager Agent (AIX)	Host	(*4)	(*3)
Device Manager Agent (Linux)	Host	(*4)	(*3)
VDS Provider	Host	200 MB	20 MB
Device Manager CLIEX (Solaris)	Client	10 MB	65 MB
Device Manager CLIEX (Windows)	Client	10 MB	13 MB

(*1) The following table lists the required disk space (Windows):

OS	Folder	Disk space	Remarks
Windows	*<Hitachi-Device-Manager-Software-installation-folder>*	0.8 GB + 0.6 GB (for the Hitachi Device Manager Software database)	
	<Common-data-area-for-Hitachi-Storage-Command-Suite-Common-Component-and-Hitachi-Storage-Command-Suite-products>	0.8 GB + 1.2 GB (for the Hitachi Storage Command Suite Common Component database)	
	The drive of the folder displayed by the TMP environment variable	300 MB	Temporary disk space is required during installation.
	The "system drive:\Program Files" folder	0.8 MB	Disk space is required for the Hitachi Network Objectplaza Trace Monitor 2 installation.

(*2) The following table lists the required disk space (Solaris/Linux):

Directory	Default installation directory	Disk space
Installation destination for the Hitachi Device Manager Software server	/opt/HiCommand #2	1.50 GB
Installation destination for Hitachi Storage Command Suite Common Component	/opt/HiCommand/Base #2	
Storage destination of the database for the Hitachi Device Manager Software server #1	/var/*<Installation-destination-for-the-Hitachi-Device-Manager-Software-server>*/database	0.60 GB
A temporary directory	/var/tmp	1.50 GB
Common data area for Hitachi Storage Command Suite Common Component and Hitachi Storage Command Suite#1	/var/*<Installation-destination-for-Hitachi-Storage-Command-Suite-Common-Component>* #3	0.01 GB
	/var/<Installation-destination-for-Hitachi-Storage-Command-Suite-Common-Component>/database #3	1.20 GB

Note

#1: The database directory can be specified during installation.
By default the database directory is specified as shown above. However, additional disk space is required if an optional directory is specified for the database directory.

#2: You can change this path in Solaris 10 (x64 edition) or Linux.

#3: The directory name under "/var" directory is set to <*Installation directory path name of Hitachi Storage Command Suite Common Component*>

(*3) The following table lists the required disk space on each OS:

OS	Folder/Directory	Disk space	Remarks
Windows	<*Hitachi-Device-Manager-Software-Agent-installation-directory*>	180 MB	About 100 MB of disk space is required in the system drive during installation.
	system-drive\Program Files\HITACHI\HGLMAgent	25 MB	
Solaris	/opt	45 MB	The following amount of disk space is required in the /var/tmp directory during installation. - New installation: 30 MB - Upgrade installation: 80 MB
	/var/opt	5 MB	
AIX	/usr	35 MB	The following amount of disk space is required in the /var/tmp directory during installation. - New installation: 30 MB - Upgrade installation: 80 MB
	/var/opt	5 MB	
Linux (x86 or x64 Edition)	/opt	100 MB	The following amount of disk space is required in the /var/tmp directory during installation. - New installation: 125 MB - Upgrade installation: 175 MB
	/var/opt	5 MB	
Linux (IPF Edition)	/opt	140 MB	The following amount of disk space is required in the /var/tmp directory during installation. - New installation: 155 MB - Upgrade installation: 205 MB
	/var/opt	5 MB	
HP-UX	/opt	20 MB	The following amount of disk space is

	/var/opt	5 MB	required in the /var/tmp directory during installation. - New installation: 30 MB - Upgrade installation: 80 MB

(*4) For the total amount of required memory of the Hitachi Device Manager Software agent, see Specifying Settings When a Host Manages 100 or More LUs in the *Hitachi Device Manager Agent Installation Guide*.
The total amount of required memory is the value of the server.agent.maxMemorySize property in the server.properties property file of the Hitachi Device Manager Software agent.
The default value of the server.agent.maxMemorySize property is 64MB.

(*5) To install Device Manager CLIEX, about 30 MB of free disk space is required in both /opt/HDVMCLIEX and /var, and about 5 MB in the RMLIB installation directory.

Fixed Problems

From 6.3.0-00 to 6.4.0-00

#	Corrected Problems	Applied products	Applied OS
1	The following problem has been corrected: For the 9200 series, the 9500V series, the Hitachi AMS/WMS series, and Hitachi SMS100, the Device Manager server reports the alert KAID11007-W, which indicates a controller failure, even though an actual controller failure has not occurred.	Device Manager server SER-483	Windows Solaris (SPARC)
2	The following problem has been corrected: If CreateOrModifyElementFromStoragePool is executed for HITACHI_StorageConfigurationService, a storage volume may be created with a RAID level different from the RAID level specified in the Goal element.	Device Manager server CIM-486	All (Note)
3	The following problem has been corrected: If CreateSetting is executed for HITACHI_StorageCapabilities, the operation fails with a return value of 4 (Failed).	Device Manager server CIM-487	All (Note)
4	The following problem has been corrected: When Device Manager agent 5.0.0-00 to 6.3.0-00 is installed, the OS becomes unstable or terminates, or the Device Manager agent fails to be stopped, installed or uninstalled due to the memory shortage.	Device Manager agent AGT-490	All (Note)
5	The following problem has been corrected: When CIM client requires an instance of CIM_BlockStorageStatisticalData class, the property "TotalIOs" could be 0 even if the actual value is not 0.	Device Manager server CIM-492	Windows Solaris (SPARC)

6	The following problem has been corrected: The TotalIOs of HITACHI_BlockStatisticalDataStorageVolume may be larger than the value that the storage subsystem stores.	Device Manager server CIM-493	All (Note)
7	The following problem has been corrected: In Detailed Array Reports, capacity values for LDEVs that are larger than 2 TB, and consumed capacity values for LDEVs that are larger than 2 TB are always output incorrectly as 2 TB.	Device Manager Web Client GUI-495	All (Note)
8	The following problem has been corrected: When an operation in Web Client or CLI is done after one of the following operations in Web Client or CLI, a heap memory shortage occurs even if the setting for the maximum heap size of Device Manager server is 1024 MB. As a result, the operation may fail, or the service of the Device Manager server may stop. (a) Storage subsystems are added, refreshed or deleted. (b) Virtualization servers are added, refreshed or deleted. (c) The mappings of external volumes are removed. If the operation fails, in the Device Manager Web Client the error message KAIC07477-E is displayed, or in CLI the error message KAIC90083-E (error code = 7477) is output. Also, the following problems may occur in Hitachi Storage Command Suite products: - An addition or deletion of a storage subsystem for Tiered Storage Manager may fail with the error message KAIC07477-E. - An operation to refresh subsystems in Replication Manager may fail with the error message RPM-01004 and an operation to refresh configuration may fail with the error message RPM-01013.	Device Manager server SER-496	All (Note)
9	The following problem has been corrected: When multiple Hitachi USP or Universal Storage Platform V/VM are mapped to the same external storage subsystem, CIM client may not be able to acquire the capacity value of HITACHI_StoragePool correctly.	Device Manager server CIM-499	All (Note)
10	The following problem has been corrected: When a storage subsystem other than SMI-S Enabled storage subsystem is connected to Hitachi USP or Universal Storage Platform V/VM as an external subsystem and Device Manager manages the subsystems, CIM client may not be able to acquire the instances of following classes. - HITACHI_AssociatedStoragePoolComponentArrayGroup - HITACHI_AssociatedStoragePoolRemainingFreeSpace - HITACHI_StoragePoolComponentArrayGroup - HITACHI_StoragePoolComponentFreeSpace	Device Manager server CIM-500	All (Note)
11	The following problem has been corrected: When Device Manager manages an SMI-S Enabled subsystem, the Refresh Storage Subsystem - Confirmation dialog box is not displayed even if the Refresh button is clicked in Web	Device Manager Web Client GUI-502	All (Note)

