HITACHI
Inspire the Next

Hitachi Command Suite

Administrator Guide

Hitachi Data Systems

MK-90HC175-25

© 2014, 2016 Hitachi, Ltd. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including copying and recording, or stored in a database or retrieval system for commercial purposes without the express written permission of Hitachi, Ltd., or Hitachi Data Systems Corporation (collectively "Hitachi"). Licensee may make copies of the Materials provided that any such copy is: (i) created as an essential step in utilization of the Software as licensed and is used in no other manner; or (ii) used for archival purposes. Licensee may not make any other copies of the Materials. "Materials" mean text, data, photographs, graphics, audio, video and documents.

Hitachi reserves the right to make changes to this Material at any time without notice and assumes no responsibility for its use. The Materials contain the most current information available at the time of publication.

Some of the features described in the Materials might not be currently available. Refer to the most recent product announcement for information about feature and product availability, or contact Hitachi Data Systems Corporation at https://support.hds.com/en_us/contact-us.html.

Notice: Hitachi products and services can be ordered only under the terms and conditions of the applicable Hitachi agreements. The use of Hitachi products is governed by the terms of your agreements with Hitachi Data Systems Corporation.

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

1) Acquiring the relevant consents as may be required under local privacy laws or otherwise from authorized employees and other individuals to access relevant data; and

2) Verifying that data continues to be held, retrieved, deleted, or otherwise processed in accordance with relevant laws.

Notice on Export Controls. The technical data and technology inherent in this Document may be subject to U.S. export control laws, including the U.S. Export Administration Act and its associated regulations, and may be subject to export or import regulations in other countries. Reader agrees to comply strictly with all such regulations and acknowledges that Reader has the responsibility to obtain licenses to export, re-export, or import the Document and any Compliant Products.

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

AIX, AS/400e, DB2, Domino, DS6000, DS8000, Enterprise Storage Server, eServer, FICON, FlashCopy, IBM, Lotus, MVS, OS/390, PowerPC, RS/6000, S/390, System z9, System z10, Tivoli, z/OS, z9, z10, z13, z/VM, and z/VSE are registered trademarks or trademarks of International Business Machines Corporation.

Active Directory, ActiveX, Bing, Excel, Hyper-V, Internet Explorer, the Internet Explorer logo, Microsoft, the Microsoft Corporate Logo, MS-DOS, Outlook, PowerPoint, SharePoint, Silverlight, SmartScreen, SQL Server, Visual Basic, Visual C++, Visual Studio, Windows, the Windows logo, Windows Azure, Windows PowerShell, Windows Server, the Windows start button, and Windows Vista are registered trademarks or trademarks of Microsoft Corporation. Microsoft product screen shots are reprinted with permission from Microsoft Corporation.

All other trademarks, service marks, and company names in this document or website are properties of their respective owners.

Contents

Preface..... 21
Intended audience..... 22
Product version..... 22
Release notes..... 22
Document organization..... 22
Related documents..... 23
Document conventions..... 24
Conventions for storage capacity values..... 25
Accessing product documentation..... 26
Getting help..... 26
Comments..... 26

1 System configuration and requirements..... 27
System configuration..... 29
Network security configuration..... 33
Common security risks..... 33
Security configuration recommended for Device Manager..... 34
System requirements for the management server and Host Data Collector computers 35
Maximum number of resources that can be managed..... 35
Changing the memory heap size..... 36
Changing the JDK of management servers..... 37
Changing the Java execution environment used by Host Data Collector..... 39
Hosts that can be managed by Device Manager..... 40
Host management software supported by Device Manager..... 40
Prerequisites for normal hosts..... 42
Prerequisites for normal hosts 43
Prerequisites for virtual machines..... 45
Prerequisites for virtual machines..... 45
Operation workflow for allocating volumes to virtual machines..... 48
Tasks required to change the virtual machine configuration..... 52
Prerequisites for virtualization servers..... 52
Prerequisites for virtualization servers..... 53

Operation workflow for managing virtualization servers..... 54
Notes on operating virtualization servers..... 54
Prerequisites for mainframe hosts.....54
Operation workflow of managing a mainframe host.....55
Prerequisites for file servers..... 55
Environment settings for NAS Platform family..... 55
Environment settings for Hitachi Data Ingestor and Hitachi NAS Platform F.....57
Operation workflow of managing file servers.....58
Notes on operating file servers..... 59
System requirements for NAS modules..... 59
Operation workflow for managing NAS modules.....60
Notes on operating NAS modules.....60
Related products.....60
System requirements for managing copy pairs..... 62
System configuration for managing copy pairs (central management method)..... 63
System configuration for managing copy pairs (other than the central management method).....67
System configuration for managing copy pairs at each host..... 69
System configuration for using a virtual command device server configuration to manage copy pairs.....73
System configuration for using an SVP configuration to manage copy pairs (when copy pairs are defined in a configuration definition file)..... 77
System configuration for using an SVP configuration to manage copy pairs (when copy pairs are defined as a device group).....80
Storage system requirements for managing copy pairs.....84
Prerequisite version of the Device Manager agent for managing copy pairs 85
Notes on managing copy pairs..... 88
Configuring a high availability system..... 93
Example of a configuration for configuring a high availability system..... 94
Requirements for configuring a high availability system (for VSP G1000, G1500 or VSP F1500).....96
Requirements for configuring a high availability system (for VSP Gx00 models)... 100
Notes on executing commands.....104

2 Network configuration..... 105

Ports used by Hitachi Command Suite products..... 106
Ports used by Common Component.....106
Ports used by the Device Manager server..... 107
Ports used by the Tiered Storage Manager server.....109
Ports used by Host Data Collector..... 109
Ports used by the Device Manager agent..... 111
Ports used by storage systems.....111
Changing ports used by Common Component..... 114
Registering firewall exceptions for Device Manager and Tiered Storage Manager.....121
Port numbers that must be registered as firewall exceptions for Device Manager and Tiered Storage Manager..... 121
Registering firewall exceptions for Device Manager and Tiered Storage Manager in Windows.....138
Registering firewall exceptions for Device Manager and Tiered Storage Manager in Red Hat Enterprise Linux 5 or Red Hat Enterprise Linux 6..... 139

Registering firewall exceptions for Device Manager and Tiered Storage Manager in Red Hat Enterprise Linux 7 or Oracle Linux 7 140
Registering firewall exceptions for Device Manager and Tiered Storage Manager in SUSE Linux Enterprise Server 140
Registering firewall exceptions for Host Data Collector (Windows) 141
Registering an exception for the Host Data Collector service (for non-SSL communication) 141
Registering an exception for the Host Data Collector service (for SSL communication) 142
Network settings with multiple IP addresses 143
Network settings for using a management server as a bridge 143
Specifying settings if the Host Data Collector machine has multiple IP addresses. 145
Device Manager settings in IPv6 environments 145
Settings for migrating Device Manager to an IPv6 environment 145
Settings for linking with storage systems that support IPv6 147
Changing the IP address or host name of the management server 148
Changing the host name of the management server 148
Changing the IP address of the management server 150
Required operations after changing the IP address or host name of the management server 152
Changing the URL for accessing Hitachi Command Suite products (hcmds64chgurl command) 154

3 User account management 157

About password policies 158
Setting password policies 158
About account locking 160
About account locking policies 160
Setting account locking policies 161
Settings for automatically locking the System account 162
Unlocking accounts 162

4 User management on an external authentication server 165

About linking to an external authentication server 166
About linking to an external authorization server 166
Operating workflow for user authentication on an external authentication server 166
Operating workflow for user authentication on an LDAP directory server 166
Operating workflow for user authentication on a RADIUS server 168
Operation workflow for user authentication on a Kerberos server 170
Account conditions for Hitachi Command Suite products 172
About the data structures of user entries 173
About the BaseDN 173
About the hierarchical structure model 173
About the flat model 174
Configurations when multiple external authentication servers are linked 175
Registering an external authentication server and an external authorization server 178
Setup items in the exauth.properties file for LDAP authentication 180
Examples of setting the exauth.properties file for LDAP authentication 187
Setup items in the exauth.properties file for RADIUS authentication 189
Examples of setting the exauth.properties file for RADIUS authentication 196

Setup items in the exauth.properties file for Kerberos authentication..... 198
Examples of setting the exauth.properties file for Kerberos authentication..... 204
About a LDAP search user account..... 205
Conditions for LDAP search user account..... 206
Registering an LDAP search user account..... 207
Deleting an LDAP search user account.....209
Checking the LDAP directory server that registered LDAP search user account.....210
Registering a shared secret..... 210
Deleting a shared secret.....211
Checking the RADIUS server that registered a shared secret on the management server..... 212
Checking connections to an external authentication server and an external authorization server.....212
Notes on commands for setting up a link to an external authentication server..... 215
Encryption types for Kerberos authentication.....216

5 Communication security settings..... 217

Secure communication for Device Manager and Tiered Storage Manager.....218
Default certificate for Device Manager..... 224
Operation workflow for secure communication between a management server and a management client (GUI)..... 225
Operation workflow for secure communication between a management server and a management client (Device Manager CLI).....227
Operation workflow for secure communication between a management server and a management client (Tiered Storage Manager CLI).....229
Operation workflow for secure communication between an LDAP directory server and a management server 230
Operation workflow for secure communication between a Device Manager server and Replication Manager server..... 230
Operation workflow for secure communication between a Tuning Manager server and a Device Manager server.....232
Operation workflow for secure communication between a Host Data Collector machine and a management server.....234
Operation workflow for secure communication between a virtualization server and Host Data Collector..... 235
Operation workflow for secure communication between a management server and Device Manager agent.....237
Operation workflow for secure communication between a storage system and a management server 239
Operation workflow for secure communication between a management server and a storage system (VSP G1000, G1500 or VSP F1500)..... 240
Operation workflow for secure communication between a management server and a storage system (VSP Gx00 models or VSP Fx00 models)..... 242
Operation workflow for secure communication between an SMI-S provider and a management server..... 243
Operation workflow for secure communication between a Tuning Manager server and a Tuning Manager API client.....243
Operation workflow for secure communication between a storage system and a management client (GUI)..... 244
Operation workflow for secure communication between a management server and a CIM client (object operations).....246

Operation workflow for secure communication between a management server and a CIM client (two-way authentication for object operations)....246
Operation workflow for secure communication between a management server and a CIM client (event indications)....248
Operation workflow for secure communication between a management server and a CIM client (two-way authentication for event indications)....248
Truststores....250
Configuring an SSL server (Common Component)....253
Creating a secret key and a certificate signing request for Common Component .253
Applying to a certificate authority for a Common Component server certificate....257
Editing the user_httpsd.conf file to enable SSL/TLS....258
Closing the port for the non-SSL communication (HBase 64 Storage Mgmt Web Service)....262
Checking the expiration date of the certificate (Common Component)....265
Configuring an SSL server (Device Manager server)....266
Creating a key pair and a self-signed certificate for Device Manager server....266
Enabling SSL/TLS for the Device Manager server....269
Creating a certificate signing request for Device Manager server....270
Applying to a certificate authority for a Device Manager server certificate....271
Importing a server certificate into the Device Manager server keystore....273
Viewing the Device Manager server key pair information in normal mode....274
Viewing the Device Manager server key pair information in verbose mode....275
Deleting a key pair from the Device Manager server keystore....276
Changing the password of a Device Manager server key pair....277
Changing the password of the Device Manager server keystore....278
Importing a certificate into the Device Manager server truststore....278
Viewing the Device Manager server truststore information in normal mode....279
Viewing the Device Manager server truststore information in verbose mode....280
Deleting a server certificate from the Device Manager server truststore....281
Changing the password of the Device Manager server truststore....283
Checking the server certificate of the Device Manager server....284
Configuring an SSL server (Host Data Collector)....284
Creating a key pair and a certificate signing request for Host Data Collector....284
Applying to a certificate authority for a Host Data Collector server certificate....286
Importing the Host Data Collector server certificates into the keystore 287
Checking a Host Data Collector server certificate....288
Configuring an SSL client....288
Downloading a Device Manager server truststore file....288
Creating a truststore file to be used in the Device Manager CLI....289
Exporting a Device Manager server self-signed certificate....290
Importing a certificate into a web browser (Internet Explorer)....291
Importing a certificate into a web browser (Firefox)....292
Importing a certificate into a web browser (Google Chrome)....292
Changing pop-up blocker settings....293
Enabling SSL/TLS for the Device Manager CLI computer....294
Downloading the Tiered Storage Manager server truststore files....295
Enabling SSL/TLS for the Tiered Storage Manager CLI computer....296
Importing a certificate into the truststore for Common Component....298
Conditions for an LDAP directory server certificate....300
Checking the certificates imported into the truststore for Common Component... 301
Deleting the certificates imported into the truststore for Common Component....302

Changing the communication protocol between the Replication Manager server and the Device Manager server..... 303
Importing a certificate into the truststore for Device Manager server..... 303
Checking the certificates imported into the truststore for Device Manager server. 305
Importing a certificate into the truststore for Host Data Collector..... 305
Checking the server certificate imported into the truststore for the Host Data Collector.....306
Changing the truststore password for the Host Data Collector..... 307
Changing virtualization server information..... 308
Importing a server certificate into the truststore for the Device Manager agent... 308
Checking the server certificate imported into the truststore for the Device Manager agent.....310
Changing the truststore password for the Device Manager agent.....311
Deleting a server certificate imported into the truststore for the Device Manager agent.....312
Changing storage system information.....313
Configuring an SSL server and clients (CIM server)..... 314
Creating a keystore file for object operations..... 314
Editing an MOF file for object operations..... 315
Exporting a server certificate for object operations..... 317
Enabling two-way authentication for object operations..... 317
Importing a client certificate for object operations.....319
Creating a keystore file for event indications..... 319
Editing an MOF file for event indications..... 321
Exporting a client certificate for event indications..... 322
Enabling two-way authentication for event indications..... 323
Importing a server certificate for event indications..... 324
Checking a self-signed certificate for a CIM server.....325
Self-signed certificate for object operations supplied with the product.....326
Disabling two-way authentication.....326
Configuring an SSL server and clients (CIM client) 327
Creating a key pair and self-signed certificate for a CIM client..... 327
Exporting a server or client certificate for a CIM client..... 328
Importing a server or client certificate into a CIM client..... 329

6 Configuring Device Manager for use with related products.....331

Settings required for linking with Storage Navigator Modular 2..... 332
Notes and requirements for connecting to Storage Navigator Modular 2.....332
Settings for using Element Manager..... 333
Deleting the settings for using Element Manager.....335
Settings required to collect storage system performance information.....336
System configuration for collecting storage system performance information.....337
Operation workflow for collecting storage system performance information.....340
Settings to enable the Device Manager server, the Tuning Manager server, and Tuning Manager - Agent for RAID to communicate..... 343
Settings for collecting performance information from enterprise-class storage systems, VSP Gx00 models, VSP Fx00 models, and HUS VM.....345
Settings for collecting performance information from midrange storage systems..347
Remote connection to the Tuning Manager server (in a non-cluster environment) 348

Remote connection to the Tuning Manager server (in a Windows cluster environment).....349
Remote connection to the Tuning Manager server (in a Red Hat Enterprise Linux cluster environment).....351
Specifying the settings for remote connection to the Tuning Manager server and the port number (htmsetup command).....352
Setting up the config.xml and configforclient.xml files.....353
Setting up the management client (to collect storage system performance information).....354
Settings required to analyze the performance of Universal Replicator by using the Replication tab.....354
System configuration for analyzing the performance of Universal Replicator by using the Replication tab.....355
Flow of tasks for analyzing the performance of Universal Replicator by using the Replication tab.....358
Setting the port numbers used for RMI communication on the Device Manager server.....360
Configuring an instance environment for a storage system.....360
Starting instances of Tuning Manager - Agent for RAID.....361
Setting up properties to remotely connect to Tuning Manager.....362
Specifying settings to collect performance information to be analyzed in the Replication tab.....363
Changing the time or interval for periodically collecting performance information to be analyzed in the Replication tab.....364
Notes on analyzing the performance of Universal Replicator.....365
Settings required to use the replication management functionality on the Replication tab 365
System configuration for using the replication management functionality on the Replication tab (configuration for multiple sites).....366
Workflow for using the replication management functionality on the Replication tab 367
Installing products necessary for the management server and pair management server.....369
Setting the port numbers used for RMI communication on the Device Manager server.....369
Changing Replication Manager on the secondary site to maintenance mode.....370
Settings required to use the VMware VVol functionality.....370
System configuration for using the VVol functionality.....370
Required configuration for the management server for VVols to improve the availability of VVol management operations.....373
Combinations of components for using the VVol functionality.....375
Flow of tasks for setting the Hitachi Command Suite products for using the VVol functionality.....377
Installing Hitachi Command Suite products on the management server.....379
Changing the Device Manager server settings on the management server.....379
Installing Hitachi Command Suite products on the management server for VVols.380
Changing the Hitachi Command Suite settings on the management server for VVols (in a non-cluster environment).....382
Changing the Hitachi Command Suite settings on the management server for VVols (in a Windows cluster configuration).....383
Changing the Hitachi Command Suite settings on the management server for VVols (in a Linux cluster configuration).....385

Changing the settings on the Hitachi Command Suite for VVols after starting an operation..... 387
Setup items for the vvoladaptersetup tool.....388
Setting the environment on the management server to obtain information on how virtual machines correspond to SLUs (VVols) (When using the Analytics tab).....390
Discarding the environment used for the VMware VVol functionality.....394
Recovering from a failure that occurred on the management server for VVols.....395
Recovering operations completed after the point in time at which the database is restored..... 398
Settings necessary to launch Hitachi Storage Services Manager..... 400

7 Setting up logs and alerts..... 403

Setting up Hitachi Command Suite common trace log files.....404
Setting up Hitachi Command Suite common trace log files (Windows).....404
Setting up Hitachi Command Suite common trace log files (Linux).....404
Setting up alerts.....405
Error detection by Device Manager.....405
Settings for displaying SNMP traps as alerts..... 407
Registering the user who receives SNMP traps (SNMP v3) 409
Format of the command for managing the user who receives SNMP traps (hdvmsnmpuser) (SNMP v3).....409
Operation flow for reporting alerts by email..... 412
Setting up the SMTP server..... 413
Setting up recipients of email alerts.....413
Property settings for reporting alerts..... 414
Registering an SMTP authentication user account in Device Manager.....415
Customizing email alert template..... 416
Sending SNMP traps to log files.....418
Setting up Device Manager to output SNMP traps.....419
Settings required to use Device Manager event notification..... 420
Setting properties for Device Manager event notification 421
Specifying SMTP user authentication information for event notification (hdvmmodmailuser command).....422
Editing the event notification template for Device Manager 423
Settings required to use Tiered Storage Manager event notification.....425
Setting properties for Tiered Storage Manager event notification..... 427
Specifying SMTP user authentication information for event notification (htsmmodmailuser command).....428
Editing event notification templates for Tiered Storage Manager.....430

8 Configuring Device Manager for CIM/WBEM..... 435

About CIM/WBEM.....436
CIM/WBEM functions in Device Manager..... 436
Specifying a namespace.....438
User account settings for using the CIM/WBEM functions..... 439
Specifying the settings for using the CIM/WBEM functions.....439
Changing CIM/WBEM port numbers..... 441
Settings for acquiring storage system performance information by using CIM/WBEM functions..... 441
Required system configuration for acquiring performance information.....442

Specifying the settings required to acquire performance information about Virtual Storage Platform or Universal Storage Platform V/VM storage systems.....443
Format of the command for registering command devices (perf_findcmddev).....445
Format of the perf_cmddev.properties file.....447
Settings required to acquire performance information of midrange storage systems 448
Format of the command for registering a user account to acquire performance information (hdvmmodpolluser).....449
Controlling the SLP service.....450
Software prerequisites for using the service discovery function.....450
Starting the SLP service (Windows).....451
Stopping the SLP service (Windows).....451
Starting the SLP daemon (Red Hat Enterprise Linux or Oracle Linux).....451
Stopping the SLP daemon (Red Hat Enterprise Linux or Oracle Linux).....452
Starting the SLP daemon (SUSE Linux Enterprise Server).....452
Stopping the SLP daemon (SUSE Linux Enterprise Server).....452
Releasing the SLP service (Windows).....453
Releasing the SLP daemon (Linux).....453
Notes on OpenSLP logs.....453

9 Starting and stopping services.....455

Starting and stopping services of Hitachi Command Suite.....456
Resident processes of Hitachi Command Suite.....456
Starting the Hitachi Command Suite services.....458
Stopping the Hitachi Command Suite services.....460
Checking the operating status of the Hitachi Command Suite services.....462
Starting and stopping services of the Host Data Collector.....462
Resident processes of the Host Data Collector.....463
Starting the Host Data Collector service.....464
Stopping the Host Data Collector service.....464
Checking the operating status of the Host Data Collector service.....465
Hitachi Command Suite product services that are registered in cluster management applications.....466

10 Managing the database.....469

Managing databases.....470
Backing up databases.....470
Backing up a database in non-cluster configuration.....471
Backing up a database in a Windows cluster configuration.....472
Backing up a database in a Red Hat Enterprise Linux cluster configuration.....474
Restoring databases.....475
Restoring a database when a data inconsistency occurs in a non-cluster configuration.....476
Restoring a database when a data inconsistency occurs in a Windows cluster configuration.....478
Restoring a database when a data inconsistency occurs in a Red Hat Enterprise Linux cluster configuration.....481
Restoring a database when it is corrupted in a non-cluster configuration.....484
Restoring a database when it is corrupted in a Windows cluster configuration.....486

Restoring a database when it is corrupted in a Red Hat Enterprise Linux cluster configuration..... 489
Migrating databases..... 491
Prerequisites and restrictions on migrating databases..... 492
Procedure for migrating databases..... 493
Installing Hitachi Command Suite products on the migration destination server... 493
Exporting databases on the migration source server (for a non-cluster configuration) 494
Exporting databases on the migration source server (for a Windows cluster configuration)..... 495
Exporting databases on the migration source server (for a Red Hat Enterprise Linux cluster configuration)..... 497
Importing databases on the migration destination server (for a non-cluster configuration)..... 499
Importing databases on the migration destination server (for a Windows cluster configuration)..... 503
Importing databases on the migration destination server (for a Red Hat Enterprise Linux cluster configuration)..... 506

11 Using the Device Manager agent..... 511

Prerequisites for running the Device Manager agent..... 512
Prerequisites for using the Device Manager agent to manage normal hosts..... 512
Prerequisites for using the Device Manager agent to manage virtual machines.... 513
Prerequisites for using a host on which multiple NICs are installed..... 515
Notes on running the Device Manager agent..... 516
Specifying the Device Manager agent environment settings..... 517
Settings for changing the Java execution environment (javapath_setup command) 517
Registering the Windows Firewall exceptions for Device Manager agent (firewall_setup command)..... 519
Registering a Java process in SED as an exception (AIX)..... 520
Managing copy pairs..... 521
Settings required for a host to manage 100 or more LUs..... 524
Resident processes of the Device Manager agent..... 528
Starting and stopping the Device Manager agent service, and checking the operating status of the service (hbsasrv command)..... 528
Changing the user who executes the Device Manager agent service (Windows)... 530
Device Manager agent operations..... 530
Checking the available agent functions (hbsa_modinfo command)..... 530
Deleting the Device Manager agent's registry entries and files (hbsa_util command) 532
Displaying the version of the Device Manager agent (hdvm_info command)..... 533
Setting the Device Manager server's information, HiScan command's execution period, and CCI's information (hdvmagt_setting command)..... 533
Reporting host information to the Device Manager server manually (HiScan command)..... 537
Acquiring device information (hldutil command)..... 539
Information displayed by the hldutil command..... 543
Configuration definition file for managing copy pairs..... 545
Prerequisite environment for using the configuration definition file..... 545
Editing the configuration definition file..... 545

Configuration definition file parameters supported Device Manager..... 547
Description conventions for the configuration definition file..... 547
HORCM_MON parameter description format.....548
HORCM_CMD parameter description format..... 550
HORCM_VCMD parameter description format..... 552
HORCM_DEV parameter description format.....553
HORCM_LDEV parameter description format..... 556
HORCM_INST parameter description format.....558
HORCM_INSTP parameter description format.....560
Changing the storage location of the configuration definition file..... 562
Notes on using the configuration definition file.....562

12 Troubleshooting..... 565

How to troubleshoot problems on the management server (Device Manager related) 566
The user cannot log in to the Device Manager GUI.....566
The services of Common Component or the Device Manager server cannot be started.....566
The Device Manager server cannot be accessed after starting up the management server or Hitachi Command Suite product services..... 567
SNMP traps of Hitachi Data Ingestor and Hitachi NAS Platform F cannot be received 567
An attempt to reconfigure or refresh a storage system failed.....568
How to troubleshoot problems on the management server (Tiered Storage Manager related)..... 569
The Tiered Storage Manager server could not be started..... 569
The Tiered Storage Manager server does not stop.....569
The Tiered Storage Manager server terminates abnormally or fails over in a cluster environment.....570
Tiered Storage Manager operations cannot be performed because an error occurred in the database.....572
How to troubleshoot problems on a host.....572
The HiScan command cannot add host information to the Device Manager server 572
A communication error occurs, and the processing of other Hitachi Command Suite products stops.....573
Two copies of HBase Agent are displayed in the Programs and Features window. 573
HBase Agent is displayed in the Programs and Features window.....573
JavaVM terminates abnormally.....574
An OutOfMemory error occurs on a host, and after a while the host stops responding.....574
The file system name is not displayed in the Device Manager GUI..... 576
Changes to the storage system configuration are not applied to the Device Manager server..... 576
Errors requiring no action..... 576
Maintenance information that must be collected if a failure occurs..... 577
Acquiring maintenance information on the management server (hcmds64getlogs command).....578
Generating the Tiered Storage Manager CLI log file.....581
Acquiring maintenance information for a Host Data Collector computer (hdc_getras command).....582

Acquiring maintenance information on a host managed by Host Data Collector (hdc_target_getras command)....583
Acquiring maintenance information on the Device Manager agent (TIC command)....584
Acquiring a thread dump of the HCS Device Manager Web Service (Windows)....585
Acquiring a thread dump of the HCS Device Manager Web Service (Linux)....586

A Device Manager server properties....587

Device Manager server property files....589
Changing Device Manager server properties....590
Syntax rules for Device Manager server property files....590
Device Manager server configuration properties (server.properties file)....591
server.http.host....591
server.http.port....592
server.https.port....593
server.rmi.port....594
server.http.entity.maxLength....594
server.base.home....595
server.horcmconfigfile.hostname....595
server.base.initialsynchro....595
server.cim.agent....595
server.cim.support....596
server.cim.support.job....596
server.cim.support.protocol....596
server.cim.http.port....596
server.cim.https.port....597
server.configchange.enabled....597
server.logicalview.initialsynchro....598
server.mail.enabled.storagesystem....598
server.mail.enabled.fileserver....598
server.mail.from....599
server.mail.smtp.host....599
server.mail.smtp.port....599
server.mail.smtp.auth....599
server.mail.errorsTo....600
server.eventNotification.mail.to....600
server.mail.alert.type.storagesystem....600
server.mail.alert.status....600
server.subsystem.ssid.availableValues....601
server.smisclient.indication.port....601
server.agent.differentialrefresh.manual.enabled....601
server.agent.differentialrefresh.periodical.enabled....602
server.logicalGroupMapping.updateInterval....602
Device Manager database properties (database.properties file)....602
dbm.traceSQL....603
dbm.startingCheck.retryCount....603
dbm.startingCheck.retryPeriod....603
Device Manager log output properties (logger.properties file)....603
logger.loglevel....604
logger.MaxBackupIndex....604
logger.MaxFileSize....604

logger.hicommandbase.loglevel....605
logger.hicommandbase.sysloglevel....605
logger.hicommandbase.MaxBackupIndex....605
logger.hicommandbase.MaxFileSize....606
Device Manager dispatcher properties (dispatcher.properties file)....606
server.dispatcher.message.timeout....606
server.dispatcher.message.timeout.in.processing....606
server.dispatcher.daemon.pollingPeriod....607
server.dispatcher.traps.purgePeriod....607
server.dispatcher.daemon.receiveTrap....607
server.dispatcher.snm2.configchange.pollingPeriod....607
server.dispatcher.configchange.pollingPeriod....608
server.dispatcher.daemon.configUpdate.detection.interval....608
server.dispatcher.daemon.autoSynchro.doRefresh....609
server.dispatcher.daemon.autoSynchro.type....610
server.dispatcher.daemon.autoSynchro.dayOfWeek....610
server.dispatcher.daemon.autoSynchro.startTime....611
server.dispatcher.daemon.autoSynchro.interval....611
server.dispatcher.daemon.configUpdate.detection.variable.enabled....611
server.dispatcher.daemon.autoSynchro.performance.doRefresh....612
server.dispatcher.daemon.autoSynchro.performance.startTime....613
server.dispatcher.daemon.autoSynchro.logicalGroup.doRefresh....613
server.dispatcher.daemon.logicalGroupMappingUpdate.startTime....614
Device Manager MIME type properties (mime.properties file)....614
Device Manager client properties (client.properties file)....614
client.rmi.port....615
client.launch.em.secure....615
Device Manager security properties (server.properties file and cimxmlscpa.properties file)....616
server.http.security.clientIP....616
server.http.security.clientIPv6....617
server.https.security.keystore....618
server.http.security.unprotected....618
server.https.security.truststore....619
server.https.enabledCipherSuites....619
server.https.protocols....619
Ciphers....620
Device Manager SNMP trap log output properties (customizedsnmptrap.properties file)....620
customizedsnmptrap.customizedSNMPTrapEnable....621
customizedsnmptrap.customizelist....621
Device Manager launchable applications properties (launchapp.properties file)....623
launchapp.snm2.url....623
launchapp.snm2.rmi.port....623
launchapp.elementmanager.role.mode....624
launchapp.elementmanager.usehostname....624
Properties for communicating with the host (host.properties file)....624
host.mf.agent.connection.timeout....625
host.agent.access.timeoutForRpm....625
Properties for connecting to Host Data Collector (hostdatacollectors.properties file)....625
hdc.request.timeout....625
hdc.rmiregistry....626

hdc.rmiserver..... 626
hdc.classloader..... 627
hdc.usessl..... 628
Properties for migrations (migration.properties file)..... 628
migration.dataErase.defaultValue..... 629
migration.plan.candidateVolumeCountLimit..... 629
migration.plan.candidateCapacityGroupDisplayMaxCount..... 629
migration.multiExecution..... 630
migration.volumeDelete.defaultValue..... 630
Properties for connecting to Tuning Manager (tuningmanager.properties file)..... 630
htnm.infoAcquirePeriod..... 630
htnm.servers..... 631
htnm.server.n.host..... 631
htnm.server.n.protocol..... 631
htnm.server.n.port..... 632
htnm.flashMode..... 632
hdvm.analytics.report.pdf.showLogo..... 632
hdvm.analytics.disabled..... 632
hdvm.analytics.healthcheck.notification.exportreport.locale..... 633
Properties related to the Replication tab (replication.properties file)..... 633
server.dispatcher.daemon.replication.config.doUpdate..... 633
server.dispatcher.daemon.replication.config.updateInterval..... 634
server.dispatcher.daemon.replication.config.offset..... 634
server.dispatcher.daemon.replication.config.minute..... 635
server.dispatcher.daemon.replication.performance.rpm.updateInterval..... 636
server.dispatcher.daemon.replication.performance.tnm.updateInterval..... 636
server.dispatcher.daemon.replication.performance.tnm.offset..... 636
server.dispatcher.daemon.replication.performance.tnm.minute..... 637
hdvm.replication.disabled..... 637
Properties for connecting to Replication Manager (rpmlib.properties file)..... 637
rpmlib.rpm.port..... 638
Properties for the CIM/WBEM functions (jserver.properties file, cimxmlcpa.properties file, cimxmlscpa.properties file)..... 638
com.wbemsolutions.jserver.bindto..... 638
HTTPPort..... 639
HTTPSPort..... 639

B Tiered Storage Manager server properties 641

Tiered Storage Manager server property files..... 642
Changing Tiered Storage Manager server properties..... 642
Syntax rules for Tiered Storage Manager server property files..... 643
Tiered Storage Manager server operations properties (server.properties file)..... 643
server.rmi.port..... 644
server.rmi.security.port..... 644
server.base.initialsynchro..... 645
server.mail.smtp.host..... 645
server.mail.from..... 645
server.mail.errorsTo..... 645
server.mail.smtp.port..... 646
server.mail.smtp.auth..... 646
server.eventNotification.mail.to..... 646

server.eventMonitoringIntervalInMinute..... 646
server.migration.multiExecution.....646
server.checkOutVolumeRange..... 646
server.migration.dataErase.defaultValue.....647
server.migrationPlan.candidateVolumeCountLimit..... 647
server.migrationPlan.candidateCapacityGroupDisplayMaxCount.....647
server.migration.maxRetryCount.....648
Tiered Storage Manager database properties (database.properties file)..... 648
dbm.traceSQL.....648
Tiered Storage Manager properties for accessing Device Manager server (devicemanager.properties file).....649
hdvm.protocol..... 649
hdvm.port..... 649
hdvm.timeout.....649
hdvm.rmi.port..... 649
Tiered Storage Manager log output properties (logger.properties file).....650
logger.messagelogLevel.....650
logger.tracelogLevel..... 651
logger.syslogLevel..... 652
logger.serverMessageFileCount..... 652
logger.serverTraceFileCount..... 652
logger.guiMessageFileCount.....653
logger.guiTraceFileCount.....653
logger.serverMessageMaxFileSize..... 653
logger.serverTraceMaxFileSize..... 654
logger.guiMessageMaxFileSize.....654
logger.guiTraceMaxFileSize.....654
Tiered Storage Manager security properties (server.properties file).....654
server.rmi.secure..... 655
server.rmi.security.enabledCipherSuites..... 655
server.rmi.security.protocols.....656

C Host Data Collector properties.....657

Host Data Collector property files..... 658
Changing Host Data Collector properties.....658
Properties related to Host Data Collector operation (hdcbase.properties file).....658
hdc.service.localport..... 659
hdc.adapter.adapterProcessNum..... 659
hdc.adapter.localport.....659
hdc.common.rmi.registryPort..... 659
hdc.common.rmi.serverPort..... 660
hdc.common.http.serverPort.....660
hdc.common.rmi.ssl.registryPort..... 661
hdc.common.rmi.ssl.serverPort..... 661
hdc.common.https.serverPort..... 662
hdc.service.rmi.registryIPAddress.....662
hdc.service.fileCleanup.startTime..... 663
hdc.adapter.esx.timeout..... 663
hdc.ssl.secure.....663
hdc.ssl.esx.certCheck..... 664
Host Data Collector logger properties (logger.properties file).....665

logger.trace.level....665
logger.trace.maxFileSize....665
logger.trace.numOfFiles....665
logger.iotrace.maxFileSize....666
logger.iotrace.numOfFiles....666
Properties related to the Host Data Collector's Java environment (javaconfig.properties file)....666
javapathlocation....667
Host Data Collector security properties (hdcbase.properties file)....667
hdc.ssl.ciphers....667
hdc.ssl.esx.enabledTLSv1....668

D Device Manager agent properties....669

Device Manager agent property files....670
Changing Device Manager agent properties....670
Device Manager agent properties for connecting to the Replication Manager server (agent.properties file) 671
agent.rm.TimeOut....671
agent.rm.everytimeShutdown....671
agent.rm.shutdownWait....672
agent.rm.horcmInstance....672
agent.rm.horcmService....673
agent.rm.horcmRange....673
agent.logger.loglevel....674
agent.logger.MaxBackupIndex....674
agent.logger.MaxFileSize....674
Device Manager agent properties for hldutil command operations (hldutil.properties file) 675
agent.util.hpux.displayDsf....675
Device Manager agent log output properties (logger.properties file) 676
logger.loglevel....677
logger.MaxBackupIndex....677
logger.MaxFileSize....677
Device Manager agent properties for program information (programproductinfo.properties file)....678
veritas.volume.manager.version....678
Device Manager agent operations properties (server.properties file)....678
server.agent.port....679
server.http.localPort....679
server.http.port....679
server.http.host....679
server.http.socket.agentAddress....680
server.http.socket.bindAddress....681
server.agent.maxMemorySize....681
server.agent.shutDownTime....681
server.agent.JRE.location....682
server.http.entity.maxLength....682
server.http.security.clientIP....682
server.server.authorization....683
server.server.serverIPAddress....683
server.server.serverPort....683

server.agent.rm.centralizePairConfiguration....684
server.agent.rm.cuLdevForm....684
server.agent.rm.exclusion.instance....685
server.agent.rm.location....685
server.agent.rm.optimization.userHorcmFile....685
server.agent.rm.horcm.poll....686
server.agent.rm.temporaryInstance....686
server.agent.rm.temporaryPort....686
server.agent.rm.pairDefinitionForm....687
server.agent.rm.userAuthentication....689
server.agent.rm.ignorePairStatus....689
server.agent.rm.horcmSource....690
server.agent.rm.moduleTimeOut....690
server.server.ssl.hdvm....691
server.http.server.timeOut....691
server.util.processTimeOut....691
server.agent.evtwait.timeout....692
server.agent.snapshotEvtwait.timeout....692
Properties for command devices connected to Device Manager agent (rgcmddev.properties file)....692

E Security settings for management clients....695

About Login warning banners....696
Conditions that apply when displaying warning banner messages....696
Creating and registering a message displayed on a warning banner....696
Deleting a message from the warning banner....698
Controlling management client access to the management server....699

F Migrating copy pair definitions....703

About migrating of copy pair definitions....704
Prerequisites for migrating copy pair definitions....707
Migrating copy pair definitions to device group definitions....708
Properties used by the pair definition migration command....710

Glossary....715

Index....725

Preface

This manual explains how to configure Hitachi Device Manager (abbreviated hereafter as *Device Manager*), Hitachi Tiered Storage Manager (abbreviated hereafter as *Tiered Storage Manager*), and Hitachi Command Suite Common Component (abbreviated hereafter as *Common Component*), and also explains how to set up an environment as well as how to troubleshoot management servers.

- Intended audience
- Product version
- Release notes
- Document organization
- Related documents
- Document conventions
- Conventions for storage capacity values
- Accessing product documentation
- Getting help
- Comments

Intended audience

This document is intended for storage administrators who use Device Manager and Tiered Storage Manager to operate and manage storage systems, and assumes that readers have:

- Basic knowledge about management tools appropriate to the individual storage system
- Basic knowledge about Storage Area Networks (SANs)
- Basic knowledge about supported OSs
- Basic knowledge about supported cluster software

Product version

This document revision applies to Hitachi Device Manager and Hitachi Tiered Storage Manager v8.5 or later.

Release notes

Read the release notes before installing and using this product. They may contain requirements or restrictions that are not fully described in this document or updates or corrections to this document. Release notes are available on Hitachi Data Systems Support Connect: https://knowledge.hds.com/Documents.

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/Appendix	Description
System configuration and requirements on page 27	This chapter provides the system configuration and system requirements for Device Manager and Tiered Storage Manager.
Network configuration on page 105	This chapter explains the Hitachi Command Suite product settings required for various network configurations.
User account management on page 157	This chapter explains the settings required for managing Hitachi Command Suite product user accounts.
User management on an external authentication server on page 165	This chapter explains how to set user authentication on the external authentication server.

Chapter/Appendix	Description
Communication security settings on page 217	This chapter explains the communication security settings that can be used to operate Hitachi Command Suite products.
Configuring Device Manager for use with related products on page 331	This chapter explains the settings required to link with related products.
Setting up logs and alerts on page 403	This chapter explains the settings required for using Hitachi Command Suite products to monitor system statuses and errors.
Configuring Device Manager for CIM/WBEM on page 435	This chapter explains how to set up CIM/WBEM.
Starting and stopping services on page 455	This chapter explains how to start and stop Hitachi Command Suite product services on the management server.
Managing the database on page 469	This chapter explains how to back up and restore Hitachi Command Suite product databases.
Using the Device Manager agent on page 511	This chapter contains precautions regarding the management of hosts and the settings and operations for Device Manager agents.
Troubleshooting on page 565	This chapter explains how to resolve problems that might occur during Device Manager and Tiered Storage Manager operations, and also how to interpret the information in log files.
Device Manager server properties on page 587	This chapter describes the Device Manager server property files.
Tiered Storage Manager server properties on page 641	This chapter describes the Tiered Storage Manager server property files.
Host Data Collector properties on page 657	This chapter describes Host Data Collector property file.
Device Manager agent properties on page 669	This chapter describes the Device Manager agent property files.
Security settings for management clients on page 695	This section describes the security settings for management clients.
Migrating copy pair definitions on page 703	This section describes how to migrate the copy pair definitions managed in configuration definition files to device group definitions on storage systems.

Related documents

The following related Hitachi Command Suite documents are available on the documentation CD:

- *Hitachi Command Suite User Guide*, MK-90HC172
- *Hitachi Command Suite Installation and Configuration Guide*, MK-90HC173
- *Hitachi Command Suite CLI Reference Guide*, MK-90HC176
- *Hitachi Command Suite Tiered Storage Manager CLI Reference Guide*, MK-90HC177

- *Hitachi Command Suite Messages*, MK-90HC178
- *Hitachi Command Suite System Requirements*, MK-92HC209
- *Hitachi Command Suite Audit Log Reference Guide*, MK-92HC213
- *Hitachi Command Suite Mainframe Agent Installation and Configuration Guide*, MK-96HC130
- *Hitachi Command Suite Tuning Manager Server Administration Guide*, MK-92HC021
- *Hitachi Command Suite Tuning Manager Installation Guide*, MK-96HC141
- *Hitachi Command Suite Replication Manager Configuration Guide*, MK-98HC151
- *Hitachi Command Suite Replication Manager User Guide*, MK-99HC166

Document conventions

This document uses the following typographic conventions:

Convention	Description
Bold	• Indicates text in a window, including window titles, menus, menu options, buttons, fields, and labels. Example: Click **OK**. • Indicates emphasized words in list items.
Italic	• Indicates a document title or emphasized words in text. • Indicates a variable, which is a placeholder for actual text provided by the user or for output by the system. Example: `pairdisplay -g group` (For exceptions to this convention for variables, see the entry for angle brackets.)
`Monospace`	Indicates text that is displayed on screen or entered by the user. Example: `pairdisplay -g oradb`
< > angle brackets	Indicates variables in the following scenarios: • Variables are not clearly separated from the surrounding text or from other variables. Example: `Status-<report-name><file-version>.csv` • Variables in headings.
[ ] 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 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 (for example, disruptive operations, data loss, or a system crash).
	WARNING	Warns the user of a hazardous situation which, if not avoided, could result in death or serious injury.

Conventions for storage capacity values

Physical storage capacity values (for example, disk drive capacity) are calculated based on the following values:

Physical capacity unit	Value
1 kilobyte (KB)	1,000 (10^3) bytes
1 megabyte (MB)	1,000 KB or $1{,}000^2$ bytes
1 gigabyte (GB)	1,000 MB or $1{,}000^3$ bytes
1 terabyte (TB)	1,000 GB or $1{,}000^4$ bytes
1 petabyte (PB)	1,000 TB or $1{,}000^5$ bytes
1 exabyte (EB)	1,000 PB or $1{,}000^6$ bytes

Logical storage capacity values (for example, logical device capacity) are calculated based on the following values:

Logical capacity unit	Value
1 block	512 bytes
1 cylinder	Mainframe: 870 KB Open-systems: • OPEN-V: 960 KB • Others: 720 KB
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 PB or $1{,}024^6$ bytes

Accessing product documentation

Product user documentation is available on Hitachi Data Systems Support Connect: https://knowledge.hds.com/Documents. Check this site for the most current documentation, including important updates that may have been made after the release of the product.

Getting help

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

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

Comments

Please send us your comments on this document to doc.comments@hds.com. Include the document title and number, including the revision level (for example, -07), and refer to specific sections and paragraphs whenever possible. All comments become the property of Hitachi Data Systems Corporation.

Thank you!

1

System configuration and requirements

This chapter describes the system configuration and system requirements for Device Manager and Tiered Storage Manager.

- ☐ System configuration
- ☐ Network security configuration
- ☐ System requirements for the management server and Host Data Collector computers
- ☐ Hosts that can be managed by Device Manager
- ☐ Host management software supported by Device Manager
- ☐ Prerequisites for normal hosts
- ☐ Prerequisites for virtual machines
- ☐ Prerequisites for virtualization servers
- ☐ Prerequisites for mainframe hosts
- ☐ Prerequisites for file servers
- ☐ System requirements for NAS modules
- ☐ Related products
- ☐ System requirements for managing copy pairs
- ☐ System configuration for managing copy pairs (central management method)

- ☐ System configuration for managing copy pairs (other than the central management method)
- ☐ Storage system requirements for managing copy pairs
- ☐ Prerequisite version of the Device Manager agent for managing copy pairs
- ☐ Notes on managing copy pairs
- ☐ Configuring a high availability system
- ☐ Notes on executing commands

System configuration

The following figure shows a basic system configuration in which Device Manager and Tiered Storage Manager are used.

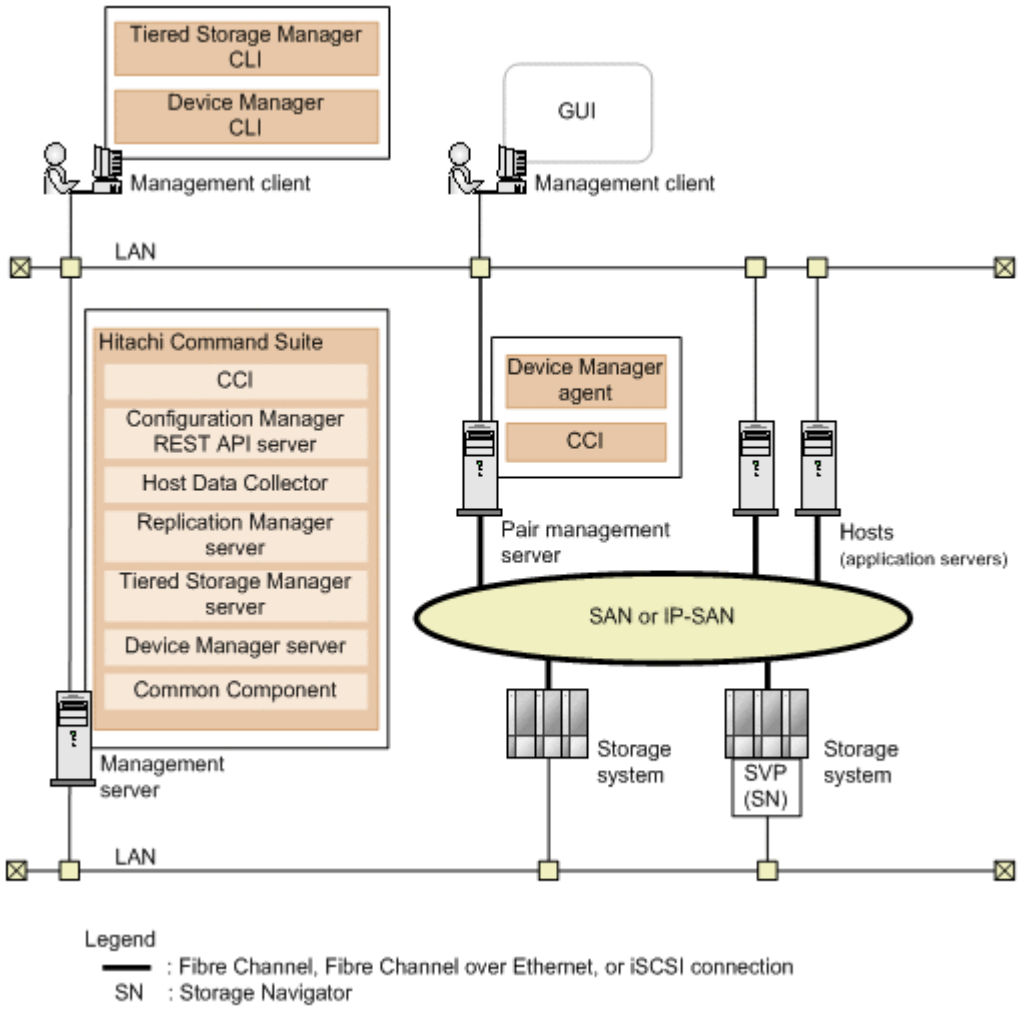


Figure 1 Basic system configuration

Management client

The computer used to operate Device Manager, Tiered Storage Manager, and Replication Manager.

GUI

Software that uses a Web browser to provide a graphical user interface.

Device Manager CLI and Tiered Storage Manager CLI

Command line interfaces that allow users to execute commands from a command line prompt.

Management server

The computer that centrally manages storage systems and hosts. Hitachi Command Suite is installed on this computer. The management server supports an active-standby type clustering configuration consisting of two computers.

Hitachi Command Suite consists of the following components, which are always installed or uninstalled together:

Common Component

Components that provide the user account management, security monitoring, and other functions that are common to all Hitachi Command Suite products.

Device Manager server

The component required by Device Manager for management of storage system volumes.

Tiered Storage Manager server

The component required by Tiered Storage Manager for migration of storage system volumes.

Replication Manager server

The component required by Replication Manager for replication of storage system volumes.

Host Data Collector

The Host Data Collector component collects information about hosts (normal hosts, virtual machines, and virtualization servers), and information about the volumes used on each host.



Tip: Only Host Data Collector can be installed on a separate computer.

Configuration Manager REST API server

The component used for obtaining information about storage systems or changing the configurations by using the REST API.



Tip: Only the Configuration Manager REST API server can be installed on a separate computer.

CCI

The program required for using the REST API. If you install the REST API when CCI is not installed on the management server, CCI is also installed.

Pair management server

The computer for collecting and managing information, such as the configuration and status of copy pairs. The following programs are installed on this computer:

Device Manager agent

The program required for collecting information about hosts and storage systems.

This program is also required for using the CIM/WBEM function of Device Manager to collect performance information for Virtual Storage Platform and Universal Storage Platform V/VM.

CCI

The program required for controlling the copy pairs in the storage systems.

Host (application server)

The computers that use volumes in the storage systems.

Storage system

Storage systems managed by Hitachi Command Suite products. The following types of storage systems can be managed:

- Enterprise-class storage system
  General terms for the following storage systems: Virtual Storage Platform G1000 (VSP G1000), Virtual Storage Platform G1500 (VSP G1500), Virtual Storage Platform F1500 (VSP F1500), Virtual Storage Platform, and Universal Storage Platform V/VM.
- Virtual Storage Platform G200, G400, G600, G800 (VSP Gx00 models)
- Virtual Storage Platform F400, F600, F800 (VSP Fx00 models)
- HUS VM
- Midrange storage system
  A general term for the following storage systems: HUS100, Hitachi AMS2000, Hitachi SMS, and Hitachi AMS/WMS.

SVP

The computer used to manage storage systems. This computer can be used for enterprise-class storage systems, VSP Gx00 models, VSP Fx00 models, or HUS VM. For enterprise-class storage systems or HUS VM, this computer is built into the storage system. For VSP Gx00 models or VSP Fx00 models, a server that provides the functionality to manage storage systems is installed and used as an SVP.

Note: When using a VSP G1000, G1500, VSP F1500, VSP Gx00 model, or VSP Fx00 model, synchronize the clocks on the management server and the SVP.

Storage Navigator (a management tool for storage systems):

A Device Manager component. It provides the functionality to configure storage systems and set up resources in more detailed conditions. The name of the storage system management tool differs depending on the storage system.

For VSP G1000, G1500, VSP F1500, VSP Gx00 models, or VSP Fx00 models: Hitachi Device Manager - Storage Navigator

For Virtual Storage Platform, Universal Storage Platform V/VM, or HUS VM: Storage Navigator

This tool is referred to as "Storage Navigator" unless there is a need to distinguish Device Manager - Storage Navigator and Storage Navigator.

Networks (LAN and SAN)

A TCP/IP network must be used to connect the management server to the management clients, and to connect the management server to the storage systems. A SAN or IP-SAN network must be used to connect the hosts and storage systems.

Note the following when you determine system configurations:

- Use one management server to manage one storage system. Do not configure a system such that multiple management servers manage a single storage system. Note that if you use the VVol management functionality of VMware® vSphere 6.0 or later, one storage system is managed by a normal management server and a management server for VVols.
- On a single Device Manager server, you cannot use multiple storage administrator accounts to manage multiple storage partitions. If you want to manage storage partitions individually, you must provide a Device Manager server for each storage partition.

- If the version of the Device Manager agent is 8.1.1 or earlier, the Global Link Manager agent is installed automatically in the following OSs:
  - Windows®
  - Solaris 10 (SPARC)
  - Solaris 11 (SPARC)
  - HP-UX

  Global Link Manager agent is required for sending LUN path information to the Global Link Manager server and for configuring required host settings when DMP (VxVM's dynamic multipathing function) or HP-UX multipathing is used to manage LUN paths between hosts and storage systems.

Network security configuration

VSP G1000, G1500, VSP F1500, VSP Gx00 models, VSP Fx00 models, Virtual Storage Platform, Universal Storage Platform V/VM and HUS VM communicate with SVP.

The following two types of Ethernet adapters are available for the SVP:

- Private (internal) Ethernet LAN adapter
  Used for communication in a storage system.
- Public LAN adapter
  Used by applications of other computers outside a storage system to communicate with the SVP. Device Manager uses this public LAN for communication with the SVP regarding storage systems and configuration changes.



WARNING: *Do not* under any circumstances attach the private LAN to an external network because this can cause serious problems on the array.

Common security risks

You must be careful when connecting HUS100, Hitachi AMS2000, Hitachi SMS, and Hitachi AMS/WMS to the public network.

System administrators frequently separate production LANs from management LANs. In such cases, management LANs act as a separate network, which isolates management traffic from a production network and reduces the risk of security-related threats. If a management controller such as the SVP exists on a production LAN, the storage systems are left open for access by any entity on the IP network. Whether the access is intentional or not, the resulting security risks can lead to DoS (Denial of Service) attacks and actual loss of storage availability. DoS attacks may lead to a

management session being hijacked for malicious purposes, such as unbinding a storage extent from a port during an I/O operation.

The following are guidelines for constructing management LANs:

- Traffic from the production LAN should not flow through, or be routed to the management LAN.
- If possible, all hosts with management interfaces or controllers on the management LAN should be hardened to their maximum level to reduce the potential that software other than the management interface will not lead to an exploit of the entire station or device. (In this case, hardening should include removal of unnecessary software, shutting down nonessential services, and updating to the latest patches.)
- The management LAN should only intersect a production LAN on those computers acting as an interface between the management LAN and the production LAN (for example, the Device Manager server).
- If possible, those computers intersecting both private LAN and management LAN should be behind a firewall of some kind, further inhibiting unintended access.

Security configuration recommended for Device Manager

The computer hosting Device Manager server must either be dual-homed or have two NICs, and every other management application must be of a similar configuration. The first NIC for each computer is attached to a LAN dedicated to manage traffic between the management computer and managed storage systems. A second NIC is attached to a LAN where access is governed by a firewall. As shown in Figure 2 Separate management LAN with a firewall configuration on page 35, each application server could also be connected to a different LAN that has a different firewall. The firewall contains strict access rules that allow the management servers to be accessed only by Device Manager clients or by specified management application clients.

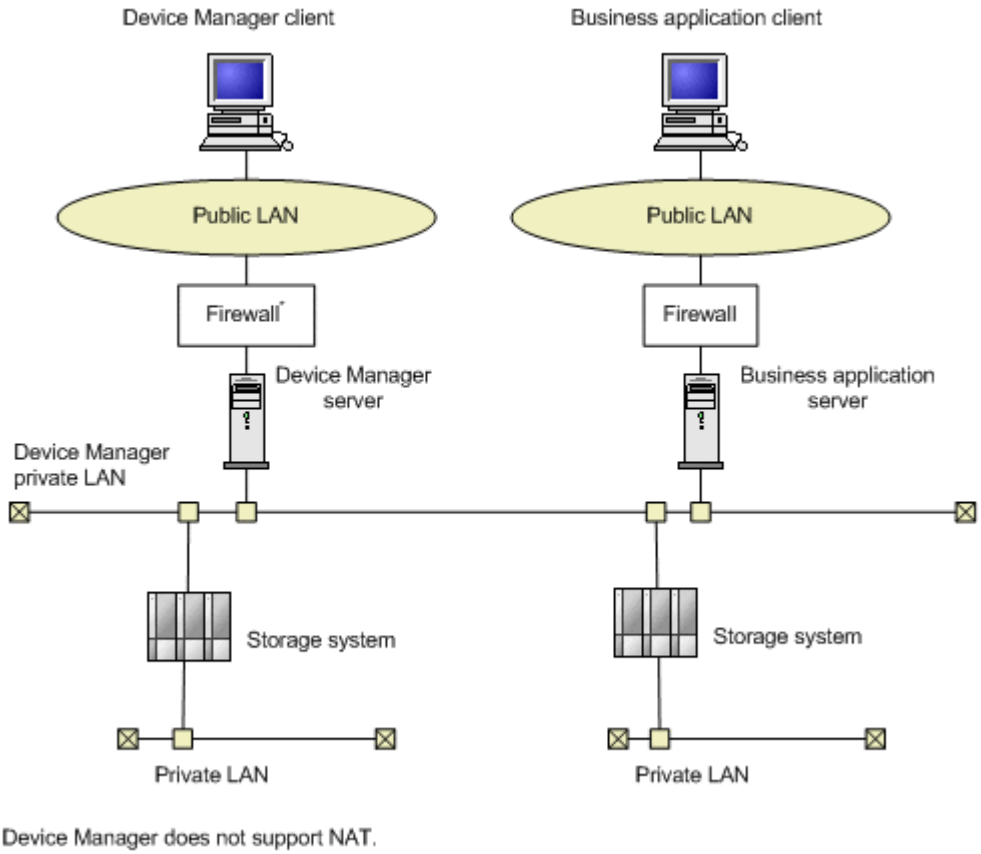


Figure 2 Separate management LAN with a firewall configuration

System requirements for the management server and Host Data Collector computers

This section describes the system requirements for the management server and the system requirements for a different computer on which Host Data Collector is installed.

Maximum number of resources that can be managed

There are upper limits to the number of resources that can be managed by Device Manager, Tiered Storage Manager, and Replication Manager.

We recommend that you operate each product within these limits.

Table 1 Maximum number of management resources

Resource	Maximum for the Device Manager server
Number of LDEVs#1	1,000,000
Total of number of LDEVs and paths#2	5,000,000
Note:	

Resource	Maximum for the Device Manager server
The maximum number of management resources when using the CIM/WBEM function is shown below. If the number of storage system resources managed by Device Manager exceeds the maximum, change the `server.cim.support` property to `false` (default: `true`). • Number of LUNs 128,000 • Number of security settings (total number of WWNs and iSCSI names assigned for configuring security settings for LUNs in storage systems managed by Device Manager, Tiered Storage Manager, or Replication Manager) 192,000 • Number of LDEVs 128,000 (The maximum number of LDEVs for open systems only is 64,000)	

#1:

The total of the number of LDEVs for mainframes and the number of LDEVs for open systems.

#2:

Number of paths = *number of LDEVs* x *average number of paths per LDEV*

Related tasks

- Changing Device Manager server properties on page 590

Related references

- server.cim.support.job on page 596

Changing the memory heap size

You can change the memory heap size on the Device Manager server by editing a file. In Windows, edit the `Server.ini` file. In Linux®, edit the `hicommand.sh` file.

Before you begin

Check the following information:

- Number of LDEVs to be managed

Table 2 Appropriate memory heap size for the Device Manager server

Managed resource	Memory heap size		
	512MB	1,024 MB	2,048 MB
Number of LDEVs per storage system	2,000 or less	6,000 or less	6,001 or more

- Configuration of the file servers or NAS modules to be managed (when managing file servers or NAS modules)

Set a memory heap size according to the number of file servers or NAS modules as shown below:

- When managing one file server or NAS module
  Set the memory heap size to 1024MB.
- When managing two or more file servers or NAS modules
  Set the memory heap size to 2048MB.

If the memory heap size calculated from the number of LDEVs and the number of copy pairs differs from the value indicated above, set the larger value as the memory heap size.

Procedure

1. Use a text editor to open the following file.

   In Windows:

   installation-folder-for-Hitachi-Command-Suite\DeviceManager\HiCommandServer\Server.ini

   In Linux:

   installation-directory-for-Hitachi-Command-Suite/hicommand.sh

2. Specify an appropriate memory heap size.

   Specify an appropriate memory heap size for `JVM_XOPT_HEAP_MAX` using the following format:

   `JVM_XOPT_HEAP_MAX=-Xmx`*new-setting-value*`m`

3. Restart the Hitachi Command Suite product services.

Related tasks

- Starting the Hitachi Command Suite services on page 458
- Stopping the Hitachi Command Suite services on page 460

Changing the JDK of management servers

After starting operations, to change the JDK used by Hitachi Command Suite products, execute the `hcmds64chgjdk` command.

Before you begin

- Check the JDK for Hitachi Command Suite products
  For details, see *Hitachi Command Suite System Requirements*.

Note:

- If you perform an overwrite or upgrade installation of an Oracle JDK during operation of any Hitachi Command Suite product, re-register the JDK after the installation.
- If you remove an Oracle JDK during operation of any Hitachi Command Suite product, make sure that you change to the JDK bundled with Hitachi Command Suite.

Procedure

1. Stop the services of Hitachi Command Suite products.
2. Execute the command below, and in the window that opens, select the JDK you want to use.

   In Windows:

   installation-folder-for-Hitachi-Command-Suite\Base64\bin\hcmds64chgjdk

   In Linux:

   installation-directory-for-Hitachi-Command-Suite/Base64/bin/hcmds64chgjdk

3. In the cases below, use the `hcmds64keytool` utility (for Windows) or the `keytool` utility (for Linux) to re-import the certificate into the truststore (`jssecacerts`).

   When the certificate is re-imported, its storage location switches to a location under the JDK being used.
   - If SSL/TLS communication is used between the Device Manager server and the Replication Manager server
   - If SSL/TLS communication is used between the Tuning Manager server and the Device Manager server
   - If the port for non-SSL communication of HBase 64 Storage Mgmt Web Service (default: 22015) is closed
   - Between Tuning Manager Agents and the Tuning Manager servers (If the Tuning Manager API is used)

4. Start the services of Hitachi Command Suite products.
5. If you change to Oracle JDK in an environment that has Windows Firewall enabled, you must manually register the `java.exe` file of Oracle JDK as a firewall exception.

Related tasks

- Importing a certificate into the truststore for Common Component on page 298
- Starting the Hitachi Command Suite services on page 458

- Stopping the Hitachi Command Suite services on page 460

Changing the Java execution environment used by Host Data Collector

To change the Java execution environment for Host Data Collector computers that are not management servers, set the installation path of the Java execution environment to the `javapathlocation` property in the `javaconfig.properties` file for Host Data Collector.

Before you begin

- Check the prerequisite Java execution environment for Host Data Collector. For details, see *Hitachi Command Suite System Requirements*.
- Log in as a user with Administrator permissions (for Windows) or as a root user (for Linux).
- Install the Jurisdiction Policy files (when using Host Data Collector as an SSL server).
  You need to download and install the Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files for the version of the Java execution environment to be used.
  Download the Jurisdiction Policy files from the Oracle corporation website. For details about how to install the files, see the documentation provided with the Jurisdiction Policy files.
- Check the following information:
  - Check the installation path of the Java execution environment to be used.

Procedure

1. Stop the Host Data Collector service.
2. Use the absolute path to set the installation path of the Java execution environment to the `javapathlocation` property in the `javaconfig.properties` file for Host Data Collector.
3. Start the Host Data Collector service.

Result

The Java execution environment used by Host Data Collector will switch to the Java execution environment in the `bin` directory on the specified path.

Related tasks

- Starting the Host Data Collector service on page 464
- Stopping the Host Data Collector service on page 464

Related references

- javapathlocation on page 667

Hosts that can be managed by Device Manager

Device Manager can manage, as hosts, computers that use volumes on managed storage systems. By using Device Manager to centrally manage the disk resources for individual hosts, you can assign the most appropriate volume based on usage. To allocate storage system volumes to hosts (application servers) or check the volume usage of each host, target hosts must be registered in Device Manager as Device Manager resources.

Device Manager can manage the volume usage of the hosts in the following table.

Table 3 Hosts that can be managed by Device Manager

Hosts		Description
Open hosts	Normal host	An environment in which virtualization software is not installed
	Virtual machine#	A virtual environment created by using virtualization software
	Virtualization server	A physical environment in which virtualization software is installed#
Mainframe hosts		Computers that use mainframe volumes
File servers	Hitachi Data Ingestor	A computer that is used to share the files in a storage system with multiple clients in the network by using the NAS functionality.
	NAS Platform	
	Hitachi NAS Platform F	

#:

After virtual machines and physical environments in which Windows Server® 2008 Hyper-V® or Windows Server 2012 Hyper-V is installed have been registered in Device Manager, Device Manager treats them as normal hosts.

Note: The names of the hosts managed by Device Manager must be 50 bytes or less.

Host management software supported by Device Manager

Device Manager centrally manages hosts by collecting information from them via the host management software.

Table 4 Host management software supported by Device Manager

Host management software	Open host			Mainframe host	File server
	Normal host	Virtual machine	Virtualization server		
Host Data Collector#	Y	Y	Y	N	N
Device Manager agent#	Y	Y	N	N	N
Mainframe Agent	N	N	N	Y	N
File server management software	N	N	N	N	Y

Legend:

Y: Supported

N: Not supported

#:

If both Host Data Collector and the Device Manager agent manage information about normal hosts or virtual machines, the Device Manager GUI or CLI uses the information acquired by the Device Manager agent.

- With Host Data Collector:
  Host Data Collector can manage normal hosts, virtual machines, and virtualization servers.
  Network hosts that are found from the Device Manager GUI are registered in Device Manager.
  When managing open hosts, we recommend using Host Data Collector as host management software for Device Manager.

  Tip: Host Data Collector transfers the module for collecting host information and the script for executing the module to the following locations of the hosts to be managed.

  For Windows hosts:`admin$` (communication by using a file sharing protocol, the SMB protocol)

  For UNIX hosts:`/tmp` (communication by using the SSH protocol)

  Host Data Collector collects information about the hosts to be managed by executing the transferred script for executing the module.

  The environment settings that allow remote operation by Host Data Collector need to be specified on the hosts to be managed.

- With Device Manager agent:

The Device Manager agent can manage normal hosts and virtual machines.
When the Device Manager agent is installed on a host, the host is registered in Device Manager.

- With Mainframe Agent:
  The Mainframe Agent can manage mainframe hosts.
  Using the Device Manager CLI, register both the mainframe hosts that you want to manage and Mainframe Agent which you will use to manage those hosts, in Device Manager.
- With file server management software:
  File server management software can manage file servers.
  Use file server management software to register target file servers in Device Manager.

Note: If Compute Systems Manager has been installed, normal hosts and virtual machines registered in Compute Systems Manager are registered in Device Manager automatically.

Note that if you access Linux hosts by using the `su` command from Compute Systems Manager, because Device Manager does not support the `su` command, you need to configure settings for the `sudo` command in advance from Device Manager to ensure that host information is properly synchronized. For details about how to specify the `sudo` command, see the description of the prerequisite environment for the normal host.

Tip: For details about the hosts to be managed by the host management software, see the *Hitachi Command Suite System Requirements*.

Related references

- Prerequisites for normal hosts on page 43

Prerequisites for normal hosts

To manage normal hosts by using Host Data Collector, you must perform environment setup of the normal hosts before registering them in Device Manager.

Note:

- If the host OS is Linux and you want to use the Device-Mapper Multipath feature (DM-Multipath), to set the alias for a multipath device for the `alias` attribute in the `multipaths` section of the `/etc/multipath.conf` file, use the following characters:
  `A` to `Z`
  `a` to `z`

0 to 9
- _ . @

- If you use Host Data Collector to register Linux hosts that recognize 256 or more logical unit numbers in a storage system, the KAIC03006-E error message is output and the operation fails. For Linux hosts managed by Host Data Collector, specify a value of 256 or less as the number of LUs per port of storage systems recognized by a host. Specify a logical unit number in the range from 0 to 255.
- For Solaris hosts with the Solaris multi-pathing feature (MPxIO) enabled that are managed by Host Data Collector, specify a logical unit number for storage systems recognized by a host in the range from 0 to 255. If the logical unit number is 256 or more, the following problems occur:
  - The information of the LDEVs whose logical unit number is 256 or more is not collected.
  - When the logical unit number of the command device is 256 or more, if you perform an operation related to the copy-pair configuration definition by using Replication Manager, the operation fails and the error message KAVN00451-E is output.

Prerequisites for normal hosts

To use Host Data Collector to manage normal hosts, install Host Data Collector, and then perform environment setup on each normal host.

Host Data Collector comes with Hitachi Command Suite, which is installed on the management server, but can also be installed on a computer other than the management server.

Before you register normal hosts in Device Manager, the following environment settings must already be specified on the normal hosts. When managing a UNIX host, the environment settings that need be specified on the UNIX host differ according to the UNIX account used to register the host in Device Manager.

When managing a Windows host

- A user with Administrator permissions is assigned as a user who can execute the Host Data Collector service.
- admin$ is shared over the network.
  You can check this by using the Windows net share command. If a security-monitoring program is installed on a normal host, Host Data Collector might not be able to collect the host information.
- In the Windows Firewall settings, File and Printer Sharing is registered as an exception.
- Startup Type of Windows Application Experience service is set to Manual or Automatic.
- If the host is managed as an Active Directory member, the following domain group policy is set to Unconfigured or Disabled.

Windows Components > Application Compatibility > Turn off Program Compatibility Assistant

When managing a UNIX host (When information about the host is collected by using the root account)

- SSH is enabled.
- Settings have been configured so that you can log in as root via a remote SSH login with password authentication.
- When the OS of a normal host to be managed is AIX, the `ODMDIR` environment variable is set.

Note: If the root account is used to register a host into Device Manager, do not use a general user account to register the host a second time.

When managing a UNIX host (When information about the host is collected by using a general user account)

- SSH is enabled.
- Settings have been configured so that you can log in by using a general user account via a remote SSH login with password authentication.
- The user account used when the host is registered has been created specifically for Host Data Collector (recommended).
- When the OS of a normal host to be managed is AIX, the `ODMDIR` environment variable is set.
- Update permissions (`rwx`) are set for the `/tmp` directory.
- Settings have been specified in the `PATH` environment variable so that the `sudo` command can be executed.
- Settings have been specified in the `/etc/sudoers` file so that the `sudo` command can be executed.
  To ensure that the `sudo` command can be executed, add the following entry:

  user-name-used-for-host-registration hosts-to-be-registered=(*execution-user-name-alias*)NOPASSWD:/tmp/FsDataGatherLauncher.Unix.sh

  For *hosts-to-be-registered*, specify the IP address, host name, or `ALL`.
  For *execution-user-name-alias*, specify `ALL`, or `root`.

Note: If a general user account is used to register a host into Device Manager, do not use the root account to register the host a second time.

Note: Do not use a name that contains a semicolon (*;*) for the following host items:

- If managing a Windows host:
  - Network connection name

- Comment field for the shared disk
- If managing a UNIX host:
  - Mount-destination directory name
  - Disk group name (volume group name and disk set name)
  - Logical volume name
  - Network name
  - Shared disk directory name
  - Device name of the network drive (directory name of the shared disk that has been set up on the reference destination host)

Tip: For details on how to set up Host Data Collector, see the *Hitachi Command Suite Installation and Configuration Guide*.

Prerequisites for virtual machines

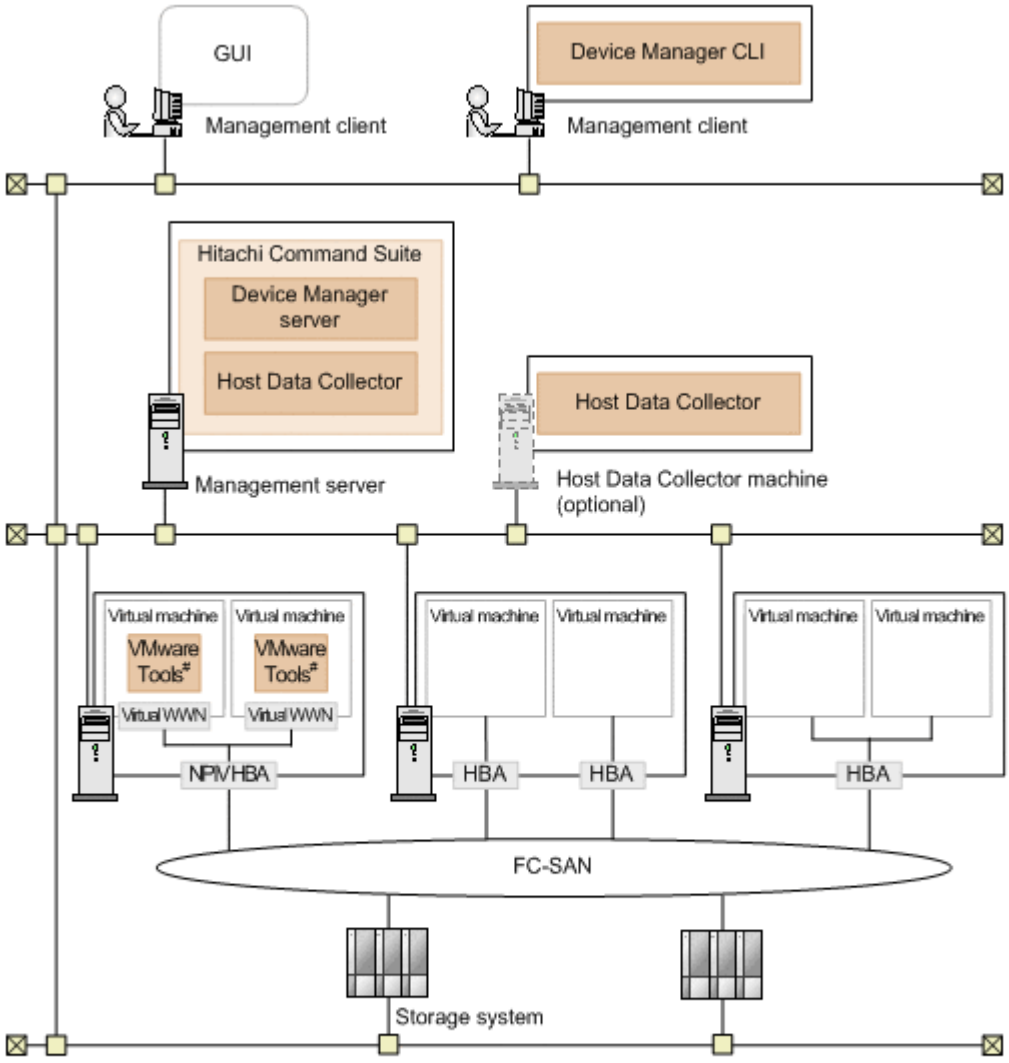
The following system configuration of virtual machines is supported by Device Manager:

- Configuration in which a virtual HBA is allocated for each virtual machine (by using NPIV HBAs) (recommended)
- Configuration in which an HBA is allocated for each virtual machine
- Configuration in which an HBA is shared by multiple virtual machines

To manage virtual machines by using Host Data Collector, you must perform environment setup of the virtual machines before registering them in Device Manager.

Prerequisites for virtual machines

To use Host Data Collector to manage virtual machines, install Host Data Collector, and then perform environment setup on each virtual machine.



(Legend)
FC: Fibre Channel

#: Required when VMware ESXi is used as the virtualization software.

Figure 3 Environment settings on virtual machines

Host Data Collector comes with Hitachi Command Suite , which is installed on the management server, but can also be installed on a computer other than the management server.

Before you register virtual machines in Device Manager, the following environment settings must already be specified on the virtual machines. When managing a UNIX host, the environment settings that need be specified on the UNIX host differ according to the UNIX account used to register the host in Device Manager.

Tip: For details on how to set up Host Data Collector, see the *Hitachi Command Suite Installation and Configuration Guide*. For details on how to

register a virtualization server, see the *Hitachi Command Suite User Guide* or *Hitachi Command Suite CLI Reference Guide*.

When managing a Windows host

- A user with Administrator permissions is assigned as a user who can execute the Host Data Collector service.
- `admin$` is shared over the network.
  You can check this by using the Windows `net share` command. If a security-monitoring program is installed on a virtual machine, Host Data Collector might not be able to collect the host information.
- In the Windows Firewall settings, File and Printer Sharing is registered as an exception.
- Startup Type of Windows Application Experience service is set to Manual or Automatic.
- If the host is managed as an Active Directory member, the following domain group policy is set to Unconfigured or Disabled.
  Windows Components > Application Compatibility > Turn off Program Compatibility Assistant
- In a configuration in which VMware ESXi is used as the virtualization software and a virtual HBA is allocated for each virtual machine (by using NPIV HBAs), the following operations have already been performed:
  - Registering virtualization servers that operate in the same physical environment in Device Manager
  - Installing VMware Tools on each of the virtual machines to be managed

When managing a UNIX host (When information about the host is collected by using the root account)

- SSH is enabled.
- Settings have been configured so that you can log in as root via a remote SSH login with password authentication.
- In a configuration in which VMware ESXi is used as the virtualization software and a virtual HBA is allocated for each virtual machine (by using NPIV HBAs), the following operations have already been performed:
  - Registering virtualization servers that operate in the same physical environment in Device Manager
  - Installing VMware Tools on each of the virtual machines to be managed



Note: If the root account is used to register a host into Device Manager, do not use a general user account to register the host a second time.

When managing a UNIX host (When information about the host is collected by using a general user account)

- SSH is enabled.
- Settings have been configured so that you can log in by using a general user account via a remote SSH login with password authentication.

- The user account used when the host is registered has been created specifically for Host Data Collector (recommended).
- Update permissions (`rwx`) are set for the `/tmp` directory.
- Settings have been specified in the `PATH` environment variable so that the `sudo` command can be executed.
- Settings have been specified in the `/etc/sudoers` file so that the `sudo` command can be executed.
  To ensure that the `sudo` command can be executed, add the following entry:

  user-name-used-for-host-registrationhosts-to-be-registered =(*execution-user-name-alias*)NOPASSWD:/tmp/FsDataGatherLauncher.Unix.sh

  For *hosts-to-be-registered*, specify the IP address, host name, or `ALL`.
  For *execution-user-name-alias*, specify `ALL`, or `root`.

- In a configuration in which VMware ESXi is used as the virtualization software and a virtual HBA is allocated for each virtual machine (by using NPIV HBAs), the following operations have already been performed:
  - Registering virtualization servers that operate in the same physical environment in Device Manager
  - Installing VMware Tools on each of the virtual machines to be managed

Note: If a general user account is used to register a host into Device Manager, do not use the root account to register the host a second time.

Operation workflow for allocating volumes to virtual machines

How to register hosts and allocate volumes differs depending on the HBA configuration.

Configuration in which a virtual HBA is allocated for each virtual machine (by using NPIV HBAs)

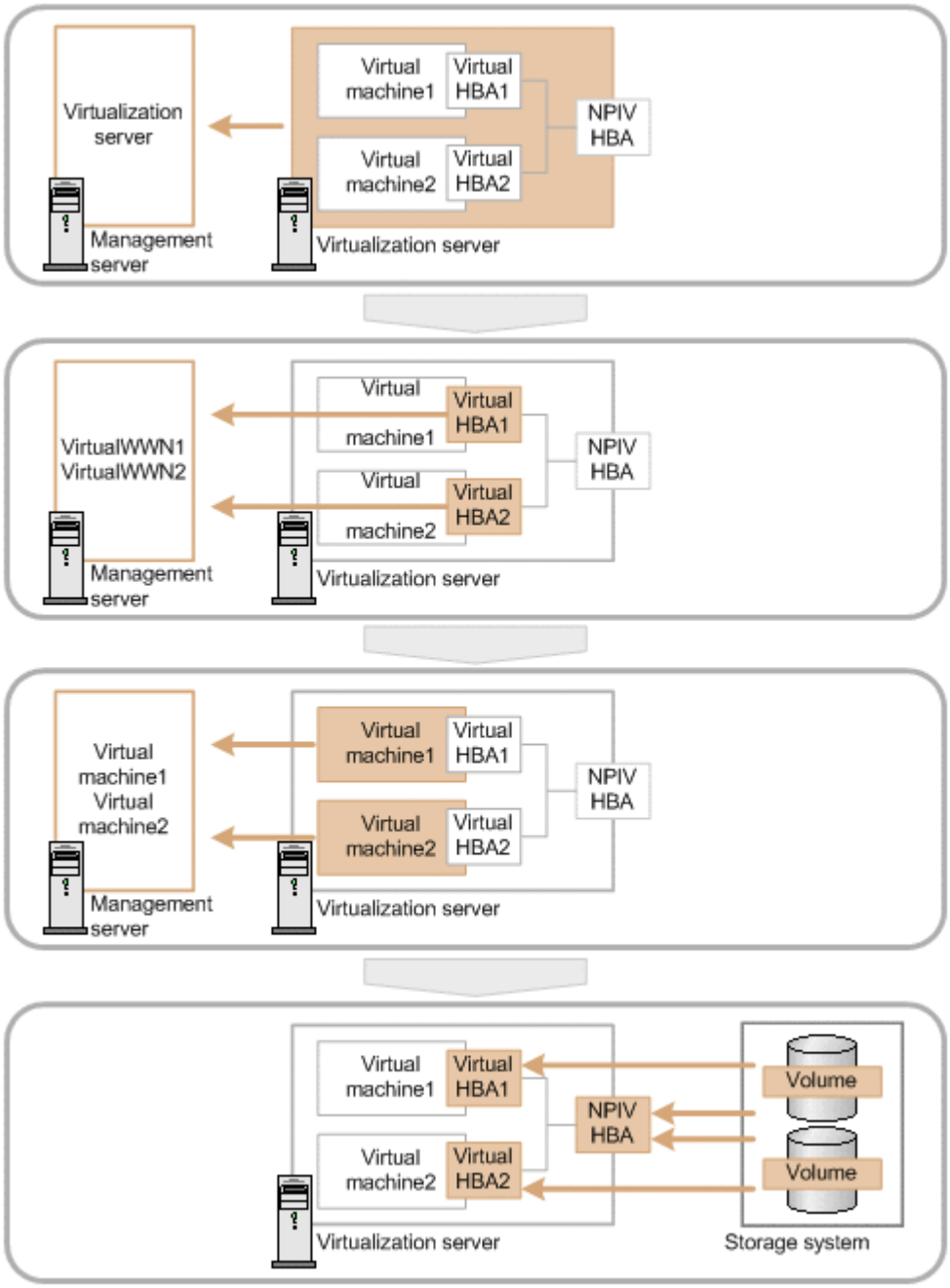


Figure 4 Operation workflow for allocating volumes to virtual machines (when allocating a virtual HBA to each virtual machine)

1. Register the virtualization servers that run the virtual machines whose volume status you want to manage in Device Manager.

   For details on how to register a virtualization server, see the *Hitachi Command Suite User Guide* or *Hitachi Command Suite CLI Reference Guide*.

2. Register the virtual machines whose volume usage you want to manage in Device Manager as normal hosts.

3. Allocate the LUN paths of volumes to both the virtualization servers (physical WWNs) and virtual machines (virtual WWNs), and then make the virtual machines recognize the volumes as RAW device.
   Note that Device Manager cannot recognize volumes that make up a datastore.
   The port for the LUN paths of volumes must be the same among the virtualization servers (physical WWNs) and virtual machines (virtual WWNs).
4. Restart the virtualization server.

Configuration in which an HBA is allocated for each virtual machine

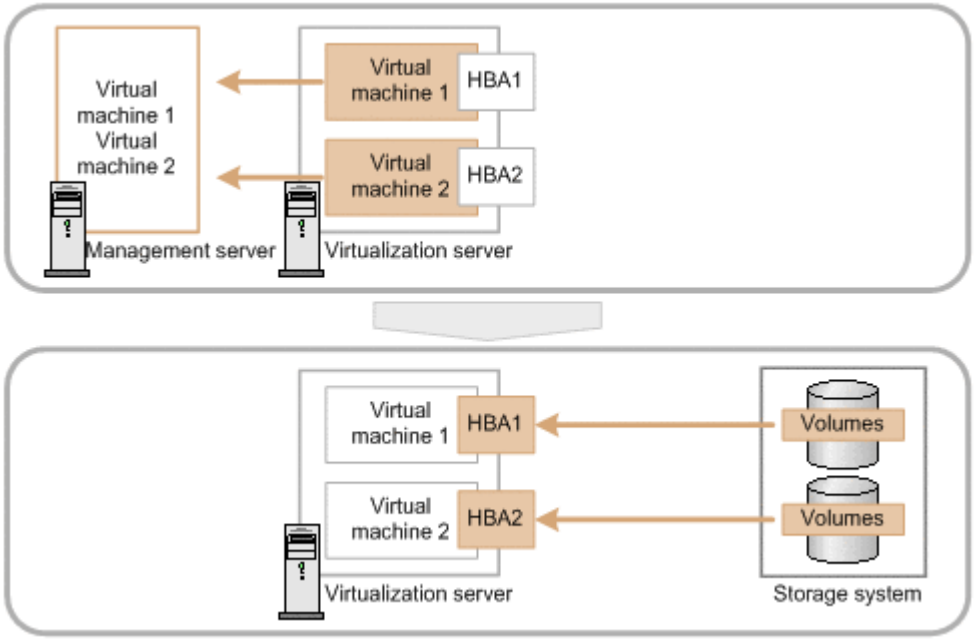


Figure 5 Operation workflow for allocating volumes to virtual machines (when allocating an HBA to each virtual machine)

1. Register each virtual machine whose volume usage you want to manage in Device Manager as a normal host.
   Do not register the virtualization server that runs in the same physical environment in Device Manager.
   For details on how to register a virtualization server, see the *Hitachi Command Suite User Guide* or *Hitachi Command Suite CLI Reference Guide*.

2. Allocate the LUN paths of volumes to each virtual machine (WWN), and then make the virtual machines recognize the volumes as RAW devices.
   Note that Device Manager cannot recognize volumes that make up a datastore.

Configuration in which an HBA is shared by multiple virtual machines

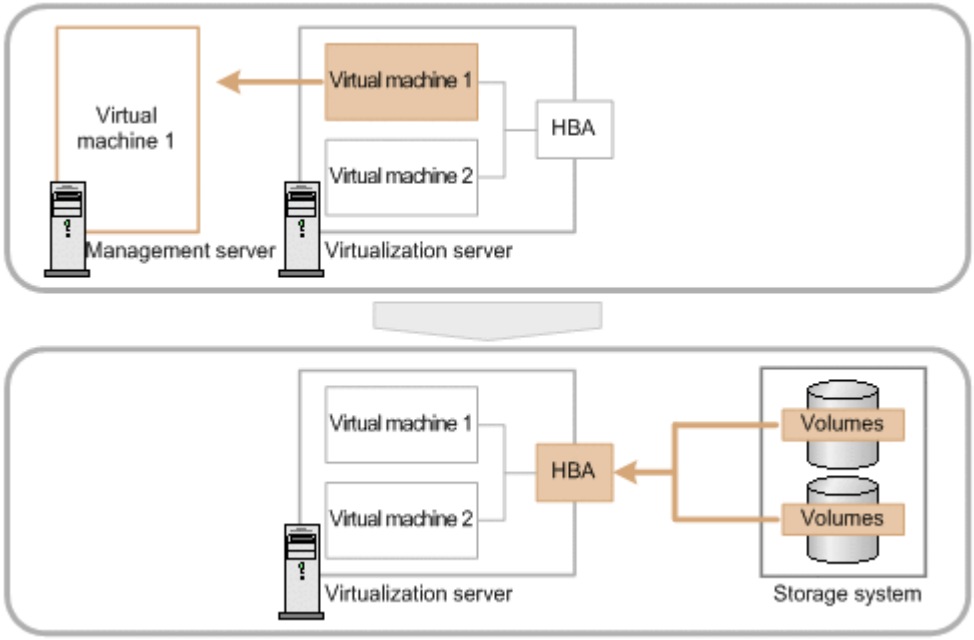


Figure 6 Operation workflow for allocating volumes to virtual machines (when sharing an HBA by multiple virtual machines)

1. Register one of the virtual machines that share an HBA as a normal host in Device Manager.

   Do not register the virtualization server that runs in the same physical environment in Device Manager.

   For details on how to register a virtualization server, see the *Hitachi Command Suite User Guide* or *Hitachi Command Suite CLI Reference Guide*.

2. Allocate the LUN paths of volumes to the virtual machine (WWN) registered in Device Manager, and then make the virtual machines recognize the volumes as RAW devices.

   Note that Device Manager cannot recognize volumes that make up a datastore.

Note: If you want to assign a volume to another virtual machine that shares the HBA, you need to assign a LUN path to the virtual machine that is managed by Device Manager. Therefore, after assigning a LUN path, we recommend that you label each volume so that in Device Manager you can identify which virtual machine the volume is actually assigned to.

Related references

- Tasks required to change the virtual machine configuration on page 52

Tasks required to change the virtual machine configuration

In a configuration in which a virtual HBA is allocated (an NPIV HBA is used) for each virtual machine, any changes to the configuration of virtual machines must also be applied to Device Manager.

If you move a virtual machine from one virtualization server to another :

You need to update (refresh) the information of the source and destination virtualization servers in Device Manager. After moving a virtual machine, if there are no volumes assigned to the source virtualization server, manually delete the information about the source virtualization server from Device Manager.

For details on how to refresh the virtualization server or virtual machine information, see the *Hitachi Command Suite User Guide* or *Hitachi Command Suite CLI Reference Guide*.

If a virtual WWN was added or changed:

Use the Device Manager GUI or CLI to refresh the information about virtual machines and virtualization servers registered in Device Manager.

For details on how to refresh the virtualization server or virtual machine information, see the *Hitachi Command Suite User Guide* or *Hitachi Command Suite CLI Reference Guide*.

If a command device was configured or released:

Restart the virtualization server.

If you change the host name of a virtual machine or remove a virtual machine:

Make sure that you update the `npivmapping.properties` file manually.

