

Hitachi Tiered Storage Manager Software Server Configuration and Operation Guide

FASTFIND LINKS

[Document Organization](#)

[Product Version](#)

[Getting Help](#)

[Table of Contents](#)

Copyright © 2010 Hitachi Ltd., Hitachi Data Systems Corporation, ALL RIGHTS RESERVED

No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording, or stored in a database or retrieval system for any purpose without the express written permission of Hitachi Ltd. (hereinafter referred to as "Hitachi") and Hitachi Data Systems Corporation (hereinafter referred to as "Hitachi Data Systems").

Hitachi and Hitachi Data Systems reserve the right to make changes to this document at any time without notice and assume no responsibility for its use. 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.

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.

Notice: Hitachi Data Systems products and services can be ordered only under the terms and conditions of Hitachi Data Systems' applicable agreement(s). The use of Hitachi Data Systems products is governed by the terms of your agreement(s) with Hitachi Data Systems.

By using this software, you agree that you are responsible for:

- a) Acquiring the relevant consents as may be required under local privacy laws or otherwise from employees and other individuals to access relevant data; and
- b) Ensuring that data continues to be held, retrieved, deleted or otherwise processed in accordance with relevant laws.

Hitachi is a registered trademark of Hitachi, Ltd. in the United States and other countries. Hitachi Data Systems is a registered trademark and service mark of Hitachi in the United States and other countries.

Lightning 9900 and Universal Storage Platform are trademarks of Hitachi Data Systems.

All other trademarks, service marks, and company names are properties of their respective owners.

Microsoft product screen shot(s) reprinted with permission from Microsoft Corporation.



Contents

Prefacexi
Intended Audience	xii
Product Version	xii
Release Notes	xii
Document Revision Level	xii
Document Organization	xiii
Referenced Documents	xiii
Document Conventions	xiv
Convention for Storage Capacity Values	xv
Getting Help	xv
Comments	xv
1 Server configuration and operation overview	1-1
Tiered Storage Manager environment	1-2
System components	1-2
Typical configuration	1-2
Cluster environment.	1-3
System requirements	1-4
Management server	1-4
Supported OSs	1-4
Required programs	1-8
Related software	1-9
Computer specifications	1-10
Management client	1-13
System requirements for the Web client.	1-13
System requirements for the CLI client	1-17
Storage subsystem domain controller	1-20
Domain controller	1-20
Connecting SMI-S Enabled subsystems	1-21
Supported storage subsystems	1-21
Required programs	1-21
Prerequisites for connecting to an SMI-S Enabled subsystem	1-21

2	Server configuration information	2-1
Configuring for an IPv6 environment		2-2
Restrictions		2-2
Settings		2-2
Settings for IPv6 addresses		2-2
Settings for SSL communication		2-3
Changing the server IP address or host name		2-4
Changing the IP address		2-4
Changing the host name		2-6
Settings required after changing the IP address or host name		2-9
Changing the ports used by Common Component		2-9
Access to the non-SSL HBase Storage Mgmt Web Service (23015)		2-11
Access to the SSL HBase Storage Mgmt Web Service (23016)		2-11
Access to the HBase Storage Mgmt Common Service AJP connection (23017)		2-12
Stop request access to the HBase Storage Mgmt Common Service (23018)		2-12
HiRDB (23032)		2-13
Configuring SSL communications		2-13
Between the HBase Storage Mgmt Web Service and the Web client		2-14
Between the Tiered Storage Manager server and the CLI client		2-14
Communication security settings on the Tiered Storage Manager server		2-14
Communication security settings on the CLI client		2-15
Configuring event notification		2-15
Registration		2-15
Customizing event notification templates		2-16
Specifying SMTP authentication user information		2-21
Registering a Web application		2-22
Using hcmdslink to register a Web application		2-23
Modifying the URL information		2-25
Security settings for user accounts		2-28
password.min.length		2-29
password.min.uppercase		2-29
password.min.lowercase		2-29
password.min.numeric		2-29
password.min.symbol		2-29
password.check.userID		2-29
account.lock.num		2-30
Configuring system account locking		2-30
Unlocking user accounts		2-31
Configuring an optional warning banner message		2-32
Editing the message		2-32
Registering the message		2-33
Deleting the message		2-34
Linking with Tuning Manager		2-35
Launching the historical report dialog box		2-35
Displaying array group usage		2-36

Starting HSSM from the Dashboard	2-37
Settings required when disconnecting the management server from the network	2-38

3 Server operation information. 3-1

Starting and stopping the server	3-2
Starting the Tiered Storage Manager server	3-2
Starting the Tiered Storage Manager server in a non-cluster configuration	3-2
Starting the Tiered Storage Manager server in a cluster configuration . . .	3-3
Stopping the Tiered Storage Manager server	3-3
Stopping the Tiered Storage Manager server in a non-cluster configuration	3-4
Stopping the Tiered Storage Manager server in a cluster configuration . .	3-5
Checking server status	3-6
Starting and stopping Common Component	3-7
Starting Common Component	3-7
Starting Common Component in a Windows environment	3-8
Starting Common Component in a Solaris or Linux environment	3-8
Stopping Common Component	3-9
Stopping Common Component in a Windows environment	3-9
Stopping Common Component in a Solaris or Linux environment	3-10
Resident processes	3-11
In Windows.	3-11
In Solaris or Linux	3-11
Moving repositories	3-12
Special precautions when moving repositories	3-13
Hitachi Storage Command Suite product type and version	3-13
User information	3-13
Folder capacity	3-13
Repository capacity	3-14
Moving repositories (Windows)	3-14
Exporting repositories on the migration source server	3-14
Importing repositories to the migration target server	3-15
Moving repositories (Solaris or Linux)	3-17
Exporting repositories on the migration source server	3-18
Importing repositories to the migration target server	3-19
Backing up repositories	3-21
Non-cluster environment (Windows)	3-22
Cluster environment (Windows)	3-23
Non-cluster environment (Solaris or Linux)	3-25
Cluster environment (Solaris)	3-26
Restoring repositories	3-29
Non-cluster environment (Windows)	3-30
Cluster environment (Windows)	3-31
Non-cluster environment (Solaris or Linux)	3-34
Cluster environment (Solaris)	3-36

4	Troubleshooting	4-1
	Troubleshooting information	4-2
	Log data output by Tiered Storage Manager	4-4
	Log types	4-5
	Message logs	4-5
	Trace logs	4-6
	Command trace logs	4-6
	Command log	4-7
	Service request reception log	4-7
	Output format	4-8
	Integrated trace log entries, message log entries, and trace log entries	4-8
	Event log entries	4-9
	syslog entries	4-10
	Command trace log entries	4-11
	Command logs	4-12
	Service request reception log entries	4-12
	Log contents	4-13
	Message ID and message type	4-13
	Event type	4-14
	Integrated logging	4-14
	Integrated log output	4-14
	Common Component trace log properties	4-15
	Specifying the number of trace log files	4-15
	Specifying the size of trace log files	4-16
	Audit log data	4-17
	Audit log objectives	4-17
	Event descriptions	4-18
	Events output to the audit log	4-18
	Audit log settings	4-36
	In Windows	4-36
	In Solaris or Linux	4-37
	Output format	4-38
	Header for audit log data	4-38
	Audit log messages	4-40
	Details of application specific information	4-43
	Calculating the volume of audit log data	4-50
	Volume of output audit log data for each GUI operation	4-51
	Volume of output audit log data for each CLI command	4-53
	Correlating user operations and audit log data	4-56
	GUI operations and corresponding output audit log data	4-56
	CLI commands and corresponding output audit log data	4-59
	Retrieving log information	4-62
	Setting up the environment for the hcmdsgetlogs command	4-63
	CLI_DIR	4-63
	SYSLOG	4-63
	Using the get logs command	4-63

A	Property descriptions and environment settings	A-1
	Property descriptions	A-2
	Environment settings	A-5
	Configuring environment settings related to Tiered Storage Manager server operations.	A-5
	server.rmi.secure	A-5
	server.rmi.port	A-6
	server.rmi.security.port	A-6
	server.base.initialsynchro	A-6
	server.mail.smtp.host	A-6
	server.mail.from	A-6
	server.mail.errorsTo	A-7
	server.mail.smtp.port	A-7
	server.mail.smtp.auth	A-7
	server.eventNotification.mail.to	A-7
	server.eventMonitoringIntervalInMinute	A-7
	server.migration.multiExecution	A-7
	server.checkOutVolumeRange	A-8
	server.repository.autoRefresh.pollingIntervalInMinute	A-8
	server.repository.autoRefresh.serverStarted	A-8
	server.repository.autoRefresh.recurringLocalTime	A-8
	server.repository.dvmModifyCheck.pollingIntervalInMinute	A-9
	server.migration.dataErase.defaultValue	A-9
	server.migrationPlan.candidateVolumeCountLimit	A-9
	server.migrationPlan.candidateCapacityGroupDisplayMaxCount.	A-10
	server.migration.maxRetryCount	A-10
	server.volumeCreation.param.defaultPortController	A-10
	Configuring environment settings related to Web client	A-11
	client.ldev.rowsperpage.retain.enabled.	A-11
	Configuring environment settings related to the repositories	A-11
	dbm.traceSQL	A-11
	Configuring environment settings related to accessing the Device Manager server.	A-11
	hdvm.protocol	A-12
	hdvm.host.	A-12
	hdvm.port.	A-12
	hdvm.timeout	A-12
	Configuring environment settings related to log output	A-12
	logger.messageLogLevel	A-13
	logger.traceLogLevel	A-14
	logger.syslogLevel	A-14
	logger.serverMessageFileCount	A-15
	logger.serverTraceFileCount	A-15
	logger.guiMessageFileCount	A-15
	logger.guiTraceFileCount.	A-16
	logger.serverMessageMaxFileSize.	A-16

logger.serverTraceMaxFileSize	A-16
logger.guiMessageMaxFileSize	A-16
logger.guiTraceMaxFileSize	A-17
Configuring environment settings related to linking to Tuning Manager . . .	A-17
htnm.infoAcquirePeriod	A-17
htnm.infoCachePeriodInMinute	A-19
htnm.servers	A-19
htnm.server. <i>n</i> .host	A-20
htnm.server. <i>n</i> .port	A-20

B **Estimating trace log volume B-1**

Estimating the volume of trace information output to the trace log file	B-2
Symbol definitions	B-2
Estimating trace log volume for different events	B-3
When refreshing a single storage domain	B-3
When performing a task information update	B-4
For event-monitoring processing	B-4
When monitoring automatic synchronization with Device Manager	B-5

Acronyms and Abbreviations

Glossary

Index



Preface

This manual describes how to set up, operate, and troubleshoot Hitachi Tiered Storage Manager, hereafter referred to as Tiered Storage Manager.

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

This preface includes the following information:

- ❑ [Intended Audience](#)
- ❑ [Product Version](#)
- ❑ [Release Notes](#)
- ❑ [Document Revision Level](#)
- ❑ [Document Organization](#)
- ❑ [Referenced Documents](#)
- ❑ [Document Conventions](#)
- ❑ [Convention for Storage Capacity Values](#)
- ❑ [Getting Help](#)
- ❑ [Comments](#)

Intended Audience

This manual is intended for system administrators who install, configure, and operate the Hitachi Tiered Storage Manager. The intended audience should have:

- Basic knowledge of the kinds of storage subsystems used by Tiered Storage Manager
- Basic knowledge of Storage Area Networks (SANs)
- Basic knowledge of migration, as described in the *Hitachi Tiered Storage Manager User's Guide*
- Knowledge of how to operate and manage systems using Hitachi Device Manager, which is a prerequisite product for running Tiered Storage Manager. Necessary knowledge includes how to manage resource group settings, how to create volumes (LDEVs), and how to create logical groups
- Knowledge of how to manage performance information using Hitachi Tuning Manager
- Basic knowledge of how to operate a supported OS of the Tiered Storage Manager server

Product Version

This document revision applies to the Hitachi Tiered Storage Manager version 6.4.

Release Notes

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

Document Revision Level

Revision	Date	Description
MK-08HC158-00	February 2009	Initial Release
MK-08HC158-01	July 2009	Revision 1, supersedes and replaces MK-08HC158-00
MK-08HC158-02	October 2009	Revision 2, supersedes and replaces MK-08HC158-01
MK-08HC158-03	December 2009	Revision 3, supersedes and replaces MK-08HC158-02
MK-08HC158-04	June 2010	Revision 4, supersedes and replaces MK-08HC158-03

Document Organization

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

Chapter	Description
Server configuration and operation overview	This chapter describes the components of Tiered Storage Manager and system requirements.
Server configuration information	This chapter describes how to set up networks, notifications, security, and linkage to related software for the Tiered Storage Manager server.
Server operation information	This chapter describes how to start and stop the Tiered Storage Manager server, how to start and stop Common Component, and the migration, backup, and restoration of repositories.
Troubleshooting	This chapter describes problems that might occur in the Tiered Storage Manager server, what to do when these problems occur, and how to obtain output log data and maintenance information.
Property descriptions and environment settings	This appendix describes the property descriptions and environment settings for Tiered Storage Manager.
Estimating trace log volume	This appendix describes the estimate of the volume of information output to the trace log files of the server.
Acronyms and Abbreviations	Defines the acronyms and abbreviations used in this document.
Glossary	Defines the special terms used in this document.
Index	Lists the topics in this document in alphabetical order.

Referenced Documents

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

- Hitachi Storage Command Suite Documents:
 - Hitachi Storage Command Suite Server Installation Guide, MK-98HC150
 - Hitachi Tiered Storage Manager User's Guide, MK-94HC090
 - Hitachi Tiered Storage Manager CLI Reference Guide, MK-94HC091
 - Hitachi Tiered Storage Manager Messages, MK-94HC092
 - Hitachi Device Manager Server Configuration and Operation Guide, MK-08HC157
 - Hitachi Device Manager Error Codes, MK-92HC016
 - Hitachi Tuning Manager Hardware Reports Reference, MK-95HC111
 - Hitachi Tuning Manager Server Administration Guide, MK-92HC021
 - Hitachi Tuning Manager Installation Guide, MK-96HC141





- Hitachi Enterprise Storage Systems Documents:
 - Universal Storage Platform and Network Storage Controller LUN Expansion, Virtual LVI/LUN and Volume Shredder User's Guide MK-94RD205
 - Hitachi TagmaStore Universal Storage Platform and Network Storage Controller Universal Volume Manager User's Guide, MK-94RD220
 - Hitachi TagmaStore USP and NSC Storage Navigator User's Guide, MK-94RD206

Document Conventions

This document uses the following typographic conventions:

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

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

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

Convention for Storage Capacity Values

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

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

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

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

Getting Help

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

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

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

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

Comments

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

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

Server configuration and operation overview

This chapter describes the Tiered Storage Manager components and the system requirements for using a Tiered Storage Manager server.

- ❑ [Tiered Storage Manager environment](#)
- ❑ [System requirements](#)

Tiered Storage Manager environment

This section describes the Tiered Storage Manager components and how to configure a Tiered Storage Manager server.

System components

Tiered Storage Manager is made up of the following components.

Table 1-1: Basic components of Tiered Storage Manager

Component	Description
Domain controller	A storage subsystem that can connect to external storage devices and integrate them into virtual volumes, allowing central management of separate storage subsystems. Both Universal Storage Platform V/VM and Hitachi USP are supported as domain controllers. Domain controllers can relocate data on storage volumes even if the volumes reside on storage subsystems of different scales or performance levels. Proper operation of Tiered Storage Manager cannot be guaranteed if you use multiple instances of Tiered Storage Manager to manage the same domain controller.
External storage subsystems	Storage subsystems that are connected to the domain controller and integrated into logical volumes.
Storage subsystems registered in Device Manager	Storage subsystems that have been registered in the Device Manager repository.
Management server	A computer on which the Tiered Storage Manager server is installed. The Tiered Storage Manager server controls the domain controller and connected external storage subsystems based on the commands executed by using the Web client or the CLI client from a management client.
Management client	A computer used by a system administrator or a host storage administrator to issue commands from the Web client or the CLI client to the Tiered Storage Manager server.
Hosts	Computers that use the storage volumes provided by the domain controller and external storage subsystems.

Typical configuration

To use a Tiered Storage Manager server in a non-cluster configuration, the following components must be connected by using a TCP/IP network:

- Management server
- Management client
- Domain controller
- External storage subsystems

- Storage subsystems registered in Device Manager
- Hosts

To use an external storage subsystem, a SAN must connect the subsystem, hosts, and the domain controller.

If Tiered Storage Manager is configured to retrieve data from Tuning Manager, any performance information collected and tabulated by Tuning Manager can be displayed as volume information in Tiered Storage Manager. This can be done even if Tuning Manager is not installed on the same computer as Tiered Storage Manager.

If you intend to use Tiered Storage Manager to manage mainframe volumes, install a Mainframe Agent on the host.



Note: Tiered Storage Manager supports only mainframe volumes that can be used with OS/390 or z/OS.

Figure 1-1: Example system configuration in a non-cluster environment shows an example of a typical system configuration in a non-cluster environment.

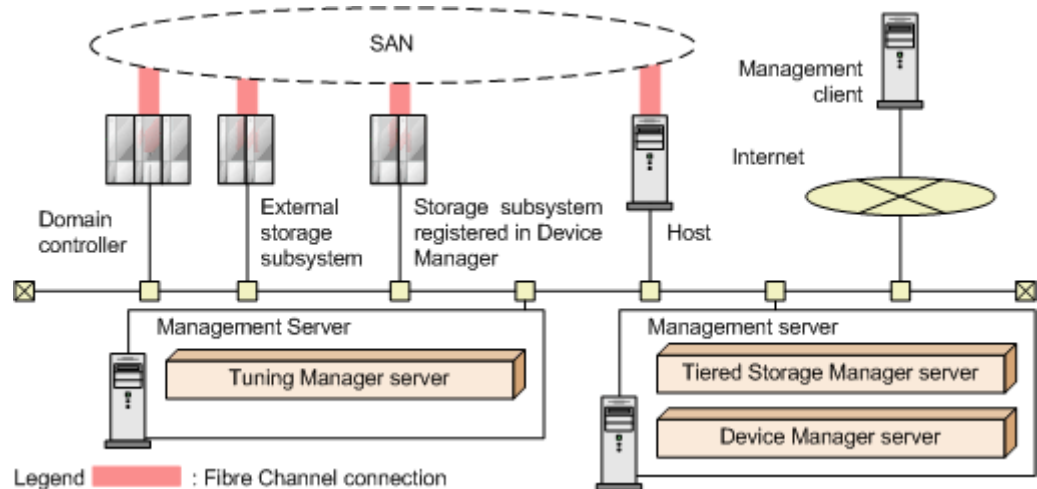


Figure 1-1: Example system configuration in a non-cluster environment

Cluster environment

A Tiered Storage Manager server can be configured for a cluster environment if the Device Manager server is configured for a cluster environment. To use a Tiered Storage Manager server in a cluster environment, the following components must be connected by using a TCP/IP network:

- Management server (executing)
- Management server (standby)
- Management client
- Domain controller
- External storage subsystems
- Storage subsystems registered in Device Manager

- Hosts

Additionally, in a system using a cluster environment, the management server requires a shared external disk. You prepare a shared external disk when you install a Tiered Storage Manager server.

[Figure 1-2: Example system configuration in a cluster environment](#) shows an example of a typical system configuration in a cluster environment.

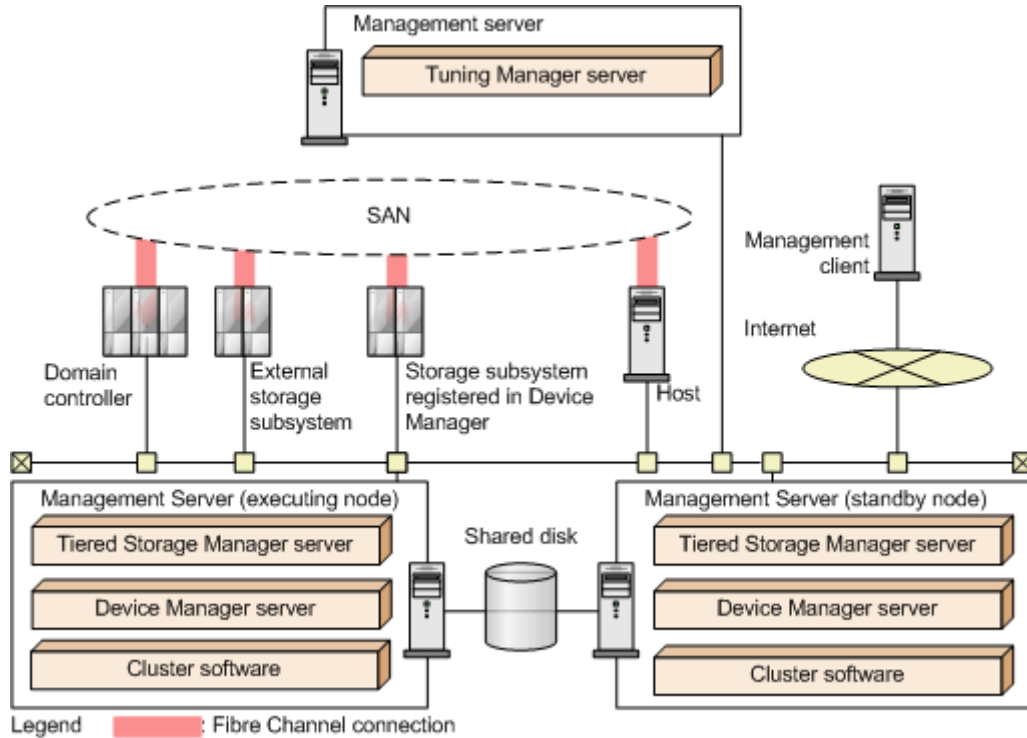


Figure 1-2: Example system configuration in a cluster environment

System requirements

This section describes the system requirements for using Tiered Storage Manager.

Management server

This section describes the system requirements for the management server on which the Tiered Storage Manager server is installed.

Supported OSs

OSs supported by the Tiered Storage Manager server are listed in [Table 1-2: OSs supported by the Tiered Storage Manager server \(Windows\)](#) and [Table 1-3: OSs supported by the Tiered Storage Manager server \(Solaris or Linux\)](#).

Table 1-2: OSs supported by the Tiered Storage Manager server (Windows)

Supported OS	Version	Service pack	IPv6 environment support
Windows Server® 2003 (x64) ^{#1#2}	Standard x64 Edition Enterprise x64 Edition Datacenter x64 Edition	SP2	Y
Windows Server 2003 (x86) ^{#1#2}	Standard Edition Enterprise Edition Datacenter Edition	SP2	Y
Windows Server 2003 R2 (x64) ^{#1#2}	Standard x64 Edition Enterprise x64 Edition Datacenter x64 Edition	SP2	Y
Windows Server 2003 R2 (x86) ^{#1#2}	Standard Edition Enterprise Edition Datacenter Edition	SP2	Y
Windows Server 2008 (x64) ^{#1#2#3}	Standard Edition Enterprise Edition Datacenter Edition Standard without Hyper-V™ Edition Enterprise without Hyper-V Edition Datacenter without Hyper-V Edition	No SP SP2	Y
Windows Server 2008 (x86) ^{#1#2#3}	Standard 32-bit Edition Enterprise 32-bit Edition Datacenter 32-bit Edition Standard without Hyper-V 32-bit Edition Enterprise without Hyper-V 32-bit Edition Datacenter without Hyper-V 32-bit Edition	No SP SP2	Y
Windows Server 2008 R2 (x64) ^{#1 #2 #3}	Standard Edition Enterprise Edition Datacenter Edition	No SP	Y
Windows Vista® (x86) ^{#1}	Business Edition Enterprise Edition Ultimate Edition	No SP SP1 SP2	Y
Windows XP (x86) ^{#1}	Professional Edition	SP2 SP3	N
Windows 7 (x64) ^{#1}	Professional Edition Enterprise Edition Ultimate Edition	No SP	Y
Windows 7 (x86) ^{#1}	Professional Edition Enterprise Edition Ultimate Edition	No SP	Y

Supported OS	Version	Service pack	IPv6 environment support
<p>Legend</p> <p>Y: Supported</p> <p>N: Not supported</p> <p>#1</p> <p>The Tiered Storage Manager server also runs on guest OSs on VMware® ESX version 3.x, VMware ESXi version 3.x, VMware ESX version 4.x, and VMware ESXi version 4.x.</p> <p>#2</p> <p>The Tiered Storage Manager server also runs on guest OSs of Hyper-V (version 1.0 or 2.0).</p> <p>#3</p> <p>The Tiered Storage Manager server does not support operations on Server Core.</p>			

Table 1-3: OSs supported by the Tiered Storage Manager server (Solaris or Linux)

Supported OS	Architecture	Required patch	IPv6 environment support
Red Hat Enterprise Linux 5.2	x86	--	Y
Red Hat Enterprise Linux 5.2 Advanced Platform	x86	--	Y
Red Hat Enterprise Linux 5.3	x64 x86	--	Y
Red Hat Enterprise Linux 5.3 Advanced Platform	x64 x86	--	Y
Red Hat Enterprise Linux 5.4	x64 x86	--	Y
Red Hat Enterprise Linux 5.4 Advanced Platform	x64 x86	--	Y
SUSE Linux Enterprise Server 10 SP2	x64 x86	--	Y
SUSE Linux Enterprise Server 10 SP3	x64 x86	--	Y
SUSE Linux Enterprise Server 11 (no SP)	x64 x86	--	Y

Supported OS	Architecture	Required patch	IPv6 environment support
Solaris 8	SPARC (32-bit or 64-bit)	Apply the following patches: <ul style="list-style-type: none"> • Patch Cluster • 108652-59 • 111293-04 • 108714-07 • 108827-30 • 121972-04 • All recommended patches listed at the Sun Microsystems web site are also required: http://www.sun.com 	N
Solaris 9	SPARC (32-bit or 64-bit)	Apply the following patch: 118335-08	N
Solaris 10 ^{#1}	SPARC (32-bit or 64 bit) ^{#2}	Apply the following patches: <ul style="list-style-type: none"> • 120664-01 • 127127-11 • 138064-03 ^{#3} 	Y
	x64	Apply the following patches: <ul style="list-style-type: none"> • 120665-01 • 127128-11 • 138065-03 ^{#3} 	Y
<p>Legend --: Not applicable Y: Supported N: Not supported</p> <p>#1 The Tiered Storage Manager server works only in a global environment (global zone). If you have created any non-global zones, make sure that you install the Tiered Storage Manager server in the global zone.</p> <p>#2 The Tiered Storage Manager server also runs on guest OSs of Solaris Logical Domains (LDom) 1.2 or 1.3.</p> <p>#3 Apply this patch if you use Solaris 10 11/06 (update 3), Solaris 10 8/07 (update 4), or Solaris 10 5/08 (update 5). Check the /etc/release file for the update number. The following shows an example of the /etc/release file for Solaris 10 11/06:</p> <pre>Solaris 10 11/06 s10s_u3wos_10 SPARC Copyright 2006 Sun Microsystems, Inc. All Rights Reserved. Use is subject to license terms. Assembled 14 November 2006</pre>			

The OSs and cluster software required for configuring the Tiered Storage Manager server in a cluster configuration are listed in [Table 1-4: OSs and cluster software required for configuring the Tiered Storage Manager server](#)

in a cluster configuration (Windows) and [Table 1-5: OSs and cluster software required for configuring the Tiered Storage Manager server in a cluster configuration \(Solaris\)](#).

Table 1-4: OSs and cluster software required for configuring the Tiered Storage Manager server in a cluster configuration (Windows)

Supported OS	Version	Service pack	Cluster software
Windows Server 2003 (x86)	Standard Edition Enterprise Edition Datacenter Edition	SP2	Microsoft® Cluster Server
Windows Server 2003 R2 (x86)	Standard Edition Enterprise Edition Datacenter Edition	SP2	
Windows Server 2008 (x64)	Standard Edition Enterprise Edition Datacenter Edition Standard without Hyper-V Edition Enterprise without Hyper-V Edition Datacenter without Hyper-V Edition	No SP SP2	Microsoft Failover Cluster
Windows Server 2008 (x86)	Standard 32-bit Edition Enterprise 32-bit Edition Datacenter 32-bit Edition Standard without Hyper-V 32-bit Edition Enterprise without Hyper-V 32-bit Edition Datacenter without Hyper-V 32-bit Edition	No SP SP2	

Table 1-5: OSs and cluster software required for configuring the Tiered Storage Manager server in a cluster configuration (Solaris)

Supported OS	Architecture	Cluster software
Solaris 9	SPARC (32-bit or 64-bit)	Sun Cluster 3.1 VERITAS Cluster Server 4.0
Solaris 10	SPARC (32-bit or 64-bit) x64	VERITAS Cluster Server 4.1 MP2 Veritas Cluster Server 5.0 MP1

Required programs

[Table 1-6: Required programs for the Tiered Storage Manager server](#) lists the programs required to run the Tiered Storage Manager server.

Table 1-6: Required programs for the Tiered Storage Manager server

Required program	Version	Description
Device Manager server	6.4	When you install the Tiered Storage Manager server, the Device Manager server is automatically installed (if it has not been installed already).
JRE	5.0.0	This program is required if the OS is Solaris 10 (x64). Install JDK 1.5.0, provided by Sun Microsystems, Inc.

Related software

By configuring Tiered Storage Manager to retrieve data from Tuning Manager, you can check performance information of storage subsystems from management clients. From the Tiered Storage Manager Web client, you can check performance information related to LDEVs or array groups by launching the Tuning Manager historical report dialog box. In addition, by using the Web client or CLI client, you can check array group usage. [Table 1-7: Software required to check performance information from management clients](#) lists all the software required to use Tuning Manager to check performance information from the management client.

Table 1-7: Software required to check performance information from management clients

Condition	Software	Version
Launching the historical report dialog box from the Web client	Tuning Manager server	6.2 or later
	Tuning Manager - Agent for RAID	6.2 or later
Checking the array group usage from the Web client or CLI client	Tuning Manager server	5.7 or later
	Tuning Manager - Agent for RAID	5.7 or later

By using Tiered Storage Manager, you can migrate and shred mainframe volumes on OS/390 or z/OS. Use the software listed in [Table 1-8: Software required to manage mainframe volumes](#) to manage mainframe volumes.

Table 1-8: Software required to manage mainframe volumes

Software	Version
Device Manager Mainframe Agent	6.0 or later

For details on the environment settings and conditions required to manage mainframe volumes by using Tiered Storage Manager, see the *Hitachi Tiered Storage Manager User's Guide*.

Computer specifications

To run the Tiered Storage Manager server, use a computer with the required specifications listed in [Table 1-9: Required computer specifications to run the Tiered Storage Manager server](#).

Table 1-9: Required computer specifications to run the Tiered Storage Manager server

Component	Minimum specification	Recommended specification
CPU	1 GHz or more	2 GHz or more
Physical memory	1 GB or more	2 GB or more
Disk capacity	1 GB or more	5 GB or more

To run the Tiered Storage Manager server on a guest OS, use a computer with a CPU clock speed of 2 GHz or higher, and allocate 2 GB or more of physical memory to the guest OS.

If adequate virtual memory is not allocated on the management server, the Hitachi Storage Command Suite products and any other installed programs might become unstable or might not start. To ensure stable operation of the management server, in addition to the virtual memory required for the OS and other programs, the management server also requires the amount of virtual memory required for both the products shown in [Table 1-10: Virtual memory requirements](#) and for Common Component. In addition to the virtual memory required for all the products installed on a management server, be sure to secure enough virtual memory (500MB) for Common Component.

[Table 1-10: Virtual memory requirements](#) shows the virtual memory requirements for each Hitachi Storage Command Suite product in v6.4.

Table 1-10: Virtual memory requirements

Product name	Virtual memory requirement (MB)
Device Manager ^{#1}	1,024
Provisioning Manager	included in Device Manager
Tiered Storage Manager	600
Tuning Manager ^{#2}	1,500
Replication Manager ^{#3}	100
Global Link Manager	300
NAS Manager ^{#4}	512
Storage Navigator Modular 2 ^{#4}	192

Product name	Virtual memory requirement (MB)
<p>Note:</p> <p>If you plan to install Device Manager, Tiered Storage Manager, and Replication Manager, and if 1,000 MB of virtual memory is already used by the OS and other programs, you must secure more than 3,224 MB of virtual memory. 1,024 (for Device Manager) + 600 (for Tiered Storage Manager) + 100 (for Replication Manager) + 500 (for Common Component) + 1,000 (already used virtual memory) = 3,224</p> <p>#1 If the Device Manager agent is installed on the management server, you need to allocate additional virtual memory for it. For details on virtual memory requirements and allocating virtual memory, see the description of the <code>server.agent.maxMemorySize</code> property in the <i>Hitachi Device Manager Agent Installation Guide</i>.</p> <p>#2 If the Tuning Manager agent is installed on the management server, you need to allocate additional virtual memory for it. For details on virtual memory requirements, see the description of memory requirements in the <i>Hitachi Tuning Manager Software Installation Guide</i>.</p> <p>#3 If Replication Manager Application Agent is installed on the management server, you need to allocate additional virtual memory for it. For details on virtual memory requirements, see the <i>Hitachi Replication Manager Software Installation and Configuration Guide</i>.</p> <p>#4 The virtual memory requirements listed in the table are for NAS Manager version 6.3 and Storage Navigator Modular 2 version 9.00. For details on the latest virtual memory requirements, see the documentation for each product.</p>	

Information about storage subsystem configurations that is collected from Device Manager is stored by Tiered Storage Manager in repositories. Therefore, depending on the storage subsystem configurations, more disk capacity might become necessary than the amount allocated at installation.

You can use the formula below to calculate the capacity required for repositories. Use this formula to ensure that the repository storage destination is large enough.

⌈x / y⌉ indicates the value obtained by rounding up the solution of x / y.

$$\begin{aligned}
 & (100 + \lceil \text{NumDomain} / 20 \rceil + \lceil \text{NumTier} / 15 \rceil + \lceil \text{NumMG} / 15 \rceil \\
 & + \lceil \text{NumMGVolume} / 60 \rceil + \lceil \text{NumTask} / 5 \rceil + \lceil \text{NumMGTaskVolume} / 15 \rceil \\
 & + \lceil \text{NumLKTaskVolume} / 30 \rceil + \lceil \text{NumSRTaskVolume} / 40 \rceil \\
 & + \lceil \text{NumCVTaskFreeSpace} / 40 \rceil + \lceil \text{NumCVTaskVolume} / 150 \rceil \\
 & + \lceil \text{NumEMTaskVolume} / 60 \rceil + \lceil \text{NumEMTaskPath} / 60 \rceil \\
 & + \lceil (\text{NumDomain} \times (\text{NumExternalSystem} + 1)) / 30 \rceil + \lceil \text{NumLDEV} / 5 \rceil \\
 & + \lceil \text{NumPath} / 10 \rceil + \lceil \text{NumRepInfo} / 50 \rceil + \lceil \text{NumExternalSystem} / 70 \rceil \\
 & + \lceil \text{NumPool} / 100 \rceil + \lceil \text{NumLabel} / 80 \rceil) \times 0.04 \text{ [MB]}
 \end{aligned}$$

Variables used in this formula to calculate the capacity requirements are listed in [Table 1-11: Variables used to calculate the capacity required for repositories](#).

Table 1-11: Variables used to calculate the capacity required for repositories

Variable	Description
NumDomain	Number of storage domains managed by Tiered Storage Manager
NumTier	Number of storage tiers managed by Tiered Storage Manager
NumMG	Number of migration groups managed by Tiered Storage Manager
NumMGVolume	Total number of volumes in the migration groups managed by Tiered Storage Manager
NumTask	Number of tasks registered to Tiered Storage Manager
NumMGTaskVolume	Total number of migration pairs in the migration tasks registered to Tiered Storage Manager
NumLKTaskVolume	Total number of volumes in the locking or unlocking tasks registered to Tiered Storage Manager
NumSRTaskVolume	Total number of volumes in the shredding tasks registered to Tiered Storage Manager
NumCVTaskFreeSpace	Total amount of free space targeted for volume creation by the volume creation tasks registered in Tiered Storage Manager
NumCVTaskVolume	Total number of volumes scheduled for creation by volume creation tasks registered in Tiered Storage Manager (number of volumes requested to be created)
NumEMTaskVolume	Total number of external volumes in the external mapping tasks registered in Tiered Storage Manager
NumEMTaskPath	Total number of mapping paths in the external mapping tasks registered in Tiered Storage Manager
NumExternalSystem	Number of external storage subsystems used by Tiered Storage Manager
NumLDEV	Number of LDEVs in the storage subsystems used by Tiered Storage Manager
NumPath	Number of paths in the storage subsystems used by Tiered Storage Manager
NumRepInfo	Total number of the following items in the storage subsystems used by Tiered Storage Manager: <ul style="list-style-type: none"> • TrueCopy pairs • ShadowImage pairs • Universal Replicator pairs • Copy-On-Write Snapshot pairs
NumPool	Number of DP pools in the storage subsystem used by Tiered Storage Manager
NumLabel	Total number of labels set for LDEVs

Management client

This section describes the management client requirements for using the Tiered Storage Manager Web client and the CLI client.

System requirements for the Web client

For OSs and browsers supported by the Tiered Storage Manager Web client, see [Table 1-12: OSs and browsers supported by the Tiered Storage Manager Web client \(Windows\)](#) and [Table 1-13: OSs and browsers supported by the Tiered Storage Manager Web client \(other than Windows\)](#).

Table 1-12: OSs and browsers supported by the Tiered Storage Manager Web client (Windows)

Supported OS	Version	Service pack	Supported browser	IPv6 environment support
Windows Server 2003 (x86)	Standard Edition Enterprise Edition Datacenter Edition	SP2	Internet Explorer® 6.0 ^{#1}	Y
			Internet Explorer 7.0 ^{#1}	N
Windows Server 2003 R2 (x86)	Standard Edition Enterprise Edition Datacenter Edition	SP2	Internet Explorer 6.0 ^{#1}	Y
			Internet Explorer 7.0 ^{#1}	N
Windows Server 2008 (x64)	Standard Edition Enterprise Edition Datacenter Edition Standard without Hyper-V Edition Enterprise without Hyper-V Edition Datacenter without Hyper-V Edition	No SP SP2	Internet Explorer 7.0 ^{#1#2#3} Internet Explorer 8.0 ^{#2#3}	Y
Windows Server 2008 (x86)	Standard 32-bit Edition Enterprise 32-bit Edition Datacenter 32-bit Edition Standard without Hyper-V 32-bit Edition Enterprise without Hyper-V 32-bit Edition Datacenter without Hyper-V 32-bit Edition	No SP SP2	Internet Explorer 7.0 ^{#1#2#3} Internet Explorer 8.0 ^{#2#3}	Y
Windows Server 2008 R2 (x64)	Standard Edition Enterprise Edition Datacenter Edition	No SP	Internet Explorer 8.0 ^{#2#3}	Y

Supported OS	Version	Service pack	Supported browser	IPv6 environment support
Windows Vista (x64)	Business Edition Enterprise Edition Ultimate Edition	No SP	Internet Explorer 7.0 Internet Explorer 8.0	Y
		SP1 SP2	Internet Explorer 7.0 ^{#1} Internet Explorer 8.0	Y
Windows Vista (x86)	Business Edition Enterprise Edition Ultimate Edition	No SP SP1 SP2	Internet Explorer 7.0 ^{#1} Internet Explorer 8.0	Y
Windows XP (x86)	Professional Edition	SP2 SP3	Internet Explorer 6.0 ^{#1} Internet Explorer 7.0 ^{#1}	Y
Windows 7 (x64)	Professional Edition Enterprise Edition Ultimate Edition	No SP	Internet Explorer 8.0	Y
Windows 7 (x86)	Professional Edition Enterprise Edition Ultimate Edition	No SP	Internet Explorer 8.0	Y
Legend Y: Supported N: Not supported #1 The Tiered Storage Manager Web client also runs on guest OSs on VMware ESX version 3.x. #2 The Tiered Storage Manager Web client does not support operations on guest OSs of Hyper-V. #3 The Tiered Storage Manager Web client does not support operations on Server Core.				