	Client. As a result, the SMI-S Enabled subsystem cannot be refreshed.		
12	The following problem has been corrected: In Device Manager Web Client, if a host containing Universal Replicator pairs is refreshed or a HiScan is performed on the host, the following problems occur: (a) Even after a pair is created in Web Client, the copy status does not refreshed, and it remains "Copying". (b) Even though an appropriate operation is performed after the status of a Universal Replicator pair managed by Web Client is manually changed, the pair information is not refreshed. (c) Even though an appropriate operation is performed after a Universal Replicator pair is created, the information regarding the created pair is not displayed.	Device Manager agent AGT-504	All (Note)
13	The following problem has been corrected: When Device Manager manages an SMI-S Enabled subsystem, the Modify Properties - *subsystem-name* dialog box is not displayed even if the Modify Properties button is clicked in Web Client. As a result, the properties of SMI-S Enabled subsystem cannot be changed.	Device Manager Web Client GUI-505	All (Note)
14	The following problem has been corrected: When Device Manager manages an SMI-S Enabled subsystem, the Remove Subsystem - Confirmation dialog box is not displayed even if the Remove Subsystem button is clicked in Web Client. As a result, the SMI-S Enabled subsystem cannot be removed.	Device Manager Web Client GUI-506	All (Note)
15	The following problem has been corrected: When Device Manager manages an SMI-S Enabled subsystem, the management tool for the SMI-S Enabled subsystem is not started even if the Manage button is clicked in Web Client.	Device Manager Web Client GUI-507	All (Note)
16	The following problems have been corrected: The following problems occur when a 17th generation or later Snapshot pair is created in a Hitachi AMS2000 or Hitachi SMS storage subsystem: (1) The status of the copy pair is displayed as simplex when the host is refreshed by using Device Manager Web Client, or when the HiScan command is executed on the host on which the agent is installed. (2) The copy pair is not displayed in the copy group list when the configuration is updated in Replication Manager Web Client.	Device Manager agent AGT-509	All (Note)
17	The following problem has been corrected: The following problems occur when deleting DP VOLs in Web Client: (1) Deleting DP VOLs takes a long time. (2) If deleting DP VOLs takes longer than the time specified for the server.dispatcher.message.timeout.in.processing property in the dispatcher.properties properties file, the operation fails with the error message KAIC07202-E.	Device Manager Web Client GUI-513	All (Note)

18	The following problem has been corrected: In web client, when two or more LDEVs were selected, the Edit Label - *object-name* dialog box was displayed, and the links for the second LDEV onward were selected, the KAIC11999-E message was displayed and the LDEV Information dialog box was not displayed.	Device Manager Web Client GUI-515	Windows Linux
19	The following problem has been corrected: By using the HiKeyTool and selecting "2) SSL with two-way authentication", authentication used for object operations or indications cannot be changed from one-way to two-way of Device Manager setting.	Device Manager server CIM-518	All (Note)
20	The following problem has been corrected: If multiple virtualization servers are managed by Device Manager, information regarding the virtual machines on the 2nd and later virtualization servers is not properly registered in Device Manager. As a result, the information regarding the virtual machines on the 2nd and later virtualization servers is not properly displayed in Tuning Manager Web Client.	Device Manager server SER-524	Windows
21	The following problem has been corrected: In Web Client, an operation for the storage subsystems fails and the KAIC05305-E error message is displayed, even if there is no user operating Hitachi AMS2100, Hitachi AMS2300, or Hitachi AMS2500.	Device Manager Web Client GUI-527	Windows Solaris (SPARC)

***Note**:* Applies to all supported operating systems in Device Manager server.

Known Problems

- Restriction on Mozilla 1.7.13 (HP-UX 11iv3) support:
  In this release, Device Manager Web Client does not support connecting to a Device Manager server by using Mozilla 1.7.13 (HP-UX 11iv3 on PA-RISC) with an IPv6 protocol.
- Restriction on Installing the Device Manager Server
  If the Device Manager server manages a large-scale environment, we do not recommend using ZFS (Zettabyte File System) because problems may occur when the storage subsystem is refreshed. Instead, we recommend using UFS (UNIX File System).
  If the Device Manager server is installed in a ZFS environment, the following procedure is available to re-install it in a UFS environment.

  (1) Exporting the database

  1. If Hitachi Storage Command Suite products have been installed, stop their services.
     For details about how to stop these services, see the relevant manual for the product version used.
  2. Execute the following commands to stop Hitachi Storage Command Suite Common Component, and then start HiRDB.

installation-directory-for-Hitachi-Storage-Command-Suite-Common-Component/bin/hcmdssrv –stop

installation-directory-for-Hitachi-Storage-Command-Suite-Common-Component/bin/hcmdsdbsrv –start

The following examples show how to execute the commands:
/opt/HiCommand/Base/bin/hcmdssrv –stop
/opt/HiCommand/Base/bin/hcmdsdbsrv -start

3. From the terminal window, execute the hcmdsdbtrans command as described below.

   The auto option can be specified only if Hitachi Storage Command Suite products have been installed:

   installation-directory-for-Hitachi-Storage-Command-Suite-Common-Component/bin/hcmdsdbtrans -export -workpath working-directory -file archive-file

   The following example shows how to execute the command:

   # /opt/HiCommand/Base/bin/hcmdsdbtrans -export -workpath /opt/trans_work -file /opt/trans_file/db_arc

   Caution: Before exporting the database, review the notes in Migrating the Server Database in the *Hitachi Device Manager Software Server Configuration and Operation Guide*.

(2) Removing the Device Manager server

Move the current directory to the root (/), and then execute the following command:

installation-directory-for-the-Device-Manager-server/Uninstall/uninstall.sh

Caution: Before uninstalling the Device Manager server, review the notes in Uninstalling the Device Manager server and Related Products in the *Hitachi Storage Command Suite Software Server Installation Guide Device Manager Provisioning Manager Tiered Storage Manager*.

(3) Performing a new installation

1. Move the current directory to the directory that stores the Device Manager server installer (install.sh). Then, execute the following command:

   # ./install.sh

2. Specify a UFS directory in which the Device Manager server database files are stored.

   Caution: Before installing the Device Manager server, review the notes in Installing the Device Manager server and Hitachi Storage Command Suite Common Component in the *Hitachi Storage Command Suite Software Server Installation Guide Device Manager Provisioning Manager Tiered Storage Manager*.

(4) Importing the database

1. From the terminal window, execute the hcmdsdbtrans command as follows:

   installation-directory-for-Hitachi-Storage-Command-Suite-Common-Component/bin/hcmdsdbtrans -import -workpath working-directory [-file archive-file] -type {ALL | Hitachi Storage Command Suite products-whose-databases-will-be-migrated} -auto

   The following example shows how to execute the command:

   # /opt/HiCommand/Base/bin/hcmdsdbtrans -import -workpath /opt/trans_work -file /opt/trans_file/db_arc -type ALL -auto

2. Synchronize the repository information with the imported Device Manager database information.

   In the server.properties file, specify true for the server.base.initialsynchro property.

   The hcmdsdbtrans command does not migrate the Hitachi Storage Command Suite products repository information other than user information. Therefore, it is necessary to synchronize the repository information with the database information of the imported Device Manager server.

3. Execute the following command to start the Hitachi Storage Command Suite product services and Hitachi Storage Command Suite Common Component of the migration destination:

   installation-directory-for-Hitachi-Storage-Command-Suite-Common-Component/bin/hcmdssrv -start

   The following example shows how to execute the command:

   # /opt/HiCommand/Base/bin/hcmdssrv -start

4. Change the value of the server.base.initialsynchro property in the server.properties file back to false.

Caution: Before importing the database, review the notes in Migrating the Server Database in the *Hitachi Device Manager Software Server Configuration and Operation Guide*.

- Restriction on using CLI to create copy pairs

  If the parameter replicationfunction is omitted in either of the following operations, an error (KAIC90083-E) occurs.

  - Creating a copy pair by using the AddReplication command
  - Creating a configuration file by using the AddConfigFileForReplication command

  If you use the above commands to perform the above operations, you must specify the parameter replicationfunction.

- Restriction on configuration changes of a storage subsystem

  When a configuration is changed during refreshing for any of the following storage subsystems, the configuration changes may fail with the error message KAIC05000-E if the operation to refresh the storage subsystem fails.

  If this problem occurs, retry the configuration changes.

  - SANRISE2000
  - SANRISE9900V
  - Hitachi USP
  - Universal Storage Platform V/VM

- Restriction on linking with the Storage Navigator Modular 2

  When an operation for a dialog box in Web Client is performed during loading the screen of Storage Navigator Modular 2 by linking with the Storage Navigator Modular 2, the error message DMEG800005 may occur.

  When the error above occurs, continue the operation in Web Client.