In Windows:

installation-folder-for-Hitachi-Command-Suite
`\DeviceManager\HiCommandServer\config`
`\npivmapping.properties`

In Linux:

installation-directory-for-Hitachi-Command-Suite/
`HiCommandServer/config/npivmapping.properties`

Prerequisites for virtualization servers

Device Manager uses Host Data Collector to collect machine information about virtualization servers and information about volumes allocated to the virtualization servers.

Prerequisites for virtualization servers

To manage virtualization servers from Host Data Collector, you must install Host Data Collector.

VMware ESXi 5.*x* or VMware ESXi 6.*x* is the virtualization server that can be managed by Host Data Collector.

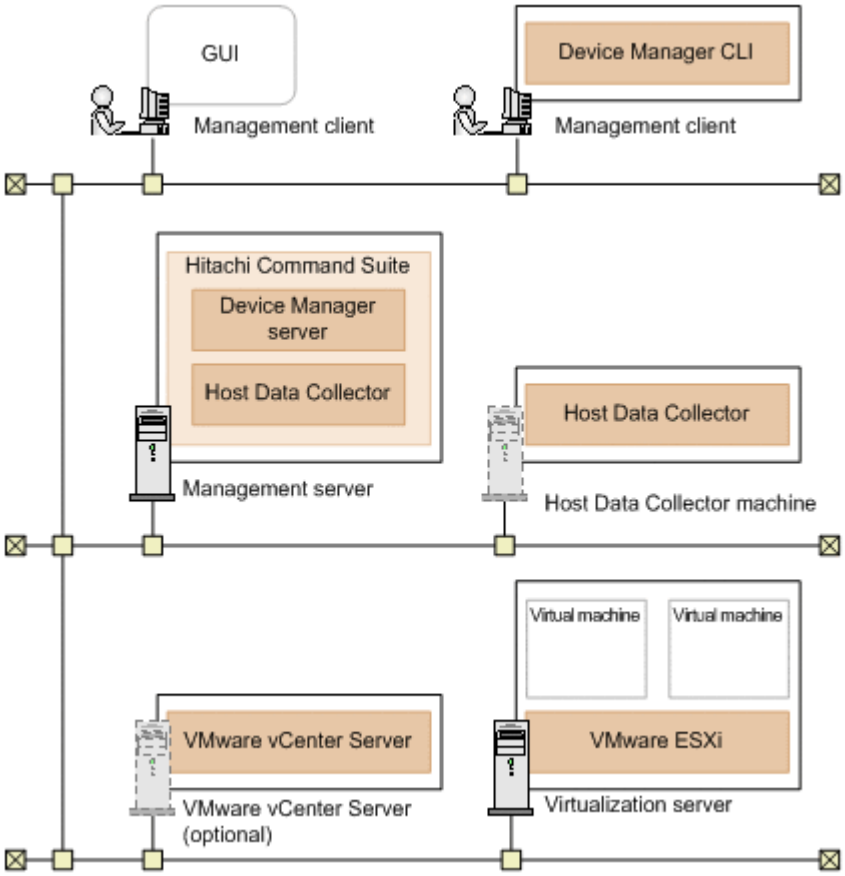


Figure 7 Environment settings on virtualization servers (when Host Data Collector is used for management)

- Host Data Collector comes with Hitachi Command Suite, which is installed on the management server, but can also be installed on a computer other than the management server.
  To install multiple Host Data Collector computers, make sure that the same Host Data Collector version and revision are installed on all computers.
- VMware Tools must be installed on the virtual machines operating on virtualization servers, if a virtual HBA is allocated to the virtual machines.
- IPv6 can also be used for communication between a Host Data Collector computer and a virtualization server, and between a Host Data Collector computer and VMware vCenter Server.

For details on how to set up Host Data Collector, see the *Hitachi Command Suite Installation and Configuration Guide*.

Operation workflow for managing virtualization servers

To manage the virtualization servers using Device Manager, you must specify the necessary environment settings.

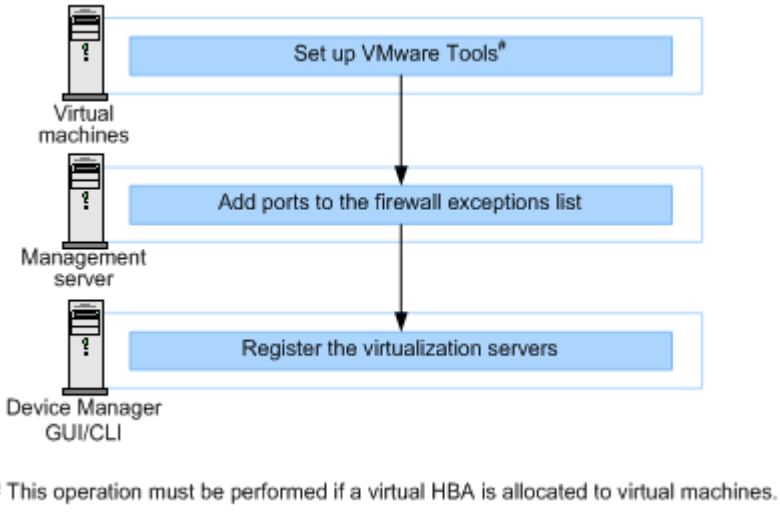


Figure 8 Operation workflow for managing virtualization server

Notes on operating virtualization servers

Note the following when operating virtualization servers:

- To check the latest volume information of virtualization servers, manually refresh information by using Device Manager.
  Note that, if you change the hardware configuration of a virtualization server, after the configuration information of the monitored virtualization server is applied to VMware vCenter Server, you need to update (refresh) the Device Manager information. If the configuration information of virtualization servers is set to be automatically applied to VMware vCenter Server, a time lag might occur from the time the configuration is changed until the information is applied to VMware vCenter Server.
  For details on how to apply the configuration information of virtualization servers to VMware vCenter Server and how to adjust the interval for applying information, see the VMware documentation.
- When Logical Domains is used, if you export the physical disk in the service domain as a virtual disk in the guest domain, specify a full disk. If you specify a disk slice, the information about the virtual disk cannot be acquired correctly.

Prerequisites for mainframe hosts

From Device Manager or Tiered Storage Manager linked with Mainframe Agent, you can perform the following operations for mainframe volumes:

- Checking the usage of mainframe volumes and the logical DKC serial numbers of storage systems (from Device Manager)

- Migrating and shredding mainframe volumes (from Tiered Storage Manager)

Operation workflow of managing a mainframe host

To manage mainframe host volumes by linking Mainframe Agent, you must specify environment settings for both Mainframe Agent and Device Manager.

For details on how to specify environment settings from the Device Manager CLI, see the *Hitachi Command Suite CLI Reference Guide* or *Mainframe Agent Installation and Configuration Guide*.

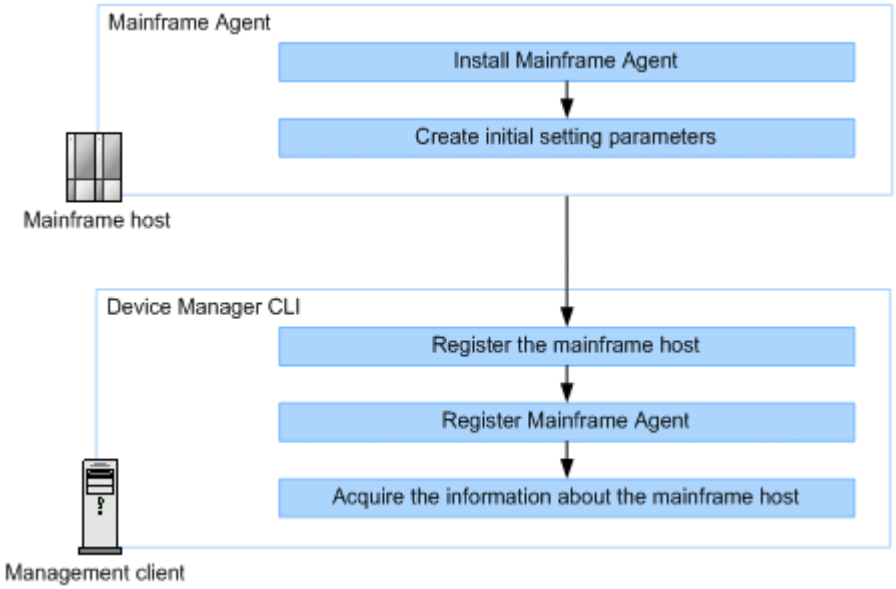


Figure 9 Operation workflow of managing a mainframe host

Prerequisites for file servers

You can use Device Manager to allocate storage system volumes to file servers or to check information about file servers.

Environment settings for NAS Platform family

To manage NAS Platform by using Device Manager, the management server must be in a system configuration in which communication with the following programs are enabled:

- System Management Unit (SMU) or NAS Manager
- Admin services EVS

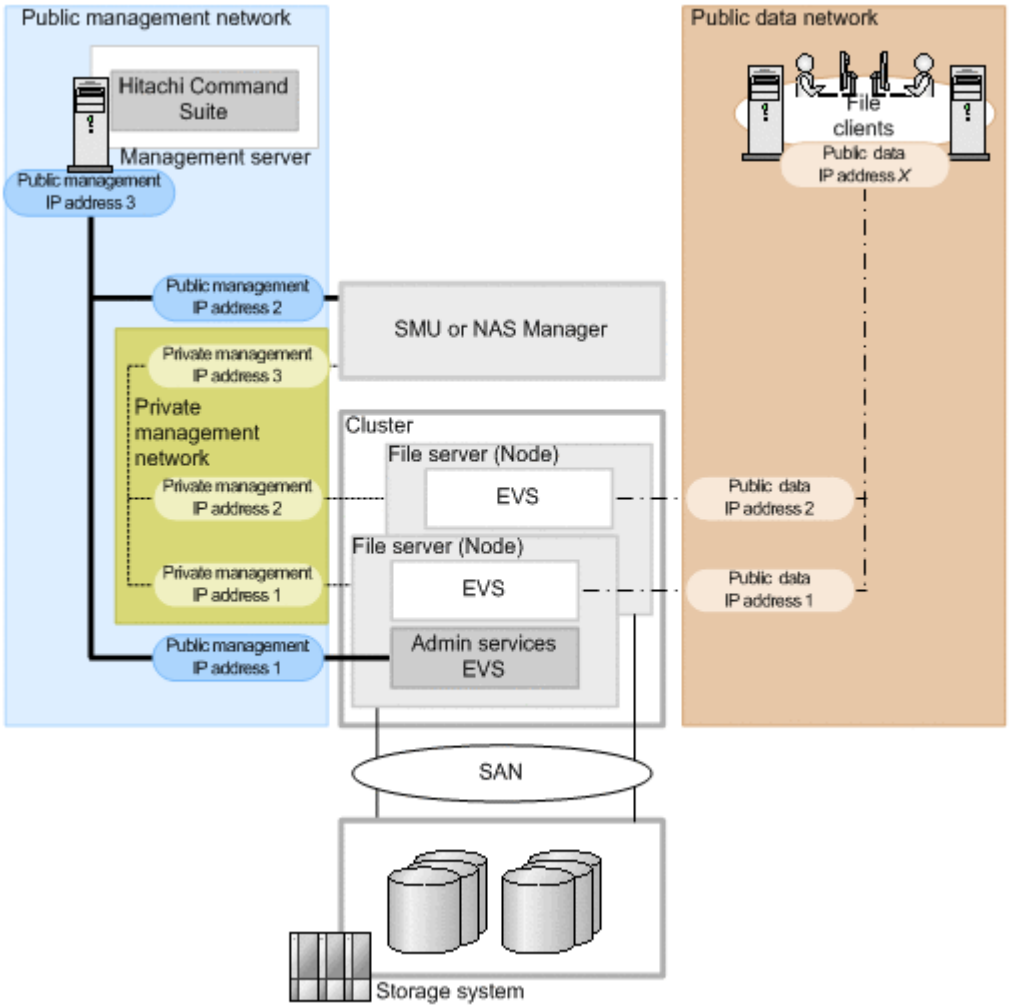


Figure 10 Environment settings for NAS Platform

- Locate the management server on a network that can communicate with SMU or NAS Manager.
  To use the Device Manager GUI to create file systems for firmware version 10.2.3071 or later of NAS Platform , set up the system so that it can also communicate with Admin services EVS.
- Make sure that the version of SMU or NAS Manager is the same or later as the firmware version of the file server (node).
- Make sure that the versions of the firmware for the file servers (nodes) in a cluster are all the same.
- If Device Manager is managing firmware version 10.2.3071 or later of NAS Platform , register the following information for each cluster by using the Device Manager GUI:
  - IP address of Admin services EVS (`Public management IP address 1` in the figure)

The IP address can be checked in the EVS Management page of SMU or NAS Manager.
For details on how to check the IP address, see the NAS Platform family manual.

- User account for the Server Control (SSC)
  A `supervisor` account is set up as the default user.

Note: If you want to use the Device Manager GUI to check information such as the system drive and storage pool information of the file server, the file system information, or the sharing and exporting information, you need to configure LUN security for the file server from the storage system volume.

Environment settings for Hitachi Data Ingestor and Hitachi NAS Platform F

To manage Hitachi Data Ingestor and Hitachi NAS Platform F by using Device Manager, you must make a system configuration in which the management server where Hitachi File Services Manager is installed and the management server where Device Manager is installed can communicate.

Depending on the operation performed in Device Manager, the installation conditions of Hitachi File Services Manager differ.

Table 5 Installation conditions of Hitachi File Services Manager

Operation from Device Manager		When installed in the same management server as Device Manager	When installed in the different management server from Device Manager
Start Hitachi File Services Manager (the login window)		Y	Y
Register or manage file servers		Y	Y
Allocate volumes to a file server		Y	Y
Create, expand, or delete a file system		Y	--
Add, edit, or cancel a file share		Y	--
Check information on the Dashboard	Check the capacity information of a file system	Y	Y
	Check the capacity information of a snapshot and the usage status of a tiered file system	Y	--
Monitor alerts of file servers		Y	Y

Legend:

Y: You can perform the operation.

--: You cannot perform the operation.

For details on how to install Hitachi File Services Manager and the environment settings, see the Hitachi Data Ingestor or Hitachi NAS Platform F manual. For details on prerequisite version of Hitachi File Services Manager, see the Hitachi Data Ingestor or Hitachi NAS Platform F manual.

Related concepts

- Setting up alerts on page 405

Operation workflow of managing file servers

To allocate volumes to file servers and check volume information, you must specify the necessary environment settings for the file server management software and Device Manager.

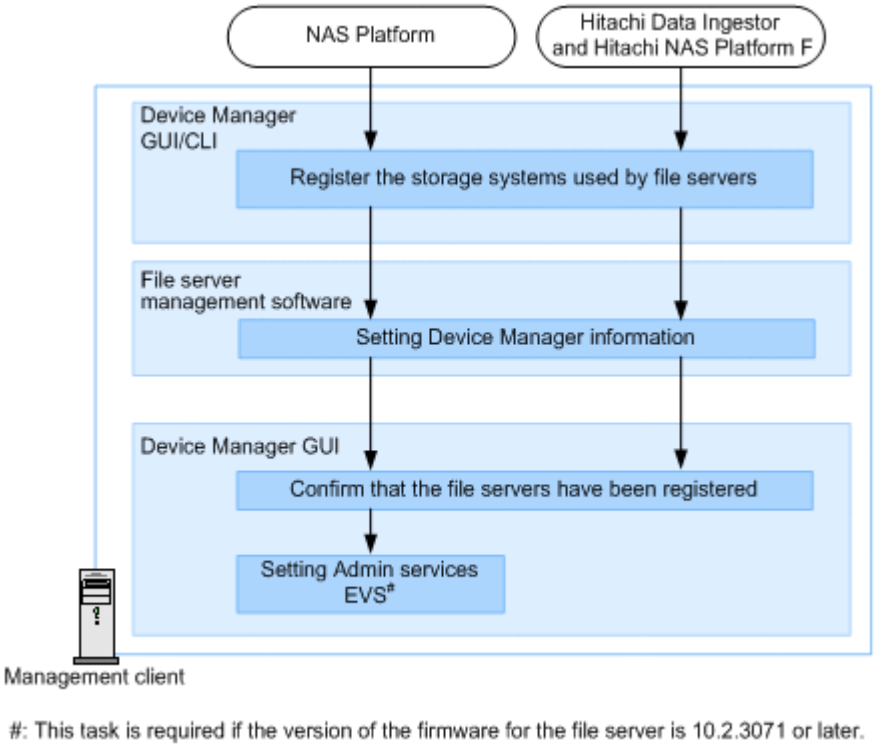


Figure 11 Operation workflow of managing file servers

For details on how to specify the settings for the storage systems and file server management software that can be used on file servers, see the file server documentation.

For details on how to specify the settings for the Device Manager GUI or CLI, see the *Hitachi Command Suite User Guide* or *Hitachi Command Suite CLI Reference Guide*.

Notes on operating file servers

Note the following when operating file servers:

- If Device Manager is upgraded from version 6.3 or earlier, we recommend that you change the value of the `server.http.entity.maxLength` property in the `server.properties` file to `1310720` or more.
- For NAS Platform, file server information is applied to the Device Manager database every day at 3:00 AM.
  When the SMU or NAS Manager version is 10.2.3071 or later:
  You can perform a synchronization operation in the SMU or NAS Manager Hitachi Device Managers window to apply the latest NAS Platform information to the Device Manager database whenever you wish.
  When the SMU version is earlier than 10.2.3071:
  When you re-register the file server from SMU, the latest NAS Platform information is applied to the Device Manager database (you do not need to delete anything).
  For details on how to specify the settings for SMU or NAS Manager, see the NAS Platform family manual.
- For Hitachi Data Ingestor and Hitachi NAS Platform F, file server information is applied to the Device Manager database once a day. You can specify when to apply by using Hitachi File Services Manager. You can also specify the settings so that file server information is automatically applied to the Device Manager database when it is applied to the Hitachi File Services Manager database.
  For details on how to specify the settings for Hitachi File Services Manager, see the manual for Hitachi Data Ingestor or Hitachi NAS Platform F.
- If NAS Platform has been registered as a normal host in Device Manager, you must unregister the platform before reregistering it as a file server.
  Note that, if the host name (the file server name) of the NAS Platform matches the host name of a file server or a normal host that has already been registered in Device Manager, the NAS Platform will be registered as a file server. (The information of the database will be overwritten.)

Related tasks

- Changing Device Manager server properties on page 590

Related references

- server.http.entity.maxLength on page 594

System requirements for NAS modules

You can use Device Manager to allocate storage system volumes to NAS modules or to check information about NAS modules.

Operation workflow for managing NAS modules

To allocate volumes to NAS modules and check volume information, you must specify the necessary environment settings for the NAS Manager management software and Device Manager.

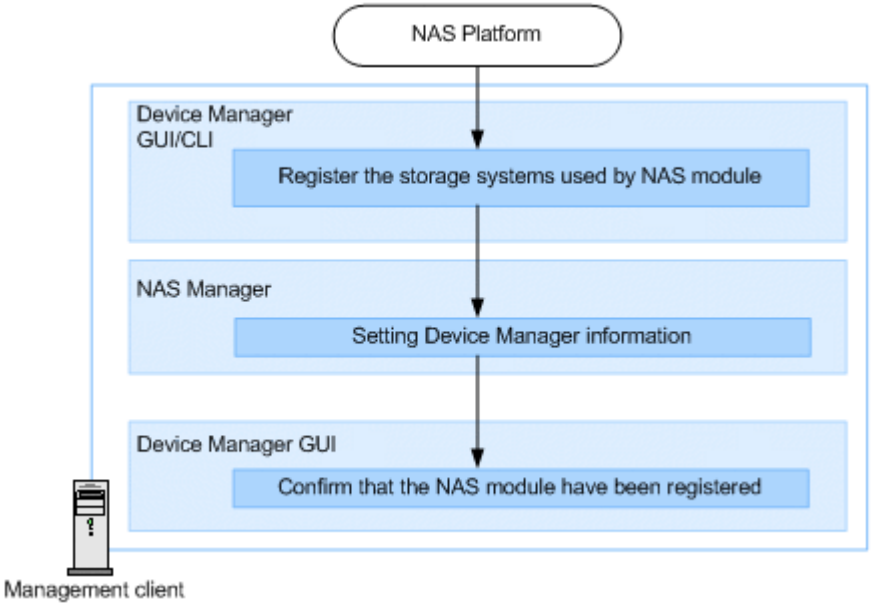


Figure 12 Operation workflow for managing file modules

For details on how to specify the settings for the Device Manager GUI or CLI, see the *Hitachi Command Suite User Guide* or *Hitachi Command Suite CLI Reference Guide*.

Notes on operating NAS modules

Note the following when operating NAS modules:

- For NAS Platform, NAS module information is applied to the Device Manager database every day at 3:00 AM.

  You can perform a synchronization operation in the NAS Manager Hitachi Device Managers window to apply the latest NAS Platform information to the Device Manager database whenever you wish.

  For details on how to specify the settings for NAS Manager, see the manual for the NAS Platform family.

- If Device Manager is to be linked with a NAS Manager that exists separately from the storage system, Device Manager can be linked with only one NAS Manager machine.

Related products

This section describes the products related to Device Manager and Tiered Storage Manager.

Replication Manager

Replication Manager provides centralized management of configurations and operating statuses of replication volumes distributed over a storage network. The Replication Manager GUI can be displayed from Device Manager GUI.

Tuning Manager

Tuning Manager provides support for the stable operation of storage systems through the centralized monitoring of performance and capacities for the entire storage network. The Tuning Manager GUI can be displayed from Device Manager GUI.

Dynamic Link Manager

Dynamic Link Manager manages each LUN path between a storage system and host.

Global Link Manager

Global Link Manager provides centralized management of LUN paths for multiple hosts. The Global Link Manager GUI can be displayed from Device Manager GUI.

Compute Systems Manager

Compute Systems Manager provides support for the operation and management of hosts (business servers) in a large-scale system environment. It can collect host asset information, check error information, and control power supplies. The Compute Systems Manager GUI can be displayed from Device Manager GUI.

Automation Director

Automation Director provides necessary tools to automate and simplify the end-to-end storage provisioning process for storage and data center administrators. The building blocks of the product are pre-packaged automation templates known as service templates.

Hitachi File Services Manager

Hitachi File Services Manager operates and manages Hitachi Data Ingestor and Hitachi NAS Platform F. The Hitachi File Services Manager GUI can be displayed from Device Manager GUI.

Hitachi Storage Services Manager

Hitachi Storage Services Manager acts as the main console for heterogeneous storage infrastructure management software, providing SAN visualization and reporting, asset management, performance and capacity monitoring and planning, and policy-driven event management.

System requirements for managing copy pairs

Device Manager improves reliability of the system by replicating storage system volumes and providing redundancy of important business data.

For Device Manager, a pair of the primary volume (P-VOL) and the secondary volume (S-VOL) to be replicated is called a *copy pair*.

In Device Manager , the following components can be used to manage copy pairs:

- When using the Replication tab
  You can manage the configuration of replications not only at one site but also across multiple sites. Each site consists of one management server, one pair management server, and multiple storage systems. By using the Replication tab, you can configure a TrueCopy pair or Universal Replicator pair between a site and another remote site, which enables operations that prepare for disaster recovery.
  You can also perform a disaster recovery test for an existing replicated configuration by simply using the Replication tab.
  To use the Replication tab, the license for Replication Manager is required.
  The following sections describe the system configuration and requirements of the copy pair management that is required for using the replication management functionality. For details about the configuration and settings necessary for linking with multiple sites when using the replication management functionality, see the chapter that describes the settings necessary for using the replication management functionality by using the Replication tab.
- When launching and using the Replication Manager GUI from the Device Manager GUI
  You can manage the configuration of replications not only at one site but also across multiple sites, and prepare operations for disaster recovery.
  By installing Replication Manager Application Agent, you can also manage volume replications from Exchange Server and SQL Server.
  Even if the Replication Manager license is not registered, you can use a part of the Replication Manager functionality by only using the Device Manager license. However, you cannot manage the configuration of replications across multiple sites.
- When using the Device Manager CLI
  You can use the Device Manager CLI to define copy pairs or change pair statuses. However, you cannot manage the configuration of replications across multiple sites.



Tip: In Device Manager, you can configure a high availability system by duplicating data on two units of the storage systems by using a global-active device functionality.

Related concepts

- Configuring a high availability system on page 93
- Settings required to use the replication management functionality on the Replication tab on page 365

Related references

- System configuration for managing copy pairs (central management method) on page 63
- System configuration for managing copy pairs (other than the central management method) on page 67
- Storage system requirements for managing copy pairs on page 84
- Notes on managing copy pairs on page 88
- Prerequisite version of the Device Manager agent for managing copy pairs on page 85

System configuration for managing copy pairs (central management method)

In this configuration, copy pairs are centrally managed by connecting a command device to a computer other than a host (application server) via Fibre Channel.

The central management method allows you to manage copy pairs for a host on which a Device Manager agent cannot be installed due to the host OS.In addition, the central management method also allows you to manage the copy pairs of volumes assigned to file servers or NAS modules.

To manage copy pairs by using the Replication tab, the system configuration must be the central management method.

Set up the management server, pair management server, and storage system so that the prerequisites are satisfied.

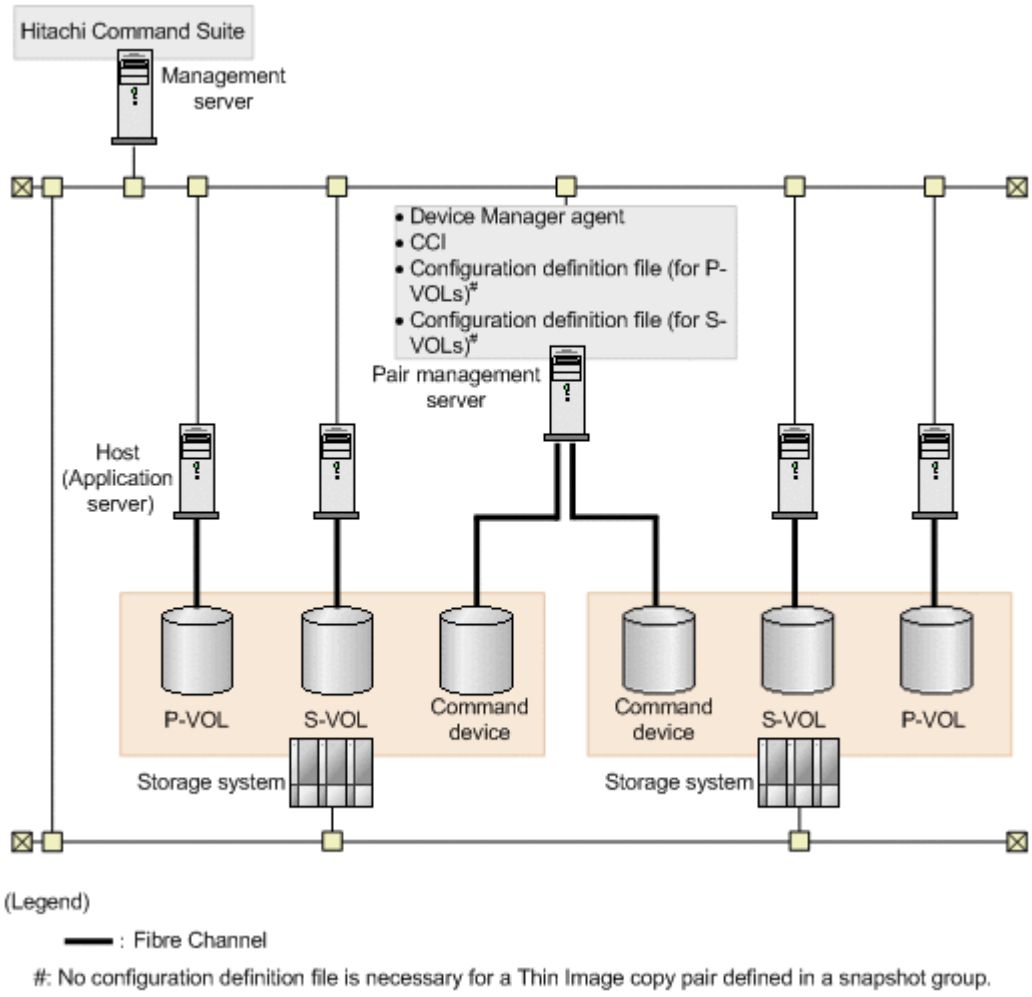


Figure 13 Example of a system configuration for managing copy pairs (central management method)

Management server conditions:

The following computers must be registered as the Device Manager management resources:

- A host that recognizes the P-VOL
- A host that recognizes the S-VOL
- Pair management server

Pair management server conditions:

- Device Manager agent must be installed on the pair management server.
- The `server.agent.rm.centralizePairConfiguration` property for the Device Manager agent on the pair management server must be set to `enable` (default: `disable`).
- CCI must be installed on the pair management server.

We recommend that you use the latest version of CCI.
If the version of the Device Manager agent is 8.0 or earlier, and CCI 01-32-03/*XX* or later is used, upgrade the Device Manager agent to version 8.0.1 or later.
If the command devices recognized by the pair management server support the authentication function, install version 01-25-03/01 or later of CCI on the pair management server.
For instructions on how to install CCI, see the CCI documentation.

- If there are multiple NICs on the pair management server, the Device Manager agent and CCI must use the same IP address.

Copy pair (P-VOL and S-VOL) conditions:

- The P-VOL and S-VOL must be managed by a single management server (Device Manager server).
- The P-VOL and S-VOL must be recognized by the hosts (application servers).
  We recommend that P-VOL and S-VOL be assigned to separate application servers.
- From the P-VOL and S-VOL, LUN security must be set for the host (application server).
  The pair management server does not need to recognize the P-VOL or S-VOL.

Command device conditions:

- The management server must recognize a command device.
  The command device security must not be used for a command device.
- From a command device, LUN security must be set for the pair management server.
  To manage copy pairs for TrueCopy or Universal Replicator, LUN security must be set for the host, from the command devices of the storage systems of both the P-VOL and S-VOL.
- A command device that belongs to a virtual storage machine and a command device that does not belong to a virtual storage machine must not be connected to the pair management server at the same time.



Tip: To check whether the host recognizes the P-VOL and S-VOL, and to check whether the pair management server recognizes the command device, use the `hldutil` command of the Device Manager agent.



Caution: Note the following when a command device whose authentication mode is enabled is connected to a pair management server:

- If multiple command devices in the same storage system are connected to the pair management server, enable authentication mode for all of the command devices.
- User authentication for the storage system must be completed before executing copy pair operations from the Device Manager GUI or CLI.
  If the version of the Device Manager agent is 8.0.1 or later, and SSL/TLS communication is used between the Device Manager server and the Device Manager agent, you do not need to manually authenticate users because user authentication is automatically performed.

Resource group conditions (when managing partitioned resources in VSP G1000, G1500, VSP F1500, VSP Gx00 models, VSP Fx00 models, Virtual Storage Platform, or HUS VM):

- The volumes below, or a storage system containing the volumes below, must be registered in a resource group managed by the user.
  - P-VOL
  - S-VOL
  - All pool volumes that make up a pool (when managing Copy-on-Write Snapshot or Thin Image pairs)
  - All journal volumes that make up a journal (when managing Universal Replicator pairs)
- A resource group in which a command device has been registered must be created and assigned to each user.
- Command devices whose storage system resource group ID is 0 (resource pools of the default virtual storage machine in VSP G1000, G1500, VSP F1500, VSP Gx00 models, or VSP Fx00 models) are connected to the pair management server, and the information of the command devices is defined in the `rgcmddev.properties` file of the Device Manager agent.
- The authentication mode for the command device is enabled.
- User authentication is completed for all command devices whose storage system resource group ID is 0 (resource pools of the default virtual storage machine in VSP G1000, G1500, VSP F1500, VSP Gx00 models, or VSP Fx00 models).
  If the version of the Device Manager agent is 8.0.1 or later, and SSL/TLS communication is used between the Device Manager server and the Device Manager agent, you do not need to manually authenticate users because user authentication is automatically performed.

When a virtual storage machine is created to manage resources in VSP G1000, G1500, VSP F1500, VSP Gx00 models, or VSP Fx00 models:

- The volumes below must be registered in a virtual storage machine by the user.
  - P-VOL
  - S-VOL
  - All pool volumes that make up a pool (when managing Copy-on-Write Snapshot or Thin Image pairs)
- Command devices and journal volumes are registered in resource groups created on the default virtual storage machine, and the command devices and the journal volumes are assigned to the user.

Caution: When the Device Manager agent is running, do not perform logout processing of user authentication for the storage system by directly executing a CCI command. If you do so, processing performed from the Device Manager GUI or CLI might not finish properly. If you need to log out, stop the Device Manager agent service first.

Related tasks

- Changing Device Manager agent properties on page 670

Related references

- Storage system requirements for managing copy pairs on page 84
- Prerequisite version of the Device Manager agent for managing copy pairs on page 85
- Acquiring device information (hldutil command) on page 539
- server.agent.rm.centralizePairConfiguration on page 684
- Properties for command devices connected to Device Manager agent (rgcmddev.properties file) on page 692

System configuration for managing copy pairs (other than the central management method)

The following describes system configurations other than the central management method.

- Configuration where copy pairs are managed at each host
  In this configuration, copy pairs are managed for each host by connecting a command device to each host (pair management server) via Fibre Channel.
- Configuration that uses a virtual command device server
  In this configuration, a command device is connected to a computer (virtual command device server) via Fibre Channel, and then copy pairs are managed by a computer on the LAN via the virtual command device server.
- Configuration that uses an SVP as a virtual command device

In this configuration, copy pairs are directly managed by using an SVP as a virtual command device instead of managed by using a storage system physical command device. You do not need to prepare a command device for the storage system. This configuration is supported only when both the P-VOL and S-VOL exist in VSP G1000, G1500, VSP F1500, VSP Gx00 models, VSP Fx00 models, Virtual Storage Platform, or HUS VM.
There are two types of configurations: configurations in which copy pairs are defined and managed by using a configuration definition file, and configurations in which copy pairs are defined and managed as a device group.

Note: When the authentication mode for command device is enabled or when SVP is used for a virtual command device and copy pairs are defined in the configuration definition file, the user authentication for the storage system must be completed before executing copy pair operation from Device Manager GUI or CLI.

If both of the following conditions are met, the user is automatically authenticated by the user account that was obtained from the Device Manager server.

- The version of the Device Manager agent is 8.0.1 or later.
- SSL/TLS communication is used between the Device Manager server and the Device Manager agent.

In other cases, execute the CCI command (`raidcom -login`) and manually authenticate the user. Note the following if you manually authenticate the user.

- If the OS of the pair management server is Windows, authenticate the user by using the user that executed the Device Manager agent service (HBsA Service).
- If you authenticate a user for a storage system once, you can access all of the command devices in the same storage system.
- If you change the authentication mode status from disabled to enabled and if there is another host that recognizes the command device, also authenticate the user on that host.

Note:

- If copy pairs are managed in a configuration that uses an SVP (the out-of-band method), the processing time of Replication Manager might increase because the command response time of CCI tends to increase, compared to when copy pairs are managed in a configuration that uses a physical command device (the in-band method).

- In SVP configurations, you can use the GUI to check the configuration of and change the pair status of copy pairs defined as device groups.

Related concepts

- Operation workflow for secure communication between a management server and Device Manager agent on page 237

Related references

- Notes on managing copy pairs on page 88
- server.agent.rm.userAuthentication on page 689

System configuration for managing copy pairs at each host

Set up the management server, hosts (pair management servers), and storage system so that the prerequisites are satisfied.

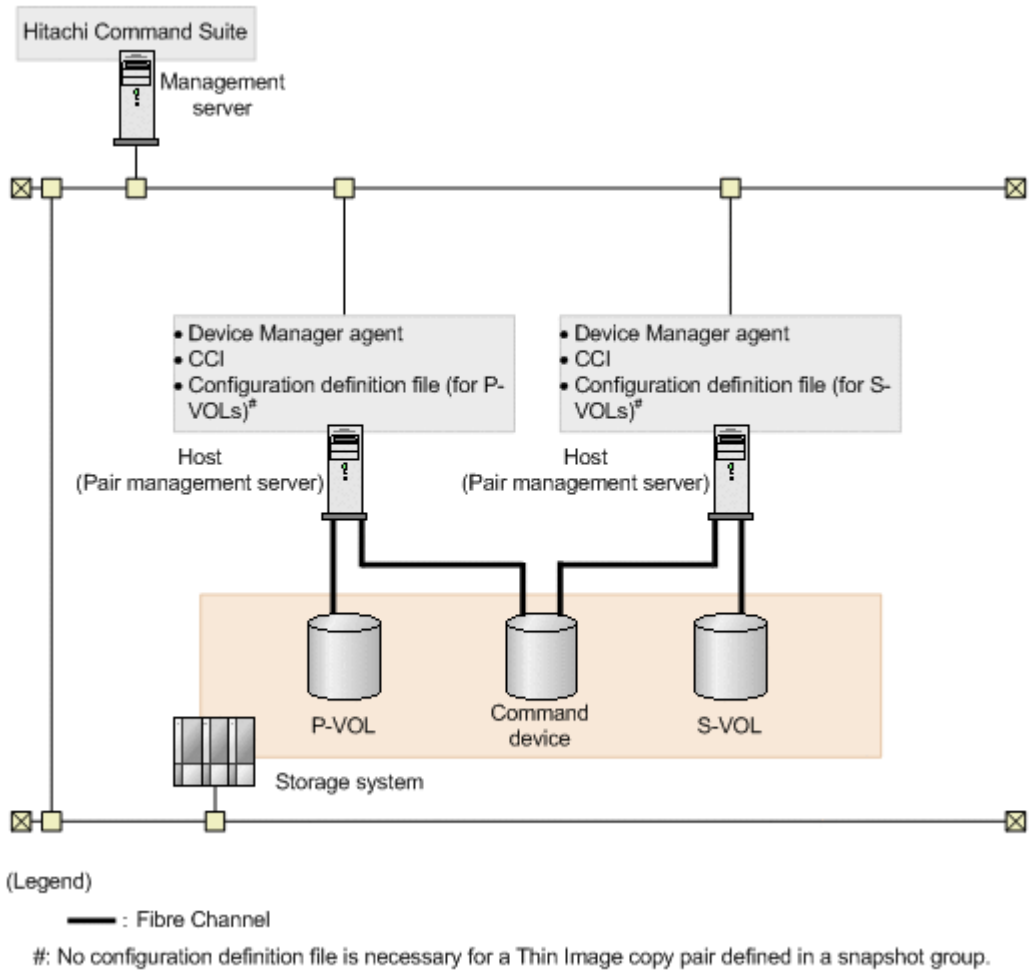


Figure 14 Example of a system configuration for managing copy pairs (for managing copy pairs at each host)

Management server conditions:

The following computers must be registered as the Device Manager management resources:

- A host that recognizes the P-VOL
- A host that recognizes the S-VOL

Host (pair management server) conditions:

- Device Manager agent must be installed on hosts as follows:
  - If there is one host that recognizes the P-VOL and one host that recognizes the S-VOL, install a Device Manager agent on each of the hosts.
  - If there are multiple hosts that recognize the P-VOL and multiple hosts that recognize the S-VOL, install a Device Manager agent on one of the hosts that recognize the P-VOL and one of the hosts that recognize the S-VOL.

  Note that if you manage copy pairs defined in a snapshot group, install a Device Manager agent on the host that recognizes the P-VOL (and you do not need to install it on the host that recognizes the S-VOL).
- CCI must be installed on hosts as follows:

  We recommend that you use the latest version of CCI.

  If the version of the Device Manager agent is 8.0 or earlier, and CCI 01-32-03/*XX* or later is used, upgrade the Device Manager agent to version 8.0.1 or later.

  If there are multiple hosts that recognize the P-VOL and multiple hosts that recognize the S-VOL, install CCI on one of the hosts that recognize the P-VOL and one of the hosts that recognize the S-VOL.

  If the command devices recognized by a host support the authentication function, install version 01-25-03/01 or later of CCI on the host.

  For instructions on how to install CCI, see the CCI documentation.
- If there are multiple NICs on the host, the Device Manager agent and CCI must use the same IP address.

Copy pair (P-VOL and S-VOL) conditions:

- The P-VOL and S-VOL must be managed by a single management server (Device Manager server).
- The P-VOL and S-VOL must be recognized by the hosts (pair management servers). Note that if you manage copy pairs defined in a snapshot group, the S-VOL does not need to be recognized by the hosts.

  We recommend that P-VOL and S-VOL be assigned to separate hosts.
- From the P-VOL or S-VOL, LUN security must be set for the host (pair management server).

From the P-VOL and S-VOL, LUN security can be set for different hosts.

Command device conditions:

- Both the host that recognizes the P-VOL and the host that recognizes the S-VOL must recognize a command device. Note that if you manage copy pairs defined in a snapshot group, the host that recognizes the S-VOL does not need to recognize a command device.
- From a command device, LUN security must be set for the hosts that recognize the P-VOL or S-VOL.
  For a host that recognizes the P-VOL, LUN security must be set from the command device on the P-VOL side. For a host that recognizes the S-VOL, LUN security must be set from the command device on the S-VOL side.
- A command device that belongs to a virtual storage machine and a command device that does not belong to a virtual storage machine must not be connected to the pair management server at the same time.

Tip: To check whether the host (pair management server) recognizes the P-VOL, S-VOL, and command device, use the `hldutil` command of the Device Manager agent.

Caution: Note the following when a command device whose authentication mode is enabled is connected to a host (pair management server):

- If multiple command devices in the same storage system are connected to the host, enable the authentication mode for all of the command devices.
- User authentication for the storage system must be completed before executing copy pair operations from the Device Manager GUI or CLI.
  If the version of the Device Manager agent is 8.0.1 or later, and SSL/TLS communication is used between the Device Manager server and the Device Manager agent, you do not need to manually authenticate users because user authentication is automatically performed.

Resource group conditions (when managing partitioned resources in VSP G1000, G1500, VSP F1500, VSP Gx00 models, VSP Fx00 models, Virtual Storage Platform, or HUS VM):

- The volumes below, or a storage system containing the volumes below, must be registered in a resource group managed by the user.
  - P-VOL
  - S-VOL

- All pool volumes that make up a pool (when managing Copy-on-Write Snapshot or Thin Image pairs)
- All journal volumes that make up a journal (when managing Universal Replicator pairs)

- A resource group in which a command device has been registered must be created and assigned to each user.
- Command devices whose storage system resource group ID is 0 (resource pools of the default virtual storage machine in VSP G1000, G1500, VSP F1500, VSP Gx00 models, or VSP Fx00 models) are connected to the host, and the information of the command devices is defined in the `rgcmddev.properties` file of the Device Manager agent.
- The authentication mode for command device is enabled.
- User authentication is completed for all command devices whose storage system resource group ID is 0 (resource pools of the default virtual storage machine in VSP G1000, G1500, VSP F1500, VSP Gx00 models, or VSP Fx00 models).
  If the version of the Device Manager agent is 8.0.1 or later, and SSL/TLS communication is used between the Device Manager server and the Device Manager agent, you do not need to manually authenticate users because user authentication is automatically performed.

When a virtual storage machine is created to manage resources in VSP G1000, G1500, VSP F1500, VSP Gx00 models, or VSP Fx00 models:

- The volumes below must be registered in a virtual storage machine by the user.
  - P-VOL
  - S-VOL
  - All pool volumes that make up a pool (when managing Copy-on-Write Snapshot or Thin Image pairs)
- Command devices and journal volumes are registered in resource groups created on the default virtual storage machine, and the command devices and the journal volumes are assigned to the user.

Caution: When the Device Manager agent is running, do not perform logout processing of user authentication for the storage system by directly executing a CCI command. If you do so, processing performed from the Device Manager GUI or CLI might not finish properly. If you need to log out, stop the Device Manager agent service first.

Related tasks

- Changing Device Manager agent properties on page 670

Related references

- Storage system requirements for managing copy pairs on page 84
- Prerequisite version of the Device Manager agent for managing copy pairs on page 85
- Acquiring device information (hldutil command) on page 539
- Properties for command devices connected to Device Manager agent (rgcmddev.properties file) on page 692

System configuration for using a virtual command device server configuration to manage copy pairs

Set up the management server, hosts (pair management servers), virtual command device server, and storage system so that the prerequisites are satisfied.

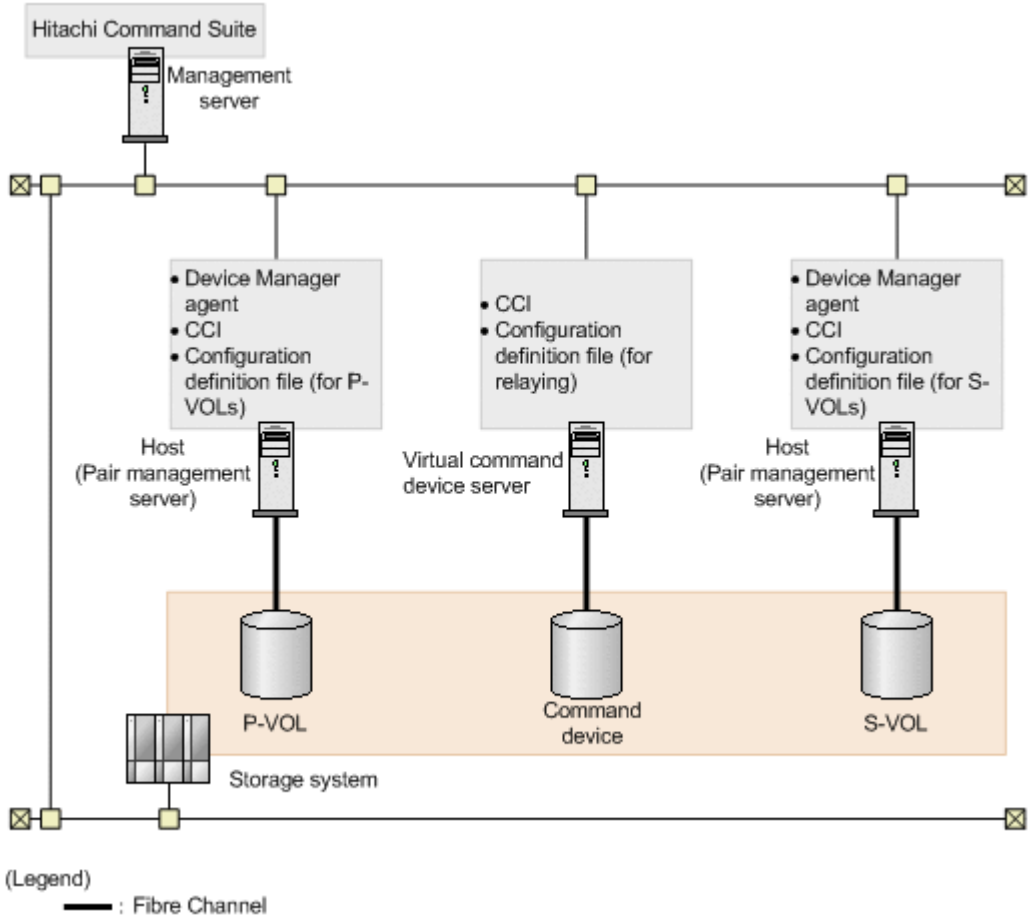


Figure 15 Example of a system configuration for managing copy pairs (virtual command device server configuration)

Management server conditions:

The following computers must be registered as the Device Manager management resources:

- A host that recognizes the P-VOL
- A host that recognizes the S-VOL

Host (pair management servers) conditions:

- Device Manager agent version 7.1 or later must be installed on the application servers.
- CCI version 01-25-03/01 or later must be installed on the application server.
  We recommend that you use the latest version of CCI.
  If the version of the Device Manager agent is 8.0 or earlier, and CCI 01-32-03/*XX* or later is used, upgrade the Device Manager agent to version 8.0.1 or later.
  For instructions on how to install CCI, see the CCI documentation.
- If there are multiple NICs on the host (pair management server), the Device Manager agent and CCI must use the same IP address.

Virtual command device server conditions:

- CCI version 01-25-03/01 or later must be installed on the virtual command device server.
  We recommend that you use the latest version of CCI.
  For instructions on how to install CCI, see the CCI documentation.
- The `horcm` instance for relay must be running on the virtual command device server.

Caution:

- If the `HORCM_ALLOW_INST` parameter is specified in the configuration definition file on the virtual command device server, the default port number (34000+*instance-number*+1) must be used for the CCI initiator port of the host (pair management server). To monitor the status of copy pairs, you need to allow access from instances used by the Replication Manager agent. Therefore, also set the instance number of the HORCM file for monitoring explained below.
  The instance numbers of the HORCM file for monitoring differ depending on the version of CCI.
  - If the version of CCI is 01-32-03/*XX* or later
  The instance numbers calculated from the values of the `agent.rm.horcmInstance` and `agent.rm.horcmRange` properties in the `agent.properties` file of the Device Manager agent are in the following range. (The default is the range from 1948 to 2047.) You do not need to set instance numbers that you want to intentionally reject.
  Maximum value: *value-specified-by-the-agent.rm.horcmInstance-property*

Minimum value: (*value-specified-by-the-agent.rm.horcmInstance-property*) - (*value-specified-by-the-agent.rm.horcmRange-property*) + 1

- If the version of CCI is earlier than 01-32-03/*XX*

Set the value specified by the `agent.rm.horcmInstance` property of the Device Manager agent, and the instance number of the *value-specified-by-the-agent.rm.horcmInstance-property* - 1. (The defaults are 2046 and 2047.)

- Note the following when a command device whose authentication mode is enabled is connected to a virtual command device server:

  - If multiple command devices in the same storage system are connected to the virtual command device server, enable authentication mode for all of the command devices.
  - User authentication for the storage system must be completed before executing copy pair operations from the Device Manager GUI or CLI.

  If the version of the Device Manager agent is 8.0.1 or later, and SSL/TLS communication is used between the Device Manager server and the Device Manager agent, you do not need to manually authenticate users because user authentication is automatically performed.

Copy pair (P-VOL and S-VOL) conditions:

- The P-VOL and S-VOL must be managed by a single management server (Device Manager server).
- The P-VOL and S-VOL must be recognized by the hosts (pair management servers).
  We recommend that P-VOL and S-VOL be assigned to separate pair management servers.
- From the P-VOL and S-VOL, LUN security must be set for the host (pair management server).
  The virtual command device server does not need to recognize the P-VOL or S-VOL.

Command device conditions:

- The virtual command device server must recognize a command device.
  The command device security must not be used for a command device.
- From a command device, LUN security must be set for the virtual command device server.

To manage copy pairs for TrueCopy or Universal Replicator, LUN security must be set for the host, from the command devices of the storage systems of both the P-VOL and S-VOL.
- A command device that belongs to a virtual storage machine and a command device that does not belong to a virtual storage machine must not be connected to the pair management server at the same time.

Tip: To check whether the host (pair management server) recognizes the P-VOL and S-VOL, and to check whether the virtual command device server recognizes the command device, use the `hldutil` command of the Device Manager agent.

Resource group conditions (when managing partitioned resources in VSP G1000, G1500, VSP F1500, VSP Gx00 models, VSP Fx00 models, Virtual Storage Platform, or HUS VM):

- The volumes below, or a storage system containing the volumes below, must be registered in a resource group managed by the user.
  - P-VOL
  - S-VOL
  - All pool volumes that make up a pool (when managing Copy-on-Write Snapshot or Thin Image pairs)
  - All journal volumes that make up a journal (when managing Universal Replicator pairs)
- A resource group in which a command device has been registered must be created and assigned to each user.
- Command devices whose storage system resource group ID is 0 (resource pools of the default virtual storage machine in VSP G1000, G1500, VSP F1500, VSP Gx00 models, or VSP Fx00 models) are connected to the virtual command device server, and the information of the command devices is defined in the `rgcmddev.properties` file of the Device Manager agent.
- The authentication mode for the command device is enabled.
- User authentication is completed for all command devices whose storage system resource group ID is 0 (resource pools of the default virtual storage machine in VSP G1000, G1500, VSP F1500, VSP Gx00 models, or VSP Fx00 models).
  If the version of the Device Manager agent is 8.0.1 or later, and SSL/TLS communication is used between the Device Manager server and the Device Manager agent, you do not need to manually authenticate users because user authentication is automatically performed.

Note that managing partitioned resources might slow down the display for some Replication Manager GUI operations. If a virtual command

device is to be used, we recommend that you allocate the resource group for each storage system (default resource group) to users.

When a virtual storage machine is created to manage resources in VSP G1000, G1500, VSP F1500, VSP Gx00 models, or VSP Fx00 models:

- The volumes below must be registered in a virtual storage machine by the user.
  - P-VOL
  - S-VOL
  - All pool volumes that make up a pool (when managing Copy-on-Write Snapshot or Thin Image pairs)
- Command devices and journal volumes are registered in resource groups created on the default virtual storage machine, and the command devices and the journal volumes are assigned to the user.

Caution: When the Device Manager agent is running, do not perform logout processing of user authentication for the storage system by directly executing a CCI command. If you do so, processing performed from the Device Manager GUI or CLI might not finish properly. If you need to log out, stop the Device Manager agent service first.

Related tasks

- Changing Device Manager agent properties on page 670

Related references

- Storage system requirements for managing copy pairs on page 84
- Prerequisite version of the Device Manager agent for managing copy pairs on page 85
- Acquiring device information (hldutil command) on page 539
- agent.rm.horcmInstance on page 672
- agent.rm.horcmRange on page 673
- Properties for command devices connected to Device Manager agent (rgcmddev.properties file) on page 692

System configuration for using an SVP configuration to manage copy pairs (when copy pairs are defined in a configuration definition file)

Set up the management server, pair management server, and storage system so that the prerequisites are satisfied.

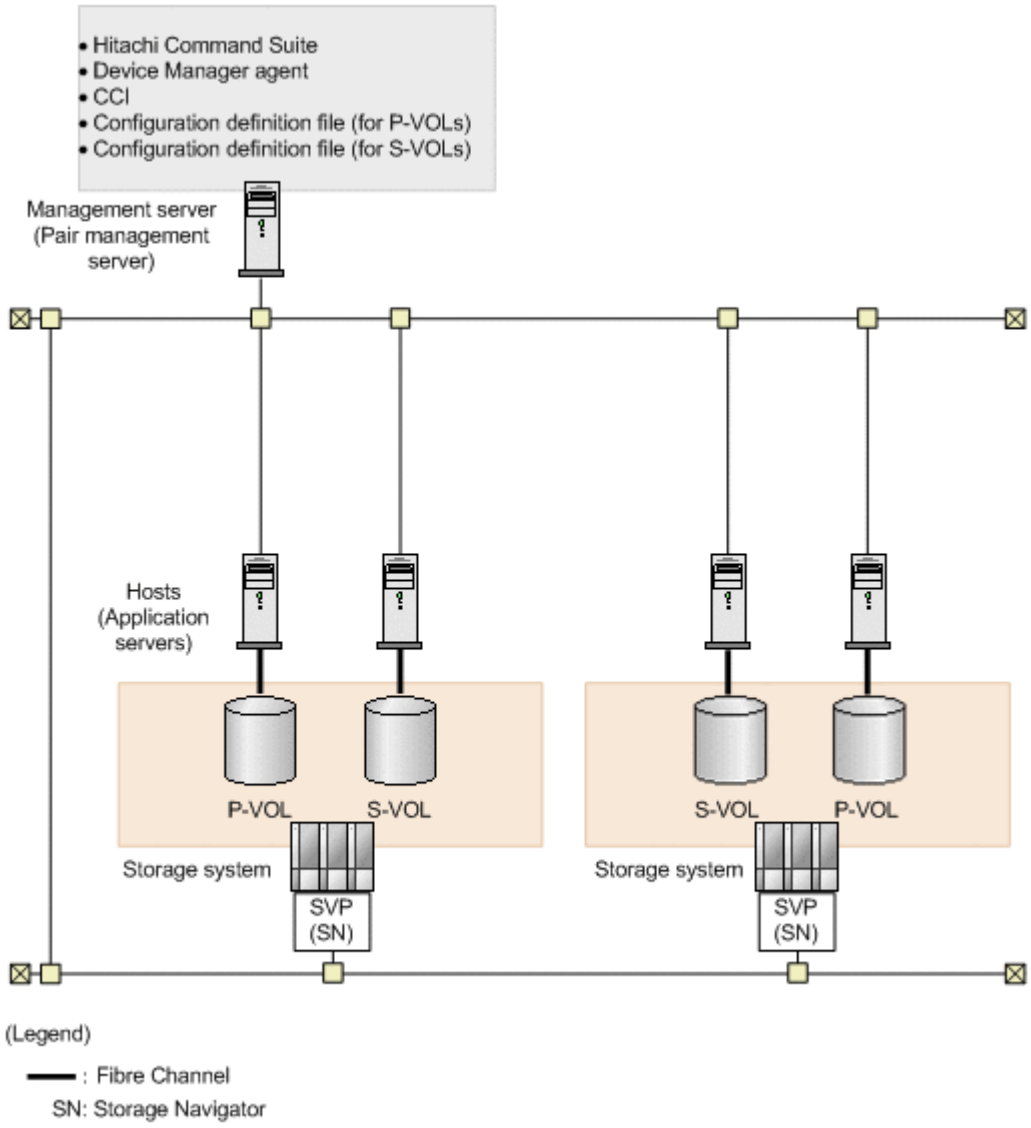


Figure 16 Example of a system configuration for managing copy pairs (when copy pairs are defined in a configuration definition file)

Management server (pair management server) conditions:

- The following computers must be registered as the Device Manager management resources:
  A host that recognizes the P-VOL
  A host that recognizes the S-VOL
- Device Manager agent version 7.1 or later must be installed on the pair management server.
- CCI version 01-25-03/01 or later must be installed on the pair management server.
  We recommend that you use the latest version of CCI.

If the version of the Device Manager agent is 8.0 or earlier, and CCI 01-32-03/*XX* or later is used, upgrade the Device Manager agent to version 8.0.1 or later.
For instructions on how to install CCI, see the CCI documentation.

Copy pair (P-VOL and S-VOL) conditions:

- The P-VOL and S-VOL must be managed by a single management server (Device Manager server).
- From the P-VOL and S-VOL, LUN security must be set for the host (application server).
  The management server does not need to recognize the P-VOL or S-VOL.
- The P-VOL and S-VOL must be recognized by the hosts (application servers).
  We recommend that P-VOL and S-VOL be assigned to separate application servers.



Tip: To check whether the host (application server) recognizes the P-VOL and S-VOL, use the `hldutil` command of the Device Manager agent.

Resource group requirements (when managing partitioned resources in VSP G1000, G1500, VSP F1500, VSP Gx00 models, VSP Fx00 models, Virtual Storage Platform, or HUS VM):

- The volumes below must be registered in a resource group managed by the user.
  - P-VOL
  - S-VOL
  - All pool volumes that make up a pool (when managing Copy-on-Write Snapshot or Thin Image pairs)
  - All journal volumes that make up a journal (when managing Universal Replicator pairs)

  Note that managing partitioned resources might slow the display for some Replication Manager GUI operations. If a virtual command device is to be used, we recommend that you allocate the resource group for each storage system (default resource group) to users.

When a virtual storage machine is created to manage resources in VSP G1000, G1500, VSP F1500, VSP Gx00 models, or VSP Fx00 models:

- The volumes below must be registered in a virtual storage machine by the user.
  - P-VOL
  - S-VOL

- All pool volumes that make up a pool (when managing Copy-on-Write Snapshot or Thin Image pairs)
- Journal volumes are registered in resource groups created on the default virtual storage machine, and the journal volumes are assigned to the user.

Caution:

- User authentication for the storage system must be completed before executing copy pair operations from the Device Manager GUI or CLI.
  If the version of the Device Manager agent is 8.0.1 or later, and SSL/TLS communication is used between the Device Manager server and the Device Manager agent, you do not need to manually authenticate users because user authentication is automatically performed.
- When the Device Manager agent is running, do not perform logout processing of user authentication for the storage system by directly executing a CCI command. If you do so, processing performed from the Device Manager GUI or CLI might not finish properly. If you need to log out, stop the Device Manager agent service first.
- If the user ID or password for the SVP is changed, the following changes must also be made from the GUI:
  1. From the Edit Storage Systems window of Device Manager, the new user ID or password for the SVP must be set.
  2. From the Configuration Setting window of Replication Manager, the configuration information of the storage system whose settings were changed must be refreshed.

Related references

- Storage system requirements for managing copy pairs on page 84
- Prerequisite version of the Device Manager agent for managing copy pairs on page 85
- Acquiring device information (hldutil command) on page 539

System configuration for using an SVP configuration to manage copy pairs (when copy pairs are defined as a device group)

Set up the management server, hosts (application servers), and storage system so that the prerequisites are satisfied.

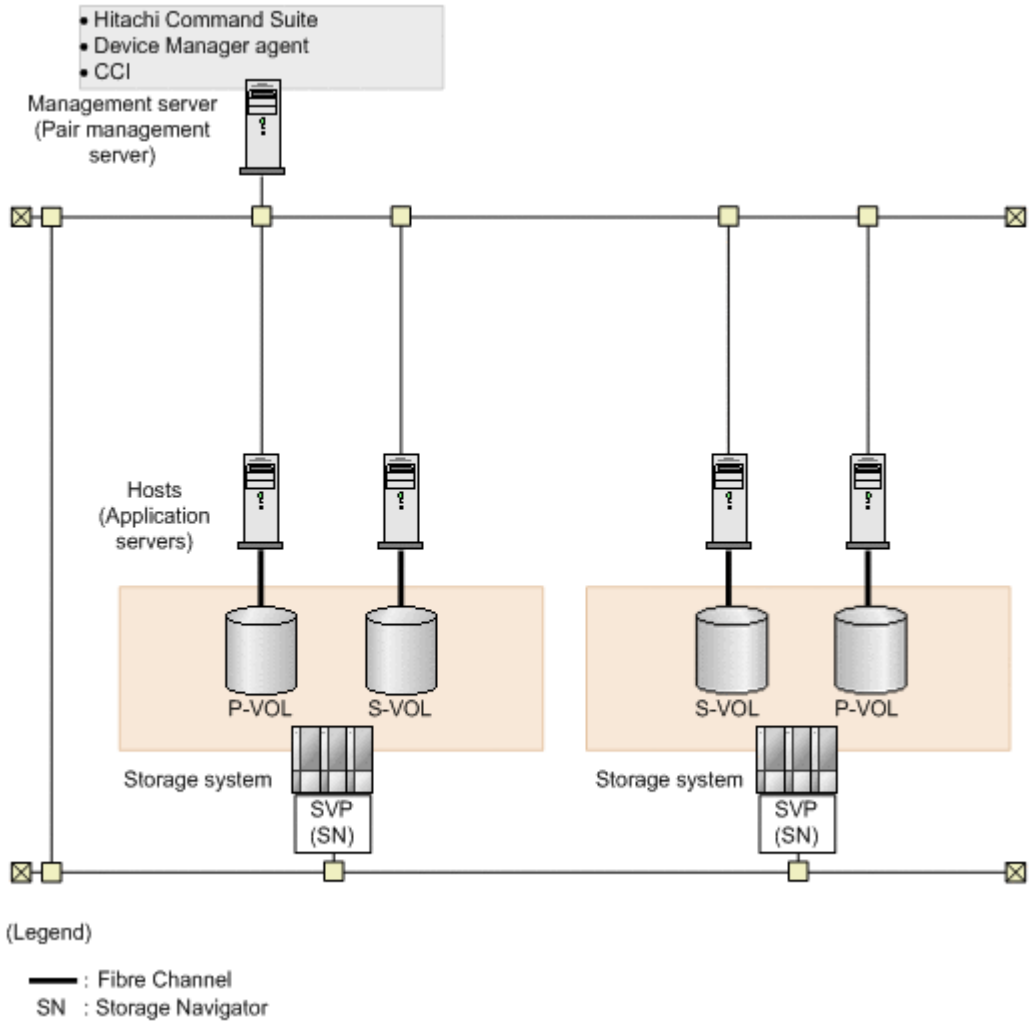


Figure 17 Example of a system configuration for managing copy pairs (when copy pairs are defined as a device group)

Management server (pair management server) conditions:

- The following computers must be registered as the Device Manager management resources:
  - A host that recognizes the P-VOL
  - A host that recognizes the S-VOL
- Device Manager agent version 7.1 or later must be installed on the management server.
- CCI version 01-25-03/01 or later must be installed on the pair management server.
  We recommend that you use the latest version of CCI.
  If the version of the Device Manager agent is 8.0 or earlier, and CCI 01-32-03/*XX* or later is used, upgrade the Device Manager agent to version 8.0.1 or later.
  For instructions on how to install CCI, see the CCI documentation.

- The Replication Manager server and the Device Manager server can communicate using SSL.
- Either of the conditions below is satisfied on the management server.
  - Neither the P-VOL nor S-VOL is assigned.
  If you want to create a copy pair from the management server, specify `enable` for the `server.agent.rm.centralizePairConfiguration` property of the Device Manager agent on the management server (default: `disable`).
  - The `server.agent.rm.ignorePairStatus` property for the Device Manager agent on the management server must be set to `true`.
  If you want to check the latest copy pair information by using the Device Manager GUI or CLI, refresh the storage systems by using the following methods:
  GUI: In the storage system view, select the target storage system, click the Refresh Storage System button.
  CLI: Execute the `AddStorageArray` command for the target storage system.

Copy pair (P-VOL and S-VOL) conditions:

- The P-VOL and S-VOL must be managed by a single management server (Device Manager server).
- From the P-VOL and S-VOL, LUN security must be set for the host (application server).
  The management server does not need to recognize the P-VOL or S-VOL.
- The P-VOL and S-VOL must be recognized by the hosts (application servers).
  We recommend that P-VOL and S-VOL be assigned to separate application servers.



Tip: To check whether the host (application server) recognizes the P-VOL and S-VOL, use the `hldutil` command of the Device Manager agent.

Resource group requirements (when managing partitioned resources in VSP G1000, G1500, VSP F1500, VSP Gx00 models, VSP Fx00 models, Virtual Storage Platform, or HUS VM):

- The volumes below must be registered in a resource group managed by the user.
  - P-VOL
  - S-VOL
  - All pool volumes that make up a pool (when managing Copy-on-Write Snapshot or Thin Image pairs)

- All journal volumes that make up a journal (when managing Universal Replicator pairs)

Note that managing partitioned resources might slow the display for some Replication Manager GUI operations. If a virtual command device is to be used, we recommend that you allocate the resource group for each storage system (default resource group) to users.

When a virtual storage machine is created to manage resources in VSP G1000, G1500, VSP F1500, VSP Gx00 models, or VSP Fx00 models:

- The volumes below must be registered in a virtual storage machine by the user.
  - P-VOL
  - S-VOL
  - All pool volumes that make up a pool (when managing Copy-on-Write Snapshot or Thin Image pairs)
- Journal volumes are registered in resource groups created on the default virtual storage machine, and the journal volumes are assigned to the user.

Caution:

- Do not install Replication Manager Application Agent on the management server.
- When the Device Manager agent is running, do not perform logout processing of user authentication for the storage system by directly executing a CCI command. If you do so, processing performed from the Device Manager GUI or CLI might not finish properly. If you need to log out, stop the Device Manager agent service first.
- If the user ID or password for the SVP is changed, the following changes must also be made from the GUI:

  1. From the Edit Storage Systems window of Device Manager, the new user ID or password for the SVP must be set.
  2. From the Configuration Setting window of Replication Manager, the configuration information of the storage system whose settings were changed must be refreshed.

Related concepts

- Operation workflow for secure communication between a Device Manager server and Replication Manager server on page 230

Related tasks

- Changing Device Manager agent properties on page 670

Related references

- Storage system requirements for managing copy pairs on page 84

- Prerequisite version of the Device Manager agent for managing copy pairs on page 85
- Acquiring device information (hldutil command) on page 539
- server.agent.rm.centralizePairConfiguration on page 684
- server.agent.rm.ignorePairStatus on page 689

Storage system requirements for managing copy pairs

To manage copy pairs, a storage system environment must be configured.

Configure a storage system environment in accordance with the following requirements. For details, see the operation manual for each storage system.

Tip: Use the Replication tab to set remote paths, journal groups, pools, and V-VOLs. For details, see *Hitachi Command Suite User Guide*.

- Remote path
  To perform operations on copy pairs by using Universal Replicator or TrueCopy, a remote path must be set between storage systems.
- Journal group
  To perform operations on copy pairs by using Universal Replicator, journal volumes must be registered to a journal group.
- Pool
  To perform operations on copy pairs by using Copy-on-Write Snapshot, Thin Image, or TrueCopy Extended Distance, pools must be set in advance.
  A pool is called a DP pool in HUS100, and a data pool in Hitachi AMS2000, Hitachi AMS/WMS, and Hitachi SMS.
- DM-LU
  A DM-LU must be set for the following cases:
  - When using TrueCopy remote replication or ShadowImage in HUS100
  - When using TrueCopy remote replication, TrueCopy Extended Distance, Copy-on-Write Snapshot, or ShadowImage in Hitachi AMS2000 and Hitachi AMS/WMS
  - When using Copy-on-Write Snapshot or ShadowImage in Hitachi SMS
- V-VOL
  To perform operations on copy pairs by using Copy-on-Write Snapshot or Thin Image, virtual volumes (V-VOL) must be created for the S-VOL.
  Perform the preparations in the following order:
  1. Create a pool.
  2. Create a V-VOL.

Caution:

- After the storage system environment has been configured, the storage system must be refreshed. Make sure that the latest information is displayed before performing operations on copy pairs.
- The storage system serial numbers managed by Device Manager must all be unique. In the case of TrueCopy or Universal Replicator, remote storage systems that are not managed by Device Manager must also have unique serial numbers.
- If you use VSP G1000, G1500, VSP F1500, VSP Gx00 models, VSP Fx00 models, Virtual Storage Platform, or HUS VM logical units to create a copy pair, do not use logical units associated with a device group.
- For an enterprise-class storage system, you can only check the configuration of mainframe volume copy pairs (copy pairs of Universal Replicator, TrueCopy, and ShadowImage) by using the Device Manager CLI.
- For Thin Image copy pairs defined in the snapshot group, you need to enable the authentication mode for the command devices.
  You also need to authenticate users by executing the `raidcom -login` command on the pair management server.
  If the version of the Device Manager agent is 8.0.1 or later, and SSL/TLS communication is used between the Device Manager server and the Device Manager agent, you do not need to manually authenticate users because user authentication is automatically performed.

Prerequisite version of the Device Manager agent for managing copy pairs

The prerequisite version of the Device Manager agent varies depending on the storage system to be managed and the program to be used.

When using the GUI to manage copy pairs

The prerequisite version of the Device Manager agent varies depending on the target storage system.

Table 6 Device Manager agent requirements for managing copy pairs by using the GUI

Storage system	Device Manager agent version
VSP G1000	8.0 or later
VSP G1500	8.5.0 or later
VSP F1500	8.5.0 or later
VSP G200, G400, G600	8.1.2 or later
VSP F400, F600	
VSP G800	8.2.0 or later

Storage system	Device Manager agent version
VSP F800	
Virtual Storage Platform	7.0 or later
Universal Storage Platform V/VM	6.0 or later
HUS VM	7.3.1 or later
HUS100	7.2.0 or later
Hitachi AMS2000	6.0 or later
Hitachi SMS	6.0 or later
Hitachi AMS/WMS	6.0 or later

When using the CLI to manage copy pairs

The prerequisite version of the Device Manager agent varies depending on the program, operations to be performed, and the model of the target storage system.

Table 7 Device Manager agent requirements for managing copy pairs by using the CLI

Program	Operation from Device Manager	Device Manager agent version#
Universal Replicator	Display the status	4.0 or later
	Display the status (3DC delta resync configuration via TrueCopy Sync and Universal Replicator)	5.5 or later
	Display the status (3DC delta resync configuration via global-active device and Universal Replicator)	8.1.4 or later
	Change the status	5.6 or later
	Change the status (3DC delta resync configuration via TrueCopy Sync and Universal Replicator)	5.5 or later
	Change the status (3DC delta resync configuration via global-active device and Universal Replicator)	8.1.4 or later
TrueCopy	Display the status	2.3 or later
	Display the status (TrueCopy Extended Distance)	5.1 or later
	Change the status	2.4 or later
	Change the status (TrueCopy Extended Distance)	5.1 or later
Simple Data Recovery	Display the status	6.0 or later
ShadowImage	Display the status	2.3 or later
	Display the status (maximum 1:3)	5.5 or later
	Change the status	2.4 or later

Program	Operation from Device Manager	Device Manager agent version#
	Change the status (maximum 1:3)	5.5 or later
Copy-on-Write Snapshot	Display the status	4.1 or later
	Change the status	4.1 or later
Thin Image	Display the status	7.4.0 or later
	Change the status	7.6.1 or later
global-active device	Display the status (if global-active device pairs consist of DP volumes)	8.0.1 or later
	Display the status (if global-active device pairs consist of normal volumes)	8.1.4 or later
	Change the status (if global-active device pairs consist of DP volumes)	8.0.1 or later
	Change the status (if global-active device pairs consist of normal volumes)	8.1.4 or later
Note: To create a configuration definition file, Device Manager agent version 3.1 or later must be installed on each host.		

#:

The following table lists the Device Manager agent version required for each storage system model.

Table 8 Device Manager agent version required for each storage system model when managing copy pairs by using the CLI

Storage system model	Device Manager agent version
VSP G1000	8.0 or later
VSP G1500	8.5.0 or later
VSP F1500	8.5.0 or later
VSP G200, G400, G600	8.1.2 or later
VSP F400, F600	
VSP G800	8.2.0 or later
VSP F800	
Hitachi Virtual Storage Platform	7.0 or later
Hitachi Universal Storage Platform V	5.7 or later
Hitachi Universal Storage Platform VM	5.8 or later
Hitachi Unified Storage VM	7.3.1 or later
Hitachi Unified Storage 150	7.2.0 or later
Hitachi Unified Storage 130	
Hitachi Unified Storage 110	

Storage system model	Device Manager agent version
Hitachi Adaptable Modular Storage AMS2500 (H/W Rev. 0100)	6.0 or later
Hitachi Adaptable Modular Storage AMS2300 (H/W Rev. 0100)	
Hitachi Adaptable Modular Storage AMS2100 (H/W Rev. 0100)	
Hitachi Adaptable Modular Storage AMS2500 (H/W Rev. 0200)	6.4 or later
Hitachi Adaptable Modular Storage AMS2300 (H/W Rev. 0200)	
Hitachi Adaptable Modular Storage AMS2100 (H/W Rev. 0200)	
Hitachi Adaptable Modular Storage AMS2010	
Hitachi Simple Modular Storage 100	6.0 or later
Hitachi Simple Modular Storage 110	6.1 or later
Hitachi Adaptable Modular Storage 1000	5.0 or later
Hitachi Adaptable Modular Storage 500	4.2 or later
Hitachi Adaptable Modular Storage 200	
Hitachi Workgroup Modular Storage 100	4.1 or later

Related references

- System configuration for managing copy pairs (central management method) on page 63
- System configuration for managing copy pairs at each host on page 69
- System configuration for using a virtual command device server configuration to manage copy pairs on page 73
- System configuration for using an SVP configuration to manage copy pairs (when copy pairs are defined in a configuration definition file) on page 77
- System configuration for using an SVP configuration to manage copy pairs (when copy pairs are defined as a device group) on page 80

Notes on managing copy pairs

Note the following when managing copy pairs:

When using CCI 01-32-03/*XX* or later

- For CCI 01-32-03/*XX* or later, you cannot specify pair definitions for both virtual IDs and physical IDs in one configuration definition file. You need to separately define virtual ID pairs in the configuration file for virtual IDs, and physical ID pairs in the configuration definition file for physical IDs. Follow the rules below to create a configuration definition file for virtual IDs and a configuration definition file for physical IDs:
  - The `HORCM_VCMD` parameter cannot be defined in a configuration definition file for physical IDs.
  - The `HORCM_VCMD` parameter can be defined in a configuration definition file for virtual IDs.

- The HORCM_DEV parameter cannot be defined in a configuration definition file for virtual IDs.
- Define pairs for storage systems that do not support virtual storage machines in a configuration definition file for physical IDs.
- You cannot define command devices for multiple storage systems in a configuration definition file for virtual IDs. Individually create a configuration definition file for virtual IDs for each storage system.

If you upgraded from CCI earlier than 01-32-03/*XX* and the above rules are not followed, you need to manually recreate the existing configuration definition files.

- When you manage copy pairs by using virtual IDs, if SSL/TLS communication is not used between the Device Manager server and the Device Manager agent, you need to perform user authentication for both the storage system and virtual storage machine.
  If user authentication has not been performed, the status of copy pairs using virtual IDs is not updated by the following operations:
  - When executing the HiScan command (manually or automatically)
  - When updating host information from the Device Manager GUI or CLI

In a configuration where virtual IDs are used to make serial numbers overlap among storage systems in VSP G1000, G1500, VSP F1500, VSP Gx00 models, or VSP Fx00 models

- If you are using CCI earlier than 01-32-03/*XX*, connect the command devices for each storage system to different pair management servers.
- If you are using CCI 01-32-03/*XX* or later, use different pair management servers to manage the configuration files that meet either of the following conditions:
  - The serial number defined for HORCM_VCMD in the configuration definition file for virtual IDs matches a serial number defined in the configuration definition file for physical IDs
  - Multiple configuration definition files for virtual IDs exist, and the same serial number is defined for HORCM_VCMD

If you migrated data by using virtual storage machines in VSP G1000, G1500, VSP F1500, VSP Gx00 models, or VSP Fx00 models

- Except when using the global-active device functionality, if you want to operate virtual volumes by using physical IDs, copy pairs must be configured in such a way that they are managed with the central management method.
- The configuration definition file must be recreated to match the new environment after migration.
  - If the CCI version is earlier than 01-32-03/*XX*, you can specify either a virtual ID or a physical ID for Serial#, devNum, and portName of the HORCM_LDEV parameter.

    - If the CCI version is 01-32-03/*XX* or later, you need to separately define virtual ID pairs in the configuration file for virtual IDs, and physical ID pairs in the configuration definition file for physical IDs.
    - For the `HORCM_CMD` parameter, specify the command devices whose storage system resource group ID is 0 (resource pools of the default virtual storage machine).
- Enable the authentication mode for the command devices if the microcode version of VSP G1000 is earlier than 80-02-01-*XX*/*XX*.
  In the following cases, operations can be performed for copy pairs by using a virtual storage machine volume, even if the authentication mode for the command device is disabled.
    - The microcode version for VSP G1000 is 80-02-01-*XX*/*XX* or later.
    - VSP G1500
    - VSP F1500
    - VSP Gx00 models
    - VSP Fx00 models

  However, when a command device with authentication mode enabled and a command device with authentication mode disabled both exist in VSP G1000, G1500, VSP F1500, VSP Gx00 models, or VSP Fx00 models, and are connected to the same pair management server, authentication mode must be enabled for all the command devices recognized by the same pair management server.
  A command device with its authentication mode enabled must be connected to the pair management server in the following cases:
    - When managing the Thin Image pairs defined in the snapshot group.
    - When managing global-active device pairs.
    - When managing pairs within the resource group by using something other than a virtual storage machine.
- User authentication must be completed for all command devices whose storage system resource group ID is 0 (meta_resource).
  If the version of the Device Manager agent is 8.0.1 or later, and SSL/TLS communication is used between the Device Manager server and the Device Manager agent, you do not need to manually authenticate users because user authentication is automatically performed.

If you migrated data by using virtual IDs in Virtual Storage Platform or HUS VM

- Copy pairs must be configured in such a way that they are managed with the central management method.
- The configuration definition file must be recreated to match the new environment after migration.

    - Specify the physical ID for `Serial#` of the `HORCM_LDEV` parameter.
    - For the `HORCM_CMD` parameter, specify the command devices whose storage system resource group ID is 0 (meta_resource).
- Enable the authentication mode for the command devices.
- User authentication must be completed for all command devices whose storage system resource group ID is 0 (meta_resource).
  If the version of the Device Manager agent is 8.0.1 or later, and SSL/TLS communication is used between the Device Manager server and the Device Manager agent, you do not need to manually authenticate users because user authentication is automatically performed.

If you use Device Manager to manage copy pairs that were created by using a management tool other than Device Manager

- When the copy pair is created by using Storage Navigator, SVP, or CCI/LIB
  You need to perform either of the following:
    - Manually create a configuration definition file to define the copy pair.
    - Dissolve the copy pair by using the management tool that was used when creating the copy pair, and then create a copy pair by using Device Manager.
- When the copy pair is a Thin Image copy pair defined in a copy group
  If you manage copy pairs of 65 generations or more from the Device Manager GUI, delete the existing copy group, and then create a copy pair by using a snapshot group.
  If you manage the copy pair from the Device Manager CLI, dissolve the copy pair by using the management tool that was used when creating the copy pair, and then create a copy pair from the Device Manager CLI.

If you changed the `server.horcmconfigfile.hostname` value in the `server.properties` file of the Device Manager server

In the following cases, you need to modify the configuration definition file because copy pairs will no longer be able to be managed from Device Manager:

- If the IP address of the host was changed when `ipaddress` is set for the `server.horcmconfigfile.hostname` property in the `server.properties` file of the Device Manager server
- If the host name was changed when `hostname` is set for the `server.horcmconfigfile.hostname` property in the `server.properties` file of the Device Manager server

To modify the configuration definition file, perform the following procedure:

1. Modify the configuration definition file of the local host.
2. Restart the Device Manager agent on the local host.
3. Modify the configuration definition file of the remote host.
4. Refresh the storage systems.

If you use Device Manager to control copy pairs that are managed by using CCI or Protection Manager

The configuration definition file on the pair management server that manages the P-VOL of the copy pair and the configuration definition file on the pair management server that manages the S-VOL of the copy pair must have the same group name and the same pair name. If different names are specified, Device Manager cannot control that copy pair. In addition, if you want to use a single pair management server to manage multiple copy pairs, make sure that these copy pairs satisfy the conditions written below. If there are copy pairs that do not satisfy the conditions, modify the configuration definition file.

- If the version of the Device Manager agent is 05-60 or earlier:
  Each copy pair on the pair management server must have a unique combination of the following items:
  Group name
  Pair name
- If the version of the Device Manager agent is 05-70 or later:
  Each copy pair on the pair management server must have a unique combination of the following items:
  Port number
  Group name
  Pair name

If you use configuration definitions files that were created by using Device Manager CLI in CCI

If you want to create a copy pair by using CCI or if CCI is already being used to manage copy pairs, you can use the Device Manager CLI to create a configuration definition file.

- You cannot use Device Manager to create copy pairs from configuration definition files created in the Device Manager CLI.
- To create copy pairs in CCI from configuration definition files created in the Device Manager CLI, you must change the MU numbers to appropriate values.
- If you have created an invalid configuration definition file by using the Device Manager, you cannot delete the file from Device Manager. To do this, you need to delete or edit the configuration definition file on the pair management server managing the copy pairs. An invalid configuration file or a configuration file that is not used for performing copy pair operations might affect system performance (for example, when adding or refreshing a storage system). Delete such configuration files from the pair management server that manages copy pairs.

Related concepts

- Managing copy pairs on page 521
- Configuration definition file for managing copy pairs on page 545

Related references

- server.horcmconfigfile.hostname on page 595

Configuring a high availability system

In Device Manager, you can configure a high availability system by duplicating data on two units of the storage system by using global-active device functionality and then making it possible to receive I/O from both units of the storage system.

The global-active device functionality can be used in the VSP G1000, G1500, VSP F1500, and VSP Gx00 models.

The VSP G1000, G1500, VSP F1500 and VSP Gx00 models can coexist in the primary storage system and the secondary storage system. The table below shows the available combinations of models in the primary storage system and the secondary storage system.

Table 9 Available combinations of models in the primary storage system and the secondary storage system

Primary storage system	Secondary storage system			
	VSP G1000 (Microcode version: 80-04-2*X-XX*/*XX* or later), VSP G1500, or VSP F1500	**VSP G1000 (Microcode version: earlier than 80-04-2*X-XX*/*XX*)**	**VSP Gx00 model (Microcode version: 83-03-2*X-XX*/*XX* or later)**	**VSP Gx00 model (Microcode version: 83-01-2*X-XX*/*XX* or later, but earlier than 83-03-2*X-XX*/*XX*)**
VSP G1000 (Microcode version: 80-04-2*X-XX*/*XX* or later), VSP G1500, or VSP F1500	Y	Y	Y	--
VSP G1000 (Microcode version: earlier than 80-04-2*X-XX*/*XX*)	Y	Y	--	--
VSP Gx00 model (Microcode version: 83-03-2*X-XX*/*XX* or later)	Y	--	Y	Y
VSP Gx00 model (Microcode version: 83-01-2*X-XX*/*XX* or later, but earlier than 83-03-2*X-XX*/*XX*)	--	--	Y	Y

(Legend)

Y: Can coexist

--: Cannot coexist

Note: By using the Replication tab, you can manage a high availability system configuration for not only one site, but also for multiple sites.

Related concepts

- Settings required to use the replication management functionality on the Replication tab on page 365

Example of a configuration for configuring a high availability system

The following figure shows an example of a system configuration for configuring a high availability system.

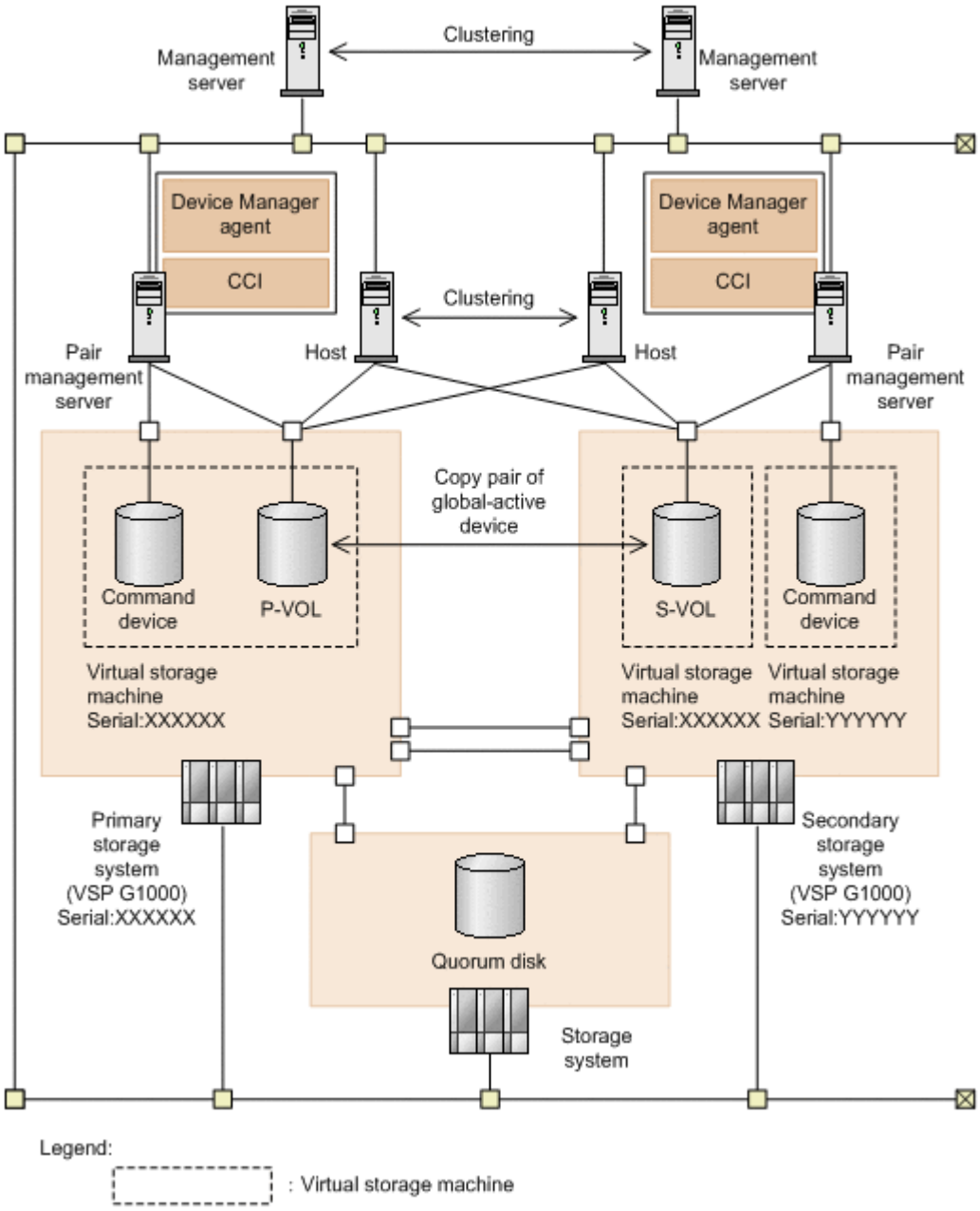


Figure 18 Example of a system configuration for configuring a high availability system

In this figure, the availability of the business system is enhanced by configuring a cluster configuration for a host and then duplicating two units of VSP G1000 by using the global-active device functionality. By providing, in a different storage system, a quorum disk that records which volume of a global-active device copy pair holds the latest information, you can continue business operations even if an error occurs in the storage systems. In addition, by configuring the management server for Hitachi Command Suite in a cluster configuration, you can continue managing the storage systems even if an error occurs in the management server.

Requirements for configuring a high availability system (for VSP G1000, G1500 or VSP F1500)

Configure the management server, pair management server, and storage systems so that the following conditions are satisfied.

Management server conditions:

- The Replication Manager license must be registered.
- The following computers must be registered as the Device Manager management resources:
  - A host that recognizes the P-VOL and the S-VOL
  - The primary site pair management server
  - The secondary site pair management server
  - The primary site storage system
  - The secondary site storage system
  - An external storage system used for quorum disks (When using the Device Manager CLI to configure a high availability system)

Host (application servers) conditions:

- Path management software must be installed.



Note:

- If the host OS is HP-UX 11i v3 and you are using the native multi-pathing features, execute the following command in advance to disable the multi-pathing features for legacy device special files:

  ```
  scsimgr save_attr -a leg_mpath_enable=false
  ```

- When the host OS is Windows or AIX, and MPIO is used, if VSP G1000 (whose microcode version is 80-04-0*X*-*XX*/*XX* or later), VSP G1500 or VSP F1500 is used, set the host mode option for the host group to `102`.