Table 1-13: OSs and browsers supported by the Tiered Storage Manager Web client (other than Windows)

Supported OS	Architecture	Supported browser	IPv6 environment support
HP-UX 11i V1.0	PA-RISC (32-bit or 64-bit)	Mozilla 1.7.8 Mozilla 1.7.12.01	N
HP-UX 11i V2.0	IPF	Mozilla 1.7.8	N
		Mozilla 1.7.12.01	Y

Supported OS	Architecture	Supported browser	IPv6 environment support
HP-UX 11i V3.0	IPF	Firefox® 2.0.0.x	N
		Mozilla 1.7.13.01	Y
Red Hat Enterprise Linux 5.2	x86	Firefox 3.0.x	Y
Red Hat Enterprise Linux 5.2 Advanced Platform	x86	Firefox 3.0.x	Y
Red Hat Enterprise Linux 5.3	x64	Firefox 3.0.x	Y
	x86	Firefox 3.0.x	Y
Red Hat Enterprise Linux 5.3 Advanced Platform	x64	Firefox 3.0.x	Y
	x86	Firefox 3.0.x	Y
Red Hat Enterprise Linux 5.4	x64	Firefox 3.0.x	Y
	x86	Firefox 3.0.x	Y
Red Hat Enterprise Linux 5.4 Advanced Platform	x64	Firefox 3.0.x	Y
	x86	Firefox 3.0.x	Y
SUSE Linux Enterprise Server 10 SP2	x64	Firefox 2.0.x	Y
	x86	Firefox 2.0.x	Y
SUSE Linux Enterprise Server 10 SP3	x64	Firefox 3.5	Y
	x86	Firefox 3.5	Y
SUSE Linux Enterprise Server 11 (no SP)	x64	Firefox 3.0.x	Y
	x86	Firefox 3.0.x	Y
Solaris 8	SPARC (32-bit or 64-bit)	Mozilla 1.4	N
Solaris 9	SPARC (32-bit or 64-bit)	Mozilla 1.7	N
Solaris 10	SPARC (32-bit or 64-bit)	Firefox 2.0.0.x	N
		Mozilla 1.7	Y
	x64	Firefox 2.0.0.x	N
		Mozilla 1.7	Y
Legend Y: Supported N: Not supported			

For a list of OSs and browsers required to launch the Tuning Manager historical report dialog box, see [Table 1-14: OSs and browsers required to launch the Tuning Manager Historical Report dialog box \(Windows\)](#) and [Table 1-15: OSs and browsers required to launch the Tuning Manager Historical Report dialog box \(other than Windows\)](#).

Table 1-14: OSs and browsers required to launch the Tuning Manager Historical Report dialog box (Windows)

OS	Edition	Service pack	Browser
Windows Server 2003 (x86)	Standard Edition Enterprise Edition	SP2	Internet Explorer 6.0 Internet Explorer 7.0
Windows Server 2003 R2 (x86)	Standard Edition Enterprise Edition	SP2	Internet Explorer 6.0 Internet Explorer 7.0
Windows Server 2008 (x64)	Standard Edition Enterprise Edition	No SP SP2	Internet Explorer 7.0 Internet Explorer 8.0
Windows Server 2008 (x86)	Standard 32-bit Edition Enterprise 32-bit Edition	No SP SP2	Internet Explorer 7.0 Internet Explorer 8.0
Windows Server 2008 R2 (x64)	Business Edition Enterprise Edition	No SP	Internet Explorer 8.0
Windows Vista (x64)	Standard Edition Enterprise Edition Ultimate Edition	No SP	Internet Explorer 7.0 Internet Explorer 8.0
Windows Vista (x86)	Business Edition Enterprise Edition Ultimate Edition	No SP	Internet Explorer 7.0 Internet Explorer 8.0
Windows XP (x86)	Professional Edition	SP2	Internet Explorer 6.0 Internet Explorer 7.0

Table 1-15: OSs and browsers required to launch the Tuning Manager Historical Report dialog box (other than Windows)

OS	Architecture	Browser
HP-UX 11i V3.0	IPF	Firefox 2.0.0.x
Red Hat Enterprise Linux 5.3 Advanced Platform	x86	Firefox 3.0.x
Red Hat Enterprise Linux 5.4 Advanced Platform	x86	Firefox 3.0.x
Solaris 8	SPARC (32-bit or 64-bit)	Mozilla 1.4
Solaris 9	SPARC (32-bit or 64-bit)	Mozilla 1.7
Solaris 10	SPARC (32-bit or 64-bit)	Firefox 2.0.0.x Mozilla 1.7
	x64	Firefox 2.0.0.x

System requirements for the CLI client

OSs and JREs supported by the CLI client are listed in [Table 1-16:OSs and JREs supported by the CLI client \(Windows\)](#) and [Table 1-17:OSs and JREs supported by the CLI client \(other than Windows\)](#).

Table 1-16: OSs and JREs supported by the CLI client (Windows)

Supported OS	Version	Service pack	Supported JRE	IPv6 environment support
Windows Server 2003 (x64) ^{#1}	Standard x64 Edition Enterprise x64 Edition Datacenter x64 Edition	SP2	JRE 5.0 (Build 07 or later) JRE 6.0	Y
Windows Server 2003 (x86) ^{#1}	Standard Edition Enterprise Edition Datacenter Edition	SP2	JRE 1.4.2 (Build 06 or later)	N
			JRE 5.0 (Build 07 or later) JRE 6.0	Y
Windows Server 2003 R2 (x64) ^{#1}	Standard x64 Edition Enterprise x64 Edition Datacenter x64 Edition	SP2	JRE 5.0 (Build 07 or later) JRE 6.0	Y
Windows Server 2003 R2 (x86) ^{#1}	Standard Edition Enterprise Edition Datacenter Edition	SP2	JRE 5.0 (Build 07 or later) JRE 6.0	Y
Windows Server 2008 (x64) ^{#1#2#3}	Standard Edition Enterprise Edition Datacenter Edition Standard without Hyper-V Edition Enterprise without Hyper-V Edition Datacenter without Hyper-V Edition	No SP SP2	JRE 6.0	Y
Windows Server 2008 (x86) ^{#1#2#3}	Standard 32-bit Edition Enterprise 32-bit Edition Datacenter 32-bit Edition Standard without Hyper-V 32-bit Edition Enterprise without Hyper-V 32-bit Edition Datacenter without Hyper-V 32-bit Edition	No SP SP2	JRE 6.0	Y
Windows Server 2008 R2 (x64) ^{#2#3}	Standard Edition Enterprise Edition Datacenter Edition	No SP	JRE 6.0	Y

Supported OS	Version	Service pack	Supported JRE	IPv6 environment support
Windows Vista (x64) ^{#1}	Business Edition Enterprise Edition Ultimate Edition	No SP SP1 SP2	JRE 6.0	Y
Windows Vista (x86) ^{#1}	Business Edition Enterprise Edition Ultimate Edition	No SP SP1 SP2	JRE 6.0	Y
Windows XP (x86) ^{#1}	Professional Edition	SP2 SP3	JRE 1.4.2 (Build 06 or later) JRE 5.0 (Build 07 or later) JRE 6.0	N
Windows 7 (x64)	Professional Edition Enterprise Edition Ultimate Edition	No SP	JRE 6.0	Y
Windows 7 (x86)	Professional Edition Enterprise Edition Ultimate Edition	No SP	JRE 6.0	Y
Legend Y: Supported N: Not supported ^{#1} The CLI client also runs on guest OSs of VMware ESX version 3.x. ^{#2} The CLI client does not support operations on guest OSs of Hyper-V. ^{#3} The CLI client does not support operations on Server Core.				

Table 1-17: OSs and JREs supported by the CLI client (other than Windows)

Supported OS	Version	Supported JRE	IPv6 environment support
HP-UX 11i V1.0	PA-RISC (32-bit or 64-bit)	JRE 1.4.2 (Build 08 or later) JRE 5.0 (Build 03 or later)	N
HP-UX 11i V2.0	IPF	JRE 1.4.2 (Build 08 or later)	N
		JRE 5.0 (Build 03 or later)	Y
	PA-RISC (64-bit)	JRE 1.4.2 (Build 08 or later)	N
		JRE 5.0 (Build 03 or later)	Y
HP-UX 11i V3.0	IPF	JRE 1.4.2 (Build 08 or later)	N
		JRE 5.0 (Build 03 or later)	Y
	PA-RISC (64-bit)	JRE 1.4.2 (Build 08 or later) JRE 5.0 (Build 03 or later)	N

Supported OS	Version	Supported JRE	IPv6 environment support
Red Hat Enterprise Linux 5.2	x86	JRE 6.0	Y
Red Hat Enterprise Linux 5.2 Advanced Platform	x86	JRE 6.0	Y
Red Hat Enterprise Linux 5.3	x64	JRE 6.0	Y
	x86	JRE 6.0	Y
Red Hat Enterprise Linux 5.3 Advanced Platform	x64	JRE 6.0	Y
	x86	JRE 6.0	Y
Red Hat Enterprise Linux 5.4	x64	JRE 6.0	Y
	x86	JRE 6.0	Y
Red Hat Enterprise Linux 5.4 Advanced Platform	x64	JRE 6.0	Y
	x86	JRE 6.0	Y
Solaris 8	SPARC (32-bit or 64-bit)	JRE 1.4.2 (Build 06 or later) JRE 5.0 (Build 07 or later) JRE 6.0	N
Solaris 9	SPARC (32-bit or 64-bit)	JRE 1.4.2 (Build 06 or later) JRE 5.0 (Build 07 or later) JRE 6.0	N
Solaris 10	SPARC (32-bit or 64-bit)	JRE 1.4.2 (Build 06 or later) JRE 5.0 (Build 07 or later) JRE 6.0	N
			Y
	x64	JRE 5.0 (Build 07 or later)	Y
SUSE Linux Enterprise Server 10 SP2	x64	JRE 5.0 (Build 10 or later)	Y
	x86	JRE 5.0 (Build 10 or later)	Y
SUSE Linux Enterprise Server 10 SP3	x64	JRE 5.0 (Build 10 or later)	Y
	x86	JRE 5.0 (Build 10 or later)	Y
SUSE Linux Enterprise Server 11 (no SP)	x64	JRE 6.0	Y
	x86	JRE 6.0	Y
Legend Y: Supported N: Not supported			

You must meet the following physical memory and disk space requirements to run the CLI client.

- Disk space: 2 MB

- Physical memory: 150 MB

Storage subsystem domain controller

This section describes the requirements for a storage subsystem to be manageable by Tiered Storage Manager.

Domain controller

For details about which storage subsystems can be used as domain controllers and the required firmware versions, see the *Hitachi Tiered Storage Manager User's Guide*.

The programs listed in [Table 1-18: Required programs](#) must be installed on the domain controller.

Table 1-18: Required programs

Program	Conditions
JAVA™ API	Must be installed.
SNMP Agent	Must be installed.
LUN Manager	Must be installed.
Volume Migration V2	Must be installed. Volume Migration V2 is software used to tune and optimize access from hosts to hard disks, and to migrate volumes. Tiered Storage Manager uses Volume Migration V2 to perform migration. For details on how to install Volume Migration V2, see the <i>Storage Navigator User's Guide</i> .
Volume Shredder	This program must be installed in the following cases: <ul style="list-style-type: none"> If you want to erase migration source volumes after migration has finished. If you want to use shredding tasks. For details, see the <i>Virtual LVI/LUN (VLL) and Volume Shredder User's Guide</i> .
Universal Volume Manager	This program must be installed if you want to perform operations on a connected, external volume by using Tiered Storage Manager. For details, see the <i>Universal Volume Manager User's Guide</i> .
Data Retention	This program must be installed if you want to use the volume lock function.
Dynamic Provisioning	This program must be installed for: <ul style="list-style-type: none"> Migration to DP pools. Migration of DP volumes.
Open Volume Management	This program must be installed if you want to erase the data on multiple migration source volumes after they have been migrated within a DP volume, and then collect and delete the source volumes.

Connecting SMI-S Enabled subsystems

This section describes system requirements for establishing an external connection to an SMI-S Enabled subsystem volume.

Supported storage subsystems

Universal Storage Platform V/VM storage subsystems can externally connect to SMI-S Enabled subsystems.

[Table 1-19: SMI-S Enabled subsystems that can be used with Tiered Storage Manager](#) lists the SMI-S Enabled subsystems that can be used with Tiered Storage Manager.

Table 1-19: SMI-S Enabled subsystems that can be used with Tiered Storage Manager

Vendor name	Product name	Model no.
EMC	CLARiiON	CX 200 ^{#1} CX 300 ^{#1} CX 400 ^{#1} CX 500 ^{#1} CX 600 ^{#1} CX 700 ^{#1} CX3 series
HP	HP StorageWorks Enterprise Virtual Array	EVA 3000 EVA 4100 EVA 4400 EVA 5000 EVA 6100 EVA 6400 ^{#2} EVA 8100 EVA 8400 ^{#2}
^{#1} Volumes that are created with RAID level 0 cannot be externally connected.		
^{#2} The required microcode version of USP V/VM is 60-03-10-xx/xx or later.		

Required programs

The following program is required for establishing an external connection with an SMI-S Enabled subsystem volume:

- Universal Volume Manager

Prerequisites for connecting to an SMI-S Enabled subsystem

The following conditions must be satisfied in order to connect Universal Storage Platform V/VM with an SMI-S Enabled subsystem:

- An external port must be set up on Universal Storage Platform V/VM.
- The external port of Universal Storage Platform V/VM must be physically connected to one or more target ports on the SMI-S Enabled subsystem.

- An array group, or a virtual volume equivalent to an array group, must have been created on the SMI-S Enabled subsystem.

Server configuration information

This chapter describes configuration procedures for the following: networks, the automatic notification function, security, and the functionality for linking related software to a Tiered Storage Manager server.

- ❑ [Configuring for an IPv6 environment](#)
- ❑ [Changing the server IP address or host name](#)
- ❑ [Changing the ports used by Common Component](#)
- ❑ [Configuring SSL communications](#)
- ❑ [Configuring event notification](#)
- ❑ [Registering a Web application](#)
- ❑ [Modifying the URL information](#)
- ❑ [Security settings for user accounts](#)
- ❑ [Configuring system account locking](#)
- ❑ [Unlocking user accounts](#)
- ❑ [Configuring an optional warning banner message](#)
- ❑ [Linking with Tuning Manager](#)
- ❑ [Starting HSSM from the Dashboard](#)
- ❑ [Settings required when disconnecting the management server from the network](#)

Configuring for an IPv6 environment

This section describes the settings required to use the Tiered Storage Manager server in IPv6 environments.

Restrictions

When you use Tiered Storage Manager in IPv6 environments, the following restrictions apply:

- Both IPv6 and IPv4 should be configured to be used because even if IPv6 is being used, IPv4 is also required for processing.
- Only global IPv6 addresses are usable. Site-local addresses and link-local addresses are not usable.
- We recommend that when you must enter either the IP address or a host name of the Tiered Storage Manager server, you enter a host name. If you enter an IP address, in Internet Explorer 6.0, you might not be able to connect to the Tiered Storage Manager server or navigate between windows.

Settings

To use the Tiered Storage Manager server in an IPv6 environment, after you install Tiered Storage Manager, edit the `httpsd.conf` file, which is stored in the following location:

- In Windows:
installation-folder-of-Common-Component\httpsd\conf
- In Solaris or Linux:
installation-directory-of-Common-Component/httpsd/conf/



Note: If you have performed a new installation of Tiered Storage Manager, it is not necessary to edit the `httpsd.conf` file. This file is configured automatically during a new installation.



Caution: Stop operations of Tiered Storage Manager and Common Component before editing the `httpsd.conf` file. After editing the file, restart Tiered Storage Manager and Common Component to enable the changes in the file.

Settings for IPv6 addresses

Remove the hash mark (#) from the line that includes `Listen [::]:23015` (the default setting). By default, all IP addresses are set to allow communication.

Specify the same port number as that used on the `Listen` line for IPv4 addresses. The default port number is 23015.

The following example shows how to specify IPv6 addresses:

```
ServerName example.com
:
```



```

Listen 23015
Listen [::]:23015
SSLDisable
:
SSLSessionCacheSize 0
Listen 23016
#Listen [::]:23016
<VirtualHost *:23016>
    ServerName example.com
    SSLEnable
:

```



Caution: Do not delete or edit the default setting, `Listen 23015`. If you do this, communication using an IPv4 address will become unavailable.

Settings for SSL communication

Remove the hash mark (#) from the line that includes `Listen [::]:23016` (the default setting). By default, all IP addresses are set to allow communication.

Specify the same port number as that used on the `Listen` line for IPv4 addresses. The default value for the port number for SSL communications is 23016. For details about setting SSL communication, see [Between the HBase Storage Mgmt Web Service and the Web client](#).

The following example shows how to specify SSL communication:

```

ServerName example.com
:
Listen 23015
Listen [::]:23015
SSLDisable
:
SSLSessionCacheSize 0
Listen 23016
Listen [::]:23016
<VirtualHost *:23016>
    ServerName example.com
    SSLEnable

```

:



Caution: Do not delete or edit the default setting, `Listen 23016`. If you do this, communication using an IPv4 address will become unavailable.

Changing the server IP address or host name

If you change the IP address or host name of the management server, you also need to change the Common Component settings files.

Changing the IP address

This section describes how to change the IP address of the management server.



- If you have changed the IP address of the management server before changing the settings files of Hitachi Storage Command Suite products, write down the new IP address.
- Do not change the settings in the cluster configuration file (the `cluster.conf` file).

To change the IP address of the management server:

1. If HiCommand Suite products whose versions are earlier than 5.7 are running, stop their services.
For details about how to stop these services, see the manual for your product version.
2. Stop the services of Hitachi Storage Command Suite products and Common Component.
 - In Windows:
Select **Start, All Programs, Hitachi Storage Command Suite, Device Manager**, and then **Stop Server with Common Services**.
 - In Solaris or Linux:
Execute the following command:
`installation-directory-of-Common-Component/bin/hcmdssrv -stop`
3. Edit the `httpsd.conf` file.
If the old IP address is specified in the `httpsd.conf` file, change the IP address to the host name or the new IP address.
The `httpsd.conf` file is stored in the following locations:
 - In Windows:
`installation-folder-of-Common-Component\httpsd\conf\httpsd.conf`
 - In Solaris or Linux:
`installation-directory-of-Common-Component/httpsd/conf/httpsd.conf`



Note: We recommend that you specify the host name in the `httpsd.conf` file.

4. Edit the `pdsys` file and the `def_pdsys` file.

If the old IP address is specified in the `pdsys` file and the `def_pdsys` file, change the IP address to the loopback address `127.0.0.1`.

The `pdsys` and `def_pdsys` files are stored in the following locations:

- In Windows:

installation-folder-of-Common-Component\HDB\CONF\pdsys

installation-folder-of-Common-Component\database\work\def_pdsys

- In Solaris or Linux:

installation-directory-of-Common-Component/HDB/conf/pdsys

installation-directory-of-Common-Component/database/work/def_pdsys

5. Edit the `pdutsys` file and the `def_pdutsys` file.

If the old IP address is specified in the `pdutsys` file and the `def_pdutsys` file, change the IP address to the loopback address `127.0.0.1`.

The `pdutsys` and `def_pdutsys` files are stored in the following locations:

- In Windows:

installation-folder-of-Common-Component\HDB\CONF\pdutsys

installation-folder-of-Common-Component\database\work\def_pdutsys

- In Solaris or Linux:

installation-directory-of-Common-Component/HDB/conf/pdutsys

installation-directory-of-Common-Component/database/work/def_pdutsys



Note: If the management server is running in a cluster configuration, you also need to change the IP address specified in the `pdutsys` file and the `def_pdutsys` file to the loopback address `127.0.0.1` on the standby node.

6. Edit the `HiRDB.ini` file.

If the old IP address is specified in the `HiRDB.ini` file, change the IP address to the loopback address `127.0.0.1`.

The `HiRDB.ini` file is stored in the following locations:

- In Windows:

installation-folder-of-Common-Component\HDB\CONF\emb\HiRDB.ini

- In Solaris or Linux:

installation-directory-of-Common-Component/HDB/conf/emb/HiRDB.ini

7. Change the IP address of the management server, and then restart the computer.

If the IP address of the management server has already been changed before you change the Common Component settings files, just restart the computer.

8. Make sure that the Common Component service is running.
 - In Windows:
Select **Start, All Programs, Hitachi Storage Command Suite, Device Manager**, and then **Server and Common Services Status**.
 - In Solaris or Linux:
Execute the following command:

```
installation-directory-of-Common-Component/bin/hcmdssrv - status
```
9. If the IP address is used in the URLs for accessing Hitachi Storage Command Suite products, change the setting.
For details about how to change the URLs, see [Modifying the URL information](#).

If you change the IP address of the management server, you might need to revise the settings for each Hitachi Storage Command Suite product. For details about the settings that need to be changed, see [Settings required after changing the IP address or host name](#).

Changing the host name

This section describes how to change the host name of the management server.



- The host name must be no more than 32 bytes. You can use the following characters:
A to Z a to z 0 to 9 -
The host name cannot start or end with a hyphen (-).
 - If you have changed the host name of the management server before changing the settings files of Hitachi Storage Command Suite products, use the `hostname` command to display the new host name and write it down (for Windows, the `ipconfig /ALL` command can also be used to display host names). For the host name in the Device Manager settings file, specify the name you recorded earlier. Note that this name is case-sensitive.
-

To change the host name of the management server:

1. If HiCommand Suite products whose versions are earlier than 5.7 are running, stop their services.
For details about how to stop these services, see the manual for your product version.
2. Stop the services of Hitachi Storage Command Suite products and Common Component.
 - In Windows:

Select **Start, All Programs, Hitachi Storage Command Suite, Device Manager**, and then **Stop Server with Common Services**.

- In Solaris or Linux:

Execute the following command:

installation-directory-of-Common-Component/bin/hcmdssrv -stop

3. If TLS/SSL is used for communication between the management server and management clients, re-create a server certificate of the management server by using the new host name.

For details on how to create a server certificate, see the *Hitachi Device Manager Server Configuration and Operation Guide*.

4. For Solaris or Linux, edit the `/etc/hosts` file.

Change the host name of the management server to the new host name. For Linux, enter the new host name into the line above the `localhost` line.

5. Edit the `httpsd.conf` file.

Change the value for the `ServerName` parameter to the new host name.

The `httpsd.conf` file is stored in the following locations:

- In Windows:

installation-folder-of-Common-Component\httpsd\conf\httpsd.conf

- In Solaris or Linux:

installation-directory-of-Common-Component/httpsd/conf/
`httpsd.conf`

If TLS/SSL is used for communication between the management server and management clients, you also need to change the following settings:

- If a host name has been specified for the `<VirtualHost>` tag, change the host name to an asterisk (*).
- Change the value for the `ServerName` parameter in the `<VirtualHost>` tag to the new host name.

6. Edit the `pdsys` file and the `def_pdsys` file.

Change the value for the `pdunit` parameter's `-x` option to the loopback address `127.0.0.1`.

The `pdsys` and `def_pdsys` files are stored in the following locations:

- In Windows:

installation-folder-of-Common-Component\HDB\CONF\pdsys
installation-folder-of-Common-Component\database\work\def_pdsys

- In Solaris or Linux:

installation-directory-of-Common-Component/HDB/conf/pdsys
installation-directory-of-Common-Component/database/work/
`def_pdsys`

7. Edit the `pdutysys` file and the `def_pdutysys` file.

Change the value for the `pd_hostname` parameter to the loopback address `127.0.0.1`. If the `pd_hostname` parameter does not exist, add the `pd_hostname` parameter, specifying the loopback address.

The `pdutysys` and `def_pdutysys` files are stored in the following locations:

- In Windows:
installation-folder-of-Common-Component\HDB\CONF\pdutysys
installation-folder-of-Common-Component\database\work\def_pdutysys
- In Solaris or Linux:
installation-directory-of-Common-Component/HDB/conf/pdutysys
installation-directory-of-Common-Component/database/work/def_pdutysys



Note: If the management server is running in a cluster configuration, you also need to change the settings in the `pdutysys` file and the `def_pdutysys` file on the standby node. For the `pd_hostname` parameter on the standby node, specify the loopback address `127.0.0.1` or the host name of the executing node.

8. Edit the `HiRDB.ini` file.

Change the value for the `PDHOST` parameter to the loopback address `127.0.0.1`.

The `HiRDB.ini` file is stored in the following locations:

- In Windows:
installation-folder-of-Common-Component\HDB\CONF\emb\HiRDB.ini
- In Solaris or Linux:
installation-directory-of-Common-Component/HDB/conf/emb/HiRDB.ini

9. Edit the `cluster.conf` file (only for a cluster configuration).

Change the corresponding logical host name, executing node's host name, and standby node's host name to the new host names.

The `cluster.conf` file is stored in the following location:

- In Windows:
installation-folder-of-Common-Component\conf\cluster.conf
- In Solaris:
installation-directory-of-Common-Component/conf/cluster.conf

10. Change the host name for the management server, and then restart the computer.

If you have changed the host name for the management server before changing the Common Component settings files, just restart the computer.

11. Make sure that the Common Component service is running.

- In Windows:
Select **Start, All Programs, Hitachi Storage Command Suite, Device Manager**, and then **Server and Common Services Status**.
- In Solaris or Linux:
Execute the following command:

```
installation-directory-of-Common-Component/bin/hcmdssrv -
status
```

12. If the host name is used in the URLs for accessing Hitachi Storage Command Suite products, change the setting.

For details about how to change the URLs, see [Modifying the URL information](#).

If you change the host name of the management server, you need to check and, if necessary, revise the settings for each Hitachi Storage Command Suite product. For details about the settings that need to be changed, see [Settings required after changing the IP address or host name](#).

Settings required after changing the IP address or host name

This section describes the settings required in Tiered Storage Manager after you change the IP address or host name of the management server. For details about the settings for other Hitachi Storage Command Suite products, see the manual for each product.

In Tiered Storage Manager, check and revise the following settings:

- Environment settings related to access to the Device Manager server
If the old host name or IP address is specified for the `hdvm.host` property in the `devicemanager.properties` file, you need to specify the new host name or IP address, and then restart the Tiered Storage Manager server.

Also, depending on the operating environment, you might need to check and revise the following settings:

- If a RADIUS server is used to authenticate accounts
Check the settings in the `exauth.properties` file. For details on how to specify settings in the `exauth.properties` file, see the *Hitachi Device Manager Software Server Configuration and Operation Guide*

Changing the ports used by Common Component

When Tiered Storage Manager server is installed, default port numbers are assigned for the Tiered Storage Manager server and Common Component.

After installing Tiered Storage Manager server, if you want to change the ports used by Common Component, perform the following procedure:

1. Stop any other Hitachi Storage Command Suite product that is running.
2. Stop Device Manager and Common Component.
 - In Windows:

Select **Start, All Programs, Hitachi Storage Command Suite, Device Manager**, and then **Stop Server with Common Services**.

- In Solaris or Linux:

Execute the following command:

installation-directory-of-the-Device-Manager-server/suitesrvctl

Command syntax:

```
# /opt/HiCommand/suitesrvctl -stop_all
```

3. Open the setup file for editing and change the port number.

For details about the setup file for each port, see [Access to the non-SSL HBase Storage Mgmt Web Service \(23015\)](#) to [HiRDB \(23032\)](#) below.

4. Start the Device Manager and Common Component.

- In Windows:

Select **Start, All Programs, Hitachi Storage Command Suite, Device Manager**, and then **Start Server with Common Services**.

- In Solaris or Linux:

Execute the following command:

installation-directory-of-the-Device-Manager-server/suitesrvctl

Command syntax:

```
# /opt/HiCommand/suitesrvctl -start_all
```

5. If you change the following port numbers, you need to change the URLs used for accessing Hitachi Storage Command Suite products:

- 23015/tcp (used for accessing the HBase Storage Mgmt Web Service)

You need to change the URLs if you use non-SSL for communication between the management server and management clients.

- 23016/tcp (used for accessing the SSL HBase Storage Mgmt Web Service)

You need to change the URLs if you use SSL for communication between the management server and management clients.

For details about how to change the URLs, see [Modifying the URL information](#).

Note that you might not need to change the URLs depending on the network environment between the management server and management clients, such as an environment that has a firewall configured.

[Table 2-1: Ports used by Common Component](#) lists the ports used by Common Component.

Table 2-1: Ports used by Common Component

Network port	Description
23015/tcp	Used by the Tiered Storage Manager server to access the non-SSL HBase Storage Mgmt Web Service

Network port	Description
23016/tcp	Used by Web browsers to access the SSL HBase Storage Mgmt Web Service
23017/tcp	Used by the HBase Storage Mgmt Web Service to access the HBase Storage Mgmt Common Service through an AJP connection
23018/tcp	Used by the HBase Storage Mgmt Common Service to receive stop requests
23032/tcp	Used by Hitachi Storage Command Suite products to connect to HiRDB
23019/tcp -23031/tcp, 23033/tcp, and 23034/tcp	Reserved ports
45001/tcp - 49000/tcp	Used by HiRDB internal communication. Do not use these ports.

Access to the non-SSL HBase Storage Mgmt Web Service (23015)

To change the port used for accessing the non-SSL HBase Storage Mgmt Web Service, you must change the port number written in the following files:

- `httpsd.conf` file
Modify `Listen`.
- `hssso.conf` file
Modify `hssso.hostport`.

The `httpsd.conf` file and `hssso.conf` file are stored in the following locations:

In Windows:

- *installation-folder-of-Common-Component*\httpsd\conf\httpsd.conf
- *installation-folder-of-Common-Component*\conf\hssso.conf

In Solaris or Linux:

- *installation-directory-of-Common-Component*/httpsd/conf/httpsd.conf
- *installation-directory-of-Common-Component*/conf/hssso.conf



Caution: When SSL is enabled for accessing the HBase Storage Mgmt Web Service, port 23015 is used for internal communication. Therefore, do not delete or comment the `Listen 23015` line.

Access to the SSL HBase Storage Mgmt Web Service (23016)

To change the port used for accessing the SSL HBase Storage Mgmt Web Service, you must change the port number written in the following file:

- `httpsd.conf` file
Modify `VirtualHost host-name:port` and `Listen`.

The `httpsd.conf` file is stored in the following locations:

In Windows:

installation-folder-of-Common-Component\httpsd\conf\httpsd.conf

In Solaris or Linux:

installation-directory-of-Common-Component/httpsd/conf/
httpsd.conf



Caution: When SSL is enabled for accessing the HBase Storage Mgmt Web Service, port 23015 is used for internal communication. Therefore, do not delete or comment the `Listen 23015` line.

Access to the HBase Storage Mgmt Common Service AJP connection (23017)

To change the port used for accessing the HBase Storage Mgmt Common Service through an AJP connection, you must change the port number written in the following files:

- `workers.properties` file
Modify `worker.worker1.port`.
- `usrconf.properties` file
Modify `webserver.connector.ajpl3.port`.

The `workers.properties` file and `usrconf.properties` file are stored in the following locations:

In Windows:

- *installation-folder-of-Common-Component*\CC\web\redirector\workers.properties
- *installation-folder-of-Common-Component*\CC\web\containers\HiCommand\usrconf\usrconf.properties

In Solaris or Linux:

- *installation-directory-of-Common-Component*/CC/web/redirector/workers.properties
- *installation-directory-of-Common-Component*/CC/web/containers/HiCommand/usrconf/usrconf.properties

Stop request access to the HBase Storage Mgmt Common Service (23018)

To change the port through which the HBase Storage Mgmt Common Service receives stop requests, you must change the port number written in the following file:

- `usrconf.properties` file
Modify `webserver.shutdown.port`.

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

In Windows:

installation-folder-of-Common-Component\CC\web\containers\HiCommand\usrconf\usrconf.properties

In Solaris or Linux:

installation-directory-of-Common-Component/CC/web/containers/HiCommand/usrconf/usrconf.properties

HiRDB (23032)

To change the port used by HiRDB, you must change the port number written in the following files:

- *HiRDB.ini* file
Modify PDNAMEPORT.
- *pdsys* file
Modify pd_name_port.
- *def_pdsys* file
Modify pd_name_port.

The *HiRDB.ini* file, *pdsys* file, and *def_pdsys* file are stored in the following locations:

In Windows:

- *installation-folder-of-Common-Component*\HDB\CONF\emb\HiRDB.ini
- *installation-folder-of-Common-Component*\HDB\CONF\pdsys
- *installation-folder-of-Common-Component*\database\work\def_pdsys

In Solaris or Linux:

- *installation-directory-of-Common-Component*/HDB/conf/emb/HiRDB.ini
- *installation-directory-of-Common-Component*/HDB/conf/pdsys
- *installation-directory-of-Common-Component*/database/work/def_pdsys

Configuring SSL communications

To implement secure communication between the management server and the management client, you need to specify necessary security settings such as SSL (Secure Sockets Layer) or TLS (Transport Layer Security) to encrypt data transmission and user authentication.

The HBase Storage Mgmt Web Service supports SSL version 3 and TLS version 1.0.

When using Tiered Storage Manager, SSL is available for the following types of communication:

- Communication between the HBase Storage Mgmt Web Service and the Tiered Storage Manager client (the Tiered Storage Manager client in this case is the Web client)
- Communication between the Tiered Storage Manager server and the Tiered Storage Manager client (the Tiered Storage Manager client in this case is the CLI client)

Between the HBase Storage Mgmt Web Service and the Web client

To use SSL for communication between the HBase Storage Mgmt Web Service and the Web client:

1. Prepare a secret key and signed certificate.
2. Edit the `httpsd.conf` file.
3. Modify the URL information used for starting the Web client.

For details on step 1 and step 2, see the chapter describing Device Manager server security in the *Hitachi Device Manager Server Configuration and Operation Guide*.

After installation of the server, http is set as the protocol for accessing the HBase Storage Mgmt Web Service from the Web client. Change this to https, and then modify the port number in the URL to a port number for SSL communication (default value: 23016). For details on changing URL information, see [Modifying the URL information](#).

Between the Tiered Storage Manager server and the CLI client

To use SSL for communication between the Tiered Storage Manager server and the CLI client:

1. Specify communication security settings on the Tiered Storage Manager server.
2. Download an electronic certificate on the CLI client.

For SSL communication between the Tiered Storage Manager server and the CLI client, an electronic certificate is necessary. You can download the electronic certificate by using the Web browser provided by the CLI client. If you have already downloaded an electronic certificate in an earlier version of Tiered Storage Manager, and you want to enable SSL advanced security mode, you must download a new electronic certificate.

For details on how to download an electronic certificate, see the *Hitachi Tiered Storage Manager CLI Reference Guide*.

3. Specify communication security settings on the CLI client.

Communication security settings on the Tiered Storage Manager server

Set the following properties in the `server.properties` file:

- `server.rmi.secure`
- `server.rmi.security.port`

For details on each property, see [server.rmi.secure](#) and [server.rmi.security.port](#).

Communication security settings on the CLI client

Do the following:

- Set the environment variable `HTSM_CLI_CERTS_PATH`.
- Set the `option.secure` property in the `htsmcli.properties` file.

If you set the `option.secure` property in the `htsmcli.properties` file, you do not need to specify the `-s` or `--secure` option of the CLI command.

For details on each setting, see the *Hitachi Tiered Storage Manager CLI Reference Guide*.

Configuring event notification

The event notification function uses email to report an event that occurs asynchronously with user operations. You can configure event notification to send you an email you when any of the events occur that are listed in [Table 2-2: Event types](#).

Table 2-2: Event types

Event	Description
Migration task ended	This event occurs when a migration task ends successfully, ends due to a failure, or is canceled.
Shredding task ended	This event occurs when a shredding task ends successfully, ends due to a failure, or is canceled.
Locking task ended	This event occurs when a locking task ends successfully, ends due to a failure, or is canceled.
Unlocking task ended	This event occurs when an unlocking task ends successfully, ends due to a failure, or is canceled.
Volume creation task ended	This event occurs when a volume creation task ends successfully, ends due to a failure, or is canceled.
External connection settings task ended	This event occurs when an external connection settings task ends successfully, ends due to a failure, or is canceled.
Volume lock period expired	This event occurs when the volume lock period has expired for a volume in a migration group.
Specified time elapsed	This event occurs when a user-specified period has elapsed (for the GUI, the period is until a specified date; for the CLI the period is a specified number of days).

Registration

The event notification function is registered by specifying the following properties in the `server.properties` file:

- `server.mail.smtp.host`
- `server.mail.smtp.port`
- `server.mail.smtp.auth`
- `server.eventNotification.mail.to`
- `server.eventMonitoringIntervalInMinute`

After the `server.eventNotification.mail.to` property is specified, event notification will be performed for all events that occur on the server. For details about the property settings, see [Configuring environment settings related to Tiered Storage Manager server operations](#).



Caution: The `server.properties` file, the Web client, and the CLI client each have properties settings for specifying event notification. Specifying event notification in more than one of these locations results in delivery of duplicate or triplicate event notifications.

When an event notification email encounters a delivery error, an undeliverable notification email is sent to the email address specified in `server.mail.from` or `server.mail.errorsTo`.

The conditions for sending undeliverable notification email, the send destination, and the processing when an attempt to send an undeliverable notification email fails vary depending on the SMTP server.

Customizing event notification templates

You can edit the template files to customize the contents of event notification email.

Template files are stored in the following location:

- In Windows:
installation-folder-of-the-Tiered-Storage-Manager-server\conf
- In Solaris or Linux:
installation-directory-of-the-Tiered-Storage-Manager-server/conf

A template file is provided for each event. [Table 2-3: Template files](#) lists the template files and the events they are used for.

Table 2-3: Template files

Type	Event	Template file
Task ended	Migration task ended	mail-migrationtask-end.txt
	Shredding task ended	mail-shreddingtask-end.txt
	Locking task ended	mail-lockingtask-end.txt
	Unlocking task ended	mail-unlockingtask-end.txt
	Volume creation task ended	mail-volumecreationtask-end.txt
	External connection settings task ended	mail-externalmappingtask-end.txt

Type	Event	Template file
Time lapse	Volume lock period expired	mail-retention-term-expired.txt
	Specified time elapsed	mail-migrationgroup-reminder.txt

By specifying, within the template files, parameters that will automatically be filled in with event information at the time of an event, you can add useful information to the email notifications.

The following shows how to create a template, using the template for the *Migration task ended* event (mail-migrationtask-end.txt) as an example.

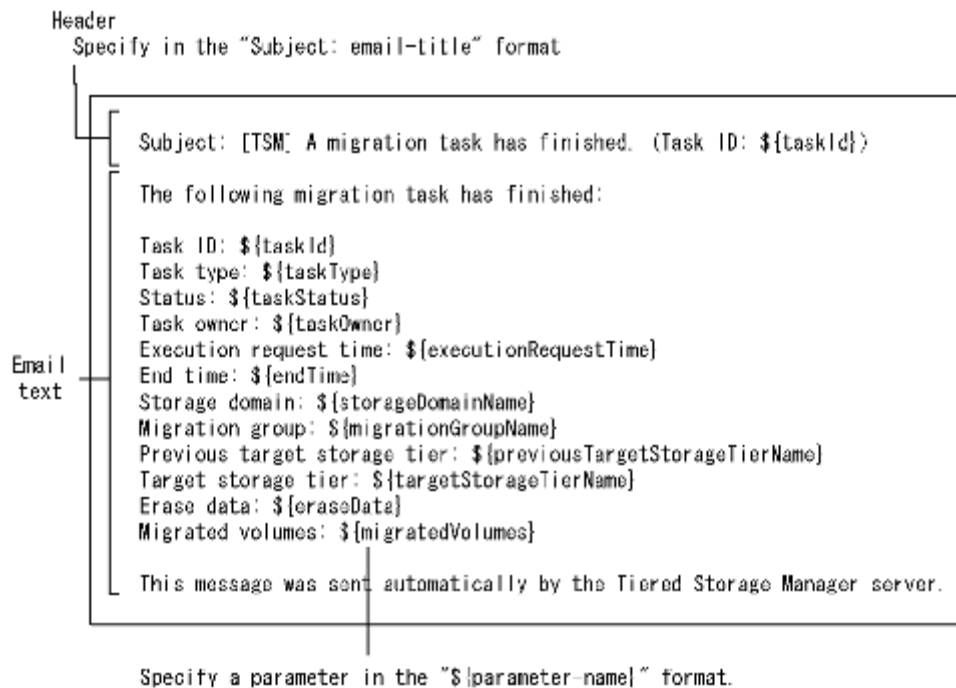


Figure 2-1: Creating a template

These items have a fixed format.

- **Header**—Specify as `Subject: email-title`.
- **Parameter**—Specify as `${parameter-name}`.

Note the following when you customize a template file:

- Use UTF-8 encoding to code the template file.
- The size of the template file must not exceed 64 KB.
- The length of each line in the template file must not exceed 1,024 bytes, excluding the linefeed character.
- Specify only one header.

[Table 2-4:Template parameters \(task ended\)](#) and [Table 2-5:Template parameters \(time lapse\)](#) list the parameters that can be specified in a template.