Installation Precautions

Please review the following manual references for installation:

- Device Manager Server

  See Installing in the *Hitachi Storage Command Suite Software Server Installation Guide Device Manager, Provisioning Manager, Tiered Storage Manager*.

- Web Client

  See the online help

- CLI

  (CLI)

See Requirements for CLI Operations in the *Hitachi Device Manager Software Command Line Interface (CLI) User's Guide.*

(CLIEX)

See System Requirements in the *Hitachi Device Manager Software Command Line Interface (CLI) User's Guide.*

- Device Manager Agent

  See Installing the Device Manager Agent in Windows and Installing the Device Manager Agent in UNIX in the *Hitachi Device Manager Agent Installation Guide*.

- Device Manager VDS Provider:

  See Installation Requirements and Procedures in the *Hitachi Storage Command Suite Software Server Installation Guide Device Manager, Provisioning Manager, Tiered Storage Manager.*

Usage Precautions

Hard disks supported in this version

In this version, the following hard disks are supported by the Hitachi SMS, Hitachi AMS/WMS, 9500V series and 9200 series.

Hard	Type	Hitachi SMS series	Hitachi AMS (*1)	Hitachi AMS/WMS (*2)	9500V series	9200 series
9 GB	FC	--	--	--	--	S
18 GB	FC	--	--	--	--	S
36 GB	FC	--	--	--	S	S
72 GB	FC	--	--	S	S	S
146 GB	FC/SAS	S	S	S	S	--
180 GB	FC	--	--	--	--	S
250 GB	SATA	--	--	S	S	--
300 GB	FC/SAS	S	S	S	S	--
400 GB	SATA	--	--	S	S	--
400 GB	FC/SAS	S	S	S	--	--
450 GB	SAS	S	S	--	--	--
500 GB	SATA	S	S	S	S	--
750 GB	SATA	S	S	S	--	--
1 TB	SATA	S	S	S	--	--

Legend

S: Supported

--: Not supported

(*1) For AMS2500, AMS2300, and AMS2100.

(*2) For AMS1000, AMS500, AMS200, and WMS100.

About the SMI-S Indication Function

In interop namespace, only the query described in SMI-S1.3 can be set for the Query property of CIM_IndicationFilter.

Notes on using the Device Manager agent on the VMware ESX Server 4.x guest OS or on the VMware ESXi Server 4.x guest OS

When using the Device Manager agent on the VMware ESX Server 4.x guest OS or the VMware ESXi Server 4.x guest OS, the following problems may occur if creating or deleting a copy pair from Web Client:

- Even after a copy pair is created, the Copy Type of the target volumes remains Unpaired.

- Even after a copy pair is deleted, the Copy Type of the target volumes remains the same status as that before the deletion.

To correctly display the statuses of the Copy Type, refresh the storage subsystem.

Note on referencing a Physical Configuration of Storage Subsystem report (in HTML format)

If a Physical Configuration of Storage Subsystem report (in HTML format) is retrieved for a storage subsystem that meets either of the conditions below, the message "No channel adapters were reported for this Storage Subsystem." is displayed even if a channel adapter exists.

(1) The storage subsystem does not contain any hard disks.

(2) Any of the following storage subsystems are added by a user ID that has storage partitioning administrator permissions, and the assigned SLPR contains only virtual volumes:

- Hitachi Universal Storage Platform
- Hitachi Universal Storage Platform 1100
- Hitachi Universal Storage Platform 600
- Hitachi Universal Storage Platform 100
- Universal Storage Platform V

If either of these conditions is met, refer to the figure in the window for channel adapter information.

Notes on adding storage systems

The KAIC07133-E error may occur when storage subsystem is added. If an error occurs, perform the following the procedures below to check the number of WWNs, and then delete any unnecessary WWNs.

(1) When using Storage Navigator Modular or Storage Navigator Modular 2:

(1-1) When using Storage Navigator Modular 2 to add Hitachi AMS 2000 or Hitachi SMS storage subsystem:

Follow the procedure below to check the number of WWNs:

1. Select a group from the navigation area.
2. Select a host group from the application area.
3. Select the WWN tab from the application area.
4. Click the [Filter] button.
5. Set the port specified by Device Manager as a condition, and then click the [OK] button.
6. Count the number of WWNs in the displayed results.

Use Storage Navigator Modular 2 to delete WWNs.

(1-2) When using Storage Navigator Modular to add Hitachi AMS/WMS or Thunder 9500V storage subsystem:

Add up the WWNs in 1. and 2. below. If the same WWN is in both 1. and 2., count it as one WWN:

1. The WWNs that are automatically detected when the target port is selected under Host Groups.
2. The WWNs displayed for the WWN property of each host group.

Use Storage Navigator Modular to delete WWNs.

(2) When using Device Manager CLI:

Execute the GetStorageArray (subtarget=Port) command, and then count the number of WWN instances. Use the DeleteWWN command to delete WWNs. For details, see the Device Manager CLI manual.

Notes on changing Threshold1 from the Modify DP Pool dialog box

If the state of the DP pool is not "Normal", the dropdown list for Threshold1 is inactive.

- If the state of the DP pool is "Over Threshold":

Use Physical View to change Threshold1.

- If the state of the DP pool is neither "Normal" nor "Over Threshold":

  Threshold1 for the DP pool cannot be changed due to the device specifications.

Note on file server cluster names

Specify file server cluster name to be unique in the Device Manager server. If a cluster name is not unique, the cluster cannot be properly identified.

Note on the host name length of Device Manager Agent host

The host name length of Device Manager Agent host must be 50 bytes or fewer.

Note on when Device Manager manages VMware ESX 3.5 without using VMware vSphere Management Assistant (vMA)

If Device Manager is managing multiple instances of VMware ESX 3.5 without using vMA, only one virtual machine can be managed among any virtual machines whose configuration files have the same name (#) and whose configuration file names (#) exceed 60 bytes.

Use vMA to avoid this problem.

#: The full path with the virtual machine working location

Ex. "[Datastore1] vm1/vm1.vmx"

Note on the Modify Properties - subsystem-name dialog box

The description below is shown in the Help dialog displayed when the [Help] button is clicked in the Modify Properties - *subsystem-name* dialog box. However, it is not necessary to enter a user ID and password. You only need to enter a user ID and password when you want to change them.

- "When Account Authentication is used in Hitachi SMS and Hitachi AMS2000/AMS/WMS, you must enter an Account Authentication user ID and password."

Notes on upgrading Device Manager in an environment where virtualization servers are managed

In an environment where Device Manager manages virtualization servers, after upgrading Device Manager, make sure to refresh the information for all the managed virtualization servers.

If virtualization servers are managed in a system configuration where VMware vSphere Management Assistant (vMA) monitors VMware vCenter, re-register the vMA information into Device Manager to refresh the information for all the virtualization servers connected to the monitored VMware vCenter.

Note on the error KAIC10480-E occurs

If the error KAIC10480-E occurs and the error code is 48L, log out and then log in again.

If the problem is not solved, collect maintenance information, and then contact customer support.

Notes on settings when linking to a Windows2008 Active Directory (Domain Controller) as a Kerberos external authentication server from HSCS products for Windows

When Domain functional level of Windows Server 2008 Active Directory (domain controller) is configured by other than Windows Server 2008 level, Kerberos authentication between HSCS products for Windows and the Active Directory server fails.

To avoid this problem, the type of encryption that HSCS products use must be restricted to "rc4-hmac" only. In detail, perform the following procedures:

(1) Open the following file by text editor.

<*installation-folder-for-Common-Component*>\conf\exauth.properties

(2) Append the following line to the file described in (1).

```
auth.kerberos.default_tkt_enctypes=rc4-hmac
```

(3) Overwrite the file described in (2), and then quit the text editor.

Notes on when Device Manager manages a virtual machine

When Device Manager manages a virtual machine, the characters of the machine name in the followings are displayed as encoded characters:

(a) In Web Client:

- Value of [VMname] displayed in a virtual machine name subwindow

(b) In CLI:

- name attribute value for VM inctances that is collected by executing the GetHost command.

The following characters may be displayed as encoded characters.