Storage system conditions (common to the primary and secondary sites):

- The prerequisite software for global-active device must be installed and the license must be enabled.
- The primary site and secondary site storage systems must be connected via two or more Fibre Channels or iSCSI, and a bidirectional remote path must be set between the primary site and secondary site storage systems.
- An external volume for quorum disk must exist on both the primary site and secondary site storage systems, and the same quorum disk ID must be set.
- There must be sufficient space in the storage system's cache and shared memory.

For details about prerequisite software, caches, or shared memory, see the global-active device documentation.

Conditions for external storage systems used for quorum disks

- There must be fibre-channel or iSCSI connections between the primary site storage system and the external storage system used for quorum disks, and between the secondary site storage system and the external storage system used for quorum disks.
- External paths must be set between the external port of the primary site storage system and the port of the external storage system used for quorum disks, and between the external port of the secondary site storage system and the port of the external storage system used for quorum disks.

Pair management server conditions (common to the primary and secondary sites):

- When VSP G1000 is used, Device Manager agent version 8.0.1 or later must be installed on the pair management server. When VSP G1500 or VSP F1500 is used, Device Manager agent version 8.5.0 or later must be installed on the pair management server.
- CCI version 01-32-03/*XX* or later must be installed on the pair management server.
  For instructions on how to install CCI, see the CCI documentation.
- If there are multiple NICs on the pair management server, the Device Manager agent and CCI must use the same IP address.

Pair volume conditions:

- The P-VOL and S-VOL must be managed by a single management server (Device Manager server).
- The P-VOL and S-VOL must be recognized by the hosts (application servers).
- Both the P-VOL and S-VOL must be open volumes.
- Both the P-VOL and S-VOL must be DP volumes or normal volumes (internal or external volumes).
- The volume types (DP volumes, internal volumes, or external volumes) of the P-VOL and S-VOL are the same.
- The model name and serial number of the virtual storage machine that the P-VOL belongs to must be the same as the model name and serial number of the virtual storage machine that the S-VOL belongs to.

Command device conditions:

- The command device security must not be set.
- Command devices must belong to the default virtual storage machine.
- When managing partitioned resources in the storage system, the host (pair management server) must be connected to the command devices whose storage system resource group ID is 0 (resource pools of the default virtual storage machine), and the information of the command devices is defined in the `rgcmddev.properties` file of the Device Manager agent.
- The authentication mode for the command device is enabled.

- User authentication for the storage system is completed before performing operations on global-active device copy pairs from the Device Manager GUI or CLI.

Tip: To check whether the host and the pair management server recognize the P-VOL, S-VOL, and command device, use the `hldutil` command of the Device Manager agent.

Note: The following describes how to perform user authentication for a storage system.

To automatically perform user authentication:

If SSL/TLS communication is used between the Device Manager server and the Device Manager agent, user authentication is automatically performed by using a user account obtained from the Device Manager server.

To manually perform user authentication:

Execute the CCI command (`raidcom -login`) and manually authenticate the user.

Note the following if you manually authenticate the user.

- If the OS of the pair management server is Windows, authenticate the user by using the user that executed the Device Manager agent service (HBsA Service).

- If you authenticate a user for a storage system once, you can access all of the command devices in the same storage system.

- If you change the authentication mode status from disabled to enabled and if there is another host that recognizes the command device, also authenticate the user on that host.

Tip: The default virtual storage machine is a virtual storage machine that satisfies both of the following conditions:

- The model name of the virtual storage machine is the same as the model name of the storage system that the virtual storage machine belongs to.
- The serial number of the virtual storage machine is the same as the serial number of the storage system that the virtual storage machine belongs to.

Caution: When VSP G1000 is used, also check the following conditions:

- To create global-active device copy pairs by using normal volumes (internal volumes or external volumes), the following requirements must also be met:
  - The microcode version of both the primary and secondary storage systems (VSP G1000) must be 80-02-4*X*-*XX*/*XX* or later.

- The version of Device Manager agent must be 8.1.4 or later.

- For a configuration (3DC delta resync configuration) that uses the global-active device and Universal Replicator copy pairs and the Universal Replicator delta resync pairs, the following requirements must also be met:
  - The microcode version of both the primary and secondary storage systems (VSP G1000) must be 80-02-4*X*-*XX*/*XX* or later.
  - The version of Device Manager agent must be 8.1.4 or later.
  - The version of CCI must be 01-32-03/09 or later.
- To perform operations on global-active device pairs by using consistency group IDs, the following requirements must also be met:
  - The microcode version of both the primary and secondary storage systems (VSP G1000) must be 80-02-2*X*-*XX*/*XX* or later.
  - The version of Device Manager agent must be 8.1.2 or later.
  - The version of CCI must be 01-32-03/07 or later.
- When creating global-active device copy pairs in a volume where data is migrated by using the nondisruptive migration functionality, the following requirements must also be satisfied:
  - The microcode version of both the primary and secondary storage systems (VSP G1000) must be 80-02-01-*XX*/*XX* or later.
  - The version of Device Manager agent must be 8.1 or later.
  - Data migration by using the nondisruptive migration functionality is completed.
    Before creating a copy pair, make sure that data migration is completed.

Caution: When VSP G1500 or VSP F1500 is used, also check the following conditions:

- For a configuration (3DC delta resync configuration) that uses the global-active device and Universal Replicator copy pairs and the Universal Replicator delta resync pairs, the version of CCI must be 01-32-03/09 or later.
- To perform operations on global-active device pairs by using consistency group IDs, the version of CCI must be 01-32-03/07 or later.
- When creating global-active device copy pairs in a volume where data is migrated by using the nondisruptive migration functionality, make sure that data migration by using the nondisruptive migration functionality is completed.
  Before creating a copy pair, make sure that data migration is completed.

For details about remote path settings, pair management server settings, quorum disk settings, or virtual storage machines, see the *Hitachi Command Suite User Guide* or *Hitachi Command Suite CLI Reference Guide*.

Related concepts

- Operation workflow for secure communication between a management server and Device Manager agent on page 237

Related references

- Acquiring device information (hldutil command) on page 539
- Properties for command devices connected to Device Manager agent (rgcmddev.properties file) on page 692

Requirements for configuring a high availability system (for VSP Gx00 models)

Configure the management server, pair management server, and storage systems so that the following conditions are satisfied.

Management server conditions:

- The Replication Manager license must be registered.
- The following computers must be registered as the Device Manager management resources:
  - A host that recognizes the P-VOL and the S-VOL
  - The primary site pair management server
  - The secondary site pair management server
  - The primary site storage system
  - The secondary site storage system
  - An external storage system used for quorum disks (When using the Device Manager CLI to configure a high availability system)

Host (application servers) conditions:

- Path management software must be installed.



Note:

- If the host OS is HP-UX 11i v3 and you are using the native multi-pathing features, execute the following command in advance to disable the multi-pathing features for legacy device special files:
  `scsimgr save_attr -a leg_mpath_enable=false`
- When the host OS is Windows or AIX, and MPIO is used, if the microcode version for VSP Gx00 models is 83-03-0*X*-*XX*/*XX* or later, set the host mode option for the host group to `102`.

Storage system conditions (common to the primary and secondary sites):

- The prerequisite software for global-active device must be installed and the license must be enabled.
- The primary site and secondary site storage systems must be connected via two or more Fibre Channels or iSCSI, and a bidirectional remote path must be set between the primary site and secondary site storage systems.
- An external volume for quorum disk must exist on both the primary site and secondary site storage systems, and the same quorum disk ID must be set.
- There must be sufficient space in the storage system's cache and shared memory.

For details about prerequisite software, caches, or shared memory, see the global-active device documentation.

Conditions for external storage systems used for quorum disks

- There must be fibre-channel or iSCSI connections between the primary site storage system and the external storage system used for quorum disks, and between the secondary site storage system and the external storage system used for quorum disks.
- External paths must be set between the external port of the primary site storage system and the port of the external storage system used for quorum disks, and between the port of the secondary site storage system and the port of the external storage system used for quorum disks.

Pair management server conditions (common to the primary and secondary sites):

- Device Manager agent version 8.2.0 or later must be installed on the pair management server.
- CCI version 01-34-03/*XX* or later must be installed on the pair management server.
  For instructions on how to install CCI, see the CCI documentation.
- If there are multiple NICs on the pair management server, the Device Manager agent and CCI must use the same IP address.

Pair volume conditions:

- The P-VOL and S-VOL must be managed by a single management server (Device Manager server).
- The P-VOL and S-VOL must be recognized by the hosts (application servers).

- Both the P-VOL and S-VOL must be open volumes.
- Both the P-VOL and S-VOL must be DP volumes.
- Both the P-VOL and S-VOL must be DP volumes or normal volumes (internal or external volumes).
- The volume types (DP volumes, internal volumes, or external volumes) of the P-VOL and S-VOL are the same.
- The model name and serial number of the virtual storage machine that the P-VOL belongs to must be the same as the model name and serial number of the virtual storage machine that the S-VOL belongs to.

Command device conditions:

- The command device security must not be set.
- Command devices must belong to the default virtual storage machine.
- When managing partitioned resources in the storage system, the host (pair management server) must be connected to the command devices whose storage system resource group ID is 0 (resource pools of the default virtual storage machine), and the information of the command devices is defined in the `rgcmddev.properties` file of the Device Manager agent.
- The authentication mode for the command device is enabled.
- User authentication for the storage system is completed before performing operations on global-active device copy pairs from the Device Manager GUI or CLI.



Tip: To check whether the host and the pair management server recognize the P-VOL, S-VOL, and command device, use the `hldutil` command of the Device Manager agent.



Note: The following describes how to perform user authentication for a storage system.

To automatically perform user authentication:

If SSL/TLS communication is used between the Device Manager server and the Device Manager agent, user authentication is automatically performed by using a user account obtained from the Device Manager server.

To manually perform user authentication:

Execute the CCI command (`raidcom -login`) and manually authenticate the user.

Note the following if you manually authenticate the user.

- If the OS of the pair management server is Windows, authenticate the user by using the user that executed the Device Manager agent service (HBsA Service).

- If you authenticate a user for a storage system once, you can access all of the command devices in the same storage system.

- If you change the authentication mode status from disabled to enabled and if there is another host that recognizes the command device, also authenticate the user on that host.

Tip: The default virtual storage machine is a virtual storage machine that satisfies both of the following conditions:

- The model name of the virtual storage machine is the same as the model name of the storage system that the virtual storage machine belongs to.
- The serial number of the virtual storage machine is the same as the serial number of the storage system that the virtual storage machine belongs to.

Caution: In the following cases, the microcode version of the storage systems of both the primary site and the secondary site (VSP Gx00 models) must be 83-03-0*X*-*XX*/*XX* or later.

- To create global-active device copy pairs by using normal volumes (internal volumes or external volumes)
- To use a configuration (3DC delta resync configuration) that uses the global-active device and Universal Replicator copy pairs and the Universal Replicator delta resync pairs
  In this case, the storage systems of both the primary site and the secondary site must be VSP G800.
- To perform operations on global-active device pairs by using consistency group IDs
- To create global-active device copy pairs in a volume where data is migrated by using the nondisruptive migration functionality
  In this case, make sure that data migration by using the nondisruptive migration functionality is completed, and then create the copy pairs.

For details about remote path settings, pair management server settings, quorum disk settings, or virtual storage machines, see the *Hitachi Command Suite User Guide* or *Hitachi Command Suite CLI Reference Guide*.

Related concepts

- Operation workflow for secure communication between a management server and Device Manager agent on page 237

Related references

- Acquiring device information (hldutil command) on page 539
- Properties for command devices connected to Device Manager agent (rgcmddev.properties file) on page 692

Notes on executing commands

In Windows, if the User Account Control (UAC) function is enabled, you must open a command prompt window as a member of the Administrators group in order to execute commands.

2

Network configuration

This chapter describes the settings for the Hitachi Command Suite products that are required in various network configurations.

- Ports used by Hitachi Command Suite products
- Changing ports used by Common Component
- Registering firewall exceptions for Device Manager and Tiered Storage Manager
- Registering firewall exceptions for Host Data Collector (Windows)
- Network settings with multiple IP addresses
- Device Manager settings in IPv6 environments
- Changing the IP address or host name of the management server
- Changing the URL for accessing Hitachi Command Suite products (hcmds64chgurl command)

Ports used by Hitachi Command Suite products

Avoid specifying port numbers used by other programs installed on the same computer for the port numbers used by Hitachi Command Suite products.

If the same port number is set, either change the setting for the other program or change the setting for the Hitachi Command Suite product.

For details about the port numbers used by Configuration Manager REST API, see the *Hitachi Command Suite Configuration Manager REST API Reference Guide*.

Tip: Some port numbers are part of the port numbers that are temporarily assigned by OSs. If the port numbers used by the Hitachi Command Suite products are set in the `services` file of the OS, the port numbers can be excluded from the port numbers that can be temporarily assigned by the OS.

Ports used by Common Component

For the management server, ensure that the port numbers specified for use by Common Component are different from the port numbers used by other programs installed on the same computer.

Table 10 Ports used by Common Component

Port number	Description
22015/tcp#	Used for accessing the HBase 64 Storage Mgmt Web Service when communicating with management clients (GUI). This port number can be changed.
22016/tcp	Used for accessing the HBase 64 Storage Mgmt Web Service when performing SSL communication with management clients (GUI). This port number can be changed.
22017/tcp to 22030/tcp 22033/tcp 22034/tcp	Reserved by Common Component.
22031/tcp	Used internally for Common Component communication (single sign-on). This port number can be changed.
22032/tcp	Used internally for Common Component communication (HiRDB). This port number can be changed.
22035/tcp 22037/tcp 22038/tcp	Used internally for Common Component communication (communication with the Web server). This port number can be changed.
22036/tcp	Used internally for Common Component communication (naming service).

Port number	Description
	This port number can be changed.
22121/tcp 22123/tcp 22124/tcp	Used by HCS Device Manager Web Service. Used internally for Common Component communication (communication with the Web server). This port number can be changed.
22122/tcp	Used by HCS Device Manager Web Service. Used internally for Common Component communication (naming service). This port number can be changed.
24235/tcp to 24242/tcp	Used when Tuning Manager is installed. This port number can be changed.

#:

This port is also used when SSL is enabled. To interrupt non-SSL communication from outside the network to the management server, you need to edit the `user_httpsd.conf` file.

Related concepts

- Registering firewall exceptions for Device Manager and Tiered Storage Manager on page 121

Related tasks

- Changing ports used by Common Component on page 114
- Editing the user_httpsd.conf file to enable SSL/TLS on page 258

Ports used by the Device Manager server

For the management server, ensure that the port numbers specified for use by the Device Manager server are different from the port numbers used by other programs installed on the same computer.

Table 11 Ports used by the Device Manager server

Port number	Description
162/udp	Used for receiving SNMP traps from storage systems (VSP G1000, G1500, VSP F1500, VSP Gx00 models, VSP Fx00 models, Virtual Storage Platform, Universal Storage Platform V/VM, and HUS VM) and file servers. You cannot change the settings by using Device Manager. If products using these ports are installed on the same computer, change the settings of those products.
427/tcp	Used for communication with a CIM client (service discovery).

Port number	Description
	You cannot change the settings by using Device Manager. If products using these ports are installed on the same computer, change the settings of those products.
2001/tcp#	Used internally for Device Manager server communication, for communication with management clients (via the GUI or the CLI), for communication with storage systems, and for communication with hosts (Device Manager agents and file servers). Note that the Device Manager server cannot start if this port is being used by another product. You can change this port number by modifying the `server.http.port` property in the `server.properties` file of the Device Manager server.
2443/tcp	Used internally for Device Manager server communication, for SSL communication with management clients (via the GUI or the CLI), and for SSL communication with storage systems (VSP G1000, G1500, VSP F1500, VSP Gx00 models, or VSP Fx00 models). You can change this port number by modifying the `server.https.port` property in the `server.properties` file of the Device Manager server.
5983/tcp	Used for receiving event indications from SMI-S providers. You can change this port number by modifying the `server.smisclient.indication.port` property in the `server.properties` file of the Device Manager server.
5988/tcp	Used for non-SSL communication with a CIM client (Object operation). This port number can be changed.
5989/tcp	Used for SSL communication with a CIM client (Object operation). This port number can be changed.
23055/tcp	Used internally for Device Manager server communication. You can change this port number by modifying the `server.rmi.port` property in the `server.properties` file of the Device Manager server.
24230/tcp	Used by HiRDB. You can change this port number by using the `htmsetup` command.
Any/tcp	Used for communication with View Server of Tuning Manager. By default, any free port numbers are used. You might want to change the setting to use a specific port number if, for example, a firewall is set up between the Tuning Manager management server and the Device Manager management server. In such cases, register the port number for the `ownPort` parameter in the `config.xml` and `configforclient.xml` files.

#:

This port is also used when SSL is enabled. If you want to permit only SSL communication, set up a firewall.

Related concepts

- Registering firewall exceptions for Device Manager and Tiered Storage Manager on page 121

Related tasks

- Changing CIM/WBEM port numbers on page 441
- Changing Device Manager server properties on page 590

Related references

- Specifying the settings for remote connection to the Tuning Manager server and the port number (htmsetup command) on page 352
- Setting up the config.xml and configforclient.xml files on page 353
- server.http.port on page 592
- server.https.port on page 593
- server.rmi.port on page 594
- server.smisclient.indication.port on page 601

Ports used by the Tiered Storage Manager server

For the management server, ensure that the port numbers specified for use by the Tiered Storage Manager server are different from the port numbers used by other programs installed on the same computer.

Table 12 Ports used by the Tiered Storage Manager server

Port number	Description
20352/tcp	Used for communication with management clients. You can change the port by modifying the `server.rmi.port` property in the `server.properties` file of the Tiered Storage Manager server.
24500/tcp	Used for SSL communication with management clients. You can change the port by modifying the `server.rmi.security.port` property in the `server.properties` file of the Tiered Storage Manager server.

Related tasks

- Changing Tiered Storage Manager server properties on page 642

Related references

- server.rmi.port on page 644
- server.rmi.security.port on page 644

Ports used by Host Data Collector

For the computer on which Host Data Collector is installed, ensure that the port numbers specified for use by Host Data Collector are different from the port numbers used by other programs installed on the same computer.

Table 13 Ports used by Host Data Collector

Port number	Description
22098/tcp	Used for internal communication by Host Data Collector and for non-SSL communication between the Device Manager server and the RMI registry. You can change the port by using the `hdc.common.rmi.registryPort` property in the `hdcbase.properties` file of Host Data Collector.
22099/tcp	Used for non-SSL communication between the Device Manager server and the RMI server. You can change the port by using the `hdc.common.rmi.serverPort` property in the `hdcbase.properties` file of Host Data Collector.
22100/tcp	Used for non-SSL communication between the Device Manager server and the class loader. You can change the port by using the `hdc.common.http.serverPort` property in the `hdcbase.properties` file of Host Data Collector.
22104/tcp	Used for SSL communication between the Device Manager server and the RMI registry. You can change the port by using the `hdc.common.rmi.ssl.registryPort` property in the `hdcbase.properties` file of Host Data Collector.
22105/tcp	Used for SSL communication between the Device Manager server and the RMI server. You can change the port by using the `hdc.common.rmi.ssl.serverPort` property in the `hdcbase.properties` file of Host Data Collector.
22106/tcp	Used for SSL communication between the Device Manager server and the class loader. You can change the port by using the `hdc.common.https.serverPort` property in the `hdcbase.properties` file of Host Data Collector.
22110/tcp	Used for communication between the Service process and the Adapter process. You can change the port by using the `hdc.service.localport` property in the `hdcbase.properties` file of Host Data Collector.
22111/tcp to 22120/tcp	Used for communication between the Service process and the Adapter process. You can change these ports by using the `hdc.adapter.localport` property in the `hdcbase.properties` file of the Host Data Collector.

Related tasks

- Changing Host Data Collector properties on page 658

Related references

- hdc.service.localport on page 659
- hdc.adapter.localport on page 659
- hdc.common.rmi.registryPort on page 659
- hdc.common.rmi.serverPort on page 660

- hdc.common.http.serverPort on page 660
- hdc.common.rmi.ssl.registryPort on page 661
- hdc.common.rmi.ssl.serverPort on page 661
- hdc.common.https.serverPort on page 662

Ports used by the Device Manager agent

For the computer on which the Device Manager agent is installed, ensure that the port numbers specified for use by the Device Manager agent are different from the port numbers used by other programs installed on the same computer.

Table 14 Ports used by Device Manager agent

Port number	Description
24041/tcp	Used for communication with the Device Manager server. You can change the port by using the `server.agent.port` property in the `server.properties` file of the Device Manager agent.
24042/tcp	Used for communication with the Device Manager server. You can change the port by using the `server.http.port` property in the `server.properties` file of the Device Manager agent.
24043/tcp	Used internally for Device Manager agent communication. You can change the port by using the `server.http.localPort` property in the `server.properties` file of the Device Manager agent.

Related tasks

- Changing Device Manager agent properties on page 670

Related references

- server.agent.port on page 679
- server.http.localPort on page 679
- server.http.port on page 679

Ports used by storage systems

To use Device Manager and Tiered Storage Manager to manage storage systems, you need to provide ports for communication with the management server and management clients (GUI).

Table 15 Ports used by storage systems

Target storage system	Port number	Description
VSP G1000 VSP G1500 VSP F1500 Virtual Storage Platform	80/tcp	Used for communication with management clients (GUI). This port number cannot be changed.
	443/tcp	Used for starting Storage Navigator by SSL from management clients (GUI) .

Target storage system	Port number	Description
		This port number cannot be changed.
	1099/tcp	Used for communication with the management server or management clients (GUI). This port number cannot be changed.
	51099/tcp	Used for communication with the management server or management clients (GUI). This port number cannot be changed.
	51100/tcp	Used for communication with the management server or management clients (GUI). This port number cannot be changed.
VSP Gx00 models (SVP) VSP Fx00 models (SVP)	443/tcp	Used for starting Storage Navigator by SSL from management clients (GUI) . This port number can be changed.
	1099/tcp	Used for communication with the management server or management clients (GUI). This port number can be changed.
	51099/tcp	Used for communication with the management server or management clients (GUI). This port number can be changed.
	51100/tcp	Used for communication with the management server or management clients (GUI). This port number can be changed. If concurrent connections are established from one SVP to multiple storage systems, the number of ports used is the number of the connected storage systems. The range of ports used is from 51100/tcp to 51335/tcp by default. For details on how to confirm the port numbers that are being used by the SVP, see the documentation for VSP Gx00 models or VSP Fx00 models.
VSP Gx00 models (controller) VSP Fx00 models (controller)	443/tcp	Used for starting the maintenance utility by SSL from management clients (GUI) . This port number cannot be changed.
Universal Storage Platform V/VM	80/tcp	Used for communication with management clients (GUI). This port number cannot be changed.
	443/tcp	Used for starting Element Manager by SSL from management clients (GUI) . This port number cannot be changed.
	1099/tcp	Used for communication with the management server or management clients (GUI).

Target storage system	Port number	Description
		This port number cannot be changed.
	51099/tcp	Used for communication with the management server or management clients (GUI). This port number cannot be changed.
	51100/tcp	Used for communication with the management server or management clients (GUI). This port number cannot be changed.
HUS VM	80/tcp	Used for communication with management clients (GUI). This port number cannot be changed.
	443/tcp	Used for starting Element Manager by SSL. This port number cannot be changed.
	1099/tcp	Used for communication with management clients (GUI). This port number cannot be changed.
	51099/tcp	Used for communication with the management server. This port number cannot be changed.
	51100/tcp	Used for communication with the management server. This port number cannot be changed.
Hitachi AMS/WMS	2000/tcp	Used for communication with the management server. This port number can be changed.
	28355/tcp	Used for communication with the management server. This port number can be changed.
Hitachi AMS2000	2000/tcp	Used for non-SSL communication with the management server. This port number can be changed.
	28355/tcp	Used for SSL communication with the management server. This port number can be changed.
Hitachi SMS	2000/tcp	Used for non-SSL communication with the management server. This port number can be changed.
	28355/tcp	Used for SSL communication with the management server. This port number can be changed.
HUS100	2000/tcp	Used for non-SSL communication with the management server.

Target storage system	Port number	Description
		This port number can be changed.
	28355/tcp	Used for SSL communication with the management server. This port number can be changed.

If you changed the port number to be used by VSP Gx00 models (SVP) or VSP Fx00 models (SVP), you need to specify the following settings in Device Manager:

- Revise the registered firewall exceptions.
- Set the new port number for Device Manager.
  If you changed 1099/tcp, use the Edit Storage Systems window of the Device Manager GUI or the `AddStorageArray` command of the Device Manager CLI to set the new port number. If you changed 443/tcp, use the Device Manager GUI or CLI to refresh storage systems.

If you change the port number (2000/tcp or 28355/tcp) used by a midrange storage system (HUS100, Hitachi SMS, Hitachi AMS2000, or Hitachi AMS/WMS), you need to specify the new port number in the `services` file of the management server OS. If you operate the midrange storage system without doing so, an error (code: DMEA000006) occurs and operations might fail.

For communication between midrange storage systems and the management server (Device Manager server), use the same port number for each communication protocol (SSL and non-SSL) to be used. If communication is between midrange storage systems that have different port numbers, an error might occur if a midrange storage system uses a port number that is different from the one specified in the `services` file of the management server. In addition, even if the midrange storage systems use the same port numbers as the ones specified in the `services` file, an error will not occur but the operation might take a long time.

For details on how to change a port number and how to set the `services` file, see the manual of each storage system.

Changing ports used by Common Component

To change the ports used by Common Component after installing the Hitachi Command Suite products, you need to edit the settings file for Common Component.

Procedure

1. Stop the services of Hitachi Command Suite products.
2. Edit the Common Component settings files and change the port number.

Table 16 Port number settings files for Common Component

Default port number	Settings files	Location
22015/tcp	**In Windows:** *installation-folder-for-Hitachi-Command-Suite*\Base64\uCPSB\httpsd\conf\user_httpsd.conf[#1] **In Linux:** *installation-directory-for-Hitachi-Command-Suite*/Base64/uCPSB/httpsd/conf/user_httpsd.conf[#1]	Listen
22016/tcp	**In Windows:** *installation-folder-for-Hitachi-Command-Suite*\Base64\uCPSB\httpsd\conf\user_httpsd.conf[#1] **In Linux:** *installation-directory-for-Hitachi-Command-Suite*/Base64/uCPSB/httpsd/conf/user_httpsd.conf[#1]	• VirtualHost *host-name*:*port-number* • Listen[#2]
22031/tcp	**In Windows:** *installation-folder-for-Hitachi-Command-Suite*\Base64\uCPSB\httpsd\conf\user_hsso_httpsd.conf **In Linux:** *installation-directory-for-Hitachi-Command-Suite*/Base64/uCPSB/httpsd/conf/user_hsso_httpsd.conf	Listen 127.0.0.1:*port-number*
22032/tcp	**In Windows:** *installation-folder-for-Hitachi-Command-Suite*\Base64\HDB\CONF\emb\HiRDB.ini **In Linux:** *installation-directory-for-Hitachi-Command-Suite*/Base64/HDB/conf/emb/HiRDB.ini	PDNAMEPORT
	In Windows:	pd_name_port

Default port number	Settings files	Location
	installation-folder-for-Hitachi-Command-Suite\Base64\HDB\CONF\pdsys **In Linux:** *installation-directory-for-Hitachi-Command-Suite*/Base64/HDB/conf/pdsys	
	In Windows: *installation-folder-for-Hitachi-Command-Suite*\Base64\database\work\def_pdsys **In Linux:** *installation-directory-for-Hitachi-Command-Suite*/Base64/database/work/def_pdsys	pd_name_port
22035/tcp	**In Windows:** *installation-folder-for-Hitachi-Command-Suite*\Base64\uCPSB\CC\web\redirector\workers.properties **In Linux:** *installation-directory-for-Hitachi-Command-Suite*/Base64/uCPSB/CC/web/redirector/workers.properties	worker.HBase64StgMgmtSSOService.port
	In Windows: *installation-folder-for-Hitachi-Command-Suite*\Base64\uCPSB\CC\server\usrconf\ejb\HBase64StgMgmtSSOService\usrconf.properties **In Linux:** *installation-directory-for-Hitachi-Command-Suite*/Base64/uCPSB/CC/server/usrconf/ejb/HBase64StgMgmtSSOService/usrconf.properties	webserver.connector.ajp13.port
22036/tcp	**In Windows:** *installation-folder-for-Hitachi-Command-Suite*	ejbserver.rmi.naming.port

Default port number	Settings files	Location
	\Base64\uCPSB\CC\server \usrconf\ejb \HBase64StgMgmtSSOService \usrconf.properties **In Linux:** *installation-directory-for-Hitachi-Command-Suite*/Base64/uCPSB/CC/server/usrconf/ejb/HBase64StgMgmtSSOService/usrconf.properties	
22037/tcp	**In Windows:** *installation-folder-for-Hitachi-Command-Suite* \Base64\uCPSB\CC\server \usrconf\ejb \HBase64StgMgmtSSOService \usrconf.properties **In Linux:** *installation-directory-for-Hitachi-Command-Suite*/Base64/uCPSB/CC/server/usrconf/ejb/HBase64StgMgmtSSOService/usrconf.properties	ejbserver.http.port
22038/tcp	**In Windows:** *installation-folder-for-Hitachi-Command-Suite* \Base64\uCPSB\CC\server \usrconf\ejb \HBase64StgMgmtSSOService \usrconf.properties **In Linux:** *installation-directory-for-Hitachi-Command-Suite*/Base64/uCPSB/CC/server/usrconf/ejb/HBase64StgMgmtSSOService/usrconf.properties	ejbserver.rmi.remote.listener.port
22121/tcp	**In Windows:** *installation-folder-for-Hitachi-Command-Suite* \Base64\uCPSB\CC\web \redirector\workers.properties **In Linux:** *installation-directory-for-Hitachi-Command-Suite*/Base64/	worker.DeviceManagerWebService.port

Default port number	Settings files	Location
	uCPSB/CC/web/redirector/ workers.properties	
	In Windows: *installation-folder-for-Hitachi-Command-Suite* \Base64\uCPSB\CC\server \usrconf\ejb \DeviceManagerWebService \usrconf.properties **In Linux:** *installation-directory-for-Hitachi-Command-Suite*/Base64/ uCPSB/CC/server/usrconf/ejb/ DeviceManagerWebService/ usrconf.properties	webserver.connector.ajp13.port
22122/tcp	**In Windows:** *installation-folder-for-Hitachi-Command-Suite* \Base64\uCPSB\CC\server \usrconf\ejb \DeviceManagerWebService \usrconf.properties **In Linux:** *installation-directory-for-Hitachi-Command-Suite*/Base64/ uCPSB/CC/server/usrconf/ejb/ DeviceManagerWebService/ usrconf.properties	ejbserver.rmi.naming.port
22123/tcp	**In Windows:** *installation-folder-for-Hitachi-Command-Suite* \Base64\uCPSB\CC\server \usrconf\ejb \DeviceManagerWebService \usrconf.properties **In Linux:** *installation-directory-for-Hitachi-Command-Suite*/Base64/ uCPSB/CC/server/usrconf/ejb/ DeviceManagerWebService/ usrconf.properties	ejbserver.http.port
22124/tcp	**In Windows:**	ejbserver.rmi.remote.listener.port

Default port number	Settings files	Location
	installation-folder-for-Hitachi-Command-Suite\Base64\uCPSB\CC\server\usrconf\ejb\DeviceManagerWebService\usrconf.properties **In Linux:** *installation-directory-for-Hitachi-Command-Suite*/Base64/uCPSB/CC/server/usrconf/ejb/DeviceManagerWebService/usrconf.properties	

#1:

Do not edit the `httpsd.conf` file.

#2:

If SSL is enabled, to interrupt non-SSL communication from outside the network to the management server, you need to edit the line `Listen 22015` in the `user_httpsd.conf` file.

Note: Do not use the following port numbers:

1, 7, 9, 11, 13, 15, 17, 19, 20, 21, 22, 23, 25, 37, 42, 43, 53, 77, 79, 87, 95, 101, 102, 103, 104, 109, 110, 111, 113, 115, 117, 119, 123, 135, 139, 143, 179, 389, 465, 512, 513, 514, 515, 526, 530, 531, 532, 540, 556, 563, 587, 601, 636, 993, 995, 2049, 4045, 6000

3. Start the services of the Hitachi Command Suite products.
4. If you change the following port numbers, you need to change the URLs of all Hitachi Command Suite products that are installed on the management server:
   - 22015/tcp (used for accessing HBase 64 Storage Mgmt Web Service)
     You need to change the URLs if you use non-SSL for communication between the management server and management clients.
   - 22016/tcp (used for accessing SSL HBase 64 Storage Mgmt Web Service)
     You need to change the URLs if you use SSL for communication between the management server and management clients.

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.

Next steps

If you change the port numbers for Common Component, you might have to review the following settings depending on the operating environment:

- If Element Manager is used to operate a Hitachi AMS/WMS storage system (23015/tcp and 23016/tcp):
  You need to use launchapptool to modify the URL settings for Storage Navigator Modular 2.
- If performance information is acquired from Tuning Manager (22015/tcp and 22016/tcp):
  If the Tuning Manager server is installed on the same server, revise the `htnm.server.n.port` property settings.
- If Hitachi Data Ingestor or Hitachi NAS Platform F is registered on Device Manager as the management-target host:
  You need to report the file server configuration information to the Device Manager server.
  On the Edit HDvM Settings dialog box for Hitachi File Services Manager, select Yes for the Send information when the system is refreshed check box, and then click OK. Then in the Processing Nodes window, click the Refresh Processing Node button.
  For details on how to specify settings for Hitachi File Services Manager, see the Documentation for Hitachi Data Ingestor or Hitachi NAS Platform F.

Related tasks

- Changing the URL for accessing Hitachi Command Suite products (hcmds64chgurl command) on page 154
- Editing the user_httpsd.conf file to enable SSL/TLS on page 258
- Changing pop-up blocker settings on page 293
- Settings for using Element Manager on page 333
- Starting the Hitachi Command Suite services on page 458
- Stopping the Hitachi Command Suite services on page 460
- Changing Device Manager server properties on page 590

Related references

- Ports used by Common Component on page 106
- htnm.server.n.port on page 632

Registering firewall exceptions for Device Manager and Tiered Storage Manager

When the ports or processes used by Hitachi Command Suite products are registered as firewall exceptions, connection to the registered ports or processes from outside the network is permitted.

Note: If one of the following conditions exists, the user must manually register the ports used by the management server as firewall exceptions after installation of Hitachi Command Suite: The Windows firewall is enabled after operation starts, the management server OS is Linux, or a firewall is set up in the network connected to the management server.

- In Windows:
  Add all the components that make up Hitachi Command Suite to the firewall exceptions list.
- In Linux:
  Add all the port numbers used by Hitachi Command Suite to the firewall exceptions list.

Port numbers that must be registered as firewall exceptions for Device Manager and Tiered Storage Manager

In an environment with firewalls set up in the network that connects the management server, management clients, and storage systems, you need to register ports used by Hitachi Command Suite products as firewall exceptions.

- Table 17 Port numbers that must be registered as firewall exceptions between the management server and management clients on page 122
- Table 18 Port numbers that must be registered as firewall exceptions between the management server and storage systems on page 123
- Table 19 Port numbers that must be registered as firewall exceptions between the management client and storage systems on page 127
- Table 20 Port numbers that must be registered as firewall exceptions between the management server and a host on page 130
- Table 21 Port numbers that must be registered as firewall exceptions between the management server and a virtualization server on page 131
- Table 22 Port number that must be registered as an exception to a firewall between the management server and a mainframe host on page 131
- Table 23 Port number that must be registered as an exception to a firewall if a file server or NAS module is used on page 131

- Table 24 Port numbers that must be registered as firewall exceptions between the Device Manager management server and the Tuning Manager management server on page 132
- Table 25 Port number that must be registered as a firewall exception between the management server and the Host Data Collector computer on page 133
- Table 26 Port number that must be registered as a firewall exception between the Host Data Collector computer and a host on page 134
- Table 27 Port numbers that must be registered as firewall exceptions between the management server and an SMI-S provider on page 134
- Table 28 Port numbers that must be registered as firewall exceptions between the management server and a CIM client on page 135
- Table 29 Port numbers that must be registered as firewall exceptions between the management server and a mail server on page 136
- Table 30 Port numbers that must be registered as firewall exceptions between the management server and an external authentication server on page 137
- Table 31 Port numbers that must be registered as firewall exceptions when you manage copy pairs by using the pair management server on page 137

Table 17 Port numbers that must be registered as firewall exceptions between the management server and management clients

Originator		Destination		Remarks
Port number	Machine	Port number	Machine	
any/tcp	Management client (GUI or Device Manager CLI)	2001/tcp#	Management server	This setting is required when non-SSL communication is used.
any/tcp	Management client (GUI or Device Manager CLI)	2443/tcp#	Management server	This setting is required when SSL communication is used.
any/tcp	Management client (Tiered Storage Manager CLI)	20352/tcp#	Management server	This setting is required when non-SSL communication is used.
any/tcp	Management client (GUI)	22015/tcp#	Management server	This setting is required when non-SSL communication is used.

Originator		Destination		Remarks
Port number	Machine	Port number	Machine	
any/tcp	Management client (GUI)	22016/tcp#	Management server	This setting is required when SSL communication is used.
any/tcp	Management client (Tiered Storage Manager CLI)	24500/tcp#	Management server	This setting is required when SSL communication is used.

#:

This port number can be changed.

Table 18 Port numbers that must be registered as firewall exceptions between the management server and storage systems

Originator		Destination		Remarks
Port number	Machine	Port number	Machine	
any/udp	• VSP G1000 • VSP G1500 • VSP F1500 • VSP Gx00 models (controller) • VSP Fx00 models (controller) • Virtual Storage Platform • Universal Storage Platform V/VM • HUS VM	162/udp	Management server	-
any/tcp	Management server	443/tcp#1	• VSP G1000 • VSP G1500 • VSP F1500 • VSP Gx00 models (SVP) • VSP Fx00 models (SVP)	-

Originator		Destination		Remarks
Port number	Machine	Port number	Machine	
			• Virtual Storage Platform • HUS VM	
any/tcp	Management server	1099/tcp[#1]	• VSP G1000 • VSP G1500 • VSP F1500 • VSP Gx00 models (SVP) • VSP Fx00 models (SVP) • Virtual Storage Platform • Universal Storage Platform V/VM • HUS VM	-
any/tcp	Management server	2000/tcp[#2]	• Hitachi AMS/WMS	-
any/tcp	Management server	2000/tcp[#2]	• HUS100 • Hitachi SMS • Hitachi AMS2000	This setting is required when non-SSL communication is used.
any/tcp	Universal Storage Platform V/VM	2001/tcp[#2]	Management server	Set up the firewall so that communication can be established from any port of the storage system to the 2001/tcp port of the management server.
any/tcp	• VSP G1000 • VSP G1500 • VSP F1500 • VSP Gx00 models (SVP) • VSP Fx00 models (SVP)	2443/tcp[#2]	Management server	For VSP G1000, G1500, or VSP F1500, this setting is required when user accounts are authenticated in Hitachi Command Suite when logging in to CCI or the SVP.

Originator		Destination		Remarks
Port number	Machine	Port number	Machine	
any/tcp	Management server	8443/tcp	• VSP G400, G600, G800 (controller) in which a NAS Module is included • VSP F400, F600, F800 (controller) in which a NAS Module is included	This setting is required when the internal NAS Manager[#3] is used.
any/tcp	Management server	20443/tcp	• VSP G400, G600, G800 (controller) in which a NAS Module is included • VSP F400, F600, F800 (controller) in which a NAS Module is included	This setting is required when the internal NAS Manager[#3] is used.
any/tcp	Management server	28355/tcp[#2]	• HUS100 • Hitachi SMS • Hitachi AMS2000	This setting is required when SSL communication is used.
any/tcp	Management server	51099/tcp[#1]	• VSP G1000 • VSP G1500 • VSP F1500 • VSP Gx00 models (SVP) • VSP Fx00 models (SVP) • Virtual Storage Platform • Universal Storage Platform V/VM	-

Originator		Destination		Remarks
Port number	Machine	Port number	Machine	
			• HUS VM	
any/tcp	Management server	51100/tcp	• Universal Storage Platform V/VM	This setting is required when you perform an upgrade installation to a Device Manager server version 6.0.0-00 or later.
any/tcp	Management server	51100/tcp[#1]	• VSP G1000 • VSP G1500 • VSP F1500 • VSP Gx00 models (SVP) • VSP Fx00 models (SVP) • Virtual Storage Platform	If the communication-destination storage system is VSP Gx00 models or VSP Fx00 models, when concurrent connections are established from one SVP to multiple storage systems, the number of ports used is the number of the connected storage systems. For this reason, this setting is required for all the ports used. The range of ports used is from 51100/tcp to 51335/tcp by default. For details on how to confirm the port numbers that are being used by the SVP, see the documentation for VSP Gx00 models or VSP Fx00 models.

Legend:

-: Not applicable

#1:

For VSP Gx00 models (SVP) or VSP Fx00 models (SVP), you can change the port number.

#2:

This port number can be changed.

#3:

This refers to a NAS Manager that exists on a storage system that has a built-in NAS Module.

Table 19 Port numbers that must be registered as firewall exceptions between the management client and storage systems

Originator		Destination		Remarks
Port number	Machine	Port number	Machine	
any/tcp	Management client (GUI)	80/tcp	• VSP G1000 • VSP G1500 • VSP F1500 • Virtual Storage Platform • Universal Storage Platform V/VM • HUS VM	-
any/tcp	Management client (GUI)	443/tcp[#1]	• VSP G1000 • VSP G1500 • VSP F1500 • VSP Gx00 models (SVP and controller) • VSP Fx00 models (SVP and controller) • Virtual Storage Platform • Universal Storage Platform V/VM • HUS VM	This setting is required when using SSL for Storage Navigator.
any/tcp	Management client (GUI)	1099/tcp[#1]	• VSP G1000 • VSP G1500 • VSP F1500 • VSP Gx00 models (SVP) • VSP Fx00 models (SVP) • Virtual Storage Platform	-

Originator		Destination		Remarks
Port number	Machine	Port number	Machine	
			• Universal Storage Platform V/VM • HUS VM	
any/tcp	Management client (GUI)	20443/tcp	• VSP G400, G600, G800 (controller) in which a NAS Module is included • VSP F400, F600, F800 (controller) in which a NAS Module is included	This setting is required when using the internal NAS Manager#2.
any/tcp	Management client (GUI)	51099/tcp#	• VSP G1000 • VSP G1500 • VSP F1500 • VSP Gx00 models (SVP) • VSP Fx00 models (SVP) • Virtual Storage Platform • Universal Storage Platform V/VM • HUS VM	-
any/tcp	Management client (GUI)	51100/tcp#	• VSP G1000 • VSP G1500 • VSP F1500 • VSP Gx00 models (SVP) • VSP Fx00 models (SVP) • Virtual Storage Platform	If the communication-destination storage system is VSP Gx00 models or VSP Fx00 models, when concurrent connections are established from one SVP to multiple storage systems, the number of ports used is the number of the connected storage systems. For this reason, this setting is required for all the ports used. The range of ports used is from 51100/tcp to

Originator		Destination		Remarks
Port number	Machine	Port number	Machine	
			• Universal Storage Platform V/VM • HUS VM	51335/tcp by default. For details on how to confirm the port numbers that are being used by the SVP, see the documentation for VSP Gx00 models or VSP Fx00 models.
any/tcp	Management client (GUI)	161/udp	• VSP G1000 • VSP G1500 • VSP F1500 • VSP Gx00 models (controller) • VSP Fx00 models (controller)	This setting is required when using the management client as an SNMP manager.
any/tcp	Management client (GUI)	427/tcp	• VSP G1000 • VSP G1500 • VSP F1500 • VSP Gx00 models (SVP) • VSP Fx00 models (SVP)	This setting is required when using SMI-S.
any/tcp	Management client (GUI)	5443/tcp	• VSP G1000 • VSP G1500 • VSP F1500	This setting is required when the `raidinf` command is used in SSL communication.
any/tcp	Management client (GUI)	5989/tcp	• VSP G1000 • VSP G1500 • VSP F1500 • VSP Gx00 models (SVP) • VSP Fx00 models (SVP)	This setting is required when using SMI-S.
any/tcp	• VSP G1000 • VSP G1500 • VSP F1500	162/udp	Management client (GUI)	This setting is required when using the management client as an SNMP manager.

Originator		Destination		Remarks
Port number	Machine	Port number	Machine	

Legend:

-: Not applicable

#1:

For VSP Gx00 models (SVP) or VSP Fx00 models (SVP), you can change the port number.

#2:

This refers to a NAS Manager that exists on a storage system that has a built-in NAS Module.

Table 20 Port numbers that must be registered as firewall exceptions between the management server and a host

Originator		Destination		Remarks
Port number	Machine	Port number	Machine	
any/tcp	• Normal host • Virtual machine	2001/tcp#	Management server	-
any/tcp	Management server	24041/tcp#	• Normal host • Virtual machine	-
any/tcp	Management server	24042/tcp#	• Normal host • Virtual machine	-

Legend:

-: Not applicable

#:

This port number can be changed.

Table 21 Port numbers that must be registered as firewall exceptions between the management server and a virtualization server

Originator		Destination		Remarks
Port number	Machine	Port number	Machine	
any/tcp	Management server	443/tcp	• VMware ESXi • VMware vCenter Server that manages VMware ESXi	This setting is required when a virtual WWN is assigned to a virtual machine by using NPIV.
any/tcp	Management server	5988/tcp	VMware ESXi	This setting is required for non-SSL communication.
any/tcp	Management server	5989/tcp	VMware ESXi	This setting is required for SSL communication.

Table 22 Port number that must be registered as an exception to a firewall between the management server and a mainframe host

Originator		Destination		Remarks
Port number	Machine	Port number	Machine	
any/tcp	Management server	24042/tcp#	Mainframe host	-

Legend:

-: Not applicable

#:

This port number can be changed.

Table 23 Port number that must be registered as an exception to a firewall if a file server or NAS module is used

Originator		Destination		Remarks
Port number	Machine	Port number	Machine	
any/tcp	Management client (GUI)	443/tcp	External NAS Manager#1	-
any/tcp	• Hitachi Data Ingestor • NAS Platform	2001/tcp#2	Management server	-

Originator		Destination		Remarks
Port number	Machine	Port number	Machine	
	• Hitachi NAS Platform F			
any/tcp	External NAS Manager#1	2001/tcp#2	Management server	-
any/tcp	Management server	8443/tcp	NAS Platform	This setting is required for firmware versions 10.2.3071 and later of NAS Platform.

Legend:

-: Not applicable

#:1

This is a NAS Manager that exists separately from the storage system.

#:2

This port number can be changed.

Table 24 Port numbers that must be registered as firewall exceptions between the Device Manager management server and the Tuning Manager management server

Originator		Destination		Remarks
Port number	Machine	Port number	Machine	
any/tcp	Device Manager management server	22286/tcp#1	Tuning Manager management server	This setting is required for acquiring performance information such as parity group usage rate and volume IOPS from a remotely connected Tuning Manager.
any/tcp	Device Manager management server	22900/tcp to 22999/tcp	Tuning Manager management server	This setting is required for remotely connecting to Tuning Manager.
any/tcp	Tuning Manager management server	22015/tcp#1	Device Manager management server	This setting is required for remotely connecting to Tuning Manager.
any/tcp	Tuning Manager management server	24230/tcp#2	Device Manager management server	This setting is required for remotely connecting to Tuning Manager.
any/tcp	Tuning Manager management server	1024/tcp to 65535/tcp#3	Device Manager management server	This setting is required for acquiring performance information such as parity group usage rate and volume IOPS from a

Originator		Destination		Remarks
Port number	Machine	Port number	Machine	
				remotely connected Tuning Manager.

#1:

This port number can be changed.

#2:

This port number can be changed to one in the range from 5001 to 65535.

#3:

This port number is used for communication between Device Manager and View Server of Tuning Manager. Register the port number set for the `ownPort` parameter in the `config.xml` file and the `configforclient.xml` file.

Table 25 Port number that must be registered as a firewall exception between the management server and the Host Data Collector computer

Originator		Destination		Remarks
Port number	Machine	Port number	Machine	
any/tcp	Management server	22098/tcp#	Host Data Collector computer	This setting is required when all the following conditions exist: • Host Data Collector is installed on a computer other than the management server. • Non-SSL communication is used.
any/tcp	Management server	22099/tcp#	Host Data Collector computer	
any/tcp	Management server	22100/tcp#	Host Data Collector computer	
any/tcp	Management server	22104/tcp#	Host Data Collector computer	This setting is required when all the following conditions exist: • Host Data Collector is installed on a computer other than the management server. • SSL communication is used.
any/tcp	Management server	22105/tcp#	Host Data Collector computer	
any/tcp	Management server	22106/tcp#	Host Data Collector computer	

#:

This port number can be changed.

Table 26 Port number that must be registered as a firewall exception between the Host Data Collector computer and a host

Originator		Destination		Remarks
Port number	Machine	Port number	Machine	
any/tcp	Host Data Collector computer	22/tcp[#]	Normal host	This setting is required when the OS of the management-target normal host is UNIX.
any/tcp	Host Data Collector computer	80/tcp	• VMware ESXi • VMware vCenter Server that manages VMware ESXi	This setting is required when non-SSL communication with a management-target virtualization server is used.
any/tcp	Host Data Collector computer	135/tcp	Normal host	This setting is required when the OS of the management-target normal host is Windows.
any/tcp	Host Data Collector computer	139/tcp	Normal host	This setting is required when the OS of the management-target normal host is Windows.
any/tcp	Host Data Collector computer	443/tcp	• VMware ESXi • VMware vCenter Server that manages VMware ESXi	This setting is required when SSL communication with a management-target virtualization server is used.
any/tcp	Host Data Collector computer	445/tcp	Normal host	This setting is required when the OS of the management-target normal host is Windows.
any/udp	Host Data Collector computer	445/udp	Normal host	This setting is required when the OS of the management-target normal host is Windows.

#:

This port number can be changed.

Table 27 Port numbers that must be registered as firewall exceptions between the management server and an SMI-S provider

Originator		Destination		Remarks
Port number	Machine	Port number	Machine	
any/tcp	SMI-S provider	5983/tcp[#]	Management server	-

Originator		Destination		Remarks
Port number	Machine	Port number	Machine	
any/tcp	Management server	5988/tcp#	SMI-S provider	This setting is required when non-SSL communication is used.
any/tcp	Management server	5989/tcp#	SMI-S provider	This setting is required when SSL communication is used.

Legend:

-: Not applicable

#:

This port number can be changed.

Table 28 Port numbers that must be registered as firewall exceptions between the management server and a CIM client

Originator		Destination		Remarks
Port number	Machine	Port number	Machine	
any/tcp	CIM client	427/tcp	Management server	-
any/tcp	CIM client	5988/tcp#	Management server	This setting is required when non-SSL communication is used.
any/tcp	CIM client	5989/tcp#	Management server	This setting is required when SSL communication is used.

Legend:

-: Not applicable

#:

This port number can be changed.

Table 29 Port numbers that must be registered as firewall exceptions between the management server and a mail server

Originator		Destination		Remarks
Port number	Machine	Port number	Machine	
any/tcp	Management server (Device Manager server)	25/tcp[#1]	Mail server[#2]	This setting is required to send an email to a user when the following events occur: • An alert occurs in a storage system. • A task executed from the Migrate Data wizard completes.
any/tcp	Management server (Tiered Storage Manager server)	25/tcp[#1]	Mail server[#3]	This setting is required to send an email to a user when the following events occur: • A task executed from the Tiered Storage Manager CLI ends. • A volume lock period expires. • The period specified for a migration group elapses.
any/tcp	Management server (Storage Navigator Modular 2)	25/tcp	Mail server[#4]	This setting is required to use the Storage Navigator Modular 2 function that reports email errors for operation of a Hitachi AMS/WMS storage system.

#1:

This port number can be changed.

#2:

This is the mail server specified for the `server.mail.smtp.host` property of the Device Manager server.

#3:

This is the mail server specified for the `server.mail.smtp.host` property of the Tiered Storage Manager.

#4:

This is a mail server configured to send error information for the storage systems by using Storage Navigator Modular 2.

Table 30 Port numbers that must be registered as firewall exceptions between the management server and an external authentication server

Originator		Destination		Remarks
Port number	Machine	Port number	Machine	
any/tcp	Management server	88/tcp#	Kerberos server	-
any/tcp	Management server	88/udp#	Kerberos server	-
any/tcp	Management server	359/tcp#	LDAP directory server	-
any/tcp	Management server	1812/udp#	RADIUS server	-

Legend:

-: Not applicable

#:

This port number is generally used. However, a different port number might be used for an external authentication server.

Table 31 Port numbers that must be registered as firewall exceptions when you manage copy pairs by using the pair management server

Originator		Destination		Remarks
Port number	Machine	Port number	Machine	
any/udp	• Normal host • Virtual machine	31001/udp	• VSP G1000 • VSP G1500 • VSP F1500 • VSP Gx00 models • VSP Fx00 models • Virtual Storage Platform • HUS VM	-

Legend:

-: Not applicable

Related tasks

- Registering firewall exceptions for Device Manager and Tiered Storage Manager in Windows on page 138
- Registering firewall exceptions for Device Manager and Tiered Storage Manager in Red Hat Enterprise Linux 5 or Red Hat Enterprise Linux 6 on page 139
- Registering firewall exceptions for Device Manager and Tiered Storage Manager in SUSE Linux Enterprise Server on page 140

Related references

- Setting up the config.xml and configforclient.xml files on page 353

Registering firewall exceptions for Device Manager and Tiered Storage Manager in Windows

To add the components that make up Hitachi Command Suite to the firewall exceptions list, execute the `hcmds64fwcancel` and netsh commands.

Procedure

1. Execute the following command to add the Hitachi Command Suite Common Web Service to the exceptions list:

   installation-folder-for-Hitachi-Command-Suite`\Base64\bin\hcmds64fwcancel`

2. Execute the following command to add the other components that make up Hitachi Command Suite to the exceptions list.

   `netsh advfirewall firewall add rule name="`*name-added-to-exceptions-list*`" dir=in action=allow program="`*path*`" description="`*path*`" enable=yes`

Table 32 Names added to the exceptions list and paths specified with the netsh command

Component	Name added to the exceptions list	Path
Device Manager server	Device Manager	*installation-folder-for-Hitachi-Command-Suite*`\DeviceManager\HiCommandServer\HiCommandServer.exe`
Tiered Storage Manager server	Tiered Storage Manager(htsmService)	*installation-folder-for-Hitachi-Command-Suite*`\TieredStorageManager\bin\htsmService.exe`
JDK	Device Manager - HBase64(java)	*installation-folder-for-Hitachi-Command-Suite*`\Base64\uCPSB\hjdk\jdk\jre\bin\java.exe`#
	Tiered Storage Manager - HBase64(java)	*installation-folder-for-Hitachi-Command-Suite*`\Base64\uCPSB\hjdk\jdk\bin\java.exe`#

#

If you want to use a JDK other than the one that comes with Hitachi Command Suite, specify the absolute path to the `java.exe` in the installation folder of the JDK you will use.

3. To enable the settings, restart the Hitachi Command Suite product services.

Related tasks

- Starting the Hitachi Command Suite services on page 458
- Stopping the Hitachi Command Suite services on page 460

Related references

- Port numbers that must be registered as firewall exceptions for Device Manager and Tiered Storage Manager on page 121

Registering firewall exceptions for Device Manager and Tiered Storage Manager in Red Hat Enterprise Linux 5 or Red Hat Enterprise Linux 6

To add the port numbers used by Hitachi Command Suite to the firewall exceptions list, use the text mode setup utility.

Procedure

1. In a terminal window, execute the `setup` command.

   The Choose a Tool window of the text mode setup utility is displayed.
2. Select **Firewall configuration**, use the **Tab** key to move to the **Run Tool** button, and then press **Enter**.

   The Firewall Configuration window is displayed.
3. Set **Security Level** to **Enabled** by pressing the space key to select Enabled, use the **Tab** key to move to the **Customize** button, and then press **Enter**.

   The Firewall Configuration - Customize window is displayed.
4. In **Other ports** specify the port to be registered as an exception, use the **Tab** key to move to the **OK** button, and then press **Enter**.

   Example: **Other ports** `162:udp 2001:tcp 2443:tcp 22015:tcp`

   Note: If a port is already specified, use a space to separate it from the newly added entry.

5. After returning to the Firewall Configuration window, check that **Security Level** is **Enabled**, use the **Tab** key to move to the **OK** button, and then press **Enter**.

Related references

- Port numbers that must be registered as firewall exceptions for Device Manager and Tiered Storage Manager on page 121

Registering firewall exceptions for Device Manager and Tiered Storage Manager in Red Hat Enterprise Linux 7 or Oracle Linux 7

Specify the port numbers used by Hitachi Command Suite for the ports which the zones are applied to by using the `firewall-cmd` command, a management command of the `firewalld` service:

Procedure

1. Specify the service name that is to be enabled to the ports which the zones are applied to.

   The following shows an example of specifying the service name for the default zone and keeping the setting enabled even after the OS restarts:

   `firewall-cmd --permanent --add-service=`*service-name*

   - *service-name*
     Specify `http` for non-SSL communication, and `https` for SSL communication.

2. For the port to which the zones are applied, specify the port numbers used by Hitachi Command Suite as the port numbers through which communication is allowed for the zones applied to each port, and the combination of that port number and the protocol.

   The following shows an example of specifying the combination of a port number and the protocol for the default zone and keeping the setting enabled even after the OS restarts:

   `firewall-cmd --permanent --add-port=`*port-number*/*protocol*

   - *port-number*
     Specify the port number to be used in Hitachi Command Suite.
   - *protocol*
     Specify *tcp* or *udp*.

Related references

- Port numbers that must be registered as firewall exceptions for Device Manager and Tiered Storage Manager on page 121

Registering firewall exceptions for Device Manager and Tiered Storage Manager in SUSE Linux Enterprise Server

To add the port numbers used by Hitachi Command Suite to the firewall exceptions list, edit the `SuSEfirewall2` file.

Procedure

1. Edit the `/etc/sysconfig/SuSEfirewall2` file to specify the port to be registered as an exception.

   Specify the port numbers to be registered as exceptions, in the following format:

   - `FW_SERVICES_EXT_TCP="`*TCP-port-number*`"`
   - `FW_SERVICES_EXT_UDP="`*UDP-port-number*`"`

   In the following example, only 2001, 2443, 22015, 22016, 161, and 162 are registered as exceptions:

   ```
   FW_SERVICES_EXT_TCP="2001 2443 22015 22016"
   FW_SERVICES_EXT_UDP="161 162"
   ```

2. Execute `/sbin/SuSEfirewall2`.

Related references

- Port numbers that must be registered as firewall exceptions for Device Manager and Tiered Storage Manager on page 121

Registering firewall exceptions for Host Data Collector (Windows)

If the Windows firewall was enabled or the port used by Host Data Collector was changed immediately after Host Data Collector operation started, you need to manually register firewall exceptions.

Registering an exception for the Host Data Collector service (for non-SSL communication)

Use the `firewall_setup` command to register a firewall exception for non-SSL communication ports used by the Host Data Collector service.

A firewall exception is registered for the ports set for the following properties in the `hdcbase.properties`. The exception name `Host Data Collector Base` is assigned to these ports.

- `hdc.common.rmi.registryPort` property (Default value: 22098/tcp)
- `hdc.common.rmi.serverPort` property (Default value: 22099/tcp)
- `hdc.common.http.serverPort` property (Default value: 22100/tcp)

Operations to complete in advance

Log in with administrator permissions.

Command format

```
firewall_setup.bat {add|del}
```

Location of the command

installation-folder-for-Host-Data-Collector\HDC\Base\bin

Options

add

Adds firewall exceptions.

del

Removes firewall exceptions.

Related tasks

- Registering an exception for the Host Data Collector service (for SSL communication) on page 142

Related references

- hdc.common.rmi.registryPort on page 659
- hdc.common.rmi.serverPort on page 660
- hdc.common.http.serverPort on page 660

Registering an exception for the Host Data Collector service (for SSL communication)

Use the `netsh` command to register a firewall exception for SSL communication ports used by the Host Data Collector service.

Before you begin

- Log in with administrator permissions.
- Check the following information:
  - Port number set for the `hdc.common.rmi.ssl.registryPort` property (Default value: 22104/tcp)
  - Port number set for the `hdc.common.rmi.ssl.serverPort` property (Default value: 22105/tcp)
  - Port number set for the `hdc.common.https.serverPort` property (Default value: 22106/tcp)

Procedure

1. Execute the following command for each port.

   ```
   netsh advfirewall firewall add rule name="Host Data Collector Base" dir=in action=allow localport=port-number protocol=TCP
   ```

2. Restart the Host Data Collector service to enable the settings.

Tip: To check the registered information, execute the following commands:

```
netsh advfirewall firewall show rule name=all
```

Related tasks

- Starting the Host Data Collector service on page 464
- Stopping the Host Data Collector service on page 464
- Registering an exception for the Host Data Collector service (for non-SSL communication) on page 141

Related references

- hdc.common.rmi.ssl.registryPort on page 661
- hdc.common.rmi.ssl.serverPort on page 661
- hdc.common.https.serverPort on page 662

Network settings with multiple IP addresses

This section describes communication settings for multiple network configurations.

Network settings for using a management server as a bridge

To use the management server as a network bridge by installing multiple network interface cards (NICs) on the server, set up the networks so that the management server, management client, and storage systems can mutually communicate.

The sections where settings must be specified are explained by using the configuration example shown below.

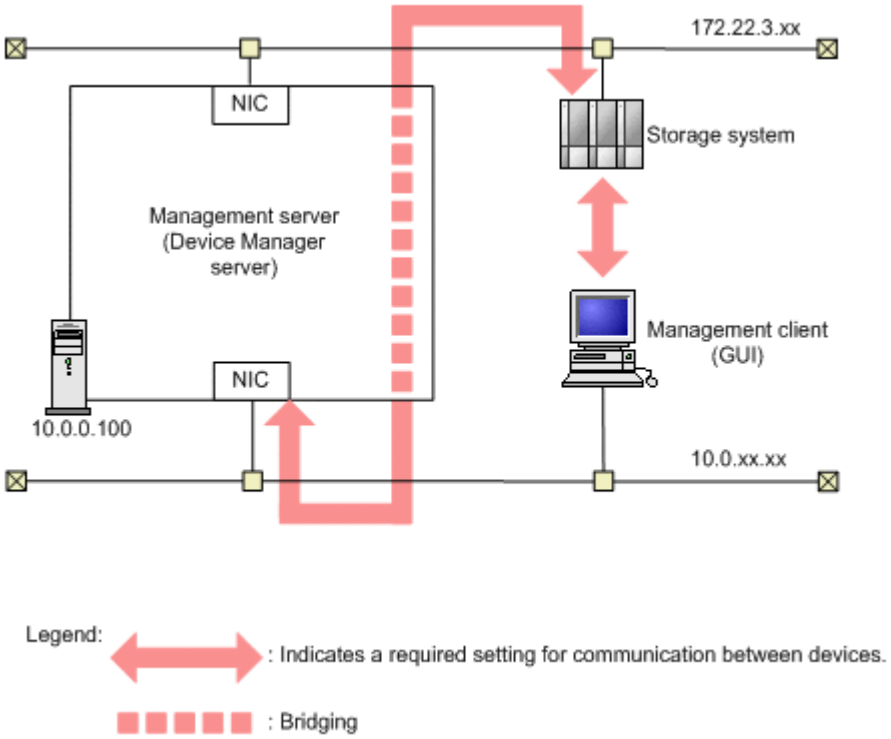


Figure 19 Example of a configuration in which the management server is used as a bridge between networks

Set up the routers, the management client, and the management server so that the devices can mutually communicate as indicated by the arrows in the above figure.

- Storage system and the management client
- Storage system and the management server

You do not have to set up communication between a management client and a member of midrange storage systems because Storage Navigator Modular 2 or Storage Navigator Modular manages this communication.

Caution: An IP address on the network to which the management client is connected (`10.0.0.100` in Figure 19 Example of a configuration in which the management server is used as a bridge between networks on page 144) must be specified for the Hitachi Command Suite product settings below. Do not specify a host name.

- The setting for the computer on which the Device Manager Web server function is running (the `server.http.host` property)
- The URL setting for the Storage Navigator Modular 2 instance launched from Device Manager (the `launchapp.snm2.url` property)

Related tasks

- Changing Device Manager server properties on page 590

Related references

- server.http.host on page 591
- launchapp.snm2.url on page 623

Specifying settings if the Host Data Collector machine has multiple IP addresses

If the Host Data Collector machine has multiple IP addresses, you must specify the IP address to be used for communication with the Device Manager server for the `hdc.service.rmi.registryIPAddress` property in the `hdcbase.properties` file for Host Data Collector.

Related references

- hdc.service.rmi.registryIPAddress on page 662

Device Manager settings in IPv6 environments

Device Manager supports IPv6-based communication. To use Device Manager in an IPv6 environment, you need to change the Device Manager settings according to the environment's requirements.

To use Device Manager in an IPv6 environment, make sure that the Device Manager settings meet the following requirements:

- Set up the OS so that both IPv6 and IPv4 can be used because, even if IPv6 is being used, IPv4 is also required for processing in the product.
- You can only use global addresses as IPv6 addresses. Global-unique local addresses (site-local addresses), and link-local addresses cannot be used.
- When specifying the IP address or host name of the Device Manager server, we recommend that you use the host name.
- When operating a Hitachi AMS/WMS storage system from Element Manager, be sure to specify a host name (not an IP address) for the Storage Navigator Modular 2 URL.

Related references

- Settings required for linking with Storage Navigator Modular 2 on page 332

Settings for migrating Device Manager to an IPv6 environment

If Device Manager is used in an IPv4 environment and you intend to use it in an IPv6 environment, edit the `user_httpsd.conf` file.

Note: If Device Manager is installed as a new installation in an IPv6 environment, the procedure described below is not necessary because the installer automatically changes the settings.

However, after the installation, if you link the system with Hitachi File Services Manager or Storage Navigator Modular 2, make sure that IPv6 communication is enabled in the following file:

- In Windows:
  installation-folder-for-Hitachi-File-Services-Manager-or-Storage-Navigator-Modular-2\Base\jdk\jre\lib\security\jssecacerts
- In Linux:
  installation-directory-for-Hitachi-File-Services-Manager-or-Storage-Navigator-Modular-2/Base/jdk/jre/lib/security/jssecacerts

---

Procedure

1. Stop the Hitachi Command Suite product services.
2. Open the `user_httpsd.conf` file.

   The `user_httpsd.conf` file is stored in the following locations:
   - In Windows:
     installation-folder-for-Hitachi-Command-Suite\Base64\uCPSB\httpsd\conf\user_httpsd.conf
   - In Linux:
     *installation-directory-for-Hitachi-Command-Suite/*Base64/uCPSB/httpsd/conf/user_httpsd.conf

   ---

   Note: Do not edit the `httpsd.conf` file that is stored in the same location as the `user_httpsd.conf` file.

   However, if the system is linked with Hitachi File Services Manager or Storage Navigator Modular 2, edit the `httpsd.conf` file that is stored in the following location.

   In Windows:

   installation-folder-for-Hitachi-File-Services-Manager-or-Storage-Navigator-Modular-2\Base\jdk\jre\lib\security\jssecacerts

   In Linux:

   installation-directory-for-Hitachi-File-Services-Manager-or-Storage-Navigator-Modular-2/Base/jdk/jre/lib/security/jssecacerts

   Use the same method to edit the file as you used for the `user_httpsd.conf` file. However, for the port number, specify the

port number for HBase Storage Mgmt Web Service (the default port for non-SSL communication is 23015, and the default port for SSL communication is 23016).

3. Delete the heading hash mark (#) from the `#Listen [::]:port-number` line to enable IPv6-based communication.

Caution:
- If you use non-SSL communication, you do not need to delete the hash mark (#) from the `Listen` line under `SSLDisable`.
- By default, all IPv6 addresses are set to allow communication.
- Specify the same port number as specified in the `Listen` line for IPv4.
- Do not delete or edit the `Listen` line. If you do so, communication via IPv4 will no longer be possible in the environment.

4. Start the Hitachi Command Suite product services.

Related tasks

- Starting the Hitachi Command Suite services on page 458
- Stopping the Hitachi Command Suite services on page 460

Settings for linking with storage systems that support IPv6

To operate Universal Storage Platform V/VM storage systems that are managed using IPv6 addresses from Element Manager, edit the `server.properties` file on the Device Manager server.

Procedure

On the Device Manager server, open the `server.properties` file, and set either of the following items for the `server.http.host` property:

- The IPv6 address of the computer on which the Device Manager server is installed
- The host name of the computer on which the Device Manager server is installed
  The host name must be resolvable to the IPv6 address.

Caution: If Universal Storage Platform V/VM storage system that is managed via an IPv4 address is also set up as a Device Manager management-target, IPv4 addresses must also be set for any NICs

that have IPv6 addresses specified for the `server.http.host` property.

Related tasks

- Changing Device Manager server properties on page 590

Related references

- server.http.host on page 591

Changing the IP address or host name of the management server

If you change the IP address or host name of the management server because of changes to the network configuration, you also need to change the settings for Hitachi Command Suite products.

Changing the host name of the management server

To apply the changed host name to the Hitachi Command Suite products, edit the `/etc/hosts` file (in Linux) , `user_httpsd.conf` file, and `cluster.conf` file (for cluster configurations), and then restart the computer.

Before you begin

- Check the following information:
  - Changed host name of the management server
    The host name must be no more than 128 bytes. For Hitachi Command Suite products, the host name is case sensitive.



Tip: If you change the host name of the management server in advance, keep a note of the new host name that is displayed by the `hostname` command. In Windows, you can also use the `ipconfig /ALL` command to display the host name.

Procedure

1. Stop the Hitachi Command Suite product services.
2. If SSL/TLS is used for communication between the following components, re-create a server certificate of the management server by using the new host name:
   - Between a management server and a management client (GUI)
   - Between a management server and a management client (Device Manager CLI)

- Between a Device Manager server and Replication Manager server
- Between a Tuning Manager server and a Device Manager server
- Between a management server and a CIM client

3. If the OS is Linux, edit the `/etc/hosts` file.
   Change the host name of the management server to the new host name. For Linux, write the new host name into the line above the `localhost` line.
4. Edit the user_httpsd.conf file.
   Change the value for the `ServerName` directive to the new host name.
   - In Windows:
     installation-folder-for-Hitachi-Command-Suite`\Base64\uCPSB\httpsd\conf\user_httpsd.conf`
   - In Linux:
     installation-directory-for-Hitachi-Command-Suite`/Base64/uCPSB/httpsd/conf/user_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` directive in the <`VirtualHost`> tag to the new host name.

   Note: Do not edit the `httpsd.conf` file and the `hsso_httpsd.conf` file.

5. 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.
   - In Windows:
     installation-folder-for-Hitachi-Command-Suite`\Base64\uCPSB\httpsd\conf\cluster.conf`
   - In Linux:
     installation-directory-for-Hitachi-Command-Suite`/Base64/uCPSB/httpsd/conf/cluster.conf`
6. 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.

7. Make sure that the Hitachi Command Suite product services are running properly.
8. If the host name is used in the URLs of Hitachi Command Suite products, change the settings of all Hitachi Command Suite products that are installed on the management server.
9. Depending on the operating environment, review the Hitachi Command Suite product settings.
10. Back up the database.

    If you change the host name, the data that you backed up can no longer be used.

Related concepts

- Backing up databases on page 470

Related tasks

- Changing the URL for accessing Hitachi Command Suite products (hcmds64chgurl command) on page 154
- Stopping the Hitachi Command Suite services on page 460
- Checking the operating status of the Hitachi Command Suite services on page 462

Related references

- Required operations after changing the IP address or host name of the management server on page 152

Changing the IP address of the management server

To apply the changed IP address to the Hitachi Command Suite products, edit the `user_httpsd.conf` file, and then restart the computer.

Before you begin

Check the following information:

- Changed IP address of the management server.



Caution: Do not change the settings in the cluster configuration file (the `cluster.conf` file).

Procedure

1. Stop the Hitachi Command Suite product services.
2. Edit the `user_httpsd.conf` file.

   If the old IP address is specified for the `ServerName` directive, change the IP address to the host name or the new IP address.

- In Windows:
  installation-folder-for-Hitachi-Command-Suite`\Base64\uCPSB\httpsd\conf\user_httpsd.conf`
- In Linux:
  installation-directory-for-Hitachi-Command-Suite`/Base64/uCPSB/httpsd/conf/user_httpsd.conf`

Note:
- Do not edit the `httpsd.conf` file.
- We recommend that you specify the host name in the `user_httpsd.conf` file.

---

3. 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.
4. Make sure that the Hitachi Command Suite product services are running properly.
5. If the IP address is used in the URLs of Hitachi Command Suite products, change the settings of all Hitachi Command Suite products that are installed on the management server.
6. Depending on the operating environment, review the Hitachi Command Suite product settings.
7. Back up the database.

   If you change the IP address, the data that you backed up can no longer be used.

Related concepts

- Backing up databases on page 470

Related tasks

- Changing the URL for accessing Hitachi Command Suite products (hcmds64chgurl command) on page 154
- Stopping the Hitachi Command Suite services on page 460
- Checking the operating status of the Hitachi Command Suite services on page 462

Related references

- Required operations after changing the IP address or host name of the management server on page 152

Required operations after changing the IP address or host name of the management server

If you change the IP address or host name of the management server, you might have to review the settings for Device Manager, Tiered Storage Manager, and Replication Manager depending on the operating environment.

- When the old host name or IP address is specified for the `server.http.host` property:
  You need to replace the old host name or IP address with the new host name or IP address, and then restart the services of Hitachi Command Suite products.
- When the Device Manager agent is used:
  You need to execute the `hdvmagt_setting` command to change the settings for the Device Manager server information.
- When the Replication Manager is used:
  If you change the IP address or the host name registered as the information source, re-register the information source.
  For details on how to register the Replication Manager information source, see the *Hitachi Command Suite Replication Manager User Guide*.
- When Element Manager is used to operate a Hitachi AMS/WMS storage system:
  You must use launchapptool to modify the URL settings.
- When a RADIUS server is used to authenticate accounts:
  Check the settings in the `exauth.properties` file.
- When the Device Manager server and the Tuning Manager server are remotely connected:
  If all the following conditions are satisfied, change the registration of repository location:
  - The IP address of the computer on which the Device Manager server is installed was changed.
  - The IP address of the computer on which the Device Manager server is installed is set in the `hsso.conf` file of the computer on which the Tuning Manager server is installed.

  For details on how to change the registration of the repository location, see the *Tuning Manager Server Administration Guide*.
- If acquiring performance information from Tuning Manager
  Revise the `ownHost` parameter setting in the `config.xml` file and the `configforclient.xml` file.
- If SNMP traps are received from file servers:

- For NAS Platform, change the host name or IP address of the notification destination for SNMP traps (the SNMP manager) by using SMU, NAS Manager, or the NAS Platform CLI.
  Make the format of the IP address (IPv6 or IPv4) to be set match the following:

Table 33 IP address format for the management server to be set (setting SNMP traps for NAS Platform)

Conditions		IP address format (IPv6 or IPv4)
The setting for SNMP traps to be sent from Admin services EVS is set in the NAS Platform CLI.		Match the format with the IP address format for Admin services EVS.
The setting for SNMP traps to be sent from Admin services EVS is not set in the NAS Platform CLI.	An EVS for mounting the file system exists.	Match the format with the IP address format for EVS where the file system is to be mounted.
	An EVS for mounting the file system does not exist.	Match the format with the IP address format for the file server (node).

- For Hitachi Data Ingestor, change the host name or IP address of the notification destination for SNMP traps (the SNMP manager) by using Hitachi File Services Manager.

  For details on how to change the SNMP trap notification destination for the file server, see the file server manuals.

- For VSP G1000, G1500, or VSP F1500, if user accounts are authenticated in Hitachi Command Suite when logging in to CCI or the SVP
  If secure communication is used between Device Manager and storage systems by using a certificate other than the default certificate bundled with Device Manager, in the Device Manager GUI, from the Edit Storage Systems window, re-set user account authentication.
- If you perform operations on VSP Gx00 models or VSP Fx00 models
  If secure communication is used between Device Manager and storage systems by using a certificate other than the default certificate bundled with Device Manager, in the Device Manager GUI, from the Edit Storage Systems window, re-set user account authentication.

If there are other script files or batch files in which an IP address or a host name is specified, review the settings.

For details about settings required for products other than Device Manager, Tiered Storage Manager, and Replication Manager, see the manuals for Hitachi Command Suite products.

Related tasks

- Registering an external authentication server and an external authorization server on page 178
- Settings for using Element Manager on page 333
- Starting the Hitachi Command Suite services on page 458
- Stopping the Hitachi Command Suite services on page 460
- Changing Device Manager server properties on page 590

Related references

- Setting up the config.xml and configforclient.xml files on page 353
- Setting the Device Manager server's information, HiScan command's execution period, and CCI's information (hdvmagt_setting command) on page 533
- server.http.host on page 591

Changing the URL for accessing Hitachi Command Suite products (hcmds64chgurl command)

Use the `hcmds64chgurl` command to change the URLs of the Hitachi Command Suite products that are registered on the GUI.

After starting Hitachi Command Suite operation, if a product URL is changed due to any of the following configuration changes, you must use the `hcmds64chgurl` command to change the URL registered in the GUI for each product:

- Changing a port used by HBase 64 Storage Mgmt Web Service
- Changing the host name or IP address of the management server
- Changing the settings for enabling or disabling SSL communication
- Migrating to a cluster environment

Procedure

1. Execute the `hcmds64chgurl` command.

   In Windows:

   installation-folder-for-Hitachi-Command-Suite`\Base64\bin\hcmds64chgurl {/print | /list | /change` *old-URL new-URL* `| /change` *new-URL* `/type` *Hitachi-Command-Suite-product-name*`}`

   In Linux:

   installation-directory-for-Hitachi-Command-Suite`/Base64/bin/hcmds64chgurl {-print | -list | -change` *old-URL new-URL* `| -change` *new-URL* `-type` *Hitachi-Command-Suite-product-name*`}`

- `print`
  Specify this option to display a list of URLs and programs that are currently registered.
- `list`
  Specify this option to display the same information as the `print` option in a different format.
- `change`
  Specify this option to change a currently registered URL.
- `type`
  If you want to change the URL for a specific Hitachi Command Suite product only, use this option to specify the name of that product. To change only the Device Manager URL, specify `DeviceManager`. To change only the Tiered Storage Manager URL, specify `TieredStorageManager`. To change only the Replication Manager URL, specify `ReplicationManager`. For details on the names of other Hitachi Command Suite products, see the documentation for each product.

Caution:

- The specified URL must be a complete URL that contains protocols and a port number. You cannot use an IPv6 address. You must use a host name to specify the URL in an IPv6 environment, as shown in the following example:
  `http://hostname:22015`
- When changing the URL during migration to a cluster environment, use the following format to specify *new-URL*:
  `http://`*logical-host-name*`:`*port-number*

---

2. In Windows, change the URL in the shortcut file.

In Windows Server 2008 R2:

Select **Start**, **All Programs**, **Hitachi Command Suite**, and then right-click **Login - HCS**. In Properties, change the URL on the **Web Document** tab.

In Windows Server 2012 or Windows Server 2012 R2:

From the Start window, display the list of applications, then under **Hitachi Command Suite**, right-click **Login - HCS**. In Properties, change the URL on the **Web Document** tab.

The URL format is as follows:

protocol://*IP-address-of-the-management-server*:*port-number*/DeviceManager/

- *protocol*
  Specify `http` for non-SSL communication, and `https` for SSL communication.
- *IP-address-of-the-management-server*
  Specify the IP address or host name of the management server.
- *port-number*
  Specify the port number that is set in the `Listen` line in the `user_httpsd.conf` file. For non-SSL communication, specify the port number for non-SSL communication (default: 22015). For SSL communication, specify the port number for SSL communication (default: 22016).
  The `user_httpsd.conf` file is stored in the following location: *installation-folder-for-Hitachi-Command-Suite*`\Base64\uCPSB\httpsd\conf\user_httpsd.conf`

Related concepts

- Operation workflow for secure communication between a management server and a management client (GUI) on page 225

Related tasks

- Changing ports used by Common Component on page 114
- Changing the host name of the management server on page 148
- Changing the IP address of the management server on page 150

3

User account management

This chapter describes the settings required for managing user accounts of Hitachi Command Suite products.

- About password policies
- About account locking

About password policies

A password policy is a set of conditions related to the number of characters or combinations of character types that can be used in passwords for user accounts.

By setting a password policy, you can prevent users from setting easily guessed passwords, and reduce the risk of unauthorized access from third parties.

You can specify the following conditions in a password policy:

- Minimum password length
- Minimum number of uppercase letters used in passwords
- Minimum number of lowercase letters used in passwords
- Minimum number of numerals used in passwords
- Minimum number of symbols used in passwords
- Ability to set passwords that are the same as the user ID

If you are using a management server to manage user accounts, we recommend that you set these conditions to increase password complexity.

Setting password policies

Password policies for Hitachi Command Suite products are set in the `security.conf` file.

Procedure

Edit the `security.conf` file.

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

In Windows:

installation-folder-for-Hitachi-Command-Suite`\Base64\conf\sec\security.conf`

In Linux:

installation-directory-for-Hitachi-Command-Suite`/Base64/conf/sec/security.conf`

The following table shows the password policies that can be set in the `security.conf` file.

Table 34 Password policies that can be set in the security.conf file

Item	Description
`password.min.length`	Specifies the minimum number of characters the password must contain. Specify a value from 1 to 256.

Item	Description
	Default: 4
password.min.uppercase	Specifies the minimum number of uppercase letters the password must contain. Specify a value from 0 to 256. If you specify 0, no restriction applies. Default: 0
password.min.lowercase	Specifies the minimum number of lowercase letters the password must contain. Specify a value from 0 to 256. If you specify 0, no restriction applies. Default: 0
password.min.numeric	Specifies the minimum number of numeric characters the password must contain. Specify a value from 0 to 256. If you specify 0, no restriction applies. Default: 0
password.min.symbol	Specifies the minimum number of symbols the password must contain. Specify a value from 0 to 256. If you specify 0, no restriction applies. Default: 0
password.check.userID	Specifies whether the password can be the same as the user ID. If `true` is specified, passwords cannot be the same as the corresponding user ID. If `false` is specified, passwords can be the same as the corresponding user ID. Default: `false`

Caution:

- In all Hitachi Command Suite products, set password policies apply only to user accounts that are added and passwords that are changed after the policy was set. New password policies do not apply to existing user accounts, so users of such accounts can log in to the system even if their passwords do not satisfy the set conditions.
- You can also set password policies from the GUI. However, if the system is in a cluster configuration, the settings from the GUI are applied only to the executing node. To apply the settings to the standby node, switch the nodes, and then specify the same settings.
- If an external authentication server is used to authenticate users, passwords are checked by using a combination of

character types specified on the external authentication server. However, if you register a password for a Hitachi Command Suite product user, you need to use character types specified in the Hitachi Command Suite products.

Result

When you change the setting values in the `security.conf` file, the new password policy takes effect immediately.

About account locking

Account locking is the locking (temporary disabling) of a user account.

By enabling account locking, you can reduce the risk of unauthorized access from third parties. If you are managing user accounts by using a management server, we recommend that you enable account locking.

In Hitachi Command Suite products, you can automatically lock user accounts that fail to log in to the GUI many times in a row.

To enable account locking, you need to set the account locking policy (the number of consecutive, unsuccessful login attempts before accounts are locked).

Tip: As a way to lock an account, you can change the lock status of a user account from the GUI.

Note that only users with the `Admin` (user management) permission can change the lock status.

Caution:

- Account locking cannot be performed on `System` accounts when initially installing Hitachi Command Suite products. `System` accounts are set with `Admin` permissions for all Hitachi Command Suite products. If you want to set account locking for `System` accounts to improve security, you need to change the settings.
- If an external authentication server is used to authenticate users, the settings on the external authentication server are used to control automatic locking.

About account locking policies

An account locking policy is the number of consecutive, unsuccessful login attempts before automatically locking (temporarily disabling) user accounts that fail to log in to the GUI many times in a row.

When you set an account locking policy, it is immediately applied to all Hitachi Command Suite products that use Single Sign-On functionality. For example, if you set the number of consecutive failed login attempts to 3 and a user fails to log in to Device Manager once, Tiered Storage Manager once, and then Replication Manager once, the user account is automatically locked.

Setting account locking policies

You can set an account locking policy for Hitachi Command Suite products in the `security.conf` file.

Procedure

Edit the security.conf file.

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

In Windows:

installation-folder-for-Hitachi-Command-Suite`\Base64\conf\sec\security.conf`

In Linux:

installation-directory-for-Hitachi-Command-Suite`/Base64/conf/sec/security.conf`

The following table shows the account locking policies that can be set in the `security.conf` file.

Table 35 Account locking policies that can be set in the security.conf file

Item	Description
`account.lock.num`	Specify the number of consecutive failed login attempts required to trigger automatic account locking. Specify a value from 0 to 10. If a user makes the specified number of unsuccessful login attempts, his or her user account will be locked. If you specify 0, any number of unsuccessful login attempts is allowed. Default: 0

Caution:

- If you change the number of consecutive failed login attempts, the new value takes effect from the first failed login after the change. If a user is currently logged in and you attempt to login 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 perform operations while still logged in.

- You can also set an account locking policy from the GUI. However, if the system is in a cluster configuration, the settings from the GUI are applied only to the executing node. To apply the settings to the standby node, switch the nodes, and then specify the same settings.

Result

If you change the setting values in the security.conf file, the new account locking policy takes effect immediately.

Settings for automatically locking the System account

To apply account locking to `System` accounts, change the settings in the `user.conf` file.

Procedure

1. Stop the Hitachi Command Suite product services.
2. Open the `user.conf` file.

   The `user.conf` file is stored in the following locations:
   - In Windows:
     installation-folder-for-Hitachi-Command-Suite\Base64\conf\user.conf
   - In Linux:
     installation-directory-for-Hitachi-Command-Suite/Base64/conf/user.conf

   If the `user.conf` file does not exist, create it.
3. Use the following format to specify the `account.lock.system` property:
   `account.lock.system=true`
4. Start the Hitachi Command Suite product services.

Result

Account locking is applied to System accounts for all Hitachi Command Suite products.

Related tasks

- Starting the Hitachi Command Suite services on page 458
- Stopping the Hitachi Command Suite services on page 460

Unlocking accounts

Locked user accounts can be unlocked by using the `hcmds64unlockaccount`

Before you begin

- Log in as a user with Administrator permissions (for Windows) or as a root user (for Linux).
- Confirmation that the locked user account has User Management `Admin` permissions
  If a user account does not have User Management Admin permissions, another user whose account has User Management Admin permissions must unlock the account.
- Check the following information:
  - The user ID and password of the locked user account

Procedure

Execute the `hcmds64unlockaccount` command to unlock the account.

In Windows:

```
installation-folder-for-Hitachi-Command-Suite\Base64\bin
\hcmds64unlockaccount [/user user-ID /pass password]
```

In Linux:

```
installation-directory-for-Hitachi-Command-Suite/
Base64/bin/hcmds64unlockaccount [-user user-ID -pass
password]
```

If the command is executed without specifying the `user` option or the `pass` option, you will be prompted to enter a user ID and password.

Caution: If any symbols are used in the user ID or password, you need to escape these symbols on the command line.

- In Windows:
  If the user ID or password ends with a backslash (`\`), use another backslash (`\`) to escape that backslash (`\`).
  Also, if the user ID or password includes an ampersand (`&`), vertical bar (`|`), or caret (`^`), enclose each character with a double quotation mark (`"`), or use a caret (`^`) to escape the symbols.
- In Linux:
  Use a backslash (`\`) to escape each character.

4

User management on an external authentication server

This chapter explains how to set user authentication on the external authentication server.

- About linking to an external authentication server
- About linking to an external authorization server
- Operating workflow for user authentication on an external authentication server
- Account conditions for Hitachi Command Suite products
- About the data structures of user entries
- Configurations when multiple external authentication servers are linked
- Registering an external authentication server and an external authorization server
- About a LDAP search user account
- Registering a shared secret
- Checking connections to an external authentication server and an external authorization server
- Notes on commands for setting up a link to an external authentication server
- Encryption types for Kerberos authentication

About linking to an external authentication server

Hitachi Command Suite products allow you to log in to the GUI or execute CLI commands by using the user accounts registered on an external authentication server.

When an external authentication server is linked to, you do not need to perform login password management and account control for Hitachi Command Suite products.

Hitachi Command Suite products can be linked to the following external authentication servers:

- LDAP directory server
- RADIUS server
- Kerberos server

About linking to an external authorization server

In addition to an external authentication server, if you also use an external authorization server to perform user authentication, access permissions for the management server (a Hitachi Command Suite product) can be controlled on the external authorization server.

When an external authorization server is also linked to, you do not need to manage accounts and set permissions for individual users because Hitachi Command Suite products manage users by using the *authorization groups* on the external authorization server.