Table 2-4: Template parameters (task ended)

Parameter	Description	Migration task ended	Shredding task ended	Locking task ended	Unlocking task ended	Volume creation task ended	External connection settings task ended
taskId	Task ID Example: TK1f21ymqv	Yes	Yes	Yes	Yes	Yes	Yes
taskType	Task type Example: Migration	Yes	Yes	Yes	Yes	Yes	Yes
taskStatus	Task status Example: Standby	Yes	Yes	Yes	Yes	Yes	Yes
taskOwner	The ID of the user who created the task. Example: user	Yes	Yes	Yes	Yes	Yes	Yes
executionRequestTime	Time that task execution was requested Example: 2007/03/25 17:00:00	Yes	Yes	Yes	Yes	Yes	Yes
endTime	Time that task execution ended Example: 2007/03/26 05:00:00	Yes	Yes	Yes	Yes	Yes	Yes
storageDomainName	Storage domain name Example: MegaTechUSP600-Primary	Yes	Yes	Yes	Yes	--	Yes
migrationGroupName	Migration group name Example: MG011	Yes	Yes	Yes	Yes	--	--
previousTargetStorageTierName	Name of the target storage tier in the previous migration Example: MegaTech-HighCost	Yes	--	--	--	--	--

Parameter	Description	Migration task ended	Shredding task ended	Locking task ended	Unlocking task ended	Volume creation task ended	External connection settings task ended
targetStorageTierName	Name of the target storage tier Example: MegaTech-HighCost	Yes	--	--	--	--	--
eraseData	Source data is to be deleted after migration Values: <ul style="list-style-type: none"> Yes No 	Yes	--	--	--	--	--
migratedVolumes	Device numbers of both migrated volumes and volumes whose data has been erased Example: 3:A6	Yes	--	--	--	--	--
shreddingMethod	Shredding method Values: <ul style="list-style-type: none"> ZERO-ONCE DoD 	--	Yes	--	--	--	--
shreddedVolumes	Device numbers of shredded volumes Example: 3:A6	--	Yes	--	--	--	--
guardMode	Lock mode Values: <ul style="list-style-type: none"> Readonly Protect 	--	--	Yes	--	--	--
retentionDays	Retention period (days) Example: 200	--	--	Yes	--	--	--
lockedVolumes	Device numbers of locked volumes Example: 3:A6	--	--	Yes	--	--	--

Parameter	Description	Migration task ended	Shredding task ended	Locking task ended	Unlocking task ended	Volume creation task ended	External connection settings task ended
unlockedVolumes	Device numbers of unlocked volumes Example: 3:A6	--	--	--	Yes	--	--
moveToMigrationGroupName	Name of the target migration group after task completion Example: MG011	--	Yes	Yes	Yes	--	--
mappedExternalSubsystemName	Name of the mapped external storage subsystem Example:USP_V@10.208.15.221	--	--	--	--	--	Yes
mappedExternalVolume	Volume ID of the mapped external volume Example:00:03:11	--	--	--	--	--	Yes
mappedVirtualArrayGroupName	Array group name of the mapped and created virtual array group Example:E200-9	--	--	--	--	--	Yes
mappedVirtualVolume	Device numbers of mapped internal virtual volumes Example:00:C1:01	--	--	--	--	--	Yes
subsystemName	Name of the operated storage subsystem Example:USP_V@10.208.15.221	--	--	--	--	Yes	--

Parameter	Description	Migration task ended	Shredding task ended	Locking task ended	Unlocking task ended	Volume creation task ended	External connection settings task ended
arrayGroupName	Name of the operated array group Example: 1-2-1	--	--	--	--	Yes	--
createdVolume	Volume ID of the created volume Example: 00:01:01	--	--	--	--	Yes	--
Legend Yes: Can be used --: Cannot be used Note: For details, see the <i>Hitachi Tiered Storage Manager CLI Reference Guide</i> .							

Table 2-5: Template parameters (time lapse)

Parameter	Description	Volume lock period expired	Specified time elapsed
storageDomainName	Storage domain name Example: MegaTechUSP600-Primary	Yes	Yes
migrationGroupName	Migration group name Example: MG011	Yes	Yes
expiredVolumes	Device numbers of expired volumes Example: 3:A6	Yes	--
remindAt	Scheduled time when an "elapsed time" event will occur Example: 2007/03/25 17:00:00	--	Yes
reminderDescription	Message that appears when an "elapsed time" event occurs Example: Data migration is scheduled to occur.	--	Yes
Legend Yes: Can be used --: Cannot be used Note: For details, see the <i>Hitachi Tiered Storage Manager CLI Reference Guide</i> .			

Specifying SMTP authentication user information

Tiered Storage Manager connects to the SMTP server in order to send event notification email. If SMTP authentication is required at this time, you must specify the SMTP authentication user information. Use the `htsmodmailuser` command to specify the information.

Changes made by using the `htsmmodmailuser` command take effect the next time Tiered Storage Manager server starts.

Execute the command after moving to the following folder or directory:

- In Windows
installation-folder-of-the-Tiered-Storage-Manager-server\bin
- In Solaris or Linux:
installation-directory-of-the-Tiered-Storage-Manager-server/bin

The following shows the syntax of the `htsmmodmailuser` command:

Syntax

```
htsmmodmailuser -u Tiered-Storage-Manager-user-ID -p Tiered-Storage-Manager-password SMTP-authentication-user-ID SMTP-authentication-password
```

Options

Tiered-Storage-Manager-user-ID

Specify a user ID that has the Admin permission of Tiered Storage Manager.

Tiered-Storage-Manager-password

Specify the logon password for the user ID used to log on to Tiered Storage Manager.

SMTP-authentication-user-ID

Specify a user ID for SMTP authentication.

SMTP-authentication-password

Specify a logon password for the user ID used to log on to the SMTP server. It is also possible to leave this setting unspecified.



Caution: If the following conditions apply, execute the `htsmmodmailuser` command from a shell such as `tcsh` or `bash` that supports commands that are longer than 256 bytes:

- You are executing the `htsmmodmailuser` command from an instance of Tiered Storage Manager running in Solaris or Linux
 - The command exceeds 256 bytes.
-

Registering a Web application

You can easily call frequently used Web applications if you use a command to register them beforehand. If the URL for starting the Web client or another Web application is modified, you can use a command to register the information again. This section describes the settings that must be specified for each application started from the Web client.

Using hcmdslink to register a Web application

When you choose **Go** and then **Links** in the global tasks bar area of the Web client, a dialog box is displayed with links that start applications for which the user is registered. By registering Web applications that you often use or information that you want to reference (such as a device installation chart) in this window, you will be able to easily call a desired application or item of reference information from the Web client.

To register a desired application or cancel the registration, use the `hcmdslink` command. This section describes how to use the `hcmdslink` command.

Format

In Windows:

```
installation-folder-of-Common-Component\bin\hcmdslink {/add|/delete} /file user-defined-application-file /user user-identifier /pass password
```

In Solaris or Linux:

```
installation-directory-of-Common-Component/bin/hcmdslink {-add|-delete} -file user-defined-application-file -user user-identifier -pass password
```

Function

The `hcmdslink` command registers a Web application to allow you to start the desired application from the Web client, or cancels the registration.

In the user-defined application file, specify a desired application name, URL, and display name. Then, use the `hcmdslink` command to register that information. A link to the registered application will be displayed in the link dialog box that appears when you choose **Go** and then **Links** in the global tasks bar area of the Web client.



Note: Once you register a link for starting an application, do not delete the user-defined application file used in this command. If you do, you will be unable to delete the link for the registered application.

Options

`add:`

Registers an application.

`delete:`

Deletes an application.

`file:`

Specifies the name of the user-defined application file. In Solaris or Linux, do not include spaces in the path.

`user:`

Specifies a user ID that is used to register or delete the user-defined application link. Specify the user ID of a user who has the Admin permission.

`pass:`

Specifies the password for the user ID used to register or delete the user-defined application link.

user-defined-application-file

[Table 2-6:Items to be specified in the application file](#) describes the items to be specified in the user-defined application file.



Caution: To code the user-defined application file, use ASCII code only. Also note that you cannot use a control code other than the CR and LF control codes.

Table 2-6: Items to be specified in the application file

Item	Description	Necessity
@TOOL-LINK	The start key. The information between the start key and the end key is the settings information.	Required
@NAME	Information used as the registration key. Specify a unique name. The maximum length of the name is 256 bytes. Use alphanumeric characters only.	Required
@URL	The target link of the URL from the Web client#. The maximum length is 256 bytes.	Optional
@DISPLAYNAME	The name displayed in the link dialog box that appears when you choose Go and then Links from the global tasks bar of the Web client. If no information is specified, the name specified in @NAME is displayed. You can specify a maximum of 80 Unicode characters. You cannot use characters that have a Unicode code point between U+10000 and U+10FFFF.	Optional
@DISPLAYORDER	The order in which links will be displayed in the link dialog box that appears when you choose Go and then Links from the global tasks bar area of the Web client. Applications in that list are displayed in ascending order based on this value. You can specify a value from -2,147,483,648 to 2,147,483,647.	Optional
@ICONURL	The URL of the icon displayed beside the link#. The maximum length is 256 bytes.	Optional
@TOOL-END	The end key.	Required
#	In IPv6 environments, use a host name to specify the URL.	

Return values

0: Normal termination

255: Failure

Command execution examples

When adding a link for an application:

```
hcmdslink /add /file C:\SampleLink.txt /user system /pass  
manager
```

When deleting a link for an application:

```
hcmdslink /delete /file C:\SampleLink.txt /user system /pass  
manager
```

Modifying the URL information

If any of the following configuration changes are made after you begin using Tiered Storage Manager, you must also change the URLs for accessing Hitachi Storage Command Suite products:

- A change to the IP address of the host in which the Tiered Storage Manager server is installed
- A change to the port used by the HBase Storage Mgmt Web Service
- A change to the settings of the Device Manager system, performed in order to use or stop using SSL
- A change from a non-cluster configuration to a cluster configuration

Use the `hcmdschgurl` command to change the URLs for accessing Hitachi Storage Command Suite products.

Format

In Windows:

```
installation-folder-for-Common-Component\bin\hcmdschgurl {/  
print | /list | /change old-URL new-URL | /change new-URL /type  
Hitachi-Storage-Command-Suite-product-name
```

In Solaris or Linux:

```
installation-directory-for-Common-Component/bin/hcmdschgurl {-  
print | -list | -change old-URL new-URL | -change new-URL -type  
Hitachi-Storage-Command-Suite-product-name
```

Options

print:

Displays a list of currently registered URLs and programs.

list:

Displays a list of the currently registered URLs and programs in a different format.

change:

Changes a currently registered URL.



- The specified URL must be a full URL that includes the protocol and the port number. In IPv6 environments, you must use a host name when specifying a URL. The following shows the possible URL formats:
`http://IP-address:port-number`
`http://host-name:port-number`
- When changing the URL during migration to a cluster environment, use the following format to specify *URL-after-change*:
`http://logical-host-name:port-number`

type:

Use this option to change the URL for a specific Hitachi Storage Command Suite product. Specifies the name of the Hitachi Storage Command Suite product URL to change. You must specify the `type` option together with the `change` option.

If you omit the `type` option, the URLs for all Hitachi Storage Command Suite products that are installed on the same management server will be changed. To change only the Tiered Storage Manager URL, specify `TieredStorageManager`. For details on the names of other Hitachi Storage Command Suite products, see the documentation for each product.

Return values

- 0: Normal
- 1: Argument error
- 2: URL or product specified as the target to be changed does not exist
- 253: Restoration failure
- 254: Backup failure
- 255: Abnormal termination

Command execution example

To change the URLs for accessing Hitachi Storage Command Suite products:

1. Make sure that the Common Component services are running.
 - In Windows:
Select **Start, All Programs, Hitachi Storage Command Suite, Device Manager**, and then **Server and Common Services Status**.
 - In Solaris or Linux:
Execute the following command:
`installation-directory-of-Common-Component/bin/hcmdssrv - status`
2. To find the URL information currently registered in the database, execute the command with the `list` option specified.
 - In Windows:
`C:\Program Files\HiCommand\Base\bin\hcmdschgurl /list`


```
http://192.168.11.33:23015
Hitachi Provisioning Manager
Hitachi Device Manager
Hitachi Tiered Storage Manager
```

- **In Solaris or Linux:**

```
# /opt/HiCommand/Base/bin/hcmdschgurl -list
http://192.168.11.33:23015
Hitachi Provisioning Manager
Hitachi Device Manager
Hitachi Tiered Storage Manager
```

3. To update the URL information, execute the command with the `change` option specified.

In the following example, the URL information `http://192.168.11.33:23015` is changed to `http://192.168.11.55:23015`.

- **In Windows:**

```
C:\Program Files\HiCommand\Base\bin\hcmdschgurl /change
"http://192.168.11.33:23015" "http://192.168.11.55:23015"
The URL was changed from "http://192.168.11.33:23015" to
"http://192.168.11.55:23015".
```

- **In Solaris or Linux:**

```
# /opt/HiCommand/Base/bin/hcmdschgurl -change
"http://192.168.11.33:23015" "http://192.168.11.55:23015"
The URL was changed from "http://192.168.11.33:23015" to
"http://192.168.11.55:23015".
```

4. To confirm the results, execute the command with the `list` option specified.

- **In Windows:**

```
C:\Program Files\HiCommand\Base\bin\hcmdschgurl /list
http://192.168.11.55:23015
Hitachi Provisioning Manager
Hitachi Device Manager
Hitachi Tiered Storage Manager
```

- **In Solaris or Linux:**

```
# /opt/HiCommand/Base/bin/hcmdschgurl -list
http://192.168.11.55:23015
Hitachi Provisioning Manager
Hitachi Device Manager
Hitachi Tiered Storage Manager
```

Security settings for user accounts

To prevent users' passwords from being guessed by a third party, Tiered Storage Manager allows you to specify password conditions. For example, you can specify a minimum number of characters and a required combination of character types. You can also have user accounts lock automatically if the wrong password is repeatedly entered for the same user ID.

If external authentication is used, password authentication and the number of unsuccessful logon attempts are managed by the external authentication server instead of Tiered Storage Manager. Therefore, password changes and automatic account locking cannot be performed in Tiered Storage Manager. A user can log in to a locked user account if its authentication location is switched to the external authentication server.

Security settings can also be specified from the Web client. However, if the system is in a cluster configuration, the settings from the Web client are only applied to the executing node. To apply the settings to the standby node, switch the nodes, and then specify the same settings. For details on how to use the Web client, see the *Hitachi Tiered Storage Manager User's Guide*.

When authenticating users by linking to an external authentication server, a combination of character types specified on the external authentication server are used to manage passwords and control user accounts, including automatic locking. However, when a new user password is registered in a Hitachi Storage Command Suite product, the password conditions that have been specified for the Hitachi Storage Command Suite product are used.



Caution: If a HiCommand product version 5.1 or later Hitachi Storage Command Suite product is installed, the user account log function and password complexity check functions are usable. These functions are enabled for users of all Hitachi Storage Command Suite products, so the following problems might occur in operations of HiCommand Suite products that are version 5.0 or earlier:

- A user is unable to log in even with a correct user ID and password.
The user account might be locked. Take appropriate action such as unlocking the relevant account or registering a new user account.
 - A password is unchangeable, or a user account is not addable.
The specified password might not follow the password-entry rules.
Specify an appropriate password as instructed by the output message.
-

The password conditions and settings related to account locking are implemented from the `security.conf` file. The `security.conf` file is stored in the following locations:

In Windows:

installation-folder-of-Common-Component\conf\sec

In a Solaris or Linux:

installation-directory-of-Common-Component/conf/sec

The password conditions that you set in the `security.conf` file are applied when a user account is created or when a password is changed, and are not applied to passwords of existing user accounts. As a result, even if an existing password does not satisfy the password conditions, a user can use the password to log in to the system.

When you change a setting in the `security.conf` file, the change takes effect immediately.

The items you can set in the `security.conf` file are described below.

password.min.length

Specifies the minimum number of characters that can be set as a password. Specify a value in the range from 1 to 256.

Default: 4

password.min.uppercase

Specifies the minimum number of uppercase letters the password must contain. Specify a value in the range from 0 to 256. If you specify 0, no restriction applies.

Default: 0 (no restriction)

password.min.lowercase

Specifies the minimum number of lowercase letters the password must contain. Specify a value in the range from 0 to 256. If you specify 0, no restriction applies.

Default: 0 (no restriction)

password.min.numeric

Specifies the minimum number of numeric characters the password must contain. Specify a value in the range from 0 to 256. If you specify 0, no restriction applies.

Default: 0 (no restriction)

password.min.symbol

Specifies the minimum number of symbols the password must contain. Specify a value in the range from 0 to 256. If you specify 0, no restriction applies.

Default: 0 (no restriction)

password.check.userID

Specifies whether the password must be different from the user ID. Specify `true` or `false`. If you specify `true`, passwords cannot be the same as the corresponding user ID. If you specify `false`, passwords can be the same as the corresponding user ID.

Default: `false` (passwords can be the same as user IDs)

account.lock.num

Specifies the number of unsuccessful login attempts to allow before a user account is automatically locked. Specify a value in the range from 0 to 10. If you specify 0, any number of unsuccessful login attempts is allowed.

Default: 0 (user accounts will not be locked)

Unsuccessful attempts to log in to other products in the Hitachi Storage Command Suite that use the Single Sign-On feature count towards the number of unsuccessful login attempts. For example, if the number of unsuccessful attempts is set to 3, and a user fails to log in to Device Manager once, fails to log in to Tiered Storage Manager once, and then fails to log in to Provisioning Manager once, his or her user account will be automatically locked.

If a user is currently logged in and you attempt to log in using his or her account, but you fail the specified number of times, his or her user account will be locked. However, the user can continue to use the account while he or she remains logged on.

You can unlock user accounts from the Web client if you have the User Management permission. For details about how to unlock user accounts, see [Unlocking user accounts](#).

Configuring system account locking

To make the `System` account subject to automatic or manual locking, specify the appropriate settings in the `account.lock.system` property of the `user.conf` file. The `user.conf` file can be found in the following location:

- In Windows:
installation-folder-of-Common-Component\conf
- In Solaris or Linux:
installation-directory-of-Common-Component/conf

If the `user.conf` file does not exist, create it.

Specify the `account.lock.system` property in the following format:

```
account.lock.system=value
```

For *value*, specify `true` or `false`. If you specify `true`, the `System` account will be subject to automatic and manual locking. If you specify `false`, the `System` account will not be subject to automatic or manual locking.

You need to restart Common Component for the value set in the `user.conf` file to take effect. For details on how to restart Common Component, see [Starting and stopping Common Component](#).



- If Hitachi Storage Command Suite product versions 6.1 or later are installed and `true` is set in the `user.conf` file, the `System` account will be subject to automatic and manual locking for all Hitachi Storage Command Suite products.
- For details on measures to take when all accounts with User Management permissions, including the `System` account, have been locked, see [Unlocking user accounts](#).

Unlocking user accounts

This section describes how to use the `hcmdsunlockaccount` command to unlock user accounts.

For a user without Admin (user management) permission:

Have a user with Admin (user management) permission unlock the account.

For a user with Admin (user management) permission:

Have another user with Admin (user management) permission unlock the account. Alternatively, execute the `hcmdsunlockaccount` command to unlock the account.

To unlock an account by using the `hcmdsunlockaccount` command:

1. Execute the following command to confirm that the Common Component services are running:

- In Windows:

```
installation-folder-of-Common-Component\bin\hcmdssrv /status
```

- In Solaris or Linux:

```
installation-directory-of-Common-Component/bin/hcmdssrv -  
status
```

If the Common Component service is not running, execute the following command:

- In Windows:

```
installation-folder-of-Common-Component\bin\hcmdssrv /start
```

- In Solaris or Linux:

```
installation-directory-of-Common-Component/bin/hcmdssrv -  
start
```

2. Execute the `hcmdsunlockaccount` command to unlock the account.

- In Windows:

```
installation-folder-of-Common-Component\bin\hcmdsunlockaccount /user user-ID /pass  
password
```

- In Solaris or Linux:

```
installation-directory-of-Common-Component/bin/  
hcmdsunlockaccount -user user-ID -pass password
```

For *user-ID*, specify the user ID of the user whose account you want to unlock. For *password*, specify the password of the user whose account you want to unlock.



Note: If certain symbols, defined below, are included in the user ID or password, you need to escape the symbols on the command line:

- In Windows
If the user ID or password ends with a backslash (\), use another backslash to escape it.
If the user ID or password includes an ampersand (&), vertical bar (|), or caret (^), enclose each symbol in double quotation marks ("), or use a caret (^) to escape the symbols.
- In Solaris or Linux:
Use a backslash (\) to escape the symbols defined above (\, &, |, and ^).
Note that if a password is not set for the target user, you cannot unlock the account by using the `hcmdsunlockaccount` command.

Configuring an optional warning banner message

In Hitachi Storage Command Suite products version 5.1 or later, an optional message (warning banner) can be displayed as a security measure at login. Issuing a warning beforehand to third parties that might attempt invalid access can help reduce the risk of problems such as data loss or information leakage.

The message that can be displayed on the Login panel must be no more than 1,000 characters. You can register messages in different languages for different regions, and the message can be automatically switched to match the locale of the accessing Web browser.

To set up the message, you must be logged on as a user who has Administrator permissions in Windows, or as the root user in Solaris or Linux.

Warning banner settings can also be specified from the Web client. However, if the system is in a cluster configuration, the settings from the Web client are only applied to the executing node. To apply the settings to the standby node, switch the nodes, and then specify the same settings again. For details on how to use the Web client, see the *Hitachi Tiered Storage Manager User's Guide*.

Editing the message

You edit the message in HTML format. No more than 1,000 characters can be used. In addition to the usual characters, you can use HTML tags to change font attributes or place line breaks in desired locations. The tag characters are also counted in the number of characters. Usable characters are in the Unicode UTF-8 encoding.

The following shows an example message:

```
<center><b>Warning Notice!</b></center>
This is a {Company Name Here} computer system, which may be
accessed and used only for authorized
{Company Name Here} business by authorized personnel. Unauthorized
access or use of this computer
system may subject violators to criminal, civil, and/or
administrative action. <br>
All information on this computer system may be intercepted,
recorded, read, copied, and disclosed
by and to authorized personnel for official purposes, including
criminal investigations.
Such information includes sensitive data encrypted to comply with
confidentiality and privacy
requirements. Access or use of this computer system by any person,
whether authorized or unauthorized,
constitutes consent to these terms. There is no right of privacy
in this system.
```



- When the message is registered, the HTML syntax is neither checked nor corrected. Edit the message correctly in accordance with HTML syntax rules because the edited message will be registered as is. If there is an error in the HTML syntax in the message, the message might not display correctly.
- There are no restrictions on the characters usable in the message, other than that the character encoding must be Unicode (UTF-8). To display a character used in HTML syntax (e.g., <, >, ", ', &), use the HTML escape sequence. For example, to display an ampersand (&) in the Login panel, write in the HTML file.
- To use line breaks to display the message in a desired location, use the HTML tag
. Even if there are linefeed characters in the message, they will be ignored when the message is registered.



Note: Sample messages in English (bannermsg.txt) and Japanese (bannermsg_ja.txt) are provided in the following locations:

- In Windows:
installation-folder-of-Common-Component\sample\resource
- In Solaris or Linux:
installation-directory-of-Common-Component/sample/resource

These sample files are initialized at installation. Back them up if you might need to access them later.

Registering the message

You use the `hcmdsbanner` command to register an edited message. Execute the command as follows:

- In Windows:
installation-folder-of-Common-Component\bin\hcmdsbanner /add /file *file-name* [/locale *locale-name*]

The following shows an example of executing the command:

```
C:\Program Files\HiCommand\Base\bin\hcmdsbanner /add /file
C:\W_Banner\wbfile1 /locale en
```

- In Solaris or Linux:

installation-directory-of-Common-Component/bin/hcmdsbanner -add
-file *file-name* [-locale *locale-name*]

The following shows an example of executing the command:

```
# /opt/HiCommand/Base/bin/hcmdsbanner -add -file /opt/  
W_Banner/wbfile1 -locale en
```

file-name

Using an absolute path, specify the file that stores the message. In Solaris or Linux, do not include spaces in the path.

locale-name

Specify the locale of the language used for the message (e.g., *en* for English, or *ja* for Japanese). If omitted, the default locale will be specified.

If the Web client will be used in multiple locales, you can register a message with the same contents in a different language for each locale and the message can be automatically switched to match the locale of the Web browser.

The locale for the warning banner displayed in the Web client is set in accordance with the language priority settings of the Web browser that is accessing it.

If the *locale* option is omitted, you can still edit the registered contents from the Web client. However, available HTML tags are limited when you edit from the Web client.

Return values

0: Normal termination

253: The number of characters in the message exceeds 1,000 characters.

255: Failure



Caution: If a message for the specified locale is already registered, it will be overwritten if a new message is registered.

Deleting the message

You use the *hcmdsbanner* command to delete a registered message. Execute the command as follows:

- In Windows:

installation-folder-of-Common-Component\bin\hcmdsbanner /delete
/file *file-name* [/locale *locale-name*]

The following shows an example of executing the command:

```
C:\Program Files\HiCommand\Base\bin\hcmdsbanner /delete /locale  
en
```

- In Solaris or Linux:

installation-directory-of-Common-Component/bin/hcmdsbanner -
delete -file *file-name* [-locale *locale-name*]

The following shows an example of executing the command:


```
# /opt/HiCommand/Base/bin/hcmdsbanner -delete -file /opt/W_Banner/wbfile1 -locale en
```

locale-name

Specify the locale of the message to be deleted (e.g., `en` for English, or `ja` for Japanese). If omitted, the default locale will be specified.

Return values

0: Normal termination

254: A message of the specified locale has not been registered.

255: Failure

Linking with Tuning Manager

By linking with Tuning Manager, Tiered Storage Manager allows you to acquire storage subsystem performance information.

Launching the historical report dialog box

From the Web client, you can launch the historical report dialog box for performance information related to LDEVs or array groups.

The following describes the prerequisites for launching the historical report dialog box:

- The Tuning Manager server has been set up.

For details about the prerequisite versions of the Tuning Manager server, see [Related software](#).

For details about the system requirements and how to set up the Tuning Manager server, see the *Hitachi Tuning Manager Installation Guide* and the *Hitachi Tuning Manager Server Administration Guide*.

If the Tuning Manager server is installed on a different machine from the one on which the Device Manager and Tiered Storage Manager servers are installed, you must set up the environment so that the Device Manager server can remotely connect to the Tuning Manager server.

For details about the settings, see the *Hitachi Tuning Manager Installation Guide* and the *Hitachi Device Manager Server Configuration and Operation Guide*.

- Tuning Manager - Agent for RAID has been set up.

For details about the prerequisite versions of Tuning Manager -Agent for RAID, see [Related software](#).

For details about system requirements and how to set up Tuning Manager - Agent for RAID, see the *Hitachi Tuning Manager Installation Guide*.

- The user has Tuning Manager View permissions.

In addition to Tiered Storage Manager user permissions, the user must also have Tuning Manager user permissions.

For details on how to grant Tuning Manager user permissions, see the *Hitachi Tuning Manager Server Administration Guide*.



Caution: If you install Tuning Manager server on a computer different from the one on which Device Manager server and Tiered Storage Manager server are installed, be sure to match the following settings on both computers:

- Time
If the times on the two computers differ by 5 minutes or more, an error will occur whenever you launch the historical report dialog box.
- Time zone
If the time zones on the two computers are different, historical reports will use the display settings on the computer where Tuning Manager server is installed.

Displaying array group usage

By linking to Tuning Manager, Tiered Storage Manager allows you to check the array group usage on the Web client or the CLI client.

The following describes the prerequisites for displaying the array group usage.

- The Tuning Manager server has been set up.
For details about the prerequisite versions of the Tuning Manager server, see [Related software](#).
For details about the system requirements and how to set up the Tuning Manager server, see the *Hitachi Tuning Manager Installation Guide* and the *Hitachi Tuning Manager Server Administration Guide*.
- Tuning Manager - Agent for RAID has been set up.
For details about the prerequisite versions of Tuning Manager -Agent for RAID, see [Related software](#).
For details about the system requirements and how to set up Tuning Manager - Agent for RAID, see the *Hitachi Tuning Manager Installation Guide*.
- Environment settings have been configured on the Tiered Storage Manager server

To configure environment settings required for the Tiered Storage Manager server:

1. Stop the Tiered Storage Manager server.

In Windows:

Choose **Start, All Programs, Hitachi Storage Command Suite, Tiered Storage Manager**, and then select **Stop Tiered Storage Manager**.

In Solaris or Linux:

Execute the following commands:

```
installation-directory-of-the-Tiered-Storage-Manager-server/bin/  
htsmserver stop
```

Example of command execution:

```
# /opt/HiCommand/TieredStorageManager/bin/htsmsserver stop
```

2. Edit the `tuningmanager.properties` file and set up the environment.

For details on the environment settings, see [htnm.infoAcquirePeriod](#) to [htnm.server.n.port](#).

3. Start the Tiered Storage Manager server.

In Windows:

Choose **Start, All Programs, Hitachi Storage Command Suite, Tiered Storage Manager**, and then select **Start Tiered Storage Manager**.

In Solaris or Linux:

Execute the following commands:

```
installation-directory-of-the-Tiered-Storage-Manager-server/bin/  
htsmsserver start
```

Example of command execution:

```
# /opt/HiCommand/TieredStorageManager/bin/htsmsserver  
start
```

4. Refresh the domain from Tiered Storage Manager.

When a storage domain is refreshed, Tiered Storage Manager acquires performance information that has been collected and summarized by Tuning Manager.

Starting HSSM from the Dashboard

To start HSSM from the **Dashboard** menu, create the `StorageServicesManager.conf` file in the following location if it has not already been created:

In Windows:

```
installation-folder-of-Common-Component\common
```

In Solaris or Linux:

```
installation-directory-of-Common-Component/common
```

In the `StorageServicesManager.conf` file, specify the `LaunchURL` parameter as follows:

In the `StorageServicesManager.conf` file:

```
LaunchURL=HSSM-URL
```

In *HSSM-URL*, specify the URL used to start HSSM. For details about this URL, see the HSSM documentation.

For example, if the name of the HSSM management server is *machine-name*, configure the `StorageServicesManager.conf` as follows:

For secure connections:

```
LaunchURL=https://machine-name
```

For nonsecure connections:

LaunchURL=http://*machine-name*

Settings required when disconnecting the management server from the network

To change the settings or perform maintenance, you might have to disconnect the management server from the network. Before disconnecting from the network, first change the Common Component settings files.

If you disconnect the management server from the network without changing the settings files, you will not be able to perform operations on Tiered Storage Manager because the Device Manager server will stop running. To return to a state where you can perform operations on Tiered Storage Manager, you need to restart the computer on which Device Manager is installed.

The procedure to change the settings file is described in steps 1 through 7 below. After you perform these steps once, you no longer have to do so when disconnecting the network.

To change a settings file:

1. If Hitachi Storage Command Suite products with version numbers earlier than 05-70 are running, stop their services.

For details about how to stop these services, see the manual for your product version.

2. Stop the services of Hitachi Storage Command Suite products and Common Component.

- In Windows:

Select **Start, All Programs, Hitachi Storage Command Suite, Device Manager**, and then **Stop Server with Common Services**.

- In Solaris or Linux:

installation-directory-of-Common-Component/bin/hcmdssrv

Example of command execution:

```
# /opt/HiCommand/Base/bin/hcmdssrv -stop
```

3. Edit the `pdsys` file and the `def_pdsys` file.

Change the value of the `pdunit` parameter's `-x` option to the loopback address `127.0.0.1`.

The default installation locations of the `pdsys` file and `def_pdsys` file are as follows:

- In Windows:

installation-folder-of-Common-Component\HDB\CONF\pdsys

installation-folder-of-Common-Component\database\work\def_pdsys

- In Solaris or Linux:

installation-directory-of-Common-Component/HDB/conf/pdsys

installation-directory-of-Common-Component/database/work/
def_pdsys

Example:

/opt/HiCommand/Base/HDB/conf/pdsys

/opt/HiCommand/Base/database/work/def_pdsys

4. Edit the `pdutysys` file and the `def_pdutysys` file.

Change the value of the `pd_hostname` parameter to the loopback address 127.0.0.1.

If the `pd_hostname` parameter does not exist, add the `pd_hostname` parameter to set a loopback address.

The default installation locations of the `pdutysys` file and `def_pdutysys` file are as follows:

- In Windows:

installation-folder-of-Common-Component\HDB\CONF\pdutysys

installation-folder-of-Common-Component\database\work\def_pdutysys

- In Solaris or Linux:

installation-directory-of-Common-Component/HDB/conf/pdutysys

installation-directory-of-Common-Component/database/work/
def_pdutysys

Example:

/opt/HiCommand/Base/HDB/conf/pdutysys

/opt/HiCommand/Base/database/work/def_pdutysys

5. Edit the `HiRDB.ini` file.

Change the value of the `PDHOST` parameter to the loopback address 127.0.0.1.

The default installation locations of the `HiRDB.ini` file are as follows:

- In Windows:

installation-folder-of-Common-Component\HDB\CONF\emb\HiRDB.ini

- In Solaris or Linux:

installation-directory-of-Common-Component/HDB/conf/emb/
HiRDB.ini

Example:

/opt/HiCommand/Base/HDB/conf/emb/HiRDB.ini

6. Restart the computer.

7. Execute the following command to make sure that the Common Component service is running:

Open the command prompt or terminal window, specify the `statusall` option, and then execute the `hcmdssrv` command.

- In Windows:

installation-folder-of-Common-Component\bin\hcmdssrv /
statusall

Example of command execution:

```
C:\> cd C:\Program Files\HiCommand\Base\bin  
C:\Program Files\HiCommand\Base\bin> hcmdssrv /statusall
```

- In Solaris or Linux:

installation-directory-of-Common-Component/bin/hcmdssrv

Example of command execution:

```
# /opt/HiCommand/Base/bin/hcmdssrv -statusall
```

8. Disconnect the network, and then change the settings or perform maintenance.
9. After the network becomes available, start the service of the Device Manager server, the services of other Hitachi Storage Command Suite products, and Common Component.
 - In Windows:
Select **Start, All Programs, Hitachi Storage Command Suite, Device Manager**, and then **Start Server with Common Services**.
 - In Solaris or Linux:
installation-directory-of-Common-Component/bin/hcmdssrv
Example of command execution:

```
# /opt/HiCommand/Base/bin/hcmdssrv -start
```
10. If Hitachi Storage Command Suite products have been installed, start their services as required.
For details about how to start these services, see the documentation for the relevant products.

Server operation information

This chapter describes how to start and stop the Tiered Storage Manager server, how to start and stop Common Component, and the migration, backup, and restoration of repositories.

- ❑ [Starting and stopping the server](#)
- ❑ [Starting and stopping Common Component](#)
- ❑ [Resident processes](#)
- ❑ [Moving repositories](#)
- ❑ [Backing up repositories](#)
- ❑ [Restoring repositories](#)

Starting and stopping the server

When starting the Tiered Storage Manager server, make sure that the Device Manager server is running. If the Device Manager server is not running, the Tiered Storage Manager server will not run.

Starting the Tiered Storage Manager server

Starting the Tiered Storage Manager server in a non-cluster configuration

The methods for starting the Tiered Storage Manager server when operating it in a non-cluster configuration are described below.

In Windows:

You can use the following methods to start the Tiered Storage Manager server:

- Starting the Tiered Storage Manager server from the Start menu
Choose **Start, All Programs, Hitachi Storage Command Suite, Tiered Storage Manager**, and then **Start Tiered Storage Manager**.

- Starting the Tiered Storage Manager server from the command prompt

Open the command prompt, and then execute the `htsmsserver` command with the `start` option specified.

installation-folder-of-the-Tiered-Storage-Manager-server\bin\htsmsserver

Example of command execution:

```
C:\> cd C:\Program  
Files\HiCommand\TieredStorageManager\bin  
  
C:\Program Files\HiCommand\TieredStorageManager\bin>  
htsmsserver start
```

- Setting the Tiered Storage Manager server to automatically be started when the OS is started

By default, the Tiered Storage Manager server is started automatically when the OS is started.

If you do not want the Tiered Storage Manager server to start automatically, choose **Start, Control Panel, Administrative Tools**, and then **Services**. Right-click **HiCommand Tiered Storage Manager**, and then choose **Properties**. In the dialog that appears, change **Startup Type** from **Automatic** to **Manual**.

In Solaris or Linux:

Open a terminal window, and then execute the `htsmsserver` command with the `start` option specified.

*installation-directory-of-the-Tiered-Storage-Manager-server/bin/
htsmsserver*

Example of command execution:


```
# /opt/HiCommand/TieredStorageManager/bin/htsmserver start
```

When the Tiered Storage Manager server is started, the message `KATS41001-I Tiered Storage Manager has started.` is output to the Tiered Storage Manager server message log.

Starting the Tiered Storage Manager server in a cluster configuration

The methods for starting the Tiered Storage Manager server when operating it in a cluster configuration are described below. You must use the executing node to start the Tiered Storage Manager server.

- For Microsoft Cluster Service

Using Cluster Administrator, right-click the following resource from the group in which the Hitachi Storage Command Suite product services have been registered, and select **Bring Online**:

- HiCommand Tiered Storage Manager

This service will be displayed by the resource name specified when the service was registered as a resource.

- For Microsoft Failover Cluster

Using Failover Cluster Management, right-click the following resource from the group in which the Hitachi Storage Command Suite product services have been registered, and select **Bring this service or application online**:

- HiCommand Tiered Storage Manager

This service will be displayed by the resource name specified when the service was registered as a resource.

- For Veritas Cluster Server

Execute the following command:

```
# hares -online cluster-resource-name-for-the-Tiered-Storage-Manager-server -sys localhost
```

- For Sun Cluster

Execute the following command:

```
# scswitch -Z -g cluster-resource-name-for-the-Tiered-Storage-Manager-server
```

When the Tiered Storage Manager server is started, the message `KATS41001-I Tiered Storage Manager has started.` is output to the Tiered Storage Manager server message log.

Stopping the Tiered Storage Manager server

When stopping Hitachi Storage Command Suite product running on the same management server, the Device Manager server must be stopped last. Do not stop the Device Manager server before the Tiered Storage Manager server.

Stopping the Tiered Storage Manager server in a non-cluster configuration

The Tiered Storage Manager server is stopped automatically when the OS is shut down. Use the following methods to stop the Tiered Storage Manager server manually:

Normal Stop

In Windows:

You can use the following methods to stop the Tiered Storage Manager server.

- Stopping the Tiered Storage Manager server from the Start menu
Choose **Start, All Programs, Hitachi Storage Command Suite, Tiered Storage Manager**, and then **Stop Tiered Storage Manager**.
- Stopping the Tiered Storage Manager server from the command prompt

Open the command prompt, and then execute the `htsmserver` command with the `stop` option specified.

installation-folder-of-the-Tiered-Storage-Manager-server\bin\htsmserver

Example of command execution:

```
C:\> cd C:\Program
Files\HiCommand\TieredStorageManager\bin

C:\Program Files\HiCommand\TieredStorageManager\bin>
htsmserver stop
```

In Solaris or Linux:

Open a terminal window, and then execute the `htsmserver` command with the `stop` option specified.

installation-directory-of-the-Tiered-Storage-Manager-server/bin/htsmserver

Example of command execution:

```
# /opt/HiCommand/TieredStorageManager/bin/htsmserver stop
```

When the Tiered Storage Manager server is stopped, the message `KATS41003-I Tiered Storage Manager has stopped.` is output to the Tiered Storage Manager server message log.

Forced Stop

In Windows:

Open the command prompt, and then execute the `htsmserver` command with the `forcestop` option specified.

installation-folder-of-the-Tiered-Storage-Manager-server\bin\htsmserver

Example of command execution:

```
C:\> cd C:\Program Files\HiCommand\TieredStorageManager\bin
C:\Program Files\HiCommand\TieredStorageManager\bin>
htsmserver forcestop
```

In Solaris or Linux:

Open a terminal window, and then execute the `htsmserver` command with the `forcestop` option specified.

```
installation-directory-of-the-Tiered-Storage-Manager-server/bin/
htsmserver
```

Example of command execution:

```
# /opt/HiCommand/TieredStorageManager/bin/htsmserver
forcestop
```



Caution: Even if a forced stop is executed to stop Tiered Storage Manager, tasks that have already been started on the storage subsystem will continue processing. Migration and shredding operations that are being executed on the storage subsystem cannot be cancelled. If a forced stop has been executed, when you next restart the Tiered Storage Manager server, check whether the results of the commands that were executed before the forced stop are still applied, and the tasks that were registered before the forced stop are still registered.



Caution: When a normal stop is executed, the Tiered Storage Manager server might not stop immediately. The Tiered Storage Manager service will not stop immediately in the following situations:

- When processing from the Web client or the CLI client is being executed, the Tiered Storage Manager server will not stop until a process completion message has been sent to the client.
- When tasks are being executed or standing by, processing to stop Tiered Storage Manager begins after execution of the tasks has finished, or approximately 10 minutes have passed since Tiered Storage Manager received the command to stop, in which case a forced stop will be executed even if not all tasks are complete.

When the Tiered Storage Manager server is stopped, the message `KATS41003-I Tiered Storage Manager has stopped` is output to the Tiered Storage Manager server message log.

Stopping the Tiered Storage Manager server in a cluster configuration

The methods for stopping the Tiered Storage Manager server when operating it in a cluster configuration are described below. You must use the executing node to stop the Tiered Storage Manager server.

- For Microsoft Cluster Service

Using Cluster Administrator, right-click the following resource from the group in which the Hitachi Storage Command Suite product services have been registered, and select **Take Offline**:

- HiCommand Tiered Storage Manager

This service will be displayed by the resource name specified when the service was registered as a resource.

