Hitachi Device Manager 8.4.1-02 Release Notes

Contents

RN-00HS266-102 (July 2016)

About this document

This document (RN-00HS266-102, July 2016) provides late-breaking information about Hitachi Device Manager v8.4.1-02. 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 Hitachi Device Manager.

Getting help

Hitachi Data Systems Support Connect is the destination for technical support of products and solutions sold by Hitachi Data Systems. To contact technical support, log on to Hitachi Data Systems Support Connect for contact information: https://support.hds.com/en_us/contact-us.html.

Hitachi Data Systems Community is a global online community for HDS customers, partners, independent software vendors, employees, and prospects. It is the destination to get answers, discover insights, and make connections**.** **Join the conversation today!** Go to community.hds.com, register, and complete your profile.

About this release

This release resolves multiple known problems.

Product package contents

Item	Contents	Revision	Release type
Software	Device Manager Server	8.4.1-02	Full Package
Documents	Hitachi Command Suite User Guide	MK-90HC172-24	
	Hitachi Command Suite CLI Reference Guide	MK-90HC176-24	
	Hitachi Command Suite Tiered Storage Manager CLI Reference Guide	MK-90HC177-21	
	Hitachi Command Suite Messages	MK-90HC178-24	
	Hitachi Command Suite Audit Log Reference Guide	MK-92HC213-10	

Item	Contents	Revision	Release type
	Hitachi Command Suite Installation and Configuration Guide	MK-90HC173-24	
	Hitachi Command Suite Administrator Guide	MK-90HC175-24	
	Hitachi Command Suite Configuration Manager REST API Reference Guide	MK-92HC229-00	
	Hitachi Command Suite Virtual Appliance Installation Guide	MK-92HC236-00	

New features and important enhancements

For 8.4.1-02

Features and enhancements	Affected components	Affected operating systems
Device Manager agent now supports the following operating systems: - Red Hat Enterprise Linux 6.8 - Oracle Linux 6.8 (x86) UEK R2 - Oracle Linux 6.8 (x64) UEK R4	Device Manager Agent	All*
Host Data Collector now supports a host that runs the following operating systems as a target host: - Red Hat Enterprise Linux 6.8 - Oracle Linux 6.8 (x86) UEK R2 - Oracle Linux 6.8 (x64) UEK R4	Host Data Collector	All*

For 8.4.1-00

Features and enhancements	Affected components	Affected operating systems
Device Manager can now configure environments in which Hitachi Virtual Storage Platform G800 (VSP G800) and Hitachi Virtual Storage Platform G1000 (VSP G1000) are mixed in a highly available system (3DC delta resync) using the following copy pairs in VSP G800 and VSP G1000. Copy pairs: - global-active device - Universal Replicator - Delta resync of Universal Replicator	Device Manager Server Device Manager CLI	All*

Features and enhancements	Affected components	Affected operating systems
Device Manager now supports the viewing and setting of the ALUA Application States and Asymmetric Access States (ALUA path priority) that are used for global-active devices in cross path configurations on VSP Gx00 models.	Device Manager Server Device Manager GUI Device Manager CLI	All*
For the VSP G1000 and Hitachi Virtual Storage Platform G200, G400, G600, G800 (VSP Gx00 models) storage systems, Device Manager now supports renaming of tiering policies and changing the allocation threshold value of a tiering policy in units of 1%.	Device Manager Server Device Manager GUI Device Manager CLI	All*
Device Manager now supports functions for viewing and setting up the following configurations in VSP G1000: - Connections to external storage systems that use iSCSI ports as external paths - Copy pairs that use iSCSI ports as remote paths	Device Manager Server Device Manager GUI Device Manager CLI	All*
The Device Manager GUI now supports Adobe Flash Player 21.	Device Manager GUI	Windows
The Device Manager GUI now supports Firefox ESR 45 for Linux.	Device Manager GUI	Linux
Device Manager now supports Hitachi NAS Platform 12.6.	Device Manager Server Device Manager GUI	All*
The Device Manager GUI supports Google Chrome for Microsoft Windows 10 and Windows 8.1.	Device Manager GUI	Windows
Device Manager now supports VSP G400, G600, G800, and Virtual Storage Platform F400, F600, F800 (VSP Fx00 models) with NAS modules.	Device Manager Server Device Manager GUI Device Manager CLI	All*
Hitachi Command Suite v8.4.1-00 now supports the Hitachi Command Suite REST API.	REST API	All*
Device Manager now supports propagating IOPH information by specifying a consistency group number or journal group ID for the following types of copy pairs: - TrueCopy (*) - TrueCopy for Mainframe (*) - Universal Replicator - Universal Replicator for Mainframe *: A journal group ID cannot be specified.	Device Manager Server Device Manager CLI	All*

Features and enhancements	Affected components	Affected operating systems
Device Manager can now manage VSP Fx00 model storage systems that are connected to DBF2 trays.	Device Manager Server Device Manager GUI Device Manager CLI	All*
HCS for VVols has been improved: When creating an SLU, only LDEV IDs that have not been assigned with a virtual LDEV ID will be properly selected.	Device Manager Server	All*
Device Manager now supports functions to configure global-active device by using the iSCSI port for VSP G1000.	Device Manager Server Device Manager GUI Device Manager CLI	All*
The Device Manager GUI now supports output to the audit log when a task status is changed and methods are requested to the storage systems in the task.	Device Manager GUI	All*
The Device Manager server, GUI, and CLI now support Oracle Linux 7.2.	Device Manager Server Device Manager GUI Device Manager CLI	Linux
Device Manager now supports the SVP running on the Kernel-based Virtual Machine (KVM).	Device Manager Server Device Manager GUI Device Manager CLI	All*
Device Manager now supports 1.9TB SSD on the VSP G200 storage system.	Device Manager Server Device Manager GUI Device Manager CLI	All*

Note: See *Hitachi Command Suite System Requirements* for details.

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

System requirements

System requirements can be found in *Hitachi Command Suite System Requirements* (MK-92HC209-22).The requirements are presented in the form of requirements for each type of server, rather than as requirements for individual Hitachi Command Suite components.