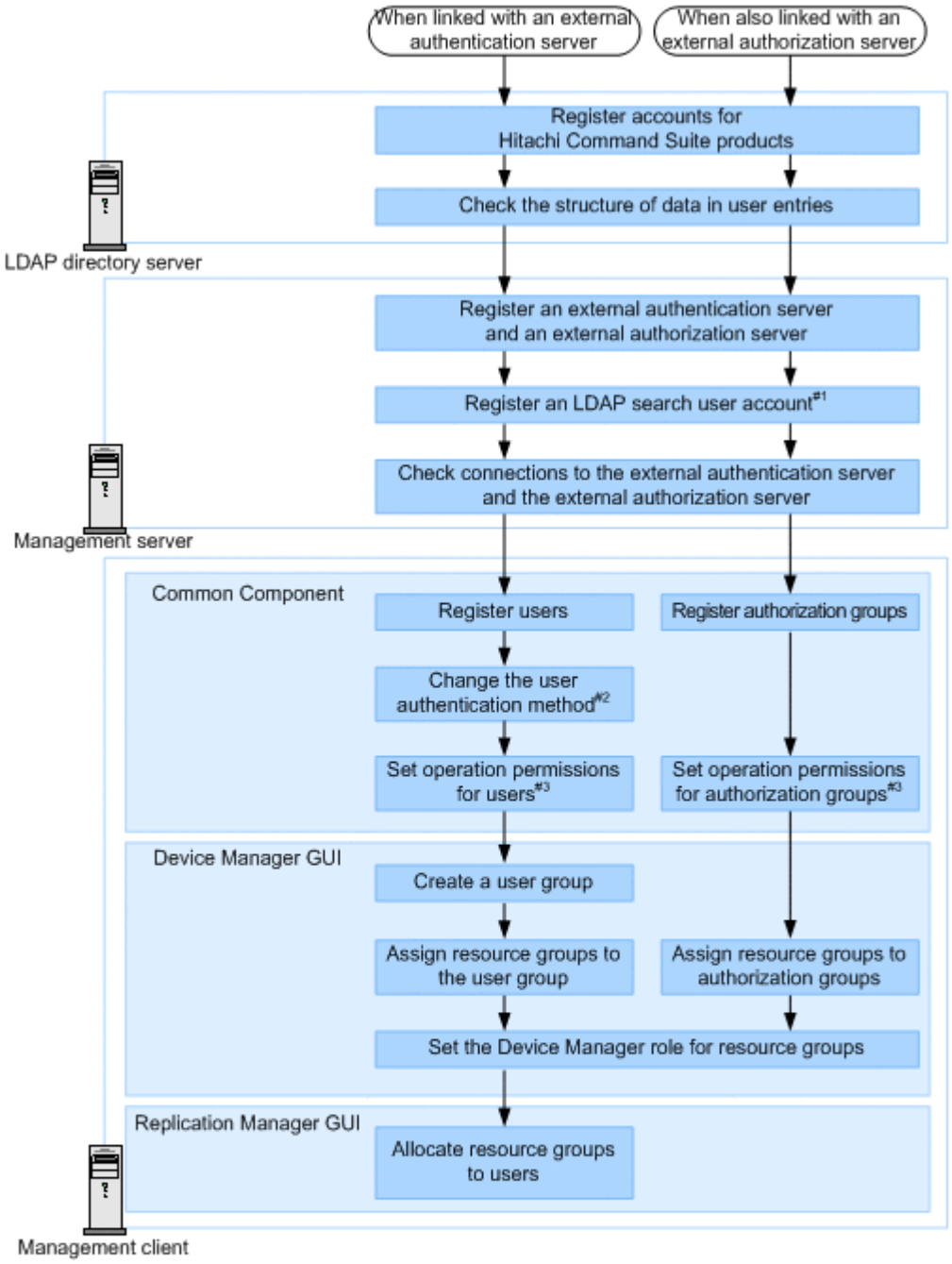
Hitachi Command Suite products can be linked to an LDAP directory server (Active Directory).

Operating workflow for user authentication on an external authentication server

To use the GUI or CLI of Hitachi Command Suite products by using the user accounts managed by an external authentication server, you need to set up an environment for the external authentication server, management server, and management clients.

Operating workflow for user authentication on an LDAP directory server

To perform user authentication on an LDAP directory server, you need to register the external authentication server and the accounts to be authenticated on the management server for Hitachi Command Suite products.



#1: This step is not required if you want to link only to an external authentication server and the structure of the data of the user entries is a flat model.
#2: This step is required if you want to change the current user authentication method.
#3: Set operation permissions according to the user job scope.

- User management
- Hitachi Command Suite products other than Device Manager
  You need to set roles and Tiered Storage Manager permissions for users who will use CLI to perform operations on Tiered Storage Manager.

Figure 20 Operating workflow for user authentication on an LDAP directory server

Note:

- When Hitachi Command Suite product is in operation, to switch to the system configuration linked to an external authorization server, delete any user ID that has the same name as the ID registered in Common Component, or change the user name. Similarly, if a user ID includes a domain name (example: user1@example.com), either delete any instances of the same user ID, or change the user ID. If the same user name is registered, when the user logs in to the Hitachi Command Suite product, the user is authenticated in Common Component (internal authentication).
- In Replication Manager, `All Resources` is automatically assigned as a resource group to users who belong to authorization groups. If the Modify permission is set for authorization groups, the Storage Administrator user role is assigned to the users that belong to the authorization groups. The user role cannot be changed.
- Users who belong to nested groups of a registered authorization group can now also use Hitachi Command Suite products via the roles (permissions) set for the authorization group.
- To use StartTLS to communicate between the LDAP directory server and the management server, you need to set up an environment specifically for this purpose to ensure secure communications.
- For details how to operation on a management client, see the *Hitachi Command Suite User Guide* or *Hitachi Command Suite Replication Manager User Guide*.

Related concepts

- About the data structures of user entries on page 173
- About a LDAP search user account on page 205
- Secure communication for Device Manager and Tiered Storage Manager on page 218

Related tasks

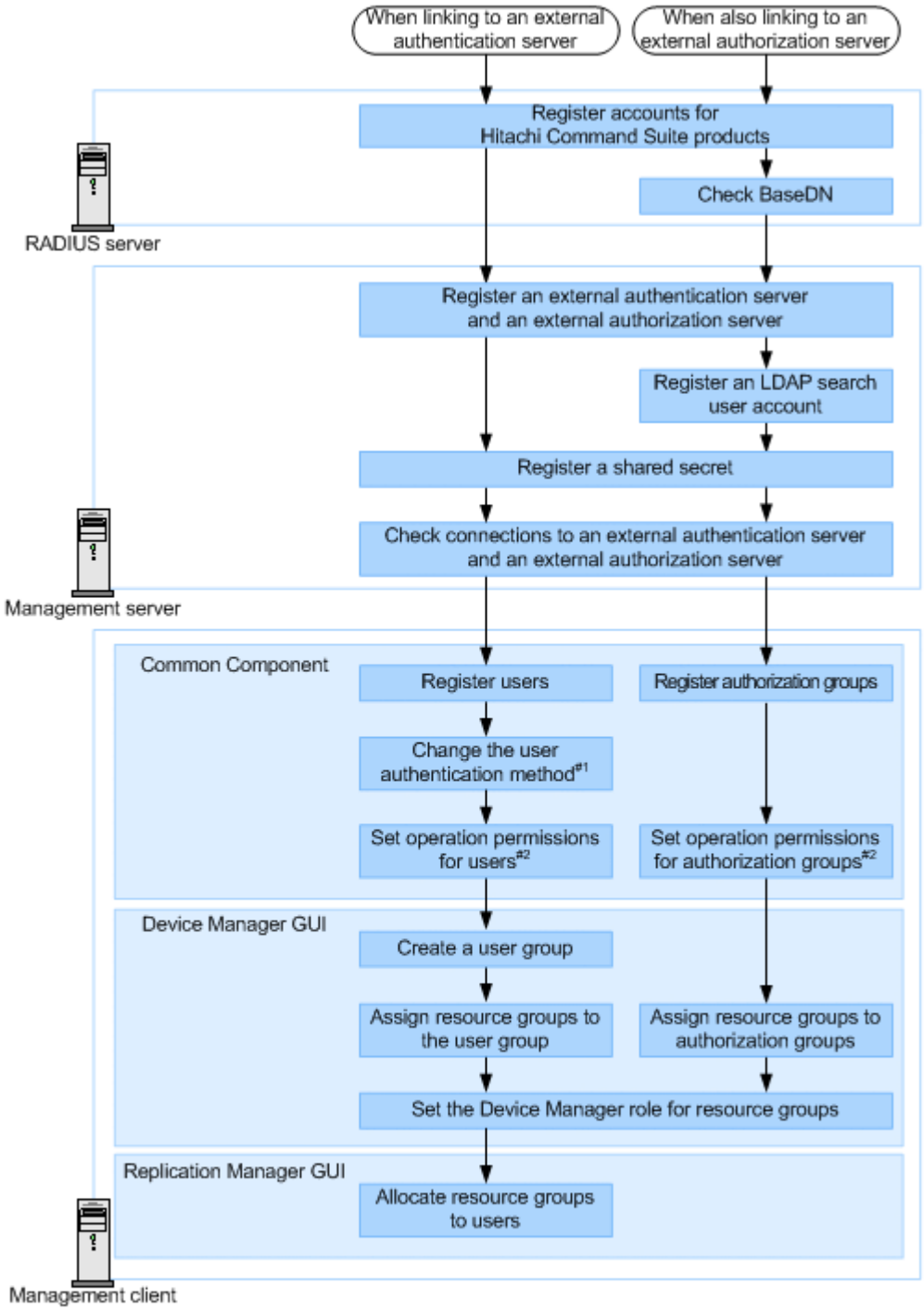
- Registering an external authentication server and an external authorization server on page 178
- Checking connections to an external authentication server and an external authorization server on page 212

Related references

- Account conditions for Hitachi Command Suite products on page 172

Operating workflow for user authentication on a RADIUS server

To perform user authentication on a RADIUS server, you need to register the external authentication server and the accounts to be authenticated on the management server for Hitachi Command Suite products.



#1: This step is required if you want to change the current user authentication method.
#2: Set operation permissions according to users' job scopes.

- User management
- Hitachi Command Suite products other than Device Manager
  You need to set roles and Tiered Storage Manager permissions for users who will operate Tiered Storage Manager by using the CLI.

Figure 21 Operating workflow for user authentication on a RADIUS server

Note:

- When a Hitachi Command Suite product is in operation, to switch to the system configuration linked to an external authorization server, delete any the user ID that has the same name as the ID registered in Common Component, or change the user name. If the same user name is registered, when the user logs in to a Hitachi Command Suite product, the user is authenticated in Common Component (internal authentication).
- In Replication Manager, `All Resources` is automatically assigned as a resource group to users who belong to authorization groups. If the Modify permission is set for authorization groups, the Storage Administrator user role is assigned to the users that belong to the authorization groups. The user role cannot be changed.
- Users who belong to nested groups of a registered authorization group can now also use Hitachi Command Suite products via the roles (permissions) set for the authorization group.
- To use StartTLS to communicate between the LDAP directory server and the management server, you need to set up an environment specifically for this purpose to ensure secure communications.
- For details how to operation on a management client, see the *Hitachi Command Suite User Guide* or *Hitachi Command Suite Replication Manager User Guide*.

Related concepts

- About the data structures of user entries on page 173
- About a LDAP search user account on page 205
- Secure communication for Device Manager and Tiered Storage Manager on page 218

Related tasks

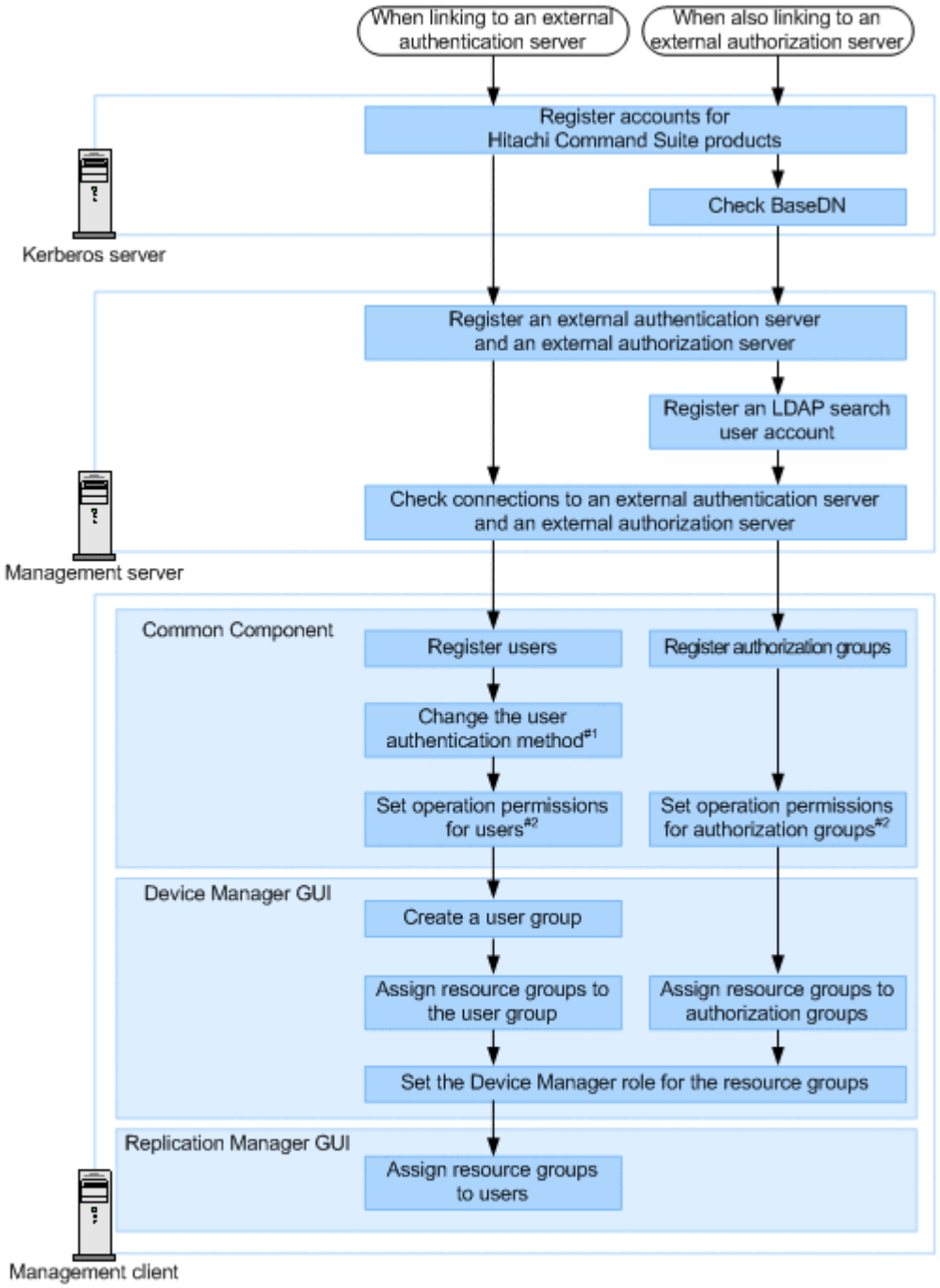
- Registering an external authentication server and an external authorization server on page 178
- Registering a shared secret on page 210
- Checking connections to an external authentication server and an external authorization server on page 212

Related references

- Account conditions for Hitachi Command Suite products on page 172

Operation workflow for user authentication on a Kerberos server

To perform user authentication on a Kerberos server, you need to register the external authentication server and the accounts to be authenticated on the management server for Hitachi Command Suite products.



#1: This step is required if you want to change the current user authentication method.
#2: Set operation permissions according to users' job scopes.

- User management
- Hitachi Command Suite products other than Device Manager
  You need to set roles and Tiered Storage Manager permissions for users who will operate Tiered Storage Manager by using the CLI.

Figure 22 Operation workflow for user authentication on a Kerberos server

Note:

- When a Hitachi Command Suite product is in operation, to switch to the system configuration linked to an external authorization server, delete any user ID that has the same name with the ID registered in Common Component, or change the user name. Similarly, if a user ID includes a realm name (example: user1@EXAMPLE.COM), either delete any instances of the same user ID, or change the user ID. If the same user name is registered, when the user logs in to a Hitachi Command Suite product, the user is authenticated in Common Component (internal authentication).
- In Replication Manager, `All Resources` is automatically assigned as a resource group to users who belong to authorization groups. If the Modify permission is set for authorization groups, the Storage Administrator user role is assigned to the users that belong to the authorization groups. The user role cannot be changed.
- Users who belong to nested groups of a registered authorization group can now also use Hitachi Command Suite products via the roles (permissions) set for the authorization group.
- To use StartTLS to communicate between the LDAP directory server and the management server, you need to set up an environment specifically for this purpose to ensure secure communications.
- For details how to operation on a management client, see the *Hitachi Command Suite User Guide* or *Hitachi Command Suite Replication Manager User Guide*.

Related concepts

- About the data structures of user entries on page 173
- About a LDAP search user account on page 205
- Secure communication for Device Manager and Tiered Storage Manager on page 218

Related tasks

- Registering an external authentication server and an external authorization server on page 178
- Checking connections to an external authentication server and an external authorization server on page 212

Related references

- Account conditions for Hitachi Command Suite products on page 172

Account conditions for Hitachi Command Suite products

User accounts (user IDs and passwords) for Hitachi Command Suite products must consist of characters that can be used in both the external authentication server and Hitachi Command Suite products.

Set user accounts so that they satisfy the following conditions:

- They are within 256 bytes.
- They use no characters other than the following:

  A to Z

  a to z

  0 to 9

  ! # $ % & ' ( ) * + - . = @ \ ^ _ |

In Hitachi Command Suite products, user IDs are not case-sensitive. The combination of character types for passwords must follow the settings in the external authentication server.

About the data structures of user entries

There are two data structures of user entries for an LDAP directory server: the hierarchical structure model and the flat model.

When performing user authentication on an LDAP directory server, check which data structure is being used, because information about the LDAP directory server registered on the management server and the operations you need to perform on the management server depend on the data structure.

In addition, when performing user authentication or authorization on an LDAP directory server, also check BaseDN, which is the start point for searching for users.

About the BaseDN

BaseDN is the start point for searching for users during authentication or authorization.

Only user entries in the hierarchies below BaseDN are subject to authentication or authorization. In Hitachi Command Suite products, user entries must contain all of the users to be authenticated or authorized. BaseDN is required when registering information about the LDAP directory server on the management server.

About the hierarchical structure model

A data structure in which the hierarchies below BaseDN branch off and in which user entries are registered in another hierarchy.

If the hierarchical structure model is used, the entries in the hierarchy below BaseDN are searched for an entry that has the same login ID and user attribute value. The following figure shows an example of the hierarchical structure model.

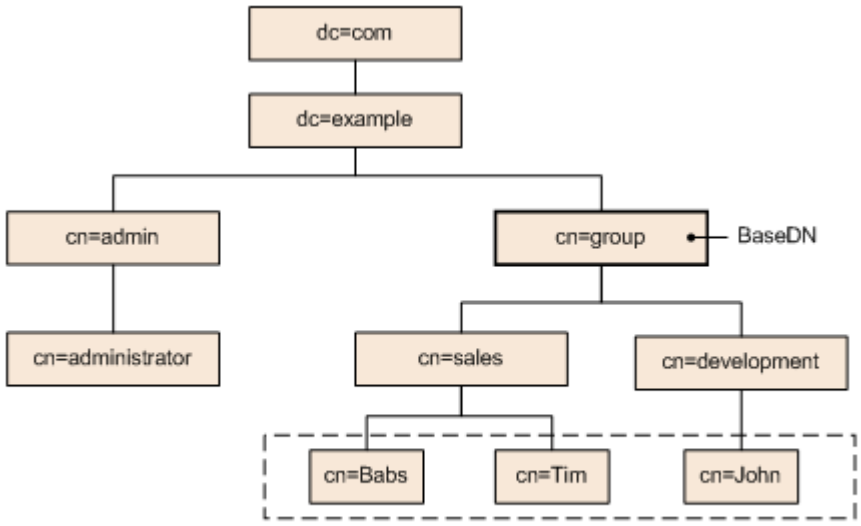


Figure 23 Example of the hierarchical structure model

The user entries enclosed by the dotted line can be authenticated. In this example, BaseDN is `cn=group,dc=example,dc=com`, because the target user entries extend across two departments (`cn=sales` and `cn=development`).

About the flat model

A data structure in which there are no branches in the hierarchy below BaseDN and in which user entries are registered in the hierarchy located just below BaseDN.

If the flat model is used, the entries in the hierarchy below BaseDN are searched for an entry that has the DN that consists of a combination of the login ID and BaseDN. If such a value is found, the user is authenticated. The following figure shows an example of the flat model.

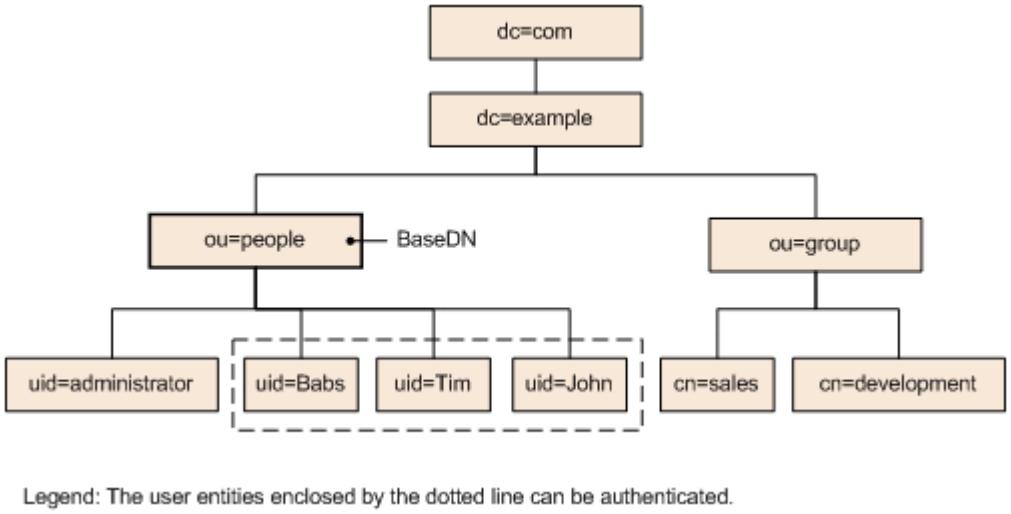


Figure 24 Example of the flat model

The user entities enclosed by the dotted line can be authenticated. In this example, BaseDN is `ou=people,dc=example,dc=com`, because all of the user entries are located just below `ou=people`.

Note, however, that even if the flat model is being used, if either of the following conditions is satisfied, specify the settings by following the explanation for the hierarchical structure model:

- If a user attribute value other than the RDN attribute value is used as the user ID of a Hitachi Command Suite product:
  If a user attribute value other than the RDN attribute value (for example, the Windows logon ID) of a user entry is used as the user ID of a Hitachi Command Suite product, you must use the authentication method for the hierarchical structure model.
- If the RDN attribute value of a user entry includes an invalid character that cannot be used in a user ID for a Hitachi Command Suite product:
  When using the authentication method for the flat model, the RDN attribute value of a user entry functions as the user ID for Hitachi Command Suite products. Therefore, if the RDN attribute value of a user entry includes an invalid character that cannot be used in a user ID of a Hitachi Command Suite product, you cannot use the authentication method for the flat model.
  Example of a valid RDN:
  `uid=John123S`
  `cn=John_Smith`
  Example of an invalid RDN:
  `uid=John:123S` (A colon is used.)
  `cn=John Smith` (A space is used between `John` and `Smith`.)

Configurations when multiple external authentication servers are linked

When multiple external authentication servers are linked, user authentication is performed in a redundant configuration or a multi-domain configuration.

A redundant configuration is used when each external authentication server manages the same user information. If a failure occurs on one external authentication server, user authentication can be performed by using another external authentication server.

A multi-domain configuration is used to manage different user information for each external authentication server. If a user logs in with a user ID that includes a domain name, the user will be authenticated by an external authentication server in the domain whose name is included in the user ID. When a Kerberos server is used as an external authentication server, you can create a configuration similar to a multi-domain configuration by managing different user information for each realm.

The following table shows external authentication servers for which redundant configurations and multi-domain configurations are supported.

Table 36 Support status for redundant configurations and multi-domain configurations

External authentication server	Redundant configuration	Multi-domain configuration
LDAP directory server	Y#1	Y#1
RADIUS server	Y	N
Kerberos server	Y	Y#2

Legend:

Y: Supported

N: Not supported

#1

You can use either a redundant configuration or a multi-domain configuration.

#2

By managing different user information for each realm, you can create a configuration that is similar to a multi-domain configuration.

When an LDAP directory server is used for user authentication in a multi-domain configuration, the user authentication process varies depending on whether you log in by entering a user ID that includes a domain name.

If you log in with a user ID that includes a domain name, as in the following figure, user authentication will be performed by using the LDAP directory server of the specified domain.

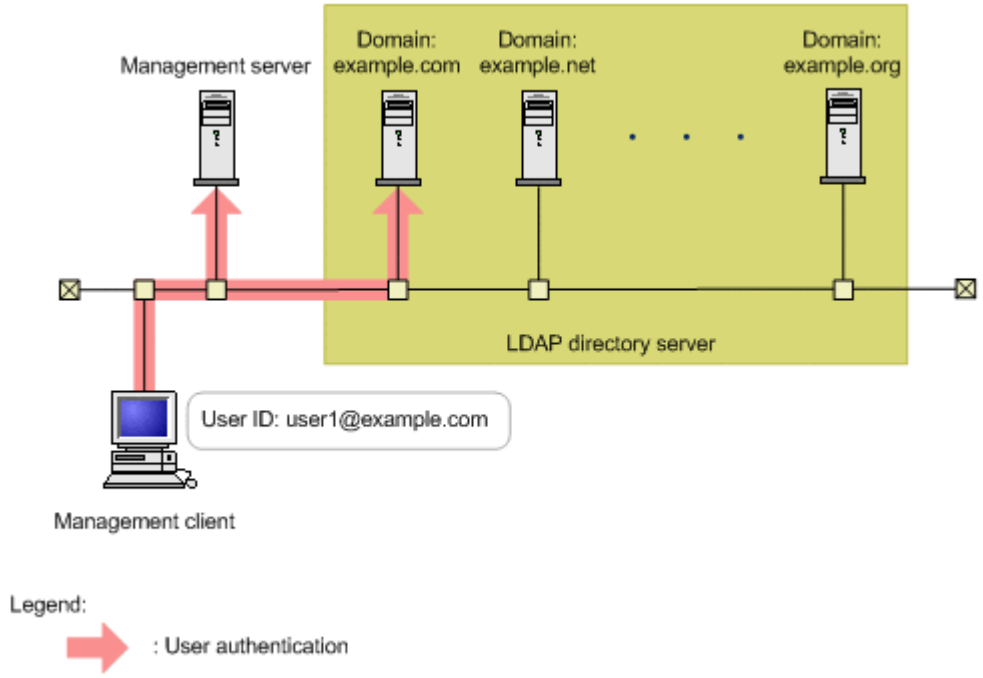


Figure 25 User authentication in a multi-domain configuration (when using a user ID that includes a domain name)

If you log in with a user ID that does not include a domain name, user authentication will be performed sequentially on all LDAP directory servers that are linked until the user is authorized, as shown in the figure below. If a large number of LDAP directory servers are linked, user authentication will take a long time. For this reason, we recommend that you log in with a user ID that includes a domain name.

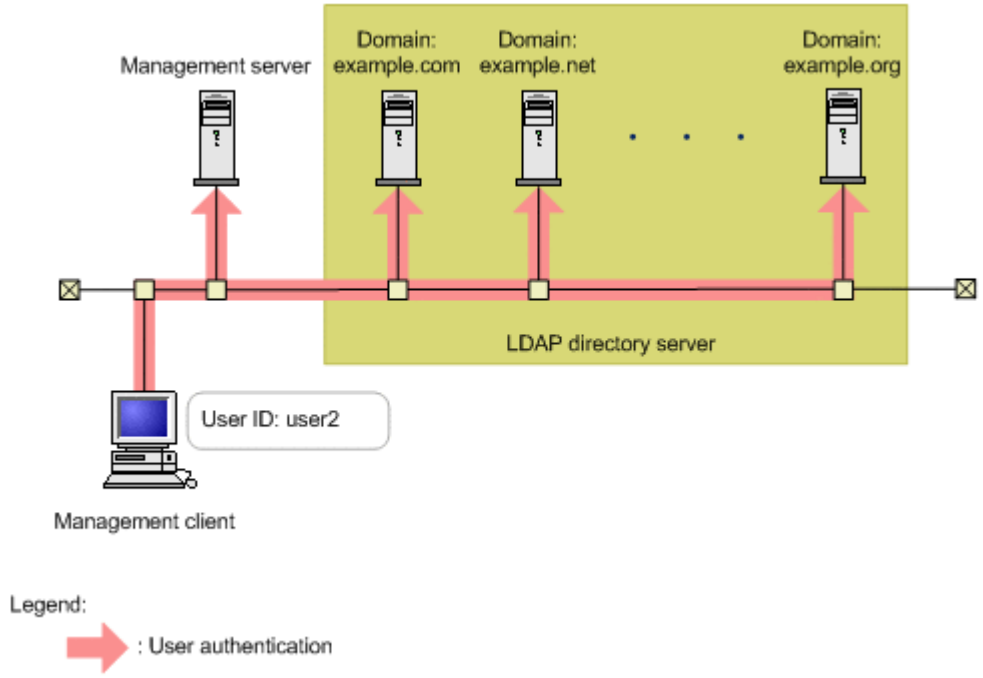


Figure 26 User authentication in a multi-domain configuration (when using a user ID that does not include a domain name)

Registering an external authentication server and an external authorization server

In the `exauth.properties` file, set the type of the external authentication server to be used, the server identification name, and the machine information about the external authentication server and external authorization server.

Before you begin

- Log in as a user with Administrator permissions (for Windows) or as a root user (for Linux).
- Copy the template of the `exauth.properties` file.

  In Windows:

  installation-folder-for-Hitachi-Command-Suite\Base64\sample\conf\exauth.properties

  In Linux:

  installation-directory-for-Hitachi-Command-Suite/Base64/sample/conf/exauth.properties

- Check the data structure of user entries (for LDAP authentication).

- Set up the environment for the DNS server on the OS of the LDAP directory server.#
- Register information about the LDAP directory server to the SRV record of the DNS server.#
- Check the following information:
  - Common information:
    - Type of the external authentication server
  - For LDAP authentication:
    - Machine information about the external authentication server and the external authorization server (Host name or IP address, Port number)
    - BaseDN
    - Domain name for external authentication servers managed by the LDAP directory server (when linking to an external authorization server)
    - Domain name for multi-domain configurations managed by the LDAP directory server (for a multi-domain configuration)
  - For RADIUS authentication:
    - Machine information about the external authentication server and the external authorization server (Host name or IP address, Port number)
    - Authentication protocol
    - Host name or IP address of the management server
    - Domain name managed by the LDAP directory server (when linking to an external authorization server)
    - BaseDN (when linking to an external authorization server)
  - For Kerberos authentication:
    - Machine information about the external authentication server and the external authorization server (Host name or IP address, Port number)
    - Realm name
    - Domain name managed by the LDAP directory server (when linking to an external authorization server)
    - BaseDN (when linking to an external authorization server)

#: This operation is required to look up the information about the LDAP directory server by using the DNS server.

Procedure

1. Specify required items in the `exauth.properties` file being copied.
2. Save the `exauth.properties` file in the following location:

   In Windows:

installation-folder-for-Hitachi-Command-Suite\Base64\conf\exauth.properties

In Linux:

installation-directory-for-Hitachi-Command-Suite/Base64/conf/exauth.properties

3. If the setting value of the `auth.ocsp.enable` or `auth.ocsp.responderURL` property is changed, the Hitachi Command Suite product services must be restarted.

   If the setting value of any other property or attribute is changed, the change takes effect immediately.

Related concepts

- About the data structures of user entries on page 173
- Configurations when multiple external authentication servers are linked on page 175

Related tasks

- Starting the Hitachi Command Suite services on page 458
- Stopping the Hitachi Command Suite services on page 460

Setup items in the exauth.properties file for LDAP authentication

In the `exauth.properties` file, set the type of the external authentication server to be used, the server identification name, and the machine information about the external authentication server.

- Common properties
  Table 37 Setup items in the exauth.properties file for LDAP authentication (common items) on page 181
- Properties for an external authentication server and an external authorization server
  Setup items in the `exauth.properties` file vary depending on whether information about the LDAP directory server being connected to is directly specified or looked up by using the DNS server.
  - When directly specifying information about the LDAP directory server:
    Table 38 Setup items in the exauth.properties file for LDAP authentication (when directly specifying information about the external authentication server) on page 182
    Table 39 Setup items in the exauth.properties file for LDAP authentication (when an external authentication server and StartTLS are used for communication) on page 184
  - When using the DNS server to look up information about the LDAP directory server:

Table 40 Setup items in the exauth.properties file for LDAP authentication (when using the DNS server to look up information about the external authentication server) on page 185

Note:

- Make sure to distinguish between uppercase and lowercase letters for property settings.
- To use StartTLS for communication between the management server and the LDAP directory server, you need to directly specify information about the LDAP directory server to connect to in the `exauth.properties` file.
- If you use the DNS server to look up the LDAP directory server to connect to, it might take longer for users to log in.
- If the LDAP directory server to which you want to connect is in a multi-domain configuration, you will not be able to look up the LDAP directory server by using the DNS server.

Table 37 Setup items in the exauth.properties file for LDAP authentication (common items)

Property	Details
`auth.server.type`	Specify an external authentication server type. Specify `ldap`. Default value: `internal` (used when not linking to an external authentication server)

`auth.server.name`	Specify the server identification names of LDAP directory servers. You can specify any name for this property in order to identify which LDAP directory servers the settings such as the port number and the protocol for connecting to the LDAP directory server (see Table 38 Setup items in the exauth.properties file for LDAP authentication (when directly specifying information about the external authentication server) on page 182 or Table 40 Setup items in the exauth.properties file for LDAP authentication (when using the DNS server to look up information about the external authentication server) on page 185) are applied to. `ServerName` has been set as the initial value. You must specify at least one name. To specify multiple server identification names, delimit the server identification names by using commas (,). Do not register the same server identification name more than once.
	
	Specifiable values: No more than 64 bytes of the following characters:
	
	`A` to `Z`
	
	`a` to `z`
	
	`0` to `9`
	
	`! # ( ) + - . = @ [ ] ^ _ { } ~`
	
	Default value: none

`auth.ldap.multi_domain`	When specifying multiple server identification names for LDAP directory servers, specify, for each server, the configuration to be used. Specify `true` to use a multi-domain configuration.

Property	Details
	Specify `false` to use a redundant configuration. Default value: `false`
`auth.group.mapping`	Specify whether to also link to an external authorization server. Specify `true` to link to an external authorization server. Specify `false` to not to link to an external authorization server. Default value: `false`

Table 38 Setup items in the exauth.properties file for LDAP authentication (when directly specifying information about the external authentication server)

Attributes	Details
`protocol`[#1]	Specify the protocol for connecting to the LDAP directory server. This attribute is required. When communicating in plain text format, specify `ldap`. When using StartTLS communication, specify `tls`. Before specifying `tls`, make sure that one of the following encryption methods can be used on the LDAP directory server. • TLS_RSA_WITH_AES_256_GCM_SHA384 • TLS_RSA_WITH_AES_256_CBC_SHA256 • TLS_RSA_WITH_AES_256_CBC_SHA • TLS_RSA_WITH_AES_128_CBC_SHA256 • TLS_RSA_WITH_AES_128_CBC_SHA • SSL_RSA_WITH_3DES_EDE_CBC_SHA Specifiable values: `ldap` or `tls` Default value: none
`host`[#2]	Specify the host name or IP address of the LDAP directory server. If you specify the host name, make sure beforehand that the host name can be resolved to an IP address. If you specify the IP address, you can use either an IPv4 or IPv6 address. When specifying an IPv6 address, enclose it in square brackets (`[]`). This attribute is required. Default value: none
`port`	Specify the port number of the LDAP directory server. Make sure beforehand that the port you specify is set as the listen port number on the LDAP directory server. Specifiable values: 1 to 65535 Default value: 389
`timeout`	Specify the amount of time to wait before timing out when connecting to the LDAP directory server. If you specify `0`, the system waits until a communication error occurs without timing out. Specifiable values: 0 to 120 (seconds)

Attributes	Details
	Default value: 15
attr	Specify the attribute (Attribute Type) to use as the user ID during authentication. • For the hierarchical structure model Specify the name of the attribute containing the unique value to be used for identifying the user. The value stored in this attribute will be used as the user ID for Hitachi Command Suite products.#3 For example, if you are using Active Directory and you want to use the Windows logon ID for the user ID of a Hitachi Command Suite product, specify the attribute name sAMAccountName in which the Windows logon ID has been defined. • For the flat model Specify the RDN attribute name of the user entry. For example, if the user's DN is uid=John,ou=People,dc=example,dc=com, specify the uid that is the attribute name of the uid=John. sAMAccountName has been set as the initial value. This attribute is required. Default value: none
basedn	Specify the BaseDN, which is the DN of the entry that will be used as the start point when searching for LDAP user information on the LDAP directory server. The user entries that are located in the hierarchy below this DN will be checked during authentication. If characters that need to be escaped are included in the specified BaseDN, escape all of those characters correctly because the specified value will be passed to the LDAP directory server without change. • For the hierarchical structure model Specify the DN of the hierarchy that includes all of the user entries to be searched. • For the flat model Specify the DN of the hierarchy just above the user entries to be searched. This attribute is required. Specify the DN by following the rules defined in RFC4514. For example, if any of the following characters are included in a DN, you need to use a backslash (\) to escape each character. Spaces # + ; , < = > \ Default value: none
retry.interval	Specify the retry interval (in seconds) for when an attempt to connect to the LDAP directory server fails. Specifiable values: 1 to 60 (seconds) Default value: 1
retry.times	Specify the number of retries to attempt when an attempt to connect to the LDAP directory server fails. If you specify 0, no retries are attempted. Specifiable values: 0 to 50 Default value: 20

Attributes	Details
`domain.name`	Specify the name of a domain for external authentication servers managed by the LDAP directory server. This item is required when an external authorization server is also linked to. Default value: none
`domain`	Specify the name of a domain for multi-domain configurations managed by the LDAP directory server. If you log in by using a user ID that includes the domain name specified in this attribute, the LDAP directory server that belongs to the specified domain will be used as the authentication server. When specifying a domain name for the server identification name of each LDAP directory server, do not specify the same domain name more than once. This value is not case sensitive. This item is required when a multi-domain configuration is used. Default value: none
`dns_lookup`	Specify `false`. Default value: `false`
Note: To specify the attributes, use the following syntax: `auth.ldap.`*`auth.server.name-property-value.attribute=value`	

#1:

When communicating by using StartTLS as the protocol for connecting to the LDAP directory server, you need to specify the security settings of Common Component.

#2:

When using StartTLS as the protocol for connecting to the LDAP directory server, in the `host` attribute specify the same host name as the value of CN in the LDAP directory server certificate. You cannot use an IP address.

#3:

The specified attribute must not include characters that cannot be used in a user ID of the Hitachi Command Suite product.

Table 39 Setup items in the exauth.properties file for LDAP authentication (when an external authentication server and StartTLS are used for communication)

Property	Details
`auth.ocsp.enable`	Specify whether or not to verify the validity of an LDAP directory server's electronic signature certificate by using an OCSP responder

Property	Details
	when the LDAP directory server and StartTLS are used for communication. If you want to verify the validity of certificates, specify `true`. To not verify the validity of certificates, specify `false`. Default value: `false`
`auth.ocsp.responderURL`	Specify the URL of an OCSP responder if you want to use an OCSP responder that is not the one written in the AIA field of the electronic signature certificate to verify the validity of the electronic signature certificate. If this value is omitted, the OCSP responder written in the AIA field is used. Default value: None

Table 40 Setup items in the exauth.properties file for LDAP authentication (when using the DNS server to look up information about the external authentication server)

Attributes	Details
`protocol`	Specify the protocol for connecting to the LDAP directory server. This attribute is required. Specifiable values: `ldap` Default value: none
`port`	Specify the port number of the LDAP directory server. Make sure beforehand that the port you specify is set as the listen port number on the LDAP directory server. Specifiable values: 1 to 65535 Default value: 389
`timeout`	Specify the amount of time to wait before timing out when connecting to the LDAP directory server. If you specify `0`, the system waits until a communication error occurs without timing out. Specifiable values: 0 to 120 (seconds) Default value: 15
`attr`	Specify the attribute (Attribute Type) to use as the user ID during authentication. • For the hierarchical structure model Specify the name of the attribute containing the unique value to be used for identifying the user. The value stored in this attribute will be used as the user ID for Hitachi Command Suite products.# For example, if you are using Active Directory and you want to use the Windows logon ID for the user ID of a Hitachi Command Suite product, specify the attribute name `sAMAccountName` in which the Windows logon ID has been defined. • For the flat model Specify the RDN attribute name of the user entry. For example, if the user's DN is `uid=John,ou=People,dc=example,dc=com`, specify the `uid` that is the attribute name of the `uid=John`.

Attributes	Details
	`sAMAccountName` has been set as the initial value. This attribute is required. Default value: none
`basedn`	Specify the BaseDN, which is the DN of the entry that will be used as the start point when searching for LDAP user information on the LDAP directory server. The user entries that are located in the hierarchy below this DN will be checked during authentication. If characters that need to be escaped are included in the specified BaseDN, escape all of those characters correctly because the specified value will be passed to the LDAP directory server without change. • For the hierarchical structure model Specify the DN of the hierarchy that includes all of the user entries to be searched. • For the flat model Specify the DN of the hierarchy just above the user entries to be searched. This attribute is required. Specify the DN by following the rules defined in RFC4514. For example, if any of the following characters are included in a DN, you need to use a backslash (`\`) to escape each character. Spaces `# + ; , < = > \` Default value: none
`retry.interval`	Specify the retry interval (in seconds) for when an attempt to connect to the LDAP directory server fails. Specifiable values: 1 to 60 (seconds) Default value: 1
`retry.times`	Specify the number of retries to attempt when an attempt to connect to the LDAP directory server fails. If you specify 0, no retries are attempted. Specifiable values: 0 to 50 Default value: 20
`domain.name`	Specify the name of a domain for external authentication servers managed by the LDAP directory server. Default value: none
`dns_lookup`	Specify `true`. However, if the following attribute values are already set, the LDAP directory server will be connected to by using the user-specified values instead of by using the DNS server to look up the information. • `auth.ldap.`*`auth.server.name-property-value`*`.host` • `auth.ldap.`*`auth.server.name-property-value`*`.port` Default value: `false`
Note: To specify the attributes, use the following syntax: `auth.ldap.`*`auth.server.name-property-value.attribute=value`	

#:

The specified attribute must not include invalid characters that cannot be used in a user ID of the Hitachi Command Suite product.

Examples of setting the exauth.properties file for LDAP authentication

Examples of how to set the `exauth.properties` file when using an LDAP directory server to perform authentication are provided below.

- When directly specifying information about an LDAP directory server (when linking to only an external authentication server)

```
auth.server.type=ldap
auth.server.name=ServerName
auth.group.mapping=false
auth.ocsp.enable=false
auth.ocsp.responderURL=
auth.ldap.ServerName.protocol=ldap
auth.ldap.ServerName.host=ldap.example.com
auth.ldap.ServerName.port=389
auth.ldap.ServerName.timeout=15
auth.ldap.ServerName.attr=sAMAccountName
auth.ldap.ServerName.basedn=dc=Example,dc=com
auth.ldap.ServerName.retry.interval=1
auth.ldap.ServerName.retry.times=20
auth.ldap.ServerName.dns_lookup=false
```

- When using the DNS server to look up an LDAP directory server (when linking to only an external authentication server)

```
auth.server.type=ldap
auth.server.name=ServerName
auth.group.mapping=false
auth.ldap.ServerName.protocol=ldap
auth.ldap.ServerName.timeout=15
auth.ldap.ServerName.attr=sAMAccountName
auth.ldap.ServerName.basedn=dc=Example,dc=com
auth.ldap.ServerName.retry.interval=1
auth.ldap.ServerName.retry.times=20
auth.ldap.ServerName.domain.name=EXAMPLE.COM
auth.ldap.ServerName.dns_lookup=true
```

- When directly specifying information about the LDAP directory server (when also linking to an authorization server)

```
auth.server.type=ldap
auth.server.name=ServerName
auth.group.mapping=true
auth.ocsp.enable=false
auth.ocsp.responderURL=
auth.ldap.ServerName.protocol=ldap
auth.ldap.ServerName.host=ldap.example.com
auth.ldap.ServerName.port=389
auth.ldap.ServerName.timeout=15
auth.ldap.ServerName.attr=sAMAccountName
auth.ldap.ServerName.basedn=dc=Example,dc=com
auth.ldap.ServerName.retry.interval=1
```

```
auth.ldap.ServerName.retry.times=20
auth.ldap.ServerName.domain.name=EXAMPLE.COM
auth.ldap.ServerName.dns_lookup=false
```

- When using the DNS server to look up the LDAP directory server (when also linking to an authorization server)

```
auth.server.type=ldap
auth.server.name=ServerName
auth.group.mapping=true
auth.ldap.ServerName.protocol=ldap
auth.ldap.ServerName.timeout=15
auth.ldap.ServerName.attr=sAMAccountName
auth.ldap.ServerName.basedn=dc=Example,dc=com
auth.ldap.ServerName.retry.interval=1
auth.ldap.ServerName.retry.times=20
auth.ldap.ServerName.domain.name=EXAMPLE.COM
auth.ldap.ServerName.dns_lookup=true
```

- When using a redundant configuration

```
auth.server.type=ldap
auth.server.name=ServerName1,ServerName2
auth.ldap.multi_domain=false
auth.group.mapping=false
auth.ldap.ServerName1.protocol=ldap
auth.ldap.ServerName1.host=ldap1.example.com
auth.ldap.ServerName1.port=389
auth.ldap.ServerName1.timeout=15
auth.ldap.ServerName1.attr=sAMAccountName
auth.ldap.ServerName1.basedn=dc=Example,dc=com
auth.ldap.ServerName1.retry.interval=1
auth.ldap.ServerName1.retry.times=20
auth.ldap.ServerName2.protocol=ldap
auth.ldap.ServerName2.host=ldap2.example.com
auth.ldap.ServerName2.port=389
auth.ldap.ServerName2.timeout=15
auth.ldap.ServerName2.attr=sAMAccountName
auth.ldap.ServerName2.basedn=dc=Example,dc=net
auth.ldap.ServerName2.retry.interval=1
auth.ldap.ServerName2.retry.times=20
```

- When using a multi-domain configuration

```
auth.server.type=ldap
auth.server.name=ServerName1,ServerName2
auth.ldap.multi_domain=true
auth.group.mapping=false
auth.ldap.ServerName1.protocol=ldap
auth.ldap.ServerName1.host=ldap1.example.com
auth.ldap.ServerName1.port=389
auth.ldap.ServerName1.timeout=15
auth.ldap.ServerName1.attr=sAMAccountName
auth.ldap.ServerName1.basedn=dc=Example,dc=com
auth.ldap.ServerName1.retry.interval=1
auth.ldap.ServerName1.retry.times=20
auth.ldap.ServerName1.domain=example.com
auth.ldap.ServerName2.protocol=ldap
auth.ldap.ServerName2.host=ldap2.example.com
```

```
auth.ldap.ServerName2.port=389
auth.ldap.ServerName2.timeout=15
auth.ldap.ServerName2.attr=sAMAccountName
auth.ldap.ServerName2.basedn=dc=Example,dc=net
auth.ldap.ServerName2.retry.interval=1
auth.ldap.ServerName2.retry.times=20
auth.ldap.ServerName2.domain=example.net
```

Setup items in the exauth.properties file for RADIUS authentication

In the `exauth.properties` file, set the type of the external authentication server to be used, the server identification name, and the machine information about the external authentication server.

- Common properties
  Table 41 Setup items in the exauth.properties file for RADIUS authentication (common items) on page 190
- Properties for an external authentication server
  Specify these property values for each RADIUS server.
  Table 42 Setup items in the exauth.properties file for RADIUS authentication (settings for the external authentication server) on page 190
- Properties for an external authorization server
  These properties need to be set when an external authorization server is also linked to. Specify information about the LDAP directory server for each domain.
  Setup items in the `exauth.properties` file vary depending on whether information about the LDAP directory server being connected to is directly specified or looked up by using the DNS server.
  - When directly specifying information about the LDAP directory server
    Table 43 Setup items in the exauth.properties file for RADIUS authentication (common settings for the external authorization server) on page 192
    Table 44 Setup items in the exauth.properties file for RADIUS authentication (when directly specifying information about the external authorization server) on page 193
    Table 45 Setup items in the exauth.properties file for RADIUS authentication (when an external authorization server and StartTLS are used for communication) on page 195
  - When using the DNS server to look up the information about the LDAP directory server
    Table 43 Setup items in the exauth.properties file for RADIUS authentication (common settings for the external authorization server) on page 192
    Table 46 Setup items in the exauth.properties file for RADIUS authentication (when using the DNS server to look up information about the external authorization server) on page 195

Note:

- Make sure to distinguish between uppercase and lowercase letters for property settings.
- To use StartTLS for communication between the management server and the LDAP directory server, you need to directly specify information about the LDAP directory server to connect to in the `exauth.properties` file.
- If you use the DNS server to look up the LDAP directory server to connect to, it might take longer for users to log in.

Table 41 Setup items in the exauth.properties file for RADIUS authentication (common items)

Property names	Details
`auth.server.type`	Specify an external authentication server type. Specify `radius`. Default value: `internal` (used when not linking to an external authentication server)

`auth.server.name`	Specify the server identification names of RADIUS servers. You can specify any name for this property in order to identify which RADIUS servers the settings such as the port number and the protocol for connecting to the RADIUS server (see Table 42 Setup items in the exauth.properties file for RADIUS authentication (settings for the external authentication server) on page 190) are applied to. `ServerName` has been set as the initial value. You must specify at least one name. When configuring a redundant configuration, separate the server identification name of each server with a comma (,). Do not register the same server identification name more than once.
	
	Specifiable values: No more than 64 bytes of the following characters:
	
	`A` to `Z`
	
	`a` to `z`
	
	`0` to `9`
	
	`! # ( ) + - . = @ [ ] ^ _ { } ~`
	
	Default value: none

`auth.group.mapping`	Specify whether to also link to an external authorization server. Specify `true` to link to an external authorization server. Specify `false` to not to link to an external authorization server. Default value: `false`

Table 42 Setup items in the exauth.properties file for RADIUS authentication (settings for the external authentication server)

Attributes	Details
`protocol`	Specify the protocol for RADIUS server authentication. This attribute is required.

Attributes	Details
	Specifiable values: PAP or CHAP Default value: none
host[#1]	Specify the host name or IP address of the RADIUS server. If you specify the host name, make sure beforehand that the host name can be resolved to an IP address. If you specify the IP address, you can use either an IPv4 or IPv6 address. When specifying an IPv6 address, enclose it in square brackets ([]). This attribute is required. Default value: none
port	Specify the port number for RADIUS server authentication. Make sure beforehand that the port you specify is set as the listen port number on the RADIUS server. Specifiable values: 1 to 65535 Default value: 1812
timeout	Specify the amount of time to wait before timing out when connecting to the RADIUS server. Specifiable values: 1 to 65535 (seconds) Default value: 1
retry.times	Specify the number of retries to attempt when an attempt to connect to the RADIUS server fails. If you specify 0, no retries are attempted. Specifiable values: 0 to 50 Default value: 3
attr.NAS-Identifier[#2]	Specify the host name of the Device Manager management server. The RADIUS server uses this attribute value to identify the management server. The host name of the management server has been set as the initial value. Specifiable values: Specify no more than 253 bytes of the following characters: A to Z a to z 0 to 9 ! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ ` { | } ~ Default value: none
attr.NAS-IP-Address[#2]	Specify the IPv4 address of the Device Manager management server. The RADIUS server uses this attribute value to identify the management server. If the format of the address is invalid, this property is disabled. Default value: none

Attributes	Details
attr.NAS-IPv6-Address[#2]	Specify the IPv6 address of the Device Manager management server. The RADIUS server uses this attribute value to identify the management server. Enclose the IPv6 address in square brackets ([]). If the format of the address is invalid, this property is disabled. Default value: none
Note: To specify the attributes, use the following syntax: auth.radius.*auth.server.name-property-value.attribute=value*	

#1:

When linking to an external authorization server that is running on the same computer and using StartTLS as the protocol for connecting to the LDAP directory server, in the `host` attribute specify the same host name as the value of CN in the LDAP directory server certificate. You cannot use an IP address.

#2:

You must specify exactly one of the following: `attr.NAS-Identifier`, `attr.NAS-IP-Address`, or `attr.NAS-IPv6-Address`.

Table 43 Setup items in the exauth.properties file for RADIUS authentication (common settings for the external authorization server)

Attributes	Details
domain.name	Specify the name of a domain managed by the LDAP directory server. This item is required when an external authorization server is also linked to. Default value: none
dns_lookup	Specify whether to use the DNS server to look up the information about the LDAP directory server. If you want to directly specify information about the LDAP directory server in the `exauth.properties` file, specify `false`. If you want to use the DNS server to look up the information, specify `true`. However, if the following attribute values are already set, the LDAP directory server will be connected to by using the user-specified values instead of by using the DNS server to look up the information. • auth.group.*domain-name*.host • auth.group.*domain-name*.port Default value: `false`

Attributes	Details
Note: To specify the attributes, use the following syntax: auth.radius.*auth.server.name-property-value.attribute=value*	

Table 44 Setup items in the exauth.properties file for RADIUS authentication (when directly specifying information about the external authorization server)

Attributes	Details
protocol[#1]	Specify the protocol for connecting to the LDAP directory server. When communicating in plain text format, specify ldap. When using StartTLS communication, specify tls. Before specifying tls, make sure that one of the following encryption methods can be used on the LDAP directory server. • TLS_RSA_WITH_AES_256_GCM_SHA384 • TLS_RSA_WITH_AES_256_CBC_SHA256 • TLS_RSA_WITH_AES_256_CBC_SHA • TLS_RSA_WITH_AES_128_CBC_SHA256 • TLS_RSA_WITH_AES_128_CBC_SHA • SSL_RSA_WITH_3DES_EDE_CBC_SHA Specifiable values: ldap or tls Default value: ldap
host[#2]	If the external authentication server and the external authorization server are running on different computers, specify the host name or IP address of the LDAP directory server. If you specify the host name, make sure beforehand that the host name can be resolved to an IP address. If you specify the IP address, you can use either an IPv4 or IPv6 address. When specifying an IPv6 address, enclose it in square brackets ([]). If you omit this attribute, the external authentication server and the external authorization server are assumed to be running on the same computer. Default value: none
port	Specify the port number of the LDAP directory server. Make sure beforehand that the port you specify is set as the listen port number on the LDAP directory server. Specifiable values: 1 to 65535 Default value: 389
basedn	Specify the BaseDN, which is the DN of the entry that will be used as the start point when searching for LDAP user information on the LDAP directory server. The user entries that are located in the hierarchy below this DN will be checked during authorization. Specify the DN of the hierarchy that includes all of the user entries to be searched.

Attributes	Details
	Specify the DN by following the rules defined in RFC4514. For example, if any of the following characters are included in a DN, you need to use a backslash (\) to escape each character. Spaces # + ; , < = > \ If characters that need to be escaped are included in the specified BaseDN, escape all of those characters correctly because the specified value will be passed to the LDAP directory server without change. If you omit this attribute, the value specified in the defaultNamingContext property of Active Directory is assumed as the BaseDN. Default value: none
timeout	Specify the amount of time to wait before timing out when connecting to the LDAP directory server. If you specify 0, the system waits until a communication error occurs without timing out. Specifiable values: 0 to 120 (seconds) Default value: 15
retry.interval	Specify the retry interval (in seconds) for when an attempt to connect to the LDAP directory server fails. Specifiable values: 1 to 60 (seconds) Default value: 1
retry.times	Specify the number of retries to attempt when an attempt to connect to the LDAP directory server fails. If you specify 0, no retries are attempted. Specifiable values: 0 to 50 Default value: 20
Note: To specify the attributes, use the following syntax: auth.group.*domain-name*.*attribute*=*value* For *domain-name*, specify the value specified for auth.radius.*auth.server.name-property-value*.domain.name.	

#1:

When communicating by using StartTLS as the protocol for connecting to the LDAP directory server, you need to specify the security settings of Common Component.

#2:

When the external authentication server and the external authorization server are running on different computers and when using StartTLS as the protocol for connecting to the LDAP directory server, in the host attribute specify the same host name as the value of CN in the LDAP directory server certificate. You cannot use an IP address.

Table 45 Setup items in the exauth.properties file for RADIUS authentication (when an external authorization server and StartTLS are used for communication)

Property	Details
`auth.ocsp.enable`	Specify whether or not to verify the validity of an LDAP directory server's electronic signature certificate by using an OCSP responder when the LDAP directory server and StartTLS are used for communication. If you want to verify the validity of certificates, specify `true`. To not verify the validity of certificates, specify `false`. Default value: `false`
`auth.ocsp.responderURL`	Specify the URL of an OCSP responder if you want to use an OCSP responder that is not the one written in the AIA field of the electronic signature certificate to verify the validity of the electronic signature certificate. If this value is omitted, the OCSP responder written in the AIA field is used. Default value: None

Table 46 Setup items in the exauth.properties file for RADIUS authentication (when using the DNS server to look up information about the external authorization server)

Attributes	Details
`protocol`	Specify the protocol for connecting to the LDAP directory server. Specifiable values: `ldap` Default value: `ldap`
`port`	Specify the port number of the LDAP directory server. Make sure beforehand that the port you specify is set as the listen port number on the LDAP directory server. Specifiable values: 1 to 65535 Default value: 389
`basedn`	Specify the BaseDN, which is the DN of the entry that will be used as the start point when searching for LDAP user information on the LDAP directory server. The user entries that are located in the hierarchy below this DN will be checked during authorization. Specify the DN of the hierarchy that includes all of the user entries to be searched. Specify the DN by following the rules defined in RFC4514. For example, if any of the following characters are included in a DN, you need to use a backslash (`\`) to escape each character. Spaces `# + ; , < = > \` If characters that need to be escaped are included in the specified BaseDN, escape all of those characters correctly because the specified value will be passed to the LDAP directory server without change.

Attributes	Details
	If you omit this attribute, the value specified in the `defaultNamingContext` property of Active Directory is assumed as the BaseDN. Default value: none
`timeout`	Specify the amount of time to wait before timing out when connecting to the LDAP directory server. If you specify `0`, the system waits until a communication error occurs without timing out. Specifiable values: 0 to 120 (seconds) Default value: 15
`retry.interval`	Specify the retry interval (in seconds) for when an attempt to connect to the LDAP directory server fails. Specifiable values: 1 to 60 (seconds) Default value: 1
`retry.times`	Specify the number of retries to attempt when an attempt to connect to the LDAP directory server fails. If you specify 0, no retries are attempted. Specifiable values: 0 to 50 Default value: 20
Note: To specify the attributes, use the following syntax: `auth.group.`*`domain-name`*`.`*`attribute`*`=`*`value`* For *domain-name*, specify the value specified for `auth.radius.`*`auth.server.name-property-value`*`.domain.name`.	

Examples of setting the exauth.properties file for RADIUS authentication

Examples of how to set the `exauth.properties` file when using a RADIUS server to perform authentication are provided below.

- When linking to only an external authentication server

```
auth.server.type=radius
auth.server.name=ServerName
auth.group.mapping=false
auth.radius.ServerName.protocol=PAP
auth.radius.ServerName.host=radius.example.com
auth.radius.ServerName.port=1812
auth.radius.ServerName.timeout=1
auth.radius.ServerName.retry.times=3
auth.radius.ServerName.attr.NAS-Identifier=host_A
```

- When directly specifying information about an external authorization server

```
auth.server.type=radius
auth.server.name=ServerName
auth.group.mapping=true
```

```
auth.ocsp.enable=false
auth.ocsp.responderURL=
auth.radius.ServerName.protocol=PAP
auth.radius.ServerName.host=radius.example.com
auth.radius.ServerName.port=1812
auth.radius.ServerName.timeout=1
auth.radius.ServerName.retry.times=3
auth.radius.ServerName.attr.NAS-Identifier=host_A
auth.radius.ServerName.domain.name=EXAMPLE.COM
auth.radius.ServerName.dns_lookup=false
auth.group.EXAMPLE.COM.protocol=ldap
auth.group.EXAMPLE.COM.host=ldap.example.com
auth.group.EXAMPLE.COM.port=389
auth.group.EXAMPLE.COM.basedn=dc=Example,dc=com
auth.group.EXAMPLE.COM.timeout=15
auth.group.EXAMPLE.COM.retry.interval=1
auth.group.EXAMPLE.COM.retry.times=20
```

- When using the DNS server to look up an external authorization server

```
auth.server.type=radius
auth.server.name=ServerName
auth.group.mapping=true
auth.radius.ServerName.protocol=PAP
auth.radius.ServerName.host=radius.example.com
auth.radius.ServerName.port=1812
auth.radius.ServerName.timeout=1
auth.radius.ServerName.retry.times=3
auth.radius.ServerName.attr.NAS-Identifier=host_A
auth.radius.ServerName.domain.name=EXAMPLE.COM
auth.radius.ServerName.dns_lookup=true
auth.group.EXAMPLE.COM.protocol=ldap
auth.group.EXAMPLE.COM.basedn=dc=Example,dc=com
auth.group.EXAMPLE.COM.timeout=15
auth.group.EXAMPLE.COM.retry.interval=1
auth.group.EXAMPLE.COM.retry.times=20
```

- When using a redundant configuration

```
auth.server.type=radius
auth.server.name=ServerName1,ServerName2
auth.group.mapping=false
auth.radius.ServerName1.protocol=PAP
auth.radius.ServerName1.host=radius1.example.com
auth.radius.ServerName1.port=1812
auth.radius.ServerName1.timeout=1
auth.radius.ServerName1.retry.times=3
auth.radius.ServerName1.attr.NAS-IP-Address=127.0.0.1
auth.radius.ServerName2.protocol=PAP
auth.radius.ServerName2.host=radius2.example.com
auth.radius.ServerName2.port=1812
auth.radius.ServerName2.timeout=1
auth.radius.ServerName2.retry.times=3
auth.radius.ServerName2.attr.NAS-IP-Address=127.0.0.1
```

Setup items in the exauth.properties file for Kerberos authentication

In the `exauth.properties` file, specify the type of the external authentication server, the server identification name, and the information about the external authentication server.

- Common properties
  Table 47 Setup items in the exauth.properties file for Kerberos authentication (common items) on page 199
- Properties for an external authentication server
  Specify these property values for each Kerberos server.
  Setup items in the `exauth.properties` file vary depending on whether information about the Kerberos server being connected to is directly specified or looked up by using the DNS server.
  - When directly specifying information about the Kerberos server:
    Table 48 Setup items in the exauth.properties file for Kerberos authentication (when directly specifying information about the external authentication server) on page 199
  - When using the DNS server to look up information about the Kerberos server:
    Table 49 Setup items in the exauth.properties file for Kerberos authentication (when using the DNS server to look up information about the external authentication server) on page 201
- Properties for an external authorization server
  These properties need to be set if you directly specify information about the Kerberos server and an external authorization server is also linked.
  Specify the properties for each realm.
  Table 50 Setup items in the exauth.properties file for Kerberos authentication (settings for the external authorization server) on page 202
  Table 51 Setup items in the exauth.properties file for Kerberos authentication (when an external authorization server and StartTLS are used for communication) on page 203

Note:

- Make sure to distinguish between uppercase and lowercase letters for property settings.
- To use StartTLS for communication between the management server and the LDAP directory server, you need to directly specify information about the LDAP directory server to connect to in the `exauth.properties` file.
- If you use the DNS server to look up the LDAP directory server to connect to, it might take longer for users to log in.

Table 47 Setup items in the exauth.properties file for Kerberos authentication (common items)

Property names	Details
`auth.server.type`	Specify an external authentication server type. Specify `kerberos`. Default value: `internal` (used when not linking to an external authentication server)
`auth.group.mapping`	Specify whether to also link to an external authorization server. Specify `true` to link to an external authorization server. Specify `false` to not to link to an external authorization server. Default value: `false`

Table 48 Setup items in the exauth.properties file for Kerberos authentication (when directly specifying information about the external authentication server)

Attributes	Details
`default_realm`	Specify the default realm name. If you specify a user ID but not a realm name in the login window of the GUI, the user is authenticated as a user who belongs to the realm specified for this attribute. This attribute is required. Default value: none
`dns_lookup_kdc`	Specify `false`. Default value: `false`
`default_tkt_enctypes`	Specify the encryption type used for Kerberos authentication. This property is enabled only if the management server OS is Windows. You can use the following encryption types: • aes128-cts • rc4-hmac • des3-cbc-sha1 • des-cbc-md5 • des-cbc-crc If you want to specify multiple encryption types, use a comma to separate the encryption types. Among the specified encryption types, an encryption type that is supported by both the management server OS and a Kerberos server will be used. Default value: None (DES-CBC-MD5 is used for authentication.)
`clockskew`	Specify the acceptable range of difference between the management server time and Kerberos server time. If the difference exceeds this value, an authentication error occurs.

Attributes	Details
	Specifiable values: 0 to 300 (seconds) Default value: 300
timeout	Specify the amount of time to wait before timing out when connecting to the Kerberos server. If you specify 0, the system waits until a communication error occurs without timing out. Specifiable values: 0 to 120 (seconds) Default value: 3
realm_name	Specify the realm identification names. You can specify any name for this attribute in order to identify which realms the property attribute settings are applied to. You must specify at least one name. When specifying multiple realm identification names, separate the names with commas (,). Do not register the same realm identification name more than once. Default value: none
value-specified-for-realm_name.realm	Specify the name of the realm set in the Kerberos server. This attribute is required. Default value: none
value-specified-for-realm_name.kdc#	Specify the information about the Kerberos server in the following format: *host-name-or-IP-address*[:*port-number*] This attribute is required. ***host-name-or-IP-address*** If you specify the host name, make sure beforehand that the name can be resolved to an IP address. If you specify the IP address, use an IPv4 address. In an IPv6 environment, you must specify the host name. Note that you cannot specify the loopback address (localhost or 127.0.0.1). ***port-number*** Make sure beforehand that the port you specify is set as the listen port number on the Kerberos server. If you do not specify a port number or the specified port number cannot be used in a Kerberos server, 88 is assumed. When configuring the Kerberos server in redundant configuration, separate the servers with commas (,) as follows: *host-name-or-IP-address*[:*port-number*] ,*host-name-or-IP-address*[:*port-number*],...
Note:	

Attributes	Details
To specify the attributes, use the following syntax: `auth.kerberos.`*`attribute`*`=`*`value`*	

#:

When using StartTLS as the protocol for connecting to the external authorization server, specify the same host name as the value of CN in the external authorization server certificate. You cannot use an IP address.

Table 49 Setup items in the exauth.properties file for Kerberos authentication (when using the DNS server to look up information about the external authentication server)

Attributes	Details
`default_realm`	Specify the default realm name. If you specify a user ID but not a realm name in the login window of the GUI, the user is authenticated as a user who belongs to the realm specified for this attribute. This attribute is required. Default value: none
`dns_lookup_kdc`	Specify `true`. This attribute is required. However, if all the following attributes values are already set, the Kerberos server will not be looked up by using the DNS server. • `realm_name` • *`value-specified-for-realm_name`*`.realm` • *`value-specified-for-realm_name`*`.kdc`
`default_tkt_enctypes`	Specify the encryption type used for Kerberos authentication. This property is enabled only if the management server OS is Windows. You can use the following encryption types: • aes128-cts • rc4-hmac • des3-cbc-sha1 • des-cbc-md5 • des-cbc-crc If you want to specify multiple encryption types, use a comma to separate the encryption types. Among the specified encryption types, an encryption type that is supported by both the management server OS and a Kerberos server will be used. Default value: None (DES-CBC-MD5 is used for authentication.)
`clockskew`	Specify the acceptable range of difference between the management server time and Kerberos server time. If the difference exceeds this value, an authentication error occurs. Specifiable values: 0 to 300 (seconds)

Attributes	Details
	Default value: 300
timeout	Specify the amount of time to wait before timing out when connecting to the Kerberos server. If you specify 0, the system waits until a communication error occurs without timing out. Specifiable values: 0 to 120 (seconds) Default value: 3
Note: To specify the attributes, use the following syntax: auth.kerberos.*attribute=value*	

Table 50 Setup items in the exauth.properties file for Kerberos authentication (settings for the external authorization server)

Attributes	Details
protocol#	Specify the protocol for connecting to the LDAP directory server. When communicating in plain text format, specify ldap. When using StartTLS communication, specify tls. StartTLS communication can be used only when directly specifying information about the Kerberos server. Before specifying tls, make sure that one of the following encryption methods can be used on the LDAP directory server. • TLS_RSA_WITH_AES_256_GCM_SHA384 • TLS_RSA_WITH_AES_256_CBC_SHA256 • TLS_RSA_WITH_AES_256_CBC_SHA • TLS_RSA_WITH_AES_128_CBC_SHA256 • TLS_RSA_WITH_AES_128_CBC_SHA • SSL_RSA_WITH_3DES_EDE_CBC_SHA Specifiable values: ldap or tls Default value: ldap
port	Specify the port number of the LDAP directory server. Make sure beforehand that the port you specify is set as the listen port number on the LDAP directory server. Specifiable values: 1 to 65535 Default value: 389
basedn	Specify the BaseDN, which is the DN of the entry that will be used as the start point when searching for LDAP user information on the LDAP directory server. The user entries that are located in the hierarchy below this DN will be checked during authorization. Specify the DN of the hierarchy that includes all of the user entries to be searched. Specify the DN by following the rules defined in RFC4514. For example, if any of the following characters are included in a DN, you need to use a backslash (\) to escape each character.

Attributes	Details
	Spaces # + ; , < = > \ If characters that need to be escaped are included in the specified BaseDN, escape all of those characters correctly because the specified value will be passed to the LDAP directory server without change. If you omit this attribute, the value specified in the defaultNamingContext property of Active Directory is assumed as the BaseDN. Default value: none
timeout	Specify the amount of time to wait before timing out when connecting to the LDAP directory server. If you specify 0, the system waits until a communication error occurs without timing out. Specifiable values: 0 to 120 (seconds) Default value: 15
retry.interval	Specify the retry interval (in seconds) for when an attempt to connect to the LDAP directory server fails. Specifiable values: 1 to 60 (seconds) Default value: 1
retry.times	Specify the number of retries to attempt when an attempt to connect to the LDAP directory server fails. If you specify 0, no retries are attempted. Specifiable values: 0 to 50 Default value: 20
Note: To specify the attributes, use the following syntax: auth.group.*realm-name*.*attribute*=*value* For *realm-name*, specify the value specified for auth.kerberos.*realm_name-property-value*.realm.	

#:

When communicating by using StartTLS as the protocol for connecting to the LDAP directory server, you need to specify the security settings of Common Component.

Table 51 Setup items in the exauth.properties file for Kerberos authentication (when an external authorization server and StartTLS are used for communication)

Property	Details
auth.ocsp.enable	Specify whether or not to verify the validity of an LDAP directory server's electronic signature certificate by using an OCSP responder when the LDAP directory server and StartTLS are used for communication.

Property	Details
	If you want to verify the validity of certificates, specify `true`. To not verify the validity of certificates, specify `false`. Default value: `false`
`auth.ocsp.responderURL`	Specify the URL of an OCSP responder if you want to use an OCSP responder that is not the one written in the AIA field of the electronic signature certificate to verify the validity of the electronic signature certificate. If this value is omitted, the OCSP responder written in the AIA field is used. Default value: None

Examples of setting the exauth.properties file for Kerberos authentication

Examples of how to set the `exauth.properties` file when using a Kerberos server to perform authentication are provided below.

- When directly specifying information about a Kerberos server (when not linking to an external authorization server)

```
auth.server.type=kerberos
auth.group.mapping=false
auth.kerberos.default_realm=EXAMPLE.COM
auth.kerberos.dns_lookup_kdc=false
auth.kerberos.clockskew=300
auth.kerberos.timeout=3
auth.kerberos.realm_name=RealmName
auth.kerberos.RealmName.realm=EXAMPLE.COM
auth.kerberos.RealmName.kdc=kerberos.example.com:88
```

- When using the DNS server to look up a Kerberos server (when not linking to an external authorization server)

```
auth.server.type=kerberos
auth.group.mapping=false
auth.kerberos.default_realm=EXAMPLE.COM
auth.kerberos.dns_lookup_kdc=true
auth.kerberos.clockskew=300
auth.kerberos.timeout=3
```

- When directly specifying information about a Kerberos server (when also linking to an external authorization server)

```
auth.server.type=kerberos
auth.group.mapping=true
auth.ocsp.enable=false
auth.ocsp.responderURL=
auth.kerberos.default_realm=EXAMPLE.COM
auth.kerberos.dns_lookup_kdc=false
auth.kerberos.clockskew=300
auth.kerberos.timeout=3
auth.kerberos.realm_name=RealmName
auth.kerberos.RealmName.realm=EXAMPLE.COM
auth.kerberos.RealmName.kdc=kerberos.example.com:88
auth.group.EXAMPLE.COM.protocol=ldap
```

```
auth.group.EXAMPLE.COM.port=389
auth.group.EXAMPLE.COM.basedn=dc=Example,dc=com
auth.group.EXAMPLE.COM.timeout=15
auth.group.EXAMPLE.COM.retry.interval=1
auth.group.EXAMPLE.COM.retry.times=20
```

- When using the DNS server to look up a Kerberos server (when also linking to an external authorization server)

```
auth.server.type=kerberos
auth.group.mapping=true
auth.kerberos.default_realm=EXAMPLE.COM
auth.kerberos.dns_lookup_kdc=true
auth.kerberos.clockskew=300
auth.kerberos.timeout=3
```

- When using a redundant configuration

```
auth.server.type=kerberos
auth.group.mapping=false
auth.kerberos.default_realm=EXAMPLE.COM
auth.kerberos.dns_lookup_kdc=false
auth.kerberos.clockskew=300
auth.kerberos.timeout=3
auth.kerberos.realm_name=S1
auth.kerberos.S1.realm=EXAMPLE.COM
auth.kerberos.S1.kdc=kerberos.example.com:
88,kerberos.example.net:88
```

- When specifying multiple realm identifiers

```
auth.server.type=kerberos
auth.group.mapping=false
auth.kerberos.default_realm=EXAMPLE.COM
auth.kerberos.dns_lookup_kdc=false
auth.kerberos.clockskew=300
auth.kerberos.timeout=3
auth.kerberos.realm_name=S1,S2
auth.kerberos.S1.realm=EXAMPLE.COM
auth.kerberos.S1.kdc=kerberos1.example.com:
88,kerberos1.example.net:88
auth.kerberos.S2.realm=EXAMPLE.NET
auth.kerberos.S2.kdc=kerberos2.example.com:
88,kerberos2.example.net:88
```

About a LDAP search user account

An LDAP search user account is used when an account needs to be authenticated or authorized, or when searching for information within an LDAP directory server.

In the following cases, you need to register an LDAP search user account on the management server.

- When an LDAP directory server is used as an external authentication server and the data structure is the hierarchical structure model

- When an LDAP directory server is used as an external authorization server[#]

In cases other than above, this step is not necessary, because LDAP user information is not searched during authentication and authorization. If a user account used to search for LDAP user information has been already registered, delete it.

#:

When registering an authorization group in Hitachi Command Suite products by using the GUI, if you want to check whether the distinguished name of the authorization group is registered on the external authorization server by using a user ID such as the `System` account registered in Hitachi Command Suite products, you need to register a user account used to search for LDAP user information on the management server.

Conditions for LDAP search user account

Conditions for the LDAP search user account vary depending on the authentication method.

Prepare a user account that satisfies the following conditions on the LDAP directory server.

For LDAP authentication:

- The user account can bind to the DN specified for `auth.ldap.`*`auth.server.name-property-value`*`.basedn` in the `exauth.properties` file
- The user account can search the attributes for all entries below the DN specified for `auth.ldap.`*`auth.server.name-property-value`*`.basedn` in the `exauth.properties` file
- The user account can reference the DN specified for `auth.ldap.`*`auth.server.name-property-value`*`.basedn` in the `exauth.properties` file
- The user account can reference the authorization groups that are under the DN specified for `auth.ldap.`*`auth.server.name-property-value`*`.basedn` in the `exauth.properties` file (when an external authorization server is also linked to)
- The user account can search the attributes of the authorization groups that are under the DN specified for `auth.ldap.`*`auth.server.name-property-value`*`.basedn` in the `exauth.properties` file and search the attributes of nested groups of the authorization groups (when an external authorization server is also linked to)

For RADIUS authentication:

- The user account can bind to the DN specified for `auth.group.domain-name.basedn` in the `exauth.properties` file
- The user account can search the attributes for all entries below the DN specified for `auth.group.domain-name.basedn` in the `exauth.properties` file
- The user account can reference the DN specified for `auth.group.domain-name.basedn` in the `exauth.properties` file
- The user account can reference the authorization groups that are under the DN specified for `auth.group.domain-name.basedn` in the `exauth.properties` file.
- The user account can search the attributes of the authorization groups that are under the DN specified for `auth.group.domain-name.basedn` in the `exauth.properties` file and search the attributes of nested groups of the authorization groups

For Kerberos authentication:

- The user account can bind to the DN specified for `auth.group.realm-name.basedn` in the `exauth.properties` file
- The user account can search the attributes for all entries below the DN specified for `auth.group.realm-name.basedn` in the `exauth.properties` file
- The user account can reference the DN specified for `auth.group.realm-name.basedn` in the `exauth.properties` file
- The user account can reference the authorization groups that are under the DN specified for `auth.group.realm-name.basedn` in the `exauth.properties` file
- The user account can search the attributes of the authorization groups that are under the DN specified for `auth.group.realm-name.basedn` in the `exauth.properties` file and search the attributes of nested groups of the authorization groups

Registering an LDAP search user account

Use the `hcmds64ldapuser` command to register the an LDAP search user account on the management server.

Before you begin

- Register an LDAP search user on the LDAP directory server.
- Check the following information:
  - DN and password of the LDAP search user
  - Server identification name or the domain name for external authentication servers of the LDAP directory server (for LDAP authentication)

Specify the server identification name that was specified for the `auth.server.name` property in the `exauth.properties` file, or specify the domain name specified for `auth.ldap.`*`value-specified-for-auth.server.name`*`.domain.name` property in the `exauth.properties` file.

- Domain name of the RADIUS server (for RADIUS authentication)
  Specify the domain name specified for `auth.radius.`*`auth.server.name-property-value`*`.domain.name` in the `exauth.properties` file.
- Realm name of the Kerberos server (for Kerberos authentication)
  If you directly specify information about a Kerberos server in the `exauth.properties` file, specify the value specified for `auth.kerberos.default_realm` or `auth.kerberos.`*`auth.kerberos.realm_name-property-value`*`.realm`.
  If you specify the settings in the `exauth.properties` file to use the DNS server to look up information about a Kerberos server, specify the realm name registered in the DNS server.

Procedure

Execute the `hcmds64ldapuser` command.

In Windows:

`installation-folder-for-Hitachi-Command-Suite``\Base64\bin\hcmds64ldapuser /set /dn `*`DN-of-user-account-used-to-search-for-LDAP-user-info`*` [/pass `*`password-of-user-account-used-to-search-for-LDAP-user-info`*`] /name `*`name`*

In Linux:

`installation-directory-for-Hitachi-Command-Suite/``Base64/bin/hcmds64ldapuser -set -dn `*`DN-of-user-account-used-to-search-for-LDAP-user-info`*` [-pass `*`password-of-user-account-used-to-search-for-LDAP-user-info`*`] -name `*`name`*

- *DN-of-user-account-used-to-search-for-LDAP-user-info*
  Specify a DN by following the rules defined in RFC4514. For example, if the following characters are included in a DN, you need to use a backslash (`\`) to escape each character.
  Spaces `# + , ; < = > \`
- *password-of-user-account-used-to-search-for-LDAP-user-info*
  This is case-sensitive and must exactly match the password registered in the LDAP directory server. If you execute the command without specifying the `pass` option, you will be prompted to enter a password.

Note:

- In the LDAP directory server, you can use double quotation marks (") for the DN and password. In the management server, however, you need to register a user account whose DN and password do not include double quotation marks.
- If you are using Active Directory, you can use the `dsquery` command provided by Active Directory to check the DN of a user. The following example shows how to use the `dsquery` command to check the DN of the user `administrator`, and also shows the execution results:

  ```
  dsquery user -name administrator
  "CN=administrator,CN=admin,DC=example,DC=com"
  ```

- If the DN includes commas such as `cn=administrator,cn=admin,dc=example,com`, specify as follows:

  In Windows:

  ```
  hcmds64ldapuser /set /dn
  "cn=administrator,cn=admin,dc=example\,com" /pass
  administrator_pass /name ServerName
  ```

  In Linux:

  ```
  hcmds64ldapuser -set -dn
  "cn=administrator,cn=admin,dc=example\\,com" -pass
  administrator_pass -name ServerName
  ```

Related references

- Notes on commands for setting up a link to an external authentication server on page 215

Deleting an LDAP search user account

Use the `hcmds64ldapuser` command to delete the LDAP search user account from the management server.

Before you begin

Check the following information:

- Server identification name or the domain name for external authentication servers of the LDAP directory server (for LDAP authentication)
- Domain name of the RADIUS server (for RADIUS authentication)
- Realm name of the Kerberos server (for Kerberos authentication)

Procedure

Execute the `hcmds64ldapuser` command.

In Windows:

```
installation-folder-for-Hitachi-Command-Suite\Base64\bin
\hcmds64ldapuser /delete /name name
```

In Linux:

```
installation-directory-for-Hitachi-Command-Suite/
Base64/bin/hcmds64ldapuser -delete -name name
```

Related references

- Notes on commands for setting up a link to an external authentication server on page 215

Checking the LDAP directory server that registered LDAP search user account

Use the `hcmds64ldapuser` command to check which LDAP directory server has registered the LDAP search user account on the management server.

Procedure

Execute the `hcmds64ldapuser` command.

In Windows:

```
installation-folder-for-Hitachi-Command-Suite\Base64\bin
\hcmds64ldapuser /list
```

In Linux:

```
installation-directory-for-Hitachi-Command-Suite/
Base64/bin/hcmds64ldapuser -list
```

Registering a shared secret

Use the `hcmds64radiussecret` command to register the RADIUS shared secret on the management server.

Before you begin

Check the following information:

- Shared secret
- RADIUS server indication name
  RADIUS-server-indication-name must match a server indication name specified for the `auth.server.name` property in the `exauth.properties` file.

Procedure

Execute the `hcmds64radiussecret` command.

In Windows:

```
installation-folder-for-Hitachi-Command-Suite\Base64\bin
\hcmds64radiussecret [/set shared-secret] /name RADIUS-
server-indication-name
```

In Linux:

```
installation-directory-for-Hitachi-Command-Suite/
Base64/bin/hcmds64radiussecret [-set shared-secret] -name
RADIUS-server-indication-name
```

- If you execute the command without specifying the `set` option, you will be prompted to enter a shared secret.

Related references

- Notes on commands for setting up a link to an external authentication server on page 215

Deleting a shared secret

Use the `hcmds64radiussecret` command to delete the shared secret.

Before you begin

Check the following information:

- RADIUS server indication name.

Procedure

Execute the `hcmds64radiussecret` command.

In Windows:

```
installation-folder-for-Hitachi-Command-Suite\Base64\bin
\hcmds64radiussecret /delete /name RADIUS-server-
indication-name
```

In Linux:

```
installation-directory-for-Hitachi-Command-Suite/
Base64/bin/hcmds64radiussecret -delete -name RADIUS-
server-indication-name
```

Related references

- Notes on commands for setting up a link to an external authentication server on page 215

Checking the RADIUS server that registered a shared secret on the management server

Use the `hcmds64radiussecret` command to check which RADIUS server has registered the shared secret on the management server.

Procedure

Execute the `hcmds64radiussecret` command.

In Windows:

```
installation-folder-for-Hitachi-Command-Suite\Base64\bin
\hcmds64radiussecret /list
```

In Linux:

```
installation-directory-for-Hitachi-Command-Suite/
Base64/bin/hcmds64radiussecret -list
```

Result

The server identification name of the RADIUS server is displayed.

Related references

- Notes on commands for setting up a link to an external authentication server on page 215

Checking connections to an external authentication server and an external authorization server

Use the `hcmds64checkauth` command to check whether the management server is correctly connected to the external authentication server and the external authorization server. If Tuning Manager is remotely connected, perform this operation on the computer on which the Device Manager server is installed.

Before you begin

- Register an external authentication server and an external authorization server
- Check the following information:
  - For LDAP authentication
    Check the user accounts registered on the LDAP directory server. For user IDs, specify the value saved in the attribute specified by

auth.ldap.*value-specified-in-auth.server.name*.attr in the exauth.properties file.

- For RADIUS authentication
  Check the user accounts registered on the RADIUS server.
- For Kerberos authentication
  When linking only to an external authentication server:
  Check the user accounts that are registered in Hitachi Command Suite products and whose authentication method is Kerberos authentication.
  When also linking to an external authorization server:
  Check the user accounts not registered in Hitachi Command Suite products.
  In addition, if you specify a user who belongs to a realm other than the realm specified for default_realm in the exauth.properties file, also check the realm that the user belongs to. If more than one realm name is specified in the exauth.properties file, check all specified realm names.

Note that you cannot specify a user account whose *user-ID* or *password* begins with a forward slash (/) in Windows, or hyphen (-) in Linux.

Procedure

Execute the hcmds64checkauth command.

In Windows:

```
installation-folder-for-Hitachi-Command-Suite\Base64\bin
\hcmds64checkauth [/user user-ID /pass password] [/
summary]
```

In Linux:

```
installation-directory-for-Hitachi-Command-Suite/
Base64/bin/hcmds64checkauth [-user user-ID -pass password]
[-summary]
```

- If you execute the command without specifying the user option or the pass option, you will be prompted to enter a user ID and password.
- If you execute the command with the summary option specified, the confirmation message is displayed in summary format.

Note: When using the Kerberos authentication method, if more than one realm name is specified in the exauth.properties file,

check the connection for each realm name. In addition, specify user IDs according to the following:

- To specify a user belonging to a realm other than the realm set for `default_realm` in the `exauth.properties` file:
  user-ID@realm-name
- To specify a user who belongs to the realm set for `default_realm` in the `exauth.properties` file:
  You can omit the realm name.
- When using the LDAP authentication method, if the `hcmds64checkauth` command is executed, all connected external authentication servers are checked and the check results for each external authentication server are displayed. For external authentication servers for which the user account specified for the `hcmds64checkauth` command is not registered, an error message indicating that the user account is not registered is displayed in phase 3 of the check result, and confirmation at phase 3 might fail.
  When this occurs, check the connection of each external authentication server by using a user account that is registered to that server.

Result

Settings in the `exauth.properties` file and connections to the external authentication server and external authorization server are checked, and check results are displayed in each of four phases. The following message is displayed if the checking in each phase finishes normally.

`KAPM15004-I The result of the configuration check of Phase phase-number was normal.`

Phase 1

The command verifies that common properties have been correctly specified in the `exauth.properties` file.

Phase 2

The command verifies that the properties for the external authentication server and properties for the external authorization server have been correctly specified in the `exauth.properties` file.

Phase 3

The command verifies that the external authentication server can be connected to.

Phase 4

If an external authorization server is also linked to, the command verifies that the external authorization server can be connected to and authorization groups can be searched.

If an error occurs, find the output message ID in the *Hitachi Command Suite Messages*, and check the cause and action to take for the error.

Related references

- Registering an external authentication server and an external authorization server on page 178
- Notes on commands for setting up a link to an external authentication server on page 215

Notes on commands for setting up a link to an external authentication server

If command line control characters are included in the arguments of commands that will be executed when specifying the settings to link to an external authentication server, escape the characters correctly according to the specifications of the command line.

Also, you need to pay attention to backslashes (`\`) included in the arguments because they are treated specially in the command line.

The following explains how to escape when executing the `hcmds64ldapuser` command, `hcmds64radiussecret` command, or `hcmds64checkauth` command.

In Windows:

If the following characters are included in an argument, enclose the argument in double quotation marks (`"`) or use a caret (`^`) to escape each character:

Spaces `& | ^ < > ( )`

A backslash might be treated as an escape character depending on the character that follows it. Therefore, if a backslash and any of the above characters are included in an argument, use a caret to escape each character rather than enclose the argument in double quotation marks.

Also, if there is a backslash at the end of an argument, escape it by using another backslash.

In Linux:

If the following characters are included in an argument, enclose the argument in double quotation marks or use a backslash to escape each character:

Spaces `# & ' ( ) ~ \ ` < > ; |`

Note that a backslash in an argument is treated as an escape character even if the argument is enclosed in double quotation marks. If a backslash is included in an argument, escape it by using another backslash.

For example, if a shared secret to be registered by the `hcmds64radiussecret` command is `secret01\`, escape it as follows:

In Windows:

```
hcmds64radiussecret /set secret01\\ /name ServerName
```

In Linux:

Use either of the following formats:

```
hcmds64radiussecret -set secret01\\ -name ServerName
```

```
hcmds64radiussecret -set "secret01\\" -name ServerName
```

Encryption types for Kerberos authentication

Configure the Kerberos server so that the encryption types supported by Hitachi Command Suite products can be used.

In Hitachi Command Suite products, the encryption types listed below can be used for Kerberos authentication.