#	character	displayed character
1	%	%25
2	/	%2f
3	\	%5c

Documentation

Available Documents

Manual Name	Manual No.	Issue Date
Hitachi Device Manager Software Server Configuration and Operation Guide	MK-08HC157-04	June, 2010
Hitachi Device Manager Software Command Line Interface (CLI) User's Guide	MK-91HC007-27	June, 2010
Hitachi Device Manager Software Error Codes	MK-92HC016-23	June, 2010
Hitachi Device Manager Agent Installation Guide	MK-92HC019-22	June, 2010
Hitachi Device Manager Software Getting Started Guide	MK-98HC149-03	December, 2009
Hitachi Storage Command Suite Software Server Installation Guide Device Manager Provisioning Manager Tiered Storage Manager	MK-98HC150-04	June, 2010

Documentation Errata

Hitachi Device Manager Software Server Configuration and Operation Guide corrections.

- The section Checking the Data Structure and Authentication Method that starts on page 3-12 and ends on page 3-14 is not valid.
- Section 3 (Settings Required to Authenticate Users by Using an External Authentication Server) in chapter 3 (Settings Required for Managing User Accounts) is not valid. The correct information is:

Active directory authorization configuration settings

Active Directory Prerequisites

Domain Name: hitachi.hds

Active Directory Certificate Services Installed (Enterprise CA)

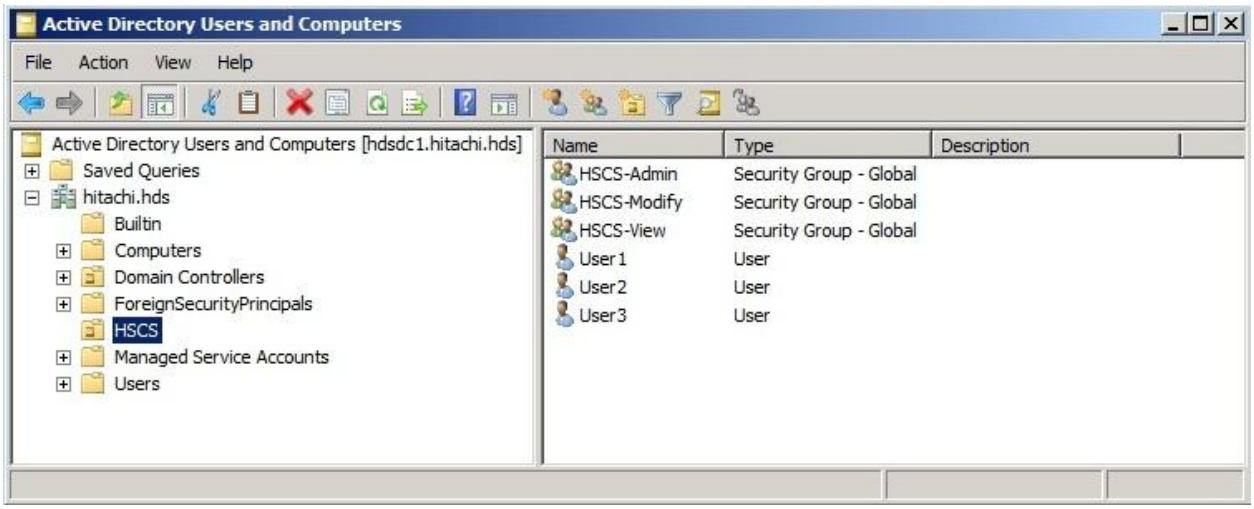
1) In Active Directory Users and Computers (ADUC), create an Organizational Unit (OU): HSCS

2) In the Hitachi Storage Command Suite Organizational Unit (HSCS OU), create the following Storage Management users:
   - User1
   - User2
   - User3

Note that in most cases, Active Directory (AD) passwords must be changed the first time you log in, and when they expire.

3) In ADUC, create the following HSCS OU groups:

- HSCS-Admin
- HSCS-Modify
- HSCS-View



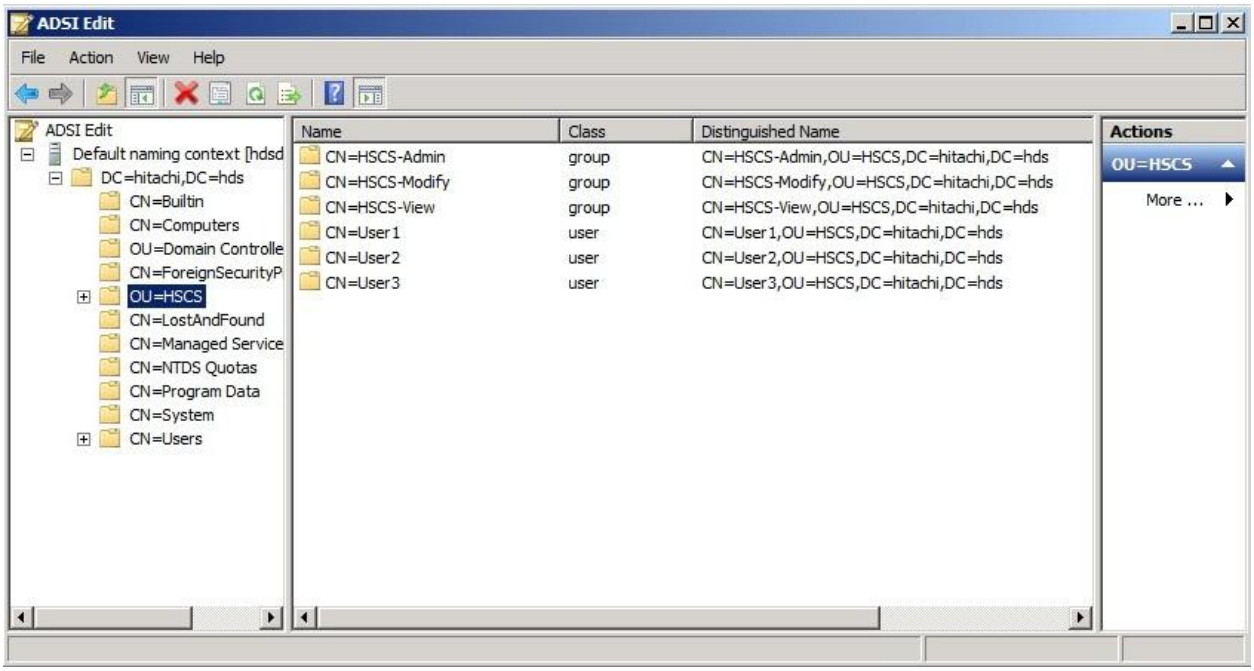
4) Add the users (created in step 2) to the groups (created in step 3) as follows:
   - User1 = HSCS-Admin
   - User2=HSCS-Modify
   - User3 = HSCS-View

5) Create or identify an AD Search User with HSCS OU access:
   - Administrator (For this test, use a Domain Administrator, but a user with directory search capabilities will also work)
6) Note the OU HSCS Distinguished Name created in step 2:
   - OU=HSCS,DC=hitachi,DC=hds

7) Note the HSCS-Admin Group Distinguished Name created in step 3:
   - CN=HSCS-Admin,OU=HSCS,DC=hitachi,DC=hds

8) Note the HSCS-Modify Group Distinguished Name created in step 3:
   - CN=HSCS-Modify,OU=HSCS,DC=hitachi,DC=hds

9) Note the HSCS-View Group Distinguished Name created in step 3:
   - CN=HSCS-View,OU=HSCS,DC=hitachi,DC=hds



10) Note the AD Search User Distinguished Name and Password created or identified in Step 5:
    - CN=Administrator,CN=Users,DC=hitachi,DC=hds

Hitachi Device Manager (HDvM) AD Authentication and Authorization – Lightweight Directory Access Protocol (LDAP) using Domain Name Service (DNS)

1) Open a command prompt and register the AD Search User as defined in chapter 3 of the document MK-08HC157. For example, the command on a Windows system can be:

```
C:\Program Files (x86)\HiCommand\Base\bin>
hcmdsldapuser /set /dn CN=Administrator,CN=Users,DC=hitachi,DC=hds"
/pass St@rt_123 /name AD
KAPM05250-I Registration of the information-search user has finished.
```

2) Note the server name for the user registration process in step 1 (for example, AD).