When upgrading Hitachi Command Suite products from v7.6.1 or earlier, if the following components are installed, upgrade them to v8.0.0 or later:

- Device Manager
- Tiered Storage Manager
- Replication Manager
- Tuning Manager
- Compute Systems Manager
- Global Link Manager

Resolved problems

From 8.4.1-00 to 8.4.1-02

Problem description	Affected products	Affected operating systems
Automatic refresh fails for the VSP Gx00 and VSP Fx00 storage systems, and the error log that contains Error Code=7278 is output to the HDvM error log. Because of the failure, the KAIC15056-W warning message appears in the GUI, and its display might persist.	Device Manager Server	All*
The Refresh Storage Systems might fail with the KAIC08823-E message. Performance information might take a long time to appear, or it might not appear at all because the database for the Replication tab is fragmented, and cannot be resolved automatically.	Device Manager Server	All*
A behavior that can be mistakenly identified as security problem has been corrected.	Device Manager GUI	All*
When attempting to log on to Tuning Manager and Replication Manager using a password that contains any of the following special characters, the logon fails with KATN12203-E and KAVN00226-E errors. - % - + - &	Device Manager GUI	All*
In the Allocate Like Volumes dialog box that is started by selecting a volume of VSP Gx00 models, VSP Fx00 models or a VSP G1000 storage system, the KAIC15007-W message appears and the like-volumes cannot be allocated.	Device Manager GUI	All*

Problem description	Affected products	Affected operating systems
HCS user authentication information might be unintentionally exposed when Replication Manager or Tuning Manager is installed on the same server machine as Device Manager, and if users fail to log on to Replication Manager or Tuning Manager.	Device Manager GUI	All*
[REST API] In the URL of affectedResources for the job object that is returned after the execution of the API function for creating a resource group, the name of the created resource group is displayed, instead of the resource group ID.	REST API	All*
[REST API] REST API operations can fail with the KART30090-E error if they are performed within 3 minutes of obtaining a list of resource groups or information about a specific resource group from a VSP G1000 storage system.	REST API	All*

From 8.4.0-02 to 8.4.1-00

Problem description	Affected products	Affected operating systems
Malicious third parties can get session information illegally.	Device Manager GUI	All*
In the Create Copy Topology or Add Copy Pairs wizard, any unusable CTG IDs that are already used by a Universal Replicator copy pair that is not managed by Replication Manager incorrectly appears as candidates in the list for creating a copy pair.	Device Manager GUI	All*
In the Create Copy Topology or Change Topology wizards, the same MU number can be specified in multiple remote copy groups, when it should only be specified in one copy group.	Device Manager GUI	All*
In the Create Copy Topology or Change Copy Topology wizard, the same CTG ID can be specified for multiple copy groups, or remote copy groups and local copy groups related to the remote copy groups, when the CTG ID should only be specified in one copy group.	Device Manager GUI	All*
In the setting dialog boxes that can be started from the wizard for copy topology operations, it is not possible to use the tab key to focus on an option.	Device Manager GUI	All*
When creating a copy pair and a host group at the same time, if Optimized is selected for the Asymmetric Access Status, it appears as Non-Optimized, regardless of the actual configuration.	Device Manager GUI	All*

Problem description	Affected products	Affected operating systems
When creating a copy topology or adding a copy pair in the Replication tab, if Non-Optimized is specified for the Asymmetric Access Status, Optimized is configured instead.	Device Manager GUI	All*
When creating an iSCSI target by using the Create Copy Topology or the Add Copy Pairs wizard in the Replication tab, the task fails with the KAIC08710-E error if Optimized is specified for the Asymmetric Access Status.	Device Manager GUI	All*
Even if you refresh a storage system managed by remote Device Manager where Thin Image (snapshot group) related to the hosts or virtual storage machines exists, the copy topology, copy groups, and copy pairs information is not updated in the Replication tab.	Device Manager GUI	All*
In the Replication tab, only one host appears from among all hosts that are connected to the volumes that compose a copy topology.	Device Manager GUI	All*
For a copy topology that includes GAD pairs with a CTG ID, a task that deletes some copy pairs can be registered (although it should not be registered) if the **continue I/O using the secondary volumes** check box is selected. The task fails with the RPM-03328 error.	Device Manager GUI	All*
In the Set up global-active device dialog box that starts from the Set up Replication/GAD dialog box, a user-defined virtual storage machine on primary side cannot be configured in Edit Virtual Storage Machine if storage systems managed by local Device Manager are selected for the primary and secondary storage systems in the Select Storage Systems and Copy Type window.	Device Manager GUI	All*
If a TI copy group in a copy topology contains copy pairs in a Simplex status, then a task that involves the copy topology either fails with the KAIC70022-E (RPM-00821) error or an improper value appears in the TI pools column in the Replication tab.	Device Manager GUI	All*
Device Manager cannot manage a volume that is allocated to a virtually connected port on a user-defined virtual storage machine if the port is incompatible with the physical port.	Device Manager Server	All*
When creating a journal group twice in a row in the Replication tab, the KAVN00209-E error occurs and the journal group cannot be created.	Device Manager GUI	All*
Fence level data for TrueCopy Sync pairs might not appear if the fence level is Data or Status.	Device Manager Server	All*
If the Health Check is performed in the Analytics tab, an improper health check report is generated. A failure also occurs when exporting the report to a PDF file and sending a notification email with the report as a file attachment.	Device Manager GUI	All*
The KAIC16993-E error appears in the Analytics tab instead of the health check report.	Device Manager GUI	All*

Problem description	Affected products	Affected operating systems
A Pool instance does not appear in the result of the CLI GetStorageArray (subtarget=Pool) command if the pool is master journal group (M-JNL) and restore journal group (R-JNL) for Universal Replicator.	Device Manager Server	All*
When creating a GAD copy pair, a volume that has a different attribute from the primary volume cannot be selected as a secondary volume for the GAD copy pair.	Device Manager GUI	All*
The volumes on a user-defined virtual storage machine cannot be selected to be a volume for a copy pair with certain copy types.	Device Manager GUI	All*
If a copy group for mainframe that is managed by CCI contains a copy pair with the simplex status, then refreshing the configuration and changing the pair status fails with the RPM-00590 or KAVN0060-E error.	Device Manager GUI	All*

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

Known problems

- When SSL communication is enabled between REST API server and VSP G1000

  If the SSL communication is enabled between the REST API server and VSP G1000 storage system, the following operations related to volumes and pools can fail with the KART40098-E error.