- For Microsoft Failover Cluster

Using Failover Cluster Management, right-click the following resource from the group in which the Hitachi Storage Command Suite product services have been registered, and select **Take this service or application offline**:

- HiCommand Tiered Storage Manager

This service will be displayed by the resource name specified when the service was registered as a resource.

- For Veritas Cluster Server

Execute the following command:

```
# hares -online cluster-resource-name-for-the-Tiered-Storage-Manager-server -sys localhost
```

- For Sun Cluster

Execute the following command:

```
# scswitch -Z -g cluster-resource-name-for-the-Tiered-Storage-Manager-server
```

When the Tiered Storage Manager server is stopped, the message KATS41003-I Tiered Storage Manager has stopped. Is output to the Tiered Storage Manager server message log.

Checking server status

Use the following methods to check the status of the Tiered Storage Manager server:

In Windows:

You can use the following methods to check the status the Tiered Storage Manager server.

- Checking the status of the Tiered Storage Manager server from the Start menu:

Choose **Start, All Programs, Hitachi Storage Command Suite, Tiered Storage Manager**, and then **Tiered Storage Manager Status**. A message regarding the status of the Tiered Storage Manager server will appear.

- Checking the status of the Tiered Storage Manager server from the command prompt:

Open the command prompt, and then execute the `htsmserver` command with the `status` or `status2` option specified.

installation-folder-of-the-Tiered-Storage-Manager-server\bin\htsmserver

Example of command execution:

```
C:\> cd C:\Program
Files\HiCommand\TieredStorageManager\bin
C:\Program Files\HiCommand\TieredStorageManager\bin>
htsmserver status2
```

If you specified the `status` option, a message is displayed indicating the status of the Tiered Storage Manager server.

If you specified the `status2` option, determine the status from the following return values:

0: The Tiered Storage Manager server is running.

1: The Tiered Storage Manager server is stopped.

2: The Tiered Storage Manager server is starting up.

255: The command ended abnormally.

In Solaris or Linux:

Open a terminal window, and then execute the `htsmserver` command with the `status` or `status2` option specified.

installation-directory-of-the-Tiered-Storage-Manager-server/bin/
`htsmserver`

Example of command execution:

```
# /opt/HiCommand/TieredStorageManager/bin/htsmserver status  
or
```

```
# /opt/HiCommand/TieredStorageManager/bin/htsmserver status2
```

If you specified the `status` option, a message is displayed indicating the status of the Tiered Storage Manager server. If you specified the `status2` option, determine the status from the following return values:

0: The Tiered Storage Manager server is running.

1: The Tiered Storage Manager server is stopped.

2: The Tiered Storage Manager server is starting up.

255: The command ended abnormally.

Starting and stopping Common Component

This section describes the procedure to start or stop Common Component. Ordinarily, you do not need to manually start Common Component.

Starting Common Component

To start Common Component, start the following services:

- HBase Storage Mgmt Web Service
- HBase Storage Mgmt Common Service
- HiRDB

When Common Component starts, the Device Manager server and Tiered Storage Manager server should also start. Make sure that the Device Manager server and Tiered Storage Manager server have started.

For details on how to check the status of the Device Manager server, see the *Hitachi Device Manager Server Configuration and Operation Guide*.

For details on how to check the status of the Tiered Storage Manager server, see [Checking server status](#).

If the services of Common Component are running but the services of the Device Manager server or the Tiered Storage Manager server are not running, executing the `hcmdssrv` command will not cause the services of the Device Manager server or the Tiered Storage Manager server to start.

Instead, check the statuses of the Device Manager server and the Tiered Storage Manager server, and then start the services if necessary. For details on how to start the services of the Device Manager server, see the *Hitachi Device Manager Server Configuration and Operation Guide*.

For details on how to start the services of the Tiered Storage Manager server, see [Starting the Tiered Storage Manager server](#).

Starting Common Component in a Windows environment

To start Common Component when the management server OS is Windows:

1. Log in to the system as a user with Administrator privileges.
2. From the command prompt, execute the following command:

installation-folder-of-Common-Component\bin\hcmdssrv

Example of command execution:

```
C:\Program Files\HiCommand\Base\bin\hcmdssrv /start
```

3. Execute the following command to check whether the Common Component services have started:

installation-folder-of-Common-Component\bin\hcmdssrv

Example of command execution:

```
C:\Program Files\HiCommand\Base\bin\hcmdssrv /statusall
```

If the following messages appear, the services are running:

```
KAPM06440-I The HiRDB service has already started.  
KAPM05007-I Already started service. Service-name=Hbase Storage  
Mgmt Web Service  
KAPM05007-I Already started service. Service-name=Hbase Storage  
Mgmt Common Service
```

If a message other than the above messages appears, take appropriate action according to the message.

Starting Common Component in a Solaris or Linux environment

To start Common Component when the management server OS is Solaris or Linux:

1. Log in to the system as root.
2. Open a terminal window, and then execute the following command:

installation-directory-of-Common-Component/bin/hcmdssrv

Example of command execution:

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

3. Execute the following command to check whether the Common Component services have started:

installation-directory-of-Common-Component/bin/hcmdssrv

Example of command execution:

```
# /opt/HiCommand/Base/bin/hcmdssrv -statusall
```

If the following messages appear, the services are running:

```
KAPM06440-I The HiRDB service has already started.  
KAPM05007-I Already started service. Service-name=Hbase Storage  
Mgmt Web Service  
KAPM05007-I Already started service. Service-name=Hbase Storage  
Mgmt Common Service
```

If a message other than the above messages appears, take appropriate action according to the message.

Stopping Common Component

To stop Common Component, stop the following services:

- HBase Storage Mgmt Web Service
- HBase Storage Mgmt Common Service
- HiRDB

When Common Component stops, the Device Manager server and Tiered Storage Manager server should automatically also stop. Any time you have stopped Common Component, make sure that the Device Manager server and Tiered Storage Manager server have also stopped.

For details on how to check the status of the Device Manager server, see the *Hitachi Device Manager Server Configuration and Operation Guide*.

For details on how to check the status of the Tiered Storage Manager server, see [Checking server status](#).

If the services of Common Component are not running but the services of the Device Manager server or the Tiered Storage Manager server are running, executing the `hcmdssrv` command will not cause the services of the Device Manager server or the Tiered Storage Manager server to stop.

Instead, check the statuses of the Device Manager server and the Tiered Storage Manager server, and then stop the services if necessary. For details on how to stop the services of the Device Manager server, see the *Hitachi Device Manager Server Configuration and Operation Guide*.

Stopping Common Component in a Windows environment

To stop Common Component when the management server OS is Windows:

1. Log in to the system as a user with Administrator privileges.
2. From the command prompt, execute the following command:

```
installation-folder-of-Common-Component\bin\hcmdssrv
```

Example of command execution:

```
C:\Program Files\HiCommand\Base\bin\hcmdssrv /stop
```

3. Execute the following command to check whether the Common Component services have stopped:

```
installation-folder-of-Common-Component\bin\hcmdssrv
```

Example of command execution:

```
C:\Program Files\HiCommand\Base\bin\hcmdssrv /statusall
```

If the following messages appear, the services have stopped:

```
KAPM06441-I The HiRDB service has already stopped.  
KAPM05009-I Already stopped service. Service-name=Hbase Storage  
Mgmt Web Service  
KAPM05009-I Already stopped service. Service-name=Hbase Storage  
Mgmt Common Service
```

If a message other than the above messages appears, take appropriate action according to the message.



Caution: In an environment in which a version of Replication Monitor 5.6 or earlier is installed, services cannot be stopped by using only the `hcmdssrv /stop` command. Execute the Device Manager `suitesrvctl /stop_hdvm` command before executing the `hcmdssrv /stop` command.

Stopping Common Component in a Solaris or Linux environment

To stop Common Component when the management server OS is Solaris or Linux:

1. Log in to the system as root.
2. Open a terminal window, and then execute the following command:

```
installation-directory-of-Common-Component/bin/hcmdssrv
```

Example of command execution:

```
# /opt/HiCommand/Base/bin/hcmdssrv -stop
```

3. Execute the following command to check whether the Common Component services have stopped:

```
installation-directory-of-Common-Component/bin/hcmdssrv
```

Example of command execution:

```
# /opt/HiCommand/Base/bin/hcmdssrv -statusall
```

If the following messages appear, the services have stopped:

```
KAPM06441-I The HiRDB service has already stopped.  
KAPM05009-I Already stopped service. Service-name=HBase Storage  
Mgmt Web Service  
KAPM05009-I Already stopped service. Service-name=HBase Storage  
Mgmt Common Service
```


If a message other than the above messages appears, take appropriate action according to the message.



- In an environment in which version 5.6 or earlier of Replication Monitor is installed, services cannot be stopped by using only the `hcmdssrv -stop` command. It is necessary to execute the Device Manager `suitesrvctl -stop_hdvm` command before executing the `hcmdssrv -stop` command.
- When you stop Common Component in a Solaris or Linux environment, make sure Common Component has completed startup before you execute the `hcmdssrv -stop` command. If you execute this command before startup is complete, then even if there are actually resident processes still running, the `statusall` option might report some Common Component services as `not running`, in which case you will be unable to use the `stop` option to stop those services. If a computer enters this state, you will need to restart it.

Resident processes

The following sections show the resident processes of Tiered Storage Manager and Common Component.

In Windows

[Table 3-1:Resident processes of Tiered Storage Manager and Common Component \(Windows\)](#) lists and describes the resident processes on a Windows system.

Table 3-1: Resident processes of Tiered Storage Manager and Common Component (Windows)

Process	Function
<code>htsmService.exe</code>	Tiered Storage Manager service process
<code>hntr2mon.exe</code>	Hitachi Storage Command Suite common trace information collection process
<code>hntr2srv.exe</code>	Hitachi Storage Command Suite common trace service process
<code>httpsd.exe</code>	Hitachi Storage Command Suite common Web service
<code>hcmdssvctl.exe</code>	Hitachi Storage Command Suite servlet service

In Solaris or Linux

[Table 3-2:Resident processes of Tiered Storage Manager and Common Component \(Solaris or Linux\)](#) lists and describes the resident processes in a Solaris or Linux system.

Table 3-2: Resident processes of Tiered Storage Manager and Common Component (Solaris or Linux)

Process	Function
htsmService.exe	Tiered Storage Manager service process
hntr2mon.exe	Hitachi Storage Command Suite common trace information collection process
httpsd	Hitachi Storage Command Suite common Web service

Moving repositories

Hitachi Storage Command Suite products have repositories for saving information specific to that product. Repositories are different for each Hitachi Storage Command Suite product. In addition to the repositories for each product, there is also a repository for saving user information.

- Tiered Storage Manager repository
This repository manages information defined for migration, as well as the status of the Tiered Storage Manager server.
- Device Manager repository
This repository manages system and hardware information about storage subsystems managed by Device Manager.
- Common Component repository
This repository is used by several Hitachi Storage Command Suite products to manage user information.

When changing the computer on which Hitachi Storage Command Suite products are installed, it is necessary to move these repositories from the old computer to the new computer. The `hcmdsdbtrans` command is used to move repositories. As shown below, repositories can be moved to computers that operate in different environments than the environment of the server computer currently being used.

- You can move repositories to a computer with a different OS
- You can move repositories to a computer with a different Hitachi Storage Command Suite product installation location
- You can move repositories to a computer with Hitachi Storage Command Suite products whose version is later than those installed on the migration source computer

The general procedure for moving repositories is as follows:

1. Use the `hcmdsdbtrans` command at the migration source server to export the repository and create an archive file.
2. Copy the repository archive file created with the `hcmdsdbtrans` command to the migration target server.
3. Use the `hcmdsdbtrans` command at the migration target server to import the repository.

Before starting to move repositories, see [Special precautions when moving repositories](#).

For details on how to move repositories in Windows, see [Moving repositories \(Windows\)](#). For details on how to move repositories in Solaris or Linux, see [Moving repositories \(Solaris or Linux\)](#).

Special precautions when moving repositories

When moving repositories, pay careful attention to the following:

Hitachi Storage Command Suite product type and version

- Install the required Hitachi Storage Command Suite products on the migration target.
Repositories for Hitachi Storage Command Suite products that have not been installed on the migration target cannot be moved.
- You must install the same versions (or later) of Hitachi Storage Command Suite products on the migration target server as those on the migration source.
Even if only one of the Hitachi Storage Command Suite products installed on the migration target is an earlier version of a product on the migration source, you will be unable to move the repositories.
- If you want to move the Tuning Manager repository, you must check whether the repository is in a movable state. For details, refer to the section that describes database management in the Tuning Manager manual.
- If the version of Tuning Manager is earlier than 6.0 and the total number of resources managed by the Tuning Manager server is more than 70% of the manageable limit, the Tuning Manager repository cannot be migrated into a repository configuration identical to the one in which it exists.
- If you want to migrate the Replication Monitor repository to the Replication Manager repository, first upgrade Replication Monitor on the source server to Replication Manager, and then migrate the repositories.

User information

When moving repositories, the repositories storing user information on the migration target computer will be overwritten by the repositories storing user information on the migration source computer. To avoid problems, pay careful attention to the following points:

- If you do not want to change the user information on the migration target computer, you must not move the repositories.
- Since user information is overwritten, Hitachi Storage Command Suite products running on multiple servers cannot be moved to a single management server.

Folder capacity

When repositories are exported, repository information is stored in one folder, and repository archive files are stored in another folder. For each folder, you must secure an amount of capacity based on which programs'

repositories you are moving. For example, if only Device Manager and Tiered Storage Manager are installed, you must secure capacity equal to the total size of the following:

- Storage folder for the repositories of Device Manager
- Storage folder for the repositories of Tiered Storage Manager
- Storage folder for the repositories of Common Component, excluding folders under the `sys` folder

Remember that this is only the target capacity for when the repositories of Device Manager and Tiered Storage Manager are installed. If other Hitachi Storage Command Suite products are installed, you must also consider the capacity required for their repositories.

Repository capacity

If the capacity of all repositories exceeds 2 GB, when exporting the repositories, creation of archive files will fail. If the creation of archive files fails, then in place of the archive files, copy to the migration target server the repository information that is collected during exporting.

Moving repositories (Windows)

This section explains the procedures for moving repositories in Windows.

Exporting repositories on the migration source server



Caution: If the Tuning Manager server is installed on a different computer than the Device Manager server, you need to stop the Tuning Manager services on that computer. After exporting repositories, restart the Tuning Manager services. For details on how to start and stop the Tuning Manager services, see the manual for the installed version of Tuning Manager.

To export repositories when the migration source server OS is Windows:

1. Log on to the management server as a user with Administrator permissions.
2. From the command prompt, specify the options below and execute the `hcmdsdbtrans` command.

Collect the repository information and create archive files for the repositories.

```
installation-folder-of-Common-Component\bin\hcmdsdbtrans /  
export /workpath work-folder /file archive-file /auto  
/workpath
```

Use an absolute path to specify a folder for storing the collected repository information. Specify an empty folder on a local disk.

```
/file
```

Use an absolute path to specify the name of an archive file to be created.

```
/auto
```

This option automatically changes the Hitachi Storage Command Suite product services and the HiRDB service that are on the same computer to the statuses required for exporting the repositories. After the command finishes, the Hitachi Storage Command Suite product services and the HiRDB service will be active.

Be sure to always specify the `/auto` option.

Example of command execution:

```
C:\Program Files\HiCommand\Base\bin> hcmdsdbtrans/export  
/workpath D:\trans_work /file D:\trans_file\db_arc /auto
```

3. Copy the archive files to the desired folder on the migration target server.

If the archive files could not be created, copy all files stored in the folder specified by the `/workpath` option to the migration target server.

Importing repositories to the migration target server



Caution: If the Tuning Manager server is installed on a different computer than the Device Manager server, you need to stop the Tuning Manager services on that computer. After importing repositories, restart the Tuning Manager services. For details on how to start and stop the Tuning Manager services, see the manual for the installed version of Tuning Manager.

To import repositories when the migration target server OS is Windows:

1. Log on to the management server as a user with Administrator permissions.
2. From the command prompt, specify the options below and execute the `hcmdsdbtrans` command.

```
installation-folder-of-Common-Component\bin\hcmdsdbtrans /  
import /workpath work-folder[/file archive-file] /type {ALL |  
name-of-Hitachi-Storage-Command-Suite-product-to-be-moved} /  
auto  
  
/workpath
```

When using archive files for importing:

Use an absolute path to specify the folder for extracting the archive files. Specify an empty folder on a local disk. If you specify this option, you must specify the `/file` option.

When not using archive files for importing:

Use an absolute path to specify the folder containing the repository information files that were copied from the source server. Do not specify the `/file` option.

```
/file
```

Use an absolute path to specify the archive files copied from the migration source server. If you are importing without using archive files, do not specify this option.

```
/type
```

Use this option to specify the name of the Hitachi Storage Command Suite products to be moved. Only the repositories for the specified products are moved. The following product names can be specified:

- DeviceManager
- TuningManager
- ReplicationManager
- TieredStorageManager
- GlobalLinkAvailabilityManager
- NASManager

Tiered Storage Manager can also be specified with its abbreviated name `HTSM`. If you want to import multiple Hitachi Storage Command Suite products at the same time, specify multiple product names, separated by commas. For details on the character strings that can be used when specifying products, see the relevant product manuals.

To collectively import the repositories of all Hitachi Storage Command Suite products installed on the migration target server, specify `ALL`. This causes all the repositories for Hitachi Storage Command Suite products installed on the migration target server to be automatically collected and imported.

The `/type` option can be used only when the following conditions are satisfied:

- The archive files are in the path specified by the `/file` option, or the repository information files are in the folder specified by the `/workpath` option.
- All specified products are installed on the migration target.

`/auto`

This option automatically changes the Hitachi Storage Command Suite product services and the HiRDB service that are on the same computer to the statuses required for importing the repositories. After the command finishes, the Hitachi Storage Command Suite product services and the HiRDB service will remain stopped.

Be sure to always specify the `/auto` option.

Example of command execution:

```
C:\Program Files\HiCommand\Base\bin> hcmdsdbtrans /import  
/workpath D:\trans_work /type ALL /auto
```

3. Use a text editor to open the `server.properties` file, and specify `true` for the `server.base.initialsynchro` property.

The `server.base.initialsynchro` property determines whether Tiered Storage Manager's navigation tree will be synchronized and updated on startup. If the navigation tree data is not updated after a migration, the tree that Tiered Storage Manager displays will be incorrect. Therefore, after a migration you must specify `server.base.initialsynchro=true` in the `server.properties` file of Tiered Storage Manager so that when Tiered Storage Manager is started, the display data for the navigation tree will be up-to-date and correct.

For details on the `server.base.initialsynchro` property, see [server.base.initialsynchro](#).

Default installation destination for the properties file:

installation-folder-of-Tiered-Storage-Manager-
server\conf\server.properties

Property format:

`server.base.initialsynchro=true`

4. Make sure that the Tiered Storage Manager server is running.

Choose **Start, All Programs, Hitachi Storage Command Suite, Tiered Storage Manager Tiered Storage Manager Status**. A message regarding the status of the Tiered Storage Manager server will appear.

5. If the configuration of the storage subsystem was changed between the time repositories were exported and the time they were imported, you must refresh the storage domain.

For details on how to refresh the storage domain, see the *Hitachi Tiered Storage Manager User's Guide*.

6. Stop the Tiered Storage Manager server.

Choose **Start, All Programs, Hitachi Storage Command Suite, Tiered Storage Manager**, and then **Stop Tiered Storage Manager**.

7. Use a text editor to open the `server.properties` file and change the `server.base.initialsynchro` property to `false` again.

Default installation destination for the properties file:

installation-folder-of-the-Tiered-Storage-Manager-
server\conf\server.properties

Property format:

`server.base.initialsynchro=false`



Caution: When updating property files, you must first stop the Tiered Storage Manager server. If property files are updated while the Tiered Storage Manager server is running, the Tiered Storage Manager server might be unable to stop normally. If the Tiered Storage Manager server is unable to stop correctly, perform a forced stop.

Moving repositories (Solaris or Linux)

This section explains the procedures for moving repositories in Solaris or Linux.

Exporting repositories on the migration source server



Caution: If the Tuning Manager server is installed on a different computer than the Device Manager server, you need to stop the Tuning Manager services on that computer. After exporting repositories, restart the Tuning Manager services. For details on how to start and stop the Tuning Manager services, see the manual for the installed version of Tuning Manager.

To export repositories when the migration source server OS is Solaris or Linux:

1. Log on to the management server as a user with root permissions.
2. Open a terminal window, and then execute the `hcmdsdbtrans` command with the options below specified:

Collect the repository information and create archive files for the repositories.

```
installation-directory-of-Common-Component/bin/hcmdsdtrans -  
export -workpath work-directory -file archive-file -auto  
-workpath
```

Use an absolute path to specify a directory for storing the collected repository information. Specify an empty directory on a local disk.

`-file`

Use an absolute path to specify the names of an archive file to be created.

`-auto`

This option automatically changes the Hitachi Storage Command Suite product services and the HiRDB service that are on the same computer to the statuses required for exporting the repositories. After the command finishes, the Hitachi Storage Command Suite product services and the HiRDB service will be active.

Be sure to always specify the `/auto` option.

Example of command execution:

```
# /opt/HiCommand/Base/bin/hcmdsdtrans -export -workpath /  
opt/trans_work -file /opt/trans_file/db_arc -auto
```

3. Copy the archive files to the desired folder on the migration target server.

If the archive files could not be created, copy all files stored in the directory specified by the `-workpath` option to the migration target server.

Importing repositories to the migration target server



Caution: If the Tuning Manager server is installed on a different computer than the Device Manager server, you need to stop the Tuning Manager services on that computer. After importing repositories, restart the Tuning Manager services. For details on how to start and stop the Tuning Manager services, see the manual for the installed version of Tuning Manager.

To import repositories when the migration target server OS is Solaris or Linux:

1. Log on to the management server as a user with root permissions.
2. Open a terminal window, and then execute the `hcmsdbtrans` command with the options below specified:

```
installation-directory-of-Common-Component/bin/hcmsdbtrans -  
import -workpath work-directory [-file archive-file] -type  
{ALL | name-of-Hitachi-Storage-Command-Suite-product-to-be-  
moved} -auto  
-workpath
```

When using archive files for importing:

Use an absolute path to specify the directory for extracting archive files. Specify an empty directory on a local disk. If you specify this option, you must specify the `/file` option.

When not using archive files for importing:

Use an absolute path to specify the folder containing the repository information files that were copied from the source server. Do not specify the `/file` option.

`-file`

Use an absolute path to specify the archive files copied from the migration source server. If you are importing without using archive files, do not specify this option.

`-type`

Use this option to specify the name of the Hitachi Storage Command Suite product to be moved. Only the repositories for the specified product are moved. The following product names can be specified:

- DeviceManager
- TuningManager
- ReplicationManager
- TieredStorageManager
- GlobalLinkAvailabilityManager
- NASManager

Note that Tiered Storage Manager can also be specified with its abbreviated name `HTSM`. If you want to import multiple Hitachi Storage Command Suite products at the same time, specify multiple product names, separated by commas. For details on the character strings that can be used when specifying products, see the relevant product manuals.

To collectively import the repositories of all Hitachi Storage Command Suite products installed on the migration target server, specify `ALL`. This causes all the repositories for Hitachi Storage Command Suite products installed on the migration target server are automatically collected and import.

The `-type` option can be used only when the following conditions are satisfied:

- The archive files are in the path specified by the `-file` option, or the repository information files are in the folder specified by the `-workpath` option.
- All specified products are installed on the migration target.

`-auto`

This option automatically changes the Hitachi Storage Command Suite product services and the HiRDB service that are on the same computer to the statuses required for importing the repositories. After the command finishes, the Hitachi Storage Command Suite product services and the HiRDB service will remain stopped.

Be sure to always specify the `-auto` option.

Example of command execution:

```
# /opt/HiCommand/Base/bin/hcmdsdbtrans -import -workpath /  
opt/trans_work -type ALL -auto
```

3. Use a text editor to open the `server.properties` file, and specify `true` for the `server.base.initialsynchro` property.

The `server.base.initialsynchro` property determines whether Tiered Storage Manager's navigation tree will be synchronized and updated on startup. If the navigation tree data is not updated after a migration, the tree that Tiered Storage Manager displays will be incorrect. Therefore, after a migration you must specify `server.base.initialsynchro=true` in the `server.properties` file of Tiered Storage Manager so that when Tiered Storage Manager is started, the display data for the navigation tree will be up-to-date and correct.

For details on the `server.base.initialsynchro` property, see [server.base.initialsynchro](#).

Installation destination for the properties file:

```
installation-directory-of-the-Tiered-Storage-Manager-server/conf/  
server.properties
```

Property format:

```
server.base.initialsynchro=true
```

4. Execute the `htsmserver` command with the `status` option specified. Make sure that Tiered Storage Manager has started.

```
installation-directory-of-the-Tiered-Storage-Manager-server/bin/  
htsmserver
```

Example of command execution:

```
# /opt/HiCommand/TieredStorageManager/bin/htsmserver status
```

5. If the configuration of the storage subsystem was changed between the time repositories were exported and the time they were imported, you must refresh the storage domain.

For details on how to refresh the storage domain, see the *Hitachi Tiered Storage Manager User's Guide*.

6. Stop the Tiered Storage Manager server.

Execute the `htsmserver` command with the `stop` option specified.

installation-directory-of-the-Tiered-Storage-Manager-server/bin/
`htsmserver`

Example of command execution:

```
# /opt/HiCommand/TieredStorageManager/bin/htsmserver stop
```

7. Use a text editor to open the `server.properties` file, and change the `server.base.initialsynchro` property to `false` again.

Installation destination for the properties file:

installation-directory-of-the-Tiered-Storage-Manager-server/conf/
`server.properties`

Property format:

```
server.base.initialsynchro=false
```



Caution: When updating property files, you must first stop the Tiered Storage Manager server. If property files are updated while the Tiered Storage Manager server is running, the Tiered Storage Manager server might be unable to stop normally. If the Tiered Storage Manager server is unable to stop correctly, perform a forced stop.

Backing up repositories

If an error occurs in the database where repositories are saved, you might be unable to operate the management server, so we recommend that you make regular backups. The procedure for backing up repositories is explained in this section. You can make backups of the repositories of all Hitachi Storage Command Suite products installed on the management server, not just the repository containing management information of Tiered Storage Manager.



Caution: Backup data for a Hitachi Storage Command Suite product's repository can be restored only to an environment containing an installation of that product with the same version and revision number as when the backup was performed.

If even a single Hitachi Storage Command Suite product differs between the environments, do not perform a restore. If a restore is performed into a different environment, Tiered Storage Manager will become unusable, always encountering an error at startup.



Caution: For the repository backup location, you must secure a capacity that is equal to the total size of the following:

- Total capacity of all the repositories of your Hitachi Storage Command Suite products
- Capacity of the Common Component repository

During backup, a temporary file is also created in the repository backup location. Therefore, in addition to the above capacity, you need to secure the following capacity: *total-capacity-of-Hitachi-Storage-Command-Suite-product-repositories* + 20 MB.

Non-cluster environment (Windows)



Caution: If the Tuning Manager server is installed on a different computer than the Device Manager server, you need to stop the Tuning Manager services on that computer. After backing up repositories, restart the Tuning Manager services. For details on how to start and stop the Tuning Manager services, see the manual for the installed version of Tuning Manager.

To back up repositories when the management server OS is Windows and the server is in a non-cluster configuration:

1. Log on to the management server as a user with Administrator permissions.
2. From the command prompt, execute the `hcmdsbackups` command with the options below specified.

installation-folder-of-Common-Component\bin\hcmdsbackups /dir
storage-location-for-backup-files /auto
/dir

Use this option to specify an empty folder for storing backup files. If the specified folder does not exist, it is automatically created.

In the specified folder, a subfolder called `database` is created, and in that subfolder a backup file called `backup.hdb` is created.

/auto

This option automatically changes the Hitachi Storage Command Suite product services and the HiRDB service that are on the same computer to the statuses required for backing up the repository. After the command finishes, the Hitachi Storage Command Suite product services and the HiRDB service will be active.

Be sure to always specify the `/auto` option.

Example of command execution:

```
C:\Program Files\HiCommand\Base\bin> hcmdsbacups /dir  
D:\backup /auto
```

Cluster environment (Windows)



- When operating in a cluster configuration, use the executing node to make backups of repositories. Specify a shared disk as the location for saving backup files.
- If the Tuning Manager server is installed on a different computer than the Device Manager server, you need to stop the Tuning Manager services on that computer. After backing up repositories, restart the Tuning Manager services. For details on how to start and stop the Tuning Manager services, see the manual for the installed version of Tuning Manager.

To back up repositories when the management server OS is Windows and the server is in a cluster configuration:

1. Log on to the management server as a user with Administrator permissions.
2. Use the cluster management application to take the following services offline:

The following services will be displayed by the resource name specified when the service was registered as a resource.

- HiCommand Tiered Storage Manager
- HiCommandServer
- HBase Storage Mgmt Web Service
- HBase Storage Mgmt Common Service
- Any other installed Hitachi Storage Command Suite product resources

For Microsoft Cluster Service

Using Cluster Administrator, right-click the above resources from the group in which the Hitachi Storage Command Suite product services have been registered, and select **Take Offline**:

For Microsoft Failover Cluster

Using Failover Cluster Management, right-click the above resources from the group in which the Hitachi Storage Command Suite product services have been registered, and select **Take this service or application offline**:

3. Open the command prompt, and then execute the `hcmdssrv` command with the `/stop` option specified.

installation-folder-of-Common-Component\bin\hcmdssrv

Example of command execution:

```
C:\Program Files\HiCommand\Base\bin> hcmdssrv /stop
```

4. Use the cluster management application to take the following service offline:

- HiRDBClusterService _HD0

This service will be displayed by the resource name specified when the service was registered as a resource.

5. Use the cluster management application to suppress failover of the resource group.

Change the settings of the resources listed below. The following services will be displayed with the resource names that were specified for them when they were registered as resources:

- HiCommand Tiered Storage Manager
- HiCommandServer
- HBase Storage Mgmt Web Service
- HBase Storage Mgmt Common Service
- HiRDBClusterService _HD0
- Any other installed Hitachi Storage Command Suite product resources

For Microsoft Cluster Service

Right-click the resource name, and choose **Properties**, the **Advanced** tab, and then **Do not restart**.

For Microsoft Failover Cluster

Right-click the resource name, and choose **Properties**, the **Policies** tab, and then **If resource fails, do not restart**.

6. Open the command prompt, and then execute the `hcmdssrv` command with the `/start` option specified.

installation-folder-of-Common-Component\bin\hcmdssrv

Example of command execution:

```
C:\Program Files\HiCommand\Base\bin> hcmdssrv /start
```

7. From the command prompt, execute the `hcmdsbackups` command with the options below specified.

installation-folder-of-Common-Component\bin\hcmdsbackups /dir
storage-location-for-backup-files

/dir

Use this option to specify an empty folder for storing backup files. If the specified folder does not exist, it is automatically created.

In the specified folder, a subfolder called `database` is created, and in that subfolder a backup file called `backup.hdb` is created.

Example of command execution:

```
C:\Program Files\HiCommand\Base\bin> hcmdssbackups /dir  
D:\backup
```

8. Open the command prompt, and then execute the `hcmdssrv` command with the `/stop` option specified.

installation-folder-of-Common-Component\bin\hcmdssrv

Example of command execution:

```
C:\Program Files\HiCommand\Base\bin> hcmdssrv /stop
```

9. Use the cluster management application to enable failover of the resource group.

Change the settings of the resources listed below. The following services will be displayed with the resource names that were specified for them when they were registered as resources:

- HiCommand Tiered Storage Manager
- HiCommandServer
- HBase Storage Mgmt Web Service
- HBase Storage Mgmt Common Service
- HiRDBClusterService _HD0
- Any other installed Hitachi Storage Command Suite product resources

For Microsoft Cluster Service

Right-click the resource name, and choose **Properties**, the **Advanced** tab, and then **Restart**.

For Microsoft Failover Cluster

Right-click the resource name, and choose **Properties**, the **Policies** tab, then **If resource fails. Attempt restart on current node** and **If restart is unsuccessful, fail over all resources in this service or application**.

10. In the cluster management application, bring online the resource group in which the Hitachi Storage Command Suite product services are registered.

Non-cluster environment (Solaris or Linux)



Caution: If the Tuning Manager server is installed on a different computer than the Device Manager server, you need to stop the Tuning Manager services on that computer. After backing up repositories, restart the Tuning Manager services. For details on how to start and stop the Tuning Manager services, see the manual for the installed version of Tuning Manager.

To back up repositories when the management server OS is Solaris or Linux and the server is in a non-cluster configuration:

1. Log on to the management server as a user with root permissions.
2. Open a terminal window, and then execute the `hcmdsbackups` command with the options below specified.

```
installation-directory-of-Common-Component/bin/hcmdsbacups -  
dir storage-directory-for-backup-files -auto  
-dir
```

Use this option to specify an empty folder for storing backup files. If the specified directory does not exist, it is automatically created.

In the specified folder, a subfolder called `database` is created, and in that subfolder a backup file called `backup.hdb` is created.

```
-auto
```

This option automatically changes the Hitachi Storage Command Suite product services and the HiRDB service that are on the same computer to the statuses required for backing up the repository. After the command finishes, the Hitachi Storage Command Suite product services and the HiRDB service will be active.

Be sure to always specify the `/auto` option.

Example of command execution:

```
# /opt/HiCommand/Base/bin/hcmdsbackups -dir /tmp/backup -auto
```

Cluster environment (Solaris)



- When operating in a cluster configuration, back up the repositories on the executing node. Specify a shared disk as the save target for backup files.
- If the Tuning Manager server is installed on a different computer than the Device Manager server, you need to stop the Tuning Manager services on that computer. After backing up repositories, restart the Tuning Manager services. For details on how to start and stop the Tuning Manager services, see the manual for the installed version of Tuning Manager.

The procedures for backing up repositories when the management server OS is Solaris and the server is in a cluster configuration are described below.

1. Log on to the management server as a user with root permissions.
2. Stop all Hitachi Storage Command Suite products running on the management server.

For Veritas Cluster Server:

Take the following resources offline:

- HiCommand Tiered Storage Manager
- HiCommandServer
- HBase Storage Mgmt Web Service
- HBase Storage Mgmt Common Service
- Any other installed Hitachi Storage Command Suite products

These services will be displayed by the resource name specified when the service was registered as a resource.

For Sun Cluster:

Disable resource monitoring by executing the following commands in the order given:

```
# /usr/cluster/bin/scswitch -n -M -j TieredStorageManager
# /usr/cluster/bin/scswitch -n -M -j HiCommandServer
# /usr/cluster/bin/scswitch -n -M -j CommonWebService
# /usr/cluster/bin/scswitch -n -M -j SingleSignOnService
```

If there are any resources related to Hitachi Storage Command Suite products other than the above, disable monitoring of them as well.

Specify the resource names that were registered when the cluster resources were set.

Disable resources by executing the following commands in the order given:

```
# /usr/cluster/bin/scswitch -n -j TieredStorageManager
# /usr/cluster/bin/scswitch -n -j HiCommandServer
# /usr/cluster/bin/scswitch -n -j CommonWebService
# /usr/cluster/bin/scswitch -n -j SingleSignOnService
```

If there are any resources related to Hitachi Storage Command Suite products other than the above, disable them as well.

Specify the resource names that were registered when the cluster resources were set.

3. Open the terminal window, and then execute the `hcmdssrv` command with the `-stop` option specified.

installation-directory-of-Common-Component/bin/hcmdssrv

Example of command execution:

```
# /opt/HiCommand/Base/bin/hcmdssrv -stop
```

4. Take the service listed below offline.

For Veritas Cluster Server:

The following service will be displayed with the resource names that were specified for them when they were registered as resources:

- HiRDB

For Sun Cluster:

Disable resource monitoring by executing the following command:

```
# /usr/cluster/bin/scswitch -n -M -j HiRDB
```

Specify the resource names that were registered when the cluster resources were set.

Disable a resource by executing the following command:

```
# /usr/cluster/bin/scswitch -n -j HiRDB
```

Specify the resource names that were registered when the cluster resources were set.

5. For Veritas Cluster Server, right-click the displayed services listed below, and then clear the **Enabled** checkbox from the displayed context menu.

The following services will be displayed with the resource names that were specified for them when they were registered as resources:

- HiCommand Tiered Storage Manager
- HiCommandServer
- HBase Storage Mgmt Web Service
- HBase Storage Mgmt Common Service
- HiRDB

- Any other installed Hitachi Storage Command Suite product resources
6. For Veritas Cluster Server, select the **Service Groups** tab in the Cluster Explorer window. Right-click the resource group in which the Hitachi Storage Command Suite product services are registered, and then from the displayed context menu, select **Freeze** and then **Temporary**.
 7. Open the terminal window, and then execute the `hcmdssrv` command with the `-start` option specified.

installation-directory-of-Common-Component/bin/hcmdssrv

Example of command execution:

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

8. Open a terminal window, and then execute the `hcmsbackups` command with the options below specified.

installation-directory-of-Common-Component/bin/hcmsbackups -dir storage-directory-for-backup-files
-dir

Use this option to specify an empty folder for storing backup files. If the specified directory does not exist, it is automatically created.

In the specified folder, a subfolder called `database` is created, and in that subfolder a backup file called `backup.hdb` is created.

Example of command execution:

```
# /opt/HiCommand/Base/bin/hcmsbackups -dir /tmp/backup
```

9. Open the terminal window, and then execute the `hcmdssrv` command with the `-stop` option specified.

installation-directory-of-Common-Component/bin/hcmdssrv

Example of command execution:

```
# /opt/HiCommand/Base/bin/hcmdssrv -stop
```

10. For Veritas Cluster Server, select the **Service Groups** tab in the Cluster Explorer window. Right-click the resource group in which the Hitachi Storage Command Suite product services are registered, and then from the displayed context menu, select **Unfreeze**.
11. Right-click the resource group in which the Hitachi Storage Command Suite product services are registered, and then from the displayed context menu, select **Enable Resources**.
12. Start the Hitachi Storage Command Suite products that were stopped in step 2.

For Veritas Cluster Server:

Bring the groups in which the resources are registered online.

For Sun Cluster:

Enable resources by executing the following commands in the order given:

```
# /usr/cluster/bin/scswitch -e -j HiRDB
# /usr/cluster/bin/scswitch -e -j SingleSignOnService
```

```
# /usr/cluster/bin/scswitch -e -j CommonWebService
# /usr/cluster/bin/scswitch -e -j HiCommandServer
# /usr/cluster/bin/scswitch -e -j TieredStorageManager
```

If there are any resources related to Hitachi Storage Command Suite products other than the above, enable them as well.

Specify the resource names that were registered when the cluster resources were set.

Enable resource monitoring by executing the following commands in the order written:

```
# /usr/cluster/bin/scswitch -e -M -j HiRDB
# /usr/cluster/bin/scswitch -e -M -j SingleSignOnService
# /usr/cluster/bin/scswitch -e -M -j CommonWebService
# /usr/cluster/bin/scswitch -e -M -j HiCommandServer
# /usr/cluster/bin/scswitch -e -M -j TieredStorageManager
```

If there are any resources related to Hitachi Storage Command Suite products other than the above, enable monitoring of them as well.

Specify the resource names that were registered when the cluster resources were set.

Restoring repositories

If the database where repositories are saved becomes corrupted, you can still restore the repositories by using the repository backup files.

You can perform a full restore or an individual restore.

Full restore

You can restore the management information for all Hitachi Storage Command Suite products, including Tiered Storage Manager, installed on the management server.

Backup data for a Hitachi Storage Command Suite product's repository can be restored only to an environment containing an installation of that product with the same version and revision number as when the backup was performed.

If even a single Hitachi Storage Command Suite product differs between the environments, do not perform a restore. If a restore is performed into a different environment, Tiered Storage Manager will become unusable, always encountering an error at startup.

Individual restore

You can choose to restore only the management information of Tiered Storage Manager.

After backing up your data, and then performing an uninstallation and re-installation of Tiered Storage Manager, do not perform an individual restore. If an individual restore is performed under these circumstances, Tiered Storage Manager will become unusable, always encountering an error at startup.

When you perform a restore, the information displayed in the navigation frame of the GUI might not match the information displayed in the information frame. If this happens, specify `true` for `server.base.initialsynchro` in the `server.properties` file, restart Tiered Storage Manager, and then refresh the storage domain. For details on how to refresh the storage domain, see the *Hitachi Tiered Storage Manager User's Guide*.



- If you change the repository storage location, you cannot perform a restore of the Tiered Storage Manager server repository by using a backup that was made before the change.
- During restoration, a temporary file is created in the repository backup location. Therefore, to account for the temporary file, you need to secure the following capacity: *total-capacity-of-Hitachi-Storage-Command-View-AE-Suite-product-repositories-to-be-restored* + 20 MB.

Non-cluster environment (Windows)



Caution: If the Tuning Manager server is installed on a different computer than the Device Manager server, you need to stop the Tuning Manager services on that computer. After restoring repositories, restart the Tuning Manager services. For details on how to start and stop the Tuning Manager services, see the manual for the installed version of Tuning Manager.