3) Open the exauth.properties file, only the following entries, and then save the file. Note the use of AD specified with the AD Search User.

```
# Select the authentication server type.
# Enter "internal", "ldap", "radius" or "kerberos".
auth.server.type=ldap

# For Directory Server or RADIUS Server.
# Specify the authentication server identification name.
auth.server.name=AD

# External authentication group definitions.
auth.group.mapping=true

# Environment Settings for the Directory Server:
# The connection protocol for the directory server.
auth.ldap.AD.protocol=ldap

# The connected server name.#
#auth.ldap.ServerName.host=ldap.example.com

# The number of the port used for the server connection. (default: 389)
auth.ldap.AD.port=389

# The connection timeout period (in seconds).
auth.ldap.AD.timeout=15

# The user identification attribute.
auth.ldap.AD.attr=sAMAccountName
```

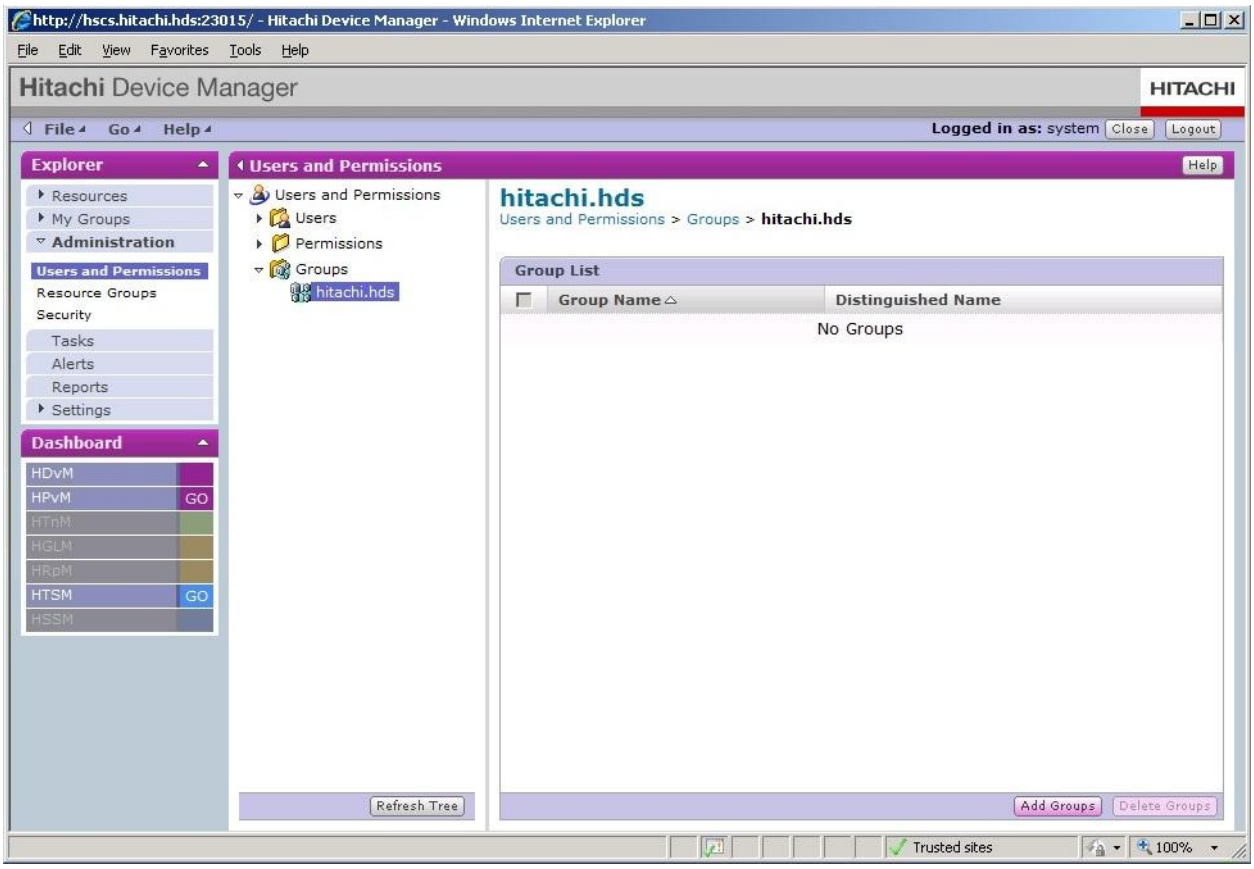
```
# The base point directory.
auth.ldap.AD.basedn=OU=HSCS,DC=hitachi,dc=hds

# The connection retry interval (in seconds).
auth.ldap.AD.retry.interval=1

# The connection retry times.
auth.ldap.AD.retry.times=20

# Authorization server domain.
auth.ldap.AD.domain.name=hitachi.hds

# DNS server reference specification of the directory server address.
auth.ldap.AD.dns_lookup=true
```

4) Log in the HDvM browser using the following link http://hscs.hitachi.test:23015/DeviceManager/ and use the local administrator account (system/manager).

5) Click the Administration tab and select **Users and Permissions**.

6) Expand Users and Permissions and then expand Groups.

7) Under Groups, verify that the AD Domain name, hitachi.hds, appears.

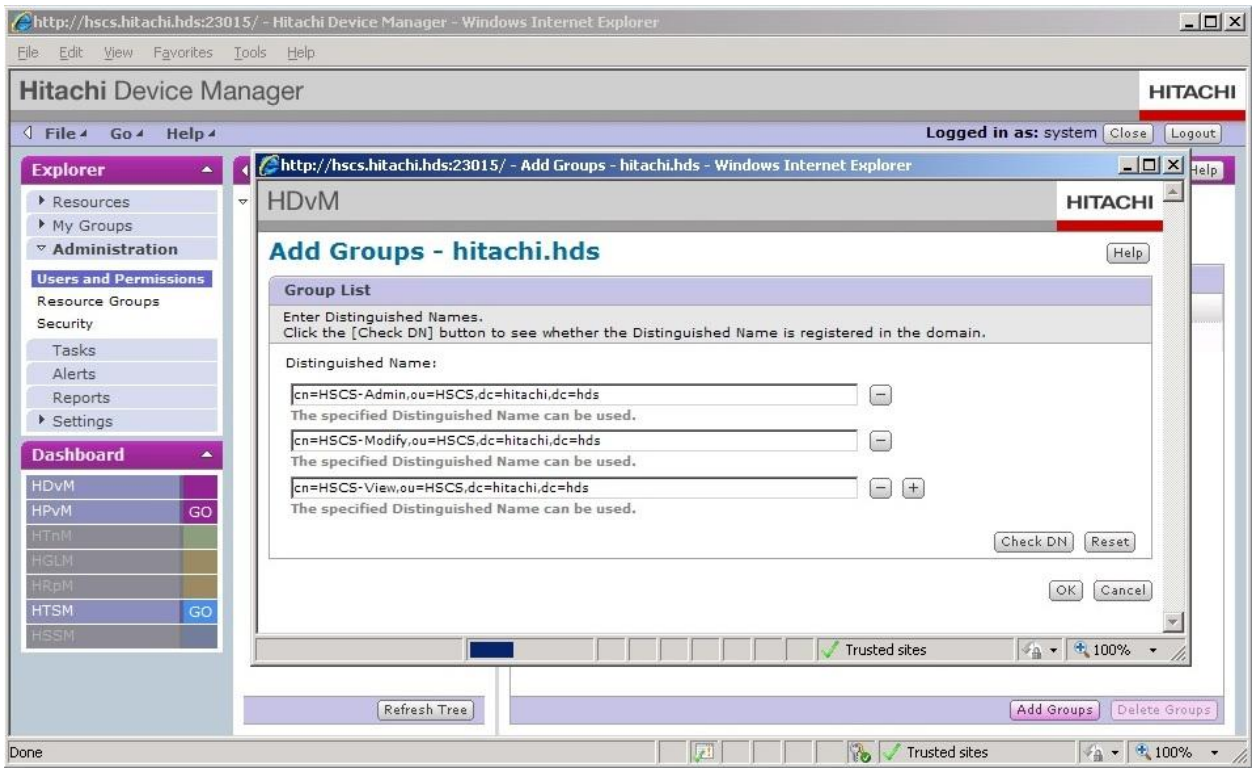


8) Click **Add Groups** in the lower right. The Add Groups dialog box appears.

9) Add the Distinguished Names for the three groups listed in steps 7, 8, and 9 of the AD section.

10) Click **Check DN**.