  - Creating a volume
  - Deleting a volume
  - Formatting a volume
  - Creating a pool
  - Deleting a pool
  - Expanding a pool
  - Shrinking a pool

  However, there is a possibility that these operations are successful. To confirm, obtain the target resource information.

- Error message ID "KART400098-E" displayed in REST API

  To resolve this error, verify the following and then retry the API operation:

  - The status of REST API server which that is running on the remote storage system.
  - The network configuration of storage system registered by the remote REST API server.
  - The network status between storage systems registered by the local and remote REST API servers.
  - The status of both storage systems registered by the local and remote REST API servers.

- Maximum limit of storage system resources that can be configured by REST API when SSL communication is enabled

  For VSP G1000, when SSL communication between REST API server and storage system is enabled, the number of storage resources is limited.

- External volume

  The number of available external volumes that can be mapped to external volume groups is limited to 2048 (standard limit is 63232).

- Copy Group/snapshot group

  The number of available groups is limited to 100 (standard limit is 2048).

- Copy pair

  The number of available copy pairs in a groups replication group is limited to 256 (standard limit is 8192).

When the number of resources exceeds any of the above limit, the resource information cannot be retrieved from the REST API. To avoid the issue, use In-Band method.

- Registration of VSP G1000 storage system by multiple REST API servers disabled when SSL communication is enabled between REST API server and storage system

  When VSP G1000 is registered and the SSL communication between the REST API server and storage system is enabled, the storage system cannot be registered by other REST API servers.

- When changing SSL communication settings between REST API server and VSP G1000

  If you change the SSL communication settings between REST API server and VSP G1000 storage system, the REST API server must be restarted.

  If the information of a remote storage system is registered in the REST API server, delete this information and register it again.

- Resource group lock not supported when SSL communication is enabled between VSP G1000 and REST API server

  Configuration changes may fail without using the resource group lock. Use the information below to review the cause and the suggested solution:

  [Cause]:A resource group of the storage system is locked by other users, or by another storage management software. Error message with error code SSB1=2E11, SSB2=2205 is displayed.

  [Solution]:Retry the operation later.

  [Cause]:Configuration change is requested to the storage system at the same time from other users, or other storage management software.

  [Solution]:Confirm the current configuration and retry the operation.

- Error messages displayed when storage systems are modified by using the particular REST API

  For a VSP G1000 storage system for which SSL communication is enabled, if an error occurs in the processing to modify the storage system by using the Hitachi Command Suite 8.4.1-02 REST API, "null" appears in the error message.

  This problem occurs when one of the following operations fails:

- Creating a host group with the host mode specified
- Creating a host group with the host mode option specified
- Creating a pool for Hitachi Dynamic Tiering
- Modifying pool information
- Modifying volume information

- Error messages displayed when storage systems are modified by using the REST API

  For a VSP G1000 storage system for which SSL communication is enabled, if an error occurs in the processing to modify the storage system by using the Hitachi Command Suite 8.4.1-02 REST API, the error information is displayed as shown in the example below.

  The "message", "cause", and "solution" attributes are displayed as part of the message content, instead of as JSON attributes.

  Display example:

  ```
  "error" : {
    "errorSource" : "URL-of-the-API-function-for-which-the-error-occurred",
    "message" : "An error occurred by the storage system. (
  details: message ID = <message-ID>,
  message = <error-message>,
  cause = <cause-of-the-error>,
  solution = <solution-for-the-error>,
  storage device ID = <storage-device-ID>)",
    "solution" : <solution-for-the-error>,
    "messageId" : <message-ID>
  }
  ```

- Btrfs file system in Oracle Linux

  Do not install Device Manager on a Btrfs file system because it is not supported.

- Details about information related to MUs (mirror units) when information about a specific journal is collected by using the REST API of Hitachi Command Suite 8.4.1-00

  When one journal ID is specified to collect information about a journal used in a 3DC configuration, if multiple MUs are specified for the journal, information about only one MU is displayed.

  To see information about all of the MUs, set basic, timer, or detail for the query parameter for collecting journal information (journalInfo). After the list containing journal information appears, check the list for the information about the corresponding journal ID.

- Attributes specified when information about a remote storage system is registered by using the REST API

  When registering information about a remote storage system by using the REST API of Hitachi Command Suite 8.4.1-00, for restServerIp, specify an IPv4 address, an IPv6 address, or a host name corresponding to an IPv4 address.

  If a host name corresponding to an IPv6 address is specified for restServerIp, the processing fails.

- Using the REST API to get job information and session information

  For VSP G1000, VSP Gx00, and VSP Fx00 storage systems, a failure results when getting job information or session information by using the REST API if all of the following conditions are met:

  1. A storage system is registered with the REST API server.
  2. Changed the user password or deleted the user account on the storage system described in (1) by using different management tool, such as Storage Navigator.
  3. The REST API server was restarted after (2).

  The following symptoms occur.

  Symptom 1:

  The API function to get job information for the storage system described in condition (1) fails with the applicable error described below.

  Symptom 2:

  The API function to get a list of sessions for the storage system described in condition (1) fails with the applicable error described below.

  Errors:

  - VSP G1000

    KART30085-E User authentication failed.

  - VSP Gx00 models and VSP Fx00 models

    KART30002-E All or part of the processing cannot be performed by the storage system.

  To recover from this problem, use the REST API to reconfigure correct user information as described in procedure (2) for the storage system described in procedure (1).

- About the KART00000-E error when getting storage system information or changing the storage system configuration using the REST API

  When getting storage system information or changing the storage system configuration by using the REST API, the operation might fail with the KART00000-E error.

  In most cases, a communication problem that exists between the REST API server and the storage system might be the cause of the error.

Check the communication path between the REST API server and the storage system, including ports and encryption related settings, and then reconfigure the settings if needed.

- Deleting a storage container for file storage VVols

  When deleting a storage container for file storage VVols, make sure that no virtual machine (VM) is in operation on a data store that is associated with the storage container.

  If you delete a storage container with a VM in operation, the deletion fails with the following error messages.

  Message column in Task Information:

  KAIC18770-E

  Message column in Storage Containers:

  KAIC18768-E

  mouse-over details:

  KAIC05273-E

  In this case, confirm the storage container's operational status with the VM administrator, remove VMs that operate on the datastore, and then delete the storage container again.