To restore repositories when the management server OS is Windows and the server is in a non-cluster configuration:

1. Log on to the management server as a user with Administrator permissions.
2. From the command prompt, execute the `hcmdsdb` command with the options below specified.

```
installation-folder-of-Common-Component\bin\hcmdsdb /restore  
absolute-path-of-backup-file /type restore-target /auto  
/restore
```

Use an absolute path to specify the backup file.

Specify a path to the `backup.hdb` file created in the procedure described in [Non-cluster environment \(Windows\)](#).

```
/type
```

Use this option to specify the restore type. The value specified in `/type` is case sensitive. Specify one of the following values:

For a full restore: `ALL`

For an individual restore: `TieredStorageManager#`

You can also specify `HTSM`, the abbreviated name of Tiered Storage Manager.

```
/auto
```

This option automatically changes the Hitachi Storage Command Suite product services and the HiRDB service that are on the same computer to the statuses required for importing the repositories. After the command finishes, the Hitachi Storage Command Suite product services and the HiRDB service will remain stopped.

Be sure to always specify the `/auto` option.

Example of command execution:

```
C:\Program Files\HiCommand\Base\bin> hcmdsdb /restore  
D:\backup\database\backup.hdb /type ALL /auto
```

3. If you performed a full restore, refresh the subsystem by using Device Manager.

If you restored the repositories for other Hitachi Storage Command Suite products, see the manuals for those products and perform necessary operations.

4. Refresh all storage domains by using Tiered Storage Manager.

Restoring repositories causes tasks that have a status of **Standby** or **Active** to change to a status of **Failure**. After you finish restoring repositories, use the following steps to check the statuses of all tasks, and then re-create and execute failed tasks as necessary.

5. See the message log of Tiered Storage Manager.

When starting Tiered Storage Manager for the first time after restoring repositories, make sure that the message KATS50354-E is output to the log file. The task IDs of tasks whose status was changed to **Failure** are output to KATS50354-E.

6. See the volume information of the tasks indicated in the message KATS50354-E and check whether those tasks are completed.

Check for completion of not only migration tasks but also shredding tasks and locking tasks.

7. If a task is not completed, create and execute the task again as necessary.

Cluster environment (Windows)



- When operating in a cluster configuration, restoration of repositories must be done on the executing node. Use the backup file saved to the shared disk.
- If the Tuning Manager server is installed on a different computer than the Device Manager server, you need to stop the Tuning Manager services on that computer. After restoring repositories, restart the Tuning Manager services. For details on how to start and stop the Tuning Manager services, see the manual for the installed version of Tuning Manager.

To restore repositories when the management server OS is Windows and the server is in a cluster configuration:

1. Log on to the management server as a user with Administrator permissions.

2. Use the cluster management application to take the following services offline:

The following services will be displayed by the resource name specified when the service was registered as a resource.

- HiCommand Tiered Storage Manager
- HiCommandServer
- HBase Storage Mgmt Web Service
- HBase Storage Mgmt Common Service
- Any other installed Hitachi Storage Command Suite product resources

For Microsoft Cluster Service

Using Cluster Administrator, right-click the above resources from the group in which the Hitachi Storage Command Suite product services have been registered, and select **Take Offline**:

For Microsoft Failover Cluster

Using Failover Cluster Management, right-click the above resources from the group in which the Hitachi Storage Command Suite product services have been registered, and select **Take this service or application offline**:

3. Open the command prompt, and then execute the `hcmdssrv` command with the `/stop` option specified.

installation-folder-of-Common-Component\bin\hcmdssrv

Example of command execution:

```
C:\Program Files\HiCommand\Base\bin> hcmdssrv /stop
```

4. Use the cluster management application to take the following service offline:

- HiRDBClusterService _HD0

This service will be displayed by the resource name specified when the service was registered as a resource.

5. Use the cluster management application to suppress failover of the resource group.

Change the settings of the resources listed below. The following services will be displayed with the resource names that were specified for them when they were registered as resources:

- HiCommand Tiered Storage Manager
- HiCommandServer
- HBase Storage Mgmt Web Service
- HBase Storage Mgmt Common Service
- HiRDBClusterService _HD0
- Any other installed Hitachi Storage Command Suite product resources

For Microsoft Cluster Service

Right-click the resource name, and choose **Properties**, the **Advanced** tab, and then **Do not restart**.

For Microsoft Failover Cluster

Right-click the resource name, and choose **Properties**, the **Policies** tab, and then **If resource fails, do not restart**.

6. Open the command prompt, and then execute the `hcmdsdb` command with the options described below specified.

```
installation-folder-of-Common-Component\bin\hcmdsdb /restore  
absolute-path-of-backup-file /type backup-target  
/restore
```

Use an absolute path to specify the backup file.

Specify a path to the backup.hdb file created in the procedure described in [Cluster environment \(Windows\)](#).

```
/type
```

Use this option to specify the backup type. The value specified in `/type` is case sensitive. Specify one of the following values:

For a full restore: **ALL**

For an individual restore: **TieredStorageManager**[#]

[#]: You can also specify **HTSM**, the abbreviated name of Tiered Storage Manager.

Example of command execution:

```
C:\Program Files\HiCommand\Base\bin> hcmdsdb /restore  
D:\backup\database\backup.hdb /type ALL
```

7. Use the cluster management application to enable failover of the resource group.

Change the settings of the resources listed below. The following services will be displayed with the resource names that were specified for them when they were registered as resources:

- HiCommand Tiered Storage Manager
- HiCommandServer
- HBase Storage Mgmt Web Service
- HBase Storage Mgmt Common Service
- HiRDBClusterService _HD0
- Any other installed Hitachi Storage Command Suite product resources

For Microsoft Cluster Service

Right-click the resource name, and choose **Properties**, the **Advanced** tab, and then **Restart**.

For Microsoft Failover Cluster

Right-click the resource name, and choose **Properties**, the **Policies** tab, then **If resource fails. Attempt restart on current node** and **If restart is unsuccessful, fail over all resources in this service or application**.

8. In the cluster management application, bring online the resource group in which the Hitachi Storage Command Suite products services are registered.
9. If you performed a full restore, refresh the subsystem by using Device Manager.

If you restored the repositories for other Hitachi Storage Command Suite products, see the manuals for those products and perform necessary operations.

10. Refresh all storage domains by using Tiered Storage Manager.

Restoring repositories causes tasks that have a status of **Standby** or **Active** to change to a status of **Failure**. After you finish restoring repositories, use the following steps to check the statuses of all tasks, and then re-create and execute failed tasks as necessary.

11. See the message log of Tiered Storage Manager.

When starting Tiered Storage Manager for the first time after restoring repositories, make sure that the message KATS50354-E is output to the log file. The task IDs of tasks whose status was changed to **Failure** are output to KATS50354-E.

12. See the volume information of the tasks indicated in the message KATS50354-E and check whether those tasks are completed.

Check for completion of not only migration tasks but also shredding tasks and locking tasks.

13. If a task is not completed, create and execute the task again as necessary.

Non-cluster environment (Solaris or Linux)



Caution: If the Tuning Manager server is installed on a different computer than the Device Manager server, you need to stop the Tuning Manager services on that computer. After restoring repositories, restart the Tuning Manager services. For details on how to start and stop the Tuning Manager services, see the manual for the installed version of Tuning Manager.

To restore repositories when the management server OS is Solaris or Linux and the server is in a non-cluster configuration:

1. Log on to the management server as a user with root permissions.
2. Open a terminal window, and then execute the `hcmdsdb` command with the options below specified.

```
installation-directory-of-Common-Component/bin/hcmdsd -restore  
absolute-path-of-backup-file -type backup-target -auto  
-restore
```

Use an absolute path to specify the backup file.

Specify the path to the `backup.hdb` file created in the procedure described in [Non-cluster environment \(Solaris or Linux\)](#) (Solaris or Linux).

`-type`

Use this option to specify the backup type. The value specified in `-type` is case sensitive. Specify one of the following values:

For a full restore: `ALL`

For an individual restore: `TieredStorageManager`[#]

[#] You can also specify `HTSM`, the abbreviated name of Tiered Storage Manager.

`-auto`

This option automatically changes the Hitachi Storage Command Suite product services and the HiRDB service that are on the same computer to the statuses required for restoring the repository. After the command finishes, the Hitachi Storage Command Suite product services and the HiRDB service will remain stopped.

Be sure to always specify the `/auto` option.

Example of command execution:

```
# /opt/HiCommand/Base/bin/hcmdsdb -restore /tmp/backup/  
database/backup.hdb -type ALL -auto
```

3. If you performed a full restore, refresh the subsystem by using Device Manager.

If you restored the repositories for other Hitachi Storage Command Suite products, see the manuals for those products and perform the necessary operations.

4. Refresh all storage domains by using Tiered Storage Manager.

Restoring repositories causes tasks that have a status of **Standby** or **Active** to change to a status of **Failure**. After you finish restoring repositories, use the following steps to check the statuses of all tasks, and then re-create and execute failed tasks as necessary.

5. See the message log of Tiered Storage Manager.

When starting Tiered Storage Manager for the first time after restoring repositories, make sure that the message KATS50354-E is output to the log file. The task IDs of tasks whose status was changed to **Failure** are output to KATS50354-E.

6. See the volume information of the tasks indicated in the message KATS50354-E and check whether those tasks are completed.

Check for completion of not only migration tasks but also shredding tasks and locking tasks.

7. If a task is not completed, create and execute the task again as necessary.

Cluster environment (Solaris)



- When operating in a cluster configuration, restoration of repositories must be done on the executing node. Use the backup file saved to the shared disk.
 - If the Tuning Manager server is installed on a different computer than the Device Manager server, you need to stop the Tuning Manager services on that computer. After restoring repositories, restart the Tuning Manager services. For details on how to start and stop the Tuning Manager services, see the manual for the installed version of Tuning Manager.
-

The procedures for restoring repositories when the management server OS is Solaris and the server is in a cluster configuration are described below.

1. Log on to the management server as a user with root permissions.
2. Stop all Hitachi Storage Command Suite products running on the management server.

For Veritas Cluster Server:

Take the following resources offline:

- HiCommand Tiered Storage Manager
- HiCommandServer
- HBase Storage Mgmt Web Service
- HBase Storage Mgmt Common Service
- Any other installed Hitachi Storage Command Suite products

These services will be displayed by the resource name specified when the service was registered as a resource.

For Sun Cluster:

Disable resource monitoring by executing the following commands in the order given:

```
# /usr/cluster/bin/scswitch -n -M -j TieredStorageManager
# /usr/cluster/bin/scswitch -n -M -j HiCommandServer
# /usr/cluster/bin/scswitch -n -M -j CommonWebService
# /usr/cluster/bin/scswitch -n -M -j SingleSignOnService
```

If there are any resources related to Hitachi Storage Command Suite products other than the above, disable monitoring of them as well.

Specify the resource names that were registered when the cluster resources were set.

Disable resources by executing the following commands in the order given:

```
# /usr/cluster/bin/scswitch -n -j TieredStorageManager
# /usr/cluster/bin/scswitch -n -j HiCommandServer
# /usr/cluster/bin/scswitch -n -j CommonWebService
# /usr/cluster/bin/scswitch -n -j SingleSignOnService
```

If there are any resources related to Hitachi Storage Command Suite products other than the above, disable them as well.

Specify the resource names that were registered when the cluster resources were set.

3. Open the terminal window, and then execute the `hcmdssrv` command with the `-stop` option specified.

installation-directory-of-Common-Component/bin/hcmdssrv

Example of command execution:

```
# /opt/HiCommand/Base/bin/hcmdssrv -stop
```

4. Take the service listed below offline.

For Veritas Cluster Server:

The following service will be displayed with the resource names that were specified for them when they were registered as resources:

- HiRDB

For Sun Cluster:

Disable resource monitoring by executing the following command:

```
# /usr/cluster/bin/scswitch -n -M -j HiRDB
```

Specify the resource names that were registered when the cluster resources were set.

Disable a resource by executing the following command:

```
# /usr/cluster/bin/scswitch -n -j HiRDB
```

Specify the resource names that were registered when the cluster resources were set.

5. For Veritas Cluster Server, right-click the displayed services listed below, and then clear the **Enabled** checkbox from the displayed context menu.

The following services will be displayed with the resource names that were specified for them when they were registered as resources:

- HiCommand Tiered Storage Manager
- HiCommandServer
- HBase Storage Mgmt Web Service
- HBase Storage Mgmt Common Service
- HiRDB
- Any other installed Hitachi Storage Command Suite product resources

6. For Veritas Cluster Server, select the **Service Groups** tab in the Cluster Explorer window. Right-click the resource group in which the Hitachi Storage Command Suite product services are registered, and then from the displayed context menu, select **Freeze** and then **Temporary**.
7. From the command prompt, execute the `hcmdsdb` command with the options below specified.

installation-directory-of-Common-Component/bin/hcmdsdb -restore absolute-path-of-backup-file -type backup-target

-restore

Use an absolute path to specify the backup file.

Specify a path to the `backup.hdb` file created in the procedure described in [Cluster environment \(Solaris\)](#).

-type

Use this option to specify the backup type. The value specified in -type is case sensitive. Specify one of the following values:

For a full restore: `ALL`

For an individual restore: `TieredStorageManager#`

You can also specify `HTSM`, the abbreviated name of Tiered Storage Manager.

Example of command execution:

```
# /opt/HiCommand/Base/bin/hcmdsdb -restore /tmp/backup/  
database/backup.hdb -type ALL
```

8. For Veritas Cluster Server, select the **Service Groups** tab in the Cluster Explorer window. Right-click the resource group in which the Hitachi Storage Command Suite product services are registered, and then from the displayed context menu, select **Unfreeze**.
9. For Veritas Cluster Server, right-click the resource group in which the Hitachi Storage Command Suite product services are registered, and then from the displayed context menu, select **Enable Resources**.
10. For Sun Cluster, execute the following commands to enable all resources.

- Enable resources by executing the following commands in the order given:

```
# /usr/cluster/bin/scswitch -e -j HiRDB  
# /usr/cluster/bin/scswitch -e -j CommonWebService  
# /usr/cluster/bin/scswitch -e -j SingleSignOnService  
# /usr/cluster/bin/scswitch -e -j HiCommandServer  
# /usr/cluster/bin/scswitch -e -j TieredStorageManager
```

Specify the resource names that were registered when the cluster resources were set.

- Enable resource monitoring by executing the following commands in the order given:

```
# /usr/cluster/bin/scswitch -e -M -j HiRDB  
# /usr/cluster/bin/scswitch -e -M -j CommonWebService  
# /usr/cluster/bin/scswitch -e -M -j SingleSignOnService  
# /usr/cluster/bin/scswitch -e -M -j HiCommandServer  
# /usr/cluster/bin/scswitch -e -M -j TieredStorageManager
```

Specify the resource names that were registered when the cluster resources were set.

11. If you performed a full restore, refresh the subsystem by using Device Manager.
If you restored the repositories for other Hitachi Storage Command Suite products, see the manuals for those products and perform the necessary operations.
12. Refresh all storage domains by using Tiered Storage Manager.
Restoring repositories causes tasks that have a status of **Standby** or **Active** to change to a status of **Failure**. After you finish restoring repositories, use the following steps to check the statuses of all tasks, and then re-create and execute failed tasks as necessary.
13. See the message log of Tiered Storage Manager.
When starting Tiered Storage Manager for the first time after restoring repositories, make sure that the message KATS50354-E is output to the log file. The task IDs of tasks whose status was changed to **Failure** are output to KATS50354-E.
14. See the volume information of the tasks indicated in the message KATS50354-E and check whether the tasks are completed.
Check for completion of not only migration tasks but also shredding tasks and locking tasks.
15. If a task is not completed, create and execute the task again as necessary.

Troubleshooting

This chapter explains problems that might occur in the Tiered Storage Manager server, countermeasures, and also how to obtain output log data and maintenance information.

- ❑ [Troubleshooting information](#)
- ❑ [Log data output by Tiered Storage Manager](#)
- ❑ [Integrated logging](#)
- ❑ [Audit log data](#)
- ❑ [Retrieving log information](#)

Troubleshooting information

This section provides general troubleshooting information for the Tiered Storage Manager server. The following procedure should be followed when errors occur in Tiered Storage Manager:

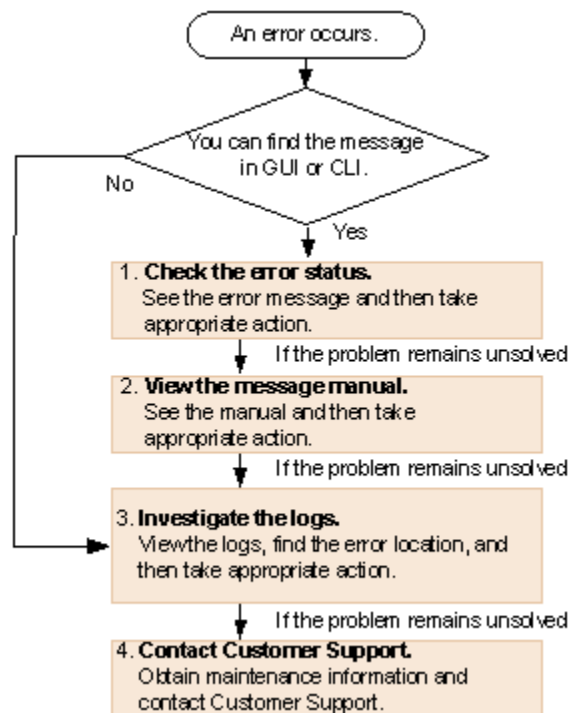


Figure 4-1: Procedure to be followed if an error occurs

1. Check the error information.

Use any messages that are displayed in the GUI window or pop-up window, check the messages to check the error information and determine appropriate action to take.

2. View the message manual.

If the problem cannot be solved by using information from the displayed message alone, reference the message manual. Follow the steps recommended in the message manual. For possible causes behind error messages output by Tiered Storage Manager and corrective action to take, see the *Hitachi Tiered Storage Manager Messages*.

3. Reference the logs.

If the messages output to the GUI or CLI do not help in correcting the problem, or if a problem is occurring but no message is being output to the GUI or CLI, view the message logs for the Tiered Storage Manager server. Identify the location where the error occurred from the message log, and then eliminate the cause of the error. Reference the message ID to identify the location of the error. For details on message logs for the Tiered Storage Manager server, see [Log data output by Tiered Storage Manager](#). For details on message IDs, see [Log contents](#).

We recommend that the system administrator of Tiered Storage Manager periodically view the message logs to check whether errors have occurred in the system.

4. Contact Customer Support.

If the problem remains after you check the message logs and take appropriate action, obtain maintenance information by using the `hcmdsgetlogs` command, and then contact Customer Support.

For details about how to obtain maintenance information, see [Retrieving log information](#).

[Table 4-1: Troubleshooting information for the Tiered Storage Manager server](#) lists various problems, their causes, and appropriate actions.

Table 4-1: Troubleshooting information for the Tiered Storage Manager server

Problem	Cause	Action
An attempt to start Tiered Storage Manager failed.	Device Manager or Common Component has not started.	Start Device Manager or Common Component.
	The user who attempted the operation does not have administrator permissions.	Perform the operation again through a user who has administrator permissions for the OS.
	The property file is invalid.	Revise the property file in accordance with the command logs or the message logs.
The Tiered Storage Manager server has not stopped.	An error occurred in the Tiered Storage Manager server during processing to stop it.	If 10 minutes have passed since the stop request, and the Tiered Storage Manager server is still not stopping, perform a forced termination.
	The user who attempted the operation does not have administrator permissions.	Perform the operation again through a user who has administrator permissions for the OS.

Problem	Cause	Action
An inconsistency exists between the repository information and the storage subsystem status.	Possible causes are as follows: <ul style="list-style-type: none"> • The Tiered Storage Manager server terminated abnormally due to a forced termination or an unexpected error. • A failover occurred in a cluster environment. 	Perform the following procedure to restore the consistency between the repository information and the storage subsystem status: <ol style="list-style-type: none"> 1. After restarting the Tiered Storage Manager server, refresh all storage domains. 2. If a migration task was being created or canceled during an abnormal termination of the Tiered Storage Manager server, perform the creation or cancellation again. If an error occurred during a cancel operation, refresh the storage domain. 3. If a migration task that was being performed failed, refresh the storage domain again. Then, take appropriate action in accordance with the troubleshooting case examples in the <i>Hitachi Tiered Storage Manager User's Guide</i>. The case examples to be checked are as follows: <ul style="list-style-type: none"> - When the status of the migration task is <i>migration failed</i>. - When the status of the migration task is <i>data erasure failed</i>.
Tiered Storage Manager operations cannot be performed because an error occurred in the repository.	The repository cannot be accessed because an error occurred in the database where the repository is stored.	Restore a backed up repository.

Log data output by Tiered Storage Manager

If an error occurs in Tiered Storage Manager, you can check the error logs to help you determine the appropriate action to take. There are logs intended for use by system administrators, logs intended for use by Tiered Storage Manager GUI or CLI users, and logs intended for use by maintenance personnel.

[Table 4-2: Log types and relevant users](#) lists the types of logs to which data is output during operation of Tiered Storage Manager, and who each type of log is intended to be used by.

Table 4-2: Log types and relevant users

Log type	For reference by system administrators and GUI or CLI Users	For reference by maintenance personnel
Message log	Y	Y
Trace log	N	Y
Command trace log	N	Y
Command log	Y	Y
Service request reception log	Y	Y
Integrated log	Y	Y
Audit log	Y	Y
Legend: Y: Intended for use N: Not intended for use		

Integrated logs are log files shared by all Hitachi Storage Command products and provided by Common Component. For details, see [Integrated logging](#). For details about audit logs, see [Audit log data](#).

This section describes the content and format of data output to the above logs, except for integrated logs and audit logs.

Log types

This section describes the output contents and output destinations of each log.

Message logs

The message logs consist of records of executed processes and the results of those processes. The message logs contain more detailed log data than the Hitachi Storage Command Suite common logs. System administrators and GUI or CLI users view the message logs. Sometimes messages are output to a message log but do not appear in the GUI or CLI. If there is a problem with operation, but no message is output to the GUI or CLI, examine the message logs. Additionally, the system administrator needs to periodically view the message logs to check whether the system has errors.

[Table 4-3: File name and output destination for message logs](#) shows the log file name and output destination for message logs.

Table 4-3: File name and output destination for message logs

Log type	Log file name	Output destination
HTSM server message log	HTSMServerMessage.log#1	In Windows: <i>installation-folder-of-the-Tiered-Storage-Manager-server\logs</i> In Solaris or Linux#2: <i>/var/installation-directory-of-the-Tiered-Storage-Manager-server/logs</i>

Log type	Log file name	Output destination
#1	<p><i>n</i> indicates a number from 1 to the value specified for <code>logger.serverMessageFileCount</code> in the <code>logger.properties</code> environment settings file. For details, see Configuring environment settings related to log output.</p>	
#2	<p>In Solaris 8, Solaris 9, and Solaris 10 (SPARC edition), the following directory is fixed as the log output destination:</p> <p><code>/var/opt/HiCommand/TieredStorageManager/logs</code></p>	

Trace logs

The trace logs consist of information to be collected and used in investigations of errors. Maintenance personnel view the trace logs.

[Table 4-4:File name and output destination for the trace logs](#) shows the log file name and output destination for the trace logs.

Table 4-4: File name and output destination for the trace logs

Log type	Log file name	Output destination
HTSM server trace log	HTSMServerTracen.log#1	<p>In Windows: <i>installation-folder-of-the-Tiered-Storage-Manager-server\logs</i></p> <p>In Solaris or Linux#2: <i>/var/installation-directory-of-the-Tiered-Storage-Manager-server/logs</i></p>
#1	<p><i>n</i> indicates a number from 1 to the number which is specified in the environment settings. To specify the number, change the value of <code>logger.serverTraceFileCount</code> in the <code>logger.properties</code> environment settings file. For details, see Configuring environment settings related to log output.</p>	
#2	<p>In Solaris 8, Solaris 9, and Solaris 10 (SPARC edition), the following directory is fixed as the log output destination:</p> <p><code>/var/opt/HiCommand/TieredStorageManager/logs</code></p>	

Command trace logs

The command trace logs consist of information from command error messages. Log data is output to the command trace logs before it is output to message logs or trace logs. Maintenance personnel refer to the command trace logs.

[Table 4-5:File name and output destination for the command trace logs](#) shows the log file name and output destination for the command trace logs.

Table 4-5: File name and output destination for the command trace logs

Log type	Log file name	Output destination
Command trace log	commandTrace n .log $\#$	<i>installation-folder-of-the-Tiered-Storage-Manager-server\logs</i>
# n is replaced by 1 or 2. Command trace log data is not created until an error occurs.		

Command log

The command log consists of information from command error messages. Log data is output to the command log before it can be output to message logs or trace logs. The output consists primarily of error messages caused by errors in the environment settings. The command log is intended for use by system administrators.

Table 4-6:File name and output destination for the command log shows the log file name and output destination for the command log.

Table 4-6: File name and output destination for the command log

Log type	Log file name	Output destination
Command log	command.log	In Windows: <i>installation-folder-of-the-Tiered-Storage-Manager-server\logs</i> In Solaris or Linux $\#$: <i>/var/installation-directory-of-the-Tiered-Storage-Manager-server/logs</i>
# In Solaris 8, Solaris 9, and Solaris 10 (SPARC edition), the following directory is fixed as the log output destination: <i>/var/opt/HiCommand/TieredStorageManager/logs</i>		

Service request reception log

The service request reception log consists of information from when the Tiered Storage Manager server starts. If the environment settings for starting the services are incorrect, an error message is output to the service request reception log. The service request reception log is intended for use by system administrators.

Table 4-7:File name and output destination for the service request reception log shows the log file name and output destination for the service request reception log:

Table 4-7: File name and output destination for the service request reception log

Log type	Log file name	Output destination
Service request reception log	booting.log	In Windows: <i>installation-folder-of-the-Tiered-Storage-Manager-server\logs</i> In Solaris or Linux [#] : <i>/var/installation-directory-of-the-Tiered-Storage-Manager-server/logs</i>
# In Solaris 8, Solaris 9, and Solaris 10 (SPARC edition), the following directory is fixed as the log output destination: <i>/var/opt/HiCommand/TieredStorageManager/logs</i>		

Output format

This section describes the format for each type of log data entry.

Integrated trace log entries, message log entries, and trace log entries

The following describes the output format of integrated trace log entries, message log entries, and trace log entries.

Output format

*sequence-number date time program-name process-ID thread-ID
message-ID event-type user-ID message-text*

Output items

Table 4-8: Output items for integrated trace log entries, message log entries, and trace log entries

Output item	Details	Length (byte)
<i>sequence-number</i>	Sequence number of the log data	4
<i>date</i>	Log data output date in <i>yyyy/mm/dd</i> format. <ul style="list-style-type: none"> <i>yyyy</i>: Year <i>mm</i>: Month <i>dd</i>: Day 	10
<i>time</i>	Log data output time in <i>hh:mm:ss.sss</i> format. <ul style="list-style-type: none"> <i>hh</i>: Hour <i>mm</i>: Minute <i>ss.sss</i>: Second and millisecond 	12
<i>program-name</i>	Component name or command name of Tiered Storage Manager. Examples of component names: <ul style="list-style-type: none"> <i>HTSMServer</i>: Tiered Storage Manager server <i>HTSMGui</i>: Tiered Storage Manager Web client <i>HTSMcli</i>: Tiered Storage Manager CLI client 	16

Output item	Details	Length (byte)
<i>process-ID</i>	ID, in hexadecimal format, of the process that output the log data.	8
<i>thread-ID</i>	ID, in hexadecimal format, of the thread that output the log data.	8
<i>message-ID</i>	Message ID and message type in <code>KATS ppmmm-z</code> format. <ul style="list-style-type: none"> <code>KATS</code>: Message ID <code>pp</code>: Output source of the message <code>mmm</code>: Sequence number of the message <code>z</code>: Message type For details, see Log contents .	16
<i>event-type</i>	Type of event that output the log data. For details, see Log contents .	4
<i>user-ID</i>	User ID, output in <code>UserID:xxxx</code> format, for the user who executed the operation for which the log data was output. The user ID might not be output, depending on the type of operation.	Variable length
<i>message-text</i>	Message text.	4,095

Output example

```
6992 2005/03/01 12:00:00.000 HTSMSTServer 005D56D5 00C354E6
KATS50102-I OC UserID:system The migration group was
created.(storage domain name: "Domain_001", migration group
name: "Mig01")
```

Event log entries

[Figure 4-2:Format of an event log entry](#) shows the output format for an event log entry.

Output format

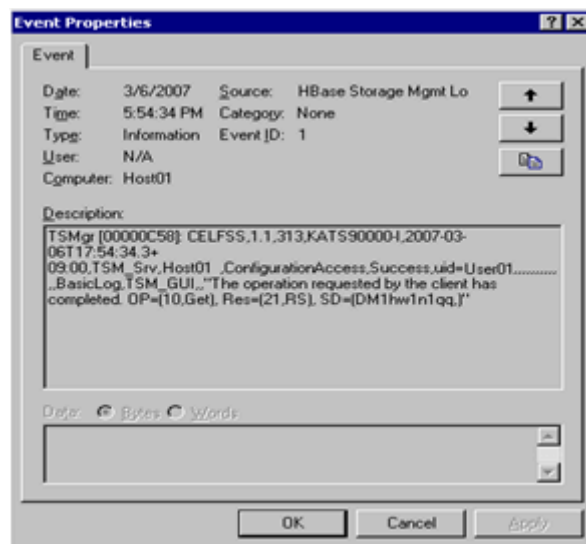


Figure 4-2: Format of an event log entry

Table 4-9: Output items of an event log entry

Output item	Details
<i>Date</i>	Log output date in <i>mm/dd/yyyy</i> format. <ul style="list-style-type: none"> <i>yyyy</i>: Year <i>mm</i>: Month <i>dd</i>: Day
<i>Time</i> [#]	Outputs the time (in the <i>hh:mm:ss</i> format) when the log was output. <ul style="list-style-type: none"> <i>hh</i>: Hour <i>mm</i>: Minute <i>ss</i>: Second
<i>Type</i>	Log type <ul style="list-style-type: none"> Information Warning Error
<i>User</i>	Always output as N/A.
<i>Computer</i>	Name of the computer for which the log was output.
<i>Source</i>	Always output as HBase Storage Mgmt Log.
<i>Category</i>	Always output as None.
<i>Event-ID</i>	Always output as 1.
<i>Description</i>	Content of the message, in HTSM[<i>pid</i>] : KATS ppmmm-z message format. <ul style="list-style-type: none"> <i>pid</i>: ID, in hexadecimal format, of the process that output the log. KATS: Message ID <i>pp</i>: Output source of the message <i>mmm</i>: Sequence number of the message <i>z</i>: Message type <i>message</i>: Message text For details, see Log contents .
[#]	The output contents might be different depending on the environment used.

syslog entries

The following describes the output format of a syslog entry.

Output format

date time host-name application-name [syslog-options] error-message

Output items

Table 4-10: Output items of syslog entries

Output item	Details
<i>date</i>	Log output date in <i>Mmm dd</i> format. <ul style="list-style-type: none"> <i>Mmm</i>: Month <i>dd</i>: Day
<i>time</i>	Log output time in <i>hh:mm:ss</i> format. <ul style="list-style-type: none"> <i>hh</i>: Hour <i>mm</i>: Minute <i>ss</i>: Second
<i>host-name</i>	Host name
<i>application-name</i>	The application name, output as HTSM[<i>proc-ID</i>]. <ul style="list-style-type: none"> <i>proc-ID</i>: Process ID
<i>syslog-options</i>	The syslog options.
<i>error-message</i>	The contents of the error.

Output example

```
Sep 1 13:41:02 fire3 HTSM[600]: [ID 702911 user.error]
KATS41006-E An attempt to start Tiered Storage Manager has
failed.

Sep 5 09:04:43 fire3 HTSM[7300]: [ID 702911 user.error]
KATS68020-E You cannot login because authentication failed or
you do not have login permission.
```

Command trace log entries

The following describes the format of command trace log entries.

Output format

date time : command-name message-text

Output items**Table 4-11: Output items of command trace log entries**

Output item	Details
<i>date</i>	Log output date in <i>yyyy/mm/dd</i> format: <ul style="list-style-type: none"> <i>yyyy</i>: Year <i>mm</i>: Month <i>dd</i>: Day
<i>time</i>	Log output time in <i>hh:mm:ss.xxx</i> format: <ul style="list-style-type: none"> <i>hh</i>: Hour <i>mm</i>: Minute <i>ss</i>: Second <i>xxx</i>: Millisecond
<i>command-name</i>	Name of the command that caused the error.
<i>message-text</i>	Message text. If a message ID exists, both the message ID and message text are output.

Output example

```
2007/10/30 14:54:01.671 htssmodhdvdfixuser.bat systemcall
error. HtssServerCommandUtli.cpp:486 , CreateProcess=2
```

Command logs

The following describes the format of command log entries.

Output format

message-ID message-text

Output items

Table 4-12: Output items of command log entries

Output item	Details	Length (byte)
<i>message-ID</i>	Message ID and message type, in <i>KATS ppmmm-z</i> format. <ul style="list-style-type: none">• <i>KATS</i>: Message ID• <i>pp</i>: Output source of the message• <i>mmm</i>: Sequence number of the message• <i>z</i>: Message type For details, see Log contents .	16
<i>message-text</i>	Message text	4,095

Output example

```
KATS41152-E A property value is invalid. Reading of the
property file will now stop. (file name:server.properties,
key:server.rmi.port)
```

Service request reception log entries

The following describes the format of service request reception log entries.

Output format

date time message-text

Output items

Table 4-13: Output items for service request reception log entries

Output item	Details
<i>date</i>	Log output date in <i>yyyy/mm/dd</i> format. <ul style="list-style-type: none">• <i>yyyy</i>: Year• <i>mm</i>: Month• <i>dd</i>: Day
<i>time</i>	Log output time in <i>hh:mm:ss.xxx</i> format. <ul style="list-style-type: none">• <i>hh</i>: Hour• <i>mm</i>: Minute• <i>ss</i>: Second• <i>xxx</i>: Millisecond

Output item	Details
<i>message-text</i>	Message text. If a message ID exists, both the message ID and message text are output.

Output example

```
2007/03/01 12:00:00.000 KATS40901-I A start request for the
Tiered Storage Manager service was received.
2007/03/01 12:00:02.016 SCM_REQUEST = INTERROGATE2007/03/01
12:00:07.422 KATS40902-I The Tiered Storage Manager service
started.
```

Log contents

This section describes the following log output items:

- Message ID and message type
- Event type

Message ID and message type

Messages produced by Tiered Storage Manager consist of a message ID that identifies the message, an indicator of the message type, and the message text.

The following describes the format of the message ID and message type indicator, and the meanings of the elements that constitute the message ID and message type.

KATS*ppmmm-z*

KATS

Indicates that the message is produced by Tiered Storage Manager.

pp

Indicates the output source of the message. The following lists the correspondences between the numbers and output sources:

- 00 Message for tracing
- 10 - 19 Message from the CLI client
- 20 - 39 Message from the Web client
- 40 - 90 Message from the Tiered Storage Manager server

mmm

Indicates the sequence number of the message.

z

Indicates the message type. [Table 4-14:Message types](#) shows the message types that can be output.

Table 4-14: Message types

Message type	Type	Description
I	Information	Processing was successful.
W	Warning	Processing continues, but a warning is issued. Refer to the warning message and check to see if there are any problems.
E	Error	Processing cannot continue due to an error.

Event type

The type of event that caused the log data to be output is output to an integrated trace log, message log, and trace log.

Table 4-15: Event type shows the event types that can be output.

Table 4-15: Event type

Event type	Time when the log data is output
OC	When an object is created
OD	When an object is destroyed
FB	When a method begins
FE	When a method ends
EC	When an exception occurs
ER	When an error occurs
PB	When called from another program
PE	When returning a value to another program
No type	Other than the above (an event type does not exist)

Integrated logging

In Common Component, you can use an integrated logging function to output all Hitachi Storage Command Suite log data into separate log files. This section describes the output destination of the log data that is intended for use by system administrators and explains how to specify the number and the size of log files.

Integrated log output

Common log files and a common library used for log data output are provided by Common Component for all program products in the Hitachi Storage Command Suite. Tiered Storage Manager uses this information to display log file details.

Table 4-16: Integrated log data output

Log type	Log file name	Description	Folder (Windows)	Directory (Solaris or Linux)
Hitachi Storage Command Suite Common trace log file	hntr2*.log	Integrated trace log data produced by Common Component. The asterisk (*) in the file name indicates a file number. For details on specifying the number and size of files, see Common Component trace log properties .	c:\Program Files\Hitachi\HNTRLib2\spool	/var/opt/hitachi/HNTRLib2/spool
Event log/ syslog file	AppEvent. EVT	In Windows, particularly important message log data is output to an event log. The event logs can be viewed in Windows by choosing Computer Management, System Tools , and then Event Viewer .	Event viewer	N/A
	messages	In Solaris or Linux, particularly important message log data is output to syslog.	N/A	Defined by /etc/syslog.conf

Common Component trace log properties

Specifying the number of trace log files

You can specify the number of trace log files, up to a maximum of 16. Large numbers of trace log files can make it difficult to find specific information.



WARNING: Changing the common trace log settings affects other program products that use the common trace log.

To specify the number of trace log files:

- In Windows:
 1. Log in to the system as a user with Administrator privileges.
 2. Execute `hntr2util.exe`.

The Windows HNTRLib2 utility is stored in the following location:

Windows-system-drive: \Program Files\Hitachi\HNTRLib2\bin\hntr2util.exe

The Hitachi Network Objectplaza Trace Utility 2 dialog box appears.

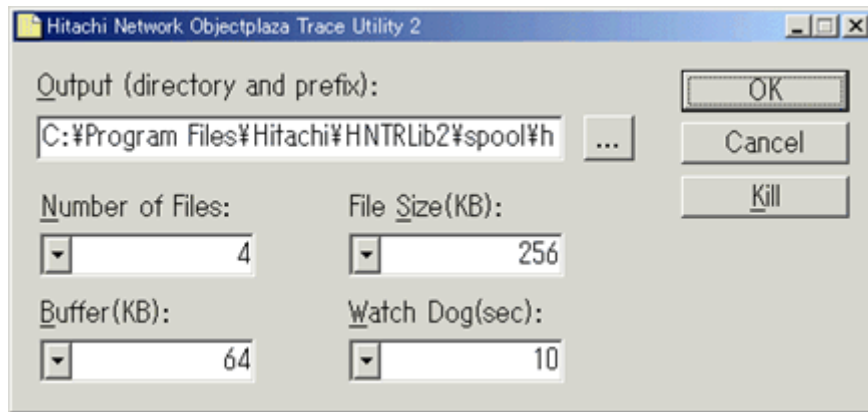


Figure 4-3: Hitachi Network Objectplaza Trace Utility 2 dialog box

3. Enter the desired number of trace log files, and then select **OK**.

- In Solaris or Linux:

1. Log in to the system as a user with root permissions.

2. Execute `hntr2util`

This utility program is stored in the following location:

```
/opt/hitachi/HNTRLib2/bin/hntr2util
```

A menu appears.

3. On the menu, choose **Number of log files**.

A submenu appears.

```
Hitachi Network Objectplaza Trace Library 2 - Configuration
Utility Rel 1.0
Type the number of files [1-16] (Type '!' to return)
Current Number: 4
New Number:
```

4. On the submenu, enter the desired number of trace log files, and then type '!'.

5. Accept the confirmation message to change the number of files, or press **E** to exit without saving your changes.

Specifying the size of trace log files

You can specify a size from 8 KB to 4 MB (4,096 KB) for each Common Component trace log file. The Common Component trace log monitoring program switches to the next file when the current output file reaches the specified size. The value should be greater than the value that you have set in the buffer.



WARNING: Changing the Common Component trace log settings affects other program products that use the common trace log.

To change the size of the trace log files:

- In Windows:

1. Log in to the system as a user with Administrator privileges.

2. Execute `hntr2util.exe`.

The Windows HNTRLib2 utility is stored in the following location:

Windows-system-drive: \Program
Files\Hitachi\HNTRLib2\bin\hntr2util.exe

The Hitachi Network Objectplaza Trace Utility 2 dialog box appears (see [Figure 4-3:Hitachi Network Objectplaza Trace Utility 2 dialog box](#)).

3. Enter the desired size for the trace log files, and then select **OK**.

- In Solaris or Linux:

1. Log in to the system as a user with root permissions.

2. Execute `hntr2util`

The utility program is stored on the following path:

`/opt/hitachi/HNTRLib2/bin/hntr2util`

A menu appears.