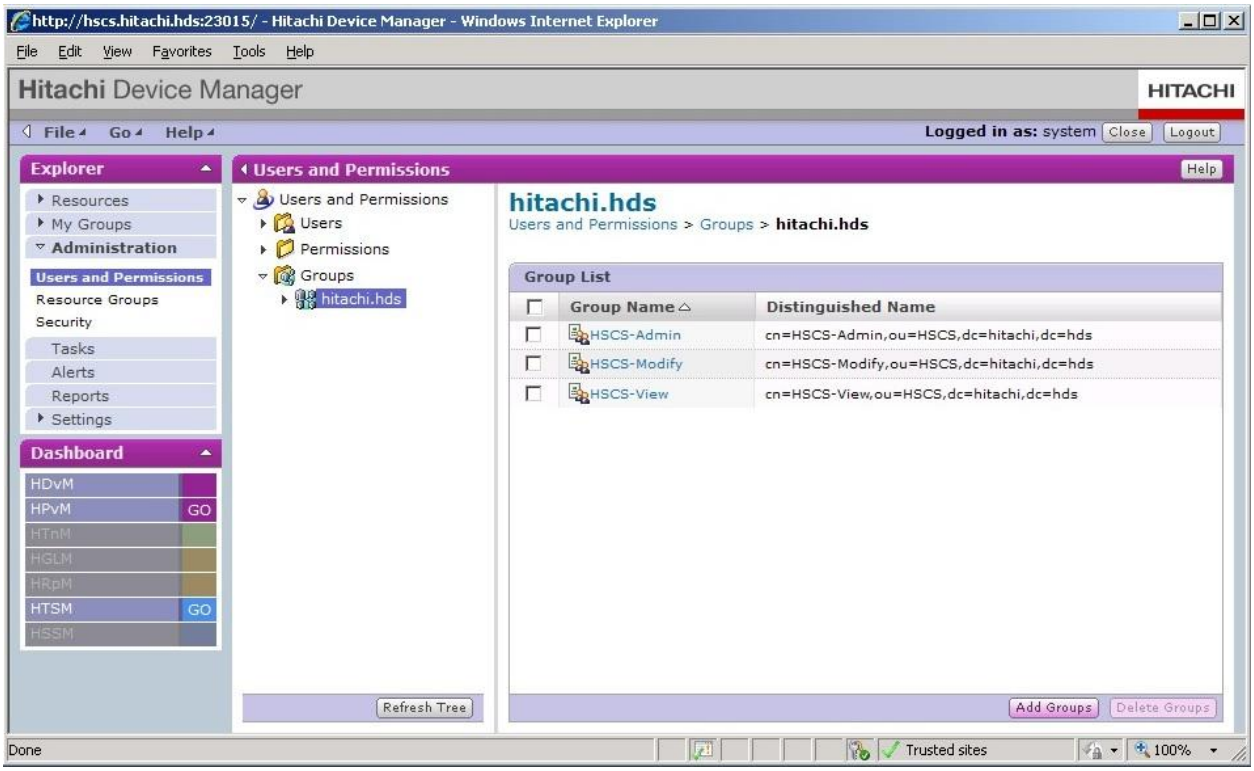
11) If the Check DN test is successful, click **OK**.



Assigning Group Permissions

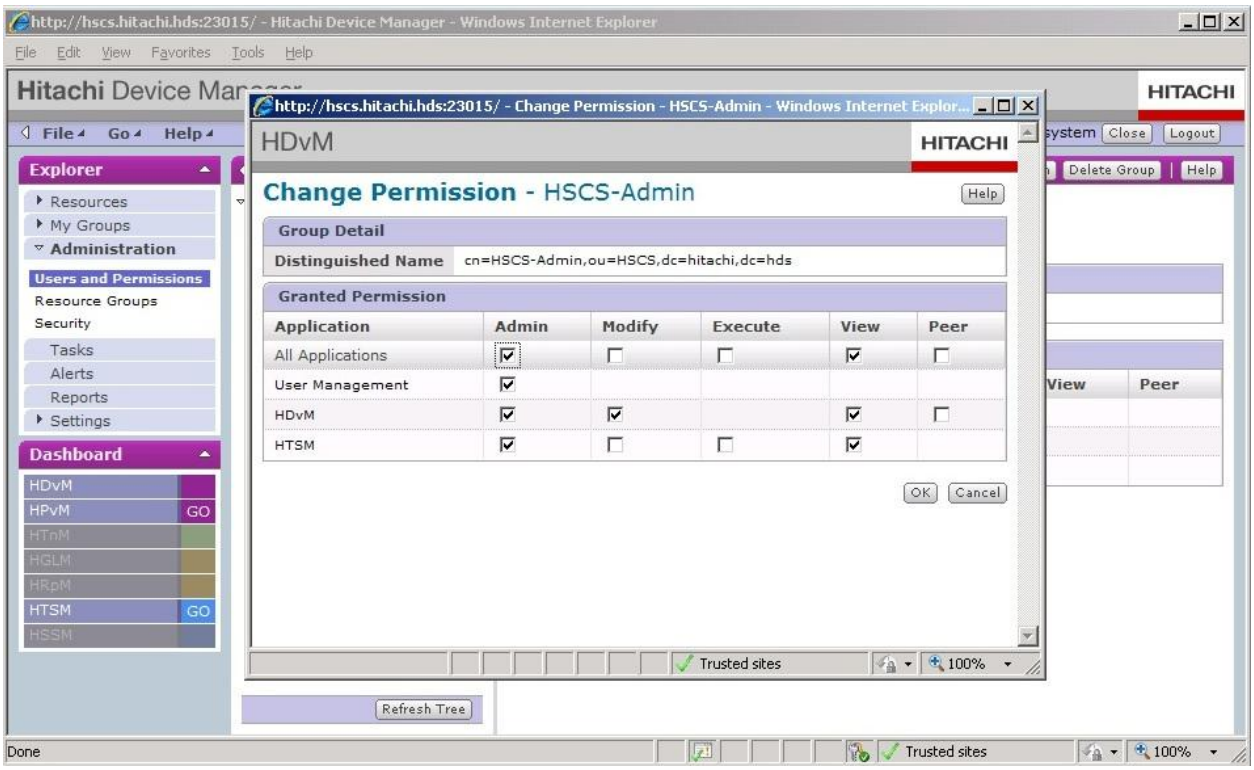
1) Under the Groups icon, expand the domain name (for example, hitachi.hds).

2) Verify that these groups appear:
   - HSCS-Admin
   - HSCS-Modify
   - HSCS-View



3) Select the appropriate group and click **Change Permission** in the upper right. A new dialog box appears.

4) Select the appropriate permission for the group and click **OK**. Repeat this for the other 2 groups.



5) Log out of HDvM.

6) Log back in using the AD User account and verify whether it has appropriate permissions.

Using LDAP with Transport Layer Security (TLS) to protect Authentication and Authorization

The directory contents affect environments and for the Active Directory, the domain controllers that HDvM securely connects to with LDAP and TLS must be configured with a certificate. This certificate can be issued by Verisign or another trusted Certificate Authority (CA) organization.

TLS Configuration Information for Active Directory

When configuring TLS to work with Active Directory, note the following.

- Unless the guidance in KB321051 is followed, AD implementation may not present the correct certificate in a multi-certificate scenario. If a Windows Server 2008 or a later version domain controller finds multiple certificates in its store, it selects the certificate whose expiration date is longest to negotiate TLS. The Authentication Certificate must have the Subject Name field populated with the Fully Qualified Domain Name (DNS Name) of the system requesting the certificate.
- For Windows Certificate Authority (Active Directory Certificate Services), the Subject Name is only populated on Domain Controller Template certificates (default).
- If your environment has Domain Controllers with additional authentication certificates (other than those based on the Domain Controller Templates), the additional templates must be modified—they must populate the Subject Name with the DNS name of the system requesting the certificate, and they must be reissued to the Domain Controllers.