- Authorization information for the REST API

  To specify authorization information for VSP G1000 that enables SSL communication, use the following format in the Remote-Authorization header:

  Basic *authentication-information*

  If you specify the token of the session as authorization information, the authentication fails.

- When users for VSP G1000 are managed only by an external authentication server

  For VSP G1000, when users are managed only by an external authentication server, the Hitachi Command Suite REST API cannot be used.

- Using the Hitachi Command Suite REST API for storage systems with an earlier microcode version

  If the Hitachi Command Suite REST API is used for storage systems with an earlier microcode version, the following problems occur:

  - The KART30074-E message appears when changing a pool name.
  - The **poolId** parameter is ignored when specifying both **ldevOption** and **poolId** to the query parameter to obtain volume information.

  To resolve the problems, upgrade the microcode to one of the following versions:

  - VSP Gxx 83-01-21-20/00 or later
  - VSP G1000 80-04-00-00/04 or later
  - HUS VM 73-03-44-00/00 or later
  - VSP 70-06-34-00/00 or later

- Obtaining volume information by using the Hitachi Command Suite REST API

  The REST API server does not respond to the request if a query parameter **resourceGroupId** is specified to obtain volume information from a VSP or HUS VM storage system.

  Do not specify **resourceGroupId** in the query parameter.

- Starting NAS Manager or SMU

  NAS Manager or SMU fails to start when all of the following conditions are met:

  - The version of NAS Manager or SMU is 12.0 or later.
  - IPv6 is enabled for NAS Manager or SMU.
  - HCS is using an IPv6 IP address to be registered with NAS Manager or SMU.

  If the above conditions are met, start NAS Manager or SMU directly.

- The connection of command devices for the Device Manager agent

  When command devices are being connected to the pair management server, command devices that belong to virtual storage machines and those that do not belong to virtual storage machines cannot be connected at the same time.

- Using the Replication tab to create multiple copy groups for remote copy at the same time

  In the Create Copy Topology wizard of the Replication tab, when you try to create multiple copy groups for remote copy, if any of the copy groups to be created share the same primary or secondary storage system and also have the same CTG ID, the operation fails with the KAIC05956-E error.

  Verify that the specified copy groups that share the same primary or secondary storage systems have different CTG IDs.

- Using a system account to log in to Device Manager, and then operating VSP Gx00 models.

  If you use a system account to log in to Device Manager, the functions that you can perform from the maintenance utility might be unintentionally restricted.

  To use the functions, log in to Device Manager as a user who belongs to a user group that has the Admin role.

- Limit on the VASA Provider (file storage) that HCS for VVols can manage

  In the file storage VVols environment managed by VASA Provider (file storage), both of the following conditions must be met:

  - The maximum number of file systems is 10 or fewer.
  - The maximum number of storage containers is 5 or fewer.

Installation precautions

Upgrading an installation

Before upgrading from the following version, complete the procedure described.

Version:

Hitachi Device Manager v8.0.0-00 to earlier than v8.4.0-00

Procedure:

For Windows:

1. If Device Manager is remotely linked with Tuning Manager, shut down the Tuning Manager server.
2. Log in to Windows as the administrator.
3. When installing Hitachi Command Suite in a cluster environment, take Hitachi Command Suite services offline. Then suppress failover of the resource group according to the following sections in the *Hitachi Command Suite Installation and Configuration Guide* depending on the version from which you are upgrading.

   For v8.0.0-00 to earlier than v8.2.0-00:

   - Suppressing failover when upgrading or overwriting Hitachi Command Suite (Windows)

   For v8.2.0-00 or later:

   - Taking Hitachi Command Suite services offline (Windows)
4. Run the Command Prompt as the administrator and then execute the following commands in the order listed.
   a. cd /d <Hitachi-Command-Suite-installation-folder>\Base64\bin
   b. hcmds64srv /stop
   c. hcmds64srv /statusall
   d. hcmds64dbsrv /start
   e. cd <Hitachi-Command-Suite-installation-folder>\Base64\sbin
   f. hcmdsdbreclaim -k index -a -c dic
   g. hcmdsdbreclaim -k index -j -c dic
   h. hcmdsdbreclaim -k table -a -c dic
   i. hcmdsdbreclaim -k table -j -c dic

For Linux:

1. If Device Manager is remotely linked with Tuning Manager, shut down the Tuning Manager server.
2. Log in as root.
3. When installing Hitachi Command Suite in a cluster environment, delete the HCS product services from the Red Hat High Availability service group according to the section "Deleting HCS product services from the service group (Red Hat Enterprise Linux)" in the *Hitachi Command Suite Installation and Configuration Guide*.
4. Start the terminal window and then execute the following commands in the order listed.
   a. cd <Hitachi-Command-Suite-installation-directory>/Base64/bin

b. ./hcmds64srv -stop
c. ./hcmds64srv -statusall
d. ./hcmds64dbsrv -start
e. cd <Hitachi-Command-Suite-installation-directory>/Base64/sbin
f. ./hcmdsdbreclaim -k index -a -c dic
g. ./hcmdsdbreclaim -k index -j -c dic
h. ./hcmdsdbreclaim -k table -a -c dic
i. ./hcmdsdbreclaim -k table -j -c dic

Upgrading the environment where a global-active device (GAD) pair is configured

If all of the following conditions are met, complete the following procedure after the upgrade installation.

1. You upgraded from one of the following versions.
   Hitachi Device Manager v8.0.1-00 to earlier than v8.4.0-00.
2. A GAD pair is configured in the storage system managed by Device Manager.
3. A pair management server that manages the GAD pair described in (2) is registered with Device Manager.
4. The pair management server described in (3) recognizes the volume that composes the GAD pair described in (2).