- AES256-CTS-HMAC-SHA1-96
- AES128-CTS-HMAC-SHA1-96
- RC4-HMAC
- DES3-CBC-SHA1
- DES-CBC-CRC
- DES-CBC-MD5

5

Communication security settings

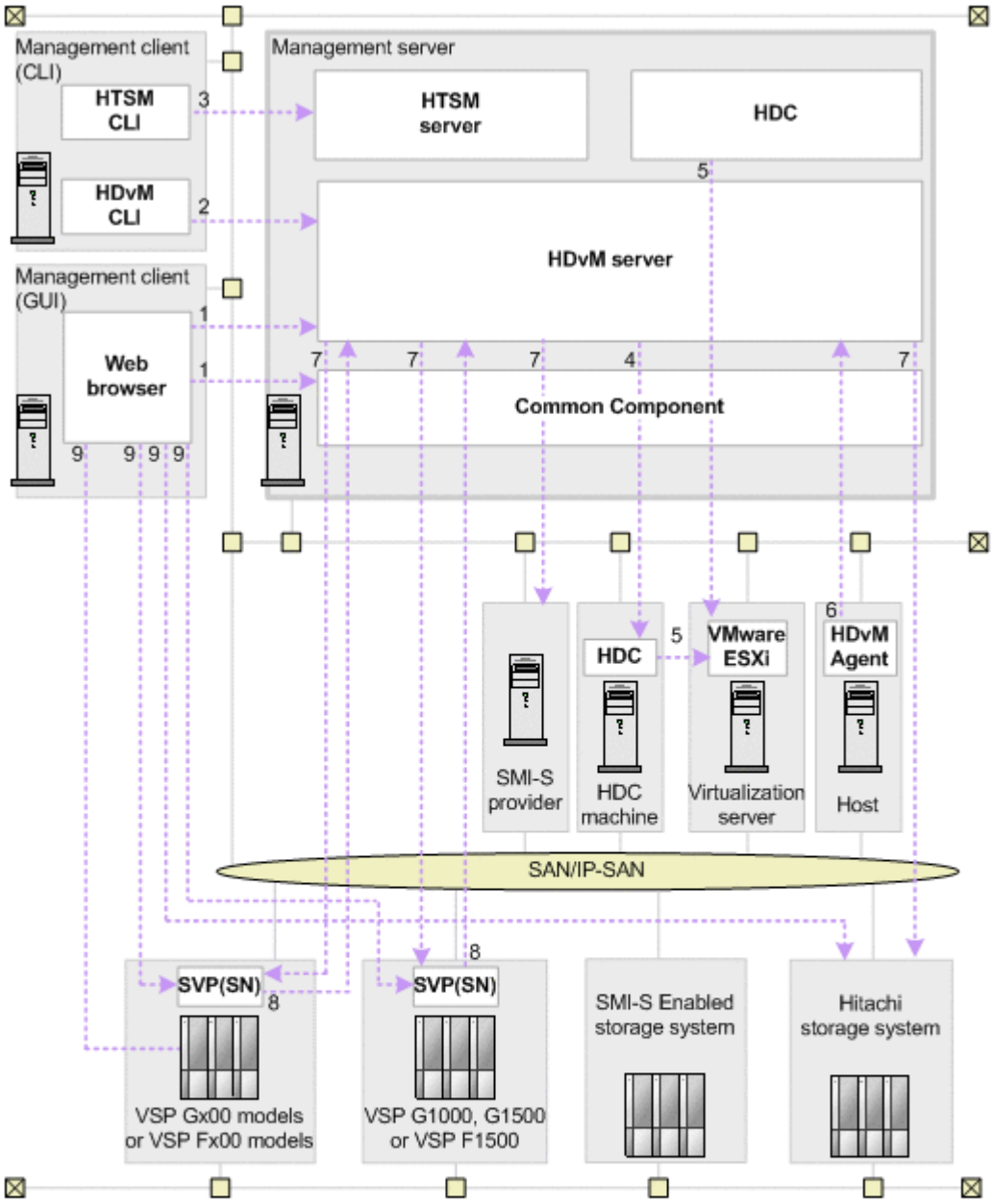
This chapter describes the communication security settings that can be used to operate Hitachi Command Suite products.

- Secure communication for Device Manager and Tiered Storage Manager
- Configuring an SSL server (Common Component)
- Configuring an SSL server (Device Manager server)
- Configuring an SSL server (Host Data Collector)
- Configuring an SSL client
- Configuring an SSL server and clients (CIM server)
- Configuring an SSL server and clients (CIM client)

Secure communication for Device Manager and Tiered Storage Manager

Device Manager and Tiered Storage Manager can use the secure inter-machine communication routes listed below.

The following two figures show the secure communication routes that are used in Device Manager and Tiered Storage Manager.



(Legend)
: Client-to-server SSL/TLS communication
HDvM: Hitachi Device Manager
HTSM: Hitachi Tiered Storage Manager
HDC: Host Data Collector
HDvM Agent : Device Manager agent
SN: Storage Navigator

Figure 27 Secure communication routes for Device Manager and Tiered Storage Manager (1/2)

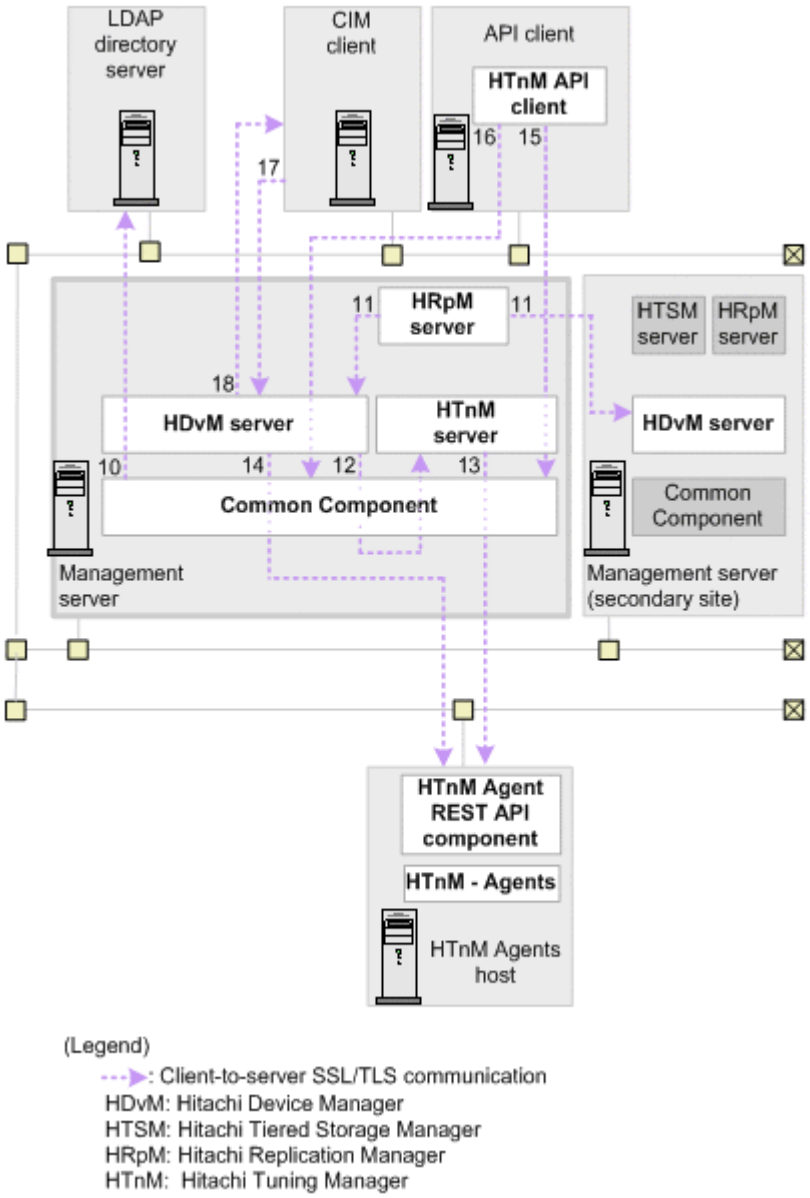


Figure 28 Secure communication routes for Device Manager and Tiered Storage Manager (2/2)

The following shows the secure communication routes that can be used in Device Manager and Tiered Storage Manager. The numbers in the table correspond to the numbers in the above figures.

Table 52 Secure communication routes that can be used in Device Manager and Tiered Storage Manager

No.	SSL server	SSL client	Remarks
1	Management server	Management client (GUI)	-

No.	SSL server	SSL client	Remarks
	• Common Component • Device Manager server		
2	Management server (Device Manager server)	Management client (Device Manager CLI)	Communications with TLS version 1.2 cannot be used.
3	Management server (Tiered Storage Manager server)	Management client (Tiered Storage Manager CLI)	Communications with TLS version 1.2 cannot be used.
4	Host Data Collector computer	Management server (Device Manager server)	-
5	Virtualization server	Host Data Collector computer	-
6	Management server (Device Manager server)	Device Manager computer	-
7	Storage system • VSP G1000 • VSP G1500 • VSP F1500 • VSP Gx00 models • VSP Fx00 models • Virtual Storage Platform • Universal Storage Platform V/VM • HUS VM • HUS100 • Hitachi AMS2000 • Hitachi SMS • SMI-S enabled storage systems (SMI-S provider)	Management server (Device Manager server)	Secure communication is always used for communication with VSP G1000, G1500, VSP F1500, VSP Gx00 models, VSP Fx00 models, Virtual Storage Platform, Universal Storage Platform V/VM, or HUS VM. Communications with TLS version 1.2 cannot be used. However, if the storage system is VSP G1000 (with a microcode version is 80-03-3*X*-*XX*/*XX* or later), VSP G1500 or VSP F1500, you can use communications with TLS version 1.2.
8	Management server (Device Manager server)	Storage system (VSP G1000, G1500, VSP F1500, VSP Gx00 models, or VSP Fx00 models)	In the following cases, you must specify settings to use secure communications between the Device Manager server and the storage system (VSP G1000, G1500, VSP F1500, VSP Gx00 models, or VSP Fx00 models): • For VSP G1000, G1500 or VSP F1500, if Hitachi Command Suite is used to authenticate user accounts to log in to CCI and the SVP • If you operate VSP Gx00 models or VSP Fx00 models

No.	SSL server	SSL client	Remarks
			The secure communication settings are enabled by default.
9	Storage system	Management client (GUI)	Secure communication can be used for communication between the Web browser of a management client and a storage system if Storage Navigator, Storage Navigator Modular 2, or the maintenance utility is used from the Device Manager GUI. If the storage system is VSP Gx00 models or VSP Fx00 models, you can use secure communication for the SVP or controllers from a management client (GUI). The secure communication settings are enabled by default.
10	LDAP directory server	Management server (Common Component)	-
11	Device Manager server	Replication Manager server	Even in a multi-site configuration, secure communication can be used between each of the secondary sites (Device Manager server) and each of the primary sites (Replication Manager server).
12	Tuning Manager server	Device Manager server	If the Device Manager server and Tuning Manager server are installed on the same management server, secure communication can be used. If the Device Manager server and the Tuning Manager server are installed on different management servers, see the section that describes SSL settings in the *Hitachi Command Suite Tuning Manager Installation Guide*.
13	Tuning Manager Agents	Tuning Manager server	• You can use secure communication when using Tuning Manager API. • Note that the Tuning Manager Agent REST API component in Figure 27 Secure communication routes for Device Manager and Tiered Storage Manager (1/2) on page 219 is a component required for using the Tuning Manager API, and "Tuning Manager Agent REST API component" is used as a general term for Tuning Manager - Agent REST Web Service and Tuning Manager - Agent REST Application Service.

No.	SSL server	SSL client	Remarks
			• For details on how to set up secure communication, see the section that describes SSL settings in the *Hitachi Command Suite Tuning Manager Installation Guide*.
14	Tuning Manager Agents	Device Manager server	• You can use security communication during use of the Alert function of Tuning Manager. If the Device Manager server and the Tuning Manager server are installed on the same management server, the same route as the above No. 13 is used. Therefore, if you have already specified the settings of No. 13, you do not need to specify additional settings. • For details about how to set security communication, see the section that describes SSL settings in the *Hitachi Command Suite Tuning Manager Installation Guide*.
15	Tuning Manager server	Tuning Manager API client	For details about how to set up security communication if the Device Manager server and the Tuning Manager server are installed on different management servers, see the section that describes SSL settings in the *Hitachi Command Suite Tuning Manager Installation Guide*.
16	Device Manager server	Tuning Manager API client	• You can use security communication during use of the Alert function of Tuning Manager. If the Device Manager server and the Tuning Manager server are installed on the same management server, the same route as above No.15 is used. Therefore, if you have already specified the settings of No.15, you do not need to specify additional settings. • For details about how to set security communication if the Device Manager server and the Tuning Manager server are installed on different management servers, see the section that describes SSL settings in the *Hitachi Command Suite Tuning Manager Installation Guide*.

No.	SSL server	SSL client	Remarks
17	Management server (Device Manager server)	CIM client	Secure communication can be used for object operations. To further improve security, you can enable two-way authentication. Communications with TLS version 1.2 cannot be used.
18	CIM client	Management server (Device Manager server)	Secure communication can be used for event indications. To further improve security, you can enable two-way authentication. Communications with TLS version 1.2 cannot be used.

Legend:

-: Not applicable

Default certificate for Device Manager

For Device Manager 8.1.3 or later, if you perform a new installation of Device Manager or perform an upgrade installation in an environment where the Device Manager server certificate does not exist, the default certificate is registered into the keystore and the SSL/TLS communication settings are enabled.

The default certificate is a self-signed certificate that is used to encrypt communication routes when user account authentication is linked between the storage system (VSP G1000, G1500, VSP F1500, VSP Gx00 models, and VSP Fx00 models) and Hitachi Command Suite. Use HiKeytool to display the contents of the certificate, and make sure that the security requirements are met. If you use another self-signed certificate or a certificate signed by a certificate authority to improve security, delete the default certificate, and then specify the SSL/TLS communication settings again.

To use secure communication between a component other than the storage system (VSP G1000, G1500, VSP F1500, VSP Gx00 models, and VSP Fx00 models) and the Device Manager server, delete the default certificate, and then reconfigure the SSL/TLS communication settings.

Note:

- Use HiKeytool when checking the contents of the default certificate or removing the certificate from the keystore.
- Do not import the default certificate into the truststore for the communication partner of the Device Manager server. If you do so, communication fails.

Related tasks

- Viewing the Device Manager server key pair information in verbose mode on page 275
- Deleting a key pair from the Device Manager server keystore on page 276

Operation workflow for secure communication between a management server and a management client (GUI)

You need to create server certificates for Common Component and the Device Manager server on the management server, and then import them into the web browser in the management client (GUI).

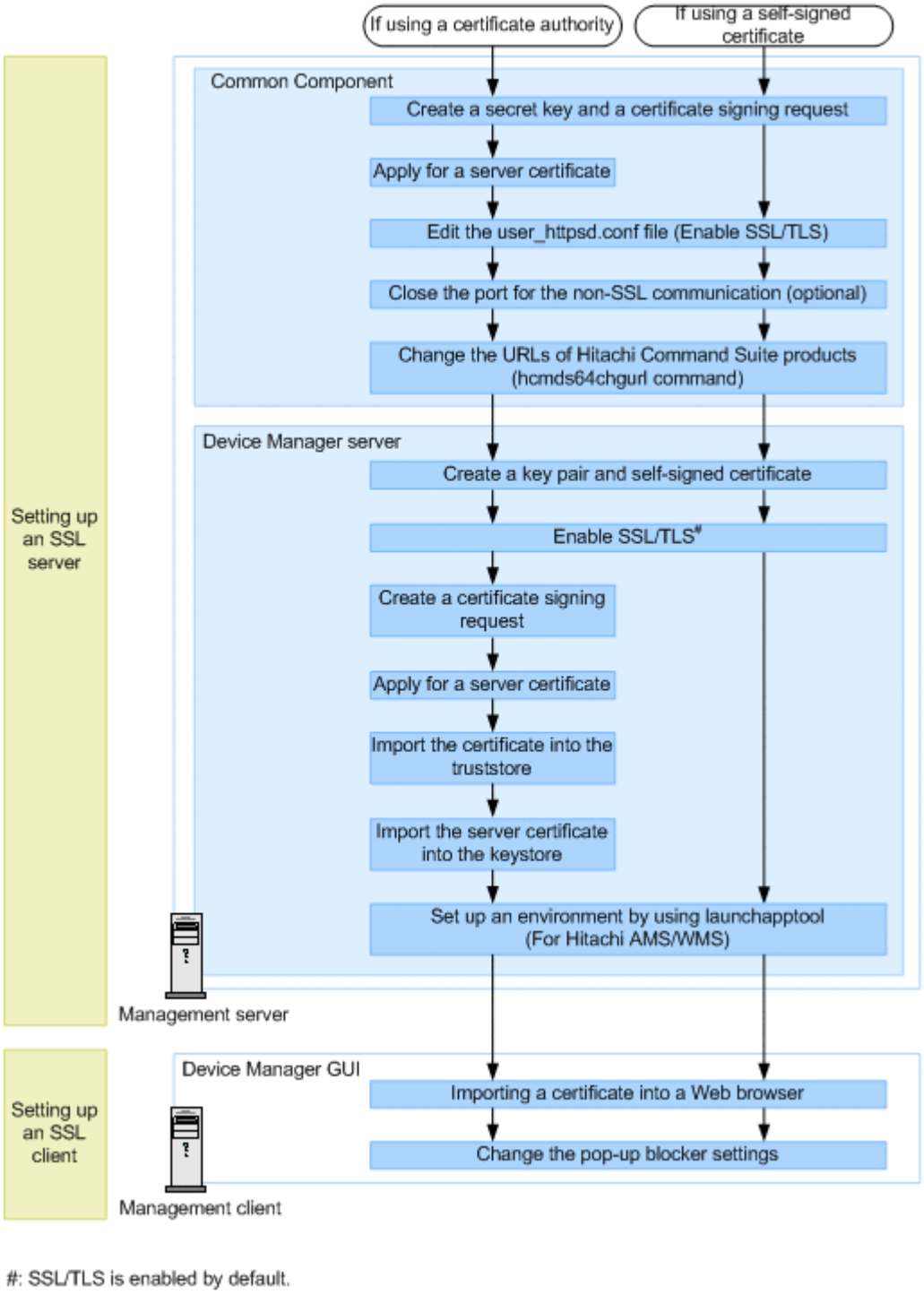


Figure 29 Operation workflow for secure communication between a management server and a management client (GUI)

Note:

- You do not need to create and import a server certificate for the Device Manager server if you do not use Storage Navigator or Storage Navigator Modular 2 from Element Manager in the Device Manager GUI.
- When using a well-known certificate authority to import the certificate to the web browser, the certificate might have already been imported to the web browser. If this is the case, you do not need to import a certificate for the web browser again.
- If you want to restrict which cipher suites are used for SSL/TLS communication, change the value of the `server.https.enabledCipherSuites` property in the `server.properties` file of the Device Manager server.

Related concepts

- Configuring an SSL server (Common Component) on page 253
- Configuring an SSL server (Device Manager server) on page 266
- Configuring an SSL client on page 288

Related tasks

- Changing the URL for accessing Hitachi Command Suite products (hcmds64chgurl command) on page 154
- Settings for using Element Manager on page 333
- Changing Device Manager server properties on page 590

Related references

- server.https.enabledCipherSuites on page 619

Operation workflow for secure communication between a management server and a management client (Device Manager CLI)

You need to create a server certificate for the Device Manager server on the management server, and then enable SSL/TLS in the management client (Device Manager CLI).

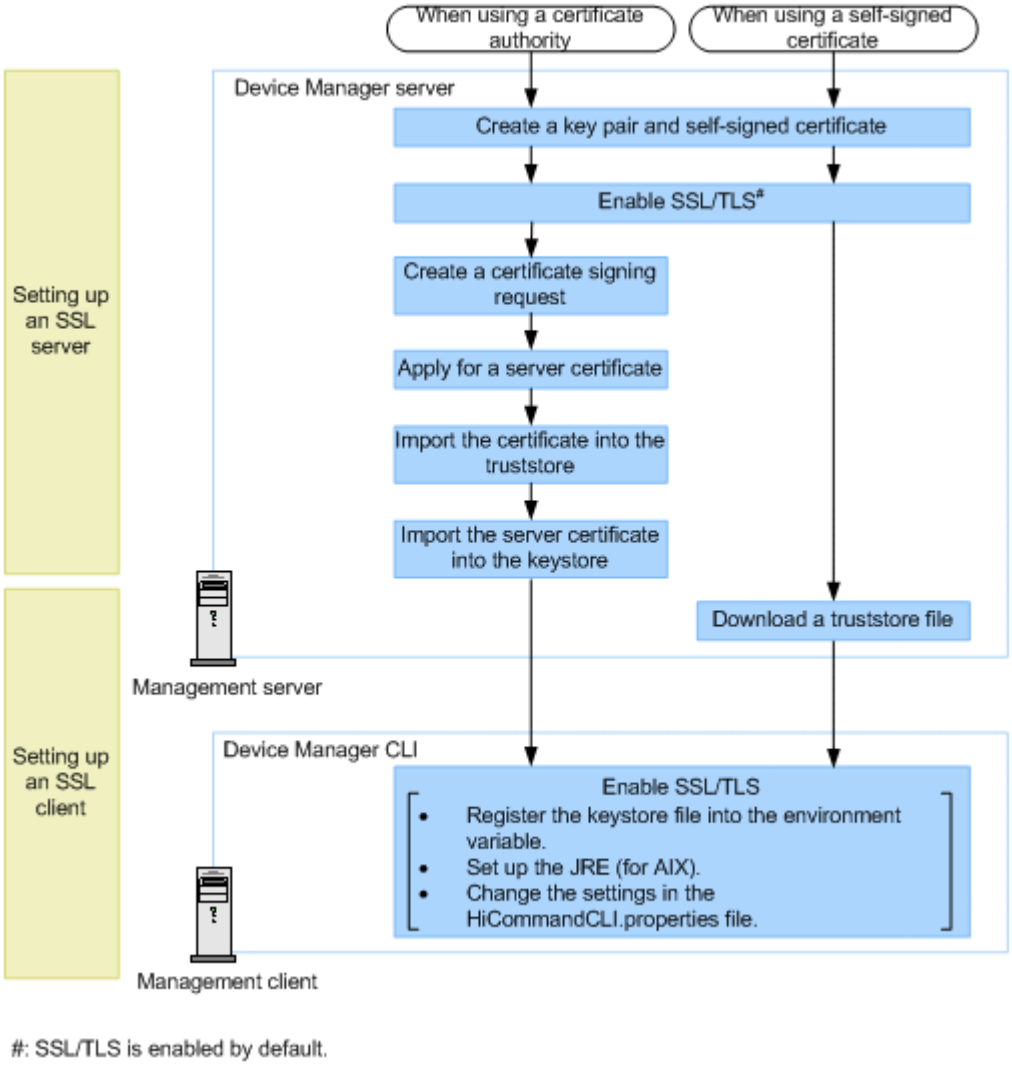


Figure 30 Operation workflow for secure communication between a management server and a management client (Device Manager CLI)

Note: If you want to restrict which cipher suites are used for SSL/TLS communication, change the value of the `server.https.enabledCipherSuites` property in the `server.properties` file of the Device Manager server.

Related concepts

- Configuring an SSL server (Device Manager server) on page 266
- Configuring an SSL client on page 288

Related tasks

- Changing Device Manager server properties on page 590

Related references

- server.https.enabledCipherSuites on page 619

Operation workflow for secure communication between a management server and a management client (Tiered Storage Manager CLI)

The self-signed certificate bundled with the Tiered Storage Manager server is used for SSL/TLS communication between a management server and a management client (Tiered Storage Manager CLI). You need to set the Tiered Storage Manager server properties on the management server, and then enable SSL/TLS in the management client (Tiered Storage Manager CLI).

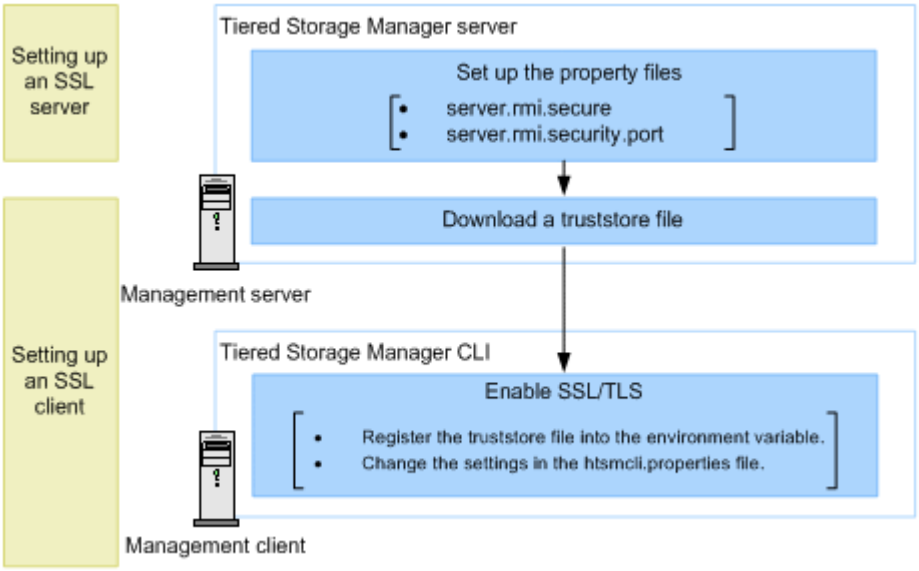


Figure 31 Operation workflow for secure communication between a management server and a management client (Tiered Storage Manager CLI)

Note: If you want to restrict which cipher suites are used for SSL/TLS communication, change the value of the `server.rmi.secure` property in the `server.properties` file of the Tiered Storage Manager server.

Related concepts

- Configuring an SSL client on page 288

Related tasks

- Changing Tiered Storage Manager server properties on page 642

Related references

- server.rmi.secure on page 655
- server.rmi.security.port on page 644
- server.rmi.security.enabledCipherSuites on page 655

Operation workflow for secure communication between an LDAP directory server and a management server

You need to specify the settings for linking with an external authentication server on the management server, and then import the certificate into the truststore (`ldapcacerts`).

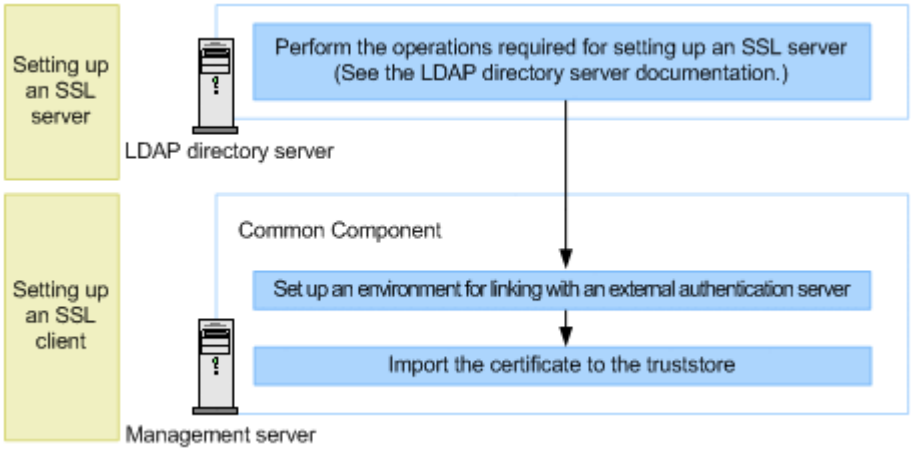


Figure 32 Operation workflow for secure communication between an LDAP directory server and a management server

If the server certificate was issued by a well-known certificate authority, the certificate of the certificate authority might already be imported to the truststore (`jssecacerts`). In this case, you do not need to import the certificate into the `ldapcacerts` truststore.

Related concepts

- Operating workflow for user authentication on an LDAP directory server on page 166
- Configuring an SSL client on page 288

Operation workflow for secure communication between a Device Manager server and Replication Manager server

You need to create a server certificate for the Device Manager server on the management server, and then import it into the truststore (`jssecacerts`).

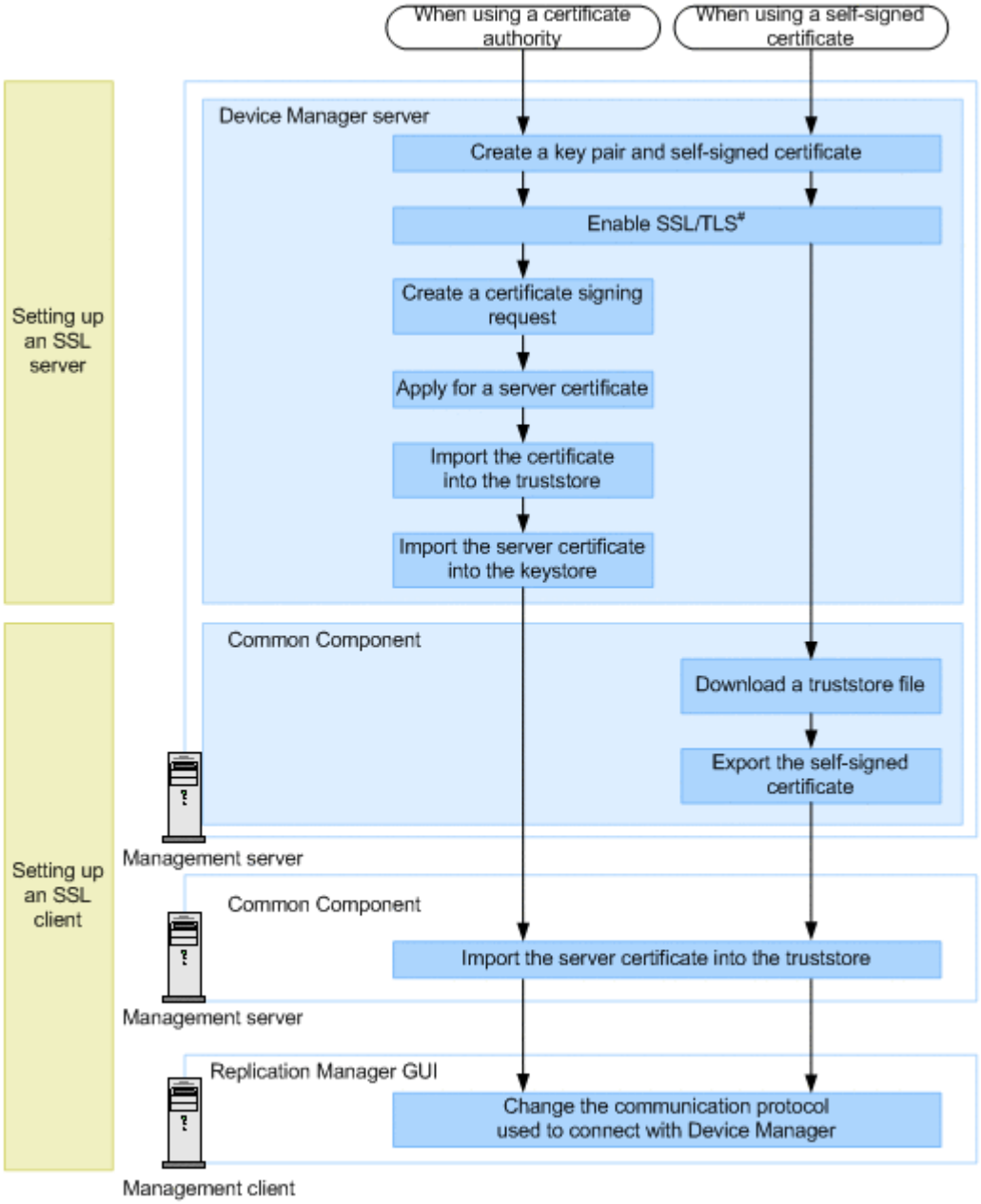


Figure 33 Operation workflow for secure communication between a Device Manager server and Replication Manager server

Note that, if the server certificate was issued by a well-known certificate authority, the certificate of the certificate authority might already be imported to the truststore (`jssecacerts`). If this is the case, you do not need to import a certificate for Device Manager server

Note:

- If you want to restrict which cipher suites are used for SSL/TLS communication, change the value of the `server.https.enabledCipherSuites` property in the `server.properties` file of the Device Manager server.
- For a multi-site configuration, transfer the Device Manager server certificate created in each secondary site to the primary site in a secure method, and then import the certificate into the truststore (`jssecacerts`).

Related concepts

- Configuring an SSL server (Device Manager server) on page 266
- Configuring an SSL client on page 288

Related tasks

- Changing Device Manager server properties on page 590

Related references

- server.https.enabledCipherSuites on page 619

Operation workflow for secure communication between a Tuning Manager server and a Device Manager server

You need to create a server certificate for Common Component on the management server, and then import it into the truststore (`jssecacerts`).

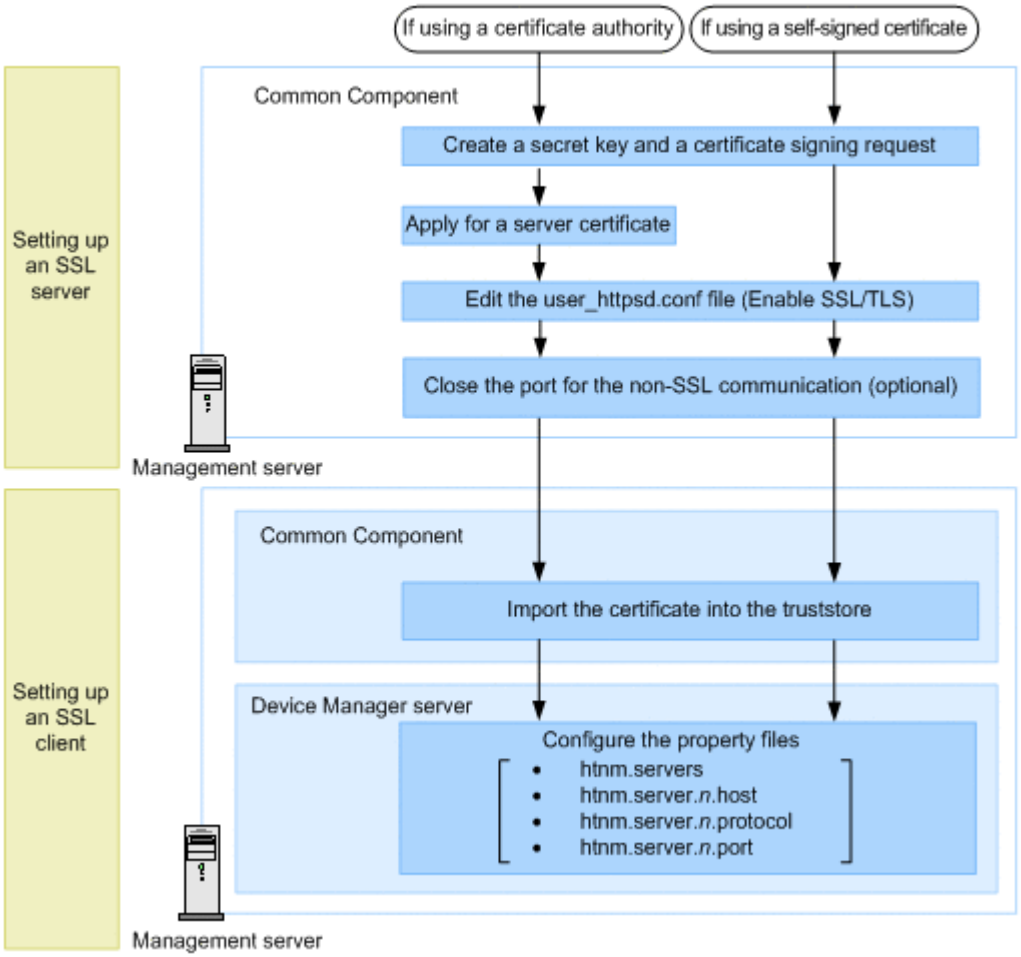


Figure 34 Operation workflow for secure communication between a Tuning Manager server and a Device Manager server

Note that for the following case, the certificate might already be imported in the truststore (`jssecacerts`). If this is the case, you do not need to import a certificate for Common Component.

- If a well-known certificate authority is used
- If closing the port for non-SSL communication for HBase 64 Storage Mgmt Web Service

Related concepts

- Configuring an SSL server (Common Component) on page 253
- Configuring an SSL client on page 288

Related tasks

- Changing Device Manager server properties on page 590

Related references

- htnm.servers on page 631
- htnm.server.n.host on page 631

- htnm.server.n.protocol on page 631
- htnm.server.n.port on page 632

Operation workflow for secure communication between a Host Data Collector machine and a management server

You need to create a server certificate for Host Data Collector on a Host Data Collector machine, and then import it into the truststore (`dvmcacerts`).

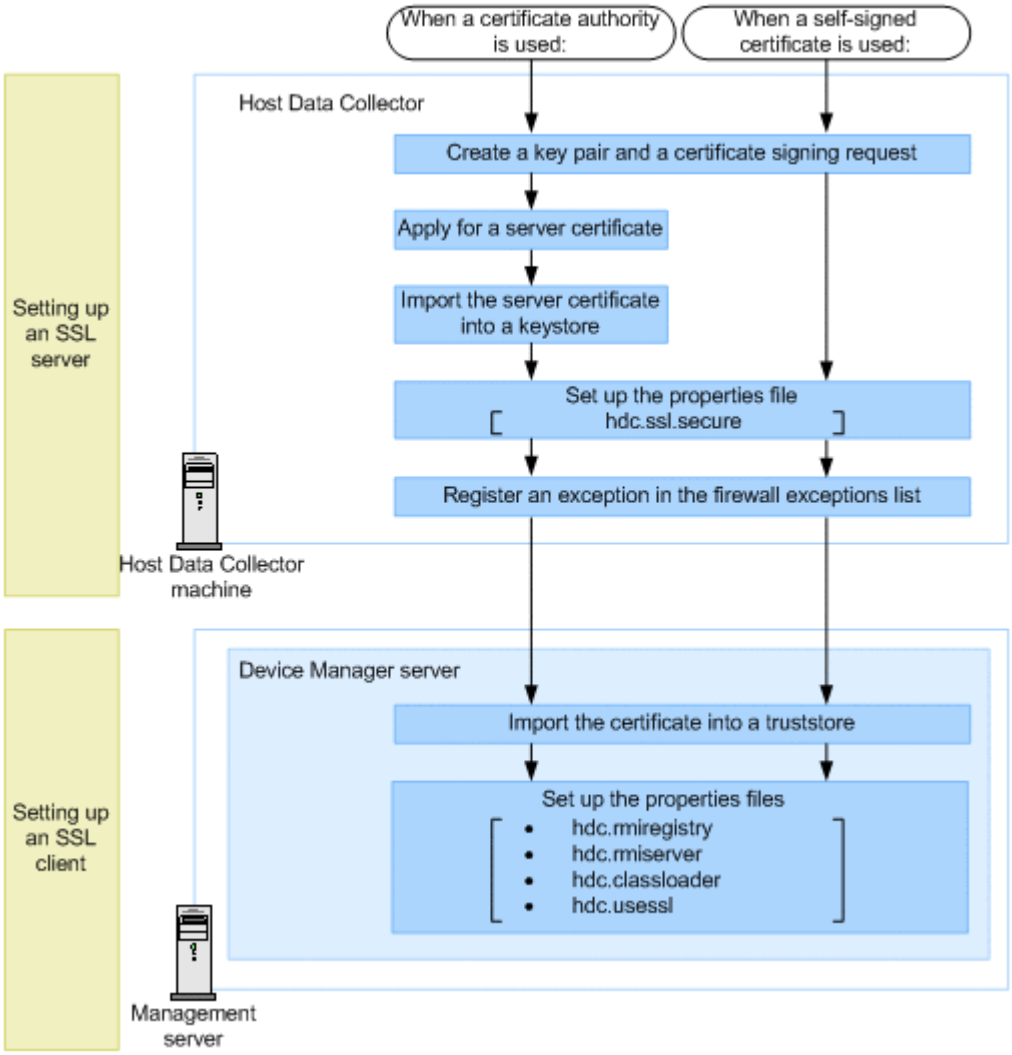


Figure 35 Operation workflow for secure communication between a Host Data Collector machine and a management server

Note:

- If you want to restrict which cipher suites are used for SSL/TLS communication, change the value of the `hdc.ssl.ciphers` property in the `hdcbase.properties` file of the Host Data Collector.

- If there are multiple computers where Host Data Collector is installed, you need to match the communication protocol (SSL or non-SSL) between the management server and all of the Host Data Collector machines.
- If the Java execution environment for Host Data Collector has been changed, you need to download and install the Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files for the version of the Java execution environment to be used.

  Download the Jurisdiction Policy files from the Oracle corporation website. For details about how to install the files, see the documentation provided with the Jurisdiction Policy files.

Related concepts

- Registering firewall exceptions for Host Data Collector (Windows) on page 141
- Configuring an SSL server (Host Data Collector) on page 284

Related tasks

- Importing a certificate into the Device Manager server truststore on page 278
- Changing Device Manager server properties on page 590
- Changing Host Data Collector properties on page 658

Related references

- hdc.rmiregistry on page 626
- hdc.rmiserver on page 626
- hdc.classloader on page 627
- hdc.usessl on page 628
- hdc.ssl.secure on page 663
- hdc.ssl.ciphers on page 667

Operation workflow for secure communication between a virtualization server and Host Data Collector

You need to configure an SSL server on a virtualization server, and then change the communication protocol used to connect with the virtualization server from the Device Manager GUI or CLI.

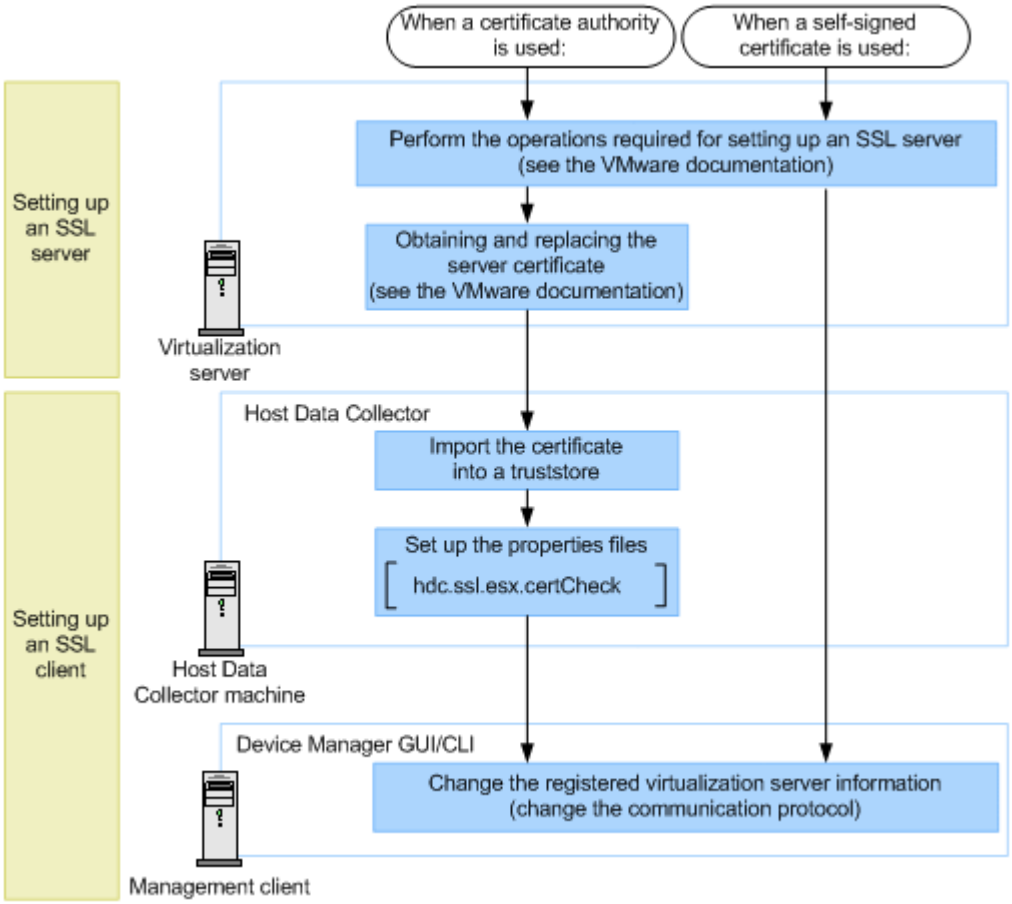


Figure 36 Operation workflow for secure communication between a virtualization server and Host Data Collector

Note: By default, SSL using the self-signed certificate is set to be used for communication between a virtualization server and Host Data Collector. To change this setting, perform the operation as follows:

- If you want to change the configuration to non-SSL communication for operation test purposes:
  If you change to a configuration that uses non-SSL communication (for example, a configuration for an operation test), first use VMware ESXi or VMware vCenter Server to change the security settings (`proxy.xml` file) of the Web proxy service, and then use the Device Manager GUI or CLI to change the communication protocol.
- When using a server certificate issued by a certificate authority:
  Apply to a certificate authority to obtain a server certificate for a virtualization server. If you are creating a certificate signing request (CSR), specify the IP address of the virtualization server that issued the certificate as a Subject Alternative Name.
  If a virtualization server that is managed by Host Data Collector includes VMware ESXi, the certificates issued by all the authorities, from the authority that issued the server certificate for the virtualization server to

the root certificate authority, form a certificate chain, and a server certificate is required.
Replace the obtained server certificate with the self-signed certificate that is imported to the virtualization server. For details, see VMware manuals.

Related tasks

- Importing a certificate into the truststore for Host Data Collector on page 305
- Changing virtualization server information on page 308
- Changing Host Data Collector properties on page 658

Related references

- hdc.ssl.esx.certCheck on page 664

Operation workflow for secure communication between a management server and Device Manager agent

You need to create a server certificate for Device Manager on the management server, and then import it into the truststore.

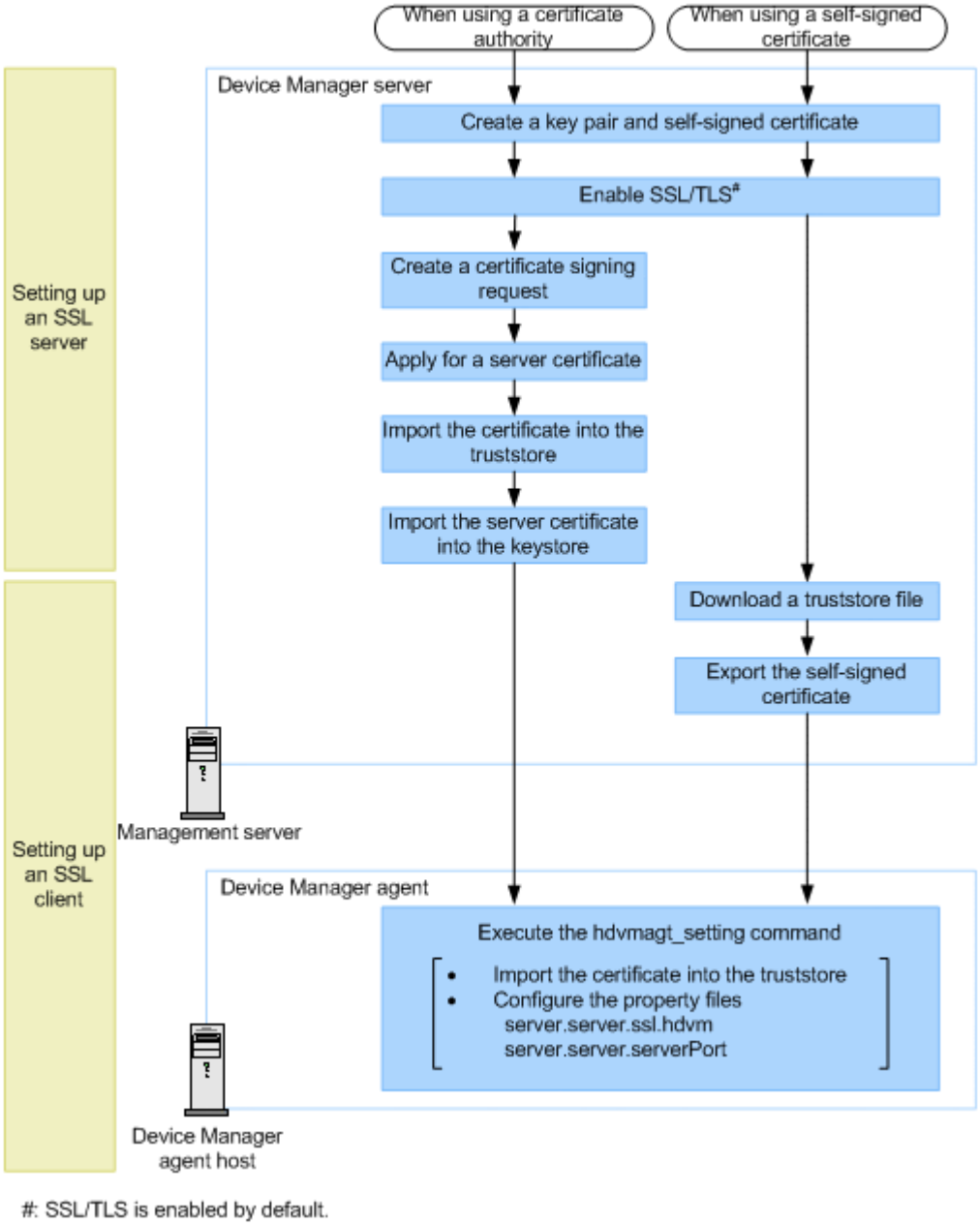


Figure 37 Operation workflow for secure communication between a management server and Device Manager agent

For a Device Manager agent version 8.2.0 or later, you can import a certificate into the truststore of the Device Manager agent and specify settings in the property file also during a new installation of a Device Manager agent. For details on how to install a Device Manager agent, see the *Hitachi Command Suite Installation and Configuration Guide*.

Note:

- If you want to restrict which cipher suites are used for SSL/TLS communication, change the value of the

`server.https.enabledCipherSuites` property in the `server.properties` file of the Device Manager server.

- If the Java execution environment for a Device Manager agent has been changed, you need to download and install the Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files for the version of the Java execution environment to be used.
  Download the Jurisdiction Policy files from the Website of Oracle corporation or IBM corporation. For details about how to install the files, see the documentation provided with the Jurisdiction Policy files.

Note: If you are using a Device Manager agent whose version is earlier than 8.2.0, manually import a certificate into the truststore of the Device Manager agent and specify settings in the property file.

Related concepts

- Configuring an SSL server (Device Manager server) on page 266

Related tasks

- Downloading a Device Manager server truststore file on page 288
- Exporting a Device Manager server self-signed certificate on page 290
- Changing Device Manager server properties on page 590

Related references

- Setting the Device Manager server's information, HiScan command's execution period, and CCI's information (hdvmagt_setting command) on page 533
- server.https.enabledCipherSuites on page 619
- server.server.serverPort on page 683
- server.server.ssl.hdvm on page 691

Operation workflow for secure communication between a storage system and a management server

To use SSL/TLS for communication between HUS100, Hitachi AMS2000, or Hitachi SMS and a management server, you need to change the communication protocol used to connect with storage systems from the Device Manager GUI or CLI.

You do not need to set up a Device Manager environment for communication with VSP G1000, G1500, VSP F1500, VSP Gx00 models, VSP Fx00 models, Virtual Storage Platform, Universal Storage Platform V/VM, or HUS VM because such communication always uses SSL/TLS.

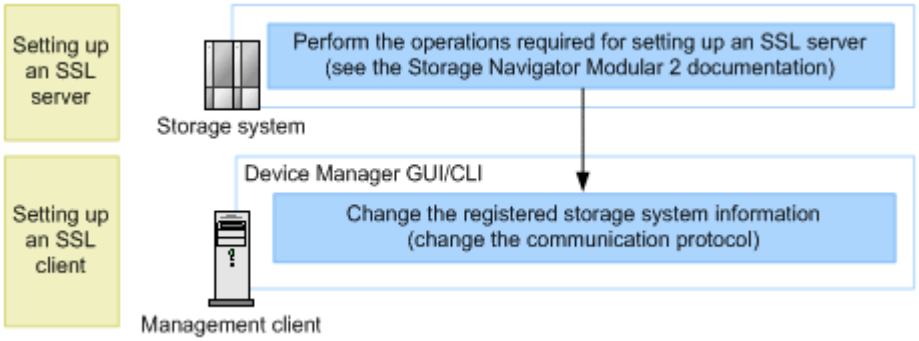


Figure 38 Operation workflow for secure communication between a storage system and a management server

Related tasks

- Changing storage system information on page 313

Operation workflow for secure communication between a management server and a storage system (VSP G1000, G1500 or VSP F1500)

To improve security when authenticating user accounts in Hitachi Command Suite when logging in to CCI or the SVP, delete the default certificate, create a server certificate for the Device Manager server, and then import the certificate into SVP. Perform the operation on SVP so that the host name that was specified when creating the server certificate for the Device Manager server can be resolved to the IP address for the Device Manager server.

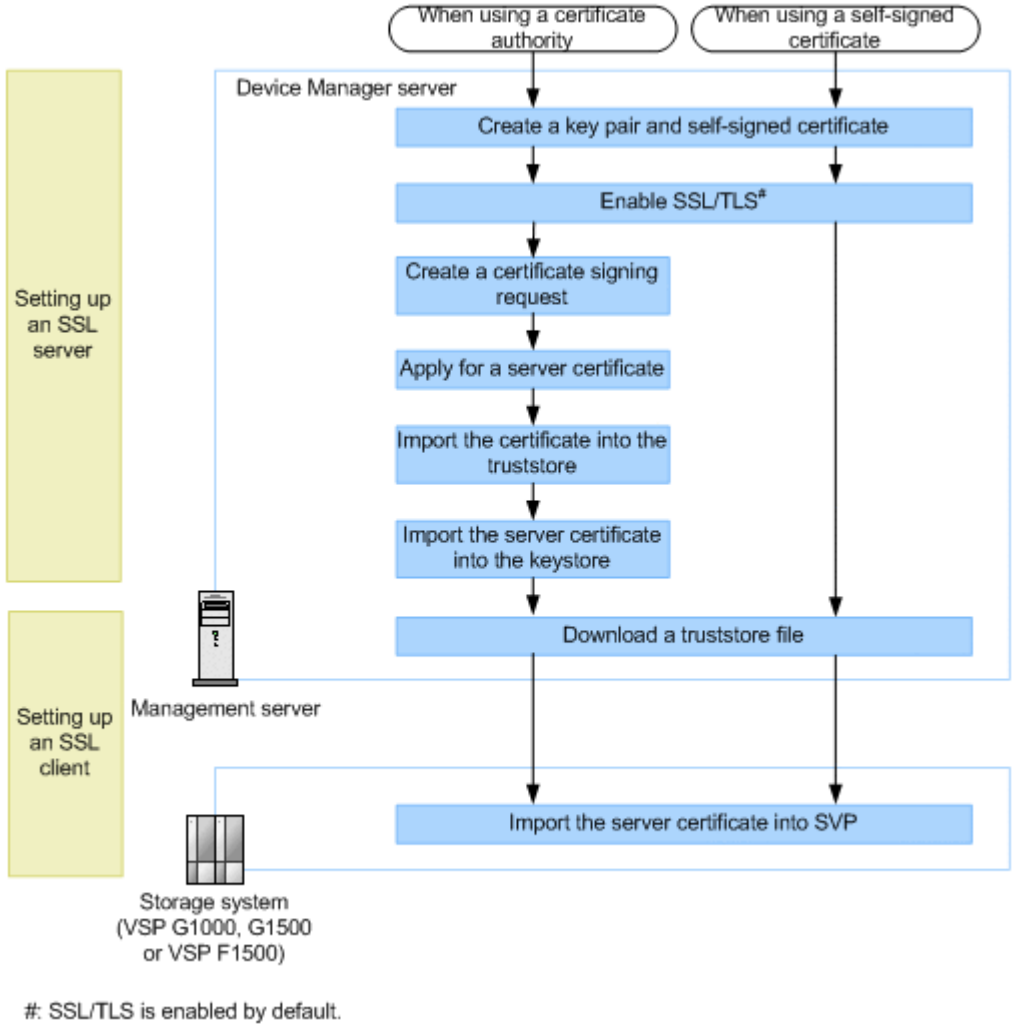


Figure 39 Operation workflow for secure communication between a management server and a storage system (VSP G1000, G1500 or VSP F1500)

For details on how to specify settings for SVP, see the manual for the storage system.

Related concepts

- Default certificate for Device Manager on page 224
- Configuring an SSL server (Device Manager server) on page 266

Related tasks

- Downloading a Device Manager server truststore file on page 288

Operation workflow for secure communication between a management server and a storage system (VSP Gx00 models or VSP Fx00 models)

For VSP Gx00 and VSP Fx00 models, if you are using the default server certificate, you do not need to configure any other settings, because settings are configured, by default, to enable encrypted communication. To improve the security of communications that occur when operations are being performed on a storage system, delete the default certificate, create a server certificate for the Device Manager server, and then import the certificate into SVP. Perform the operation on SVP so that the host name that was specified when creating the server certificate for the Device Manager server can be resolved to the IP address for the Device Manager server.

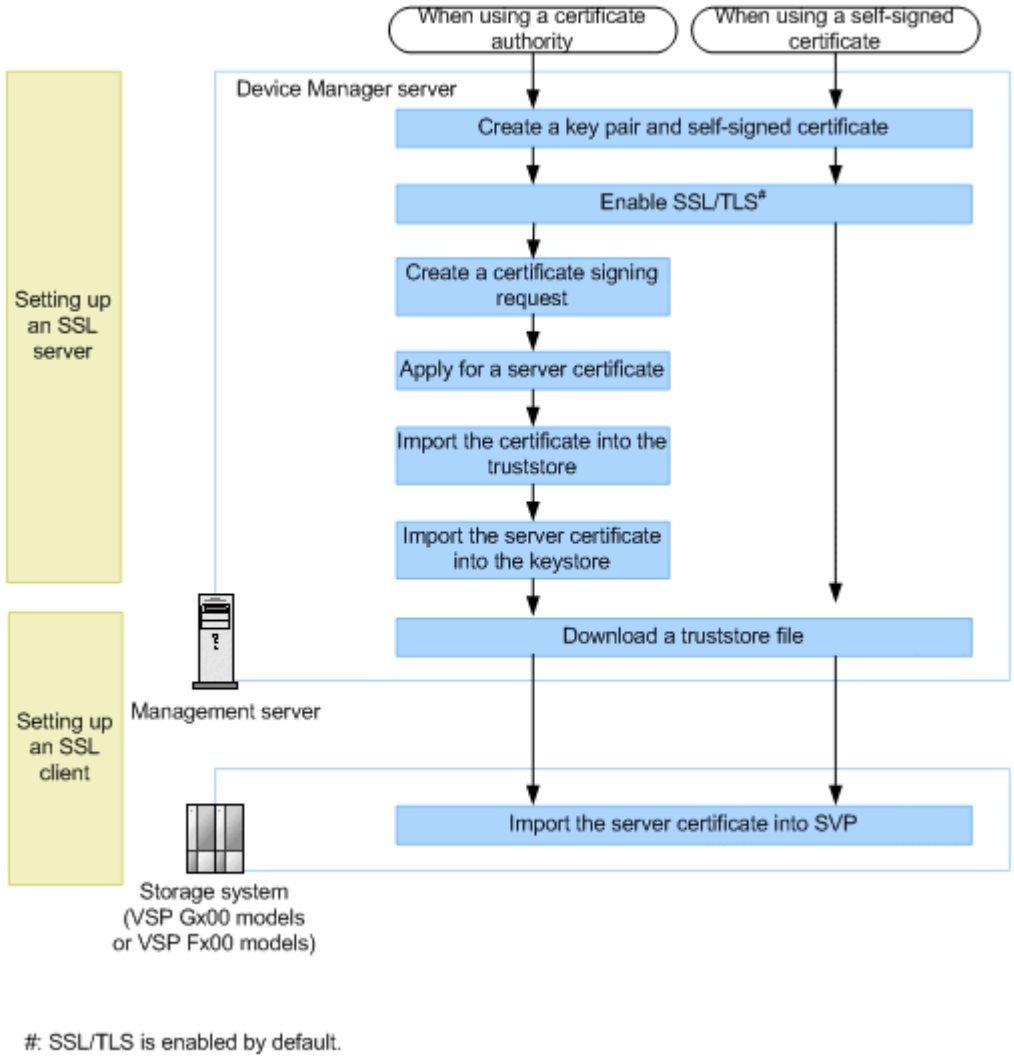


Figure 40 Operation workflow for secure communication between a management server and a storage system (VSP Gx00 models or VSP Fx00 models)

For details on the SVP settings, see the manual for the storage system.

Related concepts

- Default certificate for Device Manager on page 224
- Configuring an SSL server (Device Manager server) on page 266

Related tasks

- Downloading a Device Manager server truststore file on page 288

Operation workflow for secure communication between an SMI-S provider and a management server

You need to set up an SMI-S provider environment, and then change the communication protocol used to connect with the SMI-S provider from the Device Manager GUI or CLI.

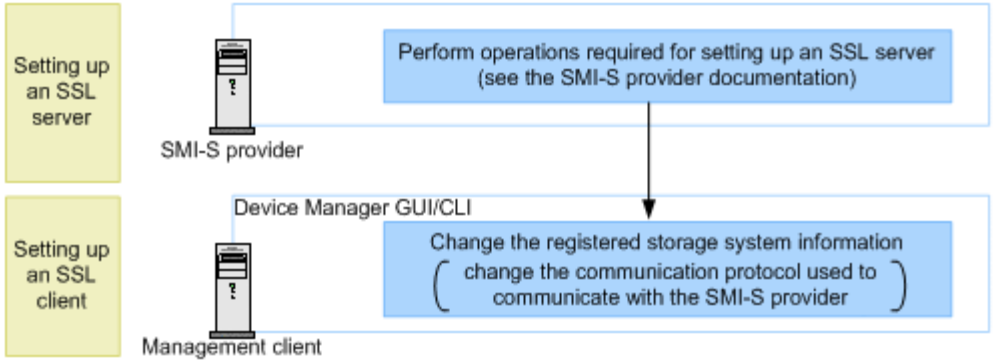


Figure 41 Operation workflow for secure communication between an SMI-S provider and a management server

Related concepts

- Configuring an SSL client on page 288

Operation workflow for secure communication between a Tuning Manager server and a Tuning Manager API client

When the Tuning Manager server and Device Manager server are installed on the same management server, you need to create a Common Component server certificate on the management server, and then import the server certificate for the Tuning Manager API client. Configure the API client-side SSL communication settings by performing the operations appropriate for the environment on each client.

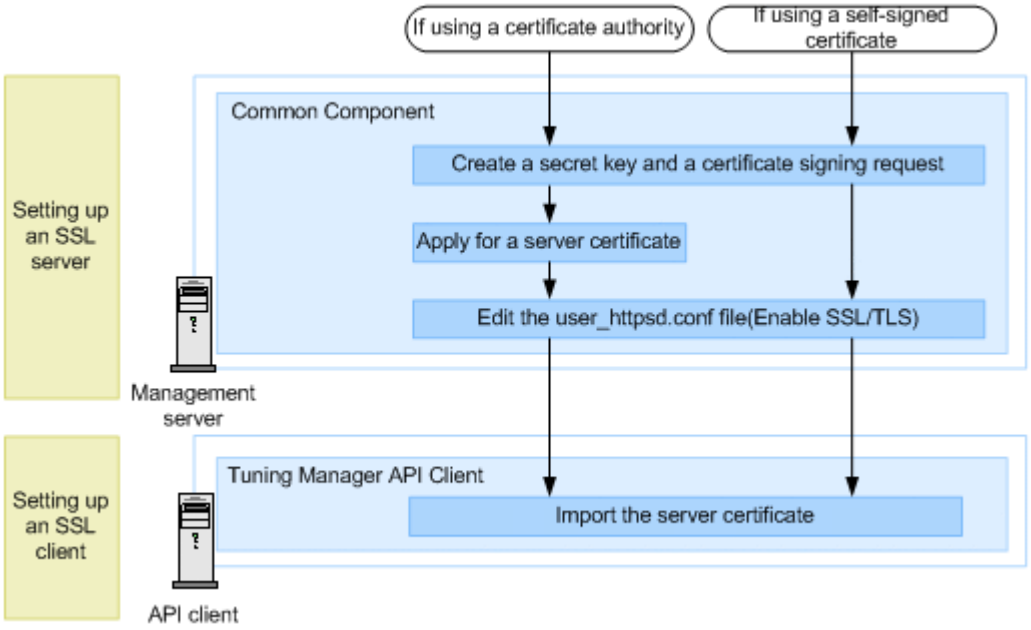


Figure 42 Operation workflow for secure communication between a Tuning Manager server and a Tuning Manager API client

Note: This manual explains how to set up SSL communication when the Tuning Manager server and Device Manager server are installed on the same management server. For details on how to set up SSL communication when the Tuning Manager server and Device Manager server are installed on different management servers, see the *Hitachi Command Suite Tuning Manager Installation Guide*.

Related concepts

- Configuring an SSL server (Common Component) on page 253

Operation workflow for secure communication between a storage system and a management client (GUI)

When you perform operations on a storage system by using Storage Navigator, Storage Navigator Modular 2, or the maintenance utility from the Device Manager GUI, communications can be secured by using the default server certificate stored in the storage system.

When operating VSP G1000, G1500, VSP F1500, VSP Gx00 models, VSP Fx00 models, Virtual Storage Platform, or HUS VM, if you launch Storage Navigator or the maintenance utility from the Device Manager GUI, a certificate warning message appears in the Web browser. Ignore this message. Communication between the storage systems and the Device Manager GUI is encrypted even if this warning message appears.

To prevent this warning message from appearing when Storage Navigator is launched, follow the operation workflow below to re-create the server

certificate for the storage system. In the server certificate, specify the host name of the storage system in `Common Name`. This host name must be the same as the host name for the storage system specified when registering by the Device Manager GUI. For VSP Gx00 models or VSP Fx00 models , specify the host name of the SVP.

For the maintenance utility, you cannot prevent this warning message from appearing because controllers of VSP Gx00 models or VSP Fx00 models are registered in the Device Manager GUI by using IP addresses.

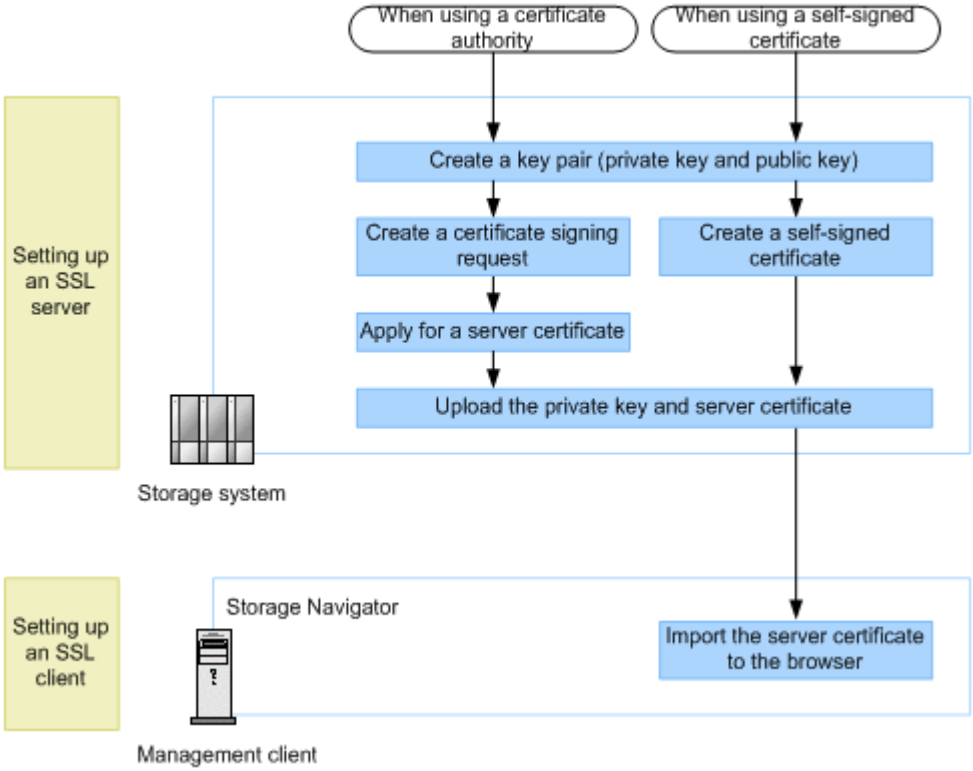


Figure 43 Operation workflow for secure communication between a storage system and a management client (GUI)

Tip: When performing operations on VSP G1000, G1500, VSP F1500, VSP Gx00 models , or VSP Fx00 models , you can simplify the information to be sent from the Device Manager GUI to Storage Navigator to improve security.

To simplify the information to be sent to Storage Navigator, specify `true` for the `client.launch.em.secure` property in the `client.properties` file of the Device Manager server.

For details on how to create and import a server certificate, see the manual for the storage system.

Related tasks

- Changing Device Manager server properties on page 590

Related references

- client.launch.em.secure on page 615

Operation workflow for secure communication between a management server and a CIM client (object operations)

To use SSL server authentication for object operations, you need to import the server certificate created by the Device Manager server into the CIM client.

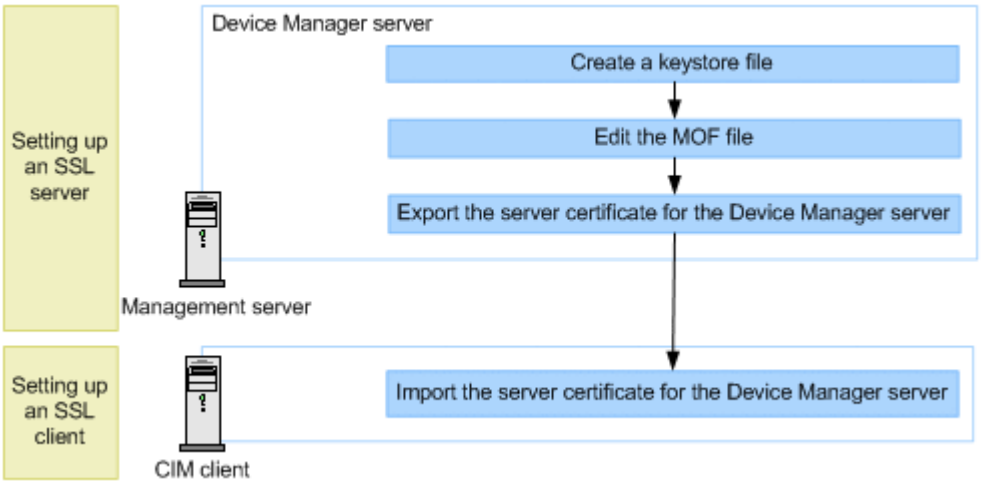


Figure 44 Operation workflow for secure communication between a management server and a CIM client (object operations)

Note: If you want to restrict which cipher suites are used for SSL/TLS communication, create a new `cimxmlscpa.properties` file, and then specify a value for the `Ciphers` property.

Related concepts

- Configuring an SSL server and clients (CIM server) on page 314
- Configuring an SSL server and clients (CIM client) on page 327

Related tasks

- Changing Device Manager server properties on page 590

Related references

- Ciphers on page 620

Operation workflow for secure communication between a management server and a CIM client (two-way authentication for object operations)

For SSL server authentication, import the Device Manager server certificate into the CIM client. For SSL client authentication, import the CIM client certificate into the Device Manager server.

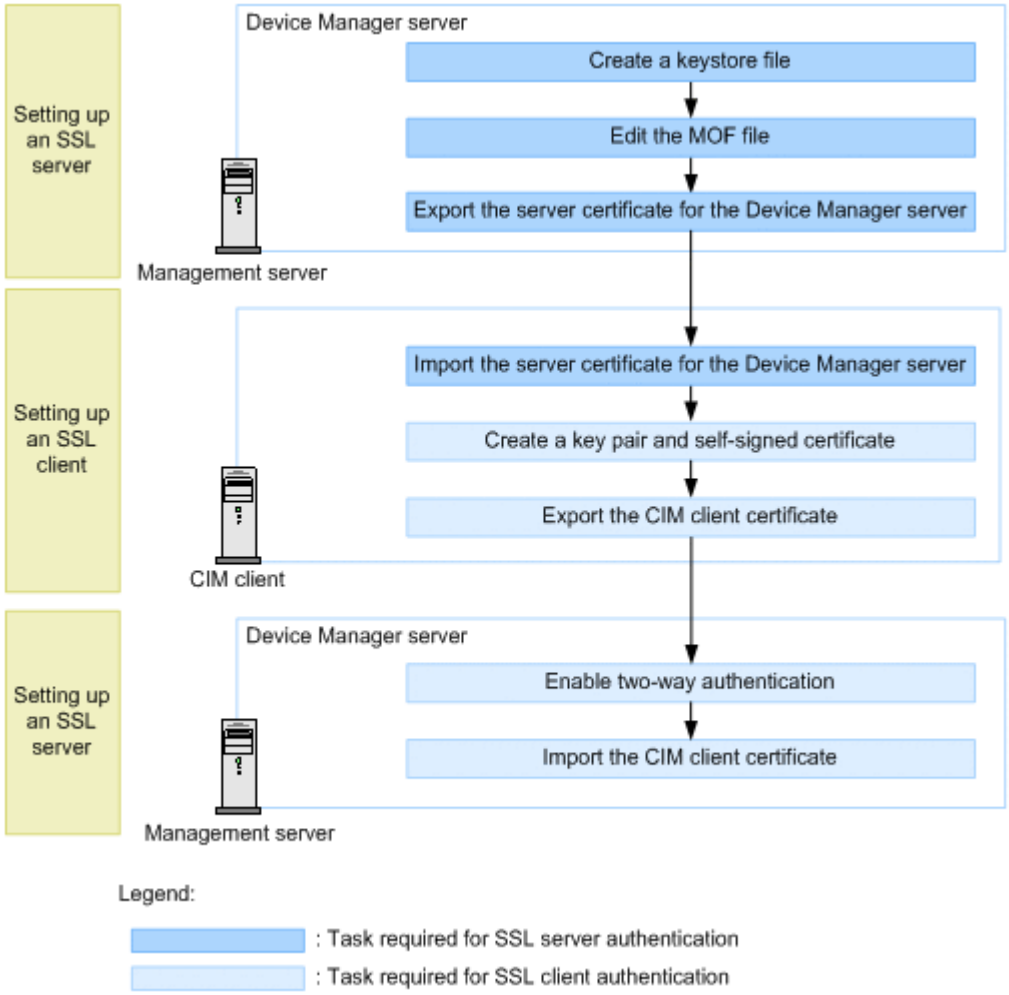


Figure 45 Operation workflow for secure communication between a management server and a CIM client (two-way authentication for object operations)

Note: If you want to restrict which cipher suites are used for SSL/TLS communication, create a new `cimxmlscpa.properties` file, and then specify a value for the `Ciphers` property.

Related concepts

- Configuring an SSL server and clients (CIM server) on page 314
- Configuring an SSL server and clients (CIM client) on page 327

Related tasks

- Changing Device Manager server properties on page 590

Related references

- Ciphers on page 620

Operation workflow for secure communication between a management server and a CIM client (event indications)

To use SSL server authentication for event indications, you need to import the server certificate created by the CIM client into the Device Manager server.

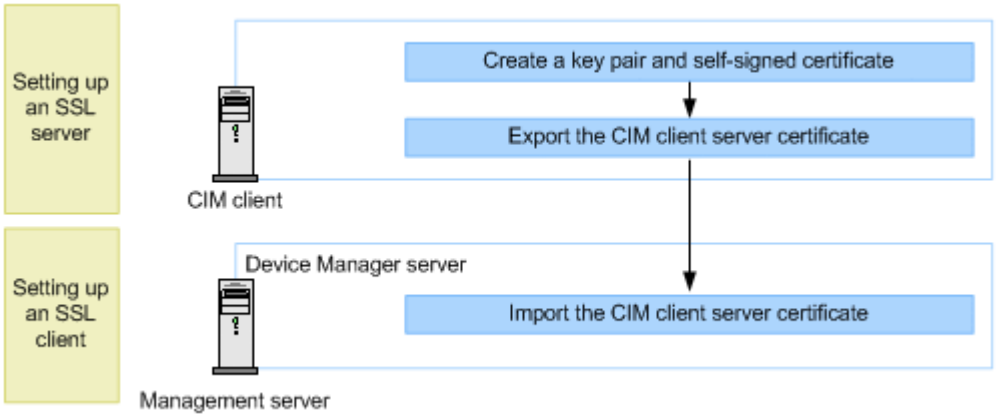


Figure 46 Operation workflow for secure communication between a management server and a CIM client (event indications)

Note: If you want to restrict which cipher suites are used for SSL/TLS communication, create a new `cimxmlscpa.properties` file, and then specify a value for the `Ciphers` property.

Related concepts

- Configuring an SSL server and clients (CIM server) on page 314
- Configuring an SSL server and clients (CIM client) on page 327

Related tasks

- Changing Device Manager server properties on page 590

Related references

- Ciphers on page 620

Operation workflow for secure communication between a management server and a CIM client (two-way authentication for event indications)

For SSL server authentication, import the server certificate of the CIM client into the Device Manager server. For SSL client authentication, import the client certificate of the Device manager server into the CIM client in the same way.

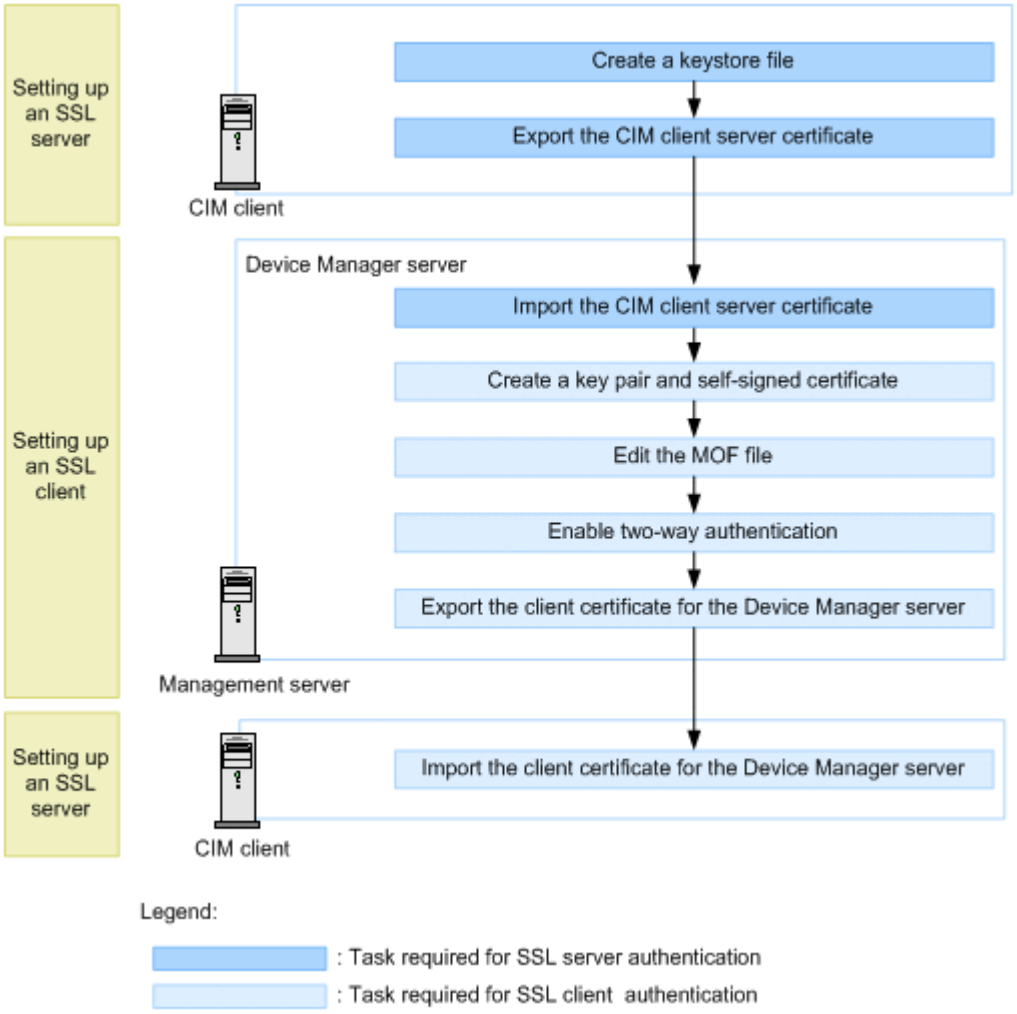


Figure 47 Operation workflow for secure communication between a management server and a CIM client (two-way authentication for event indications)

Note: If you want to restrict which cipher suites are used for SSL/TLS communication, create a new `cimxmlscpa.properties` file, and then specify a value for the `Ciphers` property.

Related concepts

- Configuring an SSL server and clients (CIM server) on page 314
- Configuring an SSL server and clients (CIM client) on page 327

Related tasks

- Changing Device Manager server properties on page 590

Related references

- Ciphers on page 620

Truststores

Truststores are stored in the following locations.

- `jssecacerts`
  The truststore for Common Component. If you use SSL/TLS for the following communication routes, import the certificate into `jssecacerts`:
  - Between the Device Manager server and the Replication Manager server
  - Between the Tuning Manager server and the Device Manager server

  In Windows:

  installation-folder-for-Hitachi-Command-Suite\Base64\uCPSB\jdk\jre\lib\security\jssecacerts

  In Linux:

  installation-directory-for-Hitachi-Command-Suite/Base64/uCPSB/jdk/jre/lib/security/jssecacerts

  Note: If the system is linked with Hitachi File Services Manager or Storage Navigator Modular 2, when you close the port for non-SSL communication for HBase 64 Storage Mgmt Web Service, also import the certificate into `jssecacerts`, which is located in the following location.
  - In Windows:
    installation-folder-for-Hitachi-File-Services-Manager-or-Storage-Navigator-Modular-2\Base\jdk\jre\lib\security\jssecacerts
  - In Linux:
    *installation-directory-for-Hitachi-File-Services-Manager-or-Storage-Navigator-Modular-2/*Base/jdk/jre/lib/security/jssecacerts

- `ldapcacerts`
  The truststore for Common Component. To use StartTLS to communicate with an LDAP directory server, import the certificate into `ldapcacerts`.

  In Windows:

  installation-folder-for-Hitachi-Command-Suite\Base64\conf\sec\ldapcacerts

  In Linux:

  installation-directory-for-Hitachi-Command-Suite/Base64/conf/sec/ldapcacerts

- `dvmcacerts`
  The truststore for the Device Manager server.

If you have applied to the certificate authority for a server certificate of the Device Manager server that is to be used for communication between the management server and the management client (GUI), import the certificate returned from the certificate authority into `dvmcacerts`.
To use SSL/TLS for communication between a Host Data Collector machine and the Device Manager server, import the server certificate for the Host Data Collector into `dvmcacerts`.

In Windows:

installation-folder-for-Hitachi-Command-Suite\DeviceManager\HiCommandServer\dvmcacerts

In Linux:

installation-directory-for-Hitachi-Command-Suite/HiCommandServer/dvmcacerts

Note:
- A truststore file can be changed by using the `server.https.security.truststore` property in the `server.properties` file of the Device Manager server.
- The initial password is `changeit`. To change the password, you must use HiKeytool. If you use other tools or commands, you will not be able to use HiKeytool to import or view server certificates.

- `hdccacerts`
  The truststore for the Host Data Collector.
  If you have applied to the certificate authority for a server certificate for the virtualization server to be used for communication between the virtualization server and the Host Data Collector, import the certificate returned from the certificate authority into `hdccacerts`. The default password is `changeit`.

  In Windows:

  installation-folder-for-Host-Data-Collector\HDC\Base\config\hdccacerts

  In Linux:

  installation-directory-for-Host-Data-Collector/HDC/Base/config/hdccacerts

- `hdvmcacerts`
  The truststore for the Device Manager agent.
  To use SSL/TLS for communication between the management server and a Device Manager agent, import the server certificate for the Device Manager server into `hdvmcacerts`. The default password is `changeit`.

In Windows:

installation-folder-for-Device-Manager-agent\agent\config\hdvmcacerts

In Unix:

installation-directory-for-Device-Manager-agent/agent/config/hdvmcacerts

- .truststore
  The truststore for object operations of the Device Manager server, which is used for SSL server authentication to communicate a CIM client. The default password is trustssl.

  In Windows:

  installation-folder-for-Hitachi-Command-Suite\DeviceManager\HiCommandServer\wsi\server\jserver\bin\.truststore

  In Linux:

  installation-directory-for-Hitachi-Command-Suite/HiCommandServer/wsi/server/jserver/bin/.truststore

- indtruststore
  The truststore for event indications of the Device Manager server, which is used for SSL client authentication to communicate with a CIM client.

  In Windows:

  installation-folder-for-Hitachi-Command-Suite\DeviceManager\HiCommandServer\wsi\server\jserver\bin\indtruststore

  In Linux:

  installation-directory-for-Hitachi-Command-Suite/HiCommandServer/wsi/server/jserver/bin/indtruststore

- Java Web Start truststore

  In Windows:

  Program-Files-folder\Java*JRE-version*\bin\cacerts

  In Linux:

  /usr/java/*JRE-version*/javaws/cacerts

  In HP-UX:

  /opt/*JRE-version*/jre/javaws/cacerts

Related tasks

- Changing Device Manager server properties on page 590

Related references

- server.https.security.truststore on page 619

Configuring an SSL server (Common Component)

To use Common Component as an SSL server, you need to prepare a private key and server certificate, and then specify their storage locations in the `user_httpsd.conf` file.

Creating a secret key and a certificate signing request for Common Component

Use the `hcmds64ssltool` command to create a private key and a certificate signing request (CSR) in Common Component.

The `hcmds64ssltool` command creates two types of private keys: certificate signing requests, and self-signed certificates supporting RSA ciphers and elliptic curve ciphers (ECC). The certificate signing request is created in PEM format. Although you can use this command to create a self-signed certificate, we recommend that you use a self-signed certificate only to test encrypted communications.

Before you begin

- Log in as a user with Administrator permissions (for Windows) or as a root user (for Linux).
- Check the following information:
  - Requirements for the certificate signing request (ask the certificate authority)
  - Version of the Web browser used on the management client
    The signature algorithm of the server certificates must be supported by the Web browser used on the management client (GUI).
  - Existing storage directories for private keys, certificate signing requests, and self-signed certificates (if you recreate them)
    If a file with the same name already exists in the output location, the command does not overwrite the file. Therefore, when you recreate a private key, certificate signing request, or self-signed certificate, you must output it to a directory other than existing storage directories.

Procedure

Execute the following command.

In Windows:

installation-folder-for-Hitachi-Command-Suite\Base64\bin\hcmds64ssltool [/key *private-key-file*] [/csr *certificate-signing-request-file*] [/cert *self-signed-certificate-file*] [/certtext *contents-of-a-self-signed-certificate*] [/validity *number-of-valid-days*] [/dname *DN*] [/sigalg *signature-algorithm-for-server-certificate-for-RSA-cipher*] [/eccsigalg *signature-algorithm-for-server-certificate-for-elliptic-curve-cipher*] [/ecckeysize *key-size-of-private-key-for-elliptic-curve-cipher*]

In Linux:

*installation-directory-for-Hitachi-Command-Suite/*Base64/bin/hcmds64ssltool [-key *private-key-file*] [-csr *certificate-signing-request-file*] [-cert *self-signed-certificate-file*] [-certtext *contents-of-a-self-signed-certificate*] [-validity *number-of-valid-days*] [-dname *DN*] [-sigalg *signature-algorithm-for-server-certificate-for-RSA-cipher*] [/eccsigalg *signature-algorithm-for-server-certificate-for-elliptic-curve-cipher*] [/ecckeysize *key-size-of-private-key-for-elliptic-curve-cipher*]

Options

key

Specify the absolute path to the location to which a private key will be output.

The private key for an RSA cipher is output with the specified file name. The private key for an elliptic curve cipher is output with a file name consisting of the prefix `ecc-` and the specified file name.

The `httpsdkey.pem` file and the `ecc-httpsdkey.pem` file are output if the option is omitted.#

csr

Specify the absolute path to the location to which the certificate signing request will be output.

The certificate signing request for an RSA cipher is output with the specified file name. The certificate signing request for an elliptic curve cipher is output with a file name consisting of the prefix `ecc-` and the specified file name.

The `httpsd.csr` file and the `ecc-httpsd.csr` file are output if the option is omitted.#

cert

Specify the absolute path to the location to which the self-signed certificate will be output.

The self-signed certificate for an RSA cipher is output with the specified file name. The self-signed certificate for an elliptic curve cipher is output with a file name consisting of the prefix `ecc-` and the specified file name.

The `httpsd.pem` file and the `ecc-httpsd.pem` file are output if the option is omitted.#

certtext

Specify the absolute path to the location to which the contents of the self-signed certificate will be output in text format.

The content of the self-signed certificate for an RSA cipher is output with the specified file name. The content of the self-signed certificate for an elliptic curve cipher is output with a file name consisting of the prefix `ecc-` and the specified file name.

The `httpsd.txt` file and the `ecc-httpsd.txt` file are output if the option is omitted.#

validity

Specify the number of days during which the self-signed certificate is valid. If this option is specified, the same content is specified for the RSA cipher and the elliptic curve cipher. If this option is omitted, the valid period is set to 3,650 days.

dname

Specify the DN to be included in the self-signed certificate and certificate signing request. If you execute the command without specifying this option, you will be prompted to specify the DN.

To specify the DN, combine each attribute type with the corresponding attribute value into one attribute by using an equal sign (=), and then specify the attributes by separating each by a comma. For the DN, you cannot specify a double quotation mark (") or backslash (\). In addition, specify each attribute value as defined by RFC2253. For example, if the specified DN includes any of the following characters, escape each of them by using a backslash (\).

A space at the beginning of or at the end of the DN

A hash mark (#) at the beginning of the DN

A plus sign (+), comma (,), semicolon (;), left angle bracket (<), equal sign (=), or right angle bracket (>)

The following table lists and describes the attribute types and values specified for the DN.

Table 53 Attribute types and values specified for the DN

Attribute type	Full name of attribute type	Attribute value
CN	Common Name	Specify the host name of the management server (HBase 64 Storage Mgmt Web Service). This attribute is required. Specify the host name used when connecting to the management server (HBase 64 Storage Mgmt Web Service of Common Component) from the management client (GUI). You can also specify the host name in FQDN format. If the management server is running in a cluster environment, specify the logical host name.
OU	Organizational Unit Name	Specify the name of the organizational unit.
O	Organization Name	Specify the organizational name. This attribute is required.
L	Locality Name	Specify the name of the city, town, or other locality.
ST	State or Province Name	Specify the name of the state or province.
C	Country Name	Specify the two-letter country code.

sigalg

Specify a signature algorithm for the server certificate for the RSA cipher. You can specify `SHA256withRSA` or `SHA1withRSA`. If you omit this specification, SHA256withRSA is used as the signature algorithm.

eccsigalg

Specify a signature algorithm for the server certificate for the elliptic curve cipher. You can specify `SHA512withECDSA`, `SHA384withECDSA`, `SHA256withECDSA`, or `SHA1withECDSA`. If you omit this specification, SHA384withECDSA is used as the signature algorithm.

ecckeysize

Specify the size of the private key for the elliptic curve cipher in bits. The specifiable values are `256` and `384`. If this option is not specified, the key size is 384 bits.

The size of a private key for an RSA cipher is 2,048 bits (fixed).