For more information on managing Active Directory Certificate Services, Enabling LDAP with SSL/TLS, and Certificate Templates, see these Microsoft sources:

- Active Directory Certificate Services (http://technet.microsoft.com/en-us/library/cc772393
- How to Enable LDAP over SSL With A Third-Party Certification Authority (http://support.microsoft.com/kb/321051)
- Implementing and Administering Certificate Templates in Windows Server 2008 (http://www.microsoft.com/downloads/details.aspx?familyid=3C670732-C971-4C65-BE9C-C0EBC3749E24&displaylang=en)

Configuring LDAP with Transport Layer Security (TLS) to protect Authentication and Authorization

1. In the following file, HDvM includes Root Certificates in the Device Manager Server TrustStore.

```
C:\program files\hicommand\base\jdk\jre\lib\security\cacerts
```

2. To see the certificates that are included in the cacerts file, use Hikeytool.bat as follows:

```
C:\Program Files\HiCommand\DeviceManager\HiCommandServer\HiKeyTool.bat
```

3. Selection **Option 1** (SSL configuration for Device Manager Server).

```
================================================================
================================

HiKeytool v6.4.0-00
================================================================
================================

1) SSL configuration for Device Manager Server
2) SSL configuration for SMI-S
3) Exit

>1
```

4. Select **Option 11** (Display contents of Device Manager Server TrustStore).

```
1) Make KeyPair/Self-Signed Certificate
2) Set Device Manager Server Security Level
```

```
3) Generate CSR
4) Import Digitally Signed Certificate
5) Display contents of Device Manager Server KeyStore
6) Display verbose contents of Device Manager Server KeyStore
7) Delete an entry from the Device Manager Server KeyStore
8) Change Device Manager Server KeyPair/Self-Signed Certificate Keypass
9) Change Device Manager Server KeyStore Password
10) Import Certificate to Device Manager Server TrustStore
11) Display contents of Device Manager Server TrustStore
12) Display verbose contents of Device Manager Server TrustStore
13) Delete an entry from the Device Manager Server TrustStore
14) Change Device Manager Server TrustStore Password
15) Exit

>11
```

5. The following appears:

```
Listing Contents of Device Manager Server TrustStore

  Alias
  ==========
1) verisignclass3ca, Thu Nov 24 19:04:38 PST 2005
  MD5  Fingerprints:10:FC:63:5D:F6:26:3E:0D:F3:25:BE:5F:79:CD:67:67
2) verisignclass3g2ca, Thu Nov 24 19:04:37 PST 2005
  MD5  Fingerprints:A2:33:9B:4C:74:78:73:D4:6C:E7:C1:F3:8D:CB:5C:E9
3) verisignclass2g2ca, Thu Nov 24 19:04:35 PST 2005
  MD5  Fingerprints:2D:BB:E5:25:D3:D1:65:82:3A:B7:0E:FA:E6:EB:E2:E1
4) verisignclass1g2ca, Thu Nov 24 19:04:34 PST 2005
  MD5  Fingerprints:DB:23:3D:F9:69:FA:4B:B9:95:80:44:73:5E:7D:41:83
```

```
5) verisignclass3g3ca, Thu Nov 24 19:04:37 PST 2005
  MD5  Fingerprints:CD:68:B6:A7:C7:C4:CE:75:E0:1D:4F:57:44:61:92:09
6) verisignclass2g3ca, Thu Nov 24 19:04:36 PST 2005
  MD5  Fingerprints:F8:BE:C4:63:22:C9:A8:46:74:8B:B8:1D:1E:4A:2B:F6
7) verisignclass1g3ca, Thu Nov 24 19:04:34 PST 2005
  MD5  Fingerprints:B1:47:BC:18:57:D1:18:A0:78:2D:EC:71:E8:2A:95:73
8) verisignclass1ca, Thu Nov 24 19:04:35 PST 2005
  MD5  Fingerprints:97:60:E8:57:5F:D3:50:47:E5:43:0C:94:36:8A:B0:62
9) verisignserverca, Thu Nov 24 19:04:38 PST 2005
  MD5  Fingerprints:74:7B:82:03:43:F0:00:9E:6B:B3:EC:47:BF:85:A5:93
10) verisignclass2ca, Thu Nov 24 19:04:36 PST 2005
  MD5  Fingerprints:B3:9C:25:B1:C3:2E:32:53:80:15:30:9D:4D:02:77:3E


(A)nother command or E(x)it?
```

6. If your Domain Controller Certificate is not CA listed in the Root Certificates file, the user has two options.
   - Option 1 – Import the certificates into the built-in “CACERTS” file listed in step 1 using the HiKeyTool. Remember that if you import your certificates into this store, they can be overwritten when the product is upgraded and will have to re-imported.
   - Option 2 – create a separate TrustStore with the name “jsseccerts”.
7. If you choose option 2, then open a command prompt, create the TrustStore and load the certificate as follows:

```
C:\Program Files\HiCommand\Base\bin>hcmdskeytool -import -alias hdsca1 -file
"c:\certs\hdsca1.cer"
 -keystore "C:\program files\hicommand\base\jdk\jre\lib\security\jsseccacerts" -
storepass St@rt_123
```

8. The following appears:

```
Owner: CN=hdsca1, DC=hitachi, DC=hds
Issuer: CN=hdsca1, DC=hitachi, DC=hds
Serial number: 34b60d200a070b8747d9ecc93e9a75d1
Valid from: Tue May 11 19:07:01 PDT 2010 until: Mon May 11 19:16:59 PDT 2015
Certificate fingerprints:
        MD5:  34:D9:33:2B:D7:69:50:17:F3:7C:0F:3F:60:D0:D9:98
        SHA1: 4B:74:8A:8D:29:1D:6E:98:9C:FF:07:A3:5D:50:45:FC:EF:CB:28:AF
Trust this certificate? [no]:  yes
Certificate was added to keystore
```

9. Repeat this to add more certificates as appropriate.

10. When the new TrustStore is created and the certificates are loaded, stop and then start Device Manager.

11. When Device Manager restarts, change the auth.LDAP.ServerName.protocol setting in the exauth.properties file from "ldap" to "tls". The entry in the file must be as follows:

```
# Environment Settings for the Directory Server:
# The connection protocol for the directory server.
auth.ldap.AD.protocol=tls
```

12. Save the exauth.properties file when finished.

Example of exauth.properties file when using Kerberos Authentication with LDAP Authorization using DNS

Device Manager can also use Kerberos Authentication, commonly used in Active Directory environments.

1) Open a command prompt and register the AD Search User as follows (name is the DNS name of the Active Directory domain and Kerberos Realm):

```
C:\Program Files\HiCommand\Base\bin>hcmdsldapuser /set /dn
"cn=administrator,cn=users,dc=hitachi,dc=hds" /pass St@rt_123 /name
hitachi.hds
KAPM05250-I Registration of the information-search user has finished.
```

2) Note the Kerberos Realm name from the user registration process in step 1. This name is used when configuring the exauth.properties file in the next step.

3) Open the exauth.properties file and use only the following entries, and then save the file. Note the use of thee Realm name specified with the AD Search User registration.

```
# Select the authentication server type.
# Enter "internal", "ldap", "radius" or "kerberos".
auth.server.type=kerberos

# External authentication group definitions.
auth.group.mapping=true

# Environment Settings for the Kerberos Server:
# This is the default realm name.
auth.kerberos.default_realm=hitachi.hds

# The value below is the DNS reference specification for the Kerberos
authentication server address.
auth.kerberos.dns_lookup_kdc=true
```

```
# The value below is the maximum allowed time difference with the Kerberos
authentication server.
auth.kerberos.clockskew=300

# The value below is the connection timeout period (in seconds).
auth.kerberos.timeout=3

# Specify the realm identification name.
#auth.kerberos.realm_name=RealmName

# The value below is the realm name of the connection destination.
#auth.kerberos.RealmName.realm=EXAMPLE.COM

# The value below is the KDC of the connection destination.
#auth.kerberos.RealmName.kdc=kerberos.example.com:88

# Authorization server environment settings for RADIUS and Kerberos servers:
# Authorization server connection protocol.
auth.group.hitachi.hds.protocol=ldap

# Port number for connecting to the authorization server (default: 389).
auth.group.hitachi.hds.port=389

# Distinguished name to use as the base point for searches.
auth.group.hitachi.hds.basedn=ou=hscs,dc=hitachi,dc=hds

# The connection timeout period (in seconds).
auth.group.hitachi.hds.timeout=15

# The connection retry interval (in seconds).
auth.group.hitachi.hds.retry.interval=1
```

```
# The connection retry times.
auth.group.hitachi.hds.retry.times=20
```

Configuration Information when Using TLS for LDAP with Kerberos Authentication

1. Refer to the Configuring LDAP with Transport Layer Security (TLS) to protect Authentication and Authorization section to verify and load trusted certificates into Device Manager. When you are done, add or edit the following text in the exauth.properties file.

```
# Authorization server environment settings for RADIUS and Kerberos servers:
# Authorization server connection protocol.
auth.group.hitachi.hds.protocol=tls
```

2. Save the exauth.properties file.

Example of exauth.properties file when using RADIUS Authentication (multiple servers) with LDAP Authorization using DNS

Device Manager can also use RADIUS Authentication, for interfacing with multi-factor authentications. RADIUS can also be supported in Active Directory environments known as Internet Authentication Services (Pre-Windows 2008), or Network Policy Servers (Windows 2008). In RADIUS authentication environments, Device Manager is treated as a Network Access Server. Consult your RADIUS server documentation as appropriate.