Procedure:

1. Stop the Hitachi Command Suite product.
2. Open the server.properties file in a text editor.
3. Configure server.agent.differentialrefresh.manual.enabled to false as described.

```
------------------------------------------------------------
server.agent.differentialrefresh.manual.enabled=false
------------------------------------------------------------
```

4. Save the change and close the editor.
5. Start the Hitachi Command Suite product.
6. Log in to the Device Manager GUI.
7. Refresh all of the storage systems registered with Device Manager one at a time.
8. After (7) is done, stop the Hitachi Command Suite product.
9. Open the server.properties file in a text editor.
10. Configure server.agent.differentialrefresh.manual.enabled to true as described.

```
------------------------------------------------------------
server.agent.differentialrefresh.manual.enabled=true
------------------------------------------------------------
```

11. Save the change and close the text editor.
12. Start the Hitachi Command Suite product.

When you install Hitachi Command Suite, some components require that you take some precautions. The following table lists the components and the location of the precaution information:

Component	Reference
Device Manager Server	See "Installing" in the *Hitachi Command Suite Installation and Configuration Guide*.
GUI	See the online help.
CLI	See "Requirements for CLI Operations" in the *Hitachi Command Suite CLI Reference Guide.*
Device Manager Agent	See Installing the Device Manager Agent in Windows and Installing the Device Manager Agent in Linux in the *Hitachi Command Suite Installation and Configuration Guide*.

Usage precautions

Updates to the request lines specified when using the search function of the Hitachi Command Suite REST API

When using the search function of the Hitachi Command Suite REST API, the request lines in the REST API Reference Guide need to be replaced as follows.

1. When searching for information related to the WWNs registered in host groups
   Replace the following request line:
   - GET <base-URL>/v1/views/host-groups-host-wwns

   with this:
   - GET <base-URL>/v1/views/host-groups-host-wwns-wwns
2. When searching for information related to the iSCSI names registered as iSCSI targets
   Replace the following request line:
   - GET <base-URL>/v1/views/host-groups-host-iscsis

   with this:
   - GET <base-URL>/v1/views/host-groups-host-iscsis-iscsis
3. When searching for the LU path information corresponding to the WWN of a host
   Replace the following request line:
   - GET <base-URL>/v1/views/host-groups-host-wwns-ldevs-luns-ports

   with this:
   - GET <base-URL>/v1/views/host-groups-host-wwns-ldevs-luns-ports-wwns

If you specify any of the above incorrect request lines from the REST API Reference Guide, you will obtain an error and the following message is displayed:

KART20009-E No resource exists at the specified URL.

REST API commands that can be run only by root users and the reason for such restrictions

For the reasons described below, only the root user can run the following REST API commands:

1. The following commands require files to be created or deleted in certain OS directories (such as the "/etc" directory) for which only root users have the necessary write permissions:
   <*Mount directory of installation media*>/ConfManager/install.sh
   <*REST API installation directory*>/ConfManager/inst/uninstall.sh

2. The following commands run shell scripts that can only be run by root users in the REST API installation directory:
   <*REST API installation directory*>/ConfManager/SupportTools/CollectTool/RestTI.sh
   <*REST API installation directory*>/ConfManager/bin/changejdk.sh
   <*REST API installation directory*>/ConfManager/bin/changeRMPort.sh
   <*REST API installation directory*>/ConfManager/bin/configureCluster.sh
   <*REST API installation directory*>/ConfManager/bin/setCertificateFile.sh
   <*REST API installation directory*>/ConfManager/bin/setCipherSuite.sh
   <*REST API installation directory*>/ConfManager/bin/deltask.sh
   <*REST API installation directory*>/ConfManager/start.sh
   <*REST API installation directory*>/ConfManager/status.sh
   <*REST API installation directory*>/ConfManager/stop.sh

Note: Command descriptions:

RestTI.sh – Collect REST API logs

changejdk.sh –Switch to a customer provided JDK

changeRMPort.sh – Change the range of port numbers to be used by CCI

configureCluster.sh – Configure REST API service to know it is in a cluster with HCS

setCertificateFile.sh – Register certificate file for SSL communication

setCipherSuite.sh – Configure cipher suite for SSL communication

deltask.sh – Unregister the REST API service information in operating system

start.sh – Start REST API service

status.sh – Get the status of REST

service stop.sh – Stop REST API service

Creating a Copy Topology and adding Copy Pairs using a storage system where a LUSE volume exists

When creating a copy topology or adding a copy pair in the Replication tab, make sure that any LDEV IDs of a non-representative volume that compose a LUSE volume are not selected for the following tasks:

- Create Copy Topology
- Add Copy Pairs

If any LDEV ID of a non-representative volume that compose a LUSE volume is selected by either of the following procedures, then the Create Copy Topology and Add Copy Pairs tasks fail with the KAIC05958-E(RPM-01004(KAIC07626-E)) error:

- Selecting any LDEV ID of a non-representative volume that compose a LUSE volume from the list in the Select Volumes dialog box.
- Automatically selecting any LDEV ID of a non-representative volume that compose a LUSE volume when the dialog box transitions to the Show Plan window.

In this case, an LDEV ID that appears in the device number of the KAIC07626-E message indicates the volume that composes a LUSE volume.

If the symptom occurred, complete the creation of the copy topology with the following procedure.

1. Make a note of the **Started** time and the **HRpM Workflow Name** for the failed task in the **Task Details** dialog box that can be open from the **Tasks & Alerts** tab.
2. In the Replication Manager, delete the task with the same **Execution Time** as the **Started** time that took note in (1) from the **Tasks** window. Also delete the workflow with the same **Workflow Name** as the **HRpM Workflow Name** that took note in (1) from the **Workflows** window.
3. Check the LDEV IDs of the volumes that compose a LUSE volume including the ones that was indicated in the KAIC07626-E message, and then create the copy topology or add copy pair again by using LDEV IDs other than the ones that compose a LUSE volume. If the copy topology was half created when it failed, complete the creation of the target topology by using Replication Manager.

To manage file storage VVols

Use VASA provider (file storage) version 3.3.0 or later to manage file storage VVols.

When using Hitachi Command Suite Configuration Manager REST API to specify a replication type to change the configuration of a remote copy pair

When using Hitachi Command Suite Configuration manager REST API to change the configuration of a remote copy pair, even if specifying replication types that are different from that of the remote copy pair, the change will be applied if specified parameters are valid.

Starting Element Manager for VSP

Starting Element Manager for VSP might fail with the KAIC00861-E error.

If the error occurs, check if the hash algorithm of the server certificate for the VSP in the SVP is MD5. If the hash algorithm is MD5, create the server certificate again by using SHA (SHA-256 is recommended).

Allocating a volume on a user-defined virtual storage machine

When allocating a volume on a user-defined virtual storage machine, if a pair management server is running on Solaris where Solaris multi-pathing feature (MPxIO) is enabled, use the virtual ports that match the physical ports on the actual storage system.