#

If this option is not specified, the file is output to the following location:

In Windows:

installation-folder-for-Hitachi-Command-Suite\Base64\uCPSB\httpsd\conf\ssl\server\

In Linux:

installation-directory-for-Hitachi-Command-Suite/Base64/uCPSB/httpsd/conf/ssl/server/

Applying to a certificate authority for a Common Component server certificate

Send the Common Component certificate signing request (CSR) that you created to a certificate authority to be digitally signed.

Before you begin

- Create a certificate signing request for Common Component.
- Check the following information:
  - How to apply to the certificate authority and what they support
    You need to have a server certificate issued in X.509 PEM format. For details about how to apply for a certificate, check the website of the certificate authority you will use.
    In addition, make sure that the certificate authority supports the signature algorithm.

Procedure

Send the created certificate signing request to a certificate authority.

Result

Make sure that you save the response from the certificate authority.

Note: Certificates issued by a certificate authority have an expiration date. You need to have a certificate reissued before your certificate expires.

To check the expiration date, use the `hcmds64checkcerts` command.

Related tasks

- Checking the expiration date of the certificate (Common Component) on page 265

Editing the user_httpsd.conf file to enable SSL/TLS

To enable SSL/TLS for Common Component, edit the `user_httpsd.conf` file.

Before you begin

- Create a private key for Common Component (required for enabling SSL/TLS).#
- Prepare a server certificate for Common Component (required for enabling SSL/TLS).#
  Prepare the server certificate sent back from the certificate authority. When testing encrypted communications, you can use a self-signed certificate.
- Check the following information:
  - Host name specified for `Common Name` in the certificate signing request (required for enabling SSL/TLS).

#:

We recommend that you copy the files into the following location.

In Windows:

installation-folder-for-Hitachi-Command-Suite\Base64\uCPSB\httpsd\conf\ssl\server

In Linux:

installation-directory-for-Hitachi-Command-Suite/Base64/uCPSB/httpsd/conf/ssl/server

Procedure

1. Stop the services of the Hitachi Command Suite product.
2. Edit the `user_httpsd.conf` file.

   Storage location of the `user_httpsd.conf` file

   In Windows:

   installation-folder-for-Hitachi-Command-Suite\Base64\uCPSB\httpsd\conf\user_httpsd.conf

   In Linux:

   installation-directory-for-Hitachi-Command-Suite/Base64/uCPSB/httpsd/conf/user_httpsd.conf

   Example of the `user_httpsd.conf` file (default)



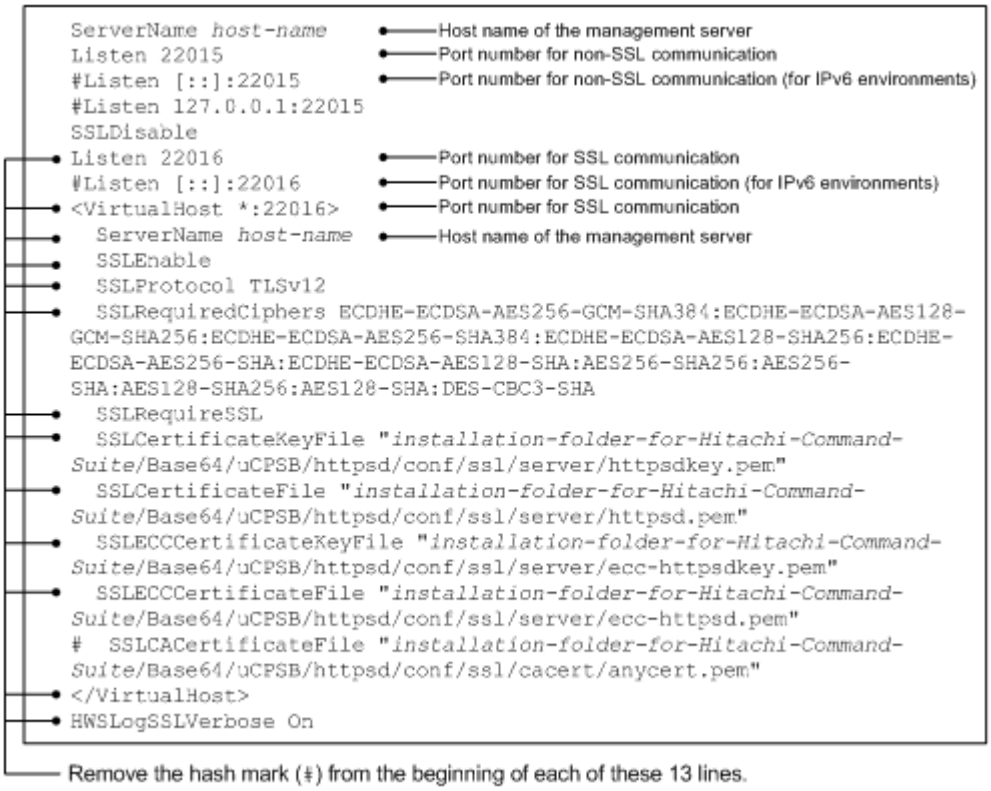
Settings required for enabling SSL/TLS

Note: Note the following when editing the directives:

- Do not specify the same directive twice.
- Do not enter a line break in the middle of a directive.
- When specifying paths in the directives listed below, do not specify symbolic links or junction points.
- When specifying certificates and private key files in the directives listed below, specify PEM-format files.
- Do not edit the `httpsd.conf` file and the `hsso_httpsd.conf` file.

- Remove the hash mark (`#`) at the beginning of the following lines:
  If you use the RSA cipher only, you do not need to remove the hash mark (`#`) at the beginning of the lines for the

SSLECCCertificateKeyFile directive and the SSLECCCertificateFile directive.



- For the ServerName directive on the top line and the ServerName directive within the <VirtualHost> tag, specify the host name (for cluster environments, specify the logical host name) that you specified for Common Name in the certificate signing request. Note that host names are case sensitive.
- For the SSLCertificateKeyFile directive, specify the absolute path to the private key file for Common Component for the RSA cipher.
- For the SSLCertificateFile directive, specify the absolute path of the server certificate for Common Component for the RSA cipher.
- For the SSLECCCertificateKeyFile directive, specify the absolute path to the private key file for the Common Component instance for the elliptic curve cipher. This setting is unnecessary if you use the RSA cipher only.
- For the SSLECCCertificateFile directive, specify the absolute path of the server certificate for the Common Component instance for the elliptic curve cipher. This setting is unnecessary if you use the RSA cipher only.

- If the certificate authority that issued the server certificate of the Common Component was an intermediate certificate authority, remove the hash mark (#) from the beginning of the line for the `SSLCACertificateFile` directive, and then specify the absolute path of all the intermediate certificate authorities. Multiple certificates can be contained in one file by chaining multiple certificates by using a text editor.
- For an IPv6 environment, remove the hash mark (#) at the beginning of the lines `#Listen [::]:22016`.



Note:

- Even if you enable SSL or use Device Manager in an IPv6 environment, do not remove or comment out the line `Listen 22015`.

  To interrupt non-SSL communication from outside the network to the management server, add a hash mark (#) at the beginning of the lines `Listen 22015` and `Listen [::]:22015` to comment them out, and then remove the hash mark at the beginning of the line `#Listen 127.0.0.1:22015`. In this case, if the system is linked with Hitachi File Services Manager or Storage Navigator Modular 2, execute the `hcmdsprmset` command for Hitachi File Services Manager or Storage Navigator Modular 2 with the `print` option specified, and then confirm that the output host name can be resolved to 127.0.0.1. If name resolution cannot be performed, specify the environment settings of the OS so that name resolution can be performed. If name resolution still cannot be performed, set a host name of your choice and 127.0.0.1 for the `hosts` file, and then execute the `hcmdsprmset` command by specifying the host name you set for the `hosts` file for the `host` option.

  If you want to close the port for non-SSL communication that is used for communication in the management server, set the port for non-SSL communication of HBase 64 Storage Mgmt Web Service to closed.

- The content of the elliptic curve cipher is not applied in the `user_httpsd.conf` file if Hitachi Command Suite is upgraded from version 8.2.1 or earlier. If you use the elliptic curve cipher, copy and use the contents of the `SSLRequiredCiphers`, `SSLECCCertificateKeyFile`, and `SSLECCCertificateFile` directives from the sample file stored in the location shown below.

  In Windows:

installation-folder-for-Hitachi-Command-Suite\Base64\sample\httpsd\conf\user_httpsd.conf
In Linux:
installation-directory-for-Hitachi-Command-Suite/Base64/sample/httpsd/conf/user_httpsd.conf

- If the system is linked with Hitachi File Services Manager or Storage Navigator Modular 2, when you enable SSL/TLS, edit the `httpsd.conf` file that is stored in the following location.
  In Windows:
  installation-folder-for-Hitachi-File-Services-Manager-or-Storage-Navigator-Modular-2\Base\httpsd\conf\httpsd.conf
  In Linux:
  installation-directory-for-Hitachi-File-Services-Manager-or-Storage-Navigator-Modular-2/Base/httpsd/conf/httpsd.conf
  Use the same method to edit the file as you used for the `user_httpsd.conf` file. However, for the port number, specify the port number for HBase Storage Mgmt Web Service (the default port for non-SSL communication is 23015, and the default port for SSL communication is 23016).
  For details about how to edit the file, see the manual *Hitachi File Services Manager* or *Storage Navigator Modular 2*.

Tip: To disable SSL/TLS, by referencing the example of the `user_httpsd.conf` file (default), add a hash mark (`#`) at the beginning of the lines from `Listen 22016` to `HWSLogSSLVerbose On` to comment them out.

3. Start the services of Hitachi Command Suite product.

Related tasks

- Closing the port for the non-SSL communication (HBase 64 Storage Mgmt Web Service) on page 262
- Starting the Hitachi Command Suite services on page 458
- Stopping the Hitachi Command Suite services on page 460

Closing the port for the non-SSL communication (HBase 64 Storage Mgmt Web Service)

To close the port for non-SSL communication for HBase 64 Storage Mgmt Web Service (default: 22015) that is used for communication in the

management server, edit the `user_httpsd.conf` file, and then import the certificate to the truststore (`jssecacerts`).

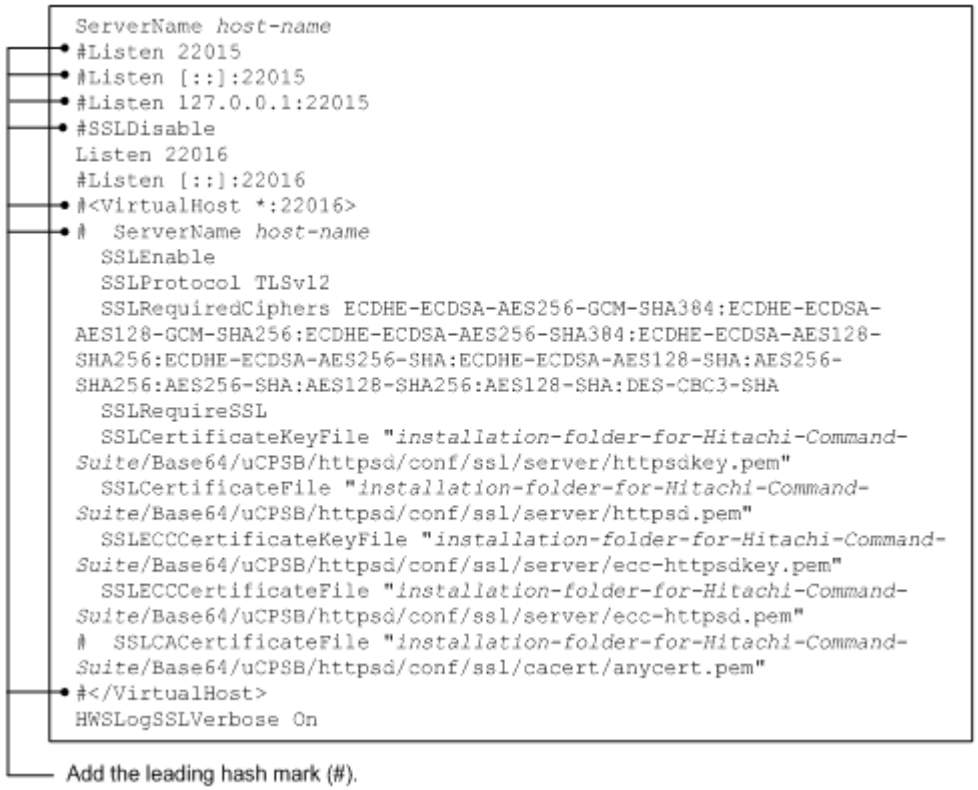
Before you begin

- Checking the host name
  Make sure that the host name specified for `Common Name` in the server certificate is the same as the host name set to the `ServerName` directive at the beginning of the `user_httpsd.conf` file.
- Name resolution settings
  Make sure that name resolution can be performed from the host name (the host name of the management server) that is set to the `ServerName` directive at the beginning of the `user_httpsd.conf` file to the IP address. To do this, execute the following command on the management server.
  `ping` *`host-name-of-the-management-server`*
- Enabling SSL/TLS for Common Component
- Setting the properties in the `tuningmanager.properties` file of the Device Manager server (when Device Manager is linked with Tuning Manager)
  The following properties must be set to SSL:
  - `htnm.server.`*`n`*`.host`
  - `htnm.server.`*`n`*`.protocol`
  - `htnm.server.`*`n`*`.port`

Procedure

1. Stop the services of the Hitachi Command Suite product.
2. Edit the `user_httpsd.conf` file to comment out the non-SSL communication port settings.

   Add a hash mark (`#`) to the beginning of the line below to turn it into a comment. The following example shows the locations for where to add hash marks (`#`). This example indicates the default port number.



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

In Windows:

installation-folder-for-Hitachi-Command-Suite
`\Base64\uCPSB\httpsd\conf\user_httpsd.conf`

In Linux:

installation-directory-for-Hitachi-Command-Suite`/Base64/uCPSB/httpsd/conf/user_httpsd.conf`

Note: Do not edit the `httpsd.conf` file.

3. Import the certificate to the truststore (`jssecacerts`).
4. Make sure that the certificate is imported to the truststore.
5. Start the services of Hitachi Command Suite product.
6. Make sure that you can log in to the Device Manager GUI.

Related tasks

- Importing a certificate into the truststore for Common Component on page 298
- Checking the certificates imported into the truststore for Common Component on page 301

- Starting the Hitachi Command Suite services on page 458
- Stopping the Hitachi Command Suite services on page 460

Checking the expiration date of the certificate (Common Component)

To check the Common Component server certificate or the expiration date of the certificate of the certificate authority, use the `hcmds64checkcerts` command.

The server certificate has an expiration date. Make sure that the certificate is not expired.

Before you begin

- Edit the `user_httpsd.conf` file

  The `hcmds64checkcerts` command enables you to check the expiration date of the certificate specified in the `user_httpsd.conf` file. Therefore, specify the following path of the certificate in the `user_httpsd.conf` file.
  - Server certificate for the Common Component instance

    When a certificate for RSA cipher or elliptic curve cipher is used, the server certificate of the Common Component instance must be specified for each type.
  - Certificate of all of the intermediate certificate authorities

- Log in as a user with Administrator permissions (for Windows) or as a root user (for Linux).

Procedure

Execute the following command to check the expiration date of the certificate.

In Windows:

```
installation-folder-for-Hitachi-Command-Suite\Base64\bin
\hcmds64checkcerts { [/days number-of-days] [/log] | /
all }
```

In Linux:

```
installation-directory-for-Hitachi-Command-Suite/
Base64/bin/hcmds64checkcerts { [-days number-of-days] [-
log] | -all }
```

days

Specify the number of days to check whether a certificate is expired, counting from the day when the command was executed. The specifiable value range is from 30 to 3652 days (10 years). When

this option is specified, certificates that will expire within the specified number of days and certificates that have already expired will be displayed. When this option is not specified, 30 is specified as the number of days.

log

If a certificate to be displayed exists, a warning message will be displayed in the event log (for Windows) or syslog (for Linux). To regularly check the expiration date of a certificate by registering this command in an OS task or cron, specify this option.

all

Displays the expiration date of all certificates specified in the `user_httpsd.conf` file.

Related tasks

- Editing the user_httpsd.conf file to enable SSL/TLS on page 258

Configuring an SSL server (Device Manager server)

To use the Device Manager server as an SSL server, you need to prepare a private key and server certificate.

Creating a key pair and a self-signed certificate for Device Manager server

To create a key pair and a self-signed certificate in the Device Manager server, from the HiKeytool main menu, select SSL configuration for Device Manager Server, and then Make KeyPair/Self-Signed Certificate.

Use the default values unless you are either very familiar with the field of cryptography and Java security or are otherwise instructed. We recommend that you use a self-signed certificate only for testing encrypted communications.

Before you begin

- Log in as a user with Administrator permissions (for Windows) or as a root user (for Linux).
- Delete the existing key pair (when re-creating a key pair).
  A keystore can contain only one key pair. A keystore containing two or more key pairs may cause a problem when the Device Manager server is running in secure mode.
- Check the following information:
  - Version of the Web browser used on the management client
    The signature algorithm of the server certificates must be supported by the Web browser used on the management client (GUI).

Procedure

1. Execute the following to start HiKeytool.

   In Windows:

   installation-folder-for-Hitachi-Command-Suite`\DeviceManager\HiCommandServer\HiKeytool.bat`

   In Linux:

   installation-directory-for-Hitachi-Command-Suite`/HiCommandServer/HiKeytool.sh`

2. In the main menu, enter `1` (**SSL configuration for Device Manager Server**).
3. In the server main menu, enter `1` (**Make KeyPair/Self-Signed Certificate**) .
4. Enter the host name.

   Specify the host name used when connecting to the management server from the management client. You can also specify the host name in FQDN format. If the management server is running in a cluster environment, specify the logical host name.

   Use the default value unless your computer is visible to the LAN or WAN under a different name, in which case you should use the name by which the Device Manager server is visible.

   Note that the backslash (`\`) cannot be used for the values specified in steps 4 to 9.
5. Enter the organizational unit .

   The default value is recommended, but you can use anything that is appropriate, for example, `Marketing`.
6. Enter your organization name.

   Ordinarily you would use the default value or your host name, but you can use another name, such as the name of your company.
7. Enter your city or locality.
8. Enter your state or province.

   Make sure that you spell it out instead of using an abbreviated code.
9. Enter your two-character country code .
10. Enter your key alias.

    Make sure that you enter the same character string as the host name that you specified in step 4.
11. Enter the private key password (minimum of 6 characters).
12. Enter the key algorithm.

Only RSA is supported.

13. Enter the key size.

    Only 2048-bit keys are supported.

14. Enter the signature algorithm.

    SHA256withRSA, SHA1withRSA and MD5withRSA are supported.

15. Enter the number of days for which the key pair and self-signed certificate are valid.
16. Enter the keystore password (minimum of 6 characters).
17. Restart the Hitachi Command Suite product services for the changes to take effect.

    If you will continue to specify other security settings by using HiKeytool, you do not have to restart the services after each setting. Changes will become effective when you restart the services after you have finished specifying all settings by using HiKeytool.

Result

A key pair and self-signed certificate are created and registered into the Device Manager server keystore file (default: `keystore`).

In Windows:

installation-folder-for-Hitachi-Command-Suite`\DeviceManager\HiCommandServer\keystore`

In Linux:

installation-directory-for-Hitachi-Command-Suite`/HiCommandServer/keystore`



Tip: You can change the Device Manager server keystore file by using the `server.https.security.keystore` property in the `server.properties` file on the Device Manager server.

```
>1


Enter Server Name [default=example]:example.com

Enter Organizational Unit [default=Device Manager
Administration]:

Enter Organization Name [default=example]:Hitachi

Enter your City or Locality:New York

Enter your State or Province:New York

Enter your two-character country-code [default=US]:
```

```
Enter Key Alias [default=example]:example.com

Passwords must only contain characters (A-Z,a-z), digits (0-9)
and whitespaces.
Do not enter special characters for your password!
This may render your keystore damaged or unusable!

Enter Key Password (6 characters minimum) [default=passphrase]:

Enter Key Algorithm [default=RSA]:

Enter Key Size [default=2048]:

Enter Signature Algorithm [default=SHA256withRSA]:

Enter number of days valid [default=365]:

Passwords must only contain characters (A-Z,a-z), digits (0-9)
and whitespaces.
Do not enter special characters for your password!
This may render your keystore damaged or unusable!

Enter KeyStore Password (6 characters minimum)
[default=passphrase]:

Creating new X500Name for
example.com...

Creating the Device Manager Server KeyPair for example.com at:
        C:\Program Files\HiCommand\DeviceManager\HiCommandServer
\keystore
        <this can take up to a minute>
        Updating KeyStore password in server.properties ...
        Saving new KeyStore password to disk...
        Updating keypass in server properties...
        Saving new keypass to disk...

All done.
```

Related tasks

- Changing Device Manager server properties on page 590

Related references

- server.https.security.keystore on page 618

Enabling SSL/TLS for the Device Manager server

To enable SSL/TLS for the Device Manager server, from the HiKeytool main menu, select SSL configuration for Device Manager Server, and then Set Device Manager Server Security Level.

Before you begin

- Log in as a user with Administrator permissions (for Windows) or as a root user (for Linux).

- Create a self-signed certificate and key pair for the Device Manager server.

Procedure

1. Start HiKeytool, and then in the main menu, enter `1` (**SSL configuration for Device Manager Server**).
2. In the server main menu, enter `2` (**Set Device Manager Server Security Level**).
3. Enter `2` (**TLS/SSL**).
4. Restart the Hitachi Command Suite product services for the changes to take effect.

   If you will continue to specify other security settings by using HiKeytool, you do not have to restart the services after each setting. Changes will become effective when you restart the services after you have finished specifying all settings by using HiKeytool.

Result

```
>2

Current Device Manager Server Security Level = User Logon (Basic
Authentication)

Options:
1) User Logon (Basic Authentication)
2) TLS/SSL (Secure Sockets)
Enter selection: [default=2]:2

Device Manager Server Security level set to: TLS/SSL Secure
Socket
You must restart the Device Manager Server for this change to
take effect.
```

Creating a certificate signing request for Device Manager server

To create a certificate signing request (CSR) in the Device Manager server, from the HiKeytool main menu, select SSL configuration for Device Manager Server, and then Generate CSR

Before you begin

- Log in as a user with Administrator permissions (for Windows) or as a root user (for Linux).
- Create a key pair for the Device Manager server.
- Enable SSL/TLS for the Device Manager server

Procedure

1. Start HiKeytool, and then in the main menu, enter `1` (**SSL configuration for Device Manager Server**).
2. In the server main menu, enter `3` (**Generate CSR**).

Result

The certificate signing request is saved as a file named *host-name*`.csr` in the following location:

In Windows:

installation-folder-for-Hitachi-Command-Suite`\DeviceManager\HiCommandServer`

In Linux:

installation-directory-for-Hitachi-Command-Suite`/HiCommandServer`

```
>3

Generating CSR...
CSR has been written to disk and saved at:
C:\Program Files\HiCommand\DeviceManager\HiCommandServer
\example.com.csr
All done!
```

The following shows an example of a CSR:

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIC0zCCAbsCAQAwgY0xCzAJBgNVBAYTAkpQMREwDwYDVQQIEwhLYW5hZ2F3YTERM
A8GA1UEBxMIWW9rb2hhbWExEjAQBgNVBAoTCVMxMDM4NDc3MzEwMC4GA1UECxMnSG
lDb21tYW5kIERldmljZSBNYW5hZ2VyIEFkbWluaXN0cmF0aW9uMRIwEAYDVQQDEwl
TMTAzODQ3NzMwggEiMA0GCSqGSIb3DQEB
...
...
...
wEYfCLrKBtlGrzv9eRpcelQIs5bRbzM9S4KGPwbnYKym31281m6MiN27U7t0XWOoI
73xC/jJVlK25+s0tVyerxO9zVYvtirWO2Q+H4KUeQ6tJHo79nY5W2OCVsWr/Vuyh
+XvbVtVnLI8oVPkMUIFnhOQijq+VPSaSlKjiba6NA/+jgT4Fe0dfq31zJ8ELIN/
YtlKCl8txEhO2MXwOQ==
-----END NEW CERTIFICATE REQUEST-----
```

Note: Your CSR will contain extra carriage returns and line feeds which must be included when it is sent to the certificate authority, or it will not be processed correctly.

Applying to a certificate authority for a Device Manager server certificate

Usually, you can apply to a certificate authority for a server certificate online. Send the Device Manager server certificate signing request (CSR) that you created to a certificate authority to be digitally signed.

Before you begin

- Create a certificate signing request for the Device Manager server.
- Check the following information:
  - How to apply to a certificate authority and the support status
    You need to have a server certificate issued in X.509 DER or X.509 PEM format. For details about how to apply for a certificate, check the website of the certificate authority you will use.

Procedure

Send the created certificate signing request to a certificate authority.

Result

Usually, server certificates issued by a certificate authority are sent via email. We recommend that you save the server certificate as a file named *host-name*`.cer` in the following location.

In Windows:

installation-folder-for-Hitachi-Command-Suite`\DeviceManager\HiCommandServer`

In Linux:

installation-directory-for-Hitachi-Command-Suite`/HiCommandServer`

Some certificate authorities might return a server certificate as an attached file with a `.cer` extension. In addition, if a certificate authority returns the response as text in the body of an email, use a text editor to save the response in a new file.



Note:

- Make sure that you save the response from a certificate authority.
- Certificates issued by a certificate authority have an expiration date. You need to have a certificate reissued before your certificate expires.
  Use the HiKeytool to check the expiration date of the certificates.
- The number of valid days specified in a server certificate by a certificate authority will override the value specified by using HiKeytool. If the key pair and associated server certificate expire, it will be impossible to establish a secure connection via SSL/TLS.
  Write down the expiration date by which you need to renew your server certificate.

The following shows an example of a server certificate issued by a certificate authority.

```
-----BEGIN CERTIFICATE-----
MIIDMDCCApmgAwIBAgIDOBcYMA0GCSqGSIb3DQEBBAUAMIGHMQswCQYDVQQGEwJa
QTEiMCAGA1UECBMZRk9SIFRFU1RJTkcgUFVSUE9TRVMgT05MWTEdMBsGA1UEChMU
VGhhd3RlIENlcnRpZmljYXRpb24xFzAVBgNVBAsTDlRFU1QgVEVTVCBURVNUMRww
...
...
...
ADANBgkqhkiG9w0BAQQFAAOBgQBtzeFG4IfvpPnA7G/khD4rrT1TvjbK4Y1pcROM
ce143uUfKgNYgY35UukoNtd120XOoudLwKvJu5JK7846zWIbEJmCr5BYlmywZuao
MQdXMyPOUnqucgg44/JG2F27xqP4atWEZsNlj5R7XGGXi4RPAO5Y0YbbbvMJD0QR
yV0Oxw==
-----END CERTIFICATE-----
```

Related tasks

- Checking the server certificate of the Device Manager server on page 284

Importing a server certificate into the Device Manager server keystore

To import a server certificate issued by a certificate authority into the Device Manager server keystore, from the HiKeytool main menu, select SSL configuration for Device Manager Server, and then Import Digitally Signed Certificate.

Before you begin

- Log in as a user with Administrator permissions (for Windows) or as a root user (for Linux)
- Delete the existing key pair
  A keystore can contain only one key pair. A keystore containing two or more key pairs may cause a problem when the Device Manager server is running in secure mode.
- Obtain a server certificate for the Device Manager server
- Import certificates
  Import the certificates for all certificate authorities including the certificate authority that issued the certificate, intermediate certificate authorities, and the root certificate authority into the Device Manager server truststore.

Procedure

1. Start HiKeytool, and then in the main menu, enter `1` (**SSL configuration for Device Manager Server**).
2. In the server main menu, enter `4` (**Import Digitally Signed Certificate**).

3. Specify the absolute path to the location to which the server certificate will be saved.
4. Restart the Hitachi Command Suite product services for the changes to take effect.

   If you will continue to specify other security settings by using HiKeytool, you do not have to restart the services after each setting. Changes will become effective when you restart the services after you have finished specifying all settings by using HiKeytool.

Result

The server certificate is imported into the keystore file in the Device Manager server (default: `keystore`).

In Windows:

installation-folder-for-Hitachi-Command-Suite`\DeviceManager\HiCommandServer\keystore`

In Linux:

installation-directory-for-Hitachi-Command-Suite`/HiCommandServer/keystore`

Tip: You can change the keystore file in the Device Manager server by editing the `server.https.security.keystore` property in the `server.properties` file.

```
>4

Preparing to import digitally signed certificate.
Enter the location of the digitally signed certificate
[default=C:\Program
Files\HiCommand\DeviceManager\HiCommandServer\example.com.cer]:
Beginning import...

Digitally signed certificate imported. You must restart the
Device Manager
Server for the changes to take effect.
```

Related tasks

- Changing Device Manager server properties on page 590

Related references

- server.https.security.keystore on page 618

Viewing the Device Manager server key pair information in normal mode

To view the key pair information registered in the Device Manager server keystore in normal mode, from the HiKeytool main menu, select SSL

configuration for Device Manager Server, and then Display contents of Device Manager Server KeyStore.

Before you begin

Log in as a user with Administrator permissions (for Windows) or as a root user (for Linux).

Procedure

1. Start HiKeytool, and then in the main menu, enter `1` (**SSL configuration for Device Manager Server**).
2. In the server main menu, enter `5` (**Display contents of Device Manager Server KeyStore**).

Result

The alias for a key pair, the date the key pair was created, and the MD5 Fingerprints are displayed as follows:

```
>5
Listing Contents of Device Manager Server KeyStore

   Alias
   ==========
1) example.com, Tue Apr 01 09:48:02 JST 2008
   MD5  Fingerprints:FC:59:A5:8A:5A:27:5E:70:E4:6B:
21:30:39:D1:00:1D
```

Viewing the Device Manager server key pair information in verbose mode

To view the key pair information registered in the Device Manager server keystore in verbose mode, from the HiKeytool main menu, select SSL configuration for Device Manager Server, and then Display verbose contents of Device Manager Server KeyStore.

Before you begin

Log in as a user with Administrator permissions (for Windows) or as a root user (for Linux).

Procedure

1. Start HiKeytool, and then in the main menu, enter `1` (**SSL configuration for Device Manager Server**).
2. In the server main menu, enter `6` (**Display verbose contents of Device Manager Server KeyStore**).

Result

The verbose information of a key pair is displayed as follows:

```
>6

Listing Contents of Device Manager Server KeyStore

1)
alias: example.com
Certificate chain length: 1
Issued by: example.com: Hitachi
Server Name: example.com
Organizational Unit: Device Manager Administration
Organization: Hitachi
Locality: New York
State: New York
Country: US
Created: Tue Apr 01 09:48:02 JST 2008
Entry Type: Key Entry
Certificate Version: 1
Serial Number: 47f18642
Valid from: Tue Apr 01 09:48:02 JST 2008
Valid to: Wed Apr 01 09:48:02 JST 2009
Certificate: VALID
MD5  Fingerprints: FC:59:A5:8A:5A:27:5E:70:E4:6B:
21:30:39:D1:00:1D
SHA1 Fingerprints: F7:C4:2D:F3:E3:F3:5A:AB:E1:57:D1:E8:9C:
80:07:89:2C:2A:48:7A
```

Deleting a key pair from the Device Manager server keystore

To delete a key pair from the Device Manager server keystore, from the HiKeytool main menu, select SSL configuration for Device Manager Server, and then Delete an entry from the Device Manager Server KeyStore.

Before you begin

Log in as a user with Administrator permissions (for Windows) or as a root user (for Linux).

Procedure

1. Start HiKeytool, and then in the main menu, enter `1` (**SSL configuration for Device Manager Server**).
2. In the server main menu, enter `7` (**Delete an entry from the Device Manager Server KeyStore**).
3. Enter the number of the key pair to be deleted.
4. Check the displayed message, and then press the **y** key.
5. Restart the Hitachi Command Suite product services for the changes to take effect.

   If you will continue to specify other security settings by using HiKeytool, you do not have to restart the services after each setting. Changes will

become effective when you restart the services after you have finished specifying all settings by using HiKeytool.

Result

```
>7

Delete an entry from the Device Manager Server KeyStore.

   Alias
   ==========
1) example.com, Tue Apr 01 09:48:02 JST 2008
   MD5  Fingerprints:FC:59:A5:8A:5A:27:5E:70:E4:6B:
21:30:39:D1:00:1D
Enter number of alias to delete (0 to abort) [default=0]:1

Delete example.com [1] ? [default=No]:y
```

Changing the password of a Device Manager server key pair

To change the password of a Device Manager server key pair, from the HiKeytool main menu, select SSL configuration for Device Manager Server, and then Change Device Manager Server KeyPair/Self-Signed Certificate Keypass.

Before you begin

- Log in as a user with Administrator permissions (for Windows) or as a root user (for Linux).
- Check the following information:
  - Password of the Device Manager server keystore
  - Current password of the Device Manager server key pair

Procedure

1. Start HiKeytool, and then in the main menu, enter `1` (**SSL configuration for Device Manager Server**).
2. In the server main menu, enter `8` (**Change Device Manager Server KeyPair/Self-Signed Certificate Keypass**).
3. Enter the Device Manager server keystore password.
4. Enter the current key pair password.
5. Enter the new key pair password.

   You can use the following characters:

   `A-Z a-z 0-9` spaces

   The password is case sensitive. If you enter a character other than the above, you might render your keystore unusable.
6. Enter the new password again.

7. Restart the Hitachi Command Suite product services for the changes to take effect.

   If you will continue to specify other security settings by using HiKeytool, you do not have to restart the services after each setting. Changes will become effective when you restart the services after you have finished specifying all settings by using HiKeytool.

Changing the password of the Device Manager server keystore

To change the password of the Device Manager server keystore, from the HiKeytool main menu, select SSL configuration for Device Manager Server, and then Change Device Manager Server KeyStore Password.

Before you begin

Check the following information:

- Current password of the Device Manager server keystore.

Procedure

1. Start HiKeytool, and then in the main menu, enter `1` (**SSL configuration for Device Manager Server**).
2. In the server main menu, enter `9` (**Change Device Manager Server KeyStore Password**).
3. Enter the existing password for the Device Manager server.
4. Enter the new keystore password.

   You can use the following characters:

   `A-Z a-z 0-9` spaces

   The password is case sensitive. If you enter a character other than the above, you might render your keystore unusable.
5. Enter the new password again.
6. Restart the Hitachi Command Suite product services for the changes to take effect.

   If you will continue to specify other security settings by using HiKeytool, you do not have to restart the services after each setting. Changes will become effective when you restart the services after you have finished specifying all settings by using HiKeytool.

Importing a certificate into the Device Manager server truststore

To import a certificate into the Device Manager server truststore, from the HiKeytool main menu, select SSL configuration for Device Manager Server, and then Import Certificate to Device Manager Server TrustStore.

Before you begin

- Log in as a user with Administrator permissions (for Windows) or as a root user (for Linux)
- Obtain certificates
  You need to have certificates issued in X.509 DER or X.509 PEM format. Prepare the certificates for all certificate authorities including the certificate authority that issued the certificate, intermediate certificate authorities, and the root certificate authority.

Procedure

1. Start HiKeytool, and then in the main menu, enter `1` (**SSL configuration for Device Manager Server**).
2. In the server main menu, enter `10` (**Import Certificate to Device Manager Server TrustStore**).
3. Enter the alias for the certificate to be imported.
4. Enter the absolute path to the certificate to be imported.
5. Repeat steps 2 through 4 if you import more than one certificate.
6. Restart the Hitachi Command Suite product services for the changes to take effect.

   If you will continue to specify other security settings by using HiKeytool, you do not have to restart the services after each setting. Changes will become effective when you restart the services after you have finished specifying all settings by using HiKeytool.

Related references

- Truststores on page 250

Viewing the Device Manager server truststore information in normal mode

To view the server certificate information registered in the Device Manager server truststore in normal mode, from the HiKeytool main menu, select SSL configuration for Device Manager Server, and then Display contents of Device Manager Server TrustStore.

Before you begin

Log in as a user with Administrator permissions (for Windows) or as a root user (for Linux).

Procedure

1. Start HiKeytool, and then in the main menu, enter `1` (**SSL configuration for Device Manager Server**).

2. In the server main menu, enter `11` (**Display contents of Device Manager Server TrustStore**).

Result

The alias for a server certificate, the date the server certificate was created, and the MD5 Fingerprints are displayed as follows:

```
>11

Listing Contents of Device Manager Server TrustStore

   Alias
   ==========
1) verisignclass3ca, Fri Nov 25 12:04:38 JST 2005
   MD5  Fingerprints:10:FC:63:5D:F6:26:3E:0D:F3:25:BE:5F:79:CD:
67:67
2) verisignclass3g2ca, Fri Nov 25 12:04:37 JST 2005
   MD5  Fingerprints:A2:33:9B:4C:74:78:73:D4:6C:E7:C1:F3:8D:CB:
5C:E9
3) verisignclass2g2ca, Fri Nov 25 12:04:35 JST 2005
   MD5  Fingerprints:
2D:BB:E5:25:D3:D1:65:82:3A:B7:0E:FA:E6:EB:E2:E1
4) verisignclass1g2ca, Fri Nov 25 12:04:34 JST 2005
   MD5  Fingerprints:DB:23:3D:F9:69:FA:4B:B9:95:80:44:73:5E:7D:
41:83
5) verisignclass3g3ca, Fri Nov 25 12:04:37 JST 2005
   MD5  Fingerprints:CD:68:B6:A7:C7:C4:CE:75:E0:1D:4F:
57:44:61:92:09
6) verisignclass2g3ca, Fri Nov 25 12:04:36 JST 2005
   MD5  Fingerprints:F8:BE:C4:63:22:C9:A8:46:74:8B:B8:1D:1E:4A:
2B:F6
7) verisignclass1g3ca, Fri Nov 25 12:04:34 JST 2005
   MD5  Fingerprints:B1:47:BC:18:57:D1:18:A0:78:2D:EC:71:E8:2A:
95:73
8) verisignclass1ca, Fri Nov 25 12:04:35 JST 2005
   MD5  Fingerprints:97:60:E8:57:5F:D3:50:47:E5:43:0C:
94:36:8A:B0:62
9) verisignserverca, Fri Nov 25 12:04:38 JST 2005
   MD5  Fingerprints:74:7B:82:03:43:F0:00:9E:6B:B3:EC:47:BF:
85:A5:93
10) verisignclass2ca, Fri Nov 25 12:04:36 JST 2005
   MD5  Fingerprints:B3:9C:25:B1:C3:2E:32:53:80:15:30:9D:4D:
02:77:3E
```

Related references

- Truststores on page 250

Viewing the Device Manager server truststore information in verbose mode

To view the server certificate information registered in the Device Manager server truststore in verbose mode, from the HiKeytool main menu, select SSL configuration for Device Manager Server, and then Display verbose contents of Device Manager Server TrustStore.

Before you begin

Log in as a user with Administrator permissions (for Windows) or as a root user (for Linux).

Procedure

1. Start HiKeytool, and then in the main menu, enter `1` (**SSL configuration for Device Manager Server**).
2. In the server main menu, enter `12` (**Display verbose contents of Device Manager Server TrustStore**).

Result

The verbose information of a server certificate is displayed as follows:

```
>12

Listing Contents of Device Manager Server TrustStore

1)
alias: verisignclass3ca
Issued by: "VeriSign, Inc."
Organizational Unit: Class 3 Public Primary Certification
Authority
Organization: "VeriSign, Inc."
Country: US
Created: Fri Nov 25 12:04:38 JST 2005
Entry Type: Trusted Certificate
Certificate Version: 1
Serial Number: 70bae41d10d92934b638ca7b03ccbabf
Valid from: Mon Jan 29 09:00:00 JST 1996
Valid to: Wed Aug 02 08:59:59 JST 2028
Certificate: VALID
MD5  Fingerprints: 10:FC:63:5D:F6:26:3E:0D:F3:25:BE:5F:79:CD:
67:67
SHA1 Fingerprints: 74:2C:31:92:E6:07:E4:24:EB:
45:49:54:2B:E1:BB:C5:3E:61:74:E2
```

Related references

- Truststores on page 250

Deleting a server certificate from the Device Manager server truststore

To delete a server certificate registered in the Device Manager server truststore, from the HiKeytool main menu, select SSL configuration for Device Manager Server, and then Delete an entry from the Device Manager Server TrustStore.

Before you begin

Log in as a user with Administrator permissions (for Windows) or as a root user (for Linux).

Procedure

1. Start HiKeytool, and then in the main menu, enter `1` (**SSL configuration for Device Manager Server**).
2. In the server main menu, enter `13` (**Delete an entry from the Device Manager Server TrustStore**).
3. Enter the number of the server certificate to be deleted.
4. Check the displayed message, and then press the **y** key.
5. Restart the Hitachi Command Suite product services for the changes to take effect.

   If you will continue to specify other security settings by using HiKeytool, you do not have to restart the services after each setting. Changes will become effective when you restart the services after you have finished specifying all settings by using HiKeytool.

Result

HiKeytool will delete the nominated entry, and redisplay the contents of the Device Manager server truststore. Confirm that the deletion has been completed.

```
>13

Delete an entry from the Device Manager Server TrustStore.

   Alias
   ==========
1) verisignclass3ca, Fri Nov 25 12:04:38 JST 2005
   MD5  Fingerprints:10:FC:63:5D:F6:26:3E:0D:F3:25:BE:5F:79:CD:
67:67
2) verisignclass3g2ca, Fri Nov 25 12:04:37 JST 2005
   MD5  Fingerprints:A2:33:9B:4C:74:78:73:D4:6C:E7:C1:F3:8D:CB:
5C:E9
3) verisignclass2g2ca, Fri Nov 25 12:04:35 JST 2005
   MD5  Fingerprints:
2D:BB:E5:25:D3:D1:65:82:3A:B7:0E:FA:E6:EB:E2:E1
4) verisignclass1g2ca, Fri Nov 25 12:04:34 JST 2005
   MD5  Fingerprints:DB:23:3D:F9:69:FA:4B:B9:95:80:44:73:5E:7D:
41:83
5) verisignclass3g3ca, Fri Nov 25 12:04:37 JST 2005
   MD5  Fingerprints:CD:68:B6:A7:C7:C4:CE:75:E0:1D:4F:
57:44:61:92:09
6) verisignclass2g3ca, Fri Nov 25 12:04:36 JST 2005
   MD5  Fingerprints:F8:BE:C4:63:22:C9:A8:46:74:8B:B8:1D:1E:4A:
2B:F6
7) verisignclass1g3ca, Fri Nov 25 12:04:34 JST 2005
   MD5  Fingerprints:B1:47:BC:18:57:D1:18:A0:78:2D:EC:71:E8:2A:
95:73
8) verisignclass1ca, Fri Nov 25 12:04:35 JST 2005
   MD5  Fingerprints:97:60:E8:57:5F:D3:50:47:E5:43:0C:
94:36:8A:B0:62
9) verisignserverca, Fri Nov 25 12:04:38 JST 2005
   MD5  Fingerprints:74:7B:82:03:43:F0:00:9E:6B:B3:EC:47:BF:
85:A5:93
```

```
10) verisignclass2ca, Fri Nov 25 12:04:36 JST 2005
   MD5  Fingerprints:B3:9C:25:B1:C3:2E:32:53:80:15:30:9D:4D:
02:77:3E

Enter number of alias to delete (0 to abort) [default=0]:1

Delete verisignclass3ca [1] ?  [default=No]:
```

Related references

- Truststores on page 250

Changing the password of the Device Manager server truststore

To change the password of the Device Manager server truststore, from the HiKeytool main menu, select SSL configuration for Device Manager Server, and then Change Device Manager Server TrustStore Password.

Before you begin

- Log in as a user with Administrator permissions (for Windows) or as a root user (for Linux).
- Check the following information:
  - Current password of the Device Manager server truststore.

Procedure

1. Start HiKeytool, and then in the main menu, enter `1` (**SSL configuration for Device Manager Server**).
2. In the server main menu, enter `14` (**Change Device Manager Server TrustStore Password**).
3. Enter the existing truststore password.
4. Enter the new truststore password.

   You can use the following characters:

   `A-Z a-z 0-9` spaces

   The password is case sensitive. If you enter a character other than the above, you might render your keystore unusable.
5. Enter the new password again.
6. Restart the Hitachi Command Suite product services for the changes to take effect.

   If you will continue to specify other security settings by using HiKeytool, you do not have to restart the services after each setting. Changes will become effective when you restart the services after you have finished specifying all settings by using HiKeytool.

Related references

- Truststores on page 250

Checking the server certificate of the Device Manager server

To check the server certificate of the Device Manager server, use the HiKeytool.

The server certificate has an expiration date. Make sure that the certificate is not expired.

Before you begin

Log in as a user with Administrator permissions (for Windows) or as a root user (for Linux).

Procedure

1. Start HiKeytool, and then in the main menu, enter `1` (**SSL configuration for Device Manager Server**).
2. In the server main menu, enter `6` (**Display verbose contents of Device Manager Server KeyStore**).

Result

Detailed information of the server certificate is displayed. Check the `Valid to:` line.

Related tasks

- Viewing the Device Manager server key pair information in verbose mode on page 275

Configuring an SSL server (Host Data Collector)

To use Host Data Collector as an SSL server, you need to prepare a key pair and server certificate.

Creating a key pair and a certificate signing request for Host Data Collector

To create a key pair and a self-signed certificate from the Host Data Collector machine, use the `hdc_ssltool` command. A certificate signing request and self-signed certificate are created with a private key size of 2,048 bits, the key algorithm RSA, and the signature algorithm SHA256withRSA. Although you can use this command to create a self-signed certificate, we recommend that you use a self-signed certificate only to test encrypted communications.

Before you begin

- Log in as a user with Administrator permissions (for Windows) or as a root user (for Linux)
- Delete an existing keystore file of Host Data Collector (if you re-create the file)
  Host Data Collector can create only one keystore file.

Procedure

Execute the following command.

In Windows:

```
installation-folder-for-Host-Data-Collector\HDC\Base\bin
\hdc_ssltool.bat -key keystore-file-name -csr
certificate-signing-request-file -keypass private-key-
password -storepass keystore-password [-cert self-signed-
certificate-file] [-validity number-of-valid-days] [-
dname entity-distinguished-name]
```

In Linux:

```
installation-directory-for-Host-Data-Collector/HDC/
Base/bin/hdc_ssltool.sh -key keystore-file-name -csr
certificate-signing-request-file -keypass private-key-
password -storepass keystore-password [-cert self-signed-
certificate-file] [-validity number-of-valid-days] [-
dname entity-distinguished-name]
```

Options

key

Specify the absolute path to the location to which a private key will be output.

csr

Specify the absolute path to the location to which the certificate signing request will be output.

keypass

Specify the private key password (minimum of 6 characters).

For the `keypass` option and the `storepass` option, specify the same password.

storepass

Specify the keystore password (minimum of 6 characters).

For the `storepass` option and the `keypass` option, specify the same password.

cert

Specify the absolute path to the location to which the self-signed certificate will be output.

validity

Specify the number of days during which the self-signed certificate is valid. If this option is omitted, the valid period is set to 3,650 days.

dname

Specify the DN to be included in the self-signed certificate and certificate signing request. If you execute the command without specifying this option, you will be prompted to specify the DN.

Related tasks

- Creating a secret key and a certificate signing request for Common Component on page 253

Applying to a certificate authority for a Host Data Collector server certificate

Usually, you can apply to a certificate authority for a server certificate online. Send the Host Data Collector certificate signing request (CSR) that you created to a certificate authority to be digitally signed.

Before you begin

- Create a certificate signing request for Host Data Collector.
- Check the following information:
  - How to apply to the certificate authority and what they support
    Make sure that the certificate authority you use supports signatures using SHA256withRSA. For details about how to apply for a certificate, check the website of the certificate authority you will use.

Procedure

Send the created certificate signing request to a certificate authority.

Result

Usually, server certificates issued by a certificate authority are sent via email. Make sure that you save the response from the certificate authority.

Note: Certificates issued by a certificate authority have an expiration date. You need to have a certificate reissued before your certificate expires.

Use the `keytool` utility to check the expiration date.

Related tasks

- Checking a Host Data Collector server certificate on page 288

Importing the Host Data Collector server certificates into the keystore

To import the server certificates into the Host Data Collector keystore, use the `keytool` utility.

Before you begin

- Log in as a user with Administrator permissions (for Windows) or as a root user (for Linux)
- Obtain certificates for certificate authorities.
  Prepare the certificates for all certificate authorities including the certificate authority that issued the certificate, intermediate certificate authorities, and the root certificate authority.
- Obtain a Host Data Collector server certificate issued by a certificate authority.
- Check the following information:
  - Information of the keystore file
    You need the information of the keystore file prepared when creating a self-signed certificate.
    - Absolute path
    - Access password

Procedure

1. Execute the following command to import a certificate of a certificate authority.

   In Windows:

   ```
   installation-folder-for-Host-Data-Collector\HDC\Base
   \uCPSB\jdk\jre\bin\keytool -import -alias alias -keystore
   keystore-file-name -file certificate-file-name
   ```

   In Linux:

   ```
   installation-directory-for-Host-Data-Collector/HDC/Base/
   uCPSB/jdk/jre/bin/keytool -import -alias alias -keystore
   keystore-file-name -file certificate-file-name
   ```

   - `alias`: Specify the name used to identify the certificate in the keystore.
     For the alias name of a certificate of a certificate authority, specify a name other than `hdc`.
   - `keystore`: Specify the keystore file by using an absolute path.
   - `file`:Specify absolute path to the certificate of the certificate authority.
2. Execute the following command to import a Host Data Collector server certificate.

In Windows:

installation-folder-for-Host-Data-Collector\HDC\Base\uCPSB\jdk\jre\bin\keytool -import -alias hdc -keystore *keystore-file-name* -file *certificate-file-name*

In Linux:

installation-directory-for-Host-Data-Collector/HDC/Base/uCPSB/jdk/jre/bin/keytool -import -alias hdc -keystore *keystore-file-name* -file *certificate-file-name*

- `alias`: Specify the name used to identify the certificate in the keystore.
  For the alias name of the Host Data Collector server certificate, always specify `hdc`.
- `keystore`: Specify the keystore file by using an absolute path.
- `file`: Specify absolute path to the certificate file.

Checking a Host Data Collector server certificate

Use the `keytool` utility to check the Host Data Collector server certificate. The server certificate has an expiration date. Make sure that the certificate is not expired.

Procedure

Execute the following command:

In Windows:

installation-folder-for-Host-Data-Collector\HDC\Base\uCPSB\jdk\jre\bin\keytool -printcert -v -file *certificate-file-name*

In Linux:

installation-directory-for-Host-Data-Collector/HDC/Base/uCPSB/jdk/jre/bin/keytool -printcert -v -file *certificate-file-name*

Configuring an SSL client

To communicate by using SSL/TLS, you need to import the server certificate created by an SSL server into an SSL client.

Downloading a Device Manager server truststore file

Download a truststore file for the Device Manager server (`HiCommandCerts`) from a Web browser.

Before you begin

- Import a server certificate of the Device Manager server, if you use a server certificate issued by a certificate authority.

- Import a certificate into the truststore .
- Import a server certificate into the keystore.

- Create a self-signed certificate for the Device Manager server, if you use a self-signed certificate.
  We recommend that you use a self-signed certificate only for testing encrypted communications or any temporary use.
- Check the following information:
  - Non-SSL communication port number for the Device Manager server (default: 2001)
    You can use the `server.http.port` property in the `server.properties` file for Device Manager server to check the port number.
  - Device Manager user account

Procedure

From the management server, use a Web browser or OS commands to download the truststore file from the URL below.

Specify your user account to download the file.

`http://`*`loopback-IP-address-or-loopback-host-name`*`:`*`Device Manager-server-port-number`*`/service/HiCommandCerts`

Related tasks

- Creating a key pair and a self-signed certificate for Device Manager server on page 266
- Importing a server certificate into the Device Manager server keystore on page 273
- Importing a certificate into the Device Manager server truststore on page 278

Related references

- server.http.port on page 592

Creating a truststore file to be used in the Device Manager CLI

To create a truststore file to be used in the Device Manager CLI, you must use the `keytool` utility and create a truststore file that has imported certificates from the certificate authority.

Before you begin

- Log in as a user with Administrator permissions (for Windows) or as a root user (for Linux)
- Obtain certificates from the certificate authority

Prepare the certificates for all certificate authorities chained from the certificate authority that issued the certificate for the Device Manager server to the root certificate authority.

Procedure

Execute the following command to create a truststore file that has imported certificates issued from the certificate authority.

In Windows:

installation-folder-for-Hitachi-Command-Suite`\Base64\uCPSB\jdk\jre\bin\keytool -import -trustcacerts -alias` *alias-name* `-keystore` *truststore-file-name* `-file` *certificate-file-name*

In Linux:

installation-directory-for-Hitachi-Command-Suite`/Base64/uCPSB/jdk/jre/bin/keytool -import -trustcacerts -alias` *alias-name* `-keystore` *truststore-file-name* `-file` *certificate-file-name*

- `alias`: Specify the name used to identify the certificate in the truststore. Specify any name.
- `keystore`: Specify the truststore file by using an absolute path.
- `file`: Specify absolute path to the certificate of the certificate authority.

Related tasks

- Applying to a certificate authority for a Device Manager server certificate on page 271

Exporting a Device Manager server self-signed certificate

To export a Device Manager Server self-signed certificate from the downloaded truststore file (`HiCommandCerts`), use the `hcmds64keytool` utility (for Windows) or the `keytool` utility (for Linux).

Before you begin

- Download the Device Manager server truststore file.
- Check the following information:
  - Alias name for the Device Manager server key pair.
    You can use the HiKeytool to check the alias.

Procedure

1. Execute the following command.

   In Windows:

installation-folder-for-Hitachi-Command-Suite\Base64\bin\hcmds64keytool -export -keystore *truststore-file* -alias *alias-name* -file *server-certificate*

In Linux:

installation-directory-for-Hitachi-Command-Suite/Base64/uCPSB/jdk/bin/keytool -export -keystore *truststore-file* -alias *alias-name* -file *server-certificate*

- `keystore`: Specify the truststore file path.
- `alias`: Specify the alias name for the key pair.
- `file`: Specify the path of the self-signed certificate file to be output.

2. Press the **Enter** key without entering the password of the Device Manager server truststore file.

Related tasks

- Viewing the Device Manager server key pair information in normal mode on page 274

Importing a certificate into a web browser (Internet Explorer)

To use the GUI, you first need to import a certificate into the web browser of the management client (GUI).

Before you begin

- Obtaining a certificate
  When using the certificate authority, the certificates issued by all the authorities from the authority that issued the following server certificates to the root certificate authority must form a certificate chain.
  - Common Component
  - Device Manager server

Procedure

1. Start Internet Explorer®, and then select **Tools** and **Internet Options**.

   The **Tools** menu might not appear. In this case, press the **Alt** key to display the menu bar, and then perform the above operation.
2. Click the **Certificates** button in the **Content** tab, and then import the certificate into the browser.

Related tasks

- Creating a secret key and a certificate signing request for Common Component on page 253

- Applying to a certificate authority for a Common Component server certificate on page 257
- Applying to a certificate authority for a Device Manager server certificate on page 271

Importing a certificate into a web browser (Firefox)

To use the GUI, you first need to import a certificate into the web browser of the management client (GUI).

Before you begin

- Obtaining a certificate

  When using the certificate authority, the certificates issued by all the authorities from the authority that issued the following server certificates to the root certificate authority must form a certificate chain.
  - Common Component
  - Device Manager server

Procedure

1. Start Firefox®, and then select the following menu options:.

   In Windows:

   Select **Tools** and **Options**.

   In Linux:

   Select **Edit** and **Preferences**.
2. Select **Advanced**.
3. Click the **View Certificates** button in the **Encryption** tab, and then import the certificate into the browser.

Related tasks

- Creating a secret key and a certificate signing request for Common Component on page 253
- Applying to a certificate authority for a Common Component server certificate on page 257
- Applying to a certificate authority for a Device Manager server certificate on page 271

Importing a certificate into a web browser (Google Chrome)

To use the GUI, you first need to import a certificate into the web browser of the management client (GUI).

Before you begin

- Obtaining a certificate

When using the certificate authority, the certificates issued by all the authorities from the authority that issued the following server certificates to the root certificate authority must form a certificate chain.
  - Common Component
  - Device Manager server

Procedure

1. Start Google Chrome, select **Customize and control Google Chrome** and then **Setting**.
2. Click **Show advanced settings**.
3. In the **HTTPS/SSL** menu, click the **Manage certificates** button to import the certificate to the web browser.

Related tasks

- Creating a secret key and a certificate signing request for Common Component on page 253
- Applying to a certificate authority for a Common Component server certificate on page 257
- Applying to a certificate authority for a Device Manager server certificate on page 271

Changing pop-up blocker settings

If you change the Hitachi Command Suite product URL to the SSL version of the URL, in Web browser, you must register the SSL version of the URL in the pop-up blocker settings.

Before you begin

- Change the Hitachi Command Suite product URL.
- Check the following information:
  - IP address or host name of the management server

Procedure

In the pop-up blocker settings in the Web browser, register the following URL for the website addresses you want to permit.

`https://`*`management-server-IP-address-or-host-name`*

Related tasks

- Changing the URL for accessing Hitachi Command Suite products (hcmds64chgurl command) on page 154

Enabling SSL/TLS for the Device Manager CLI computer

Set the environment variable `HDVM_CLI_CERTS_PATH` for the storage location of the truststore file to be used in the Device Manager CLI.

If you set the `HiCommandCLI.serverurl` property or `secure` property in the `HiCommandCLI.properties`file in advance, you can skip specifying the URL and the `secure` (`s`) option when using the Device Manager CLI.

Before you begin

- Create a truststore file (when using the certificate authority)
  Create a truststore file that has imported certificates from the certificate authority. Change the file name of the truststore file to `HiCommandCerts`, and save the file in the directory that contains the Device Manager CLI executable (`HiCommandCLI.bat`).
- Obtain a Device Manager server truststore file (when using a self-signed certificate)
  Obtain the file from the management server using a secure way, and then save it in the directory that contains the Device Manager CLI executable (`HiCommandCLI.bat`) without changing the file name.
- Set the Java environment by using the Device Manager CLI.
  In an environment that satisfies both of the following conditions, to use SSL/TLS for communication between the Device Manager server and the Device Manager CLI, you need to change the Java environment used by the Device Manager CLI:
  - The Device Manager CLI is executed from the management server in which the Device Manager server is installed.
  - The JDK bundled with Hitachi Command Suite is being used by the Device Manager CLI.

  For details, see *Hitachi Command Suite CLI Reference Guide*.
- Check the following information:
  - IP address or host name of the management server
    Check the Common Name set in the Device Manager server certificate.
  - SSL communication port number for Device Manager (default: 2443)
    You can use the `server.https.port` property in the `server.properties` file for Device Manager to check the port number.

Procedure

1. Specify the absolute path for the truststore file, including the file name, for the environment variable `HDVM_CLI_CERTS_PATH`.

2. Change the setting in the `HiCommandCLI.properties` file.

   The `HiCommandCLI.properties` file is stored in the directory in which the Device Manager CLI executable (`HiCommandCLI.bat`) is stored.

   - `HiCommandCLI.serverurl` property

     Specify the Device Manager server URL in the following format:

     ```
     HiCommandCLI.serverurl=https://management-server-IP-address-or-host-name:Device-Manager-SSL-communication-port-number/service
     ```

   - `secure` property

     Set `true`. Because the `secure` property is not included in the template file, add it as follows:

     ```
     ##### OPTIONS ####
     secure=true
     ```

Related references

- server.https.port on page 593

Downloading the Tiered Storage Manager server truststore files

Access the management server from a Web browser and download the truststore file (`TieredStorageManagerCerts`) of the Tiered Storage Manager server.

Before you begin

- Set the `server.properties` file for the Tiered Storage Manager server.
  - `server.rmi.secure` property
  - `server.rmi.security.port` property
- Check the following information:
  - Non-SSL communication port number for HBase 64 Storage Mgmt Web Service (default: 22015)

    You can use the `user_httpsd.conf` file to check the port number.
  - User account for Tiered Storage Manager

Procedure

From the management server, use a Web browser or OS commands to download the truststore file from the URL below.

Specify your user account to download the file.

```
http://loopback-IP-address-or-loopback-host-name:port-number-for-HBase-64-Storage-Mgmt-Web-Service/TieredStorageManager/TieredStorageManagerCerts
```

Related tasks

- Changing ports used by Common Component on page 114
- Changing Tiered Storage Manager server properties on page 642

Related references

- server.rmi.security.port on page 644
- server.rmi.secure on page 655

Enabling SSL/TLS for the Tiered Storage Manager CLI computer

Set the storage location of the Tiered Storage Manager server truststore file (`TieredStorageManagerCerts`) for the environment variable `HTSM_CLI_CERTS_PATH`.

If you use the `htsmcli.properties` file, change the settings for the `htsmserver.location` and `option.secure` properties.

If you set the `htsmserver.location` property or `option.secure` property in the `htsmcli.properties` file in advance, you can skip specifying the location of the Tiered Storage Manager server and the `secure` (`s`) option when using the Tiered Storage Manager CLI.

Before you begin

- Obtain a truststore file for the Tiered Storage Manager server.
  Obtain the file from the management server using a secure way.
- Copy the `htsmcli.properties` template file.
  Copy the template at the location noted below to a folder. In Windows, do not copy the file to a location immediately under the root of a drive.
  - When executing Tiered Storage Manager CLI commands from a management client
    In Windows:
    system-drive\TieredStorageManager*Tiered-Storage-Manager-version*\CLI\
    In Solaris, HP-UX, or Linux:
    /opt/TieredStorageManager/*Tiered-Storage-Manager-version*/CLI/
  - When executing Tiered Storage Manager CLI commands from the management server
    In Windows:
    installation-folder-for-Hitachi-Command-Suite\TieredStorageManager\CLI\
    In Linux:
    installation-directory-for-Hitachi-Command-Suite/TieredStorageManager/CLI/
- Set the environment variable `HTSM_CLI_HOME`

Set the storage directory for the `htsmcli.properties` file. In Windows, specify the path as follows:
  - Do not enclose the path in quotation marks (") or apostrophes (').
  - Do not place a path delimiter (\) at the end of the path.
  - Use a backslash (\) to escape a path delimiter.

- Check the following information:
  - Host name or IP address for management server
  - SSL communication port number for the Tiered Storage Manager server (default: 24500)
    You can use the `server.rmi.security.port` property in the `server.properties` file of the Tiered Storage Manager server to check the port number.

Procedure

1. Specify the absolute path of the truststore file, including the file name, for the environment variable `HTSM_CLI_CERTS_PATH`.

   If you run the Tiered Storage Manager CLI with the current directory set as the server certificate storage directory, you can omit the `HTSM_CLI_CERTS_PATH` setting.
2. Change the settings in the `htsmcli.properties` file.
   - `htsmserver.location` property
     Specify the location of the Tiered Storage Manager server in the following format:

     ```
     htsmserver.location=rmi://management-server-IP-address-or-host-name:Tiered-Storage-Manager-server-SSL-port-number/HTSMServer
     ```

   - `option.secure` property
     Set `true`. Because the `option.secure` property is not included in the template file, add it as follows:

     ```
     #####  OPTIONS ####
     option.secure=true
     ```

Related tasks

- Changing ports used by Common Component on page 114

Related references

- server.rmi.security.port on page 644

Importing a certificate into the truststore for Common Component

To import a certificate to the truststore (`ldapcacerts` or `jssecacerts`), use the `hcmds64keytool` utility (for Windows) or the `keytool` utility (for Linux).

Before you begin

- Prepare a certificate
  Obtain the certificate using a secure way.
  - For communication with an LDAP directory server
    The certificates issued by all the authorities from the authority that issued an LDAP directory server certificate to the root certificate authority must form a certificate chain. The certificate must satisfy the product requirements for Hitachi Command Suite.
  - For communication with a Replication Manager server
    When using a certificate authority:
    The certificates issued by all the authorities from the authority that issued the Device Manager server certificate to the root certificate authority must form a certificate chain.
    When using a self-signed certificate:
    Export a Device Manager server self-signed certificate from the truststore file.
  - For communication with the Tuning Manager server
    When using a certificate authority:
    The certificates issued by all the authorities from the authority which issued the Common Component server certificate to the root certificate authority must form a certificate chain
    When using a self-signed certificate:
    Obtain a Common Component self-signed certificate.
  - For closing the port (default: 22015) for the non-SSL communication of HBase 64 Storage Mgmt Web Service
    When using a certificate authority:
    The certificates issued by all the authorities from the authority which issued the Common Component server certificate to the root certificate authority must form a certificate chain
    When using a self-signed certificate:
    Obtain a Common Component self-signed certificate.

- Check the following information:
  - Path of the truststore file
  - Password to access the truststore, if the truststore already exists

Procedure

1. Execute the following command.

   In Windows:

   ```
   installation-folder-for-Hitachi-Command-Suite\Base64\bin
   \hcmds64keytool -import -alias alias -file certificate-
   file-name -keystore truststore-file-name -storepass
   password-to-access-the-truststore
   ```

   In Linux:

   ```
   installation-directory-for-Hitachi-Command-Suite/Base64/
   uCPSB/jdk/bin/keytool -import -alias alias -file
   certificate-file-name -keystore truststore-file-name -
   storepass password-to-access-the-truststore
   ```

   - `alias`: Specify the name used to identify the certificate in the truststore.
     If there are two or more server certificates, specify an alias name which is not used in the truststore.
   - `file`: Specify the certificate file.
   - `keystore`: Specify the truststore file path of the import destination. If no truststore file exists, one will be automatically created.
     We recommend that you import LDAP directory server certificates into `ldapcacerts`. If you want to share a certificate with other programs, you can import the certificate into `jssecacerts`.
     Import a certificate for communication between the Replication Manager server and the Device Manage server or between the Tuning Manager server and the Device Manager server, or the server certificate used when the port for the non-SSL communication of HBase 64 Storage Mgmt Web Service was closed into `jssecacerts`.
   - `storepass`: Specify the password used to access the truststore.

   Note:
   - Note the following when you use the `hcmds64keytool` or `keytool` utility to specify a unique name in the truststore, the truststore file name, and the password:
     - Do not use the following symbols in the file name:
     `: , ; * ? " < > |`
     - Specify the file name as a character string of no more than 255 bytes.
     - Do not include double quotation marks (`"`) in the unique name in the truststore or the password.

- If the system is linked with Hitachi File Services Manager or Storage Navigator Modular 2, when you close the port for non-SSL communication for HBase 64 Storage Mgmt Web Service, also execute the following commands:
  In Windows:
  installation-folder-for-Hitachi-File-Services-Manager-or-Storage-Navigator-Modular-2\Base\bin\hcmdskeytool -import -alias *alias* -file *certificate-file-name* -keystore *truststore-file-name* -storepass *password-to-access-the-truststore*
  In Linux:
  installation-directory-for-Hitachi-File-Services-Manager-or-Storage-Navigator-Modular-2/Base/jdk/bin/keytool -import -alias *alias* -file *certificate-file-name* -keystore *truststore-file-name* -storepass *password-to-access-the-truststore*

---

2. Restart the services of Hitachi Command Suite product.

Related tasks

- Creating a secret key and a certificate signing request for Common Component on page 253
- Applying to a certificate authority for a Common Component server certificate on page 257
- Applying to a certificate authority for a Device Manager server certificate on page 271
- Starting the Hitachi Command Suite services on page 458
- Stopping the Hitachi Command Suite services on page 460

Related references

- Truststores on page 250

Conditions for an LDAP directory server certificate

To use StartTLS to communicate between the management server and an LDAP directory server, check that the obtained LDAP directory server certificate satisfies the following requirement:

- The CN (in the `Subject` line) of the LDAP directory server certificate matches the value of the following specified attributes in the `exauth.properties` file.
  - When the server uses LDAP for the authentication method
    `auth.ldap.`*`value-specified-for-auth.server.name`*`.host`
  - When the server uses RADIUS for the authentication method and links with an external authorization server

When an external authentication server and the authorization server are running on the same computer:
`auth.radius.`*`value-specified-for-auth.server.name`*`.host`
When the external authentication server and authorization server are running on different computers:
`auth.group.`*`domain-name`*`.host`

- When the server uses Kerberos for the authentication method and links with an external authorization server
  `auth.kerberos.`*`value-specified-for-auth.kerberos.realm_name`*`.kdc`

Related tasks

- Registering an external authentication server and an external authorization server on page 178

Checking the certificates imported into the truststore for Common Component

To check the certificates imported into the Common Component truststore (`ldapcacerts` or `jssecacerts`), use the `hcmds64keytool` utility (for Windows) and the `keytool` utility (for Linux).

Before you begin

Check the following information:

- Path of the truststore file
- Password to access the truststore

Procedure

Execute the following command.

In Windows:

`installation-folder-for-Hitachi-Command-Suite``\Base64\bin\hcmds64keytool -list -v -keystore `*`truststore-file-name`*` -storepass `*`password-to-access-the-truststore`*

In Linux:

`installation-directory-for-Hitachi-Command-Suite``/Base64/uCPSB/jdk/bin/keytool -list -v -keystore `*`truststore-file-name`*` -storepass `*`password-to-access-the-truststore`*

- `keystore`: Specify the truststore file path where the certificate is stored.
- `storepass`: Specify the password for accessing the truststore.

Related references

- Truststores on page 250

Deleting the certificates imported into the truststore for Common Component

To delete the certificates imported into the Common Component truststore (`ldapcacerts` or `jssecacerts`), use the `hcmds64keytool` utility (for Windows) and the `keytool` utility (for Linux).

Before you begin

Check the following information:

- Alias name of the certificate to be deleted
- Path of the truststore file
- Password to access the truststore

Procedure

Execute the following command.

In Windows:

installation-folder-for-Hitachi-Command-Suite\Base64\bin\hcmds64keytool -delete -alias *alias-name* -keystore *truststore-file-name* -storepass *password-to-access-the-truststore*

In Linux:

installation-directory-for-Hitachi-Command-Suite/Base64/uCPSB/jdk/bin/keytool -delete -alias *alias-name* -keystore *truststore-file-name* -storepass *password-to-access-the-truststore*

- `alias`: Specify the alias name for the certificate.
- `keystore`: Specify the truststore file path where the certificate is stored.
- `storepass`: Specify the password for accessing the truststore.

Related tasks

- Checking the certificates imported into the truststore for Common Component on page 301

Related references

- Truststores on page 250

Changing the communication protocol between the Replication Manager server and the Device Manager server

You can change the communication protocol between the Replication Manager server and the Device Manager server in the Edit Device Manager window of the Replication Manager GUI.

Before you begin

- Name resolution settings
  Make sure that management clients can resolve the IP address for the management server at the primary site from the host name. For example, register the server into the `hosts` file.
- Import the Device Manager server certificate into the truststore (`jssecacerts`).
- Check the following information:
  - IP address or host name of the Device Manager server to connect to
  - SSL port number of the Device Manager server to connect to (default: 2443)
    You can use the `server.https.port` property in the `server.properties` file of the Device Manager server to check the port number.

Procedure

1. Select **Manage Replication** from the **Actions** menu in the Device Manager GUI.
2. Click **Administration**, and then **Information Source** in the **Explorer** menu.
3. Select **Device Manager** in the tree frame.
4. Click the  icon in the Device Manager to communicate via SSL/TLS.
5. Change the communication protocol and port number in the Edit Device Manager window.

Related references

- server.https.port on page 593

Importing a certificate into the truststore for Device Manager server

To import a certificate into the Device Manager server truststore, from the HiKeytool main menu, select SSL configuration for Device Manager Server, and then Import Certificate to Device Manager Server TrustStore.

Before you begin

- Log in as a user with Administrator permissions (for Windows) or as a root user (for Linux)
- Prepare a certificate
  Obtain the certificate using a secure way.
  - When using a certificate authority:
    The certificates issued by all the authorities from the authority which issued the Host Data Collector server certificate to the root certificate authority must form a certificate chain
  - When using a self-signed certificate:
    Obtain a Host Data Collector self-signed certificate.

Procedure

1. Execute the following to start HiKeytool.

   In Windows:

   ```
   installation-folder-for-Hitachi-Command-Suite
   \DeviceManager\HiCommandServer\HiKeytool.bat
   ```

   In Linux:

   ```
   installation-directory-for-Hitachi-Command-Suite/
   HiCommandServer/HiKeytool.sh
   ```

2. In the main menu, enter `1` (**SSL configuration for Device Manager Server**).
3. In the server main menu, enter `10` (**Import Certificate to Device Manager Server TrustStore**).
4. Enter the alias for the certificate to be imported.
5. Enter the absolute path to the certificate to be imported.
6. Repeat steps 1 through 5 if you import more than one certificate.
7. Restart the Hitachi Command Suite product services for the changes to take effect.

Related tasks

- Creating a key pair and a certificate signing request for Host Data Collector on page 284
- Applying to a certificate authority for a Host Data Collector server certificate on page 286
- Starting the Hitachi Command Suite services on page 458
- Stopping the Hitachi Command Suite services on page 460

Related references

- Truststores on page 250

Checking the certificates imported into the truststore for Device Manager server

To check the certificates imported into the Device Manager server truststore, use HiKeytool.

There are two methods for checking the certificates: Normal mode and verbose mode. Use them appropriately according to your needs.

Related tasks

- Viewing the Device Manager server truststore information in normal mode on page 279
- Viewing the Device Manager server truststore information in verbose mode on page 280

Importing a certificate into the truststore for Host Data Collector

To import a server certificate for a virtualization server into the truststore of the Host Data Collector, use the `keytool` utility.

Before you begin

- Log in as a user with Administrator permissions (for Windows) or as a root user (for Linux)
- Obtaining and replacing the server certificate
  Apply to a certificate authority to obtain a server certificate for a virtualization server. If you are creating a certificate signing request (CSR), specify the IP address of the virtualization server that issued the certificate as a Subject Alternative Name.
  If a virtualization server that is managed by Host Data Collector includes VMware ESXi, the certificates issued by all the authorities, from the authority that issued the server certificate for the virtualization server to the root certificate authority, form a certificate chain, and a server certificate is required.
  Replace the obtained server certificate with the self-signed certificate that is imported to the virtualization server. For details, see VMware manuals.

Procedure

1. Execute the following command.

   In Windows:

   ```
   installation-folder-for-Host-Data-Collector\HDC\Base
   \uCPSB\jdk\jre\bin\keytool -import -alias alias -keystore
   truststore-file-name -file server-certificate
   ```

   In Linux:

```
installation-directory-for-Host-Data-Collector/HDC/Base/
uCPSB/jdk/jre/bin/keytool -import -alias alias -keystore
truststore-file-name -file server-certificate
```

- `alias`: Specify the name used to identify the certificate in the truststore.
- `keystore`: Specify the following path as the truststore file of the import destination.
  In Windows:
  installation-folder-for-Host-Data-Collector\HDC\Base\config\hdccacerts
  In Linux:
  installation-directory-for-Host-Data-Collector/HDC/Base/config/hdccacerts
- `file`: Specify the absolute path of the server certificate.

2. Enter the truststore password.

   The default password is `changeit`.

Related references

- Truststores on page 250

Checking the server certificate imported into the truststore for the Host Data Collector

To check the certificate imported into the truststore, use the `keytool` utility.

Before you begin

Check the following information:
- Password for accessing the truststore

Procedure

1. Execute the following command:

   In Windows:

   ```
   installation-folder-for-Host-Data-Collector\HDC\Base
   \uCPSB\jdk\jre\bin\keytool -list -alias alias -keystore
   truststore-file-name
   ```

   In Linux:

   ```
   installation-directory-for-Host-Data-Collector/HDC/Base/
   uCPSB/jdk/jre/bin/keytool -import -list alias -keystore
   truststore-file-name
   ```

- `alias`: Specify the name used to identify the certificate in the truststore.
- `keystore`: Specify the following path as the truststore file that contains the certificate.
  In Windows:
  installation-folder-for-Host-Data-Collector`\HDC\Base\config\hdccacerts`
  In Linux:
  installation-directory-for-Host-Data-Collector`/HDC/Base/config/hdccacerts`

2. Enter the truststore password.

   The default password is `changeit`.

Related references

- Truststores on page 250

Changing the truststore password for the Host Data Collector

To change the truststore password for the Host Data Collector, use the `keytool` utility.

Before you begin

- Password for accessing the truststore

Procedure

1. Execute the following command:

   In Windows:

   installation-folder-for-Host-Data-Collector`\HDC\Base\uCPSB\jdk\jre\bin\keytool -storepasswd -keystore` *truststore-file-name*

   In Linux:

   installation-directory-for-Host-Data-Collector`/HDC/Base/uCPSB/jdk/jre/bin/keytool -storepasswd -keystore` *truststore-file-name*

   - `keystore`: Specify the following path as the truststore file whose password is to be changed:
     In Windows:
     installation-folder-for-Host-Data-Collector`\HDC\Base\config\hdccacerts`
     In Linux:

installation-directory-for-Host-Data-Collector/HDC/Base/config/hdccacerts

2. Specify the current truststore password.

   The default password is `changeit`.
3. Specify a new truststore password.

   You can use the following characters:

   `A-Z a-z 0-9` spaces

   The password is case sensitive.

   Specify a new password (minimum of 6 characters).
4. Specify the new truststore password again.

Related references

- Truststores on page 250

Changing virtualization server information

You can change the communication protocol between the Device Manager server and a virtual server in the Edit Hosts window of the Device Manager GUI or with the `ModifyVirtualizationServer` command in the Device Manager CLI.

This section explains how to change information registered in the Device Manager GUI.

For details on the`ModifyVirtualizationServer` command, see the *Hitachi Command Suite CLI Reference Guide*.

Before you begin

- Configure an SSL server on a virtual server.
  For details, see VMware manuals.

Procedure

1. Select **Managed Resources** in the **Administration** tab.
2. Select a virtual server in the **Hosts** tab, and click the **Edit Hosts** button.
3. Change the communication protocol in the Edit Hosts window.

Importing a server certificate into the truststore for the Device Manager agent

To import a server certificate for the Device Manager server into the truststore of the Device Manager agent, use the `hdvmagt_setting` command.

Use the `hdvmagt_setting` command to set the following:

- Importing a server certificate of the Device Manager server into the truststore of the Device Manager agent
- Specifying settings in the property file of the Device Manager agent
  - `server.server.ssl.hdvm`
    Set `true`.
  - `server.server.serverPort`
    Set the port number for SSL communication.

Before you begin

- Log in as a user with Administrator permissions (for Windows) or as a root user (for UNIX).
- Obtain a server certificate.
  Obtain server certificates created by the management server by using a secure method.
  - Server certificate for the Device Manager server
    When you use a self-signed certificate for testing encrypted communication or any temporary use, you first need to export the server certificate from the truststore file (`HiCommandCerts`).
- Check the following information:
  - Access password for the truststore of the Device Manager agent (if the default password is changed)
  - Port number of the Device Manager server
    You can check this value by using the `server.http.port` property (for non-SSL communication with the Device Manager server) or the `server.https.port` property (for SSL communication with the Device Manager server) in the `server.properties` file for the Device Manager server.
  - User ID and password for the Device Manager agent
    The relevant user account must belong to the Device Manager `PeerGroup`.

Procedure

Execute the following command to interactively set the SSL communication:

In Windows:

installation-folder-for-Device-Manager-agent\bin\hdvmagt_setting

In Linux:

installation-directory-for-Device-Manager-agent/bin/hdvmagt_setting

In Solaris or HP-UX:

/opt/HDVM/HBaseAgent/bin/hdvmagt_setting

In AIX:

/usr/HDVM/HBaseAgent/bin/hdvmagt_setting

Related tasks

- Applying to a certificate authority for a Device Manager server certificate on page 271

Related references

- Truststores on page 250
- Setting the Device Manager server's information, HiScan command's execution period, and CCI's information (hdvmagt_setting command) on page 533

Checking the server certificate imported into the truststore for the Device Manager agent

To check the server certificate imported into the truststore, use the hbsa_keytool utility (for Windows) or the keytool utility (for UNIX).

Before you begin

Check the following information:

- Password for accessing the truststore

Procedure

Execute the following command:

In Windows:

installation-folder-for-Device-Manager-agent\bin\hbsa_keytool -list -keystore *truststore-file-name* -storepass *password-for-accessing-truststore*

In Linux:

installation-directory-for-Device-Manager-agent/agent/JRE1.5/bin/keytool -list -keystore *truststore-file-name* -storepass *password-for-accessing-truststore*

In Solaris, AIX, and HP-UX:

installation-directory-for-JDK-or-JRE/bin/keytool -list -keystore *truststore-file-name* -storepass *password-for-accessing-truststore*

- keystore: Specify the following path as the truststore file that contains the server certificate.
  In Windows:
  installation-folder-for-Device-Manager-agent\agent\config\hdvmcacerts
  In UNIX:
  installation-directory-for-Device-Manager-agent/agent/config/hdvmcacerts
- storepass: Specify the password for accessing the truststore.

Related references

- Truststores on page 250

Changing the truststore password for the Device Manager agent

To change the truststore password for the Device Manager agent, use the hbsa_keytool utility (for Windows) or the keytool utility (for UNIX).

Before you begin

- Password for accessing the truststore

Procedure

1. Execute the following command:

   In Windows:

   installation-folder-for-Device-Manager-agent\bin\hbsa_keytool -storepasswd -keystore *truststore-file-name*

   In Linux:

   installation-directory-for-Device-Manager-agent/agent/JRE1.5/bin/keytool -storepasswd -keystore *truststore-file-name*

   In Solaris, AIX, and HP-UX:

   installation-directory-for-JDK-or-JRE/bin/keytool -storepasswd -keystore *truststore-file-name*

   - keystore: Specify the following path as the truststore file whose password is to be changed:
     In Windows:

installation-folder-for-Device-Manager-agent\agent\config\hdvmcacerts

In UNIX:

installation-directory-for-Device-Manager-agent/agent/config/hdvmcacerts

2. Specify the current truststore password.
3. Specify a new truststore password.

   You can use the following characters:

   `A-Z a-z 0-9` spaces

   The password is case sensitive.

   Specify a new password (minimum of 6 characters).
4. Specify the new truststore password again.

Related references

- Truststores on page 250

Deleting a server certificate imported into the truststore for the Device Manager agent

To delete a server certificate imported into the truststore , use the `hbsa_keytool` utility (for Windows) or the `keytool` utility (for UNIX).

Before you begin

Check the following information:

- Alias name of the server certificate to be deleted
- Password for accessing the truststore

Procedure

Execute the following command:

In Windows:

installation-folder-for-Device-Manager-agent\bin\hbsa_keytool -delete -alias *alias-name* -keystore *truststore-file-name* -storepass *password-for-accessing-truststore*

In Linux:

installation-directory-for-Device-Manager-agent/agent/JRE1.5/bin/keytool -delete -alias *alias-name* -keystore *truststore-file-name* -storepass *password-for-accessing-truststore*

In Solaris, AIX, and HP-UX:

```
installation-directory-for-JDK-or-JRE/bin/keytool -delete
-alias alias-name -keystore truststore-file-name -
storepass password-for-accessing-truststore
```

- `alias`: Specify the alias name for the server certificate.
- `keystore`: Specify the following path as the truststore file that contains the server certificate.
  In Windows:
  installation-folder-for-Device-Manager-agent`\agent\config\hdvmcacerts`
  In UNIX:
  installation-directory-for-Device-Manager-agent`/agent/config/hdvmcacerts`
- `storepass`: Specify the password for accessing the truststore.

Related tasks

- Checking the server certificate imported into the truststore for the Device Manager agent on page 310

Related references

- Truststores on page 250

Changing storage system information

You can change the communication protocol between the Device Manager server and a storage system from the Edit Storage Systems window in the Device Manager GUI or the `AddStorageArray` command of the Device Manager CLI.

This section shows how to change registered information from the Device Manager GUI.

For details on the `AddStorageArray` command, see the *Hitachi Command Suite CLI Reference Guide*.

Before you begin

- Configure an SSL server in the storage system.
  For details, see Storage Navigator Modular 2 manuals.
- Refresh the storage system
- Check the following information (For SMI-S enabled storage systems):
  - Port to communicate with the SMI-S provider (default: 5989).

Procedure

1. Select **Managed Resources** in the **Administration** tab.
2. Select a storage system in the **Storage Systems** tab, and click the **Edit Storage Systems** button.
3. Change a communication protocol and port in the Edit Storage Systems window.

Configuring an SSL server and clients (CIM server)

To use SSL server authentication for object operations, you need to create a server certificate in the Device Manager server, and then import it into the CIM client. To use two-way authentication, you need to create a client certificate in the CIM client and then import it into the Device Manager server.

To use SSL server authentication for event indications, you need to create a server certificate in the CIM client, and then import it into the Device Manager server. To use two-way authentication, you need to create a client certificate in the Device Manager server and then import it into the CIM client.

Creating a keystore file for object operations

To create a keystore file for object operations, use the `hcmds64keytool` utility (for Windows) or the `keytool` utility (for Linux)

Before you begin

- Delete the existing keystore file for object operations.

  In Windows:

  installation-folder-for-Hitachi-Command-Suite\DeviceManager\HiCommandServer\wsi\server\jserver\bin\.keystore

  In Linux:

  installation-directory-for-Hitachi-Command-Suite/HiCommandServer/wsi/server/jserver/bin/.keystore

Procedure

1. Execute the following command to create a keystore file for object operations.

   In Windows:

   installation-folder-for-Hitachi-Command-Suite\Base64\bin\hcmds64keytool -genkey -keystore *keystore-file-name* -storepass *keystore-password* -alias *alias* -dname *entity-*

distinguished-name -validity *validity-of-certificate* -keypass *private-key-password* -keyalg *key-algorithm* -sigalg *signature-algorithm* -keysize *key-size*

In Linux:

installation-directory-for-Hitachi-Command-Suite/Base64/uCPSB/jdk/bin/keytool -genkey -keystore *keystore-file-name* -storepass *keystore-password* -alias *alias* -dname *entity-distinguished-name* -validity *validity-of-certificate* -keypass *private-key-password* -keyalg *key-algorithm* -sigalg *signature-algorithm* -keysize *key-size*

- `keystore`: Specify the keystore file for object operations (`.keystore`) .
- `storepass` and `keypass`: Specify the same password.

2. Execute `WSIEncryptString.jar` to encrypt the keystore password.

   `WSIEncryptString.jar` is stored at the following paths.

   In Windows:

   installation-folder-for-Hitachi-Command-Suite\DeviceManager\HiCommandServer\wsi\server\jserver\lib\

   In Linux:

   installation-directory-for-Hitachi-Command-Suite/HiCommandServer/wsi/server/jserver/lib/

   ```
   > java -jar WSIEncryptString.jar keystore-password
   ```

Result

The encrypted keystore password is displayed. You will need to specify this string in the MOF file for object operations.

Editing an MOF file for object operations

Set the keystore password encrypted by `WSIEncryptString.jar` in the MOF file for object operations, and then compile the file.

Before you begin

- Create a keystore file for object operations.
- Check the following information:
  - Keystore password encrypted by `WSIEncryptString.jar`.

Procedure

1. Stop the Hitachi Command Suite product services.
2. Set the keystore password encrypted by `WSIEncryptString.jar` in the MOF file for object operations (`CIMXMLSCOMATLSSettingData_instances.mof`).

   The MOF file is stored in the following locations.

   In Windows:

   installation-folder-for-Hitachi-Command-Suite
   `\DeviceManager\HiCommandServer\wsi\server\jserver\mof\wbemserver`

   In Linux:

   installation-directory-for-Hitachi-Command-Suite/
   `HiCommandServer/wsi/server/jserver/mof/wbemserver`

   Replace `XXXXXX` in `KeyStorePassword` with the encrypted keystore password.

```
instance of HITACHI_CIMXMLSCOMATLSSettingData {
    InstanceID          =
HITACHI:HITACHI_CIMXMLSCOMATLSSettingData:001";
    ElementName         = "CIM-XML Client Adapter TLS
Settings";
    MutualAuthenticationRequired = false;
    KeyStoreFile        = "{0}/jserver/bin/.keystore";
    KeyStorePassword = "XXXXXX";
    TrustStoreFile      = "{0}/jserver/bin/.truststore";
};
```

3. Execute the `mofcomp` command to compile the MOF file for object operations.

   In Windows:

   installation-folder-for-Hitachi-Command-Suite
   `\DeviceManager\HiCommandServer\wsi\bin\mofcomp.bat`

   In Linux:

   installation-directory-for-Hitachi-Command-Suite/
   `HiCommandServer/wsi/bin/mofcomp`

```
mofcomp -m -o ..\server\jserver\logr ..\server\jserver\mof
\wbemserver
\CIMXMLSIndicationHandlerTLSSettingData_instances.mof
```

4. Start the Hitachi Command Suite product services.

Related tasks

- Starting the Hitachi Command Suite services on page 458

- Stopping the Hitachi Command Suite services on page 460

Exporting a server certificate for object operations

To export a Device Manager server certificate for object operations from the keystore file (`.keystore`), select SSL configuration for SMI-S, and then Export Server's Certificate from KeyStore for Object Operations from the HiKeytool main menu.

Before you begin

- Edit the MOF file for object operations.
- Check the following information:
  - Keystore password for object operations
  - Alias name of the server certificate for object operations

Procedure

1. Execute the following to start HiKeytool.

   In Windows:

   ```
   installation-folder-for-Hitachi-Command-Suite
   \DeviceManager\HiCommandServer\HiKeytool.bat
   ```

   In Linux:

   ```
   installation-directory-for-Hitachi-Command-Suite/
   HiCommandServer/HiKeytool.sh
   ```

2. In the main menu, enter `2` (**SSL configuration for SMI-S**).
3. In the SMI-S main menu, enter `5` (**Export Server's Certificate from KeyStore for Object Operations**).
4. Specify the keystore password, alias name, and output destinations for the server certificate for object operations.