Set RADIUS Shared Secret

1) Open a command prompt and register the Shared Secret for every RADIUS Server. When specifying multiple RADIUS servers, register each one with a unique name as follows:

```
C:\Program Files\HiCommand\Base\bin>hcmdsradiussecret /set radiussecret
/name hd
sdc1
KAPM05280-I Registration of a secret has succeeded.
```

```
C:\Program Files\HiCommand\Base\bin>hcmdsradiussecret /set radiussecret
/name hd
sdc2
KAPM05280-I Registration of a secret has succeeded.

C:\Program Files\HiCommand\Base\bin>hcmdsradiussecret /list
[ServerName]
hdsdc1
hdsdc2
```

2) Note the RADIUS server names from the SharedSecret Registration process in step 1. These names are required when configuring the exauth.properties file.

3) Ensure that you configure the Device Manager server as a Network Access Server on the RADIUS servers using the same shared secret specified in Step 1.

Setting LDAP Search User for Authorization

1) Open a command prompt and register the AD Search User as follows (name is the DNS name of the Active Directory domain):

```
C:\Program Files\HiCommand\Base\bin>hcmdsldapuser /set /dn
"cn=administrator,cn=users,dc=hitachi,dc=hds" /pass St@rt_123 /name
hitachi.hds
KAPM05250-I Registration of the information-search user has finished.
```

2) Note the DNS Name from the user registration in step 1. This name is required when configuring the exauth.properties file in the next step.

3) Open the exauth.properties file and only use the following entries. Then, save the file. Note the use of the RADIUS server aliases and Active Directory DNS names defined in previous steps:

```
# Select the authentication server type.
# Enter "internal", "ldap", "radius" or "kerberos".
auth.server.type=radius

# For Directory Server or RADIUS Server.
# Specify the authentication server identification name.
auth.server.name=hdsdc1,hdsdc2

# External authentication group definitions.
auth.group.mapping=true

# Environment Settings for the RADIUS Server:
# The authentication protocol for the RADIUS server.
auth.radius.hdsdc1.protocol=PAP
auth.radius.hdsdc2.protocol=PAP

# The connected server name.
auth.radius.hdsdc1.host=hdsdc1.hitachi.hds
auth.radius.hdsdc2.host=hdsdc2.hitachi.hds

# The number of the port used for the server connection. (default: 1812)
auth.radius.hdsdc1.port=1812
auth.radius.hdsdc2.port=1812

# The connection timeout period (in seconds).
auth.radius.hdsdc1.timeout=1
auth.radius.hdsdc2.timeout=1

# The connection retry times.
auth.radius.hdsdc1.retry.times=3
auth.radius.hdsdc2.retry.times=3
```

```
# The client IPv4 address.
#auth.radius.hdsdc1.attr.NAS-IP-Address=192.168.1.210
#auth.radius.hdsdc2.attr.NAS-IP-Address=192.168.1.210

# The client IPv6 address.
#auth.radius.ServerName.attr.NAS-IPv6-Address=

# The client identifier.
auth.radius.hdsdc1.attr.NAS-Identifier=hscs.hitachi.hds
auth.radius.hdsdc2.attr.NAS-Identifier=hscs.hitachi.hds

# Authorization server domain.
auth.radius.hdsdc1.domain.name=hitachi.hds
auth.radius.hdsdc2.domain.name=hitachi.hds

# DNS server reference specification of the authorization server address when
linked to an external authentication group.
auth.radius.hdsdc1.dns_lookup=true
auth.radius.hdsdc2.dns_lookup=true

# Authorization server environment settings for RADIUS and Kerberos servers:
# Authorization server connection protocol.
auth.group.hitachi.hds.protocol=ldap

# Authorization server host name for RADIUS servers.
#auth.group.EXAMPLE.COM.host=ldap.example.com

# Port number for connecting to the authorization server (default: 389).
auth.group.hitachi.hds.port=389

# Distinguished name to use as the base point for searches.
```

```
auth.group.hitachi.hds.basedn=ou=hscs,dc=hitachi,dc=hds

# The connection timeout period (in seconds).
auth.group.hitachi.hds.timeout=15

# The connection retry interval (in seconds).
auth.group.hitachi.hds.retry.interval=1

# The connection retry times.
auth.group.hitachi.hds.retry.times=20
```

Configuration Information when Using TLS for LDAP with RADIUS Authentication

1. Refer to the Configuring LDAP with Transport Layer Security (TLS) to protect Authentication and Authorization section to verify and load trusted certificates into Device Manager. When you are done, add or edit the following text in the exauth.properties file.

```
# Authorization server environment settings for RADIUS and Kerberos servers:
# Authorization server connection protocol.
auth.group.hitachi.hds.protocol=tls
```

2. Save the exauth.properties file.

NOTES:

- When you create a group, you can change the permission. However, you cannot change the DN once the group is created. To change the DN, remove the group and then add it again.
- When using external authentication and authorization, local storage administrator accounts are not required.
- If an externally authenticated storage management user is a member of multiple groups in Device Manager, the user permissions are the sum of all group memberships.
- As security best practices, organizations enforce password rotation policies. When creating the LDAP Search User (especially in Active Directory environments), HDvM does not automatically warn you that the password is about to expire. As part of the LDAP Search User creation, an HDvM administrator must update the password as per organizational policy, or obtain an account with a password that does not expire. When changing the authentication process of externally authenticated users on existing HDvM installations, group mappings and their permissions must be removed and reconfigured.

Copyrights and Licenses

Hitachi Data Systems reserves the right to make changes to this document at any time without notice and assumes no responsibility for its use. Hitachi Data Systems products and services can only be ordered under the terms and conditions of Hitachi Data Systems' applicable agreements. All of the features described in this document may not be currently available. Refer to the most recent product announcement or contact your local Hitachi Data Systems sales office for information on feature and product availability.

This document contains the most current information available at the time of publication. When new and/or revised information becomes available, this entire document will be updated and distributed to all registered users.

Hitachi Data Systems is a registered trademark and service mark of Hitachi, Ltd., and the Hitachi Data Systems design mark is a trademark and service mark of Hitachi, Ltd. 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.

AIX is a registered trademark of the International Business Machines Corp. in the U.S.

All Borland brand names and product names are trademarks or registered trademarks of Borland Software Corporation in the United States and other countries.

Brocade is a trademark or a registered trademark of Brocade Communications Systems, Inc. in the United States and/or in other countries.

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

ESCON is a registered trademark of the International Business Machines Corp. in the U.S.

HP is a trademark of the Hewlett-Packard Company.

HP Tru64 UNIX is a trademark of Hewlett-Packard Company.

HP-UX is a product name of Hewlett-Packard Company.

HP StorageWorks is a trademark of Hewlett-Packard Company.

IBM is a registered trademark of the International Business Machines Corp. in the U.S.

OS/390 is a registered trademark of the International Business Machines Corp. in the U.S.

z/OS is a registered trademark of the International Business Machines Corp. in the U.S.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries.

Linux is a registered trademark or trademark of Linus Torvalds in the U.S. and other countries.

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

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

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

Mozilla is a trademark of the Mozilla Foundation in the U.S and other countries.

NetWare is a registered trademark of Novell, Inc.

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

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

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

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

Hitachi Device Manager Software includes RSA BSAFE Cryptographic software from RSA Security Inc.

RSA is a registered trademark of RSA Security Inc.

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

All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc., in the United States and other countries. Products bearing SPARC trademarks are based upon an architecture developed by Sun Microsystems, Inc.

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

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

Sun StorEdge is a trademark or registered trademark 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 in the United States and other countries, licensed exclusively through X/Open Company Limited.

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

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

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

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

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

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

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

This product includes software developed by Borland Software Corp.

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

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

EMC and CLARiiON are registered trademarks of EMC Corporation.

Hitachi Device Manager Software includes some parts whose copyrights are reserved by Sun Microsystems, Inc.

Hitachi Device Manager Software includes some parts whose copyrights are reserved by UNIX System Laboratories, Inc.

SUSE is a registered trademark of Novell, Inc. in the United States and other countries.

Kerberos is a name of network authentication protocol created by Massachusetts Institute of Technology.

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