Otherwise, Device Manager will be unable to manage the volume. To manage the volume, use Element Manager instead.

Storage systems with NAS modules

When using the cache partition function on a storage system with NAS modules, do not use the CLPR name, NASSystemCLPR.

Note: You can confirm CLPR names in Device Manager - Storage Navigator.

Changing configuration of remote copy pairs

After creating, splitting, resyncing, or deleting a remote copy pair, if the job progress takes more than five minutes to complete, the job might appear as Failed regardless of the actual status.

Additionally, the following message appears:

KART40097-E An error occurred on the REST API server managing the remote storage system. (details: message ID = KART40047-E, message = The specified token is invalid., cause = An invalid token was specified, or the session might be disabled., solution = Revise the token info. If the problem persists, recreate the session.) See the details of the message, and remove the cause of the error on the REST API server managing the remote storage system.

In this case, check the applicable resources for the actual status.

Recording SNMP v3 trap to a log file

To record the SNMP v3 trap to a log file, specify the following value for the EnterpriseID and generic trap number in the **customizedsnmptrap.customizelist** property of the **customizedsnmptrap.properties** file.

- EnterpriseID:
  - Generic trap: ".1.3.6.1.2.1.11"
  - Specific trap: Expected EnterpriseID to be recorded in the log file.

- Generic trap number:
  Specify any of the following values accordingly to the SNMP trap content.
  - coldStart : 0
  - warmStart : 1
  - linkDown : 2
  - linkUp : 3
  - authenticationFailure : 4
  - epgNeighborLoss : 5
  - enterpriseSpecific : 6

Property file name:

customizedsnmptrap.properties

Location of the file:

- Windows:

  <Device Manager-installation-folder>\HiCommandServer\config

- Linux:

  <Device Manager-Installation-directory>/HiCommandServer/config

When an error occurs during a volume operation of a global-active device pair

If an error occurs during a volume operation of a global-active device pair, check the following items, refresh the host of the pair management server that manages the global-active device pair, and then try the operation again.

- Check that the Device Manager agent service of the pair management server is running.
- Check the state of the command device recognized by the pair management server.

Using Device Manager to manage Hitachi VSP Fx00 models

When Hitachi VSP Fx00 models (where the DKC microcode version is earlier than 83-03-01-XX/XX-XX) is registered in Device Manager, the storage system model is displayed as VSP Gx00 models.

Similarly, the storage system name is sometimes displayed as VSP Gx00 models.

Best practice is to change the storage system name so that VSP Fx00 models can be distinguished from VSP Gx00 models.

When KAIC07755-E, KAIC07762-E, KAIC07774-E, KAIC07776-E, KAIC07777-E, or KAIC07780-E occurs during copy pair operation

The following error messages might contain SSB code in the format shown.

Error messages:

- KAIC07755-E
- KAIC07762-E
- KAIC07774-E
- KAIC07776-E
- KAIC07777-E
- KAIC07780-E

SSB code: SSB=0xXXXX,0xYYYY

(Example: SSB=0xD004,0xFC7E)

The SSB code is information generated by CCI to distinguish errors.

See the CCI user guide and refer to the SSB code to resolve the error.

Installation of the Device Manager server and Hitachi File Services Manager (HFSM) on the same server and importing an HFSM databases

If you import an HFSM database by executing the hcmdsdbtrans command on a server where the Device Manager server and HFSM are both installed, the command fails with the KAPM05915-E message.

If this problem occurs, perform the following recovery procedure:

Step 1: Set the management server of the HFSM user account to a primary server.

<HFSM-installation-path>\Base\bin\hcmdsprmset /host 127.0.0.1 /port non-SSL-port-number

Step 2: Execute the following command to import the HFSM database.

<HFSM-installation-path>\Base\bin\hcmdsdbtrans /import

/type FileServicesManager /workpath XXX /file YYY /auto

XXX: Working directory (must be empty).

YYY: Archive file of the HFSM database.

Step 3: Set the management server of the HFSM user account to a secondary server.

To perform this step, see the latest manual of Hitachi File Service Manager (HFSM) or Storage Navigator Modular 2 (SNM2).

Displaying the capacity for file storage VVols

If you expand the capacity of file systems by using SMU, the capacity of the file systems and associated storage containers is not refreshed to the expanded value in HCS for VVols.

To reference the latest capacity, use SMU or HCS.

Creating or editing the storage container for file storage VVols

If multiple users create or edit storage containers at the same time by using HCS for VVols, a file system might be added to the wrong storage container.

Displaying the Enterprise Virtual Server (EVS) of a file system on file storage VVols

In HCS for VVols, an incorrect value is displayed as the EVS of a file system.

To check the correct EVS, use SMU or HCS.

Displaying the Enterprise Virtual Server (EVS) and status of a file system on file storage VVols

In HCS for VVols, the EVS value and status of a file system might not be displayed.

To check the correct EVS and status, use SMU or HCS.

Editing a template file for email notification

When saving a template file for email notification, do not save it with an option to include the byte order mark (BOM).

If the BOM is included in the template file, sending an email fails with the KAIC18797-E message.

If the BOM is already included in the template file, open the file with a text editor and then save it without adding the BOM.

Note: Some text editors do not have an option to save a file without the BOM.

For example, the Windows default text editor Notepad can only save BOM encoded files, so that the files saved by Windows Notepad always contain the BOM.

Editing storage containers for file storage VVols

If a file system is removed from the storage container associated with the datastore used by VMs, the VMs might become unavailable.

Before removing a file system from the associated storage container, confirm with the VM administrator that no VM is in operation on the datastore.