```
Enter keystore-password:serverssl
Enter alias:foocorpserver
Enter authentication-filename(absolute path):c:\tmp\server.cer
```

Enabling two-way authentication for object operations

To enable two-way authentication for object operations, select SSL configuration for SMI-S, and then Set Security Level for Object Operations from the HiKeytool main menu.

Procedure

1. Stop the Hitachi Command Suite product services.
2. Execute the following to start HiKeytool.

   In Windows:

   installation-folder-for-Hitachi-Command-Suite\DeviceManager\HiCommandServer\HiKeytool.bat

   In Linux:

   *installation-directory-for-Hitachi-Command-Suite/*HiCommandServer/HiKeytool.sh

3. In the main menu, enter `2` (**SSL configuration for SMI-S**).
4. In the SMI-S main menu, enter `1` (**Set Security Level for Object Operations**) .
5. Enter `2` (**SSL with two-way authentication**) .

   The MOF file for object operations will be compiled and the SMI-S main menu will appear again.
6. Start the Hitachi Command Suite product services.

```
You must stop the Device Manager Server before specifying this
setting.
1) SSL without two-way authentication
2) SSL with two-way authentication

>2
```

Note: If the message `The compilation of the MOF file failed.` appears, collect all the files in the following location, and then contact maintenance personnel.

In Windows:

installation-folder-for-Hitachi-Command-Suite\DeviceManager\HiCommandServer\wsi\server\jserver\mof\wbemserver

In Linux:

*installation-directory-for-Hitachi-Command-Suite/*HiCommandServer/wsi/server/jserver/mof/wbemserver

Related tasks

- Starting the Hitachi Command Suite services on page 458
- Stopping the Hitachi Command Suite services on page 460

Importing a client certificate for object operations

To import a CIM client certificate for object operations in two-way authentication into the truststore file (`.truststore`), select SSL configuration for SMI-S, and then Import Client's Certificate to TrustStore for Object Operations from the HiKeytool main menu.

Before you begin

- Obtain the client certificate for object operations from a CIM client.
- Delete the existing truststore file for object operations (`.truststore`).

Procedure

1. Execute the following to start HiKeytool.

   In Windows:

   installation-folder-for-Hitachi-Command-Suite
   `\DeviceManager\HiCommandServer\HiKeytool.bat`

   In Linux:

   installation-directory-for-Hitachi-Command-Suite/
   `HiCommandServer/HiKeytool.sh`

2. In the main menu, enter `2` (**SSL configuration for SMI-S**).
3. In the SMI-S main menu, enter `3` (**Import Client's Certificate to TrustStore for Object Operations**) .
4. Specify the alias name, truststore password, and absolute path of the client certificate for object operations.

```
Enter alias:foocorpclient
Enter truststore-password:truststssl
Enter authentication-filename(absolute path):c:\tmp\client.cer
```

Related tasks

- Exporting a server or client certificate for a CIM client on page 328

Related references

- Truststores on page 250

Creating a keystore file for event indications

To create a keystore file for event indications, use the`hcmds64keytool` utility (for Windows) or the `keytool` utility (for Linux).

Before you begin

- Delete the existing keystore file for event indications if you want to re-create the file.

  In Windows:

  installation-folder-for-Hitachi-Command-Suite\DeviceManager\HiCommandServer\wsi\server\jserver\bin\indkeystore

  In Linux:

  installation-directory-for-Hitachi-Command-Suite/HiCommandServer/wsi/server/jserver/bin/indkeystore

Procedure

1. Execute the following command to create a keystore file for event indications:

   In Windows:

   installation-folder-for-Hitachi-Command-Suite\Base64\bin\hcmds64keytool -genkey -keystore *keystore-file-name* -storepass *keystore-password* -alias *alias* -dname *entity-distinguished-name* -validity *validity-of-certificate* -keypass *private-key-password* -keyalg *key-algorithm* -sigalg *signature-algorithm* -keysize *key-size*

   In Linux:

   installation-directory-for-Hitachi-Command-Suite/Base64/uCPSB/jdk/bin/keytool -genkey -keystore *keystore-file-name* -storepass *keystore-password* -alias *alias* -dname *entity-distinguished-name* -validity *validity-of-certificate* -keypass *private-key-password* -keyalg *key-algorithm* -sigalg *signature-algorithm* -keysize *key-size*

   - `keystore`: Specify the keystore file for event indications (`indkeystore`).
   - `storepass` and `keypass`: Specify the same password.

2. Execute `WSIEncryptString.jar` to encrypt the keystore password.

   `WSIEncryptString.jar` is stored at the following paths.

   In Windows:

   installation-folder-for-Hitachi-Command-Suite\DeviceManager\HiCommandServer\wsi\server\jserver\lib\

   In Linux:

installation-directory-for-Hitachi-Command-Suite/
HiCommandServer/wsi/server/jserver/lib/

```
> java -jar WSIEncryptString.jar keystore-password
```

Result

An encrypted keystore password is displayed. Specify this string in the MOF file for event indications.

Editing an MOF file for event indications

Specify a keystore password encrypted by `WSIEncryptString.jar` in the MOF file for event indications, and then compile the file.

Before you begin

- Create a keystore file for event indications.
- Check the following information:
  - Keystore password encrypted by `WSIEncryptString.jar`.

Procedure

1. Stop the Hitachi Command Suite product services.
2. Set the keystore password encrypted by `WSIEncryptString.jar` in the MOF file for event indications (`CIMXMLSIndicationHandlerTLSSettingData_instances.mof`), and then change the `MutualAuthenticationRequired` value to `true`.

   The MOF file is stored in the following locations:

   In Windows:

   installation-folder-for-Hitachi-Command-Suite
   \DeviceManager\HiCommandServer\wsi\server\jserver\mof
   \wbemserver

   In Linux:

   installation-directory-for-Hitachi-Command-Suite/
   HiCommandServer/wsi/server/jserver/mof/wbemserver

   Replace `xxxxxxx` in `KeyStorePassword` with the encrypted keystore password.

```
 instance of HITACHI_CIMXMLSIndicationHandlerTLSSettingData {

    InstanceID          =
"HITACHI:HITACHI_CIMXMLSIndicationHandlerTLSSettingData:001";
    ElementName         = "CIM_XML-TLS Indication Handler
Settings";
    MutualAuthenticationRequired = true;
```

```
    KeyStoreFile        = "{0}/jserver/bin/indkeystore";
    KeyStorePassword = "xxxxxxx";
    TrustStoreFile      = "{0}/jserver/bin/indtruststore";
};
```

3. Execute the `mofcomp` command to compile the MOF file for event indications.

   In Windows:

   installation-folder-for-Hitachi-Command-Suite
   `\DeviceManager\HiCommandServer\wsi\bin\mofcomp.bat`

   In Linux:

   installation-directory-for-Hitachi-Command-Suite/
   `HiCommandServer/wsi/bin/mofcomp`

```
mofcomp -m -o ..\server\jserver\logr ..\server\jserver\mof
\wbemserver\CIMXMLSCOMATLSSettingData_instances.mof
```

4. Start the Hitachi Command Suite product services.

Related tasks

- Starting the Hitachi Command Suite services on page 458
- Stopping the Hitachi Command Suite services on page 460

Exporting a client certificate for event indications

To export a client certificate for event indications in two-way authentication from the keystore (`indkeystore`) file, select SSL configuration for SMI-S, and then Export Server's Certificate from KeyStore for Event Indications from the HiKeytool main menu.

Before you begin

- Edit the MOF file for event indications.
- Check the following information:
  - Keystore password for event indications
  - Alias name of the client certificate for event indications

Procedure

1. Execute the following to start HiKeytool.

   In Windows:

   installation-folder-for-Hitachi-Command-Suite
   `\DeviceManager\HiCommandServer\HiKeytool.bat`

   In Linux:

installation-directory-for-Hitachi-Command-Suite/
HiCommandServer/HiKeytool.sh

2. In the main menu, enter 2 (**SSL configuration for SMI-S**).
3. In the SMI-S main menu, enter 6 (**Export Server's Certificate from KeyStore for Event Indications**) .
4. Specify the keystore password, alias name, and output destinations for the client certificate for event indications.

```
Enter keystore-password:serverindtrust
Enter alias:foocorpindserver
Enter authentication-filename(absolute path):c:\tmp
\serverind.cer
```

Enabling two-way authentication for event indications

To enable two-way authentication for event indications, select SSL configuration for SMI-S, and then Set Security Level for Event Indications from the HiKeytool main menu.

Procedure

1. Stop the Hitachi Command Suite product services.
2. Execute the following to start HiKeytool.

   In Windows:

   installation-folder-for-Hitachi-Command-Suite
   \DeviceManager\HiCommandServer\HiKeytool.bat

   In Linux:

   installation-directory-for-Hitachi-Command-Suite/
   HiCommandServer/HiKeytool.sh

3. In the main menu, enter 2 (**SSL configuration for SMI-S**).
4. In the SMI-S main menu, enter 2 (**Set Security Level for Event Indications**) .
5. Enter 2 (**SSL with two-way authentication**) .

   The MOF file for event indications will be compiled, and the SMI-S main menu will appear again.
6. Start the Hitachi Command Suite product services.

```
You must stop the Device Manager Server before specifying this
setting.
1) SSL without two-way authentication
2) SSL with two-way authentication
```

```
>2
```

Note: If the message `The compilation of the MOF file failed.` appears, collect all the files at the following location, and then contact maintenance personnel.

In Windows:

installation-folder-for-Hitachi-Command-Suite\DeviceManager\HiCommandServer\wsi\server\jserver\mof\

In Linux:

installation-directory-for-Hitachi-Command-Suite/HiCommandServer/wsi/server/jserver/mof/

Related tasks

- Starting the Hitachi Command Suite services on page 458
- Stopping the Hitachi Command Suite services on page 460

Importing a server certificate for event indications

To import a server certificate for event indications of a CIM client into the truststore file (`indtruststore`), select SSL configuration for SMI-S, and then Import Client's Certificate to TrustStore for Event Indications from the HiKeytool main menu.

Before you begin

- Obtain a CIM client server certificate for event indications.
- Delete the existing truststore file for event indications (`indtruststore`).

Procedure

1. Execute the following to start HiKeytool.

   In Windows:

   installation-folder-for-Hitachi-Command-Suite\DeviceManager\HiCommandServer\HiKeytool.bat

   In Linux:

   installation-directory-for-Hitachi-Command-Suite/HiCommandServer/HiKeytool.sh

2. In the main menu, enter `2` (**SSL configuration for SMI-S**).
3. In the SMI-S main menu, enter `4` (**Import Client's Certificate to TrustStore for Event Indications**) .

4. Specify the alias name, truststore password, and absolute path of the CIM client server certificate.

```
Enter alias:foocorpindclient
Enter truststore-password:indtrust
Enter authentication-filename(absolute path):c:\tmp
\clientind.cer
```

Related tasks

- Exporting a server or client certificate for a CIM client on page 328

Related references

- Truststores on page 250

Checking a self-signed certificate for a CIM server

To check a Device Manager server (CIM server) self-signed certificate for object operations or event indications, use the `hcmds64keytool` utility (for Windows) or the `keytool` utility (for Linux).

Before you begin

Check the following information:

- Keystore password

Procedure

Execute the following command:

In Windows:

installation-folder-for-Hitachi-Command-Suite\Base64\bin\hcmds64keytool -list -keystore *keystore-file-name* -storepass *keystore-password*

In Linux:

installation-directory-for-Hitachi-Command-Suite/Base64/uCPSB/jdk/bin/keytool -list -keystore *keystore-file-name* -storepass *keystore-password*

- `keystore`: Specify the keystore file you want to check.
- `storepass`: Specify the keystore password.

Self-signed certificate for object operations supplied with the product

The self-signed certificate for object operations that comes with Device Manager uses the SHA256withRSA algorithm and has a key size of 2,048 bits.

The self-signed certificate is stored in the following keystore file (whose password is `wbemssl`):

In Windows:

installation-folder-for-Hitachi-Command-Suite\DeviceManager\HiCommandServer\wsi\server\jserver\bin\.keystore

In Linux:

installation-directory-for-Hitachi-Command-Suite/HiCommandServer/wsi/server/jserver/bin/.keystore

Disabling two-way authentication

Use HiKeytool to disable two-way authentication for object operations or event indications.

Procedure

1. Stop the Hitachi Command Suite product services.
2. Execute the following to start HiKeytool.

   In Windows:

   installation-folder-for-Hitachi-Command-Suite\DeviceManager\HiCommandServer\HiKeytool.bat

   In Linux:

   installation-directory-for-Hitachi-Command-Suite/HiCommandServer/HiKeytool.sh

3. In the main menu, enter `2` (**SSL configuration for SMI-S**).
4. In the SMI-S main menu, enter `1` (**Set Security Level for Object Operations**) or `2` (**Set Security Level for Event Indications**) .
5. Enter `1` (SSL without two-way authentication)

   The MOF file will be compiled and the SMI-S main menu will appear again.
6. Start the Hitachi Command Suite product services.

```
You must stop the Device Manager Server before specifying this
setting.
1) SSL without two-way authentication
```

```
2) SSL with two-way authentication

>1
```

Note: If the message `The compilation of the MOF file failed.` appears, collect all the files at the following location, and then contact maintenance personnel:

In Windows:

installation-folder-for-Hitachi-Command-Suite\DeviceManager\HiCommandServer\wsi\server\jserver\mof\

In Linux:

installation-directory-for-Hitachi-Command-Suite/HiCommandServer/wsi/server/jserver/mof/

Related tasks

- Starting the Hitachi Command Suite services on page 458
- Stopping the Hitachi Command Suite services on page 460

Configuring an SSL server and clients (CIM client)

To use SSL server authentication for object operations, you need to create a server certificate in the Device Manager server, and then import it into the CIM client. To use two-way authentication, you need to create a client certificate in the CIM client, and then import into the Device Manager server.

To use SSL server authentication for event indications, you need to create a server certificate in the CIM client, and then import it into the Device Manager server. To use two-way authentication, you need to create a client certificate in the Device Manager server, and then import it into the CIM client.

Creating a key pair and self-signed certificate for a CIM client

To create a key pair and self-signed certificate from a CIM client, use the `keytool` utility.

Before you begin

Install Java onto a CIM client.

Procedure

1. Execute the following command to create a key pair and self-certificate:

keytool -genkey -keystore *keystore-file-name* -storepass *keystore-password* -alias *alias* -dname *entity-distinguished-name* -validity *validity-of-certificate* -keypass *private-key-password* -keyalg *key-algorithm* -sigalg *signature-algorithm* -keysize *key-size*

- Do not use the following symbols in the file name:
  : , ; * ? " < > |
- Specify the file name as a character string of no more than 255 bytes.
- Do not include double quotation marks (") in the alias or password.
- For the storepass option and the keypass option, specify the same password.

2. Execute the following command to check the contents of the created key pair and self-signed certificate:

   keytool -list -keystore *keystore-file-name* -storepass *keystore-password*

Exporting a server or client certificate for a CIM client

Use the keytool utility to export a server or client certificate for a CIM client from the client's keystore file.

Before you begin

- Install Java onto the CIM client.
- Create a CIM client server certificate.
- Check the following information:
  - Path of the keystore file in the CIM client
  - Alias name for the server certificate in the CIM client
  - Keystore password in the CIM client

Procedure

1. Execute the following command to export the server or client certificate for a CIM client:

   keytool -export -keystore *keystore-file-name* -storepass *keystore-password* -alias *alias* -file *certificate-file-name*

2. Execute the following command to check the contents of the exported server or client certificate:

   keytool -printcert -v -file *certificate-file-name*

Importing a server or client certificate into a CIM client

Use the `keytool` utility to import a server or client certificate for the Device Manager into a CIM client truststore.

Before you begin

- Install Java onto the CIM client.
- Obtain a Device Manager server certificate.
- Check the following information:
  - CIM client truststore password

Procedure

1. Execute the following command to import a server or client certificate for the Device Manager:

   `keytool -import -alias` *`alias`* `-keystore` *`truststore-file-name`* `-storepass` *`truststore-password`* `-trustcacerts -file` *`certificate-file-name`*

   - Do not use the following symbols in the file name:
     `: , ; * ? " < > |`
   - Specify the file name as a character string of no more than 255 bytes.

2. Execute the following command to check the contents of the truststore file:

   `keytool -list -keystore`*`truststore-file-name`* `-storepass` *`truststore-password`*

Related tasks

- Exporting a server certificate for object operations on page 317
- Exporting a client certificate for event indications on page 322

6

Configuring Device Manager for use with related products

This chapter describes the settings required for linking with related products.

- Settings required for linking with Storage Navigator Modular 2
- Settings required to collect storage system performance information
- Settings required to analyze the performance of Universal Replicator by using the Replication tab
- Settings required to use the replication management functionality on the Replication tab
- Settings required to use the VMware VVol functionality
- Settings necessary to launch Hitachi Storage Services Manager

Settings required for linking with Storage Navigator Modular 2

If Device Manager is linked with Storage Navigator Modular 2, you can launch Storage Navigator Modular 2, which is the version of Element Manager for midrange storage systems.

You can use Element Manager to view detailed information on or change the configuration of the storage systems.

Notes and requirements for connecting to Storage Navigator Modular 2

The prerequisites for using Storage Navigator Modular 2 are as follows:

- Before installing Storage Navigator Modular 2, read *Hitachi Command Suite Release Notes* for precautions on installing Hitachi File Services Manager or Storage Navigator Modular 2 and linking it to the system after installing Hitachi Command Suite.
- To manage HUS 100, Hitachi AMS2000, or Hitachi SMS storage systems from the Device Manager GUI, install Device Manager server and Storage Navigator Modular 2 on the same server.
- The web server for Storage Navigator Modular 2 can be accessed via only one NIC even if multiple NICs are installed on the computer. To link with Storage Navigator Modular 2 in a computer environment where multiple NICs are installed, you need to specify the NIC to be used to access the web server for Storage Navigator Modular 2. The IP address specified for this setting must be the same as that specified during installation of the Device Manager server. For details on how to specify the settings, see the documentation for Storage Navigator Modular 2.
- Make sure that Storage Navigator Modular 2 works properly by itself. You need to set up the Java Plug-in in Storage Navigator Modular 2. For details about how to specify environment settings and how to start Storage Navigator Modular 2, see the documentation for Storage Navigator Modular 2.
- In Storage Navigator Modular 2, you can register only storage systems that are supported by Device Manager.
- To manage HUS100, Hitachi AMS2000, and Hitachi SMS, specify the user settings so that the following conditions are satisfied:
  - The `Modify` permission of Storage Navigator Modular 2 has been set.
  - The resource groups that correspond to the target storage systems are assigned.
  - `Modify` has been assigned as the Device Manager's role for the assigned resource group.

For details about how to assign resource groups, see the *Hitachi Command Suite User Guide*.

- For storage systems for which password protection or account authentication is enabled, do not use a user ID that starts with `HDvM`.
  If you launch Storage Navigator Modular 2 while password protection or account authentication is enabled, the system creates a temporary user account for Storage Navigator Modular 2 to access the storage system. This user account is automatically registered into the system with a user ID that starts with `HDvM`, and is automatically deleted after you exit Storage Navigator Modular 2. Therefore, manually registering a user account that starts with `HDvM` or changing the registration details might cause the launch to fail.
- When you enable or disable the advanced security mode in a HUS100, Hitachi AMS2000, or Hitachi SMS storage system, user accounts registered in that storage system will be deleted. To re-register them, use Storage Navigator Modular 2.
- To manage HUS100, Hitachi AMS2000, and Hitachi SMS, match the communication protocol setting in Storage Navigator Modular 2 to the setting in the Device Manager GUI or CLI.
  If you change the communication protocol of a storage system registered in the Device Manager server, make sure that you change the protocol from Device Manager. If you do so from Storage Navigator Modular 2, the Device Manager server and the storage system might not be able to communicate.

Caution: Do not update the firmware or change the microprogram by using Element Manager. In addition, you cannot use Element Manager while the firmware is updated or the microprogram is changed. If you do, the DMES059510 error occurs.

Settings for using Element Manager

To operate a Hitachi AMS/WMS storage system from Element Manager, you must use launchapptool to specify environment settings.

Procedure

1. To operate a Hitachi AMS/WMS storage system from Element Manager, you must use launchapptool to specify environment settings.
   - In Windows:
     installation-folder-for-Hitachi-Command-Suite\DeviceManager\HiCommandServer\tools\launchapptool.bat
   - In Linux:
     installation-directory-for-Hitachi-Command-Suite/HiCommandServer/tools/launchapptool.sh

2. The main menu appears. Select `1`.

```
============================================================
launchapptool
============================================================
1) Storage Navigator Modular 2 launch setup
2) Delete launch settings
3) Exit

>1
Launch Settings for Storage Navigator Modular 2 will now
Start.
```

If the environment settings for using Element Manager have already been specified, a confirmation message is displayed asking you whether you want to change the current settings.

Select `y` to change the settings, or `n` to leave the settings unchanged.

3. Specify the protocol to be used in the web server URL.

Select `1` to use the http protocol, or `2` to use the https protocol.

```
Specify the URL protocol.
 1) http
 2) https
    Caution: To use https, settings to enable SSL
communication
             with the web server must be specified in
advance.

Enter Value [default=1]
>1
```

Caution: Before selecting `2`, make sure that the proper settings are specified to enable SSL communication between the Web server (Common Component) and the GUI.

4. Enter the IP address or host name to be used in the web server's URL.

Specify an IP address in IPv4 format or a host name that can be accessed from the management client (the GUI).

```
Specify the IP address or hostname of the web server.
Enter Value [default=10.208.64.140]
>10.208.64.140
```

Note:

- To use a local host, specify its IP address rather than the host name.
- If the management server has multiple NICs, for the IP address, specify the IP address on the network that connects to the management client (GUI). Do not specify the host name.

5. Enter the port number to be used in the web server's URL.

```
Specify the port number of the web server.
Enter Value [default=23015]
>23015
```

6. If you changed the port number for RMI communication in Storage Navigator Modular 2, enter the new port number.

```
Specify the port number for RMI communications.
Enter Value [default=1099]
>1099
```

> **Caution:** Do not enter anything if you did not change the communication port number.

7. Exit launchapptool.

```
Launch setup has successfully completed.

You must restart the Device Manager Server and Common
Component Services
for this these changes to take effect.

Exit - Default is n?(y, n):
```

8. Restart the Hitachi Command Suite product services.

   The changes to the launch environment settings now apply.

9. Use either the Device Manager GUI or CLI to refresh the storage systems that will be operated from Element Manager.

Related tasks

- Starting the Hitachi Command Suite services on page 458
- Stopping the Hitachi Command Suite services on page 460

Deleting the settings for using Element Manager

If it is no longer necessary to operate a Hitachi AMS/WMS storage system from Element Manager, the settings for using Element Manager can be deleted.

Procedure

1. Execute the following command from the command prompt or terminal window:
   - In Windows:
     installation-folder-for-Hitachi-Command-Suite\DeviceManager\HiCommandServer\tools\launchapptool.bat
   - In Linux:
     installation-directory-for-Hitachi-Command-Suite/HiCommandServer/tools/launchapptool.sh
2. The main menu appears. Select `2`.

A list of the launch environment settings appears.

3. Select `1`.

   A deletion confirmation message appears.

```
============================================================
===========
launchapptool
============================================================
===========

1) Storage Navigator Modular 2 launch setup
2) Delete launch settings
3) Exit

>2

Specify the launch setting to be deleted.
1) Storage Navigator Modular 2
2) Cancel
Enter Value
>1

Launch settings will now be deleted.

Would you like to delete launch settings?(y, n):y
```

4. Select `y` if you are sure you want to delete the settings necessary for using Element Manager. If you do not want to delete the settings, select `n`.
5. Restart the Hitachi Command Suite product services.

   The settings for using Element Manager are now deleted.

```
Launch settings have successfully been deleted.

You must restart the Device Manager Server and Common
Component Services
for this these changes to take effect.

Exit - Default is n?(y, n):
```

Related tasks

- Starting the Hitachi Command Suite services on page 458
- Stopping the Hitachi Command Suite services on page 460

Settings required to collect storage system performance information

By linking Device Manager or Tiered Storage Manager to Tuning Manager, you can use the Mobility tab or the Analytics tab to check the parity group usage, volume IOPS, and other performance information that has been collected.

By linking Tiered Storage Manager to Tuning Manager, you can check the usage of hardware tiers and the I/O performance of volumes from the

Mobility tab, set tiering policies as necessary, and then migrate volumes. This allows you to optimize the usability of storage resources.

By linking Device Manager to Tuning Manager, you can perform the following from the Analytics tab:

- If an application performance error occurs on an application server, you can analyze whether a storage system caused the error.
- You can analyze the performance of an entire storage system periodically to detect any potential problems (a health check).
  The health check results email notification can be sent to users.

System configuration for collecting storage system performance information

Before you can collect storage system performance information, you must install the Tuning Manager server and Tuning Manager - Agent for RAID.

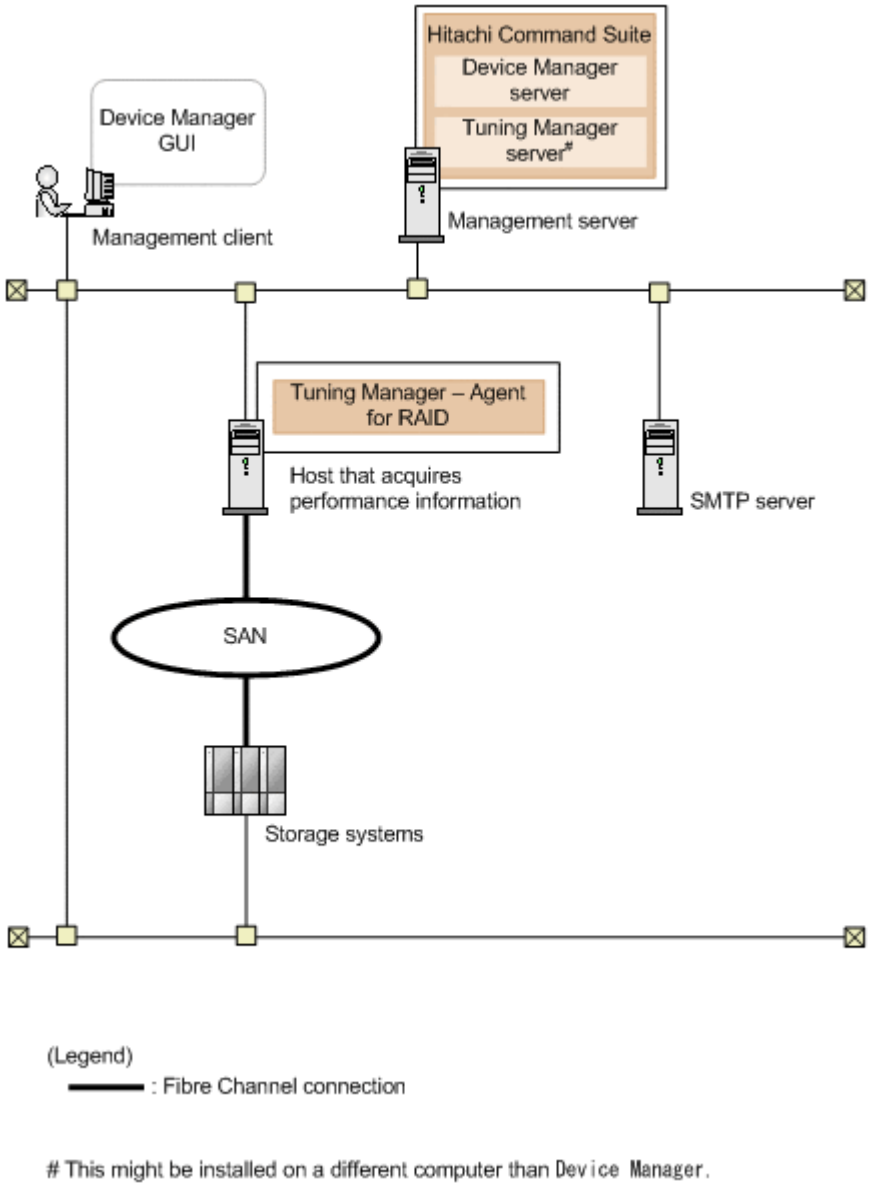


Figure 48 Example of a system configuration for collecting storage system performance information

The following shows the settings that are prerequisite for storage systems and machines.

Storage system

Set each storage system to allow Tuning Manager - Agent for RAID to collect performance information from the storage system.

Host that acquires performance information

Set up as follows:

- Install Tuning Manager - Agent for RAID

- Set up the instance environment of each monitoring-target storage system
  To analyze the following performance information, specify `Y` for `Unassigned Open Volume Monitoring`, which is the instance information for Tuning Manager - Agent for RAID.
  - SLUs (VVol)
  - DP pools that include I/O operations performed via a SLU
  - Parity groups that include the I/O operations performed via a DP volume or SLU
- Set up the machine on which the Tuning Manager server is installed (required only if the Tuning Manager server and Tuning Manager - Agent for RAID are installed on different machines)

After the settings are completed, execute the `jpcstart` command to restart the Tuning Manager - Agent for RAID instance. Tuning Manager - Agent for RAID starts to collect performance data after the instance restarts. Note that it might take up to one hour to obtain data the first time.

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

Management server

Device Manager server

Set the properties related to linkage with Tuning Manager. After setting these properties, refresh the monitoring-target storage systems from the Device Manager GUI or CLI.

Optionally, specify other settings, such as those for remote connection to the Tuning Manager server and for reporting health check results by email.

Tuning Manager server

Install the Tuning Manager server.

If the Device Manager server and the Tuning Manager server are installed on different machines, specify settings so that the Tuning Manager server can connect to the Device Manager server.

For details about how to set up the Tuning Manager server, see the *Hitachi Command Suite Tuning Manager Installation Guide*.

Management client

If you want to launch Performance Reporter of Tuning Manager from the Analytics tab, import the report definition file.

SMTP server

If you want to report health check results by email, specify SMTP authentication settings so that the Device Manager server can connect to the SMTP server.

Related tasks

- Changing Device Manager server properties on page 590

Operation workflow for collecting storage system performance information

Before you can collect storage system performance information, you must set the environment settings on the management server, on the host that collects the performance information, and on the storage system. Then you must refresh the monitoring-target storage systems from the management client.

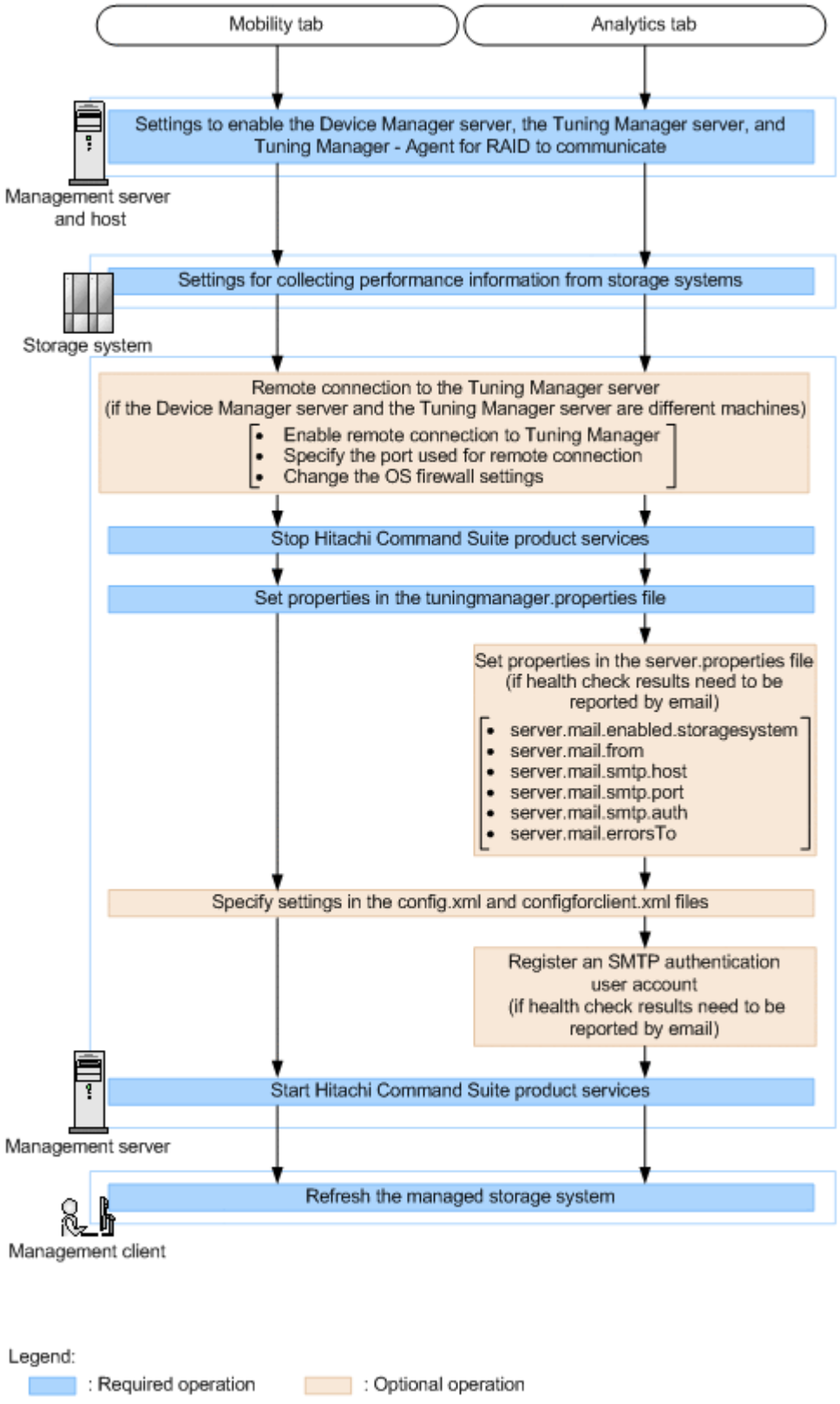


Figure 49 Operation workflow for collecting storage system performance information

Caution:

- The following restrictions apply to remote connection to the Tuning Manager server:
  - Communication using IPv6 is not supported.
  - Communication encrypted by SSL or TLS is not supported.
- If you execute the `hcmds64dbclustersetup` command to configure a cluster, the settings for remote connection with Tuning Manager are initialized. Re-specify the settings.
- If you execute any of the following commands or the following combination of commands to perform a database restoration or database migration, re-specify the remote connection settings on the destination machine:
  `hcmds64dbtrans`
  `hcmds64backups` and `hcmds64db -restore`
  `hcmds64dbtrans` and `hcmds64dbrepair`

Note: After you refresh managed storage systems, confirm that refresh processing has finished normally.

When using the Device Manager GUI:

From the Data Collection Tasks tab, confirm that `Completed` is displayed under Status for the `Refresh Storage Systems` task.

When using the Device Manager CLI:

Confirm that the `AddStorageArray` command has ended normally.

Tip: If the Device Manager server and the Tuning Manager server are installed on the same machine, you can use the Analytics tab by simply refreshing the storage system to be monitored. You do not have to edit the `tuningmanager.properties` file. In this case, the system will run under the following settings:

- `htnm.servers=1` (the number of Tuning Manager servers to be connected to)
- `htnm.server.0.host=127.0.0.1` (the IP address of the Tuning Manager server to be connected to)
- `htnm.server.0.protocol=http` (the communication method between the Tuning Manager server and Common Component)
- `htnm.server.0.port=22015` (the port number for HBase 64 Storage Mgmt Web Service of the Tuning Manager server to be connected to)

If you use the Mobility tab or the operation environment is different from the one shown above, be sure to specify appropriate values for the four properties above.

Related tasks

- Remote connection to the Tuning Manager server (in a non-cluster environment) on page 348
- Remote connection to the Tuning Manager server (in a Windows cluster environment) on page 349
- Registering an SMTP authentication user account in Device Manager on page 415
- Starting the Hitachi Command Suite services on page 458
- Stopping the Hitachi Command Suite services on page 460

Related references

- Settings to enable the Device Manager server, the Tuning Manager server, and Tuning Manager - Agent for RAID to communicate on page 343
- Settings for collecting performance information from enterprise-class storage systems, VSP Gx00 models, VSP Fx00 models, and HUS VM on page 345
- Settings for collecting performance information from midrange storage systems on page 347
- Setting up the config.xml and configforclient.xml files on page 353
- server.mail.enabled.storagesystem on page 598
- server.mail.from on page 599
- server.mail.smtp.host on page 599
- server.mail.smtp.port on page 599
- server.mail.smtp.auth on page 599
- server.mail.errorsTo on page 600
- Properties for connecting to Tuning Manager (tuningmanager.properties file) on page 630

Settings to enable the Device Manager server, the Tuning Manager server, and Tuning Manager - Agent for RAID to communicate

For the Device Manager server, the Tuning Manager server, and Tuning Manager - Agent for RAID to communicate correctly, the machines on which these programs are installed must satisfy the following conditions:

- There is no time difference (based on GMT) among the machines.
  If there is a time difference of five or more minutes (GMT), an error might occur.
- If other programs are installed on the computers, port numbers are not used more than once. In addition, if firewalls have been configured between the computers, the port numbers that will be used have been registered as firewall exceptions.
  For details on the port numbers used by the Tuning Manager server, see the *Hitachi Command Suite Tuning Manager Installation Guide*. For details on the port number used by Tuning Manager - Agent for RAID, see the *Hitachi Command Suite Tuning Manager Agent Administration Guide*.

- When performing a specific operation in the Analytics tab, make sure that the prerequisite conditions for setting the Performance database and Tuning Manager API are met.
  The following table shows the required settings for each operation:

Table 54 Settings required for the Performance database and Tuning Manager API in order to an perform operation in the Analytics tab

Operation	Performance database type	Settings to enable the use of Tuning Manager API
In the Identify Performance Problems wizard, setting the period to be analyzed as more than 72 minutes, and setting the interval in units of minutes	Hybrid Store	Not required
	Store database	Required
Analyzing the performance of MP blades or MP units	Hybrid Store	Not required
	Store database	Required
Analyzing the performance of each host	Hybrid Store	Not required

  As the Performance database type, we recommend using Hybrid Store that is supported by version 8.1.3 or later of Tuning Manager - Agent for RAID. When the Performance database is changed to Hybrid Store, the use of Tuning Manager API becomes enabled.
  For details on how to install Tuning Manager - Agent for RAID, see the *Hitachi Command Suite Tuning Manager Installation Guide*, and for details on how to migrate the performance database, see the *Hitachi Command Suite Tuning Manager Agent Administration Guide*.
  If the Performance database type is Store database, execute the `htmrestctrl` command to enable the use of Tuning Manager API. For details on the `htmrestctrl` command, see the *Hitachi Command Suite Tuning Manager CLI Reference Guide*.
- The computers the Tuning Manager server and Tuning Manager - Agent for RAID are installed on can resolve IP addresses from host names.
  - If operations are performed in an IPv6 environment, configure settings to use both IPv4 and IPv6. In addition, configure settings to resolve IPv6 addresses from host names.
  - If multiple NICs are present in the computers the Tuning Manager server or Tuning Manager - Agent for RAID are installed on, set the IP addresses in the `jpchosts` file and use the same `jpchosts` file in the system.
- If the Tuning Manager server and the Device Manager server are installed on the same computer and if TLS/SSL is used for communication, the settings are completed on the Tuning Manager server and the Device Manager server.

For details on how to set up the Tuning Manager server and Tuning Manager - Agent for RAID, see the *Hitachi Command Suite Tuning Manager Installation Guide*.

Tip: If operations are performed in an environment where the time zone differs between the computers the Device Manager and Tuning Manager - Agent for RAID are installed on, and the system clock of the Device Manager server computer is faster than the system clock of the Tuning Manager - Agent for RAID computer, performance information might not be correctly displayed, depending on when the Mobility tab is viewed. Depending on the time difference, perform either of the following for operation:

- Change the value of the `server.dispatcher.daemon.autoSynchro.performance.startTime` property in the `dispatcher.properties` file of the Device Manager server. Specify a time that is after the time when the local times of both computers are the same date.
- Refresh the performance information at a time that is after the time when the local times of both computers are the same date.
  To refresh performance information, select the Refresh Performance data check box in the Refresh Storage Systems window, or execute the `RefreshPerformanceData` command.

Related concepts

- Registering firewall exceptions for Device Manager and Tiered Storage Manager on page 121
- Operation workflow for secure communication between a Tuning Manager server and a Device Manager server on page 232

Related tasks

- Changing Device Manager server properties on page 590

Related references

- server.dispatcher.daemon.autoSynchro.performance.startTime on page 613

Settings for collecting performance information from enterprise-class storage systems, VSP Gx00 models, VSP Fx00 models, and HUS VM

Before Tuning Manager - Agent for RAID can collect performance information from enterprise-class storage systems, VSP Gx00 models, VSP Fx00 models, and HUS VM, specify the necessary settings in the enterprise-class storage systems, VSP Gx00 models, VSP Fx00 models, and HUS VM:

- The microcode versions of the storage systems to be monitored are supported by Tuning Manager - Agent for RAID.

For details on the prerequisite microcode versions of the storage systems to be monitored by Tuning Manager - Agent for RAID, see the *Hitachi Command Suite Tuning Manager Installation Guide*.

- The computers Tuning Manager - Agent for RAID is installed on can access the Tuning Manager - Agent for RAID command devices that are created in the storage systems to be monitored.
  For details on how to set command devices, see the *Hitachi Command Suite Tuning Manager Installation Guide*.
- When you configure the instance environment for Tuning Manager - Agent for RAID, `1` or `3` must be specified for the value of `Method for Collecting` in the instance information.
  Device Manager cannot link with Tuning Manager - Agent for RAID instances that are configured with `2` specified for `Method for Collecting`.
  For details on how to set up the instance environment, see *Hitachi Command Suite Tuning Manager Installation Guide*.
- When performing a health check, the record storage period must be set to the records below.
  - `PI_CLMS` record (This record does not have to be set for Universal Storage Platform V/VM.)
  - `PI_CLPS` record
  - `PI_LDA` record
  - `PI_PLS` record
  - `PI_PRCS` record
  - `PI_PTS` record
  - `PI_RGS` record

  Use Performance Reporter of Tuning Manager to set the record storage period. For details on how to set the record storage period, see the *Hitachi Command Suite Tuning Manager Agent Administration Guide*.
  For details on the record storage period to be set, see Table 55 Record storage period to be set when performing a health check (for enterprise-class storage systems, VSP Gx00 models, VSP Fx00 models, and HUS VM) on page 347.

Table 55 Record storage period to be set when performing a health check (for enterprise-class storage systems, VSP Gx00 models, VSP Fx00 models, and HUS VM)

Performance database type	Property name	Setting value
Store database version 1.0	Product Interval - Hour Drawer	Month
	Product Interval - Day Drawer	Year
Store database version 2.0	Period - Hour Drawer (Day)	9 or more
	Period - Day Drawer (Week)	5 or more
Hybrid Store	Retention - hourly	216 or more
	Retention - daily	35 or more

Tip: When executing Analyze Host Group for each host, set the storage period of the PI_LDS record, to match the period that you want to analyze.

Settings for collecting performance information from midrange storage systems

Before Tuning Manager - Agent for RAID can collect performance information from midrange storage systems (HUS100, Hitachi AMS2000, Hitachi SMS, and Hitachi AMS/WMS), specify the necessary settings in the midrange storage systems.

- The microcode versions of the storage systems to be monitored are supported by Tuning Manager - Agent for RAID.
  For details on the prerequisite microcode versions of the storage systems to be monitored by Tuning Manager - Agent for RAID, see the *Hitachi Command Suite Tuning Manager Installation Guide*.
- If the storage systems to be monitored are HUS100, Hitachi AMS2000, Hitachi SMS, or Hitachi AMS/WMS, and Account Authentication is enabled, a Tuning Manager - Agent for RAID account has been created.
  For details on how to create a Tuning Manager - Agent for RAID account, see the *Hitachi Command Suite Tuning Manager Installation Guide*.
- The settings for the following records have been configured so that performance information can be collected by using Storage Navigator Modular or Storage Navigator Modular 2:
  - PD_CLPC record
  - PI_CLCS record
  - PI_CLPS record
  - PI_LDA record
  - PI_LDS record
  - PI_PDOS record
  - PI_PRCS record
  - PI_PTS record

- PI_RGS record

For details on how to set a record for collecting performance information, see the *Hitachi Command Suite Tuning Manager Installation Guide*.

- When performing a health check, the record storage period must be set to the records below.
  - PI_CLCS record
  - PI_LDA record
  - PI_PRCS record
  - PI_PTS record
  - PI_RGS record

Use Performance Reporter of Tuning Manager to set the record storage period. For details on how to set the record storage period, see the *Hitachi Command Suite Tuning Manager Agent Administration Guide*.
For details on the record storage period to be set, see Table 56 Record storage period be set when performing a health check (for midrange storage systems) on page 348.

Table 56 Record storage period be set when performing a health check (for midrange storage systems)

Performance database type	Property name	Setting value
Store database version 1.0	Product Interval - Hour Drawer	Month
	Product Interval - Day Drawer	Year
Store database version 2.0	Period - Hour Drawer (Day)	9 or more
	Period - Day Drawer (Week)	5 or more
Hybrid Store	Retention - hourly	216 or more
	Retention - daily	35 or more

Tip: When executing Analyze Host Group for each host, set the storage period of the PI_LDS record, to match the period that you want to analyze.

Remote connection to the Tuning Manager server (in a non-cluster environment)

To switch the status (enabled or disabled) of remote connection to the Tuning Manager server in a non-cluster environment, execute the htmsetup command.

Before you begin

- Edit the hosts file on the Device Manager server.
  Register the host name and IP address of the Tuning Manager server.

  Location of the hosts file

In Windows: *Windows-system-folder*\system32\drivers\etc\hosts

In Linux: /etc/hosts

- Set up the port that is used for remote connection (when a firewall is enabled in Linux)
- Log in as a user with Administrator permissions (for Windows) or as a root user (for Linux)

Procedure

1. Stop the Hitachi Command Suite product services.
2. Execute the `htmsetup` command.
3. When a menu is displayed, select `1` (`Configure the settings for remote connection`).
4. Enter the port number (specifiable values: 5001 through 65535, default value: 24230).

   When port setup finishes, HiRDB starts. In Windows, at this time, registration in the Windows Firewall exceptions list has also finished.
5. Start the Hitachi Command Suite product services.

Related tasks

- Stopping the Hitachi Command Suite services on page 460

Related references

- Port numbers that must be registered as firewall exceptions for Device Manager and Tiered Storage Manager on page 121

Remote connection to the Tuning Manager server (in a Windows cluster environment)

In a Windows cluster environment, to switch the status (enabled or disabled) of remote connection to the Tuning Manager server, remove Hitachi Command Suite product services and resource groups from cluster management, and then execute the `htmsetup` command. A group of clustered services (the set of services for which failover is performed) is called a resource group.

Before you begin

- Edit the `hosts` file (*Windows-system-folder*\system32\drivers\etc\hosts) on the Device Manager server:
  Register the physical host name and physical IP address of the Tuning Manager server
- Log in as a user with Administrator permissions

Procedure

1. Execute the following command to take the Hitachi Command Suite product services offline.

   installation-folder-of-Hitachi-Command-Suite\Base64\ClusterSetup\hcmds64clustersrvstate /soff /r *resource-group-name*

   soff

   Use this option to suppress failover by taking the following offline: the Hitachi Command Suite product services registered to the resource group of the cluster management application.

   r

   Specify the name of the resource group.

2. Execute the `htmsetup` command.
3. When a menu is displayed, select `1` (`Configure the settings for remote connection`).
4. Enter the port number (specifiable values: 5001 through 65535, default value: 24230).

   When port setup finishes, HiRDB starts. At this time, registration in the Windows Firewall exceptions list has also finished.
5. Stop the Hitachi Command Suite product services.
6. Move the group in which the Hitachi Command Suite product services have been registered to the standby node.
7. On the standby node, execute the `htmsetup` command.

   Specify the same settings as those on the executing node.
8. Stop the Hitachi Command Suite product services.
9. Execute the command below to bring the following online: the resource group of the cluster management application and the Hitachi Command Suite product services.

   installation-folder-of-Hitachi-Command-Suite\Base64\ClusterSetup\hcmds64clustersrvstate /son /r *resource-group-name*

   son

   Use this option to enable failover by bringing the following online: the resource group set for the cluster management application.

   r

   Specify the name of the resource group.

Related tasks

- Stopping the Hitachi Command Suite services on page 460

Related references

- Hitachi Command Suite product services that are registered in cluster management applications on page 466

Remote connection to the Tuning Manager server (in a Red Hat Enterprise Linux cluster environment)

In a Red Hat Enterprise Linux cluster environment, to switch the status (enabled or disabled) of remote connection to the Tuning Manager server, remove the Hitachi Command Suite product services from the service group, and then execute the `htmsetup` command.

Before you begin

- Edit the `hosts` file (`/etc/hosts`) on the Device Manager server:
  Register the physical host name and physical IP address of the Tuning Manager server
- Log in as a user with root permissions
- Check the following information:
  - The file name of the script created to register services into a service group.
    For details about how to register the Hitachi Command Suite product services to a service group, see *Hitachi Command Suite Installation and Configuration Guide*.

Procedure

1. Remove the Hitachi Command Suite product services from the service group.

   For details, see *Hitachi Command Suite Installation and Configuration Guide*.
2. Confirm that the service group was moved to the executing node.

   If the service group has not been moved, move the service group to the executing node.
3. Execute the `htmsetup` command.
4. When a menu is displayed, select `1` (`Configure the settings for remote connection`).
5. Enter the port number (specifiable values: 5001 through 65535, default value: 24230).

   When port setup finishes, HiRDB starts.
6. Stop the Hitachi Command Suite product services.
7. Move the service group to the standby node.
8. On the standby node, execute the `htmsetup` command.

Specify the same settings as those on the executing node.

9. Stop the Hitachi Command Suite product services.
10. Re-register the Hitachi Command Suite product services removed in step 1 to the service group.
11. Start the service group to which the Hitachi Command Suite product services were registered.

    For details, see *Hitachi Command Suite Installation and Configuration Guide*.

Related tasks

- Stopping the Hitachi Command Suite services on page 460

Specifying the settings for remote connection to the Tuning Manager server and the port number (htmsetup command)

To change the settings for remote connection with Tuning Manager or set the port number that is used for remote connection, use the `htmsetup` command.

The command interactively specifies the following settings for remote connection to Tuning Manager.

- Enabling or disabling remote connection (default: disabling)
- Specifying the port number used when remote connection is enabled (range of specifiable values: 5001 to 65535, default: 24230)

In an OS in which Windows Firewall has been installed, the command also performs registration in the Windows Firewall exception list when remote connection is enabled, and performs unregistration when remote connection is disabled. When the settings have been completed, HiRDB is activated.

Note: You cannot concurrently execute multiple instances of the `htmsetup` command.

Operations to complete in advance

- Log in as a user with Administrator permissions (for Windows) or as a root user (for Linux)
- Add the host name and IP address to the host settings file (when enabling remote connection)
  Add the host name and IP address of the local machine to the host settings file.
- Stop all Hitachi Command Suite product services
- Make sure that no other commands are running
  Make sure that no other commands that can change Common Component settings are running.
- Remove the services and resource groups of Hitachi Command Suite products from cluster software management (in a cluster environment)

Make sure that the services and resource groups of Hitachi Command Suite products on both the active and standby nodes are no longer monitored by the cluster software.

Command format