3. On the menu, choose **Size of a log file**.

A submenu appears.

```
Hitachi Network Objectplaza Trace Library 2 - Configuration
Utility Rel 1.0
Type new file size [8-4096] (Type '!' to return)
Current Size (KB): 256
New Size (KB):
```

4. On the submenu, enter the desired size for trace log files, and then type **!**.

5. Accept the confirmation message to change the size of the files, or select **E** to exit without saving your changes.

Audit log data

This section explains the audit log data that Tiered Storage Manager can generate. For details about audit logs data of other products, see the manuals for the respective products.

Audit log objectives

The following are the three objectives of generating audit log data.

- Regulatory compliance

You need an audit log to prove to auditors and evaluators compliance with regulations, security evaluation standards, and other business standards.

- Retention of data evidence

You can use an audit log to clarify where responsibility lies or the causes of incidents or errors that might occur.

- Collection of information required for operations

You need various types of audit log data, including activity log data and operation log data, for systems operations such as error monitoring and security incident response.

Event descriptions

This section explains the timing of audit events for each log data type. Tiered Storage Manager outputs the following four types of audit log data:

- `StartStop`
This is output when the SSO server starts or stops.
- `Authentication`
This is output whenever logon or logout succeeds, or logon or authentication fails.
- `ConfigurationAccess`
This is output when a user accesses the resources managed by Tiered Storage Manager.
- `AccessControl`
This is output when a user's attempt to access to the resources managed by Tiered Storage Manager fails due to lack of execution permission.

Events output to the audit log

[Table 4-17: Audit events output to the audit log](#) lists and describes the types of audit log data and the audit events within those types that are output to the audit log for Tiered Storage Manager. Each audit event is assigned a severity level.

Table 4-17: Audit events output to the audit log

Type	Type description	Audit event	Severity	Message ID
StartStop	Start and stop of software	Successful SSO server start	6	KAPM00090-I
		Failed SSO server start	3	KAPM00091-E
		SSO server stop	6	KAPM00092-I

Type	Type description	Audit event	Severity	Message ID
Authentication	Administrator or end user authentication	Successful logon	6	KAPM01124-I
		Successful logon (external authentication server logon)	6	KAPM02450-I
		Failed logon (wrong user ID or password)	4	KAPM02291-W
		Failed logon (logged on as a locked user)	4	KAPM02291-W
		Failed logon (logged on as a non-existing user)	4	KAPM02291-W
		Failed logon (no permission)	4	KAPM01095-E
		Failed logon (authentication failed)	4	KAPM01125-E
		Failed logon (Authentication by an external authentication server failed.)	4	KAPM02451-W
		Successful logout	6	KAPM08009-I
	Automatic account lock	Account automatically locked (Authentication repeatedly failed or account expired.)	4	KAPM02292-W
Configuration Access	User registration (GUI)	Successful user registration	6	KAPM07230-I
		Failed user registration	3	KAPM07240-E

Type	Type description	Audit event	Severity	Message ID
	User deletion (GUI)	Successful single user deletion	6	KAPM07231-I
		Failed single user deletion	3	KAPM07240-E
		Successful multiple user deletion	6	KAPM07231-I
		Failed multiple user deletion	3	KAPM07240-E
	Password change (from the administrator panel)	Successful password change by the administrator	6	KAPM07232-I
		Failed password change by the administrator	3	KAPM07240-E
	Password change (from the user's own panel)	Failed authentication processing to verify old password	3	KAPM07239-E
		Successful change of login user's own password (from the user's own panel)	6	KAPM07232-I
		Failed change of login user's own password (from the user's own panel)	3	KAPM07240-E
	Profile change	Successful profile change	6	KAPM07233-I
		Failed profile change	3	KAPM07240-E
	Permission change	Successful permission change	6	KAPM02280-I
		Failed permission change	3	KAPM07240-E
	Account lock	Successful account lock ^{#1}	6	KAPM07235-I
		Failed account lock	3	KAPM07240-E

Type	Type description	Audit event	Severity	Message ID
	Account lock release	Successful account lock release #2	6	KAPM07236-I
		Failed account lock release	3	KAPM07240-E
		Successful account lock release using the <code>hcmdsunlockac</code> count command	6	KAPM07236-I
		Failed account lock release using the <code>hcmdsunlockac</code> count command	3	KAPM07240-E
	Authentication method change	Successful authentication method change	6	KAPM02452-I
		Failed authentication method change	3	KAPM02453-E
	Authorization group addition (GUI)	Successful addition of an authorization group	6	KAPM07247-I
		Failed addition of an authorization group	3	KAPM07248-E
	Authorization group deletion (GUI)	Successful deletion of one authorization group	6	KAPM07249-I
		Failed deletion of one authorization group	3	KAPM07248-E
		Successful deletion of multiple authorization groups	6	KAPM07249-I
		Failed deletion of multiple authorization groups	3	KAPM07248-E

Type	Type description	Audit event	Severity	Message ID
	Authorization group permission change (GUI)	Successful change of an authorization group's permission	6	KAPM07250-I
		Failed change of an authorization group's permission	3	KAPM07248-E
	User registration (GUI and CLI)	Successful registration of user	6	KAPM07241-I
		Failed user registration	3	KAPM07242-E
	User information update(GUI and CLI)	Successful update of user information	6	KAPM07243-I
		Failed update of user information	3	KAPM07244-E
	User deletion (GUI and CLI)	Successful deletion of user	6	KAPM07245-I
		Failed user deletion	3	KAPM07246-E
	Authorization group registration (GUI and CLI)	Successful registration of an authorization group	6	KAPM07251-I
		Failed registration of an authorization group	3	KAPM07252-E
	Authorization group deletion (GUI and CLI)	Successful deletion of an authorization group	6	KAPM07253-I
		Failed deletion of an authorization group	6	KAPM07254-E

Type	Type description	Audit event	Severity	Message ID
	Authorization group permission change (GUI and CLI)	Successful change of an authorization group's permission	6	KAPM07255-I
		Failed change of an authorization group's permission	3	KAPM07256-E
	Database backup or restore	Successful backup using the <code>hcmsdbackup</code> command	6	KAPM05561-I
		Failed backup using the <code>hcmsdbackup</code> command	3	KAPM05562-E
		Successful full restore using the <code>hcmsdb</code> command	6	KAPM05563-I
		Failed full restore using the <code>hcmsdb</code> command	3	KAPM05564-E
		Successful partial restore using the <code>hcmsdb</code> command	6	KAPM05565-I
		Failed partial restore using the <code>hcmsdb</code> command	3	KAPM05566-E
	Database input/output	Successful data output using the <code>hcmsdbmove</code> command	6	KAPM06543-I
		Failed data output using the <code>hcmsdbmove</code> command	3	KAPM06544-E
		Successful data input using the <code>hcmsdbmove</code> command	6	KAPM06545-I

Type	Type description	Audit event	Severity	Message ID
	Database area creation of deletion	Failed data input using the <code>hcmdsdbmove</code> command	3	KAPM06546-E
		Successful database area creation using the <code>hcmdsdbsetup</code> command	6	KAPM06348-I
		Failed database area creation using the <code>hcmdsdbsetup</code> command	3	KAPM06349-E
		Successful database area deletion using the <code>hcmdsdbsetup</code> command	6	KAPM06350-I
		Failed database area deletion using the <code>hcmdsdbsetup</code> command	3	KAPM06351-E
	Authentication data input/output	Successful data output using the <code>hcmdsauthmove</code> command	6	KAPM05832-I
		Failed data output using the <code>hcmdsauthmove</code> command	3	KAPM05833-E
		Successful data input using the <code>hcmdsauthmove</code> command	6	KAPM05834-I
		Failed data input using the <code>hcmdsauthmove</code> command	3	KAPM05835-E
	Acquisition of storage domain information	Successful acquisition of all storage domain information	6	KATS90000-I
		Failed acquisition of storage domain information	4	KATS90001-W

Type	Type description	Audit event	Severity	Message ID
		Successful acquisition of storage domain information	6	KATS90000-I
		Failed acquisition of storage domain information	4	KATS90001-W
		Successful acquisition of all storage domain summary information	6	KATS90000-I
		Failed acquisition of all storage domain summary information	4	KATS90001-W
		Successful acquisition of storage domain summary information	6	KATS90000-I
		Failed acquisition of storage domain summary information	4	KATS90001-W
		Successful acquisition of storage domain refresh status	6	KATS90000-I
		Failed acquisition of storage domain refresh status	4	KATS90001-W
	Acquisition of license information	Successful acquisition of license information	6	KATS90000-I
		Failed acquisition of license information	4	KATS90001-W
	Acquisition of migration group information	Successful acquisition of all migration group information	6	KATS90000-I
		Failed acquisition of all migration group information	4	KATS90001-W

Type	Type description	Audit event	Severity	Message ID
		Successful acquisition of migration group information	6	KATS90000-I
		Failed acquisition of migration group information	4	KATS90001-W
		Successful acquisition of all migration group summary information	6	KATS90000-I
		Failed acquisition of all migration group summary information	4	KATS90001-W
		Successful acquisition of migration group summary information	6	KATS90000-I
		Failed acquisition of migration group summary information	4	KATS90001-W
	Acquisition of storage subsystem information	Successful acquisition of storage subsystem information	6	KATS90000-I
		Failed acquisition of storage subsystem information	4	KATS90001-W
		Successful acquisition of emulation type information	6	KATS90000-I
		Failed acquisition of emulation type information	4	KATS90001-W

Type	Type description	Audit event	Severity	Message ID
	Acquisition of task information	Successful acquisition of all task information	6	KATS90000-I
		Failed acquisition of all task information	4	KATS90001-W
		Successful acquisition of task information	6	KATS90000-I
		Failed acquisition of task information	4	KATS90001-W
		Successful acquisition of all task summary information	6	KATS90000-I
		Failed acquisition of all task summary information	4	KATS90001-W
		Successful acquisition of task summary information	6	KATS90000-I
		Failed acquisition of task summary information	4	KATS90001-W

Type	Type description	Audit event	Severity	Message ID
	Acquisition of storage tier information	Successful acquisition of all storage tier information	6	KATS90000-I
		Failed acquisition of all storage tier information	4	KATS90001-W
		Successful acquisition of storage tier information	6	KATS90000-I
		Failed acquisition of storage tier information	4	KATS90001-W
		Successful acquisition of all storage tier summary information	6	KATS90000-I
		Failed acquisition of all storage tier summary information	4	KATS90001-W
		Successful acquisition of storage tier summary information	6	KATS90000-I
		Failed acquisition of storage tier summary information	4	KATS90001-W
	Acquisition of volume information, or check of volumes to be allocated to storage	Successful acquisition of volume information	6	KATS90000-I
		Failed acquisition of volume information	4	KATS90001-W
		Successful acquisition of volume summary information	6	KATS90000-I

Type	Type description	Audit event	Severity	Message ID
		Failed acquisition of volume summary information	4	KATS90001-W
		Successful check of volumes to be allocated to storage	6	KATS90000-I
		Failed check of volumes to be allocated to storage	4	KATS90001-W
		Successful check of volumes whose allocation to storage is to be canceled	6	KATS90000-I
		Failed check of volumes whose allocation to storage is to be canceled	4	KATS90001-W
		Successful acquisition of the number of volumes in a search result	6	KATS90000-I
		Failed acquisition of the number of volumes in a search result	4	KATS90001-W
		Successful acquisition of volume range information	6	KATS90000-I
		Failed acquisition of volume range information	4	KATS90001-W
	Acquisition of pool information	Successful acquisition of pool information	6	KATS90000-I
		Failed acquisition of pool information	4	KATS90001-W

Type	Type description	Audit event	Severity	Message ID
		Successful acquisition of the number of pools in a search result	6	KATS90000-I
		Failed acquisition of the number of pools in a search result	4	KATS90001-W
	Acquisition of keystore file information	Successful acquisition of keystore file information	6	KATS90000-I
		Failed acquisition of keystore file information	4	KATS90001-W
	Acquisition of volume information	Successful acquisition of volume information	6	KATS90000-I
		Failed acquisition of volume information	4	KATS90001-W
		Successful acquisition of the number of volumes in a search result	6	KATS90000-I
		Failed acquisition of the number of volumes in a search result	4	KATS90001-W
		Successful acquisition of volume range information	6	KATS90000-I
		Failed acquisition of volume range information	4	KATS90001-W
	Acquisition of free space information	Successful acquisition of free space information	6	KATS90000-I
		Failed acquisition of free space information	4	KATS90001-W

Type	Type description	Audit event	Severity	Message ID
		Successful acquisition of free space range information	6	KATS90000-I
		Failed acquisition of free space range information	4	KATS90001-W
		Successful acquisition of the number of free spaces in a search result	6	KATS90000-I
		Failed acquisition of the number of free spaces in a search result	4	KATS90001-W
	Acquisition of external connection settings	Successful acquisition of external connection settings	6	KATS90000-I
		Failed acquisition of external connection settings	4	KATS90001-W
		Successful acquisition of path group information	6	KATS90000-I
		Failed acquisition of path group information	4	KATS90001-W
	Storage domain operations	Successful registration of a storage domain	6	KATS90000-I
		Failed registration of a storage domain	4	KATS90001-W
		Successful deletion of a storage domain	6	KATS90000-I
		Failed deletion of a storage domain	4	KATS90001-W

Type	Type description	Audit event	Severity	Message ID
		Successful update of storage domain information	6	KATS90000-I
		Failed update of storage domain information	4	KATS90001-W
		Successful update of a storage domain	6	KATS90000-I
		Failed update of a storage domain	4	KATS90001-W
	Update of information about operated volumes	Successful update of information about operated volumes	6	KATS90000-I
		Failed update of information about operated volumes	4	KATS90001-W
	Addition of licenses	Successful license addition	6	KATS90000-I
		Failed license addition	4	KATS90001-W
	Migration group operations	Successful volume addition to a migration group	6	KATS90000-I
		Failed volume addition to a migration group	4	KATS90001-W
		Successful acquisition of the list of storage tiers that can be specified as migration destinations	6	KATS90000-I
		Failed acquisition of the list of storage tiers that can be specified as migration destinations	4	KATS90001-W

Type	Type description	Audit event	Severity	Message ID
		Successful registration of a migration group	6	KATS90000-I
		Failed registration of a migration group	4	KATS90001-W
		Successful deletion of a migration group	6	KATS90000-I
		Failed deletion of a migration group	4	KATS90001-W
		Successful update of migration group information	6	KATS90000-I
		Failed update of migration group information	4	KATS90001-W
		Successful creation of a migration plan	6	KATS90000-I
		Failed creation of a migration plan	4	KATS90001-W
		Successful deletion of a migration plan	6	KATS90000-I
		Failed deletion of a migration plan	4	KATS90001-W
	Task operations	Successful task cancellation	6	KATS90000-I
		Failed task cancellation	4	KATS90001-W
		Successful task status change	6	KATS90000-I
		Failed task status change	4	KATS90001-W
		Successful registration of a migration task	6	KATS90000-I
		Failed registration of a migration task	4	KATS90001-W
		Successful task registration	6	KATS90000-I
		Failed task registration	4	KATS90001-W

Type	Type description	Audit event	Severity	Message ID
		Successful task deletion	6	KATS90000-I
		Failed task deletion	4	KATS90001-W
		Successful task execution	6	KATS90000-I
		Failed task execution	4	KATS90001-W
		Successful update of task information	6	KATS90000-I
		Failed update of task information	4	KATS90001-W
	Storage tier operations	Successful registration of a storage tier	6	KATS90000-I
		Failed registration of a storage tier	4	KATS90001-W
		Successful deletion of a storage tier	6	KATS90000-I
		Failed deletion of a storage tier	4	KATS90001-W
		Successful update of storage tier information	6	KATS90000-I
		Failed update of storage tier information	4	KATS90001-W
AccessControl	Storage domain operation failure	No permission to create a storage domain	4	KATS90010-W
		No permission to delete a storage domain	4	KATS90010-W
		No permission to change a storage domain	4	KATS90010-W
		No permission to refresh a storage domain	4	KATS90010-W

Type	Type description	Audit event	Severity	Message ID
	Storage tier operation failure	No permission to create a storage tier	4	KATS90010-W
		No permission to delete a storage tier	4	KATS90010-W
		No permission to change a storage tier	4	KATS90010-W
	Migration group operation failure	No permission to create a migration group	4	KATS90010-W
		No permission to delete a migration group	4	KATS90010-W
		No permission to change a migration group	4	KATS90010-W
		No permission to add volumes to a migration group	4	KATS90010-W
		No permission to delete volumes from a migration group	4	KATS90010-W
		Task operation failure	No permission to create a task	4
	No permission to delete a task		4	KATS90010-W
	No permission to change a task		4	KATS90010-W
	No permission to execute a task		4	KATS90010-W
	No permission to cancel a task		4	KATS90010-W
	No permission to stop a task		4	KATS90010-W
#1 If an account is locked because the authentication method was changed for a user whose password is not set, this information is not recorded in the audit log.				
#2 If an account is unlocked because a password was set for a user, this information is not recorded in the audit log.				

Audit log data is output to the event log (application log) in Windows and to the `syslog` file in Solaris or Linux.

You can filter audit log data to be output according to the severity level of the audit event. [Table 4-18:Severity levels of audit events](#) shows the severity levels of audit events.

Table 4-18: Severity levels of audit events

Severity	syslog	Event log
0	Emergency	Error
1	Alert	
2	Critical	
3	Error	
4	Warning	Warning
5	Notice	Information
6	Informational	
7	Debug	

Audit log settings

To generate Tiered Storage Manager audit log data, you need to edit the environment settings file (`auditlog.conf`). Within `auditlog.conf`, if you specify the type of audit events to collect in `Log.Event.Category`, audit log data will be generated. When you change the setting values in the `auditlog.conf` file, to enable the new settings, restart Common Component and all Hitachi Storage Command Suite products.



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

In Windows

The `auditlog.conf` file is stored in the following location:

installation-folder-of-Common-Component\conf\sec\auditlog.conf

[Table 4-19:Setting Items for auditlog.conf \(in Windows\)](#) shows the items that are set for the `auditlog.conf` file.

Table 4-19: Setting Items for auditlog.conf (in Windows)

Item	Description
<code>Log.Event.Category</code>	Specify the type of audit events to be generated. When specifying multiple types, separate each type with a comma, but do not insert spaces. If this item is not specified, the audit log data is not output. For details about the available types, see Table 4-17:Audit events output to the audit log . This item is not case sensitive. If you specify an invalid type, it is ignored. Default value: (Not specified)

Item	Description
Log.Level #	Specify the maximum severity level of audit events that you want to be output. The items that have the specified severity level or lower are output. For details about the audit events that are output from Tiered Storage Manager and event severity levels, see Table 4-17: Audit events output to the audit log . If you specify an invalid numerical value or a character that is not numerical, the default value is used. Available values: 0 to 7 (severity levels) Default value: 6
#	If Log.Event.Category is not specified, then even if Log.Level is specified, nothing is output.

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

```
Log.Event.Category
StartStop,Authentication,AccessControl,ConfigurationAccess
Log.Level 6
```

In the example above, all audit log data that can be generated by Tiered Storage Manager is output.

In Solaris or Linux

The `auditlog.conf` file is stored in the following location:

installation-directory-of-Common-Component/conf/sec/auditlog.conf

[Table 4-20: Setting Items for auditlog.conf \(in Solaris or Linux\)](#) shows the items that are to be set for the `auditlog.conf` file.

Table 4-20: Setting Items for auditlog.conf (in Solaris or Linux)

Item	Description
Log.Facility	Specify the facility (by number) to be used when the audit log data is output to the <code>syslog</code> file. For details about the available values, see Table 4-21: Available values for log.facility and corresponding values in syslog.conf . If you specify a non-numeric or otherwise invalid value, the default value is used. Default value: 1
Log.Event.Category	Specify the type of audit events to be generated. When specifying multiple types, separate each type with a comma, but do not insert spaces. If this item is not specified, the audit log data is not output. For details about the available types, see Table 4-17: Audit events output to the audit log . This item is not case sensitive. If you specify an invalid type, it is ignored. Default value: (Not specified)

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

```
Log.Facility 1
Log.Event.Category
StartStop,Authentication,AccessControl,ConfigurationAccess
```

In this example above, all audit log data that can be generated by Tiered Storage Manager is output to the `syslog` file that is defined as the `user` facility in the `syslog.conf` file.

Table 4-21: Available values for log.facility and corresponding values in syslog.conf

Facility	Values specified by <code>syslog.conf</code>
1	<code>user</code>
2	<code>mail#</code>
3	<code>daemon</code>
4	<code>auth#</code>
6	<code>lpr#</code>
16	<code>local0</code>
17	<code>local1</code>
18	<code>local2</code>
19	<code>local3</code>
20	<code>local4</code>
21	<code>local5</code>
22	<code>local6</code>
23	<code>local7</code>
#	These values can be specified, but we do not recommend that you specify them.

Output format

This section describes the output format for audit log data.

Header for audit log data

The output format of the header is different between the `syslog` file and event logs.

In Windows

The format of an event log header and output information are as follows:

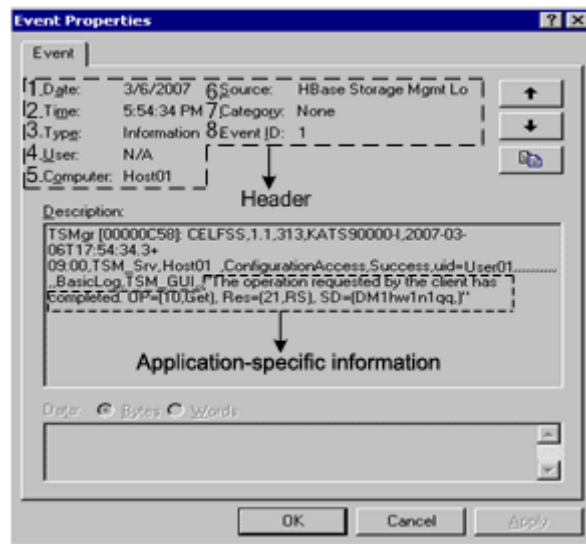


Figure 4-4: Header output format

The numbers in the screenshot correspond to the numbers in [Table 4-22:Information output to the header \(event log\)](#).

Table 4-22: Information output to the header (event log)

No.	Item	Description
1	<i>date</i>	Outputs the date (in the <i>yyyy/mm/dd</i> format) when the log data was output. <ul style="list-style-type: none"> <i>yyyy</i>: Year <i>mm</i>: Month <i>dd</i>: Day
2	<i>time[#]</i>	Outputs the time (in the <i>hh:mm:ss</i> format) when the log was output. <ul style="list-style-type: none"> <i>hh</i>: Hour <i>mm</i>: Minutes <i>ss</i>: Seconds
3	<i>type</i>	Outputs the type of log data: <ul style="list-style-type: none"> Information Warning Error
4	<i>user</i>	Outputs N/A.
5	<i>computer (detected-location)</i>	Outputs the name of the computer to which the log data was output.
6	<i>source</i>	Outputs HBase Storage Mgmt Log.
7	<i>facility</i>	Outputs None.
8	<i>event-ID</i>	Outputs 1.
[#] The output contents might be different depending on the environment used.		

In Solaris or Linux

The format of the `syslog` header and output information are as follows:

Header output format

date-and-time host-name

Table 4-23: Information output to the header (syslog)

Item	Description
<i>date-and-time</i>	This item outputs the date and time (in the <i>Mmm dd hh:mm:ss</i> format) when the log was output. <ul style="list-style-type: none">• <i>Mmm</i>: Month• <i>dd</i>: Day• <i>hh</i>: Hour• <i>mm</i>: Minutes• <i>ss</i>: Seconds
<i>host-name</i>	Host name

Output example:

Mar 2 21:39:03 Host01

Audit log messages

The formats of the audit log messages and output information are as follows:

Output format of audit log messages

- *program-name* [*process-ID*] : *uniform-identifier*, *uniform-specification-revision-number*, *serial-number*, *message-ID*, *date-and-time*, *detected-entity*, *detected-location*, *audit-event-type*, *audit-event-result*, *subject-identification-information*, *reserved-area-1*, *reserved-area-2*, *reserved-area-3*, *reserved-area-4*, *reserved-area-5*, *reserved-area-6*, *reserved-area-7*, *reserved-area-8*, *reserved-area-9*, *reserved-area-10*, *batch-operation-identifier*, *log-type-information*, *application-identifier-information*, *reserved-area-11*, "application-specific-information"

Table 4-24: Information output to audit log messages

Item #1	Description
<i>program-name</i>	Program name [process ID]
<i>uniform-identifier</i>	Fixed as CELFSS
<i>uniform-specification-revision-number</i>	Fixed as 1.1
<i>serial-number</i>	Serial number of audit log messages
<i>message-ID</i>	Message ID set by the product ^{#2}
<i>date-and-time</i>	The date and time when the message was output. This is output in the format of <i>yyyy-mm-ddThh:mm:ss.s</i> .
<i>detected-entity</i>	Fixed to TSM_Srv
<i>detected-location</i>	Host name
<i>audit-event-type</i>	StartStop, Authentication, AccessControl, ConfigurationAccess

Item #1	Description
<i>audit-event-result</i>	Event result
<i>subject-identification-information</i>	User ID (<i>uid=xxx</i>) of the user (logged-on user) or Hitachi Storage Command Suite user name. However, this is fixed as <i>TSM_Srv</i> for operations prior to logon, such as acquisition or addition of license information.
<i>reserved1-area</i>	No output. This is a reserved space.
<i>reserved2-area</i>	No output. This is a reserved space.
<i>reserved3-area</i>	No output. This is a reserved space.
<i>reserved4-area</i>	No output. This is a reserved space.
<i>reserved5-area</i>	No output. This is a reserved space.
<i>reserved6-area</i>	No output. This is a reserved space.
<i>reserved7-area</i>	No output. This is a reserved space.
<i>reserved8-area</i>	No output. This is a reserved space.
<i>reserved9-area</i>	No output. This is a reserved space.
<i>reserved10-area</i>	No output. This is a reserved space.
<i>batch-operation-identifier</i>	A common batch operation identifier for both the basic log and detailed log to associate the two logs for when they are separated during a batch operation. Integers from 0 to 2 ³² are applied in increments. Do not set this item when only a basic log exists. ^{#3}
<i>log-type-information</i>	Fixed to <i>BasicLog</i> or <i>DetailLog</i>
<i>application-identifier-information</i>	<i>TSM_GUI</i> : Request from Tiered Storage Manager Web client <i>TSM_CLI</i> : Request from Tiered Storage Manager CLI client <i>TSM_Srv</i> : Request from Tiered Storage Manager server
<i>reserved11-area</i>	No output. This is a reserved space.
<i>application-specific-information</i>	Information specific to an application, such as management operation details, operation targets, parameters, or reasons for audit events. Because this information is specific to an application, its display format cannot easily be unified with the display format of information from other applications. For details, see Table 4-26:Information output to the application specific information area .

Item #1	Description
#1	Some items are not output for some audit events.
#2	Table 4-25: Message IDs and contents output to the audit log shows the message IDs and the contents that are output to the audit log.
#3	<p>When array information is output to the message in <i>application specific information</i>, the basic log data indicating the start of the array is output first, then the detailed log data is output one line at a time for each element of the array, and finally basic log data indicating the end of the array is output.</p> <p>Output example:</p> <pre> ...,i,BasicLog,,, ".....NumSD=n, Start SDs" ...,i,DetailLog,,, "SD[1]=(domainId-1,domainName-1) " ...,i,DetailLog,,, "SD[2]=(domainId-2,domainName-2) ",i,DetailLog,,, "SD[n]=(domainId-n,domainName-n) " ...,i,BasicLog,,, "End SDs" </pre> <p>However, when the array length is 1, only basic log data is output, and the detailed log is not used.</p>

Table 4-25: Message IDs and contents output to the audit log

Message ID	Message (specific application information)	Description
KATS90000-I	The operation requested by the client has completed.	<p>If the audit log data contains multiple lines, this message appears in the first line.</p> <p>This message occurs when, due to a successful access of the resources managed by Tiered Storage Manager, an audit event of the <i>Configuration Access</i> type occurred.</p>
KATS90001-W	The operation requested by the client has failed.	<p>If the audit log data contains multiple lines, this message appears in the first line.</p> <p>This message occurs when, due to a failure in accessing resources managed by Tiered Storage Manager, an audit event of the <i>Configuration Access</i> type occurred.</p>
KATS90010-W	The user does not have permission for the operation.	<p>This message occurs when, due to a failure in accessing resources managed by Tiered Storage Manager because of a lack of execution permissions, an audit event of the <i>Access Control</i> type occurred.</p>

Message ID	Message (specific application information)	Description
KATS90020-I	Outputs the subsequent lines of the KATS90000-I message.	If the audit log data contains multiple lines, this message appears immediately following the KATS90000-I message. This message occurs when, due to successful access to the resources managed by Tiered Storage Manager, an audit event for the Configuration Access type occurred.
KATS90021-W	Outputs the subsequent lines of the KATS90001-W message.	If the audit log data contains multiple lines, this message appears immediately following the KATS90001-W message. This message occurs when, due to a failure in accessing resources managed by Tiered Storage Manager, an audit event for the Configuration Access type occurred.
KATS90030-I	Outputs the last line of the KATS90000-I message.	If the audit log data contains multiple lines, this message appears immediately following the KATS90020-I message. This message occurs when, due to successful access to the resources managed by Tiered Storage Manager, an audit event for the Configuration Access type has occurred.
KATS90031-W	Outputs the last line of the KATS90001-W message.	If the audit log data contains multiple lines, this message appears immediately following the KATS90021-W message. This message occurs when, due to a failure in accessing resources managed by Tiered Storage Manager, an audit event for the Configuration Access type occurred.

Details of application specific information

The formats of the application specific information and output information are as follows:

Output format of application specific information[#]

- "message-text operation-type (OP), operation-target (Res)[, failure-cause (RC)][, storage-domain-information (SD)][, subsystem-information (SS)][, migration-group-information (MG)][, target-migration-group-information-after-task-completion(MG_moveTo)][, storage-tier-information (ST)][, pool-information(PO)][, volume-information(VL)][, volume-pair (VP)][, free-space-information (FS)][, external-connection-settings (EM)][, path-group-information (PG)][, emulation-type-information (EM)][, task-information (TK)][, license-information (LC)][, option-per-audit-event (opt)]"

#

The item *failure-cause* (RC) and each item after *failure-cause* (RC) might not be output.

Table 4-26: Information output to the application specific information area

Item	Description	Output format
<i>message-text</i>	Message explaining the event	Message text is output.
<i>operation-type</i> (OP)	Type of operation requested for Tiered Storage Manager server: 1. Operation ID (<i>OpId</i>) 2. Operation name (<i>OpName</i>)	OP= (<i>OpId</i> , <i>OpName</i>) For details about OpId and OpName, see Table 4-27:Operation types (OP) .
<i>operation-target</i> (Res)	Type of resource for the operation: 1. Resource ID (<i>ResId</i>) 2. Resource name (<i>ResName</i>)	Res= (<i>ResId</i> , <i>ResName</i>) For details about ResId and ResName, see Table 4-28:Operation targets (Res) .

Item		Description	Output format
Additional Information	<i>failure-cause</i> (RC)	Error code indicating the cause of a failure event	RC=KATSppmm-Z For details on the message contents, see the <i>Hitachi Tiered Storage Manager Messages</i> .
	<i>storage-domain-information</i> (SD)	When a single item exists: 1. Storage domain ID (<i>id</i>) 2. Storage domain name (<i>name</i>)	SD= (<i>id</i> , <i>name</i>)
		When multiple items exist: 1. Number of elements (<i>n</i>) 2. Storage domain ID (<i>id</i>) 3. Storage domain name (<i>name</i>)	NumSD= <i>n</i> , Start SDs SD[1]= (<i>id</i> -1, <i>name</i> -1) ... SD[<i>n</i>]= (<i>id</i> - <i>n</i> , <i>name</i> - <i>n</i>) End SDs
		Number of storage domain information items (<i>n</i>)	NumSD= <i>n</i>
	<i>subsystem-information</i> (SS)	For storage domain registration: 1. Display model name (<i>model</i>) 2. Serial number (<i>serial</i>) 3. Domain controller name (<i>name</i>) 4. Logical DKC number (<i>ldkc</i>) [#]	SS= (<i>model</i> , <i>serial</i> , <i>name</i> , <i>ldkc</i>)
		For situations other than the above: 1. Subsystem name (<i>name</i>) 2. Logical DKC number (<i>ldkc</i>)	SS= (, , <i>name</i> , <i>ldkc</i>)
		Number of subsystem information items (<i>n</i>)	NumSS= <i>n</i>
	<i>Migration-group-information</i> (MG)	When a single item exists: 1. Migration group ID (<i>id</i>) 2. Migration group name (<i>name</i>)	MG= (<i>id</i> , <i>name</i>)
		When multiple items exist: 1. Number of elements (<i>n</i>) 2. Migration group ID (<i>id</i>) 3. Migration group name (<i>name</i>)	NumMG= <i>n</i> , Start MGs MG[1]= (<i>id</i> -1, <i>name</i> -1) ... MG[<i>n</i>]= (<i>id</i> - <i>n</i> , <i>name</i> - <i>n</i>) End MGs
		Number of migration group information items (<i>n</i>)	NumMG= <i>n</i>
	<i>target-migration-group-information-after-task-completion</i> (MG_moveTo)	1. Migration group ID (<i>id</i>) 2. Migration group name (<i>name</i>)	MG_moveTo= (<i>id</i> , <i>name</i>)
	<i>storage-tier-information</i> (ST)	When a single item exists: 1. Storage tier ID (<i>id</i>) 2. Storage tier name (<i>name</i>)	ST= (<i>id</i> , <i>name</i>)

Item		Description	Output format
		When multiple items exist: 1. Number of elements (<i>n</i>) 2. Storage tier ID (<i>id</i>) 3. Storage tier name (<i>name</i>)	NumST= <i>n</i> , Start STs ST[1]=(<i>id</i> -1, <i>name</i> -1) ... ST[<i>n</i>]=(<i>id</i> - <i>n</i> , <i>name</i> - <i>n</i>) End STs
		Number of storage tiers (<i>n</i>)	NumST= <i>n</i>
	<i>pool-information</i> (PO)	Storage domain ID (<i>id</i>)	SD=(<i>id</i> ,)
		Number of pools (<i>n</i>)	NumPO= <i>n</i>
	<i>volume-information</i> (VL)	When a single item exists: 1. Controller logical device number (<i>devnum</i>) 2. Object ID of LU or LDEV (<i>id</i>)	VL=(<i>devnum</i> , <i>id</i>)
		When multiple items exist: 1. Number of elements (<i>n</i>) 2. Controller logical device number (<i>devnum</i>) 3. Object ID of LU or LDEV (<i>id</i>)	NumVL= <i>n</i> , Start VLs VL[1]=(<i>devnum</i> -1, <i>id</i> -1) ... VL[<i>n</i>]=(<i>devnum</i> - <i>n</i> , <i>id</i> - <i>n</i>) End VLs
		Number of volumes (<i>n</i>)	NumVL= <i>n</i>
	<i>volume-pair</i> (VP)	When a single item exists: 1. Controller logical device number of the migration source volume (<i>sdevnum</i>) 2. Object ID of the migration source LDEV (<i>sid</i>) 3. Controller logical device number of the migration target volume (<i>tdevnum</i>) 4. Object ID of the migration target LDEV (<i>tid</i>)	VP=(<i>sdevnum</i> , <i>sid</i> , <i>tdevnum</i> , <i>tid</i>)
		When multiple items exist: 1. Number of elements (<i>n</i>) 2. Controller logical device number of the migration source volume (<i>sdevnum</i>) 3. Object ID of the migration source LDEV (<i>sid</i>) 4. Controller logical device number of the migration target volume (<i>tdevnum</i>) 5. Object ID of the migration target LDEV (<i>tid</i>)	NumVP= <i>n</i> , Start VPs VP[1]=(<i>sdevnum</i> -1, <i>sid</i> -1, <i>tdevnum</i> -1, <i>tid</i> -1) ... VP[<i>n</i>]=(<i>sdevnum</i> - <i>n</i> , <i>sid</i> - <i>n</i> , <i>tdevnum</i> - <i>n</i> , <i>tid</i> - <i>n</i>) End VPs
		Number of volume pairs	NumVP= <i>n</i>
	<i>free-space-information</i> (FS)	When a single item exists: 1. Array group name (<i>agname</i>) 2. Free space number (<i>fsnum</i>)	FS=(<i>agname</i> , <i>fsnum</i>)
		When multiple items exist: Number of free space information items	NumFS= <i>n</i>

Item		Description	Output format
	<i>external-connection-settings</i> (EM)	Number of external connection settings items	NumEM= <i>n</i>
	<i>path-group-information</i> (PG)	When a single item exists: Path group ID (<i>id</i>)	PG= (<i>id</i>)
		When multiple items exist: Number of path group information items	NumPG= <i>n</i>
	<i>emulation-type-information</i> (EM)	Number of emulation type information items	NumEM= <i>n</i>
	<i>task-information</i> (TK)	For a migration task: 1. Task ID (<i>id</i>) 2. Task type (<i>type</i>) = 0 3. Whether to erase data (<i>erase</i>) Y: Erase data. N: Do not erase data.	TK= (<i>id</i> , 0, <i>erase</i>)
		For a locking task: 1. Task ID (<i>id</i>) 2. Task type (<i>type</i>) = 2 3. Lock status (<i>mode</i>) 4. ReadOnly: Read only 5. Protect: Protected 6. Lock period (<i>days</i>)	TK= (<i>id</i> , 2, <i>mode</i> , <i>days</i>)
		For an unlocking task: 1. Task ID (<i>id</i>) 2. Task type (<i>type</i>) = 3	TK= (<i>id</i> , 3)
		For a shredding task: 1. Task ID (<i>id</i>) 2. Task type (<i>type</i>) = 4 3. Shredding method (<i>method</i>) 0: Zero once 1: DOD	TK= (<i>id</i> , 4, <i>method</i>)
		For a volume creation task: 1. Task ID (<i>id</i>) 2. Task type (<i>type</i>) = 5	TK= (<i>id</i> , 5)
		For an external connection settings task: 1. Task ID (<i>id</i>) 2. Task type (<i>type</i>) = 6	TK= (<i>id</i> , 6)

Item		Description	Output format
		For multiple types of task information: 1. Number of tasks 2. Task ID (<i>id</i>) 3. Task type (<i>type</i>) 0: Migration task 2: Locking task 3: Unlocking task 4: Shredding task 5: Volume creation task 6: External connection settings task	NumTK= <i>n</i> , Start TKs TK[1]= (<i>id</i> -1, <i>type</i> -1) ... TK[<i>n</i>]= (<i>id</i> - <i>n</i> , <i>type</i> - <i>n</i>) End TKs
	<i>license-information</i> (LC)	License status (<i>status</i>) 0: Permanent license key 1: Temporary license key 2: Emergency license key 3: Unregistered license key	LC= (<i>status</i>)
	<i>option-per-audit-event</i> (opt)	When canceling a task: Whether to perform a forced cancel (<i>emergency</i>) Y: Emergency specification N: No emergency specification	opt= (<i>emergency</i>)
		When adding volumes: Migration permission (<i>moveFromMigrationGroup</i>) Y: Permit migration N: Do not permit migration	opt= (<i>moveFromMigrationGroup</i>)
		When changing a task: 1.Task status after the change (<i>status</i>) 0x01020600: Executing a task	opt= (<i>status</i> , <i>emergency</i>)
		0x02030000: Erased 0x02040000: Stopped 0x02050000: Stopping mid-task	
		2.Whether to perform a forced change (<i>emergency</i>) Y: Emergency specification N: No emergency specification	
# Leave blank for items other than Universal Storage Platform V.			

The following are examples of audit log data output:

Example of audit log data output by Common Component:

```
UserManagement[00000974]:CELFSS,1.1,1,KAPM01124-I,2006-10-
24T21:53:43.7+09:00,
HBase-
SSO,Hostname1,Authentication,Success,uid=user01,,,,,,,,,BasicLo
g,,,
"The login process has completed properly."
```

Example of audit log data output by Tiered Storage Manager:

```
TSMgr[00000974]:CELFSS,1.1,1,KATS90000-I,2006-11-
09T19:58:45.4+09:00,TSM_Srv,
Hostname1,ConfigurationAccess,Success,uid=user01,,,,,,,,,BasicL
og,,,
"The operation requested by the client has completed.
OP=(30,Delete),
Res=(20,SD), SD=(DM1hc2idzx,Domain-A)"
```

The type of operation requested of the Tiered Storage Manager server is output to *operation-type* in the application specific information. [Table 4-27:Operation types \(OP\)](#) shows the operation IDs and operation names that are output to *operation-type*.

Table 4-27: Operation types (OP)

OpId	OpName	Meaning
10	Get	Acquire information
11	Get_summary	Acquire summary information
12	Get_num	Acquire only a count of information items
20	Create	Create
30	Delete	Delete
40	Modify	Update
50	Add	Add
60	Remove	Remove
70	Change	Change status
80	Execute	Execute
90	Refresh	Refresh
100	Cancel	Cancel
110	Stop	Stop
120	Choose	Select
130	Check	Check

[Table 4-28:Operation targets \(Res\)](#) shows the corresponding resource IDs and resource names output to the *operation-target* in the application specific information area.