Documentation

Available documents

Document name	Document number	Issue date
Hitachi Command Suite User Guide	MK-90HC172-24	May 2016
Hitachi Command Suite CLI Reference Guide	MK-90HC176-24	
Hitachi Command Suite Tiered Storage Manager CLI Reference Guide	MK-90HC177-21	
Hitachi Command Suite Messages	MK-90HC178-24	
Hitachi Command Suite Audit Log Reference Guide	MK-92HC213-10	
Hitachi Command Suite Installation and Configuration Guide	MK-90HC173-24	
Hitachi Command Suite Administrator Guide	MK-90HC175-24	
Hitachi Command Suite Configuration Manager REST API Reference Guide	MK-92HC229-00	
Hitachi Command Suite Virtual Appliance Installation Guide	MK-92HC236-00	

Documentation errata

For 8.4.1-02

Manual Name: Hitachi Command Suite Administrator Guide

#	Section	Existing Content	Changes
1.	p.106 Ports used by Common Component	Table 9 Ports used by Common Component Port number : 22017/tcp Description : Used internally for Common Component communication (communication with the Web server). This port number can be changed.	Table 9 Ports used by Common Component Port number : 22017/tcp, 22018/tcp Description : Used when Global Link Manager is installed. This port number can be changed.
2.	p.106 Ports used by Common Component	Table 9 Ports used by Common Component Port number : 22018/tcp Description : Used internally for Common Component communication (receiving a termination message from the Web server). This port number can be changed.	[Content Removed]
3.	p.106 Ports used by Common Component	[Content Nonexistent]	Table 9 Ports used by Common Component Port number : 22121/tcp Description : Used internally for Common Component communication (communication with the Web server). This port number can be changed.
4.	p.106 Ports used by Common Component	[Content Nonexistent]	Table 9 Ports used by Common Component Port number : 22122/tcp Description : Used internally for Common Component communication (naming service). This port number can be changed.
5.	p.106 Ports used by Common Component	[Content Nonexistent]	Table 9 Ports used by Common Component Port number : 22123/tcp,22124/tcp Description : Used internally for Common Component communication (communication with the Web server). This port number can be changed.

#	Section	Existing Content	Changes
6.	p.115 Changing ports used by Common Component	[Content Nonexistent]	Table 15 Port number settings files for Common Component Default port number : 22121/tcp Setting files : In Windows: installation-folder-for-Hitachi-Command-Suite\Base64\uCPSB\CC\server\usrconf\ejb\DeviceManagerWebService\usrconf.properties In Linux: installation-directory-for-Hitachi-Command-Suite/Base64/uCPSB/CC/server/usrconf/ejb/DeviceManagerWebService/usrconf.properties Location : webserver.connector.ajp13.port
7.	p.115 Changing ports used by Common Component	[Content Nonexistent]	Table 15 Port number settings files for Common Component Default port number : 22122/tcp Setting files : In Windows: installation-folder-for-Hitachi-Command-Suite\Base64\uCPSB\CC\server\usrconf\ejb\DeviceManagerWebService\usrconf.properties In Linux: installation-directory-for-Hitachi-Command-Suite/Base64/uCPSB/CC/server/usrconf/ejb/DeviceManagerWebService/usrconf.properties Location : ejbserver.rmi.naming.port

#	Section	Existing Content	Changes
8.	p.115 Changing ports used by Common Component	[Content Nonexistent]	Table 15 Port number settings files for Common Component Default port number : 22123/tcp Setting files : In Windows: installation-folder-for-Hitachi-Command-Suite\Base64\uCPSB\CC\server\usrconf\ejb\DeviceManagerWebService\usrconf.properties In Linux: installation-directory-for-Hitachi-Command-Suite/Base64/uCPSB/CC/server/usrconf/ejb/DeviceManagerWebService/usrconf.properties Location : ejbserver.http.port
9.	p.115 Changing ports used by Common Component	[Content Nonexistent]	Table 15 Port number settings files for Common Component Default port number : 22124/tcp Setting files : In Windows: installation-folder-for-Hitachi-Command-Suite\Base64\uCPSB\CC\server\usrconf\ejb\DeviceManagerWebService\usrconf.properties In Linux: installation-directory-for-Hitachi-Command-Suite/Base64/uCPSB/CC/server/usrconf/ejb/DeviceManagerWebService/usrconf.properties Location : ejbserver.rmi.remote.listener.port

#	Section	Existing Content	Changes
10.	p.448 Resident processes of Hitachi Command Suite	Table 73 Resident processes in Windows Process name : hcmdssvctl.exe,cjstartweb.exe Service name : HBase 64 Storage Mgmt Common Service Function : Hitachi Command Suite servlet service. If the Device Manager server and other Hitachi Command Suite products are installed on the same computer, a process of a service other than HBase 64 Storage Mgmt Common Service might be started by using the name hcmdssvctl.exe and cjstartweb.exe.	Table 73 Resident processes in Windows Process name : hcmdssvctl.exe,cjstartweb.exe Service name : HBase 64 Storage Mgmt Common ServiceService Function : Hitachi Command Suite servlet service.
11.	p.448 Resident processes of Hitachi Command Suite	Table 73 Resident processes in Windows Process name : hcmdssvctl.exe,cjstartweb.exe Service name : HCS Device Manager Web Service Function : Device Manager servlet service	Table 73 Resident processes in Windows Process name : hcmdssvctl.exe,cjstartsv.exe Service name : HCS Device Manager Web Service Function : Device Manager servlet service
12.	p.449 Resident processes of Hitachi Command Suite	Table 74 Resident processes in Linux Process name : hcs_sso,cjstartweb Function : Hitachi Command Suite servlet service /bin/sh installation-directory-for-Hitachi-Command-Suite/Base64/uCPSB/CC/web/containers/HiCommand64/hcs_sso installation-directory-for-Hitachi-Command-Suite/Base64/uCPSB/CC/web/bin/cjstartweb	[Content Removed]
13.	p.449 Resident processes of Hitachi Command Suite	Table 74 Resident processes in Linux Process name : hcs_dm,cjstartweb Function : Device Manager servlet service /bin/sh installation-directory-for-Hitachi-Command-Suite/Base64/uCPSB/CC/web/containers/DeviceManagerWebService/hcs_dm installation-directory-for-Hitachi-Command-Suite/Base64/uCPSB/CC/web/bin/cjstartweb	Table 74 Resident processes in Linux Process name : hcs_dm,cjstartsv Function : Device Manager servlet service /bin/sh installation-directory-for-Hitachi-Command-Suite/Base64/uCPSB/CC/server/repository/DeviceManagerWebService/hcs_dm installation-directory-for-Hitachi-Command-Suite/Base64/uCPSB/CC/server/bin/cjstartsv

#	Section	Existing Content	Changes
14.	p.458 Hitachi Command Suite product services that are registered in cluster management applications	Table 77 Hitachi Command Suite product services that are registered in the cluster management applications on the management server Product name : Common Component Displayed service name : HBase 64 Storage Mgmt Common Service Service name : HBase64StgMgmtComService Remarks : This service is available if Device Manager and Global Link Manager are installed on the same management server.	Table 77 Hitachi Command Suite product services that are registered in the cluster management applications on the management server Product name : Common Component Displayed service name : HBase 64 Storage Mgmt Common Service Service name : HBase64StgMgmtComService Remarks : This service is available if Global Link Manager is installed on the same management server.
15.	p.578 Acquiring a thread dump of the HCS Device Manager Web Service (Windows)	installation-folder-for-Hitachi-Command-Suite\Base64\uCPSB\CC\web\containers\DeviceManagerWebService	installation-folder-for-Hitachi-Command-Suite\Base64\uCPSB\CC\server\public\ejb\DeviceManagerWebService

#	Section	Existing Content	Changes
16.	p.578 Acquiring a thread dump of the HBase 64 Storage Mgmt Common Service (Linux)	To acquire a thread dump of HBase 64 Storage Mgmt Common Service, execute the kill command, and then restart the Hitachi Command Suite product services. Procedure 1. Execute the following command: 578 Troubleshooting Hitachi Command Suite Administrator Guide # kill -3 PID PID is a process ID written in the installation-directory-for- Hitachi-Command-Suite/Base64/uCPSB/CC/web/containers/HiCommand64/logs/cjstdout.log file. Multiple process IDs are written to the cjstdout.log file. Specify the last process ID written to the file. 2. Restart the Hitachi Command Suite product services. Result The javacorexxx.xxx.txt file is output when using JDK bundled with Hitachi Command Suite, or the HiCommand64.log file is output when using Oracle JDK, to the following directory: installation-directory-for-Hitachi-Command-Suite/Base64/uCPSB/CC/web/containers/HiCommand64 If you are using the Oracle JDK, the HiCommand64.log file is overwritten each time it is output. We recommend saving the file by using a different name after the file is output. Related tasks • Starting the Hitachi Command Suite services on page 450 • Stopping the Hitachi Command Suite services on page 452	[Content Removed]
17.	p.579 Acquiring a thread dump of the HCS Device Manager Web Service (Linux)	installation-directory-for-Hitachi-Command-Suite/Base64/uCPSB/CC/web/containers/DeviceManagerWebService/logs/cjstdout.log	installation-directory-for-Hitachi-Command-Suite/Base64/uCPSB/CC/server/public/ejb/DeviceManagerWebService/logs/CC/maintenance/cjstdout.log

#	Section	Existing Content	Changes
18.	p.580 Acquiring a thread dump of the HCS Device Manager Web Service (Linux)	installation-directory-for-Hitachi-Command-Suite/Base64/uCPSB/CC/web/containers/DeviceManagerWebService	installation-directory-for-Hitachi-Command-Suite/Base64/uCPSB/CC/server/public/ejb/DeviceManagerWebService

Manual Name: Hitachi Command Suite Installation and Configuration Guide

#	Section	Existing Content	Changes
1.	p.138 Hitachi Command Suite services to register in cluster management applications (Windows)	Table 36 HCS services to be registered in the cluster management application *: This service is used if Device Manager and Global Link Manager are installed on the same management server.	Table 36 HCS services to be registered in the cluster management application *: This service is used if Global Link Manager is installed on the same management server.
2.	p.148 Creating scripts for registering Hitachi Command Suite services (Red Hat Enterprise Linux)	2. Unzip the script files to the /etc/init.d directory. Script files are included for registering the following HCS services: Service name Script name HiRDB sc_hbase64_hirdb HBase 64 Storage Mgmt SSO Service sc_hbase64_hsso HBase 64 Storage Mgmt Web SSO Service sc_hbase64_hweb HBase 64 Storage Mgmt Web Service sc_hbase64_web HBase 64 Storage Mgmt Common Service sc_hbase64_sso HCS Device Manager Web Service sc_hbase64_dm HiCommandServer sc_hicommand HiCommand Tiered Storage Manager sc_htsmserver Configuration Manager REST API sc_confmanagerctrl* * This is a script file included in HCS_LinuxCluster_SampleScripts_ConfManager.zip. This script file is required only when using the REST API.	2. Unzip the script files to the /etc/init.d directory. Script files are included for registering the following HCS services: Service name Script name HiRDB sc_hbase64_hirdb HBase 64 Storage Mgmt SSO Service sc_hbase64_hsso HBase 64 Storage Mgmt Web SSO Service sc_hbase64_hweb HBase 64 Storage Mgmt Web Service sc_hbase64_web HCS Device Manager Web Service sc_hbase64_dm HiCommandServer sc_hicommand HiCommand Tiered Storage Manager sc_htsmserver Configuration Manager REST API sc_confmanagerctrl* * This is a script file included in HCS_LinuxCluster_SampleScripts_ConfManager.zip. This script file is required only when using the REST API.

#	Section	Existing Content	Changes
3.	p.149-150 Registering Hitachi Command Suite services (Red Hat Enterprise Linux)	Table 37 Values to specify for each service item registered in a service group 5 HBase 64 Storage Mgmt Common Service sc_hbase64_sso /etc/init.d/sc_hbase64_sso 6 HCS Device Manager Web Service sc_hbase64_dm /etc/init.d/sc_hbase64_dm 7 HiCommandServer sc_hicommand /etc/init.d/sc_hicommand 8 HiCommand Tiered Storage Manager sc_htsmserver /etc/init.d/sc_htsmserver 9 Configuration Manager REST API sc_confmanagerctrl /etc/init.d/sc_confmanagerctrl	Table 37 Values to specify for each service item registered in a service group 5 HCS Device Manager Web Service sc_hbase64_dm /etc/init.d/sc_hbase64_dm 6 HiCommandServer sc_hicommand /etc/init.d/sc_hicommand 7 HiCommand Tiered Storage Manager sc_htsmserver /etc/init.d/sc_htsmserver 8 Configuration Manager REST API sc_confmanagerctrl /etc/init.d/sc_confmanagerctrl
4.	p.188 HCS server ports	Table 42 Port numbers used by HCS 22015-22018/tcp 22025/tcp 22026/tcp 22032/tcp Common Component ports Change the settings for the product that uses this port or change Common Component settings.	Table 42 Port numbers used by HCS 22015-22018/tcp 22032/tcp 22121-22124/tcp Common Component ports Change the settings for the product that uses this port or change Common Component settings.

Copyrights and licenses