Table 4-28: Operation targets (Res)

ResId	ResName	Formal name	Meaning
10	LC	License	License information
20	SD	StorageDomain	Storage domain
21	RS	RefreshStatus	Storage refresh status
30	MG	MigrationGroup	Migration group
40	ST	StorageTier	Storage tier
50	MP	MigrationPlan	Migration plan
60	SS	Subsystem	Storage subsystem
70	TK	Task	Task

ResId	ResName	Formal name	Meaning
80	VL	Volume	Volume
90	VP	VolumePair	Volume pair
100	VR	VolumeRange	Volume range information
110	LOG	LoggerInfo	Information about data output to logs
120	PO	Pool	Pool
130	KS	KeyStore	KeyStore file information
140	FS	FreeSpace	Free space
150	FSR	FreeSpaceRange	Free space range information
160	EXM	ExternalMapping	External connection settings
170	PG	PathGroup	Path group
180	EM	Emulation	Emulation

Calculating the volume of audit log data

This section explains how the volume of output audit log data is estimated based on the operations of Tiered Storage Manager.

[Table 4-29: Number of lines output to the audit log for GUI operations](#) and [Table 4-30: Number of lines output to the audit log for CLI commands](#) show the number of lines output to audit log files during GUI operations and CLI command executions. To calculate the total number of output lines, multiply the number of output lines for a particular operation by the number of times that operation is executed.

To calculate the physical size of the output data in bytes, multiply the number of output lines by one of the following:

- For event logs: 340 bytes
- For syslog: 310 bytes

However, a value obtained by following the above procedure is a rough estimate, and the actual value varies depending on the length of names or the types of operations. Therefore, we recommend that you assume a value that is 10% to 20% greater than what is obtained with the above procedure.

When calculating the volume of audit log data output by Tiered Storage Manager, take into consideration the volume of the Device Manager audit log. When calculating the bytes that are output, factor in the number of audit log lines that Device Manager outputs.

However, note that the size of the Device Manager audit log data is different from the bytes shown above.



Caution: In Windows event logs, a single character is stored as 2 bytes, therefore multiply the number of bytes calculated above by 2. However, if you save the contents of an event log as a text file (tab separated) or as a CSV file (comma separated), the size will be the same as obtained by using the above calculation.

Volume of output audit log data for each GUI operation

Table 4-29: Number of lines output to the audit log for GUI operations shows the number of lines of information output to the audit log for GUI operations of Tiered Storage Manager.

Table 4-29: Number of lines output to the audit log for GUI operations

GUI operation	Condition	Number of lines
Logging on	--	3
Creating a storage domain	--	$6 + N (+ 23 + 6 \times SS)^{\#1}$ N: Time required for refresh (seconds) / 5 seconds (rounded up to nearest second) SS: Number of subsystems that have been registered in Device Manager
Editing a storage domain	When started from the List window	4
	When started from the Details window	6
Refreshing a storage domain	When started from the Details window	$9 + N (+ 28 + 2 \times SS)^{\#1}$ N: Time required for refresh (seconds) / 5 seconds (rounded up to nearest second) SS: Number of subsystems that have been registered in Device Manager
Deleting a storage domain	--	7
Displaying a storage domain list	--	1
Displaying storage domain detailed information	Details tab	2
	Storage Tier tab	3
	Migration Group tab	3
Creating a storage tier	--	$8 + 3 \times S$ S: Number of searches
Editing a storage tier	When started from the Details window (Volume List tab)	$12 + 3 \times S$ S: Number of searches
Deleting a storage tier	When started from the List window	7
	When started from the Details window	5
Displaying a storage tier list	--	2
Displaying storage tier detailed information	Volume List tab	4
	Details tab	2

GUI operation	Condition	Number of lines
Creating a migration group	--	7 + A + N x (5 + 3 x S) A: Number of added volumes N: Number of executed operations of <i>adding volumes</i> S: Number of searches
Editing a migration group (includes adding and deleting volumes)	When started from the Details window	8 + A + D + NA x (5 + 3 x S) + ND A: Number of added volumes D: Number of deleted volumes NA: Number of executed <i>adding volumes</i> operations ND: Number of executed <i>deleting volumes</i> operations S: Number of searches
Editing a migration group (only includes changing the name or attributes)	When started from the List window	8
Deleting a migration group	When started from the List window	7
Displaying a migration group list	--	2
Displaying migration group detailed information	Volume List tab	4
	Details tab or Rules tab	2
Searching for a volume	--	4 + 3 x S S: Number of searches
Searching for a pool	--	4 + 3 x S S: Number of searches
Searching for a task	--	2
Migrate MG	When started from the Migration Group List window	12 + P (+ 2) ^{#1} P: Number of volume pairs ^{#2}
Executing a task	When started from the Task List window	4 + (4 + 8 x P + N) ^{#1} P: Number of volume pairs N: Time to completion (minutes) / 5 (round up seconds)
Displaying a task list	--	1
Displaying task details	--	1
Canceling a task	--	4 (+ 2) ^{#1}
Stopping a task	--	4
Modifying a task (Edit)	--	3
Deleting a task	--	4
Updating a task	--	1

GUI operation	Condition	Number of lines
Migration Wizard	--	$13 + T + P (+ 2)^{\#1}$ T: Number of storage tiers that can be specified as migration destinations ^{#2} P: Number of volume pairs ^{#2}
License information (Display)	--	1
License information (Edit)	--	3
Legend: --: No condition #1 Values in parentheses are estimates of the number of lines in audit logs output by the Device Manager server. These values might vary depending upon the version of the Device Manager server. #2 If this number is 1, subtract 2 from the result of the calculation.		

When a GUI operation ends, the contents of the window used for that operation are refreshed. The values in [Table 4-29: Number of lines output to the audit log for GUI operations](#) include the values output to the audit log at these refreshes. For example, the value for *creating a storage domain* includes the values output to the audit log when the *Storage Domain List window* is refreshed after the creation operation finishes.

Volume of output audit log data for each CLI command

[Table 4-30: Number of lines output to the audit log for CLI commands](#) shows the number of lines of information output to the audit log for CLI commands issued to Tiered Storage Manager.

Table 4-30: Number of lines output to the audit log for CLI commands

CLI command	Condition	Number of lines
AddVolumeToMigrationGroup	--	4
CancelTask	--	1
CreateLockingTask	When --execute is not specified	$2 + V$ V: Number of volumes ^{#1}
	When --execute is specified	$4 + V$ V: Number of volumes ^{#1}
CreateMigrationGroup	--	2

CLI command	Condition	Number of lines
CreateMigrationPlan	--	3 + T T: Number of specified storage tiers ^{#1}
	When a migration plan is created by specifying a storage tier consisting of volumes.	1
	When a migration plan is created by specifying a storage tier consisting of a pool.	1
CreateMigrationTask	When --execute is not specified	2 + P P: Number of volume pairs ^{#1}
	When --execute is specified	4 + P P: Number of volume pairs ^{#1}
CreateShreddingTask	When --execute is not specified	2 + V V: Number of volumes ^{#1}
	When --execute is specified	4 + V V: Number of volumes ^{#1}
CreateStorageDomain	--	2
CreateStorageTier	--	2
CreateUnlockingTask	When --execute is not specified	2 + V V: Number of volumes ^{#1}
	When --execute is specified	4 + V V: Number of volumes ^{#1}
DeleteMigrationGroup	--	2
DeleteStorageDomain	--	2
DeleteStorageTier	--	2
DeleteTasks	When --force is not specified	1 + K K: Number of tasks
	When --force and task IDs are specified	1
	When --force is specified but task IDs are not specified	2 + K K: Number of tasks ^{#1}
ExecuteTask	--	1
GetFreeSpaces	--	1 + 2 x SS SS: Number of storage subsystems specified in the subsystemname parameter
GetMigrationGroups	When migration group names are specified	2 + M M: Number of specified migration groups ^{#1}
	When migration group names are not specified	1

CLI command	Condition	Number of lines
GetPools	--	$1 + 2 \times N / 10,000$ (rounded up to nearest integer) N: Amount of pool information to be acquired
GetStorageDomains	When storage domain names are specified	$4 + 2 \times S$ S: Number of storage domains ^{#2}
	When storage domain names are not specified	$3 + S$ S: Number of storage domains ^{#1}
GetStorageTiers	When storage tier names are specified	$3 + T$ T: Number of specified storage tiers ^{#1}
	When storage tier names are not specified	2
GetTasks	--	1
GetVolumes	--	$1 + 2 \times N / 10,000$ (rounded-up to nearest integer) N: Amount of volume information to be acquired
ModifyMigrationGroup	--	2
ModifyStorageDomain	--	2
ModifyStorageTier	--	2
ModifyTask	--	2
Refresh	When storage domain names are specified	1
	When storage domain names are not specified	$1 + S$ S: Number of storage domains
RemoveVolumeFromMigrationGroup	--	4
StopTask	--	1
Legend: --: No condition ^{#1} If this number is 1, subtract 2 from the result of the calculation. ^{#2} If this number is 1, subtract 4 from the result of the calculation.		

Each time you execute a CLI command, login processing is performed by using the user name specified in the `-u` or `--username` option. At this time, audit log data of the `Authentication` type is output from the HSSO server. This audit log data and the audit log data from the Tiered Storage Manager servers are output together.

The total number of lines output to the audit log as a result of executing CLI commands is about double the total number of lines calculated for CLI commands by using [Table 4-30: Number of lines output to the audit log for](#)

[CLI commands](#). Also note that the total number of bytes of audit log data output from the HSSO server can be calculated by using the following values:

- For event logs: 275 x 2 bytes per line
- For syslog: 235 bytes per line

Correlating user operations and audit log data

This section explains what audit log data is output as a result of operations that a user performs with the CLI or GUI.

GUI operations and corresponding output audit log data

To determine what GUI operations were performed by examining the output audit log data:

1. Extract the audit log data output by Tiered Storage Manager (data where the program name is `TSMgr`).

The audit log data created by using the GUI is output by Tiered Storage Manager and has the `TSM_GUI` application identifier information.

When multiple users are accessing Tiered Storage Manager at the same time, you can perform filtering by the user IDs that are output to *subject-identification-information*.

2. To determine the GUI operation used, compare the details of the audit log data with the contents of [Table 4-31:GUI operations and corresponding audit log data](#) and look for a matching pattern.

Among the output audit log data, there will be evidence of many calls to `Get`-type operations. These are frequently called to refresh the screen and cannot be attributed completely to user actions. However, information that corresponds to operations such as creating, updating, and deleting various resources in Tiered Storage Manager also exists in the audit log. [Table 4-31:GUI operations and corresponding audit log data](#) shows the main information for identifying log data of these operations. You can identify operations performed by the user by looking for audit log data that has *M* in the *key* column. In the actual audit logs, data for `Get`-type operations is output before and after the information [Table 4-31:GUI operations and corresponding audit log data](#).

Users will specify *names*, such as a storage domain name and migration group name, during user operations. However, audit log data output by the Tiered Storage Manager server might output only *IDs*, such as storage domain IDs and migration group IDs, which are internally managed by Tiered Storage Manager. In such cases, you cannot identify the name corresponding to the ID simply by examining that particular audit log. However, if you search the audit log data around that entry, you will find an audit log entry that has both the name and ID, and you can use this information to identify the name.

In log data of creation tasks, both information items are output to the audit event information of `Create` *xx*.

In log data of non-creation tasks, the GUI and CLI issue *Get*-type requests to acquire information on the operation targets. Therefore, information on the operation targets of both the GUI and CLI can be obtained by examining log data of *Get*-type requests.

The following example demonstrates how to find a corresponding name and ID, using a storage domain refresh operation log as an example:

Example:

OP=(10,Get), Res=(20,SD), SD=(domainId,domainName) ...(1)
(Domain selection)

OP=(90,Refresh), Res=(20,SD), SD=(domainId) ...(2) (Domain refresh)

When examining only the information in [CLI commands and corresponding output audit log data](#), you can only see the *domainId*, but when examining the information in [GUI operations and corresponding output audit log data](#), you can also see the corresponding *domainName*.

[Table 4-31:GUI operations and corresponding audit log data](#) shows GUI operations of Tiered Storage Manager and the corresponding main information output to the audit log.

Table 4-31: GUI operations and corresponding audit log data

GUI operation	Key	OpName #	ResName #	Additional information #	Note
Logging on	M	Get	LC	--	--
Creating a storage domain	--	Get	SS	NumSS	--
	M	Create	SD	SD, SS	--
	--	Refresh	SD	SD	--
Editing a storage domain	M	Modify	SD	SD	--
Refreshing a storage domain	--	Get	SD	SD	--
	M	Refresh	SD	SD	--
	--	Get	RS	SD	Repeats until the refresh is completed.
Deleting a storage domain	M	Delete	SD	SD	--
Displaying a storage domain list	M	Get	SD	NumSD	--
Displaying storage domain detailed information	M	Get	SD	SD	--
	--	Get	RS	SD	--
Creating a storage tier	M	Create	ST	SD, ST	--
Editing a storage tier	M	Modify	ST	SD, ST	--
Deleting a storage tier	M	Delete	ST	ST	--

GUI operation	Key	OpName #	ResName #	Additional information #	Note
Displaying a storage tier list	M	Get	ST	SD, NumST	--
Displaying storage tier detailed information	M	Get	ST	SD, ST	--
Creating a migration group	M	Create	MG	SD, MG	--
Editing a migration group	M	Modify	MG	SD, MG	--
Deleting a migration group	M	Delete	MG	MG	--
Displaying a migration group list	M	Get	MG	SD, NumMG	--
Displaying migration group detailed information	M	Get	MG	SD, MG	--
Adding volumes to a migration group	M	Add	VL	MG, VL	Information about the added volumes is output.
Deleting volumes from a migration group	M	Remove	VL	MG, VL	Information about the deleted volumes is output.
Searching for a volume	--	Get	VR	SD	--
	M	Get_num	VL	NumVL	--
	M	Get	VL	SD, NumVL	--
Searching for a pool	M	Get_num	PO	NumPO	--
	M	Get	PO	SD, NumPO	--
Searching for a task	M	Get_summary	TK	NumTK	--
Migrate MG	M	Create	MP	SD, MG, ST	--
Creating a migration task	M	Create	TK	TK, SD, MG, ST, NumVP, VPs	--
Executing a task	M	Execute	TK	TK	--
Displaying a task list	M	Get_summary	TK	NumTK	--
Displaying task detailed information	M	Get	TK	TK	--
Canceling a task	M	Cancel	TK	TK	--
Stopping a task	M	Change	TK	TK	--
Modifying a task	M	Modify	TK	TK	--
Deleting a task	M	Delete	TK	TK	--

GUI operation	Key	OpName #	ResName #	Additional information #	Note
License information (Display)	M	Get	LC	--	--
License information (Edit)	M	Add	LC	LC	--
Legend: M: Main key --: Not applicable # For details, see Table 4-26:Information output to the application specific information area , Table 4-27:Operation types (OP) , and Table 4-28:Operation targets (Res) .					

CLI commands and corresponding output audit log data

To estimate the user-performed CLI commands by examining the output audit log data:

1. Extract the audit log data output by Tiered Storage Manager (data where the program name is `TSMgr`).

Audit log data created by executing CLI commands is output by Tiered Storage Manager and has the `TSM_CLI` application identifier information.

When multiple users are accessing Tiered Storage Manager at the same time, you can perform filtering by the user IDs that are output to *subject-identification-information*.

2. To determine the CLI command used, compare the details of the output audit log data with the contents of [Table 4-32:CLI commands and corresponding audit log data](#) and look for a matching pattern.

Except for commands starting with `Get`, you can identify user-executed commands by examining the audit log data that has an *M* in the *key* column.

[Table 4-32:CLI commands and corresponding audit log data](#) lists CLI commands of Tiered Storage Manager and corresponding data output to the audit log.

Table 4-32: CLI commands and corresponding audit log data

CLI command	Key #1	OpName #2	ResName #2	Additional information #2	Note
AddVolumeToMigrationGroup	M	Add	VL	SD, MG, VL	--
	--	Get	MG	SD, MG	--
	--	Get	SD	SD	--
	--	Get	VL	SD, NumVL	--
CancelTask	M	Cancel	TK	TK	--

CLI command	Key #1	OpName #2	ResName #2	Additional information #2	Note
CreateLockingTask	M	Create	TK	TK, SD, MG, NumVL, VLs	TK= (id, 2, ...)
	--	Execute	TK	TK	--
	--	Get	TK	TK	--
CreateMigrationGroup	--	Get	SD	SD	--
	M	Create	MG	SD, MG	--
CreateMigrationPlan	--	Get	ST	SD, NumST, [STs]	--
	M	Create	MP	SD, MG, ST	--
CreateMigrationTask	M	Create	TK	TK, SD, MG, ST, NumVP, VPs	TK= (id, 0, ...)
	--	Execute	TK	TK	When --execute is specified
	--	Get	TK	TK	When --execute is specified
CreateShreddingTask	M	Create	TK	TK, SD, MG, NumVL, VLs	TK= (id, 4, ...)
	--	Execute	TK	TK	When --execute is specified
	--	Get	TK	TK	When --execute is specified
CreateStorageDomain	M	Create	SD	SD, SS	--
	--	Refresh	SD	SD	--
CreateStorageTier	--	Get	SD	SD	--
	M	Create	ST	SD, ST	--
CreateUnlockingTask	M	Create	TK	TK, SD, MG, NumVL, VLs	TK= (id, 3, ...)
	--	Execute	TK	TK	When --execute is specified
	--	Get	TK	TK	When --execute is specified
DeleteMigrationGroup	--	Get	MG	SD, MG	--
	M	Delete	MG	MG	--
DeleteStorageDomain	--	Get	SD	SD	--
	M	Delete	SD	SD	--
DeleteStorageTier	--	Get	ST	SD, ST	--
	M	Delete	ST	SD, ST	--
DeleteTasks	--	Get	TK	{TK NumTK}	When --force is not specified
	M	Delete	TK	{TK NumTK, TKs}	--

CLI command	Key #1	OpName #2	ResName #2	Additional information #2	Note
ExecuteTask	M	Execute	TK	TK	--
GetFreeSpaces	--	Get	SS	NumSS	--
	--	Get_num	FS	SS, NumFS	Only acquires the number of storage subsystems specified in the subsystemname parameter
	M	Get	FS	SS, NumFS	Only acquires the number of storage subsystems specified in the subsystemname parameter
GetMigrationGroups	M	Get	MG	SD, NumMG, [MGs]	--
GetPools	--	Get_num	PO	NumPO	--
	--	Get	SD	SD	--
	M	Get	PO	SD, NumPO	--
GetStorageDomains	M	Get	SD	NumSD, [SDs]	--
	--	Get	RS	NumSD, SDs	--
GetStorageTiers	M	Get	ST	SD, NumST, [STs]	--
	--	Get	SD	SD	--
GetTasks	M	Get	TK	{TK NumTK}	--
GetVolumes	--	Get_num	VL	NumVL	--
	--	Get	SD	SD	Acquires information on 10,000 volumes at a time
	M	Get	VL	SD, NumVL	Acquires information on 10,000 volumes at a time
ModifyMigrationGroup	--	Get	MG	SD, MG	--
	M	Modify	MG	SD, MG	--
ModifyStorageDomain	--	Get	SD	SD	--
	M	Modify	SD	SD	--
ModifyStorageTier	--	Get	ST	SD, ST	--
	M	Modify	ST	SD, ST	--
ModifyTask	--	Get	TK	TK	--
	M	Modify	TK	TK	--

CLI command	Key #1	OpName #2	ResName #2	Additional information #2	Note
Refresh	--	Get_summary	SD	NumSD	When storage domain names have been specified
	M	Refresh	SD	SD	--
RemoveVolumeFromMigrationGroup	--	Get_summary	SD	SD	--
	--	Get	MG	SD, MG	--
	--	Get	VL	SD, NumVL	--
	M	Remove	VL	SD, MG, VL	--
StopTask	M	Change	TK	TK	opt = 0x02040000 or 0x02050000
Legend: M: Main key --: Not applicable #1 Indicates key audit log data for determining the command. #2 For details, see Table 4-26:Information output to the application specific information area , Table 4-27:Operation types (OP) , and Table 4-28:Operation targets (Res) .					

Retrieving log information

When an error occurs on the Tiered Storage Manager server, use the `hcmdsgetlogs` command to obtain the information you will need for error analysis. By using the `hcmdsgetlogs` command, the following information can be obtained and stored in a desired folder:

- Log data^{#1, #2}
- Setting information (properties)
- License information
- Information about the connection and startup service
- Repository information

#1

In Windows, installation-related trace log data that is output to the root folder of the drive with Windows installed, or that is output to the root folder of the drive where Tiered Storage Manager is or was installed, cannot be obtained by using the `hcmdsgetlogs` command. Such installation-related trace log data must be obtained directly from the folders to which it was output.

#2

To output the CLI client log, the `CLI_DIR` property must be set in the `HtsmgetTI.properties` file. The `CLI_DIR` property determines the location to which the CLI client log will be output.

Setting up the environment for the `hcmdsgetlogs` command

To use the `hcmdsgetlogs` command, its environment first needs to be set up. To set up the environment, use the `HtsmgetTI.properties` file. This file is stored in the following location:

In Windows

installation-folder-of-the-Tiered-Storage-Manager-server\SupportTools\CollectTool

In Solaris or Linux

*installation-directory-of-the-Tiered-Storage-Manager-server/
SupportTools/CollectTool/*

When updating the properties file, use a text editor.

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

- `CLI_DIR`
- `SYSLOG`

The following explains each property:

CLI_DIR

If you want to use CLI on the management server, in `CLI_DIR` specify the directory to which CLI is installed. This will also enable CLI information to be collected. There is no need to specify `CLI_DIR` if you are using CLI on a different machine from the management server. The following are the default installation directories:

In Windows:

installation-folder-of-the-Tiered-Storage-Manager-server\CLI

In Solaris or Linux:

installation-directory-of-the-Tiered-Storage-Manager-server/CLI

SYSLOG

Specifies the absolute path to syslog. The default directory is:

In Solaris:

/var/adm/messages

In Linux:

/var/log/messages

Using the `get logs` command

This section explains how to use the `hcmdsgetlogs` command. Before using the `hcmdsgetlogs` command, make sure of the following:

- If using Windows, you logged in to Windows using a user ID that has the Administrator permission.

- If using Solaris or Linux, you logged in to Solaris or Linux using a user ID that has root permissions.
- Another instance of the `hcmdsgetlogs` command is not running.
- The Java execution path is set to the environment variable **PATH**.



- Do not perform Tiered Storage Manager operations, such as creating storage domains or executing migration tasks when the `hcmdsgetlogs` command is executing. Execution of the `hcmdsgetlogs` command will compete for resources with Tiered Storage Manager operations and might cause an error or slow responses in Tiered Storage Manager.

When the `hcmdsgetlogs` command is executed, four archive files (`.jar`, `.hdb.jar`, `.db.jar`, and `.csv.jar`) are created.

Command specification:

- In Windows:

```
installation-folder-for-Common-Component\bin\hcmdsgetlogs /dir
name-of-output-destination-folder [/types Hitachi-Storage-
Command-Suite-product-name [ Hitachi-Storage-Command-Suite-
product-name...] [/arc archive-file-name] [/logtypes log-file-
type [ log-file-type...]]
```

- In Solaris or Linux:

```
installation-directory-for-Common-Component/bin/hcmdsgetlogs -
dir name-of-output-directory [-types Hitachi-Storage-Command-
Suite-product-name [ Hitachi-Storage-Command-Suite-product-
name...] [-arc archive-file-name] [-logtypes log-file-type [ log-
file-type...]]
```

Parameters

`dir`

Specifies the output destination for maintenance information. If the specified folder name contains a character that is invalid in the OS, an error occurs.

The specified folder must be empty. If the specified folder does not exist, it will be created.

`types`

If you want to obtain maintenance information for only specific Hitachi Storage Command Suite products, for example, in the case of a failure, use this option to specify the name of the Hitachi Storage Command Suite product from which to collect maintenance information. To obtain maintenance information for Tiered Storage Manager, specify `TieredStorageManager`. For details about other Hitachi Storage Command Suite products, see the documentation for each product. To specify multiple product names, separate the product names by a space.

When you specify the `types` option, also specify the log file type `log` for the `logtypes` option.

If this option is omitted, maintenance information for all Hitachi Storage Command Suite products that are installed on the management server is collected.

arc

Specifies the name of the archive file that will hold the collected maintenance information. Specify the file name without an extension. If the specified file name contains a character that is invalid in the OS, an error occurs. The specified file name will receive a `.jar` extension, designating it as maintenance information.

If this option is omitted, the file name will be `HiCommand_log.jar`.

logtypes

If you want to obtain only specific log files, for example in the case of a failure, use this option to specify the name of specific log files that you want to collect. Specify the following log file types:

`log`—obtains only `.jar` and `.hdb.jar` files

`db`—obtains only `.db.jar` files

`csv`—obtains only `.csv.jar` files

To specify multiple types, separate them by a space. If you omit this option, all log files will be obtained.



Caution: You can use the following characters in the `dir` and `arc` options:

- In Windows:

A to Z a to z 0 to 9 . _

You can use a backslash (`\`), forward slash (`/`), and colon (`:`) as separators, except at the end of the path name.

- In Solaris or Linux:

A to Z a to z 0 to 9 . _

You can use a forward slash (`/`) as a separator, except at the end of the path name.

Return values

0: Normal termination

1: Parameter error

2: Abnormal termination

Example:

This example shows the command for collecting maintenance information for Hitachi Storage Command Suite products. In this example, the archive file named `hicmd_log` is created in the `logs_work` directory.

- In Windows:

```
C:\Program Files\HiCommand\Base\bin\hcmdsgetlogs /dir
```

```
C:\logs_work /arc hicmd_log
```

- In Solaris or Linux:

```
# /opt/HiCommand/Base/bin/hcmdsgetlogs -dir /opt/logs_work -  
arc hicmd_log
```



Caution: If the KAPM05318-I or KAPM05319-E message is not output after the `hcmdsgetlogs` command is executed, the command did not complete because sufficient free space was not available for the directory specified in the `dir` option.

Free up sufficient disk space, and then re-execute the `hcmdsgetlogs` command.

Property descriptions and environment settings

This appendix describes the property files of Tiered Storage Manager and how to set up the environment.

- ❑ [Property descriptions](#)
- ❑ [Environment settings](#)

Property descriptions

The property files of the Tiered Storage Manager server are stored in the following locations:

In Windows:

installation-folder-of-the-Tiered-Storage-Manager-server\conf

In Solaris or Linux:

installation-directory-of-the-Tiered-Storage-Manager-server/conf

Use a text editor when editing the property files. Templates for property files are stored in the `template` folder, which is located under the folder where Tiered Storage Manager is installed.

The property files are in the Java property file format. The property file conventions are:

- Each property must be entered as a combination of a property name and value separated by an equals sign (=). For example,
`server.rmi.port=20352.`
- A literal (character string or value) does not need to be enclosed by quotation marks.
- The backslash (\) is reserved as an escape character. Since absolute path names in Windows include *backslashes*, you must add an escape character before every backslash in a Windows path name.

For example, the path name of the file

`c:\HiCommand\TieredStorageManager` should be entered as

`c:\\HiCommand\\TieredStorageManager`. When you specify properties, there is no need to precede other characters with the escape character \.

- Each property must be separated by a line delimiter (a line feed character).
- A line beginning with a hash mark (#) is a comment line.
- If a line ends with a backslash (\), the next line is a continuation of the current line.

If incorrect properties are specified, the loading of the properties will fail and the Tiered Storage Manager server will not start. Properties that are incorrect are output to the command log or message log.

In a cluster configuration, use the same property files on both the executing and standby nodes unless there is a special reason not to.



Caution: Before updating a property file, stop the Tiered Storage Manager server. If a property file is updated while the Tiered Storage Manager server is running, the Tiered Storage Manager server might not be able to stop normally. In such a case, forcibly stop the server.

[Table A-1: Tiered Storage Manager properties](#) lists the Tiered Storage Manager properties.

Table A-1: Tiered Storage Manager properties

Property	Description
<code>server.properties</code> file	A property file used to configure the environment settings related to the Tiered Storage Manager server operations
<code>server.rmi.secure</code>	Specifies whether to use SSL for communication between the Tiered Storage Manager server and the CLI client.
<code>server.rmi.port</code>	Specifies the RMI port number (for non-SSL communication) that Tiered Storage Manager uses to accept processing requests.
<code>server.rmi.security.port</code>	Specifies the RMI port number (for SSL communication) that Tiered Storage Manager uses to accept processing requests.
<code>server.base.initialsynchro</code>	Specifies whether to synchronize the Tiered Storage Manager configuration information in the navigation tree with the data in the Common Component repository when starting the Tiered Storage Manager server.
<code>server.mail.smtp.host</code>	Specifies the host name or IP address of the SMTP server that is used to send event notification email.
<code>server.mail.from</code>	Specifies the email address of the sender of event notification email.
<code>server.mail.errorsTo</code>	Specifies the email address to which an undeliverable notification email is sent when a delivery error occurs for an event notification email.
<code>server.mail.smtp.port</code>	Specifies the port number of the SMTP server to be accessed when event notification email is sent.
<code>server.mail.smtp.auth</code>	Specifies whether to enable SMTP authentication when event notification email is sent.
<code>server.eventNotification.mail.to</code>	Specifies the email address for event notification email.
<code>server.eventMonitoringIntervalInMinute</code>	Specifies the interval at which to check for the expiration of the volume lock period or the passing of a specified time of volume lock.
<code>server.migration.multiExecution</code>	Specifies the number of migrations that can be performed at the same time on each storage domain.
<code>server.checkOutVolumeRange</code>	Specifies whether the values specified for filter conditions are checked for validity.
<code>server.repository.autoRefresh.pollingIntervalInMinute</code>	Specifies the polling interval (in minutes) for checking for a refresh of the Device Manager repositories. At the specified intervals, Tiered Storage Manager checks whether Device Manager has refreshed the storage subsystems and, if a refresh is detected, refreshes their storage domains.
<code>server.repository.autoRefresh.serverStarted</code>	Specifies whether to refresh all storage domains when the Tiered Storage Manager server starts.
<code>server.repository.autoRefresh.recurringLocalTime</code>	Specifies whether to refresh all storage domains when a user-specified time has been reached.

Property	Description
<code>server.repository.dvmModifyCheck.pollingIntervalInMinute</code>	Specifies the polling interval (in minutes) for checking for a refresh of the Device Manager repositories. At the specified intervals, Tiered Storage Manager checks whether Device Manager has refreshed the storage subsystems and, if a refresh is detected, outputs a message prompting the user to refresh the storage domains of the refreshed subsystems.
<code>server.migration.dataErase.defaultValue</code>	Specifies whether source volume data will be deleted by default after a migration.
<code>server.migrationPlan.candidateVolumeCountLimit</code>	Specifies whether to limit the number of candidate volumes displayed when creating a migration plan.
<code>server.migrationPlan.candidateCapacityGroupDisplayMaxCount</code>	Specifies how many volumes with capacities larger than the migration source volume to display when creating a migration plan. These volumes are displayed in addition to any volumes with equal capacity to the migration source volume.
<code>server.migration.maxRetryCount</code>	Specifies the maximum number of retries Tiered Storage Manager sends to the storage subsystem when the storage subsystem is temporarily unable to receive task execution requests.
<code>server.volumeCreation.param.defaultPortController</code>	Specifies the default port number to use when creating volumes with the volume creation task.
<code>client.properties</code> file	A property file used to configure the environment settings related to the Web client display and operations.
<code>client.ldev.rowsperpage.retain.enabled</code>	Specifies whether to keep the setting when the number of lines displayed per page for a sortable table is changed.
<code>database.properties</code> file	A property file used to configure the environment settings related to repositories.
<code>dbm.traceSQL</code>	Specifies whether SQL is output to a trace log.
<code>devicemanager.properties</code> file	A property file used to configure the environment settings related to access to the Device Manager server.
<code>hdvm.protocol</code>	Specifies the protocol to be used when accessing the Device Manager server.
<code>hdvm.host</code>	Specifies the host name or IP address of the Device Manager server.
<code>hdvm.port</code>	Specifies the port number of the Device Manager server.
<code>hdvm.timeout</code>	Specifies the timeout period for communications with the Device Manager server.
<code>logger.properties</code> file	A property file used to configure the environment settings related to log output.
<code>logger.messageLogLevel</code>	Sets the threshold output level for the messages logged by the Tiered Storage Manager server and the Web client.
<code>logger.traceLogLevel</code>	Sets the threshold output level for the trace logging by the Tiered Storage Manager server and the Web client.
<code>logger.syslogLevel</code>	Sets the threshold output level for event logs.
<code>logger.serverMessageFileCount</code>	Sets the number of message log files output by the server.
<code>logger.serverTraceFileCount</code>	Sets the number of trace log files output by the server.

Property	Description
<code>logger.guiMessageFileCount</code>	Sets the number of message log files output by the Web client.
<code>logger.guiTraceFileCount</code>	Sets the number of trace log files output by the Web client.
<code>logger.serverMessageMaxFileSize</code>	Specifies the maximum file size of server message log files.
<code>logger.serverTraceMaxFileSize</code>	Specifies the maximum file size of server trace log files.
<code>logger.guiMessageMaxFileSize</code>	Specifies the maximum file size of client message log files.
<code>logger.guiTraceMaxFileSize</code>	Specifies the maximum file size of client trace log files.
<code>tuningmanager.properties file</code>	A property file used to configure the environment settings related to linking to Tuning Manager.
<code>htnm.infoAcquirePeriod</code>	Specifies whether performance information acquired from Tuning Manager is summarized by week or month.
<code>htnm.infoCachePeriodInMinute</code>	Specifies how long correspondences between Tuning Manager agents and the storage subsystems they manage are kept in the cache.
<code>htnm.servers</code>	Specifies the number of Tuning Manager servers to connect to.
<code>htnm.server.n.host</code>	Specifies the host name or IP address of the Tuning Manager server to be accessed.
<code>htnm.server.n.port</code>	Specifies the port number of the HBase Storage Mgmt Web Service of the Tuning Manager server to be accessed.

Environment settings

Configuring environment settings related to Tiered Storage Manager server operations

You can configure the environment settings related to Tiered Storage Manager server operations in the `server.properties` file.

The following describes the properties set in the `server.properties` file.

server.rmi.secure

This setting specifies whether to use SSL for communications between the Tiered Storage Manager server and the CLI client. By using SSL, such communications can be encrypted.

Specify 1, 2, or 3 for this property.

- 1: Do not use SSL.
- 2: Use SSL.
- 3: Use SSL in advanced security mode.

If you select 1, the value specified for the `server.rmi.port` property is enabled. If you select 2 or 3, the value specified for the `server.rmi.security.port` property is enabled.

Default: 1

server.rmi.port

For configurations not using SSL communication, this setting specifies the RMI port number used by Tiered Storage Manager to accept processing requests.

The range of specifiable values is from 1024 to 65535.

Default: 20352

server.rmi.security.port

For configurations using SSL communication, this setting specifies the RMI port number used by Tiered Storage Manager to accept processing requests.

The range of specifiable values is from 1024 to 65535.

Default: 24500

server.base.initialsynchro

This setting specifies whether the Tiered Storage Manager configuration information contained in the navigation tree is synchronized with the Common Component repository when the Tiered Storage Manager server starts.

Specify a Boolean value for this property. Specify `true` to synchronize information. Specify `false` if you do not want to synchronize information.

If you restore Tiered Storage Manager repositories individually, inconsistencies may arise between the storage configuration information in Tiered Storage Manager and the Common Component repository when the Tiered Storage Manager server is restarted. In such a case, set this property to `true`.

Default: `false`

server.mail.smtp.host

This setting specifies the host name or IP address of the SMTP server to access when sending event notification email.

When entering an IPv6 address, enclose it with `[` and `]`.

Default: `None`

server.mail.from

This setting specifies the email address of the sender of event notification email.

Default: `htsmserver`

server.mail.errorsTo

This setting specifies the email address to which an undeliverable notification email will be sent when event notification email cannot be delivered. If this property is not specified, the undeliverable notification email is sent to the email address specified in `server.mail.from`.

Note that the conditions for sending undeliverable notification email vary according to the SMTP server settings. Make sure to review these settings.

Default: `None`

server.mail.smtp.port

This setting specifies the SMTP server port number to use when sending event notification email. The range of specifiable values is from 1 to 65535.

Default: 25

server.mail.smtp.auth

This setting specifies whether to enable SMTP authentication when sending event notification email. Specify a Boolean value for this property. Specifying `true` enables SMTP authentication. Specifying `false` disables SMTP authentication.

Note that if you enable SMTP authentication when your email server does not support it, email will be sent without SMTP authentication being performed. Check the specifications of your email server before specifying SMTP authentication.

Default: `false`

server.eventNotification.mail.to

This setting specifies the email address for event notification email. Specify a character string for this property. Notification email for all events is sent to the email address specified in this property.

Default: `None`

server.eventMonitoringIntervalInMinute

This setting specifies the monitoring interval in minutes for checking whether the volume lock period or the specified time limit for volume locks has passed. The range of specifiable values is from 1 to 35791.

Default: 180

server.migration.multiExecution

Specifies the number of migrations that can be simultaneously performed on a storage domain. The range for specifiable values is from 1 to 64.

Default: 8

server.checkOutVolumeRange

Specifies whether filter conditions used for searching volumes or defining storage tiers have their values checked for validity.

Specify a Boolean value for this property. If you specify `true`, values will be checked. If you specify `false`, values will not be checked.

Default: `true`



Caution: If you specify `false`, filter conditions will not be checked so make sure that you enter correct filter conditions. Normally, leave this property as the default value of `true` so that filter conditions are checked.

server.repository.autoRefresh.pollingIntervalInMinute

Specifies the polling interval (in minutes) of checks for refreshes of the Device Manager repositories. You can specify `0` or a value from `10` to `1,440`. If `0` is specified, an automatic refresh is not performed after detecting a refresh of Device Manager repositories. If an integer value other than `0` is specified, Tiered Storage Manager uses that value to check for refreshes of Device Manager repositories at the specified polling intervals. When Tiered Storage Manager detects a refresh of a storage subsystem within Device Manager, Tiered Storage Manager refreshes the Tiered Storage Manager storage domain associated with the storage subsystem that was refreshed in Device Manager.

Default: `10`

server.repository.autoRefresh.serverStarted

This setting specifies whether to refresh all storage domains when the Tiered Storage Manager server starts.

Specify a Boolean value for this property. If you specify `true`, all storage domains will be refreshed whenever the Tiered Storage Manager server starts.

If you specify `false`, storage domains will not be refreshed when the Tiered Storage Manager server starts.

Default: `false`

server.repository.autoRefresh.recurringLocalTime

This setting sets a refresh of all storage domains to occur at a scheduled time. Each day, when the specified time is reached, all storage domains are refreshed. The specified value must be in the `hh:mm:ss` format.

If an empty character string is specified, no scheduled automatic refreshes will occur. If a value is specified in the `hh:mm:ss` format, an automatic refresh is performed at the specified time.

Default: `None`

server.repository.dvmModifyCheck.pollingIntervalInMinute

Specify the polling interval (in minutes) for checks for refreshes of the Device Manager repositories.

You can specify 0 or a value from 30 to 1,440. If 0 is specified, Tiered Storage Manager does not monitor for refreshes of Device Manager repositories. When an integer greater than or equal to 30 is specified, Tiered Storage Manager monitors whether any refreshes of Device Manager repositories occurred since the last specified polling interval. When Tiered Storage Manager detects a refresh, it displays a warning message to prompt the user to refresh the Tiered Storage Manager storage domain associated with the storage subsystem that was refreshed in Device Manager.

Default: 0

If the properties

`server.repository.dvmModifyCheck.pollingIntervalInMinute` and `server.repository.autoRefresh.pollingIntervalInMinute` are both specified with the same valid, non-zero value, on detecting a storage subsystem refresh in Device Manager, Tiered Storage Manager will automatically refresh the Tiered Storage Manager storage domain associated with the storage subsystem that was refreshed in Device Manager.

server.migration.dataErase.defaultValue

This setting specifies whether to delete source volume data by default after a migration.

Specify a Boolean value for this property. If you specify `true`, source volume data will be deleted by default. If you specify `false`, source volume data will not be deleted by default.

To prevent data leaks, we recommend that you delete the data on migration source volumes after migration.

Default: `false`



Caution: If you modify this property value, you must restart the HBase Storage Mgmt Common Service to enable the changes.

server.migrationPlan.candidateVolumeCountLimit

This setting specifies whether to limit the number of candidate volumes that are displayed when creating a migration plan.

Specify a Boolean value for this property. If you specify `true`, the number of displayed candidate volumes will be limited. If you specify `false`, there will be no limit imposed on the number of displayed candidate volumes.

Default: `true`

server.migrationPlan.candidateCapacityGroupDisplayMaxCount

This setting specifies how many volumes with a larger capacity than the migration source volume to display in addition to the volumes with the same capacity as the migration source volume when creating a migration plan.

You can specify a value from 0 to 10. Specify 0 to display only volumes with the same capacity as the migration source volume.

Default: 4



- If you specify a volume with a larger capacity than the migration source volume for the migration target volume, the migration target volume is deleted prior to migration, and then created again with the same capacity as the migration source volume. Therefore, the migration task will require more time than when migrating to a volume of the same capacity.
- If the migration target volume is recreated, the free capacity of the array group increases by the difference in capacity with the migration source volume. For example, if a volume that has 30 GB is specified as a migration target for a migration source volume that has 10 GB, the free capacity of the array group increases by 20 GB. Therefore, we recommend that you specify, as a migration target, a volume that is as close in capacity to the migration source volume as possible.

server.migration.maxRetryCount

This setting specifies the maximum number of retries to be sent by the Tiered Storage Manager server when requesting that the storage subsystem retry task execution. If the storage subsystem is temporarily unable to receive such requests because the user has modified the configuration of the storage subsystem or the storage subsystem is operating in Modify mode, requests to the storage subsystem can be retried every five minutes.

You can specify a value from 0 to 2,147,483,647. If 0 is specified, no retries are attempted.

Default: 5

server.volumeCreation.param.defaultPortController

This setting specifies the port number to be used when a volume is created by a volume creation task. Note that this setting only applies to volume creation within the following storage subsystems, which are managed by Device Manager:

- Thunder 9500V
- Hitachi AMS 2000/AMS/WMS series

You can specify a value from 0 to 2,147,483,647.

Default: 0

Configuring environment settings related to Web client

In the `client.properties` file, you can configure environment settings related to the Web client display and operations.

The following describes the properties set in the `client.properties` file.

`client.ldev.rowsperpage.retain.enabled`

This property specifies whether to keep the setting when the number of lines displayed per page for a sortable table is changed.

If this property is set to `true`, when a user changes the number of displayed lines for a sortable table, that table is initially displayed using the new setting the next time the same user views the same sortable table. The number of displayed lines that you specify is kept for each user account and for each sortable table.

If this property is set to `false`, the sortable table is set to the initial display of 25 lines per page.

Default: `true`



Note: Even if the property value is changed from `true` to `false`, the setting for the number of displayed lines changed by each user is saved in the Tiered Storage Manager server. Therefore, if this property is set to `true` again, the sortable table will be initially displayed using the setting that each user previously set.

Configuring environment settings related to the repositories

In the `database.properties` file, you can configure the environment settings related to repositories.

The following describes the properties set in the `database.properties` file.

`dbm.traceSQL`

This setting specifies whether SQL should be output to a trace log.

Specify a Boolean value for this property. Specifying `true` outputs SQL. If you specify `false`, SQL is not output.

Default: `false`

Configuring environment settings related to accessing the Device Manager server

In the `devicemanager.properties` file, you can configure the environment settings related to access to the Device Manager server.

The following describes the properties set in the `devicemanager.properties` file.

hdvm.protocol

This setting specifies the protocol to be used when accessing the Device Manager server.

Specify a character string for this property.

Default: `http`

hdvm.host

This setting specifies the host name or IP address of the Device Manager server you are accessing.

Specify a character string for this property.

When entering an IPv6 address, enclose it with [and].

Default: `127.0.0.1`

hdvm.port

This setting specifies the port number of the Device Manager server you are accessing. This is the value specified in the `server.http.port` property in the configuration file (`server.properties`) of the Device Manager server. For details about this file, see the *Hitachi Device Manager Server Configuration and Operation Guide*.

The range of specifiable values is from 1024 to 65535.

Default: `2001`

hdvm.timeout

This setting specifies the timeout period (in milliseconds) for communications with the Device Manager server you are accessing. Specifying 0 disables the timeout function.

The range of specifiable values is from 0 to 2,147,483,647.

Default: `0`

Configuring environment settings related to log output

In the `logger.properties` file, you can configure the environment settings related to log output.

The following describes the properties set in the `logger.properties` file.

[Figure A-1:Relationship between the threshold value of the output levels and the output messages](#) shows the relationship between the threshold value of the output levels and the output messages.

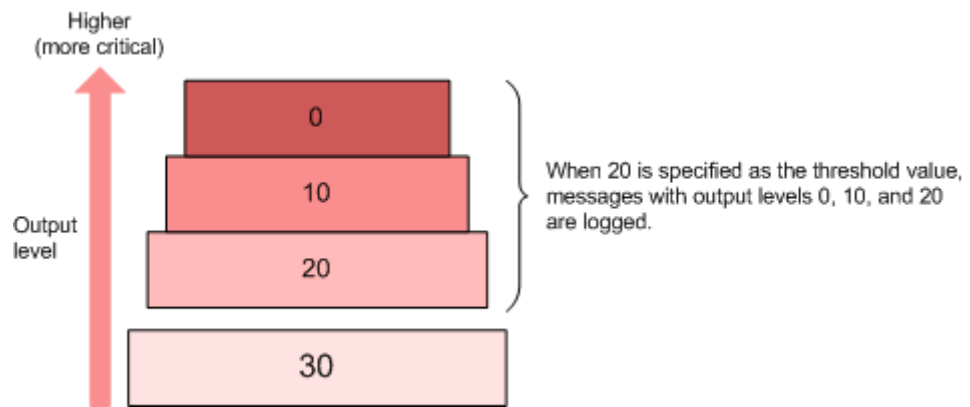


Figure A-1: Relationship between the threshold value of the output levels and the output messages

logger.messageLogLevel

This setting specifies a threshold output level for the messages logged by Tiered Storage Manager. This property applies to the Tiered Storage Manager server message log (`HTSMServerMessage.log`) and the Web client message log (`HTSMGuiMessage.log`).

Messages with an output level equal to or lower than the level specified in this property will be written to the message log.

Specify a value from 0 to 30. We recommend that the default value be used. Note that the same messages are output whether you specify 20 or 30, because there are no messages whose output level is 30.

Default: 0

The output levels are based on the contents of the logged messages. [Table A-2: Output level of message log data](#) shows the output levels.

Table A-2: Output level of message log data

Type of message	Output level	Message descriptions
Error	0	An error occurred that affects the operation of the management server or Java servlet.
	10	An execution error occurred due to a reason such as an operational mistake.
Warning	20	An error occurred, but execution can continue with limitations.
Information	0	Information has been produced about the actions of the management server and the Web client.
	20	Information has been produced about the processing for an operation.



Caution: If you have changed the property value, restart the HBase Storage Mgmt Common Service to enable the new value.

logger.tracelogLevel

This setting specifies a threshold output level for the trace logging by Tiered Storage Manager. This property applies to the Tiered Storage Manager server trace log (HTSMServerTracen.log) and the Web client trace log (HTSMGuiTracen.log).

Messages with an output level equal to or lower than the level specified in this property will be written to the trace log.

Specify a value from 0 to 30. We recommend that the default value be used.

Default: 20

Output levels are based on the contents of the logged messages. [Table A-3: Output level of trace log data](#) shows the output levels.

Table A-3: Output level of trace log data

Type of message	Output level	Message descriptions
Error	0	An error occurred that affects the operation of the management server or Java servlet.
	10	An execution error occurred due to a reason such as an operational mistake.
Warning	20	An error occurred, but execution can continue with limitations.
Information	0	Information has been produced about the actions of the management server and management client.
	10	Information has been produced about exchanges with other programs or machines.
	20	Information has been produced about the starting/stopping of a major method, or the creation/deletion of a major object.
	30	Detailed information has been produced.



Caution: If you have changed the property value, restart the HBase Storage Mgmt Common Service to enable the new value.

logger.syslogLevel

This setting specifies a threshold output level for event log data and syslog data output by Tiered Storage Manager. Messages with an output level equal to or lower than the one specified in this property will be written to an event log or syslog.

Any value from 0 to 30 can be specified. We recommend that the default value be used.

Default: 0



Caution: If you have changed the property value, restart the HBase Storage Mgmt Common Service to enable the new value.

logger.serverMessageFileCount

Specify the number of message log files used by the Tiered Storage Manager server. The range of specifiable values is from 2 to 16.

The log files are produced in accordance with the size specified by the `logger.serverMessageMaxFileSize` property, and are assigned names with a log number appended (for example, `HTSMServerMessage1.log` and `HTSMServerMessage2.log`). The log files are used and written to in the order of the log numbers. A round robin method is applied, meaning that after the end of the last file has been reached, the first file is overwritten.

After the Tiered Storage Manager server starts, writing continues to the file to which the last log data was written, regardless of whether the server stopped normally last time.

Default: 10

logger.serverTraceFileCount

Specify the number of trace log files used by the Tiered Storage Manager server. The range of specifiable values is from 2 to 16.

The log files are produced in accordance with the size specified by the `logger.serverTraceMaxFileSize` property, and are assigned names with a log number appended (for example, `HTSMServerTrace1.log` and `HTSMServerTrace2.log`). The log files are used and written to in the order of the log numbers. A round robin method is applied, meaning that, after the end of the last file has been reached, the first file is overwritten.

After the Tiered Storage Manager server starts, writing continues to the file to which the last log data was written, regardless of whether the server stopped normally last time.

For details on how to estimate the amount of trace log files output by the Tiered Storage Manager server, see [Estimating trace log volume](#).

Default: 10

logger.guiMessageFileCount

Specify the number of message log files used by the Web client. The range of specifiable values is from 2 to 16.

The log files are produced in accordance with the size specified by the `logger.guiMessageMaxFileSize` property, and are assigned names with a log number appended (for example, `HTSMGuiMessage1.log` and `HTSMGuiMessage2.log`). The log files are used and written to in the order of the log numbers. A round robin method is applied, meaning that, after the end of the last file has been reached, the first file is overwritten.

After the Tiered Storage Manager server starts, writing continues to the file to which the last log data was written, regardless of whether the server stopped normally last time.

Default: 10



Caution: If you have changed the property value, restart the HBase Storage Mgmt Common Service to enable the new value.

logger.guiTraceFileCount

Specify the number of trace log files used by the Web client. The range of specifiable values is from 2 to 16.

The log files are produced in accordance with the size specified by the `logger.guiTraceMaxFileSize` property, and are assigned names with a log number appended (for example, `HTSMGuiTrace1.log` and `HTSMGuiTrace2.log`). The log files are used and written to in the order of the log numbers. A round robin method is applied, meaning that, after the end of the last file has been reached, the first file is overwritten.

After the Tiered Storage Manager server starts, writing continues to the file to which the last log data was written, regardless of whether the server stopped normally last time.

Default: 10



Caution: If you have changed the property value, restart the HBase Storage Mgmt Common Service to enable the new value.

logger.serverMessageMaxFileSize

Specify the maximum size of message log files used by the Tiered Storage Manager server (`HTSMServerMessageN.log`). The range of specifiable values is from 32,768 bytes (32 KB) to 2,147,483,647 bytes (less than 2,048 MB). When specifying this property, use `KB` to represent the size in kilobytes, and `MB` to represent the size in megabytes. If a unit is not specified, it is assumed that the value is specified in bytes.

Default: 1,048,576 (1 MB)

logger.serverTraceMaxFileSize

The maximum size of trace log files used by the Tiered Storage Manager server (`HTSMServerTraceN.log`). The range of specifiable values is from 32,768 bytes (32 KB) to 2,147,483,647 bytes (less than 2,048 MB). When specifying this property, use `KB` to represent the size in kilobytes, and `MB` to represent the size in megabytes. If a unit is not specified, it is assumed that the value is specified in bytes.

Default: 5,242,880 (5 MB)

logger.guiMessageMaxFileSize

Specify the maximum size of message log files used by the Web client (`HTSMGuiMessageN.log`). The range of specifiable values is from 32,768 bytes (32 KB) to 2,147,483,647 bytes (less than 2,048 MB). When

specifying this property, use `KB` to represent the size in kilobytes, and `MB` to represent the size in megabytes. If a unit is not specified, it is assumed that the value is specified in bytes.

Default: 1,048,576 (1 MB)



Caution: If you have changed the property value, restart the HBase Storage Mgmt Common Service to enable the new value.

logger.guiTraceMaxFileSize

Specify the maximum size of trace log files used by the Web client (`HTSMGuiTracen.log`). The range of specifiable values is from 32,768 bytes (32 KB) to 2,147,483,647 bytes (less than 2,048 MB). When specifying this property, use `KB` to represent the size in kilobytes, and `MB` to represent the size in megabytes. If a unit is not specified, it is assumed that the value is specified in bytes.

Default: 5,242,880 (5 MB)



Caution: If you have changed the property value, restart the HBase Storage Mgmt Common Service to enable the new value.

Configuring environment settings related to linking to Tuning Manager

In the `tuningmanager.properties` file, you can configure the environment settings related to linking to Tuning Manager.

The following describes the properties set in the `tuningmanager.properties` file.

htnm.infoAcquirePeriod

Tuning Manager collects performance information from the monitored storage subsystems every minute, every hour, or at some other interval. Tuning Manager summarizes the collected information by week or by month. This property specifies whether Tiered Storage Manager acquires performance information summarized by week or by month. Specify the character string `week` or `month` for this property.

Default: `week`

Tiered Storage Manager uses the performance information that was collected by Tuning Manager and summarized by a time period of either week or month. If information for both the last period and the current period is acquired, the information of the last period is displayed. If information for only one period is acquired, the acquired information is displayed. If no information for a period has been acquired, no performance information is displayed.

[Table A-4: Relationship between the performance information acquired and the information displayed by Tiered Storage Manager](#) shows the relationship between the performance information acquired and the information displayed by Tiered Storage Manager.

Table A-4: Relationship between the performance information acquired and the information displayed by Tiered Storage Manager

Performance information acquisition summarized by Tuning Manager		Information displayed by Tiered Storage Manager
Data of last week (last month)	Data of this week (this month)	
Yes	Yes	Data of last week (last month)
Yes	--	
--	Yes	Data of this week (this month)
--	--	Nothing
Legend: Yes: Acquired, --: Not acquired		

Figure A-2: When week is specified for the `htnm.infoAcquirePeriod` Property shows the information acquired from Tuning Manager when `week` is specified for the `htnm.infoAcquirePeriod` property.

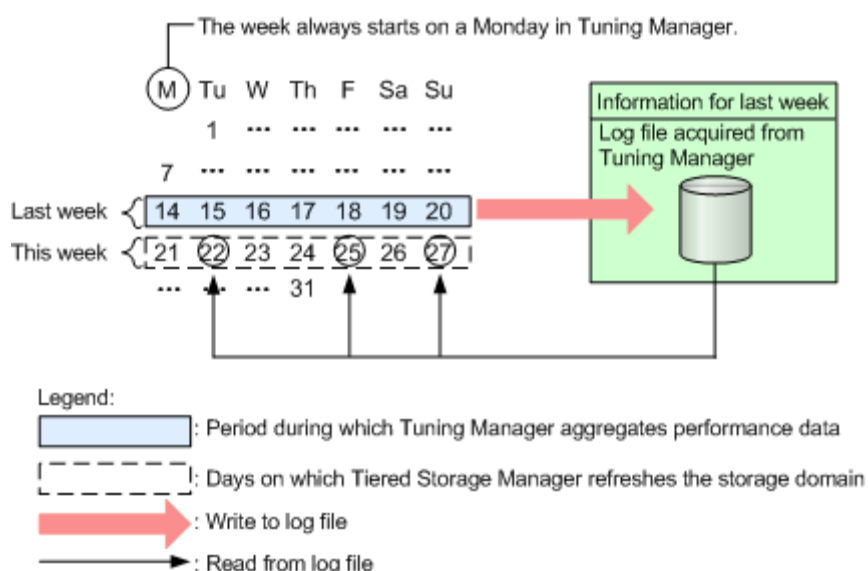


Figure A-2: When week is specified for the `htnm.infoAcquirePeriod` Property

No matter how many times the storage domain is refreshed during the week, the same information (for last week) is collected from Tuning Manager.

Figure A-3: When month is specified for the `htnm.infoAcquirePeriod` Property shows the information acquired from Tuning Manager when `month` is specified for the `htnm.infoAcquirePeriod` property.

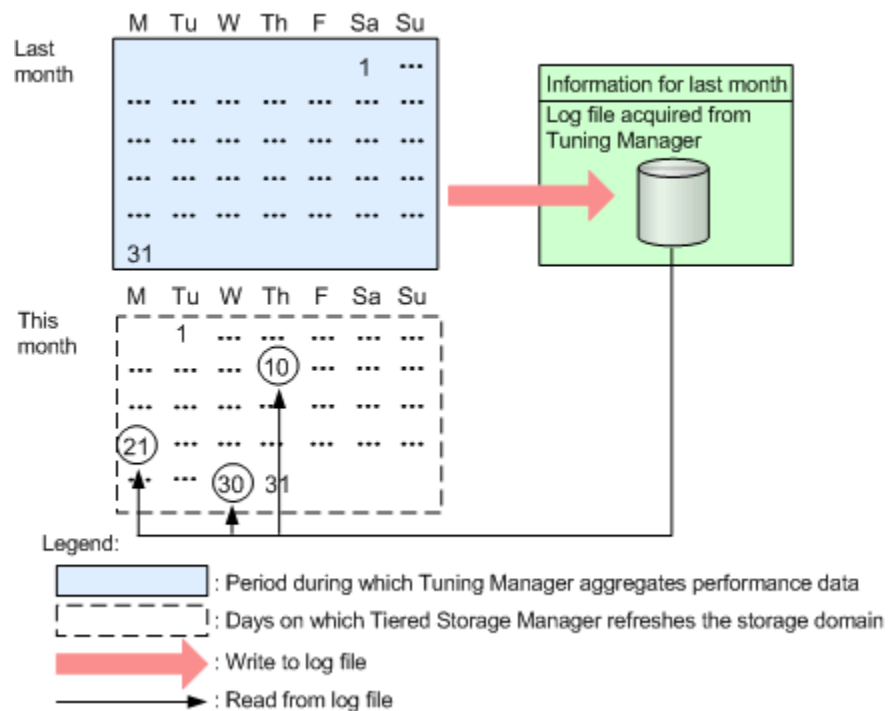


Figure A-3: When month is specified for the `htnm.infoAcquirePeriod` Property

No matter how many times the storage domain is refreshed during the month, the same information (for last month) is collected from Tuning Manager.

Tuning Manager summarizes the collected data by units of hour, day, week, month, and year. Use the Tuning Manager GUI to view performance information that Tiered Storage Manager cannot acquire from Tuning Manager. For details on the performance information that is summarized by Tuning Manager, and how to interpret the performance information, see the manuals for Tuning Manager.

htnm.infoCachePeriodInMinute

Tuning Manager manages the correspondence between each Tuning Manager Agent and the storage subsystem it monitors. Tiered Storage Manager caches this correspondence information to shorten the time needed for acquiring performance information from Tuning Manager. This property allows you to specify the period of time (in minutes) that information about the correspondence between a Tuning Manager agent and its storage subsystem is kept in the cache. The range of specifiable values is from 5 to 10,080.

Default: 60

htnm.servers

This setting specifies the number of Tuning Manager servers to be connected. The range of specifiable values is from 0 to 3.

Default: 0

htnm.server.*n*.host

This setting specifies the host name or IP address of a Tuning Manager server to access. Specify a character string for this property. Note that an IPv6 address cannot be used.

Default: None

For *n* in the property name, specify a value in the range from 0 to *value-specified-in-htnm.servers-property* - 1.

Example: `htnm.server.0.host=htnm_sv1`

htnm.server.*n*.port

This setting specifies the port number to access of a HBase Storage Mgmt Web Service for a Tuning Manager server. The range of specifiable values is from 1024 to 65535.

Default: None

For *n* in the property name, specify a value in the range from 0 to *value-specified-in-htnm.servers-property* - 1.

Example: `htnm.server.0.port=23015`

Estimating trace log volume

When setting the log output environment, you need to first estimate how much information will be output to the log file. This appendix describes how to estimate the volume of information output to the trace log files of the server.

- ❑ [Estimating the volume of trace information output to the trace log file](#)
- ❑ [Estimating trace log volume for different events](#)

Estimating the volume of trace information output to the trace log file

The trace log file has the following two properties:

- `logger.serverTraceFileCount...(1)`
- `logger.serverTraceMaxFileSize...(2)`

The size of trace information that you can save is (1) x (2).

Use the trace information to perform an investigation when a failure occurs. Because of the typical time lag between a failure and the collection of information about that failure, we recommend that you save one week's worth of trace information.

For details on estimating the volume of trace information that is output, see [Symbol definitions](#) and the sections following it. [Symbol definitions](#) and the sections following it provide formulas for estimating trace information output by the operations and processes listed below. These operations and processes account for the majority of trace information:

- Storage domain refreshing
- Scheduling for task information updates
- Event monitoring
- Monitoring of automatic synchronization with Device Manager

There are operations other than those listed above that output trace information. However, the information output in those operations is proportionately small and the individual values are not provided. Furthermore, the values acquirable with these formulas are approximations, and the actual values fluctuate depending on factors such as name lengths. Therefore, we recommend that you assume a value 10-20% higher than the estimation reached with the formulas.

Symbol definitions

[Table B-1:Symbol definitions](#) shows the definitions of the symbols.

Table B-1: Symbol definitions

Symbol	Description
<i>NumDomain</i>	Number of storage domains managed by Tiered Storage Manager
<i>MaxDeviceNumber</i>	Maximum number of devices on the controller ^{#1}
<i>NumArrayGroup</i>	Number of array groups on the controller ^{#2}
<i>NumPath</i>	Number of paths on the controller ^{#2}
<i>NumMF</i>	Number of mainframes on the controller ^{#2}
<i>NumLDEV</i>	Number of LDEVs on the controller ^{#2}
<i>NumExternalSystem</i>	Number of external subsystems

Symbol	Description
<i>MaxExternalDeviceNumber</i>	Maximum number of devices on each external subsystem
<i>SumExternalArrayGroup</i>	Total number of array groups on the external subsystem (only groups used by the storage domain)
<i>SumExternalPath</i>	Total number of paths on the external subsystem (only paths used by the storage domain)
<i>NumExternalLDEV</i>	Number of externally connected LDEVs
<i>NumLogicalGroupPath</i>	Number of paths that belong to logical groups (for all logical groups registered to Device Manager)
<i>NumHSDPath</i>	Number of paths that belong to the host storage domain (only in the corresponding storage domain)
<i>NumLockedVolume</i>	Number of locked volumes
<i>NumSubsystem</i>	Number of subsystems registered in Device Manager
#1 For Universal Storage Platform V: (maximum-number-of-devices-in-the-corresponding-storage-domain) - (minimum-number-of-devices-in-the-corresponding-storage-domain) + 1 #2 For Universal Storage Platform V, this is the number of items that belong to the storage domain. The number of items that do not belong to the logical DKC specified during the creation of the storage domain is not included.	

Estimating trace log volume for different events

This section describes how to estimate trace log volume for the following events.

When refreshing a single storage domain

<Number of lines>

```

500 +
12 x (MaxDeviceNumber / 50) + 56 x (MaxDeviceNumber / 5,000) +
4 x NumArrayGroup +
2 x NumPath +
4 x (NumMF / 5,000) +
4 x (NumLDEV / 5,000) +
58 x NumExternalSystem +
4 x sum of (MaxExternalDeviceNumber / 5,000) for each external
subsystem
4 x SumExternalArrayGroup +
2 x SumExternalPath +
4 x NumExternalLDEV +
4 x (NumLogicalGroupPath / 100) +
4 x (NumHSDPath / 100) +
8 x NumLockedVolume +
6 x NumSubsystem

```

<Bytes>

number-of-lines-calculated x 200 [Unit: Bytes]

When performing a task information update

Volume per output

Condition: There are no tasks being executed or requested.

<Number of lines>

$12 + 92 \times NumDomain$

<Bytes>

$1,850 + 17,500 \times NumDomain$ [Unit: Byte]

Volume per day

Condition: The execution interval is five minutes (288 executions per day).

<Number of lines>

$3,500 + 27,000 \times NumDomain$

<Bytes>

$525,000 + 5,000,000 \times NumDomain$ [Unit: Byte]

or

$0.5 + 4.8 \times NumDomain$ [Unit: MB]

For event-monitoring processing

Volume per output

Condition: No events to be processed have occurred.

<Number of lines>

$24 \times NumDomain + \text{sum of } 8 \times NumLockedVolume\text{-for-each-storage-domain}$

<Bytes>

$5,000 \times NumDomain + 3,500 \times \text{sum of } NumLockedVolume\text{-for-each-storage-domain}$ [Unit: Byte]

Volume per day

Conditions:

- The execution interval is 180 minutes (8 executions per day)[#].
You can change this condition by using `server.eventMonitoringIntervalInMinute`.
- The value to be output is for one storage domain.
- No events to be processed have occurred.

<Number of lines>

$192 + 64 \times \text{NumLockedVolume}$

<Bytes>

$40,000 + 28,000 \times \text{NumLockedVolume}$ [Unit: Byte]

or

$0.04 + 0.03 \times \text{NumLockedVolume}$ [Unit: MB]

When monitoring automatic synchronization with Device Manager

Volume per output

Condition: You only want to check whether synchronization is required. For details about cases where refreshing has occurred, see [When refreshing a single storage domain](#).

<Number of lines>

$12 + 8 \times \text{NumDomain}$

<Bytes>

$2,250 + 1,500 \times \text{NumDomain}$ [Unit: Byte]

Volume per day

Condition: The execution interval is 30 minutes (48 executions per day)[#].

[#] You can change this condition by using `server.repository.autoRefresh.pollingIntervalInMinute`.

<Number of lines>

$576 + 384 \times \text{NumDomain}$

<Bytes>

$105 + 70 \times \text{NumDomain}$ [Unit: KB]

or

$0.1 + 0.07 \times \text{NumDomain}$ [Unit: MB]



Acronyms and Abbreviations

The following acronyms and abbreviations might be used in this guide.

A

AJP

Apache JServ Protocol

API

Application Programming Interface

ASCII

American Standard Code for Information Interchange

C

CLI

Command Line Interface

CPU

Central Processing Unit

CSV

Comma Separated Value

D

DKC

Disk Controller

#	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
---	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------

DP

Dynamic Provisioning

F**FC**

Fibre Channel

G**GB**

Gigabyte(s)

GUI

Graphical User Interface

H**HSSM**

Hitachi Storage Service Manager

HSSO

HiCommand Single Sign On

HTML

Hypertext Markup Language

HTTP

Hypertext Transfer Protocol

HTTPS

Hypertext Transmission Protocol Secure

I**ID**

Identifier

IP

Internet Protocol

IPF

Itanium[®] Processor Family

#	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
---	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------

Acronyms—2

IPv4

Internet Protocol Version 4

IPv6

Internet Protocol Version 6

J**JDK**

Java Development Kit

JRE

Java Runtime Environment

K**KB**

Kilobyte(s)

L**LDEV**

Logical Device

LDKC

Logical Disk Controller

LU

Logical Unit

LUN

Logical Unit Number

LVI

Logical Volume Image

M**MRCF-Lite**

Multiple RAID Coupling Feature – Lite

#	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
---	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------	-------------------

O

OS

Operating System

R

RADIUS

Remote Authentication Dial-In User Service

RAID

Redundant Array of Independent Disks

RMI

Remote Method Invocation

S

SAN

Storage Area Network

SCSI

Small Computer System Interface

SMI-S

Storage Management Initiative – Specification

SMTP

Simple Mail Transfer Protocol

SNMP

Simple Network Management Protocol

SSL

Secure Sockets Layer

SSO

Single Sign On

T

TCP/IP

Transmission Control Protocol/Internet Protocol

#	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---

TLS

Transport Layer Security

U**UID**

User Identifier

URL

Uniform Resource Locator

UTF

UCS Transformation Format

#	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---

#	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---



Glossary

This glossary defines the special terms used in this document. Click the desired letter below to display the glossary entries that start with that letter.

C

client.properties file

A property file used to configure the environment settings related to the Web client display and operations.

command log

Log data from command error messages when the message log and the trace log are not ready to accept the messages. The log data consists primarily of error messages caused by environment settings errors.

Common Component

A component that provides functions shared by Hitachi Storage Command Suite products.

This component is installed as a part of Device Manager, and provides functions such as login, integrated log output, and Web services.

D

database.properties file

A property file used to configure the environment settings for the repositories of the Tiered Storage Manager server.

data erasure

A function to erase the data on the migration source volumes after migration finishes.

#	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---

Device Manager

A prerequisite program product of Tiered Storage Manager. Device Manager provides a unified interface for managing a system consisting of storage subsystems.

devicemanager.properties file

A property file used to configure the environment settings related to access from the Tiered Storage Manager server to the Device Manager server.

Device Number (DEVN)

A number that is used to identify an LDEV.

domain controller

The storage subsystem used to control a storage domain. Universal Storage Platform V/VM and Hitachi USP can be used as domain controllers.

E

emulation type

An LDEV attribute used when an LDEV is created in an array group of the Universal Storage Platform V/VM, Hitachi USP, Lightning 9900V, or Lightning 9900 storage subsystems. The LDEV size is determined from its emulation type attribute.

external storage subsystem

A storage subsystem connected to the domain controller by the external storage connection function provided by Universal Volume Manager. Tiered Storage Manager registers an external storage subsystem as belonging to the same storage domain as the internal storage subsystem (Universal Storage Platform V/VM or Hitachi USP) it is connected to.

external volume

A volume on an external storage subsystem.

H

Hitachi Storage Command Suite common log

Contains common log data output by Hitachi Storage Command Suite products. The Hitachi Storage Command Suite common log data consists of the following three types:

Integrated trace log data

Event log data (Windows)

syslog (Solaris or Linux)

#	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---

Hitachi Storage Command Suite products

A general term for Hitachi storage-related products.

Versions earlier than 6.0 used the brand name *HiCommand*. Since version 6.0, however, the brand name is *Hitachi Storage Command Suite*.

I

internal volume

A volume in Universal Storage Platform V/VM or Hitachi USP. Specifically, this term is used to distinguish such volumes from external volumes.

K

KB

Kilobyte(s).

L

(LDEV) logical device

A logical partition of storage areas in an array group of a storage subsystem. An LDEV is represented by a combination of the storage subsystem's product name, serial number, and an internal LU. Also called a *logical device*.

logger.properties file

A property file used to configure the environment settings related to log output.

LU (logical unit)

A logical disk made public to a host as a SCSI LDEV on a storage-subsystem port.

M

management client

A computer that uses the Web client or the CLI client of Tiered Storage Manager.

management server

A computer on which the Tiered Storage Manager server is installed.

#	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---

message log

A history of user-executed processes and processing results. Log data output to the message log is more detailed than log data output to the Hitachi Storage Command Suite common log.

migration

Relocation of application data from the current storage location to another storage location. This change in data storage location does not affect applications.

P

property file

A file used for settings such as server operation and default options for CLI execution. The six Tiered Storage Manager server property files are as follows:

```
server.properties file
client.properties file
database.properties file
devicemanager.properties file
logger.properties file
tuningmanager.properties file
```

There are two CLI client property files:

```
htsmcli.properties file
htsmclienv.properties file
```

R

repository

A database used to manage information about Hitachi Storage Command Suite products. In a repository, common information about Hitachi Storage Command Suite products and individual product information are managed separately.

A database used to manage Tiered Storage Manager information is generally called a Tiered Storage Manager *repository*. In this manual and Tiered Storage Manager messages, a Tiered Storage Manager repository might be referred to simply as a *database*.

#	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---

S

server.properties file

A property file used to configure the environment settings related to the Tiered Storage Manager server operations.

storage subsystem

An external memory device connected to a host. It includes a controller and disk drives.

T

trace log

Log data collected to determine the cause of problems that occur on the Tiered Storage Manager server.

U

Universal Volume Manager

A program that enables storage subsystems to establish external connections with Universal Storage Platform V/VM or Hitachi USP. For details on storage subsystems that support external connections to Universal Storage Platform V/VM and Hitachi USP, see the Universal Volume Manager User's Guide.

V

volume

A storage area in which application data is stored. A logical unit (LU) is a type of volume.

#	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---

#	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---

Index

Numerics

- 23015/tcp 2-10
- 23016/tcp 2-11
- 23017/tcp 2-11
- 23018/tcp 2-11
- 23019/tcp 2-11
- 23031/tcp 2-11
- 23032/tcp 2-11
- 23033/tcp 2-11
- 23034/tcp 2-11
- 45001/tcp 2-11
- 49000/tcp 2-11, 2-12

A

- account.lock.num 2-30
- audit log
 - AccessControl 4-34
 - audit event 4-18
 - Authentication 4-19
 - ConfigurationAccess 4-19
 - event descriptions 4-18
 - objective 4-17
 - output format 4-38
 - output volume 4-50
 - settings 4-36
 - severity 4-36
 - StartStop 4-18

B

- backing up
 - repositories (Solaris or Linux) 3-25
 - repositories (Solaris) 3-26
 - repositories (Windows) 3-22, 3-23

C

- changing
 - 23018/tcp 2-12, 2-13
 - host name of management server 2-6
 - IP address of management server 2-4
 - URL information 2-25
- checking

- Tiered Storage Manager server status 3-6
- client.ldev.rowsperpage.retain.enabled A-11
- client.properties A-11
- command log 4-7
- command logs
 - output format 4-12
- command trace log entries
 - output format 4-11
- command trace logs 4-6
- Common Component
 - integrated logging output log files 4-14
 - starting (Solaris or Linux) 3-8
 - starting (Windows) 3-8
 - stopping (Solaris or Linux) 3-10
 - stopping (Windows) 3-9
- components
 - Tiered Storage Manager 1-2
- computer specifications
 - management server 1-10
- configuring
 - SSL 2-13
- configuring environment settings related to log output A-12
- configuring environment settings related to the repositories A-11
- customizing
 - event notification templates 2-16

D

- database.properties A-11
- dbm.traceSQL A-11
- deleting
 - warning banner message 2-34
- disconnecting
 - management server network 2-38
- domain controller 1-2
 - storage subsystem 1-20

E

- editing
 - warning banner message 2-32
- estimating

- volume of trace log files B-2
- event log 4-15
- event log entries
 - output format 4-9
- event notification
 - registering 2-15
- event notification function 2-15
- event type 4-14
- exporting
 - repositories (Solaris or Linux) 3-18
 - repositories (Windows) 3-14
- external storage subsystem 1-2

G

- generating
 - audit log data 4-17

H

- hcmdschgurl command 2-25
- hcmsggetlogs command 4-62, 4-63
 - setting up environment 4-63
- hdvm.host A-12
- hdvm.port A-12
- hdvm.protocol A-12
- hdvm.timeout A-12
- Hitachi Storage Command Suite Common trace
 - log file 4-15
- HSSM
 - starting 2-37
- htnm.infoAcquirePeriod A-17
- htnm.infoCachePeriodInMinute A-19
- htnm.server.n.host A-20
- htnm.server.n.port A-20
- htnm.servers A-19
- HtsmgetTI.properties 4-63
- htsmmodmailuser 2-21

I

- importing
 - repositories (Solaris or Linux) 3-19
 - repositories (Windows) 3-15
- integrated logging
 - output log files 4-14
- integrated trace log entries
 - output format 4-8
- IPv6 2-2
- IPv6 environment
 - restrictions 2-2
 - settings 2-2

L

- logger.guiMessageFileCount A-15
- logger.guiMessageMaxFileSize A-16
- logger.guiTraceFileCount A-16
- logger.guiTraceMaxFileSize A-17
- logger.properties A-12
- logger.serverMessageFileCount A-15
- logger.serverMessageMaxFileSize A-16

- logger.serverTraceFileCount A-15
- logger.serverTraceMaxFileSize A-16
- logger.syslogLevel A-14
- logger.tracelogLevel A-14

M

- management client 1-2
 - disk space 1-19
 - memory 1-20
- management server 1-2
 - changing host name 2-6
 - changing IP address 2-4
 - computer specifications 1-10
 - CPU 1-10
 - disk capacity 1-10
 - memory 1-10
 - related software 1-9
 - required programs 1-8
- message ID 4-13
- message log entries
 - output format 4-8
- message logs 4-5
- message type 4-13
- moving
 - repositories (cautionary notes) 3-13
 - repositories (Solaris or Linux) 3-17
 - repositories (Windows) 3-14

N

- network
 - settings required when disconnecting
 - management server 2-38
- non-cluster environment
 - system configuration 1-2

P

- password.check.userID 2-29
- password.min.length 2-29
- password.min.lowercase 2-29
- password.min.numeric 2-29
- password.min.symbol 2-29
- password.min.uppercase 2-29
- ports
 - changing 2-9
- prerequisites
 - SMI-S Enabled subsystem 1-21
- properties
 - Tiered Storage Manager A-2

R

- registering
 - application 2-23
 - event notification 2-15
 - warning banner message 2-33
- related software
 - management server 1-9
- repositories
 - backing up (Solaris or Linux) 3-25

Index-2

- backing up (Solaris) 3-26
- backing up (Windows) 3-22, 3-23
- exporting (Solaris or Linux) 3-18
- exporting (Windows) 3-14
- importing (Solaris or Linux) 3-19
- importing (Windows) 3-15
- moving (cautionary notes) 3-13
- moving (Solaris or Linux) 3-17
- moving (Windows) 3-14
- restoring (Solaris or Linux) 3-34
- restoring (Solaris) 3-36
- restoring (Windows) 3-30, 3-31
- required programs
 - management server 1-8
 - SMI-S Enabled subsystem 1-21
- restoring
 - repositories (Solaris or Linux) 3-34
 - repositories (Solaris) 3-36
 - repositories (Windows) 3-30, 3-31
- restrictions
 - IPv6 environments 2-2

S

- security.conf 2-28
- server 3-2
- server. A-10, A-9
- server.base.initialsynchro A-6
- server.checkOutVolumeRange A-8
- server.eventMonitoringIntervalInMinute A-7
- server.eventNotification.mail.to A-7
- server.mail.errorsTo A-7
- server.mail.from A-6
- server.mail.smtp.auth A-7
- server.mail.smtp.host A-6
- server.mail.smtp.port A-7
- server.migration.dataErase.defaultValue A-9
- server.migration.maxRetryCount A-10
- server.migration.multiExecution A-7
- server.properties A-5
- server.repository.autoRefresh.pollingIntervalInMinute A-8
- server.repository.autoRefresh.recurringLocalTime A-8
- server.repository.dvmModifyCheck.pollingIntervalInMinute A-9
- server.rmi.port A-6
- server.rmi.secure A-5
- server.rmi.security.port A-6
- server.volumeCreation.param.defaultPortController A-10
- service request reception log 4-7
- service request reception log entries
 - output format 4-12
- setting
 - IPv6 environments 2-2
 - locking System account 2-30
 - user accounts security 2-28
- settings
 - audit log 4-36

- warning banner 2-32
- SMI-S Enabled subsystem
 - prerequisites for connecting 1-21
 - required programs 1-21
 - storage subsystems 1-21
- SMTP
 - authentication user information 2-21
- specifying
 - number of trace log files 4-15
 - size of trace log files 4-16
 - SMTP authentication user information 2-21
- SSL 2-13
 - configuring 2-13
- SSL communication
 - electronic certificate 2-14
- starting
 - Common Component (Solaris or Linux) 3-8
 - Common Component (Windows) 3-8
 - HSSM 2-37
 - Tiered Storage Manager server 3-2
- stopping
 - Common Component (Solaris or Linux) 3-10
 - Common Component (Windows) 3-9
 - Tiered Storage Manager server 3-3
- storage subsystem
 - domain controller 1-20
- storage subsystems
 - SMI-S Enabled subsystem 1-21
- supported OSs
 - management server 1-4
- syslog entries
 - output format 4-10
- syslog file 4-15
- System account
 - settings for locking 2-30
 - unlocking 2-31
- system configuration
 - cluster environment 1-3
 - non-cluster environment 1-2
- system requirements for the CLI client
 - management client 1-17
- system requirements for the Web client
 - management client 1-13

T

- Tiered Storage Manager server
 - checking status 3-6
 - starting 3-2
 - stopping 3-3
- Tiered Storage Manager
 - components 1-2
 - property descriptions A-2
- TLS 2-13
- trace log 4-6
 - estimating volume B-2
 - specifying size of file 4-16
- trace log entries
 - output format 4-8
- troubleshooting information 4-2

U

unlocking
 System account 2-31

URL
 changing 2-25

user account
 security settings 2-28

W

warning banner
 configuration 2-32
 deleting message 2-34
 editing message 2-32
 registering message 2-33

Web application
 registering 2-23

Hitachi Data Systems

Corporate Headquarters

750 Central Expressway
Santa Clara, California 95050-2627
U.S.A.
Phone: 1 408 970 1000
www.hds.com
info@hds.com

Asia Pacific and Americas

750 Central Expressway
Santa Clara, California 95050-2627
U.S.A.
Phone: 1 408 970 1000
info@hds.com

Europe Headquarters

Sefton Park
Stoke Poges
Buckinghamshire SL2 4HD
United Kingdom
Phone: + 44 (0)1753 618000
info.eu@hds.com



MK-08HC158-04