```
htmsetup
```

Location of the command

In Windows:

installation-folder-for-Hitachi-Command-Suite\DeviceManager\HiCommandServer\tools\htmsetup.bat

In Linux:

*installation-directory-for-Hitachi-Command-Suite/*HiCommandServer/tools/htmsetup.sh

Related tasks

- Stopping the Hitachi Command Suite services on page 460

Setting up the config.xml and configforclient.xml files

In some cases, the settings in the `config.xml` and `configforclient.xml` files must be changed.

- When a firewall is configured between the Tuning Manager management server and the Device Manager management server:
  Change the setting for the `ownPort` parameter so that a specific port number is used; by default, any available port number is used. Different port numbers must be set for the `ownPort` parameter of each file. You can specify a value in the range from 1024 to 65535. Note that, to avoid a conflict with port numbers used by other processes, do not specify a port automatically assigned by the OS. The port number specified here must be registered as a firewall exception.
- When multiple NICs are installed on the Device Manager management server:
  For the `ownHost` parameter, from the IPv4 address and host name of the Device Manager management server, specify the one that belongs to the network to which the Tuning Manager management server is connected. The same value must be specified for the `ownHost` parameter in the `config.xml` file and the `configforclient.xml` file.
- When performance information is obtained from 13 or more storage systems or when performance information is obtained two or more times per day:
  Change the value of the `logFileSize` parameter in the `config.xml` file to `30`

The storage destination of the `config.xml` file and the `configforclient.xml` file is as follows:

In Windows:

installation-folder-for-Hitachi-Command-Suite\DeviceManager\HiCommandServer\vsa\conf

In Linux:

installation-directory-for-Hitachi-Command-Suite/HiCommandServer/vsa/conf

Related references

- Port numbers that must be registered as firewall exceptions for Device Manager and Tiered Storage Manager on page 121

Setting up the management client (to collect storage system performance information)

If you want to launch Performance Reporter of Tuning Manager from the Analytics tab, import the report definition file.

The latest report definition file is `AnalyticsReportDefV840`. The report definition file is stored at the following location on the integrated installation media:

DVD-drive:\HTNM_SERVER\Definitions\Report_Definitions

If another report definition has been imported, delete it. After that, import the latest report definition file.

Note that you must also set user permission to use the Mobility and Analytics tabs.

For details about how to set necessary user permission, how to register licenses in Device Manager and Tiered Storage Manager, and how to set resource groups and roles in Device Manager, see the *Hitachi Command Suite User Guide*.

For details about how to register licenses and specify permission settings in Tuning Manager, see the *Tuning Manager Server Administration Guide*.

For details about how to import report definitions into Performance Reporter of Tuning Manager see the *Tuning Manager Server User Guide*.

Settings required to analyze the performance of Universal Replicator by using the Replication tab

If Device Manager, Replication Manager, and Tuning Manager are linked, you can check the performance information of Universal Replicator from the

Replication tab to analyze the cause of C/T Delta deterioration in Universal Replicator.

Information required for analysis is collected from Replication Manager and Tuning Manager. From Replication Manager, configuration information from copy groups and pair management servers, and performance information such as C/T Delta performance information and journal volume usage are collected. From Tuning Manager, configuration information from storage systems, and performance information such as the ratios of storage system processor usage and data in storage system cache memory that is waiting to be written.

System configuration for analyzing the performance of Universal Replicator by using the Replication tab

To analyze the performance of Universal Replicator by using the Replication tab, you must have the programs below. Note that Replication Manager is already installed, and that Universal Replicator is being used.

- Device Manager
- Replication Manager
- Tuning Manager
- Tuning Manager - Agent for RAID

The following show examples of system configurations for analyzing the performance of Universal Replicator by using the Replication tab:

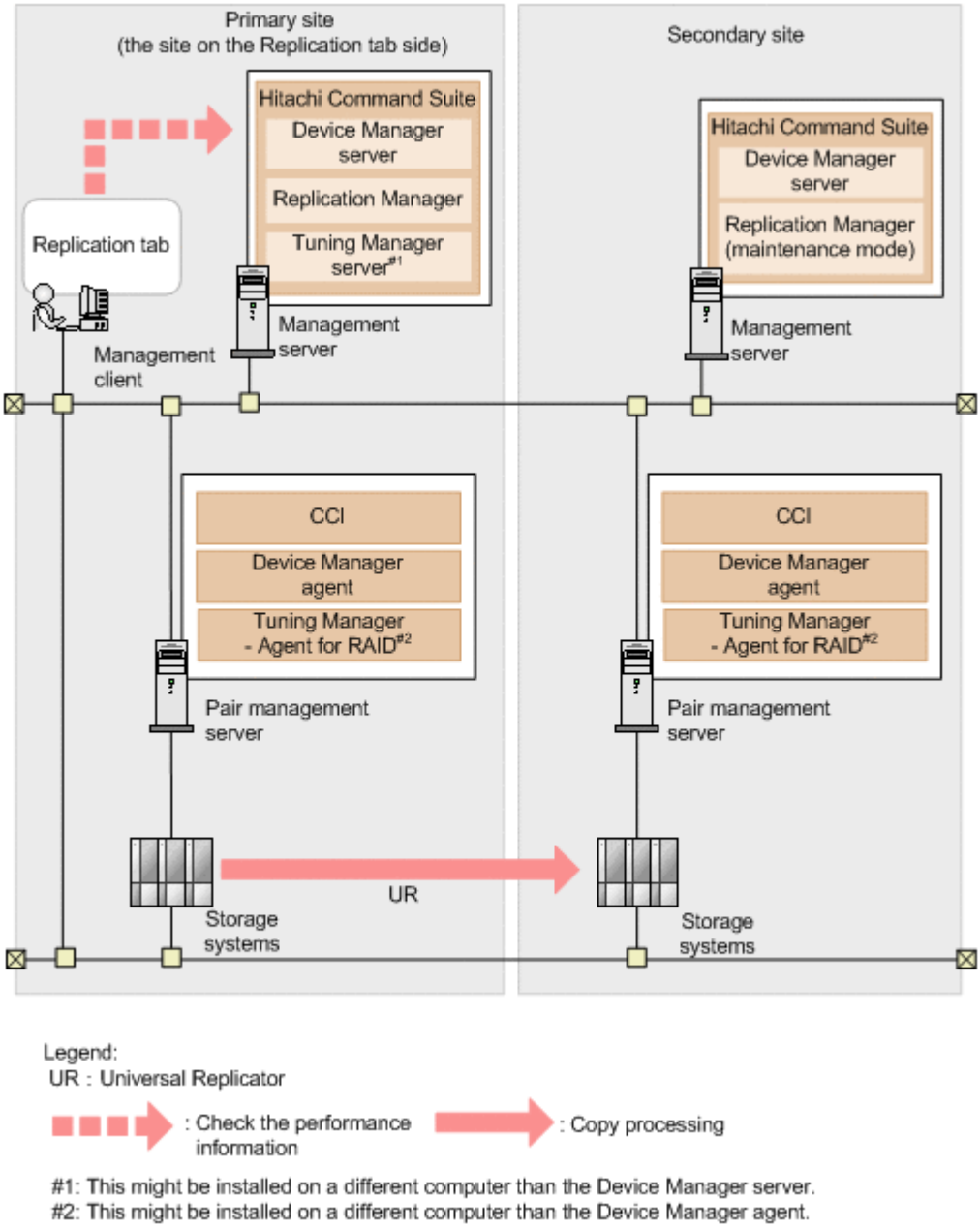


Figure 50 Example of a system that is configured to analyze performance by connecting from the management client to the Device Manager server at the primary site

The prerequisites for each product are shown below. If you are using the Replication tab, the management client can connect to the Device Manager server on the primary site or on the secondary site.

- The C/T delta for the Universal Replicator pair whose performance is to be analyzed can be checked from the Replication Manager running on the same management server as the Device Manager server that is connected from the management client.

- More than one Tuning Manager is running on the same site as the Device Manager server that is connected from the management client.
- Tuning Manager - Agent for RAID is set up at both sites.
- The Replication Manager on a different site (the secondary site in the figure) as the Device Manager connected from the management client is set to maintenance mode.
  For details on the maintenance mode of Replication Manager, see the *Hitachi Command Suite Replication Manager Configuration Guide*.
- The settings for communication among the Device Manager server, the Tuning Manager server, and Tuning Manager - Agent for RAID are correctly specified.
  - There is no time difference (based on GMT) among the machines.
    If there is a time difference of five or more minutes (GMT), an error might occur.
  - If other programs are installed on the computers, port numbers are not used more than once. In addition, if firewalls have been configured between the computers, the port numbers that will be used have been registered as firewall exceptions.
    For details on the port numbers used by the Tuning Manager server, see the *Hitachi Command Suite Tuning Manager Installation Guide*. For details on the port number used by Tuning Manager - Agent for RAID, see the *Hitachi Command Suite Tuning Manager Agent Administration Guide*.
  - The computers the Tuning Manager server and Tuning Manager - Agent for RAID are installed on can resolve IP addresses from host names.
    If the host name is 33 bytes or longer, set the alias name, and then configure the settings to be able to resolve the name from the alias name to IP address.
    If operations are performed in an IPv6 environment, configure settings to use both IPv4 and IPv6. In addition, configure settings to be able to resolve IPv6 addresses from host names.
  - If you are installing Tuning Manager server onto a different computer than a Device Manager server, make sure that the installation destination computers of the Device Manager server and the Tuning Manager server have settings configured that will resolve the host names to IP addresses.
- The use of Tuning Manager API is enabled in Tuning Manager - Agent for RAID.
  As the database type, we recommend using Hybrid Store that is supported by version 8.1.3 or later of Tuning Manager - Agent for RAID Performance. When the Performance database is changed to Hybrid Store, the use of Tuning Manager API becomes enabled.
  For details on how to install Tuning Manager - Agent for RAID, see the *Hitachi Command Suite Tuning Manager Installation Guide*, and for details

on how to migrate the performance database, see the *Hitachi Command Suite Tuning Manager Agent Administration Guide*.
If the Performance database type is Store database, execute the `htmrestctrl` command to enable the use of Tuning Manager API. For details on the `htmrestctrl` command, see the *Hitachi Command Suite Tuning Manager CLI Reference Guide*.

Note: To move the management server environment to a new machine, you must perform the procedure for handing over the collected performance information. If you do not perform the procedure correctly, the collected performance information might be lost. For details, see *Hitachi Command Suite Release Notes*.

Tip: If the following operations are performed, the history information of C/T Delta and journal volume usage was being displayed in the Replication tab is no longer displayed:

- The pair management server is changed
- The WWN of the pair management server is changed

Related concepts

- Registering firewall exceptions for Device Manager and Tiered Storage Manager on page 121

Flow of tasks for analyzing the performance of Universal Replicator by using the Replication tab

To analyze the performance of Universal Replicator by using the Replication tab, you must set Device Manager, Replication Manager, and Tuning Manager on the management server, and set Tuning Manager - Agent for RAID on the pair management server.

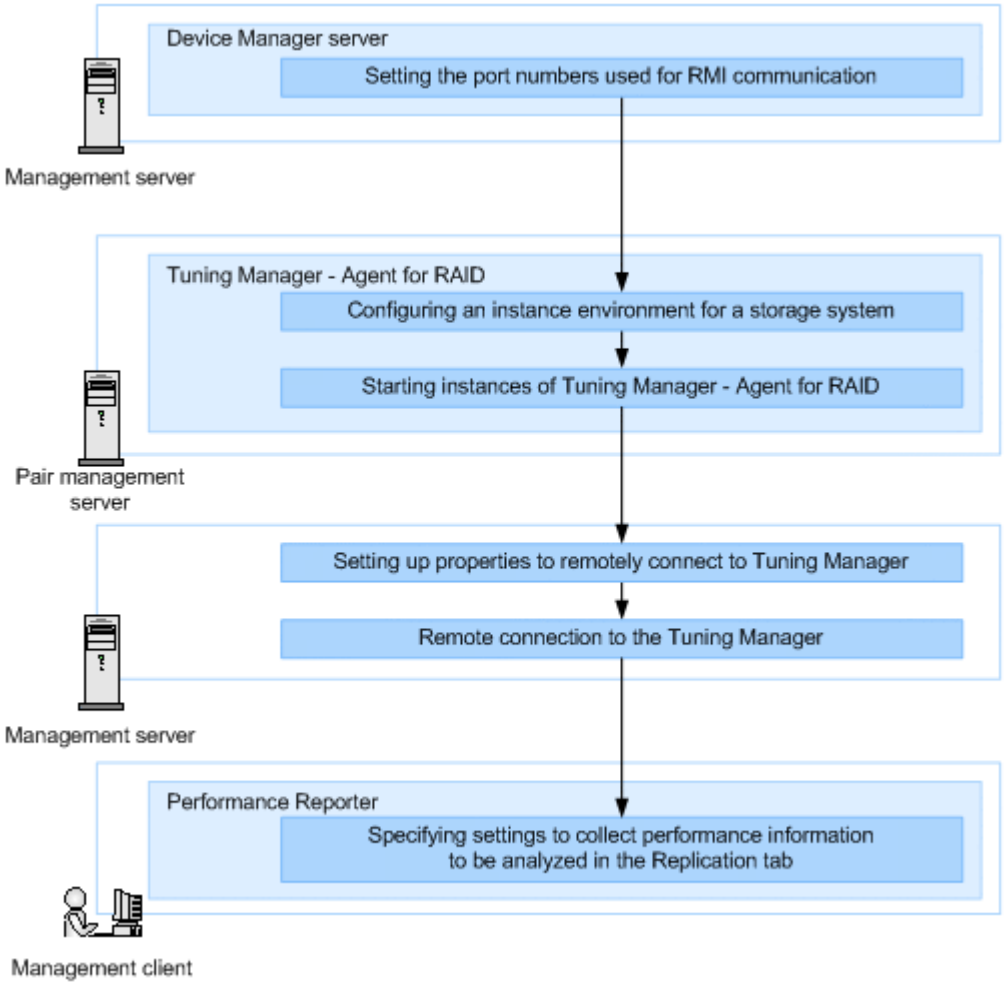


Figure 51 Flow of tasks for analyzing the performance of Universal Replicator by using the Replication tab

Related tasks

- Remote connection to the Tuning Manager server (in a non-cluster environment) on page 348
- Remote connection to the Tuning Manager server (in a Windows cluster environment) on page 349
- Setting the port numbers used for RMI communication on the Device Manager server on page 360
- Configuring an instance environment for a storage system on page 360
- Starting instances of Tuning Manager - Agent for RAID on page 361
- Setting up properties to remotely connect to Tuning Manager on page 362
- Specifying settings to collect performance information to be analyzed in the Replication tab on page 363

Setting the port numbers used for RMI communication on the Device Manager server

Set the port numbers used for RMI communication on the Device Manager server because if the Replication tab is used, RMI communication needs to be used to link with Replication Manager.

Before you begin

Log in as a user with Administrator permissions (for Windows) or as a root user (for Linux).

Procedure

1. Stop the services of Hitachi Command Suite product.
2. Set up the `rpmlib.rpm.port` property in the `rpmlib.properties` file of the Device Manager server.

   Enter the port number that is set for the `base.rmi.port` property in the `base.properties` file of Replication Manager. If you have not changed the value for the `base.rmi.port` property (default: 25200), this operation is unnecessary.

   The `base.properties` file is stored in the following location:

   In Windows:

   installation-folder-for-Hitachi-Command-Suite\ReplicationManager\conf

   In Linux:

   installation-directory-for-Hitachi-Command-Suite/ReplicationManager/conf

   For details on the `base.properties` file and the `base.rmi.port` property of Replication Manager, see the *Replication Manager Configuration Guide*.
3. Start the services of Hitachi Command Suite product.

Related tasks

- Starting the Hitachi Command Suite services on page 458
- Stopping the Hitachi Command Suite services on page 460

Related references

- rpmlib.rpm.port on page 638

Configuring an instance environment for a storage system

Configure an instance environment for each storage system on the pair management server to use Tuning Manager - Agent for RAID to monitor the primary and secondary storage systems to be analyzed.

Before you begin

Log in as a user with Administrator permissions (for Windows) or as a root user (for Linux).

Procedure

1. Execute the `jpctdlistraid` command to check the command devices of the storage systems to be analyzed.

   Check the value of `DEVICE_FILE`.

   For details on the `jpctdlistraid` command, see the *Hitachi Command Suite Tuning Manager CLI Reference Guide*.
2. Execute the `jpcinssetup` command interactively to configure instance environments for the storage systems to be analyzed.

   Create one instance per storage system.

   Enter the following instance information interactively.
   - `Storage Model`: `2`
   - `Method for Collecting`: `1` or `3`
   - `Command Device File Name`: The value of the `DEVICE_FILE` checked by using the `jpctdlistraid` command in step 1
   - `Unassigned Open Volume Monitoring`: `Y`
   - `Mainframe Volume Monitoring`: Any value
   - `Store Version`: Not specified

   For details on the `jpcinssetup` command, see the *Hitachi Command Suite Tuning Manager CLI Reference Guide*.
3. Execute the `jpctdchkinst` command to check the contents of the instance information you set.

   No problem exists if the KAVF18850-I message is output to `[Check result]`.

   For details on the `jpctdchkinst` command, see the *Hitachi Command Suite Tuning Manager CLI Reference Guide*.

Starting instances of Tuning Manager - Agent for RAID

Start Tuning Manager - Agent for RAID on the pair management server so that you can operate the configured instance environments by using Tuning Manager - Agent for RAID.

Before you begin

Log in as a user with Administrator permissions (for Windows) or as a root user (for Linux).

Procedure

1. Execute the `jpcstart` command to start the target instances of Tuning Manager - Agent for RAID.

   For details on the `jpcstart` command, see the *Hitachi Command Suite Tuning Manager CLI Reference Guide*.
2. Execute the `jpcctrl list` command to check the status of the target instances.

   Make sure the statuses of the instances meet the following conditions:
   - `DA1` and `DS1` are registered in the service names for each instance.
   - The `statuses` of `DA1` and `DS1` are `Active`.

   For details on the `jpcctrl list` command, see the *Hitachi Command Suite Tuning Manager CLI Reference Guide*.

Setting up properties to remotely connect to Tuning Manager

If Tuning Manager is installed on a different computer than the Device Manager server, to remotely connect to Tuning Manager, set up the properties in the `tuningmanager.properties` file of the Device Manager server.

Before you begin

Log in as a user with Administrator permissions (for Windows) or as a root user (for Linux).

Procedure

1. Stop the services of Hitachi Command Suite product.
2. Set up the following properties in the `tuningmanager.properties` file of the Device Manager server.
   - `htnm.servers`
   - `htnm.server.`*`n`*`.host`
   - `htnm.server.`*`n`*`.protocol`
   - `htnm.server.`*`n`*`.port`

   For *n*, specify a value in the range from `0` to *value-specified-in-htnm.servers-property* - 1.
3. Start the services of Hitachi Command Suite product.

Related tasks

- Starting the Hitachi Command Suite services on page 458
- Stopping the Hitachi Command Suite services on page 460

Related references

- htnm.servers on page 631
- htnm.server.n.host on page 631
- htnm.server.n.protocol on page 631
- htnm.server.n.port on page 632

Specifying settings to collect performance information to be analyzed in the Replication tab

To collect performance information for the metrics that can be analyzed in the Replication tab, use Performance Reporter of Tuning Manager to change the properties for each record corresponding to each metric so that performance data of Tuning Manager - Agent for RAID is recorded.

Procedure

1. Display the Properties window of the Agent Collector service in Performance Reporter.

   For details on how to display the Properties window of the Agent Collector service in Performance Reporter to change the method for recording performance data, see the *Hitachi Command Suite Tuning Manager Agent Administration Guide*.
2. Expand the **Interval Records** node in **Service Properties**.
3. Select a record, and then set the **Log** property to **Yes**.

   The following table describes the correspondence between metrics and records that need to be set up.

Table 57 Correspondence between metrics and records that need to be set up to be analyzed in the Replication tab

Metric	Record
Processor Busy Rate	PI_PRCS#1
Cache Write Pending Rate	PI_CLMS#2
Port Transfer Rate	PI_PTS#1
Host Write Transfer Rate to M-JNL	PI_JNLS
M-JNL Async Transfer Rate to RCU	
Host Write IOPS to M-JNL	
Read M-JNL Process Time	
Host Write Block Size to M-JNL	
End-to-End Journal Copy Time	

Metric	Record
R-JNL Transfer and Process Time	
P-VOL Write Transfer Rate	PI_LDS#1

#1

By default, the **Log** property is set to **Yes**.

#2

For Tuning Manager - Agent for RAID version 8.1.1 or later, by default, the **Log** property is set to **Yes**.

Changing the time or interval for periodically collecting performance information to be analyzed in the Replication tab

You can periodically collect information required for analysis from Replication Manager and Tuning Manager, but if you want to change the time or interval at which information is collected, edit the properties in the `replication.properties` file of the Device Manager server.

Note: In the following cases, information is not periodically collected:

- While the configuration information or performance information is being collected by the Device Manager GUI or CLI.
- The start time for the next collection comes during the execution of a periodic collection.

Before you begin

Log in as a user with Administrator permissions (for Windows) or as a root user (for Linux).

Procedure

1. Stop the services of Hitachi Command Suite product.
2. Set up the properties in the `replication.properties` file of the Device Manager server.
3. Start the services of Hitachi Command Suite product.

Related tasks

- Starting the Hitachi Command Suite services on page 458
- Stopping the Hitachi Command Suite services on page 460

Related references

- Properties related to the Replication tab (replication.properties file) on page 633

Notes on analyzing the performance of Universal Replicator

This section provides notes for when analyzing the performance of Universal Replicator by using the Replication tab.

- If you change the locale of the Device Manager server, graphs might not be displayed correctly in the Replication tab. For this reason, we do not recommend that you change the locale.
- When daylight saving time applies, the information collection time required for analysis is coordinated according to the daylight saving time.

Settings required to use the replication management functionality on the Replication tab

By using the replication management functionality on the Replication tab, you can manage the configuration of replications not only at one site but also across multiple sites.

Each site consists of one management server, one pair management server, and multiple storage systems. By using the Replication tab, you can configure a TrueCopy pair or Universal Replicator pair between a site and another remote site, which enables operations that prepare for disaster recovery.

This section describes configurations where multiple sites are linked and the settings required to use the replication management functionality.

For details about the system configuration or requirements of the copy pair management that is required for using the replication management functionality, see the chapter that describes copy pair management. For details about the system configuration or requirements for configuring a high availability system, see the chapter that describes configuration of a high availability system.

Related concepts

- Configuring a high availability system on page 93

Related references

- System configuration for managing copy pairs (central management method) on page 63
- System configuration for managing copy pairs (other than the central management method) on page 67
- Storage system requirements for managing copy pairs on page 84
- Notes on managing copy pairs on page 88
- Prerequisite version of the Device Manager agent for managing copy pairs on page 85

System configuration for using the replication management functionality on the Replication tab (configuration for multiple sites)

The following show examples of system configurations where multiple sites are linked by using the replication management functionality:

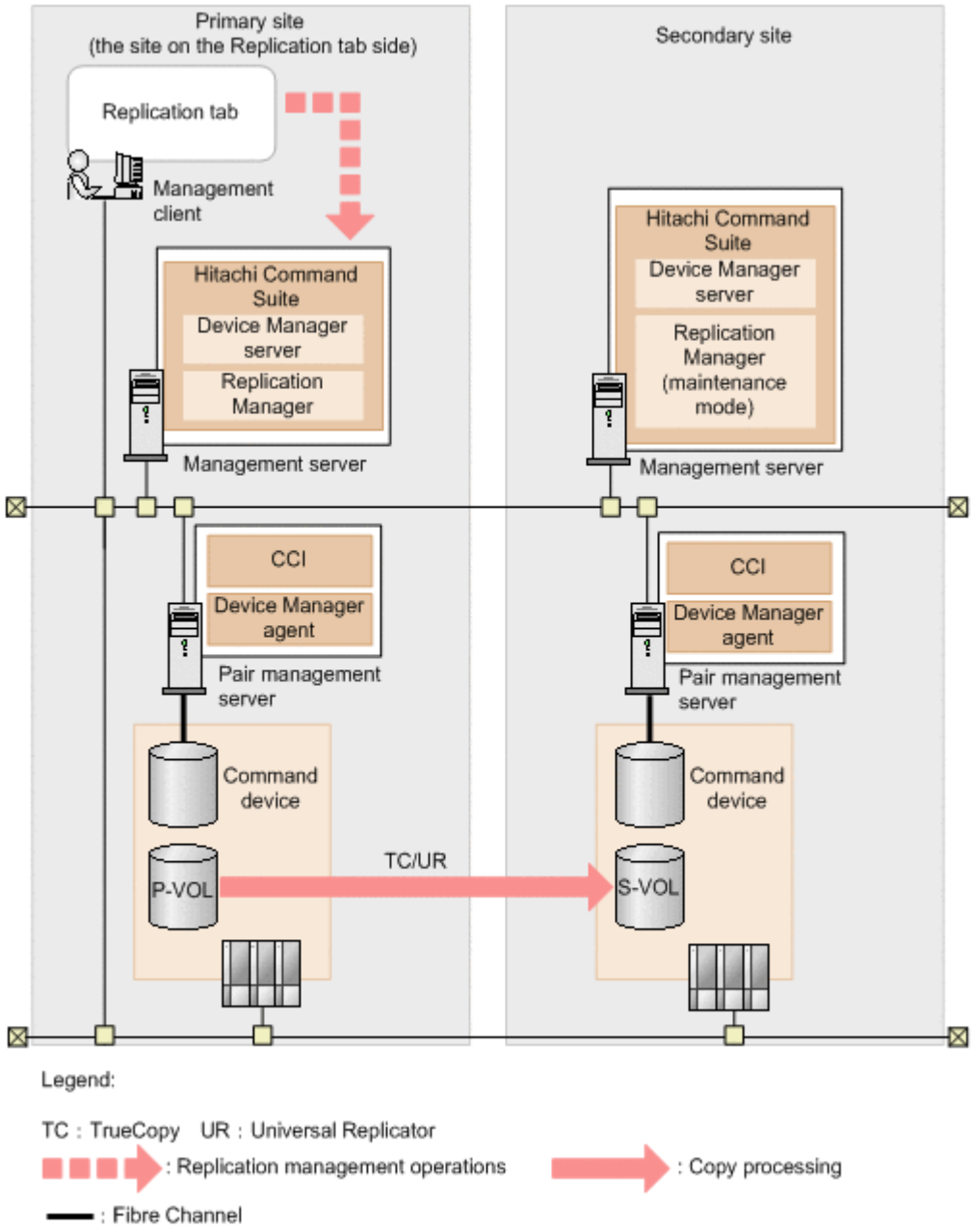


Figure 52 System configuration example when using the replication management functionality (configuration for two sites)

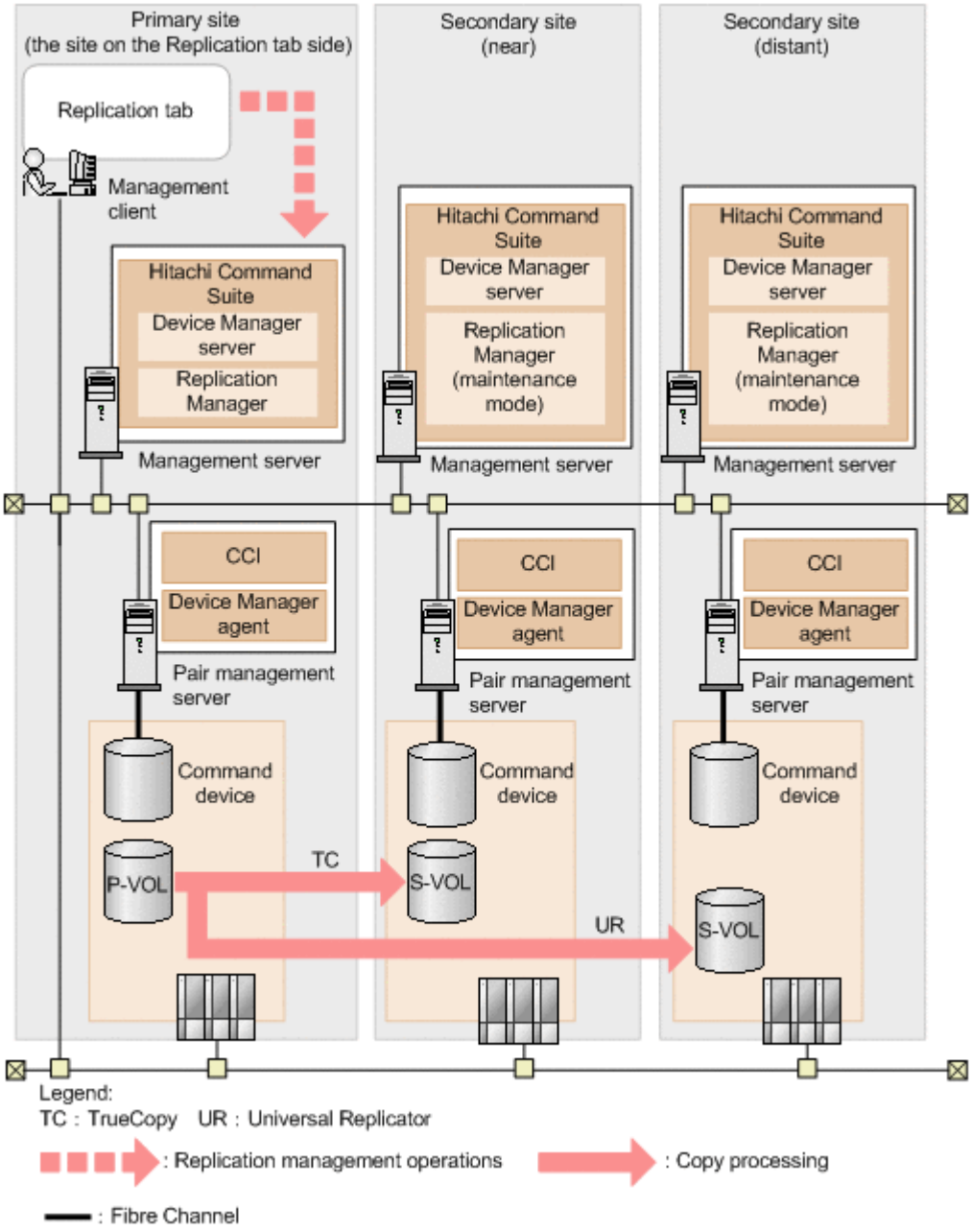


Figure 53 System configuration example when using the replication management functionality (configuration for three sites)

Workflow for using the replication management functionality on the Replication tab

The following describes the workflow for specifying settings to use the replication management functionality on the Replication tab.

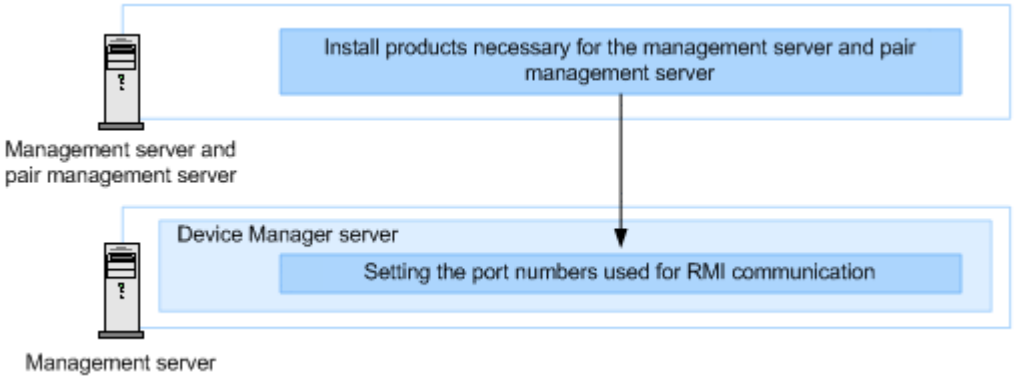


Figure 54 Workflow for using the replication management functionality on the Replication tab (configuration for one site)

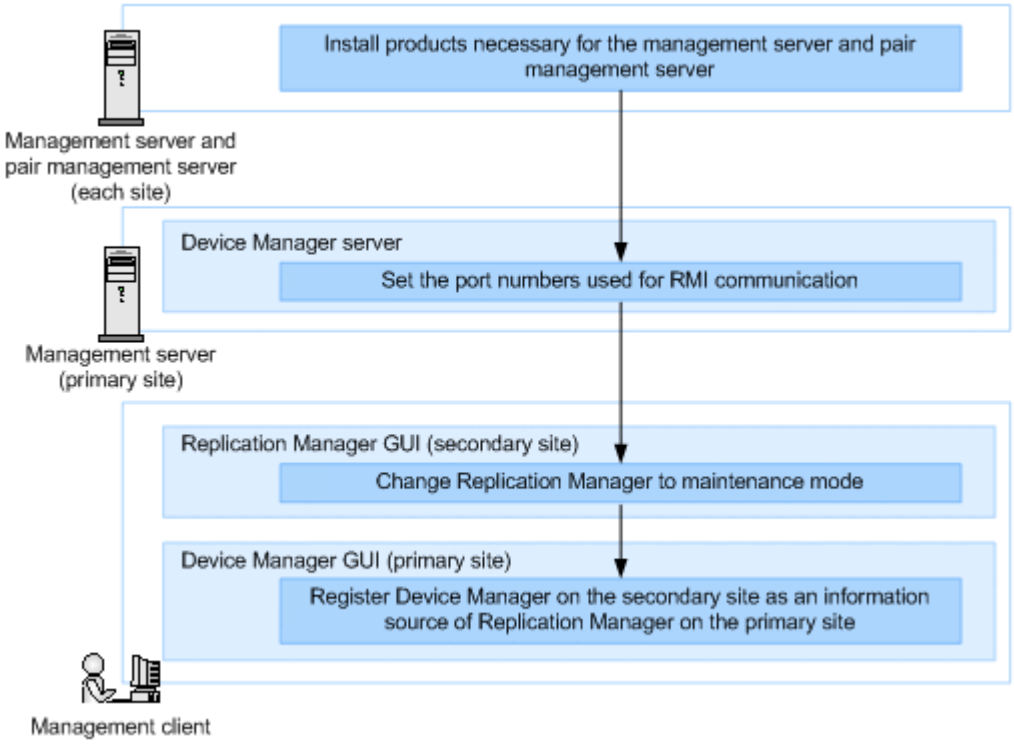


Figure 55 Workflow for using the replication management functionality on the Replication tab (configuration for multiple sites)

Use the Replication tab to register Device Manager on the secondary site as an information source of Replication Manager on the primary site. For details, see *Hitachi Command Suite User Guide*.

Related tasks

- Installing products necessary for the management server and pair management server on page 369
- Setting the port numbers used for RMI communication on the Device Manager server on page 369

- Changing Replication Manager on the secondary site to maintenance mode on page 370

Installing products necessary for the management server and pair management server

Based on the system configuration, install the products necessary for the management server and pair management server.

Procedure

1. Install Hitachi Command Suite on the management server.

   For details about how to install Hitachi Command Suite, see the *Hitachi Command Suite Installation and Configuration Guide*.
2. Install CCI and Device Manager agent on the pair management server.

   For details about how to install CCI, see the manuals of CCI.

   For details about how to install Device Manager agent, see the *Hitachi Command Suite Installation and Configuration Guide*.

Setting the port numbers used for RMI communication on the Device Manager server

Set the port numbers used for RMI communication on the Device Manager server because if the Replication tab is used, RMI communication needs to be used to link with Replication Manager.

Before you begin

Log in as a user with Administrator permissions (for Windows) or as a root user (for Linux).

Procedure

1. Stop the services of Hitachi Command Suite product.
2. Set up the `rpmlib.rpm.port` property in the `rpmlib.properties` file of the Device Manager server.

   Enter the port number that is set for the `base.rmi.port` property in the `base.properties` file of Replication Manager. If you have not changed the value for the `base.rmi.port` property (default: 25200), this operation is unnecessary.

   The `base.properties` file is stored in the following location:

   In Windows:

   installation-folder-for-Hitachi-Command-Suite\ReplicationManager\conf

   In Linux:

installation-directory-for-Hitachi-Command-Suite/
ReplicationManager/conf

For details on the `base.properties` file and the `base.rmi.port` property of Replication Manager, see the *Replication Manager Configuration Guide*.

3. Start the services of Hitachi Command Suite product.

Related tasks

- Starting the Hitachi Command Suite services on page 458
- Stopping the Hitachi Command Suite services on page 460

Related references

- rpmlib.rpm.port on page 638

Changing Replication Manager on the secondary site to maintenance mode

For a configuration for multiple sites, change operation mode of Replication Manager on the secondary site to maintenance mode.

Before you begin

Log in to the GUI of Device Manager on the secondary site.

Procedure

1. Select **Manage Replication** from the **Actions** menu in the Device Manager GUI.
2. Click **Administration**, and then **Maintenance** in the **Explorer** menu.
3. Click the **Change Mode** button.
4. Check the message, and then change operation mode to maintenance mode.

Settings required to use the VMware VVol functionality

Hitachi Command Suite supports the storage management using the VVol functionality provided by VMware vSphere 6.0 or later. This section describes the system configuration required to use the VVol functionality and how to set the environment of Hitachi Command Suite. For an overview of the storage management using VVols and the flow of tasks for environment configuration and operations, see the *Hitachi Command Suite User Guide*.

System configuration for using the VVol functionality

The following shows an example of the system configuration for using the VVol functionality.

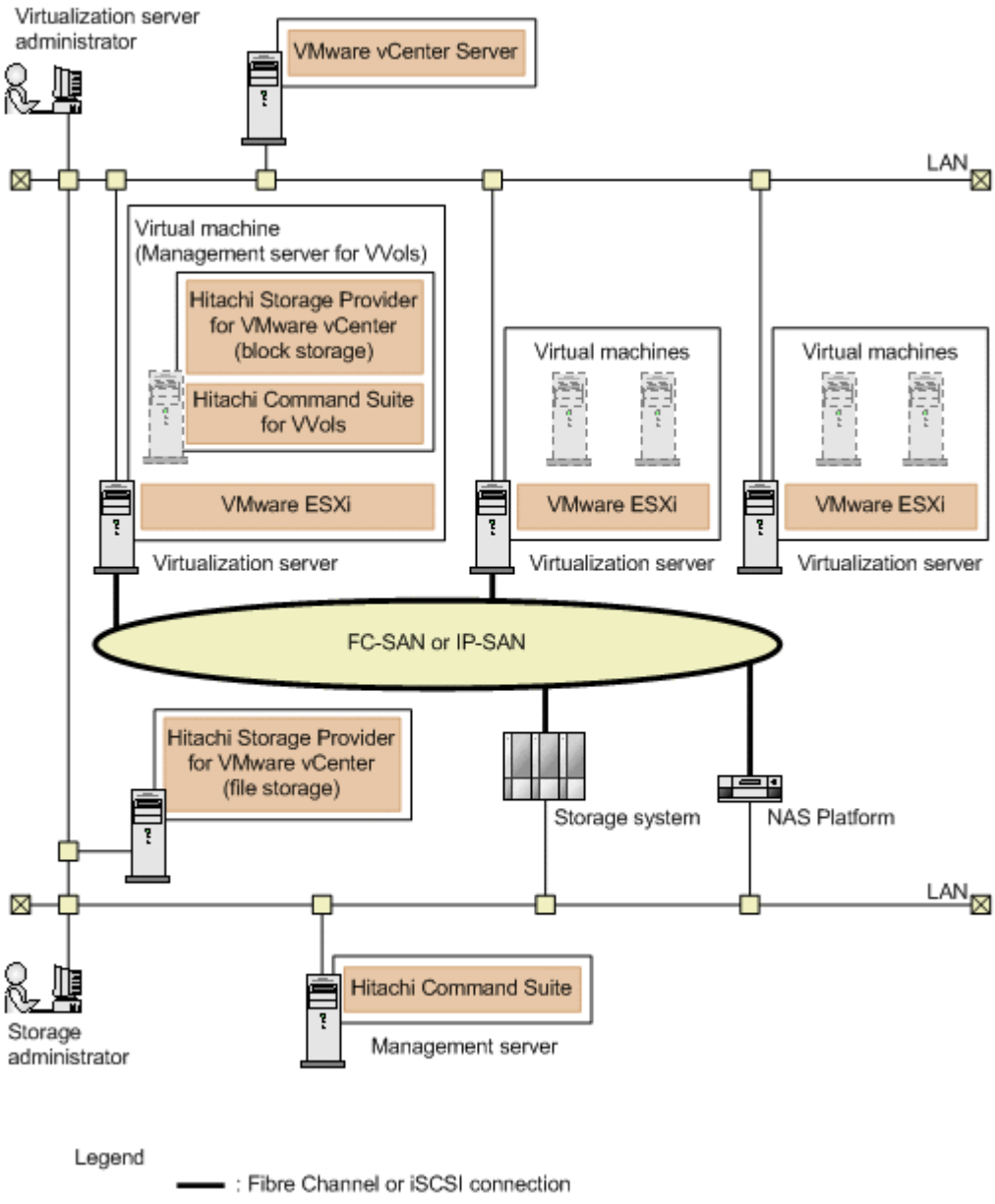


Figure 56 Example of the system configuration for using the VVol functionality

VMware vCenter Server

Software used for integrated management of VMware vSphere. For details about installation and environment configuration of VMware vCenter Server, see the VMware documentation.

Hitachi Storage Provider for VMware vCenter (VASA Provider)

Performs various operations, based on the VASA API requests from VMware vCenter Server or VMware ESXi. There are two types of VASA Providers: VASA Provider (block storage) and VASA Provider (file

storage). VASA Provider (block storage) performs operations on storage systems by linking with Hitachi Command Suite for VVols. VASA Provider (file storage) performs operations on storage systems by linking with NAS Platform and the management server for VVols.

For details about installation and environment configuration of VASA Provider, see the VASA Provider documentation.

Hitachi Command Suite for VVols

A Hitachi Command Suite dedicated to performing various VVol-related operations. In addition to the usual management server for operations management of the storage system, you need to prepare a dedicated management server (management server for VVOLs), install Hitachi Command Suite, and specify settings in order to operate as Hitachi Command Suite for VVols.

We recommend that you deploy Hitachi Command Suite for VVols in a configuration on a virtual server, in which Hitachi Command Suite is stored on one virtual machine together with VASA provider (block storage), by using a VASA provider (block storage) virtual appliance. In this case, Hitachi Command Suite for VVols is deployed in a state in which any required settings are complete. For details on VASA provider virtual appliances, see the manual for VASA provider (block storage).



Tip: If the OS of the management server for VVols is Windows, it might takes 5 seconds or more to display information about storage system VVols because it takes time to resolve the name of the VASA Provider (file storage). If this problem occurs, add the IP address and host name of the VASA Provider (file storage) to the `hosts` file on the management server.

Storage systems

To use the VVol functionality by linking with VASA Provider (block storage), a VSP G1000, G1500, VSP F1500, VSP Gx00 models or VSP Fx00 models system is required.

To use the VVol functionality by linking with VASA Provider (file storage), storage systems supported by NAS Platform are required.

Management server of Hitachi Command Suite

If the target storage system is VSP G1000, Hitachi Command Suite version 8.2.0 or later is required. If the target storage system is VSP Gx00 models or VSP Fx00 models, Hitachi Command Suite version 8.2.1 or later is required. If the target storage system is VSP G1500 or VSP F1500, Hitachi Command Suite version 8.5.0 or later is required. To use the VVol functionality by linking with VASA Provider (file storage), Hitachi Command Suite version 8.2.1 or later is required.

To use the VVol functionality, you need to change the Device Manager server settings.

To use Element Manager to perform storage system management excluding VVol-related operations that require access to Hitachi Command Suite for VVols, no Hitachi Command Suite management server is required.

For details about system requirements of the Hitachi Command Suite products, see *Hitachi Command Suite System Requirements*.

Required configuration for the management server for VVols to improve the availability of VVol management operations

If you use the VVol functionality by linking with VASA Provider (block storage), important data for using the VVol functionality is stored in the management server for VVols. If the services of the Hitachi Command Suite for VVols stop, the virtual machines will continue running, however you will not be able to perform management operations such as configuration changes on the virtual machines, creating snapshots, and power-on operations. To avoid stopping VVol management operations, we recommend that you improve the settings for availability and the fault tolerance of Hitachi Command Suite for VVols.

Configuration for improving the availability and the fault tolerance of Hitachi Command Suite for VVols

The recommended configuration for Hitachi Command Suite for VVols is one that is deployed on a virtual server by using the virtual appliance for a VASA provider (block storage). By using the volumes in the storage system as disks to be assigned to the virtual machine, you can use the replication functionality of the storage system. In addition, we strongly recommend that you use the VMware functionality for improving the availability of the virtual machine, and for protecting or recovering data.

We strongly recommend that you create a cluster configuration when you want to install Hitachi Command Suite for VVols on a physical server without using the virtual appliance for a VASA provider (block storage). Use a disk with a RAID configuration for the installation destination disk and the shared disk for the Hitachi Command Suite products to be installed on the management server for VVols.

Caution:

- If you stop the services of Hitachi Command Suite for VVols after starting operation that uses the VVol functionality, do so in a way that avoids these problems.
- Do not change the IP address or the host name of the management server for VVols after starting an operation that uses the VVol functionality. If the IP address or host name is changed, communication from a VASA provider

to the management server for VVols cannot be established, preventing operations from being performed on the virtual machine.

Data used for recovery after a failure occurs

The management server for VVols automatically obtains the following two types of data to recover the contents of the database when a failure occurs:

- Backup of the database
- System log of the database
  The system log is a change history log for the database. The management server for VVols automatically backs up the system log contents to the unload directory by using the automatic log unloading facility. If a failure occurs in the management server for VVols, you can recover the database to the state at a specific time by using the backup data and the unloaded system log data.

Note:

- Ensure that the installation destination of Hitachi Command Suite for VVols and the storage location for data that is obtained to recover the database when a failure occurs are on different physical disks. Only a single data store can be used immediately after a virtual appliance is deployed. For details on how to divide a data store, see the manual of the VASA provider (block storage).
- Do not use daylight saving time on the management server for VVols. If the clock of the OS of the management server for VVols is delayed due to daylight saving time, the contents of the system log become inconsistent, and they cannot be used to recover the database if a failure occurs. To use daylight saving time, you need to stop the services of Hitachi Command Suite for VVols before the OS clock is delayed, and then start the services after the delayed time has elapsed. During this operation, the operation of virtual machines stops.

After operations that use VVols have started, monitor whether the database is backed up and whether the system log is obtained normally by the management server for VVols.

Monitor the status of backup operations:

You must monitor whether the database is backed up normally.

When a backup operation is performed, log data is output to the event log or syslog of the OS, regardless of whether the backup succeeds or fails. Confirm that the log data that indicates a backup failure (KAIC30962-E) is not output and that the log data that indicates a successful backup (KAIC30963-I) is properly output.

For periodic backup operations, if a request from the VASA provider is received while a backup operation is being performed, backup processing stops, and processing based on the request from the VASA provider is prioritized. When a backup operation is suspended in this way for more than one day, restoration might take a long time. Stop the operations related to VVols and restart the services of Hitachi Command Suite as necessary. The database will be backed up after the services restart.

Note: We recommend that you periodically back up the backup directory in case the backup directory becomes inaccessible due to a failure on the disk where the backup directory is located.

Monitor the automatic log unloading facility:

If a failure occurs in the unload directory and the system log data is continuously prevented from being unloaded, the database can no longer be updated when the capacity of the system log file reaches the maximum. If the automatic log unloading facility stops, a log entry that indicates that the functionality has stopped (KFPS01150-E) is output to the event log or syslog of the OS. If this occurs, perform the following actions:

- If a failure occurred on the disk, stop the services of Hitachi Command Suite, and then change the location of the unload directory to another disk.
- If the disk does not have sufficient space, the directory does not exist, or permissions are invalid, remove the cause of the failure, and then restart the services of Hitachi Command Suite.
- For other cases than the above, contact maintenance personnel.

Combinations of components for using the VVol functionality

This section describes how the following system components can be combined to use the VVol functionality: VMware vCenter Server, VASA Provider, Hitachi Command Suite for VVols, and storage systems.

The following table shows how components can be combined for use.

Table 58 Combining components for using VVols

Components	Combination
VMware vCenter Server and VASA Provider (block storage)	• An instance of VMware vCenter Server can be linked to multiple instances of VASA Provider (block storage).

Components	Combination
	• Multiple instances of VMware vCenter Server can be linked to a single instance of VASA Provider (block storage).[#1]
Hitachi Command Suite for VVols and storage systems	• A single Hitachi Command Suite for VVols can be used to manage multiple storage systems. • Multiple Hitachi Command Suite for VVols can be used to manage a single storage system.[#2]
Hitachi Command Suite for VVols and VASA Provider (file storage)	A single Hitachi Command Suite for VVols can be specified as the linkage destination of only one instance of VASA Provider (file storage).
VASA Provider (file storage) and NAS Platform	An instance of VASA Provider (file storage) can be linked to multiple instances of NAS Platform.

#1

This applies when the version of VASA Provider (block storage) is 3.3 or later.

#2

This applies when the versions of Hitachi Command Suite for VVols are 8.4.1 or later.

The following figure shows an example of a system configuration when multiple storage systems are managed by multiple instances of VMware vCenter Server, multiple instances of VASA Provider, and multiple Hitachi Command Suite for VVols.

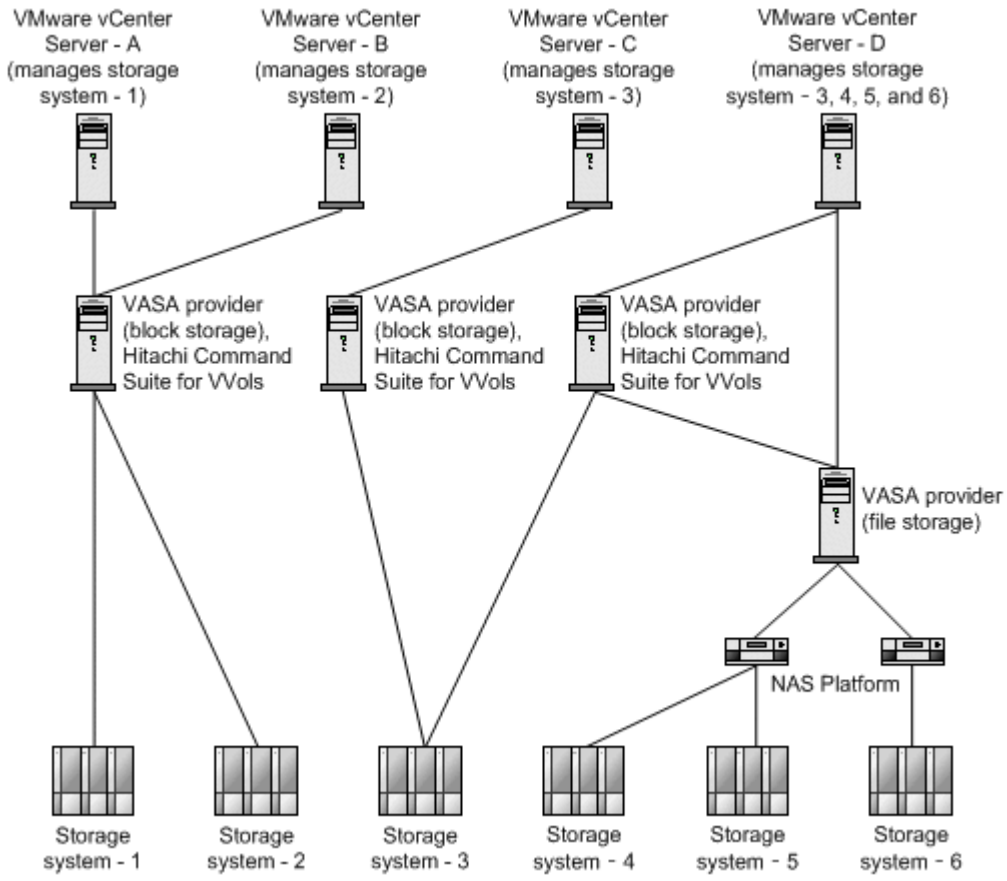


Figure 57 Example of the system configuration with multiple storage systems

Flow of tasks for setting the Hitachi Command Suite products for using the VVol functionality

To use the functionality for VVols, you must specify the settings for a VASA provider and the management server for VVols. For details on installing and setting up the VASA provider, see the manual of the VASA provider. This section describes the flow of tasks for setting the environment of the Hitachi Command Suite products, which is required to use the VVol functionality. After installing and setting up the products on the management server and the management server for VVols, the storage administrator registers storage systems and ESXi hosts, and specifies settings for the storage systems, which are required to use the VVol functionality.

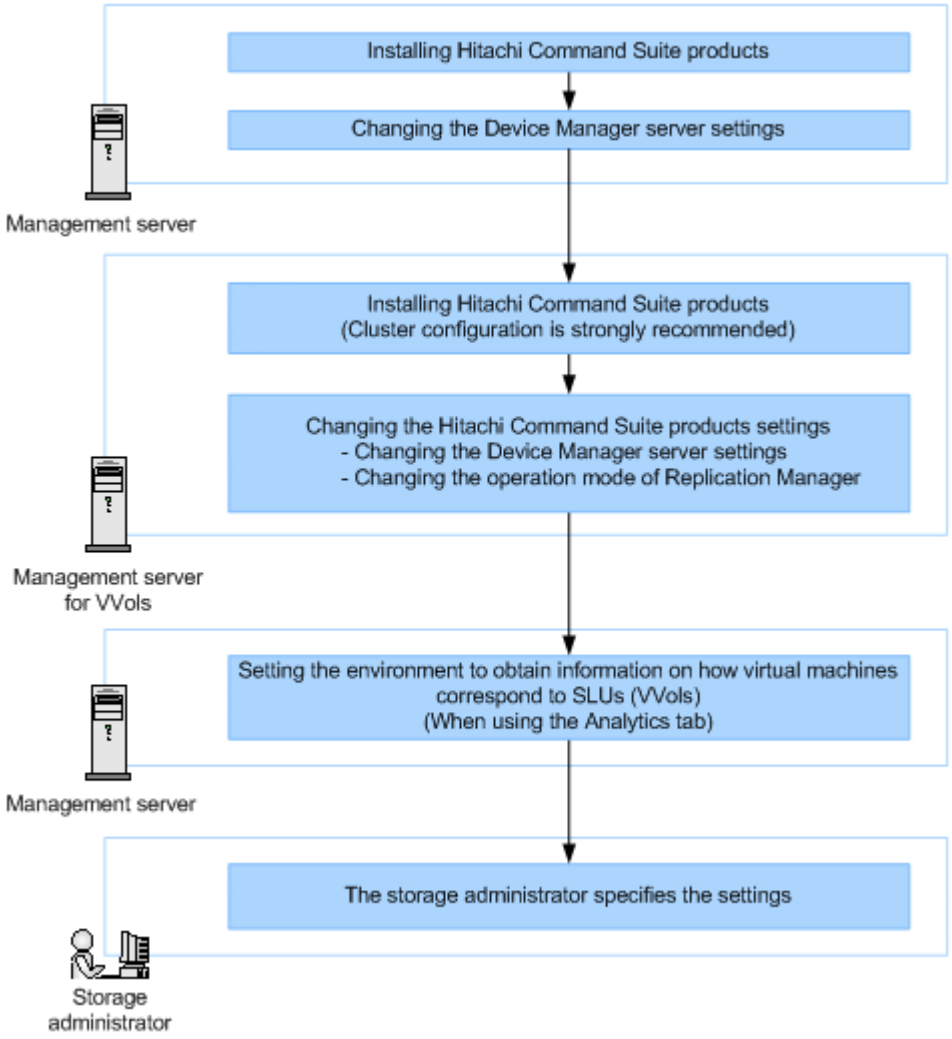


Figure 58 Flow of tasks for configuring the environment for using the VVol functionality

When configuring a management server for VVols by using a VASA provider (block storage) virtual appliance, these tasks are not required on the management server for VVols. They are not required because Hitachi Command Suite for VVols is deployed in the state in which installation and setting changes are complete in the management server for VVols. For details about deploying a VASA provider (block storage) virtual appliance, see the manual for VASA provider (block storage).

Related concepts

- Installing Hitachi Command Suite products on the management server on page 379
- Installing Hitachi Command Suite products on the management server for VVols on page 380

Related tasks

- Changing the Device Manager server settings on the management server on page 379
- Changing the Hitachi Command Suite settings on the management server for VVols (in a non-cluster environment) on page 382
- Changing the Hitachi Command Suite settings on the management server for VVols (in a Windows cluster configuration) on page 383
- Changing the Hitachi Command Suite settings on the management server for VVols (in a Linux cluster configuration) on page 385
- Setting the environment on the management server to obtain information on how virtual machines correspond to SLUs (VVols) (When using the Analytics tab) on page 390

Installing Hitachi Command Suite products on the management server

On the management server, install the Hitachi Command Suite products. Follow the normal procedure to perform installation.

For details about how to install the Hitachi Command Suite products, see the *Hitachi Command Suite Installation and Configuration Guide*.

Changing the Device Manager server settings on the management server

To use the VVol management functionality, you need to change the settings of the properties of the Device Manager server.

Before you begin

- Log in as a user with Administrator permissions (for Windows) or as a root user (for Linux).
- Install Hitachi Command Suite on the management server.

Procedure

1. Stop the services of the Hitachi Command Suite products.
2. Use a text editor to change the values of the following properties:

   Note: We recommend that you make a note of the original settings before changing the values in the property files.

   - For `server.dispatcher.daemon.configUpdate.detection.interval` in the `dispatcher.properties` file, specify `0`.
   - For `server.dispatcher.daemon.autoSynchro.doRefresh` in the `dispatcher.properties` file, specify `false`.

- For `server.subsystem.ssid.availableValues` in the `server.properties` file, specify `4-7FFF`.

The property file of the Device Manager server is in the following location:

In Windows:

Hitachi-Command-Suite-installation-folder\DeviceManager\HiCommandServer\config

In Linux:

Hitachi-Command-Suite-installation-directory/HiCommandServer/config

3. Start the services of the Hitachi Command Suite products.

Note: If you change the settings, the functionality for automatically refreshing the configuration information and updating the database to the latest state when the storage system configuration is changed by using a tool other than Hitachi Command Suite becomes unavailable. Manually refresh the configuration information of the storage system as necessary.

Related tasks

- Starting the Hitachi Command Suite services on page 458
- Stopping the Hitachi Command Suite services on page 460

Related references

- server.subsystem.ssid.availableValues on page 601
- server.dispatcher.daemon.configUpdate.detection.interval on page 608
- server.dispatcher.daemon.autoSynchro.doRefresh on page 609

Installing Hitachi Command Suite products on the management server for VVols

To install Hitachi Command Suite for VVols, we recommend that you use a VASA provider (block storage) virtual appliance. For details about VASA provider (block storage) virtual appliances, see the manual for VASA provider (block storage). This section describes how to install Hitachi Command Suite onto a management server for VVols without using a virtual appliance.

Note:

- If you use the VVol functionality by linking with VASA Provider (block storage), we strongly recommend that you use the management server for VVols in a cluster configuration to prevent the VVol management operation from stopping. Important data for the VVol functionality is stored in the

management server for VVols. For this reason, use a disk with a RAID configuration for the installation destination disk and shared disk.

- If you perform an overwrite or upgrade installation of Hitachi Command Suite on the management server for VVols, the services of the Hitachi Command Suite products stop temporarily on the management server for VVols. If the services of the Hitachi Command Suite products stop on the management server for VVols, the virtual machines will continue running, but you will be unable to perform configuration changes on the virtual machines, or perform management operations such as snapshot operations and power-on operations. If you perform an overwrite or upgrade installation of Hitachi Command Suite on the management server for VVols after starting an operation that uses the VVol functionality, perform the overwrite or upgrade installation in a way that avoids these problems.

The procedures for installing Hitachi Command Suite on the management server for VVols, configuring a cluster environment, and changing the settings of Hitachi Command Suite vary depending on the OS of the management server for VVols.

- In Windows:
  Perform the installation and configure the cluster environment according to the normal procedure. After that, change the settings of Hitachi Command Suite.

- In Linux:
  Install Hitachi Command Suite on the executing and standby nodes, and then change the settings of Hitachi Command Suite on the both nodes. After that, configure the cluster environment according to the normal procedure.

For details on installation and cluster environment configuration of the Hitachi Command Suite products, see the *Hitachi Command Suite Installation and Configuration Guide*.

Note: For the management server for VVols, only register the license for Device Manager. Do not register licenses for other Hitachi Command Suite products.

Related tasks

- Changing the Hitachi Command Suite settings on the management server for VVols (in a non-cluster environment) on page 382
- Changing the Hitachi Command Suite settings on the management server for VVols (in a Windows cluster configuration) on page 383
- Changing the Hitachi Command Suite settings on the management server for VVols (in a Linux cluster configuration) on page 385

Changing the Hitachi Command Suite settings on the management server for VVols (in a non-cluster environment)

To use the VVol functionality, you need to change the following settings on the management server for VVols:

- Change the Device Manager server settings.
  To change the Device Manager server settings, use the `vvoladaptersetup` tool.
- Change the operation mode of Replication Manager.
  To suppress access from Replication Manager to storage systems and the Device Manager server, change the operation mode of Replication Manager to maintenance mode.

Before you begin

- Log in as a user with Administrator permissions (for Windows) or as a root user (for Linux).
- Complete the installation of Hitachi Command Suite.

Procedure

1. Stop the services of the Hitachi Command Suite product.
2. Execute the `vvoladaptersetup` tool from the command prompt or terminal window.

   In Windows:

   Hitachi-Command-Suite-installation-folder\DeviceManager\HiCommandServer\tools\vvoladaptersetup.bat

   In Linux:

   Hitachi-Command-Suite-installation-directory/HiCommandServer/tools/vvoladaptersetup.sh
3. In the main menu, specify `1`.

   Specify the settings according to the message displayed in the window.
4. In the main menu, specify `2` to check the settings.
5. If no problem with the settings exists, in the main menu, specify `3` to end the tool.
6. Open the following files by using a text editor.

   In Windows:

   Hitachi-Command-Suite-installation-folder\ReplicationManager\conf\base.properties

   In Linux:

Hitachi-Command-Suite-installation-directory/ReplicationManager/conf/base.properties

7. Add the following text to the content of the file, and then save it.

   ```
   base.operationmode.forcemaintenancemode=true
   ```

8. Start the services of the Hitachi Command Suite product.

Note: If you execute the `vvoladaptersetup` tool, the settings of the following properties of the Device Manager server will not be applied to the system:

- The `logger.MaxBackupIndex` property, `logger.MaxFileSize` property, `logger.hicommandbase.MaxBackupIndex` property, and `logger.hicommandbase.MaxFileSize` property in the `logger.properties` file
- The `server.dispatcher.snm2.configchange.pollingPeriod` property, `server.dispatcher.configchange.pollingPeriod` property, `server.dispatcher.daemon.configUpdate.detection.interval` property, and `server.dispatcher.daemon.autoSynchro.doRefresh` property in the `dispatcher.properties` file
- The `server.cim.support` property, `server.mail.enabled.storagesystem` property, `server.mail.enabled.fileserver` property, and `server.subsystem.ssid.availableValues` property in the `server.properties` file

---

Related references

- Setup items for the vvoladaptersetup tool on page 388
- Device Manager server configuration properties (server.properties file) on page 591
- Device Manager log output properties (logger.properties file) on page 603
- Device Manager dispatcher properties (dispatcher.properties file) on page 606

Changing the Hitachi Command Suite settings on the management server for VVols (in a Windows cluster configuration)

To use the VVol functionality, you need to change the following settings on the management server for VVols:

- Change the Device Manager server settings.
  To change the Device Manager server settings, use the `vvoladaptersetup` tool.

- Change the operation mode of Replication Manager.
  To suppress access from Replication Manager to storage systems and the Device Manager server, change the operation mode of Replication Manager to maintenance mode.

Specify settings on both the executing and standby nodes.

Before you begin

- Log on as a user with Administrator permissions.
- Complete the configuration of the cluster environment.

Procedure

1. On the standby node, execute the `vvoladaptersetup` tool from the command prompt.

   Hitachi-Command-Suite-installation-folder\DeviceManager\HiCommandServer\tools\vvoladaptersetup.bat
2. In the main menu, specify `1`.

   Specify the settings according to the message displayed in the window.

   Specify a path to the location on the shared disk for the backup directory and the unload directory.
3. In the main menu, specify `2` to check the settings.
4. If no problem with the settings exists, in the main menu, specify `3` to end the tool.
5. Open the following files by using a text editor.

   Hitachi-Command-Suite-installation-folder\ReplicationManager\conf\base.properties
6. Add the following text to the content of the file, and then save it.

   ```
   base.operationmode.forcemaintenancemode=true
   ```
7. Stop the services of the Hitachi Command Suite product.
8. Bring the resource group and the services of the Hitachi Command Suite products online.
9. From the Hitachi Command Suite GUI, register the license for Device Manager.
10. Take the services of the Hitachi Command Suite products offline.
11. Move the owner of the resource group in which the services of the Hitachi Command Suite products are registered to the executing node.
12. On the executing node, perform the same operations described in steps 1 to 9.

Note: If you execute the `vvoladaptersetup` tool, the settings of the following properties of the Device Manager server will not be applied to the system:

- The `logger.MaxBackupIndex` property, `logger.MaxFileSize` property, `logger.hicommandbase.MaxBackupIndex` property, and `logger.hicommandbase.MaxFileSize` property in the `logger.properties` file
- The `server.dispatcher.snm2.configchange.pollingPeriod` property, `server.dispatcher.configchange.pollingPeriod` property, `server.dispatcher.daemon.configUpdate.detection.interval` property, and `server.dispatcher.daemon.autoSynchro.doRefresh` property in the `dispatcher.properties` file
- The `server.cim.support` property, `server.mail.enabled.storagesystem` property, `server.mail.enabled.fileserver` property, and `server.subsystem.ssid.availableValues` property in the `server.properties` file

Related tasks

- Stopping the Hitachi Command Suite services on page 460

Related references

- Setup items for the vvoladaptersetup tool on page 388
- Device Manager server configuration properties (server.properties file) on page 591
- Device Manager log output properties (logger.properties file) on page 603
- Device Manager dispatcher properties (dispatcher.properties file) on page 606

Changing the Hitachi Command Suite settings on the management server for VVols (in a Linux cluster configuration)

To use the VVol functionality, you need to change the following settings on the management server for VVols:

- Change the Device Manager server settings.
  To change the Device Manager server settings, use the `vvoladaptersetup` tool.
- Change the operation mode of Replication Manager.
  To suppress access from Replication Manager to storage systems and the Device Manager server, change the operation mode of Replication Manager to maintenance mode.

Specify settings on both the executing and standby nodes.

Before you begin

- Log in as a root user.
- Complete the installation of Hitachi Command Suite on the executing and standby nodes.
  The installation procedures are the same as those performed for a normal cluster environment. See the *Hitachi Command Suite Installation and Configuration Guide*.

Procedure

1. On the standby node, execute the `vvoladaptersetup` tool from the terminal window.

   Hitachi-Command-Suite-installation-directory`/HiCommandServer/tools/vvoladaptersetup.sh`
2. In the main menu, specify `1`.

   Specify the settings according to the message displayed in the window.

   Specify a path to the location on the shared disk for the backup directory and the unload directory.
3. In the main menu, specify `2` to check the settings.
4. If no problem with the settings exists, in the main menu, specify `3` to end the tool.
5. Open the following files by using a text editor.

   Hitachi-Command-Suite-installation-directory`/ReplicationManager/conf/base.properties`
6. Add the following text to the content of the file, and then save it.

   `base.operationmode.forcemaintenancemode=true`
7. Stop the services of the Hitachi Command Suite product.
8. Move the service group to the executing node.
9. On the executing node, perform the same operations described in steps 1 to 7.
10. Create a script for registering the services of the Hitachi Command Suite products.

    Subsequent steps are the same as described in the normal procedure for configuring a cluster environment. For details, see the *Hitachi Command Suite Installation and Configuration Guide*.

Note: If you execute the `vvoladaptersetup` tool, the settings of the following properties of the Device Manager server will not be applied to the system:

- The `logger.MaxBackupIndex` property, `logger.MaxFileSize` property, `logger.hicommandbase.MaxBackupIndex` property, and `logger.hicommandbase.MaxFileSize` property in the `logger.properties` file
- The `server.dispatcher.snm2.configchange.pollingPeriod` property, `server.dispatcher.configchange.pollingPeriod` property, `server.dispatcher.daemon.configUpdate.detection.interval` property, and `server.dispatcher.daemon.autoSynchro.doRefresh` property in the `dispatcher.properties` file
- The `server.cim.support` property, `server.mail.enabled.storagesystem` property, `server.mail.enabled.fileserver` property, and `server.subsystem.ssid.availableValues` property in the `server.properties` file

Related tasks

- Stopping the Hitachi Command Suite services on page 460

Related references

- Setup items for the vvoladaptersetup tool on page 388
- Device Manager server configuration properties (server.properties file) on page 591
- Device Manager log output properties (logger.properties file) on page 603
- Device Manager dispatcher properties (dispatcher.properties file) on page 606

Changing the settings on the Hitachi Command Suite for VVols after starting an operation

To change the settings by using the `vvoladaptersetup` tool after starting an operation that uses the VVol functionality:

Before you begin

Log in as a user with Administrator permissions (for Windows) or as a root user (for Linux).

Procedure

1. Make sure that the owner or the service groups of the resource group in which the services of the Hitachi Command Suite products are registered have been moved to the executing node.
2. Perform the following on the executing node:

   For Windows, take the Hitachi Command Suite product services offline.

   For Linux, delete the Hitachi Command Suite product services from the service group.
3. Execute the `vvoladaptersetup` tool from the command prompt or terminal window to change the settings.
4. Stop the Hitachi Command Suite product services.
5. Move the owner or the service groups of the resource group to the standby node.
6. Perform steps 3 and 4 on the standby node.
7. Move the owner or the service groups of the resource group to the executing node.
8. Perform the following on the executing node:

   For Windows, bring the resource group and the Hitachi Command Suite product services online.

   For Linux, re-register the Hitachi Command Suite product services that were deleted in step 2 to the service group.

Tip: For a non-cluster configuration, execute the `vvoladaptersetup` tool again. If you want to change the backup directory or the unload directory, stop the Hitachi Command Suite product services, execute the `vvoladaptersetup` tool, and then start the service.

Related references

- Setup items for the vvoladaptersetup tool on page 388

Setup items for the vvoladaptersetup tool

For the `vvoladaptersetup` tool, specify the following settings:

- Change of the operation mode for Hitachi Command Suite for VVols
- Backup directory for the database
- Interval at which the database is backed up
- Number of generations of backed up files of the database
- Unload directory for the system log for the database

- Other property settings

The following table shows the items to be entered to set the command:

Table 59 Items to be entered for the vvoladaptersetup tool

Item	Description	Default value
Backup directory	Specify the storage location of the backup file of the database as an absolute path. The backup files are stored in the backup directory, and the files are stored with a name that starts with `backup_`. To estimate the disk capacity (in MB) required for a backup directory, use the following formula: *number-of-VMs* x (1 + *number-of-generations* + 2 x *number-of-days-for-backup-interval*) + 10000 You cannot specify locations on network drives. The maximum specifiable length for an absolute path is 136 bytes.	None
Interval at which the database is backed up	Specify the interval at which the database is backed up in units of minutes. The specifiable range of values is from 720 to 10080.	1440
Number of generations of backed up files of the database	Specify the number of generations of backed up files of the database. In addition to being backed up at the specified intervals, the database is also backed up when the Device Manager service is restarted. A backup obtained when the service is restarted is also counted as one generation. The specifiable range of values is from 1 to 1000.	14
Unload directory	Specify the storage location of the unloaded files for backing up the system log contents as an absolute path. To estimate the disk capacity (in MB) required for the unload directory, use the following formula: (3 x *number-of-VMs* x *number-of-days-for-backup-interval*) + 10000 Specify an empty directory. You cannot specify locations on network drives.	None

Item	Description	Default value
	The maximum specifiable length for an absolute path is 136 bytes.	
Other properties	Specify the following properties: • `server.subsystem.ssid.availableValues`# • `logger.MaxBackupIndex` • `logger.MaxFileSize` • `logger.hicommandbase.MaxBackupIndex` • `logger.hicommandbase.MaxFileSize`	A recommended value for each property is displayed as the default.

#:

For a configuration in which multiple management servers for VVols are used to manage a single storage system, specify this property so that the management servers for VVols do not have the same range of SSIDs. If you are managing storage systems by using a Hitachi Command Suite management server, make sure the management server does not use the same range of SSIDs as the ranges used by management servers for VVols. If you are managing storage systems by using Element Manager, make sure Element Manager does not use the range of SSIDs as the ranges used by the management servers for VVols.

Setting the environment on the management server to obtain information on how virtual machines correspond to SLUs (VVols) (When using the Analytics tab)

If VVol is being used to identify performance issues of the storage systems for each virtual machine by using the Analytics tab, from Hitachi Command Suite for VVols, you need to obtain information about how virtual machines correspond to SLUs. To obtain information about how virtual machines correspond to SLUs, from Hitachi Command Suite for VVols, download Device Manager CLI to the management server and setup the environment for the Device Manager CLI to be executed.

Before you begin

- Log in as a user with Administrator permissions (for Windows) or as a root user (for Linux).
- Check the version of Host Data Collector (if a Host Data Collector machine is used).

If Host Data Collector is installed on a machine other than the management server, confirm that the version of Host Data Collector is 8.2.0 or later.

- Check the version of Tuning Manager - Agent for RAID.
  Confirm that the version of Tuning Manager - Agent for RAID is 8.2.0 or later.
- Set for analyzing storage system performance information.
  When configuring an instance environment for each monitoring target storage system on the host that collects performance information, specify `Y` for `Unassigned Open Volume Monitoring`, which is instance information for Tuning Manager - Agent for RAID. For details about how to configure the instance environment, see *Hitachi Command Suite Tuning Manager Installation Guide*.
- Configure the SSL server on the management server for VVols (when communicating by using HTTPS)
  Configure the management server for VVols as the SSL server.
- Obtain the truststore file of the management server for VVols. (when communicating by using HTTPS)
  Obtain the file from the management server using a secure way. Do not change the file name.
- Prepare the JRE to execute Device Manager CLI
  If communicating by using HTTPS, use the JRE that was downloaded from the Oracle web site. We recommend using the JRE that was downloaded from the Oracle web site even if HTTP is used for communication, but the JRE that was shipped together with the Hitachi Command Suite products can also be used.

Procedure

1. In the following directory, create a file named `hdvm_cli_jre_path`.

   In Windows:

   Hitachi-Command-Suite-installation-folder\DeviceManager\HiCommandServer\vvoladapter

   In Linux:

   Hitachi-Command-Suite-installation-directory/HiCommandServer/vvoladapter

2. In the `hdvm_cli_jre_path` file, use the text editor and enter the path to the JRE as an absolute path.

   The following is an example of specifying a path for the JRE that was shipped together with the Hitachi Command Suite products.

In Windows:

Hitachi-Command-Suite-installation-folder\Base64\uCPSB\jdk\jre\bin

In Linux:

Hitachi-Command-Suite-installation-directory/Base64/uCPSB/jdk/jre/bin

---

Note:

- Enter the path of the JRE on a single line.
- Do not enter a space or tab before or after the path of the JRE.
- Do not enclose the path of the JRE in double quotation marks (").

---

3. Execute the following command from the command prompt or terminal window.

   In Windows:

   ```
   for /f "usebackq delims=" %i in (`type "Hitachi-Command-Suite-installation-folder\DeviceManager\HiCommandServer\vvoladapter\hdvm_cli_jre_path"`) do set HDVM_CLI_JRE_PATH=%i
   ```

   In Linux:

   ```
   while read LINE; do LINE=`echo ${LINE}`; if [ -n "${LINE}" ]; then export HDVM_CLI_JRE_PATH=${LINE}; fi done < "Hitachi-Command-Suite-installation-directory/HiCommandServer/vvoladapter/hdvm_cli_jre_path"
   ```

   To execute commands by using the methods below, execute the commands in the command prompt or in the terminal window that was activated in step 3.

4. In the following directories, create a number of directories (with names of your choice) equal to the number of management servers for VVols.

   In Windows:

   Hitachi-Command-Suite-installation-folder\DeviceManager\HiCommandServer\vvoladapter

   In Linux:

   Hitachi-Command-Suite-installation-directory/HiCommandServer/vvoladapter

5. From the **Tools** menu for the Device Manager GUI of the management server for VVols, select **Download** to download the Device Manager CLI file.

   Perform the following procedure for all the created directories.
6. Copy the downloaded Device Manager CLI file to one of the created directories, and then decompress the file.
7. Use the text editor and change the settings of the properties file (`HiCommandCLI.properties`).

   `HiCommandCLI.serverurl` property

   Set the URL of Hitachi Command Suite for VVols in the following format:

   `HiCommandCLI.serverurl=`*`protocol`*`://`*`management-server-for-VVols-IP-address-or-host-name`*`:`*`management-server-for-VVols-port-number`*`/service`

   For *protocol*, specify `http` if using HTTP, or `https` if using HTTPS.

   If the management server for VVols is used in a cluster configuration, specify the logical host name for *management-server-for-VVols-IP-address-or-host-name*.

   For *management-server-for-VVols-port-number*, if using HTTP, specify the port number used for HTTP communication (default: 2001). If using HTTPS, specify the port number used for HTTPS communication (default: 2443).

   `user` property

   Set a user ID to log in to the Hitachi Command Suite for VVols.

   For the user ID, `All Resources` must be assigned as a resource group. Also, `Admin`, `Modify`, or `View` must be assigned as a Device manager role.

   `secure` property

   If using HTTPS for communication, set `true`. Because the `secure` property is not included in the template file, add it as follows:

   ```
   ##### OPTIONS ####
   secure=true
   ```
8. If using HTTPS for communication, copy the truststore file downloaded from the management server for VVols to one of the created directories.

   You do not need to set the environment variable `HDVM_CLI_CERTS_PATH` here.
9. Register a password to log in to the Hitachi Command Suite for VVols.

Execute the `hdvmaccount` command to register the encoded password to the properties file. For details, see the *Hitachi Command Suite CLI Reference Guide*.

10. Execute the following command from the command prompt or terminal window, and then confirm that the command is successful.

    In Windows:

    ```
    HiCommandCLI.bat GetServerInfo
    ```

    In Linux:

    ```
    ./HiCommandCLI.sh GetServerInfo
    ```

Related concepts

- Operation workflow for secure communication between a management server and a management client (Device Manager CLI) on page 227
- Settings required to collect storage system performance information on page 336

Related tasks

- Downloading a Device Manager server truststore file on page 288

Discarding the environment used for the VMware VVol functionality

This section describes how to cancel operations that use the VVol functionality, and how to discard the environment.

Procedure

1. From the management server for VVols, remove Hitachi Command Suite.
2. Undo the changes to the settings of the Device Manager server properties that were changed in the management server.
3. To use the **Analytics** tab, delete all of the directories and files that were created under the following directory:

   In Windows:

   Hitachi-Command-Suite-installation-folder`\DeviceManager\HiCommandServer\vvoladapter`

   In Linux:

   Hitachi-Command-Suite-installation-directory`/HiCommandServer/vvoladapter`

Related tasks

- Changing the Device Manager server settings on the management server on page 379

Recovering from a failure that occurred on the management server for VVols

The following describes the recovery procedure that uses another server if a physical failure occurs on the management server for VVols and the server can no longer be used when you use the VVol functionality by linking with VASA Provider (block storage).

Note:

- The procedure described here is provided to allow you to quickly resume operations. Some operations must be performed by maintenance personnel for complete recovery.
- If you restore the contents of the database in order to recover the database to the state at a certain point in time, you might not be able to use some of the objects on which operations are completed after the time point.
- If a logical failure occurs, operations must be performed by maintenance personnel.

Procedure

1. Make sure that you can use the data used for recovery.

   The database can be recovered in either of the following cases:

   - When the backed up files in the backup directory and the unloaded files in the unload directory can be used
     Use the backed up files and the unloaded files to recover the database to the point when the latest unloaded file was obtained.
   - When only the backed up files can be used
     Use the backed up files to recover the database to the point when the backup was obtained.
     If you can access the backed up files in the backup directory, use those files. If you cannot access the backup directory, and a backup exists of the backup directory itself, use the latest backed up files from that directory.

   If there are no backed up files that can be used, you cannot recover the server.
2. Configure a management server for VVols to be used for recovery separately from the management server for VVols where a failure occurred.

   Specify the same settings as those of the management server for VVols where a failure occurred, such as installation of Hitachi Command Suite, configuration of a cluster environment, and changes to the Device

Manager server settings. Match the settings of the following items to those of the management server for VVols where a failure occurred:

- OS
- Time zone
- Version of Hitachi Command Suite to be installed
- Installation destination
- IP address and host name
- Time

3. On the management server for VVols for recovery, stop the services of Hitachi Command Suite.
   - If the OS of the management server for VVols is in a Windows cluster configuration, make sure that the owner of the resource group in which the services of the Hitachi Command Suite products are registered has been moved to the executing node, and then take the services offline by using the `hcmds64clustersrvstate` command.
   - If the OS of the management server for VVols is in a Linux cluster configuration, make sure that the service group has been moved to the executing node, and then remove the services of the Hitachi Command Suite products from the service group.
   - For a non-cluster configuration, stop the services by using the `hcmds64srv` command.
4. Restore the data of the management server for VVols where a failure occurred to the management server for VVols for recovery.

   The restoration procedure differs depending on the state of the data that can be used for the restoration.

   If both the backed up files in the backup directory and the unloaded files in the unload directory can be used:

   Overwrite the backup directory and the unload directory created on the management server for VVols for recovery with the backup directory and unload directory used for recovery. At this time, make sure that you have created a backup for the backup directory and the upload directory. Check the last updated date and time of the files in the unload directory, and then perform a restore operation by specifying the last updated time.

   Execute the following command:

   In Windows:

installation-folder-for-Hitachi-Command-Suite
\DeviceManager\HiCommandServer\tools\databaserestore.bat
-restoretime *time-to-be-restored*

In Linux:

installation-directory-for-Hitachi-Command-Suite/
HiCommandServer/tools/databaserestore.sh -restoretime
time-to-be-restored

For *time-to-be-restored*, specify the time in the `yyyymmdd_hhmmss` format.

For example, specify `20151001_221030` when the time to be restored is 22:10:30, October 1, 2015.

If only the backed up files can be used:

Use the backup directory or the backed up files of the latest backup of the backup directory for restoration.

Execute the following command:

In Windows:

installation-folder-for-Hitachi-Command-Suite
\DeviceManager\HiCommandServer\tools\databaserestore.bat
-backupfile *absolute-path-to-the-backup-file*

In Linux:

installation-directory-for-Hitachi-Command-Suite/
HiCommandServer/tools/databaserestore.sh -backupfile
absolute-path-to-the-backup-file

The numerical values assigned to the file names of the backup files are in UNIX time (the time that has elapsed since 00:00:00, January 1, 1970 in UTC). Based on these values, identify the point in time at which the restore operation was performed.

5. Start the services of Hitachi Command Suite.
   - If the OS of the management server for VVols is in a Windows cluster configuration, use the `hcmds64srv` command to make sure that all the services have stopped, and then use the `hcmds64clustersrvstate` command to bring the resource group and services online.
   - If the OS of the management server for VVols is in a Linux cluster configuration, re-register the services of the Hitachi Command Suite products from the service group.
   - For a non-cluster configuration, start the services by using the `hcmds64srv` command.

6. Refresh the storage systems.
7. Log in to vCenter, and then rescan the VASA provider.
8. Regarding the operations performed after the point in time at which the database is restored, perform recovery operations as needed.
9. Resume operations.
10. Obtain the following maintenance information, and then contact customer support:
    - Output results of the `hcmds64getlogs` command
    - Backup directory
    - Unload directory
    - Backup of the backup directory
    - Parameters specified when the `databaserestore` command was executed

Related tasks

- Starting the Hitachi Command Suite services on page 458
- Stopping the Hitachi Command Suite services on page 460

Related references

- Recovering operations completed after the point in time at which the database is restored on page 398
- Acquiring maintenance information on the management server (hcmds64getlogs command) on page 578

Recovering operations completed after the point in time at which the database is restored

When the database of the management server for VVols is restored, if operations on an object were completed before the point in time at which the database was restored, you can continue the operations simply by refreshing the storage systems. For operations that were completed after the point in time at which the database was restored, you might not be able to continue the operations because the management server for VVols does not have data for the operations.

The following table describes how to recover operations that were completed after the point in time at which the database was restored.

Table 60 How to recover operations completed after the point in time at which the database is restored

Software used for operations	Operations performed	Recovery operations
Hitachi Command Suite	Operations performed on resource groups	Recovery operations are not required.
	Operations performed on DP pools, and on Thin Image data pools	Recovery operations are not required.
	Operations performed on PEs	Recovery operations are not required.
	Zero page reclaim operations	Recovery operations are not required.
vCenter	Creating a datastore	If the capability profile is displayed in the vCenter screen, recovery operations are not required. If the capability profile is not displayed, perform the following operations. **1.** Re-create the storage container. **2.** Unmount the datastore you created. **3.** Create a datastore.
	Operations on datastores other than creating a datastore	Recovery operations are not required.
	Operations performed on a VM Storage Policy	Recovery operations are not required.
	Powering on a VM	Back up important data on the VM to another machine, and then power the VM off and then on again.
	Powering off a VM	Recovery operations are not required.
	Suspending a VM	Power the VM off and then on again, and then suspend the VM.
	Expanding VM capacity	Recovery operations are not required.
	Reducing VM capacity	Recovery operations are not required.
	Adding hard disks to a VM	You cannot use a VM to which a hard disk was added after the point in time at which the database was restored. Perform the following operations: **1.** Back up the data on the OS to another machine, and then power the VM off. (Note: Only perform this operation if the VM is already powered on.) **2.** Delete the VM to which the hard disk was added from the inventory. **3.** Re-create the VM.
	Removing hard disks from a VM	Recovery operations are not required.
	Creating a VM	You cannot use a VM created after the point in time at which the database was restored. Perform the following operations:

Software used for operations	Operations performed	Recovery operations
		1. Back up the data on the OS to another machine, and then power the VM off. (Note: Only perform this operation if the VM is already powered on.) 2. Delete the created VM from the inventory. 3. Re-create the VM.
	Removing a VM	Recovery operations are not required.
	Storage vMotion	You cannot use a VM on which vMotion operations were completed after the point in time at which the database was restored. Perform the following operations: 1. Back up the data on the OS to another machine, and then power the VM off. (Note: Only perform this operation if the VM is already powered on.) 2. Delete the VM on which Storage vMotion was executed from the inventory. 3. Re-create the VM.
	Creating a snapshot	You cannot use a snapshot created after the point in time at which the database was restored. Delete the created snapshot, and then re-create the snapshot.
	Returning to the snapshot from a certain point in time	Recovery operations are not required.
	Removing snapshots	Recovery operations are not required.
	Creating clones from VVols to VMFS	Recovery operations are not required.
	Creating clones from VMFS to VVols, or from VVols to VVols	You cannot use clones created after the point in time at which the database was restored. Delete the created clones, and then re-create the clones.

For operations other than the above performed from Hitachi Command Suite on the management server for VVols, and for operations performed from vCenter, re-execute the operations if they were completed after the point in time at which the database was restored.

Settings necessary to launch Hitachi Storage Services Manager

Before you can launch Hitachi Storage Services Manager from the Device Manager GUI, you must create the `StorageServicesManager.conf` file.

Before you begin

- Log in as a user with Administrator permissions (for Windows) or as a root user (for Linux).

- Check the following information:
  - Hitachi Storage Services Manager startup URL
    For details, see the applicable Hitachi Storage Services Manager manual.

Procedure

1. Use a text editor to create a file named `StorageServicesManager.conf`.

   In the `StorageServicesManager.conf` file you created, set the `LaunchURL` parameter in the following format:

   `LaunchURL=`*`Hitachi-Storage-Services-Manager-startup-URL`*
2. Move the `StorageServicesManager.conf` file to the following location:

   In Windows:

   `installation-folder-for-Hitachi-Command-Suite``\Base64\common`

   In Linux:

   `installation-directory-for-Hitachi-Command-Suite``/Base64/common`

7

Setting up logs and alerts

This chapter describes the settings required to use the Hitachi Command Suite products to monitor the status of the system and errors.

- ☐ Setting up Hitachi Command Suite common trace log files
- ☐ Setting up alerts
- ☐ Sending SNMP traps to log files
- ☐ Settings required to use Device Manager event notification
- ☐ Settings required to use Tiered Storage Manager event notification

Setting up Hitachi Command Suite common trace log files

Common Component provides a common library used for logging. Hitachi Command Suite products use this library to output trace log information to log files.

Setting up Hitachi Command Suite common trace log files (Windows)

To change the number or size of Hitachi Command Suite common trace log files, use the Windows HNTRLib2 utility.

WARNING: Changing settings affects other program products that use Hitachi Command Suite common trace logs.

Before you begin

Log in to the system as a member of the Administrators group.

Procedure

1. Execute the Windows HNTRLib2 utility stored in the following location:

   program-files-folder\Hitachi\HNTRLib2\bin\hntr2util.exe
2. In the Hitachi Network Objectplaza Trace Utility 2 dialog box, for **Number of Files**, specify the number of trace log files.

   You can set a maximum of 16 trace log files. The default is 4.
3. In the Hitachi Network Objectplaza Trace Utility 2 dialog box, for **File Size**, specify the size of the trace log files.

   When the size of a trace log file has reached the specified value, the next trace log file is used.

   You can specify the trace log file size in the range from 8 KB to 4096 KB. The default is 256 KB. Specify a value greater than the value specified for **Buffer**.
4. Click **OK**.
5. Restart the OS to apply the changes.

Setting up Hitachi Command Suite common trace log files (Linux)

To change the number or size of Hitachi Command Suite common trace log files, use the utility program (`hntr2util`).

WARNING: Changing settings affects other program products that use Hitachi Command Suite common trace logs.

Before you begin

Log in to the system as a root user.

Procedure

1. Execute the utility program stored in the following location:

   ```
   /opt/hitachi/HNTRLib2/bin/hntr2util
   ```
2. In the menu, select `2` (**Number of log files**).
3. In the submenu, enter the desired number for trace log files, and then press **Enter**.

   You can set a maximum of 16 trace log files. The default is 4.
4. In the menu, select `1` (**Size of a log file**).
5. In the submenu, enter the desired number for trace log files, and then press **Enter**.

   When the size of a trace log file has reached the specified value, the next trace log file is used.

   You can specify the trace log file size in the range from 8 KB to 4096 KB. The default is 256 KB. Specify a value greater than the value specified for **Size of buffer**.
6. Check the contents you specified, enter **e**, and then press **Enter**.
7. Enter **y** to save the changes.
8. Execute the following command to delete the memory mapped file:

   ```
   # rm /opt/hitachi/HNTRLib/mmap/hntrmmap.mm
   ```
9. Restart the OS to apply the changes.

Setting up alerts

In Device Manager, information about errors that occurred in management-target storage systems or file servers is displayed in the Device Manager GUI/CLI as alerts. Alerts can also be sent by email.

Error detection by Device Manager

Device Manager detects errors in management-target storage systems or file servers as follows:

- Polling (default)
  Device Manager regularly monitors the operating status of the storage systems and file servers, and displays an alert when an error is detected. An alert includes the location where an error occurred and overview of the error.
  The polling interval can be set by using the `server.dispatcher.daemon.pollingPeriod` property of the Device Manager server.

- SNMP traps (optional)
  When SNMP traps are received from storage systems or file servers, they are displayed as alerts. SNMP traps are useful for determining the cause of an error, because they include information about the location of the error in addition to the site of the error.
  To receive SNMP traps in Device Manager, you must specify environment settings.

The alerts that Device Manager can display differ depending on the storage systems and file servers. The table below lists the alerts that are supported by each storage system or file server.

Table 61 Alerts that can be displayed by Device Manager

Management target		Polling	SNMP traps	Email notification of alerts
Storage system	VSP G1000	Y	v1, v3[#1]	Y
	VSP G1500	Y	v1, v3	Y
	VSP F1500	Y	v1, v3	Y
	VSP Gx00 models	Y	v1, v3[#2]	Y
	VSP Fx00 models	Y	v1, v3[#2]	Y
	Virtual Storage Platform	Y	v1	Y
	Universal Storage Platform V/VM	Y	v1	Y
	HUS VM	Y	v1	Y
	HUS100	Y	--	Y
	Hitachi AMS2000	Y	--	Y
	Hitachi SMS	Y	--	Y
	Hitachi AMS/WMS	Y	--	Y
	SMI-S enabled storage systems	--	--	--
File server	Hitachi Data Ingestor	--	v2c	--
	NAS Platform	Y[#3]	v1[#3]	Y[#3]
	Hitachi NAS Platform F	--	v2c	--

Legend

Y: Supported

--: Not supported

v1: Supports SNMP v1

v2c: Supports SNMP v2c

v3: Supports SNMP v3

#1

Supports SNMP v3 when the microcode version for VSP G1000 is 80-03-0*X*-*XX*/*XX* or later.

#2

Supports SNMP v3 when the microcode version for VSP Gx00 models and VSP Fx00 models is 83-01-2*X*-*XX*/*XX* or later.

For NAS modules, only SNMP v1 is supported.

#3

For file server, both of the following conditions must be satisfied to detect error information:

- The version of NAS Platform is 12.0 or later.

- Admin services EVS is set.

Note: For file server or NAS module, the timing of when polls and SNMP traps detect errors is different, but the same information is displayed in their alerts. Set SNMP traps only when you want to receive alerts in intervals less than 5 minutes. The default obtains alerts by polling in 5-minute intervals.

Related concepts

- Settings for displaying SNMP traps as alerts on page 407

Related tasks

- Changing Device Manager server properties on page 590

Related references

- server.dispatcher.daemon.pollingPeriod on page 607

Settings for displaying SNMP traps as alerts

To display SNMP traps as alerts, the following settings are required:

- Installing rpm packages (for Linux)
  Install the rpm packages necessary for receiving SNMP traps. For details about the necessary rpm packages, see *Hitachi Command Suite System Requirements*.
- Settings for Device Manager to receive SNMP traps
  - Device Manager must be able to use port `162/udp` of the management server.
  - Specify `true` for the `server.dispatcher.daemon.receiveTrap` property.
  - When using SNMP v3, the authentication information about the user who receives SNMP traps must be registered and encryption settings must be specified by using the `hdvmsnmpuser` command.

- Settings for reporting SNMP traps to Device Manager
  - For storage systems, the IP address of the management server must be registered in the SNMP Agent settings (common to SNMP v1 and SNMP v3).
  - When using SNMP v3, the authentication information about the user who receives SNMP traps must be registered and encryption settings must be specified from an SNMP Agent.

    Specify the same settings as the management server. For details about how to register and specify encryption settings for the authentication information, see the *Hitachi SNMP Agent User Guide*.
  - For NAS Platform, the host name or IP address of the management server and a port number (`162/udp`) must be set from SMU, NAS Manager, or the NAS Platform CLI as a target for trap notifications.

    Make the format of the IP address (IPv6 or IPv4) to be set match the following:

Table 62 IP address format for the management server to be set (setting SNMP traps for NAS Platform)

Conditions		IP address format (IPv6 or IPv4)
The setting for SNMP traps to be sent from Admin services EVS is set in the NAS Platform CLI.		Match the format with the IP address format for Admin services EVS.
The setting for SNMP traps to be sent from Admin services EVS is not set in the NAS Platform CLI.	An EVS for mounting the file system exists.	Match the format with the IP address format for EVS where the file system is to be mounted.
	An EVS for mounting the file system does not exist.	Match the format with the IP address format for the file server (node).

  - For Hitachi Data Ingestor, the host name or IP address of the Device Manager management server and a port number (`162/udp`) must be set in Hitachi File Services Manager.

When communicating between Device Manager and a storage system or file server in SNMP v1 or SNMP v2c, when the above settings are finished, the Device Manager server receives the SNMP traps of all communities and displays them as alerts.

When communicating between Device Manager and a storage system in SNMP v3, the Device Manager server receives all SNMP traps and displays them as alerts based on the authentication information set for the user who receives SNMP traps.

Related tasks

- Registering the user who receives SNMP traps (SNMP v3) on page 409

- Changing Device Manager server properties on page 590

Related references

- server.dispatcher.daemon.receiveTrap on page 607

Registering the user who receives SNMP traps (SNMP v3)

In Device Manager, to receive SNMP v3 traps from storage systems, you need to register the user who receives SNMP traps.

Before you begin

- Log in as a user with Administrator permissions (for Windows) or as a root user (for Linux).
- Check the following information:
  - The user account that is to be used for authentication with Device Manager when the `hdvmsnmpuser` command is executed.
    Check the ID and password of the Device Manager user for which `All Resources` is assigned and `Admin` is set as the Device Manager role.

Procedure

On the Device Manager server, execute the `hdvmsnmpuser` command.

Note that you do not need to restart the Device Manager server to make the settings that were specified by using the `hdvmsnmpuser` command valid.

Related references

- Format of the command for managing the user who receives SNMP traps (hdvmsnmpuser) (SNMP v3) on page 409

Format of the command for managing the user who receives SNMP traps (hdvmsnmpuser) (SNMP v3)

To set information about the user who receives SNMP traps, execute the `hdvmsnmpuser` command.

You can use the `hdvmsnmpuser` command to register, change, delete, and obtain user information.

Command format

When registering the user information:

`hdvmsnmpuser -u` *Device-Manager-user-ID* `-p` *Device-Manager-password* `add --user_name` *user-name-who-receives-SNMP-traps* `--security_level` *security-level* `[--auth_protocol` *authentication-*

protocol --auth_password *authentication-password* [--encrypt_protocol *encryption-protocol* --encrypt_key *encryption-key*]]

When changing the user information:

hdvmsnmpuser -u *Device-Manager-user-ID* -p *Device-Manager-password* modify --user_name *user-name-who-receives-SNMP-traps* [--security_level *security-level*] [--auth_protocol *authentication-protocol*] [--auth_password *authentication-password*] [--encrypt_protocol *encryption-protocol* --encrypt_key *encryption-key*]

When deleting the user information:

hdvmsnmpuser -u *Device-Manager-user-ID* -p *Device-Manager-password* delete --user_name *user-name-who-receives-SNMP-traps*

When obtaining the user information:

hdvmsnmpuser -u *Device-Manager-user-ID* -p *Device-Manager-password* get [--user_name *user-name-who-receives-SNMP-traps*]

Location of the command

In Windows:

installation-folder-for-Hitachi-Command-Suite\DeviceManager\HiCommandServer\tools\hdvmsnmpuser.bat

In Linux:

*installation-directory-for-Hitachi-Command-Suite/*HiCommandServer/tools/hdvmsnmpuser.sh

Options

You can use the following characters for the name of the user who receives SNMP traps, the authentication password, and the encryption key:

A-Z a-z 0-9 spaces single-byte symbols

The following symbols cannot be used:

\ , / : ; * ? " < > | & % ^

The characters are case-sensitive. Do not specify a space at the beginning or end of the character string.

-u *Device-Manager-user-ID*, -p *Device-Manager-password*

Specify the user ID and password of Device Manager.

--user_name *user-name-who-receives-SNMP-traps*

Specify the user name who will receive SNMP traps. The maximum number of characters that can be specified is 32 characters.

If you obtain user information, information about the user who receives SNMP traps and who is specified for this option is output. If you omit this option, information about all users who receive SNMP traps and who are registered in the Device Manager server is output.

--security_level *security-level*

Specify the security level. The following values can be specified:

`authPriv` (authentication and encryption)

`authNoPriv` (authentication but no encryption)

`noAuthNoPriv` (no authentication and no encryption)

--auth_protocol *authentication-protocol*

Specify `SHA` or `MD5` as the protocol to be used for authentication.

Specify this option when setting `authPriv` or `authNoPriv` to `--security_level` .

--auth_password *authentication-password*

Specify the password for authentication. For VSP G1000, G1500, or VSP F1500, specify a password that consists of 8 to 180 characters.For VSP Gx00 models or VSP Fx00 models, specify a password that consists of 8 to 64 characters.

Specify this option when setting `authPriv` or `authNoPriv` to `--security_level` .

--encrypt_protocol *encryption-protocol*

Specify `AES` or `DES` as the encryption protocol to be used during communication.

Specify this option when setting `authPriv` to `--security_level` .

--encrypt_key *encryption-key*

Specify the key for restoring the encrypted information. For VSP G1000, G1500, or VSP F1500, specify a key that consists of 8 to 180 characters. For VSP Gx00 models or VSP Fx00 models, specify a key that consists of 8 to 64 characters.

Specify this option when setting `authPriv` to `--security_level` .

In addition, this option must be specified when `--encrypt_protocol` is set.

Operation flow for reporting alerts by email

When an alert is issued, the alert can be automatically reported to users by email. This enables users to be aware of failures that have occurred in storage systems or file servers without logging in to the management client.

The settings required for sending alerts to users by email are described below.

Procedure

1. Setting up the SMTP server

   Set the SMTP server so that the Device Manager server can connect to the SMTP server. Follow the procedure for setting the SMTP server to be used.
2. Setting up recipients of email alerts

   Use the Device Manager GUI to set up user accounts that receive email messages.
3. Setting properties for reporting alerts

   Set the SMTP server information and the email address from which alerts are reported as properties of the Device Manager server.
4. Registering an SMTP authentication user account (when SMTP authentication is used)

   Register an SMTP authentication user account in the Device Manager server. If an SMTP authentication user account has already been registered due to event notification or notification of the health check results, you do not have to register it again.
5. Customizing email alert template (optional)

   Edit the template file as necessary, and set the email output contents.

Note:

- Device Manager sends email only once when an alert is issued. If the Device Manager server fails to send an email, the same email will not be sent again. Information on an alert and email address of the intended destination of this email, are output to the Device Manager trace log file.
- If the Device Manager server service stops before the Device Manager server sends an email about an alert, the email will not be sent. In this case, even if the Device Manager server service is started again, the Device Manager server will not send the email that has not been sent. After the Device Manager server service is started again, execute the `GetAlerts` command from the CLI or use the alert management function from the GUI, to make sure that actions have been taken for every alert.

- When you create environments or perform maintenance on storage systems or file servers that have already been registered in the Device Manager server, the storage systems or file servers might generate a lot of alerts. We recommend that you disable the email notification function beforehand by specifying `false` for the `server.mail.enabled.storagesystem` property or `server.mail.enabled.fileserver` property of the Device Manager server.

Related tasks

- Changing Device Manager server properties on page 590

Related references

- server.mail.enabled.storagesystem on page 598
- server.mail.enabled.fileserver on page 598

Setting up the SMTP server

Set up your SMTP server so that the Device Manager can connect to it.

Make sure that you specify the authentication methods in the SMTP server that you use. The Device Manager server supports the following SMTP authentication methods: LOGIN or PLAIN.

Note:

- When there are multiple SMTP authentication methods that the SMTP server specifies, the Device Manager server selects an authentication method (LOGIN or PLAIN in that priority order), and then sends an email. If LOGIN or PLAIN is not specified, the Device Manager server will send an email without using the SMTP authentication.
- If SMTP authentication is disabled on the SMTP server, even if the setting is enabled on the Device Manager server, the Device Manager server will send an email without using SMTP authentication.

Setting up recipients of email alerts

Use the Device Manager GUI to set up user accounts that receive email messages.

The conditions required for email destination users are shown below. Emails with the same contents are sent to the users who meet these conditions.

- The resource groups that correspond to the resources to be managed are assigned.
- `Modify` is set as the role in Device Manager for the assigned resource group.
- An email address is registered in the profile for the user.

This setting is necessary if user accounts have been registered in Hitachi Command Suite products. If user accounts are managed by an external authorization server, register, on the external authorization server, the user email addresses to be notified.
For details on how to set up user accounts in the Device Manager GUI, see the *Hitachi Command Suite User Guide*.

Tip: The users who receive emails need to use email software that supports Unicode (UTF-8) encoding because, when sending an email, the Device Manager server sets the character encoding of the email to Unicode (UTF-8).

Property settings for reporting alerts

To report alerts by email, the SMTP server information and the email address from which alerts are reported must be set for the properties in the `server.properties` file of the Device Manager server.

The following properties must be set:

- `server.mail.enabled.storagesystem`
- `server.mail.enabled.fileserver`
- `server.mail.from`
- `server.mail.smtp.host`
- `server.mail.smtp.port`
- `server.mail.smtp.auth`
- `server.mail.errorsTo`
- `server.eventNotification.mail.to`
- `server.mail.alert.type.storagesystem`
- `server.mail.alert.status`

Related tasks

- Changing Device Manager server properties on page 590

Related references

- server.mail.enabled.storagesystem on page 598
- server.mail.enabled.fileserver on page 598
- server.mail.from on page 599
- server.mail.smtp.host on page 599
- server.mail.smtp.port on page 599
- server.mail.smtp.auth on page 599
- server.mail.errorsTo on page 600
- server.eventNotification.mail.to on page 600
- server.mail.alert.type.storagesystem on page 600
- server.mail.alert.status on page 600

Registering an SMTP authentication user account in Device Manager

If SMTP authentication is enabled, use the `hdvmmodmailuser` command to register an SMTP authentication user account in Device Manager. If an SMTP authentication user has already been set for event notification or health check results email notification, then these settings are not required here.

Caution:

- If SMTP authentication is enabled on the Device Manager server, but an SMTP authentication user is not registered, email will be sent without using SMTP authentication.
- Only one SMTP authentication user can be set on the Device Manager server. The set SMTP authentication user information will be updated each time you execute the command.
- You cannot delete the SMTP authentication user information that you set on the Device Manager server.

Before you begin

- Log in as a user with Administrator permissions (for Windows) or as a root user (for Linux).
- Set the `server.mail.smtp.auth` property of the Device Manager server Specify `true`.
- Check the following information:
  - User ID and password for which `All Resources` has been assigned as a resource group and `Admin` has been set as the role in Device Manager.
  - User ID and password used for SMTP authentication.

Procedure

1. Execute the following command.

   In Windows:

   installation-folder-for-Hitachi-Command-Suite\DeviceManager\HiCommandServer\tools\hdvmmodmailuser.bat -u *Device-Manager-user-ID* -p *Device-Manager-password* *SMTP-authentication-user-ID* [*SMTP-authentication-password*]

   In Linux:

   installation-directory-for-Hitachi-Command-Suite/HiCommandServer/tools/hdvmmodmailuser.sh -u *Device-*

Manager-user-ID -p *Device-Manager-password SMTP-authentication-user-ID* [*SMTP-authentication-password*]

2. Restart the Hitachi Command Suite product services.

Related tasks

- Starting the Hitachi Command Suite services on page 458
- Stopping the Hitachi Command Suite services on page 460
- Changing Device Manager server properties on page 590

Related references

- server.mail.smtp.auth on page 599

Customizing email alert template

Email contents can be changed in the template file (`mail-alert-detection.txt`). After changing the template file, restart the Hitachi Command Suite product services.

Operations to complete in advance

Log in as a user with Administrator permissions (for Windows) or as a root user (for Linux).

Use a text editor to edit the template file (`mail-alert-detection.txt`) stored in the following location:

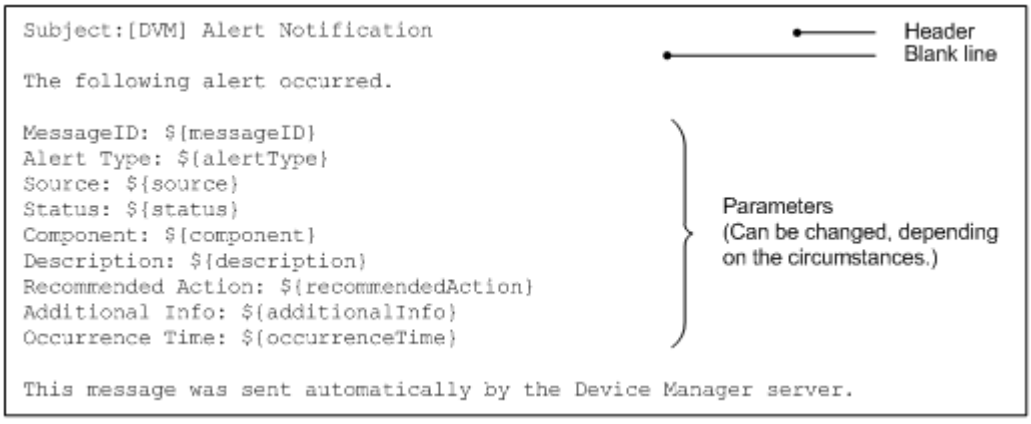
In Windows:

installation-folder-for-Hitachi-Command-Suite\DeviceManager\HiCommandServer\config

In Linux:

installation-directory-for-Hitachi-Command-Suite/HiCommandServer/config

The following shows the settings of the default `mail-alert-detection.txt` file:



Specify the `mail-alert-detection.txt` file so that all of the conditions below are satisfied. If at least one condition is not satisfied, the Device Manager server will create an email by using the default settings.

- Do not change the file name and location.
- Specify a header in the first line, nothing in the second line, and the email body and parameters in the third and following lines.
- Specify a header in the format `Subject: email-title`.
- Specify parameters in the format `${parameter-name}`.
  The parameter name is case sensitive.
- Use UTF-8 encoding to code.
- The file size must not exceed 64 KB.
- The length of each line must not exceed 1024 bytes, excluding linefeed characters.

Note: Do not apply the byte order mark (BOM) when saving the `mail-alert-detection.txt` file.

If the byte order mark (BOM) is applied to the `mail-alert-detection.txt` file, error message KAIC18797-E is output and sending of the email will fail.

The following table shows the specifiable parameters:

Table 63 Parameters you can set in the mail-alert-detection.txt file

Parameter name	Description
messageID	Alert ID
alertType	Alert type
source	Alert source For storage systems or NAS modules, the storage system name For file server, the cluster name or node name
status	Alert severity
component	Component on which the problem occurred For storage systems or NAS modules, the storage system component where the alert occurred For file server, `File Controller`
description	Alert description
recommendedAction	Action to be taken for the alert
additionalInfo	Supplementary information
occurrenceTime	For storage systems, the time at which the Device Manager server acquired alert information

Parameter name	Description
	For file server or NAS module, the time at which the alert occurred Display format: *yyyy/mm/dd hh:mm:ss* *hh* is displayed by using 24-hour display.

Related tasks

- Starting the Hitachi Command Suite services on page 458
- Stopping the Hitachi Command Suite services on page 460

Sending SNMP traps to log files

Device Manager receives SNMP traps issued by devices on the network and outputs them to log files. SNMP traps (SNMP v1 and SNMP v3 only) issued by devices that are not management targets can also be output to log files, as well as SNMP traps issued by the management-target storage systems.

Received SNMP traps are output to the following files:

- Event log or `syslog`
- Hitachi Command Suite common trace log files (`hntr2n.log`)
- Device Manager trace log files (`HDvMtracen.log`)
- Trace log files (`trace.log`)
- Error log files (`error.log`)#

#:

Output only if the severity level is `Error`, `Critical`, or `Alert`. The severity levels for SNMP traps are specified for the `customizedsnmptrap.customizelist` property in the `customizedsnmptrap.properties` file.

The following SNMP trap information is output:

- Message ID indicating that a trap was received (prefix: KAID)
- Sender (`agent`)
- Enterprise ID (`enterprise`)
- Generic trap number (`generic`)
- Specific trap number (`specific`)

If integrated management software is linked with, you can centrally monitor the operational status of all network resources, including the storage resources managed by Device Manager.

Related concepts

- Setting up Device Manager to output SNMP traps on page 419

Related tasks

- Changing Device Manager server properties on page 590

Related references

- customizedsnmptrap.customizelist on page 621

Setting up Device Manager to output SNMP traps

To set up Device Manager to receive SNMP traps and output them to log files, the following settings must be specified:

- Settings required for Device Manager to receive SNMP traps#
  - Device Manager must be able to use port `162/udp` of the management server.
  - Specify `true` for the `server.dispatcher.daemon.receiveTrap` property.
  - When using SNMP v3, the authentication information about the user who receives SNMP traps must be registered and encryption settings must be specified by using the `hdvmsnmpuser` command.
- Settings required to report SNMP traps to Device Manager#
  - The management server information must be registered in SNMP related software as the target for trap notification.
    For example, to receive storage system SNMP traps, SNMP Agent settings must be specified.
  - When using SNMP v3, the authentication information about the user who receives SNMP traps must be registered and encryption settings must be specified from an SNMP Agent.
    Specify the same settings as the management server. For details about how to register and specify encryption settings for the authentication information, see the *Hitachi SNMP Agent User Guide*.
- Settings required to output received SNMP traps to log files
  - Specify `true` for the `customizedsnmptrap.customizedSNMPTrapEnable` property.
  - The output contents must be set in the `customizedsnmptrap.customizelist` property.

#: These settings are the same as the settings required to display SNMP traps in Device Manager GUI/CLI as alerts.

When communicating between Device Manager and a storage system or file server in SNMP v1 or SNMP v2c, when the above settings are finished, the Device Manager server receives the SNMP traps of all communities and outputs them to log files.

When communicating between Device Manager and a storage system in SNMP v3, the Device Manager server receives all SNMP traps and outputs them to log files based on the authentication information set for the user who receives SNMP traps.

Related tasks

- Registering the user who receives SNMP traps (SNMP v3) on page 409
- Changing Device Manager server properties on page 590

Related references

- server.dispatcher.daemon.receiveTrap on page 607
- customizedsnmptrap.customizedSNMPTrapEnable on page 621
- customizedsnmptrap.customizelist on page 621

Settings required to use Device Manager event notification

Device Manager GUI uses email to report to users the results of all events with some exceptions.

However, notifications for the following HCS tasks are not sent by email:

- Editing of the template for an HDT pool monitoring schedule
- Deletion of the template for an HDT pool monitoring schedule

If you enable email notifications when creating a Device Manager GUI task, the execution results are sent to the following address:

- Email address that was set when the Device Manager GUI task was created
- Email address that is set in the `server.eventNotification.mail.to` property in the Device Manager server `server.properties` file

To send event notifications by email, you need to specify the settings below. If the settings required for sending alerts by email have already been specified, the settings in 1 to 4 are not required.

Procedure

1. Setting up the SMTP server

   Set up the SMTP server so that the Device Manager server can connect to the SMTP server.
2. Setting up recipients of email notifications (optional)

   If the email address of the logged in user is registered, the email address is automatically input when the user creates a task by using the Device Manager GUI.
3. Setting properties for event notification

   Set the SMTP server information and the email address from which events are reported as properties of the Device Manager server.
4. Setting up an SMTP authentication user

To use SMTP authentication for connection, you need to set up an authentication user account in the Device Manager server by using the `hdvmmodmailuser` command.

5. Editing the event notification template (optional)

   The content of email messages sent to users as event notifications are set in the template file. Edit the template file as necessary.

Related tasks

- Setting properties for Device Manager event notification on page 421
- Specifying SMTP user authentication information for event notification (hdvmmodmailuser command) on page 422
- Editing the event notification template for Device Manager on page 423

Related references

- Setting up the SMTP server on page 413
- Setting up recipients of email alerts on page 413
- server.eventNotification.mail.to on page 600

Setting properties for Device Manager event notification

By setting information such as SMTP server information and a notification-source email address for the following properties in the Device Manager server `server.properties` file, the execution results for events related to Device Manager can be sent by email:

- `server.mail.enabled.storagesystem`
- `server.mail.from`
- `server.mail.smtp.host`
- `server.mail.smtp.port`
- `server.mail.smtp.auth`
- `server.mail.errorsTo`
- `server.eventNotification.mail.to`

Related references

- server.mail.enabled.storagesystem on page 598
- server.mail.from on page 599
- server.mail.smtp.host on page 599
- server.mail.smtp.port on page 599
- server.mail.smtp.auth on page 599
- server.mail.errorsTo on page 600
- server.eventNotification.mail.to on page 600

Specifying SMTP user authentication information for event notification (hdvmmodmailuser command)

The event notification functionality establishes a connection with the SMTP server. To use SMTP authentication for the connection, an SMTP authentication user account must be set up in the Device Manager server by using the `hdvmmodmailuser` command.

The SMTP authentication user settings set by the `hdvmmodmailuser` command are also used for alert email notification and health check results email notification. If an SMTP authentication user has already been set for alert email notification or health check results email notification, then these settings are not required here.

The following is the syntax of the `hdvmmodmailuser` command:

Format

In Windows:

installation-folder-for-Hitachi-Command-Suite\DeviceManager\HiCommandServer\tools\hdvmmodmailuser.bat -u *Device-Manager-user-ID* -p *Device-Manager-password SMTP-authentication-user-ID* [*SMTP-authentication-password*]

In Linux:

*installation-directory-for-Hitachi-Command-Suite/*HiCommandServer/tools/hdvmmodmailuser.sh -u *Device-Manager-user-ID* -p *Device-Manager-password SMTP-authentication-user-ID* [*SMTP-authentication-password*]

Options

-u *Device-Manager-user-ID*

Specify the ID of a user for which `All Resources` has been assigned as a resource group and `Admin` has been set as the role in Device Manager.

-p *Device-Manager-password*

Specify the password used to log in to Device Manager by the user *Device-Manager-user-ID* specified using the `-u` option.

SMTP-authentication-user-ID

Specify a user ID used for SMTP authentication.

SMTP-authentication-password

Specify a logon password for the user ID used to log on to the SMTP server.

Caution:

- If SMTP authentication is enabled on the Device Manager server, but an SMTP authentication user is not registered, email will be sent without using SMTP authentication.
- Only one SMTP authentication user can be set on the Device Manager server. The set SMTP authentication user information will be updated each time you execute the command.
- You cannot delete the SMTP authentication user information that you set on the Device Manager server.

To enable the settings set by the `hdvmmodmailuser` command, after the `hdvmmodmailuser` command finishes executing, restart the Hitachi Command Suite product services.

Related tasks

- Starting the Hitachi Command Suite services on page 458
- Stopping the Hitachi Command Suite services on page 460

Editing the event notification template for Device Manager

The content of emails sent to users as event notifications are set in template files. You can edit the template files to customize the contents of emails as necessary and set which items to send notifications out for.

The template file is stored in the following location:

In Windows:

installation-folder-for-Hitachi-Command-Suite\DeviceManager\HiCommandServer\config\mail-taskStatusNotification.txt

In Linux:

installation-directory-for-Hitachi-Command-Suite/HiCommandServer/config/mail-taskStatusNotification.txt

Tip: To reset the template file to the setting of when a new installation was performed, use the template stored in the following location:

In Windows:

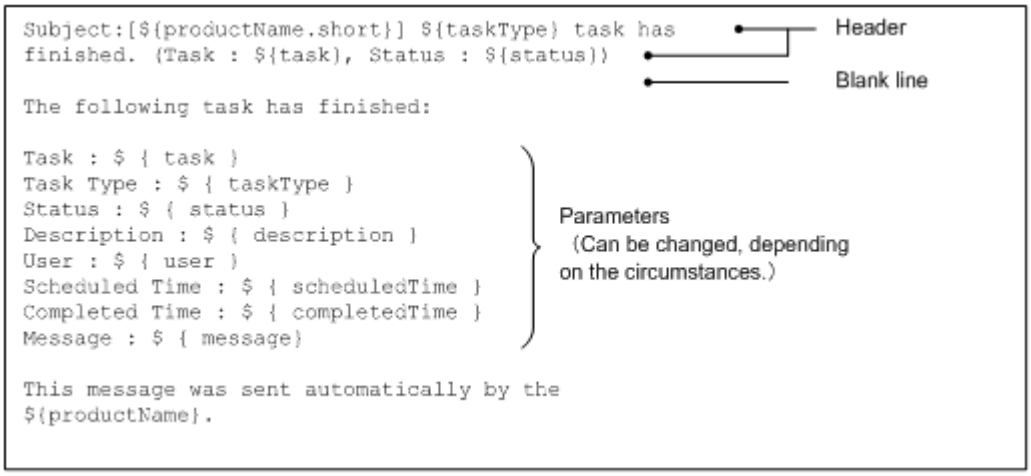
installation-folder-for-Hitachi-Command-Suite\DeviceManager\HiCommandServer\template\mail-taskStatusNotification.txt

In Linux:

installation-directory-for-Hitachi-Command-Suite/HiCommandServer/template/mail-taskStatusNotification.txt

By specifying parameters in the template file, you can add event information to email notifications.

The following shows an example of writing the template file (`mail-taskStatusNotification.txt`):



Set up template files using the following format:

- Specify a header in the first line, nothing in the second line, and the email body in the third and following lines.
- Specify a header in the format `Subject: email-title`.
- Specify parameters in the format `${parameter-name}`.
- 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 1024 bytes, excluding linefeed characters.

Note: Do not apply the byte order mark (BOM) when saving the template file.

If the byte order mark (BOM) is applied to the template file, error message KAIC18797-E is output and sending of the email will fail.

The following table shows the parameters that can be set in the template file:

Table 64 Parameters for events that occur when tasks end

Parameter	Description	Header	Contents
`task`	Task name	Y	Y
`taskType`	Task type	Y	Y
`status`	Task status	Y	Y

Parameter	Description	Header	Contents
description	Task description	--	Y
user	The user ID of the user who created the task.	--	Y
scheduledTime	Time the task execution was requested	--	Y
completedTime	Time the task execution ended	--	Y
message	Error message	--	Y
productName	Product name	--	Y
productName.short	Product name (abbreviation)	Y	Y

Legend:

Y: Can be specified

--: Cannot be specified

Settings required to use Tiered Storage Manager event notification

Tiered Storage Manager uses email to report to users the results of events that are not directly the result of user actions, such as the end of migration and shredding tasks.

The following events can be reported by email:

Table 65 Tiered Storage Manager events that can be reported via email

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 created via the Tiered Storage Manager CLI ends successfully, ends due to a failure, or is canceled.
Locking task ended	This event occurs when a locking task created via the Tiered Storage Manager CLI ends successfully, ends due to a failure, or is canceled.
Unlocking task ended	This event occurs when an unlocking task created via the Tiered Storage Manager CLI 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 created via the Tiered Storage Manager CLI.
Specified time elapsed	This event occurs when a period specified by a user for a migration group created via the Tiered Storage

Event	Description
	Manager CLI has elapsed (the period is a specified number of days).

The range of events to be reported varies depending on how the notification-destination email addresses are set, as follows:

- Setting when creating tasks
  If you set a notification-destination email address when creating tasks such as migration and shredding, the results of the tasks are reported to the user.
- Setting in the `server.properties` files of Device Manager and Tiered Storage Manager
  If an email address is set for the `server.eventNotification.mail.to` property in the `server.properties` file, the results of all events related to Tiered Storage Manager are reported to the user.
- Setting when creating migration groups
  If an email address is set when creating a migration group by using the Tiered Storage Manager CLI, the results of all events are reported to the user.

The settings work independently. For example, if the email address set in the `server.properties` file, and the email address set when creating migration tasks are the same, an email is sent two times when a migration task is completed.

To report events by email, you need to specify the settings below. If the settings required for sending alerts by email have already been specified, the settings in 1 and 2 are not required.

Procedure

1. Setting up the SMTP server

   Set up the SMTP server so that the Device Manager server can connect to the SMTP server.
2. Setting up recipients of email notifications (optional)

   If the email address of the logged in user is registered, the email address is automatically entered when the user creates a task by using the Device Manager GUI.
3. Setting properties for event notification

   Set the SMTP server information and the email address from which events are reported as properties of the Device Manager server and the Tiered Storage Manager server.
4. Setting up an SMTP authentication user

To use SMTP authentication for connection, you need to set up an authentication user account.

The command to be used varies depending on the task type. For tasks executed from the Device Manager GUI, use the `hdvmmodmailuser` command. For tasks executed from the Tiered Storage Manager CLI, use the `htsmmodmailuser` command.

5. Editing the event notification template (optional)

   The content of email messages sent to users as event notifications are set in template files. Edit the template files as necessary.

Related tasks

- Specifying SMTP user authentication information for event notification (hdvmmodmailuser command) on page 422
- Setting properties for Tiered Storage Manager event notification on page 427
- Specifying SMTP user authentication information for event notification (htsmmodmailuser command) on page 428
- Editing event notification templates for Tiered Storage Manager on page 430

Related references

- Setting up the SMTP server on page 413
- Setting up recipients of email alerts on page 413
- server.eventNotification.mail.to on page 646

Setting properties for Tiered Storage Manager event notification

By setting information such as SMTP server information and a notification-source email address for the following properties in the Device Manager server `server.properties` file, the execution results for events related to Tiered Storage Manager can be sent via email.

- `server.mail.enabled.storagesystem`
- `server.mail.from`
- `server.mail.smtp.host`
- `server.mail.smtp.port`
- `server.mail.smtp.auth`
- `server.mail.errorsTo`
- `server.eventNotification.mail.to`

Tip: To send notifications about executed tasks via the Tiered Storage Manager CLI, the following properties in the Tiered Storage Manager server `server.properties` file must be set:

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

Related references

- server.mail.enabled.storagesystem on page 598
- server.mail.from on page 599
- server.mail.smtp.host on page 599
- server.mail.smtp.port on page 599
- server.mail.smtp.auth on page 599
- server.mail.errorsTo on page 600
- server.eventNotification.mail.to on page 600
- server.mail.from on page 645
- server.mail.smtp.host on page 645
- server.mail.smtp.port on page 646
- server.mail.smtp.auth on page 646
- server.mail.errorsTo on page 645
- server.eventNotification.mail.to on page 646
- server.eventMonitoringIntervalInMinute on page 646

Specifying SMTP user authentication information for event notification (htsmmodmailuser command)

To use the event notification functionality for executed tasks via the Tiered Storage Manager CLI, an SMTP authentication user account must be set up on the Tiered Storage Manager server by using the `htsmmodmailuser` command.

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

In Windows:

installation-folder-for-Hitachi-Command-Suite
\TieredStorageManager\bin

In Linux:

*installation-directory-for-Hitachi-Command-Suite/*TieredStorageManager/bin

The following shows the syntax of the htsmmodmailuser command:

Format

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

Options

-u *Tiered-Storage-Manager-user-ID*

Specify the ID of a user for whom All Resources has been assigned as a Device Manager resource group and who has Admin permission for Tiered Storage Manager.

-p *Tiered-Storage-Manager-password*

Specify a logon password for the user ID used to log on to Tiered Storage Manager via the u option.

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.

To enable the settings set by the htsmmodmailuser command, after the htsmmodmailuser command finishes executing, restart the Hitachi Command Suite product services

---

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 Linux.
- The command exceeds 256 bytes.

Related tasks

- Starting the Hitachi Command Suite services on page 458
- Stopping the Hitachi Command Suite services on page 460

Editing event notification templates for Tiered Storage Manager

The content of emails sent to users as event notifications are set in template files. You can edit the template files to customize the contents of emails as necessary and set which items to send notifications out for.

A template file is provided for each event. The following table lists the template files and the events they are used for.

Table 66 Template files for event notification email

Type	Event	Template file
Task ended	Migration task ended	• For migration tasks created by using the Migrate data wizard[#1] In Windows: *installation-folder-for-Hitachi-Command-Suite*\DeviceManager\HiCommandServer\config\mail-migrationtask-end.txt In Linux: *installation-directory-for-Hitachi-Command-Suite*/HiCommandServer/config/mail-migrationtask-end.txt • For migration tasks created by using the Tiered Storage Manager CLI[#2] In Windows: *installation-folder-for-Hitachi-Command-Suite*\TieredStorageManager\conf\mail-migrationtask-end.txt In Linux: *installation-directory-for-Hitachi-Command-Suite*/TieredStorageManager/conf/mail-migrationtask-end.txt
	Shredding task ended[#2]	• In Windows: *installation-folder-for-Hitachi-Command-Suite*\TieredStorageManager\conf\mail-shreddingtask-end.txt • In Linux: *installation-directory-for-Hitachi-Command-Suite*/TieredStorageManager/conf/mail-shreddingtask-end.txt
	Locking task ended[#2]	• In Windows: *installation-folder-for-Hitachi-Command-Suite*\TieredStorageManager\conf\mail-lockingtask-end.txt • In Linux: *installation-directory-for-Hitachi-Command-Suite*/TieredStorageManager/conf/mail-lockingtask-end.txt
	Unlocking task ended[#2]	• In Windows: *installation-folder-for-Hitachi-Command-Suite*\TieredStorageManager\conf\mail-unlockingtask-end.txt

Type	Event	Template file
		• In Linux: *installation-directory-for-Hitachi-Command-Suite*/TieredStorageManager/conf/mail-unlockingtask-end.txt
Time lapse	Volume lock period expired#2	• In Windows: *installation-folder-for-Hitachi-Command-Suite*\TieredStorageManager\conf\mail-retention-term-expired.txt • In Linux: *installation-directory-for-Hitachi-Command-Suite*/TieredStorageManager/conf/mail-retention-term-expired.txt
	Specified time elapsed#2	• In Windows: *installation-folder-for-Hitachi-Command-Suite*\TieredStorageManager\conf\mail-migrationgroup-reminder.txt • In Linux: *installation-directory-for-Hitachi-Command-Suite*/TieredStorageManager/conf/mail-migrationgroup-reminder.txt

#1:

The template files are stored in the following locations:

- In Windows:
  installation-folder-for-Hitachi-Command-Suite\DeviceManager\HiCommandServer\template
- In Linux:
  installation-directory-for-Hitachi-Command-Suite/HiCommandServer/template

#2:

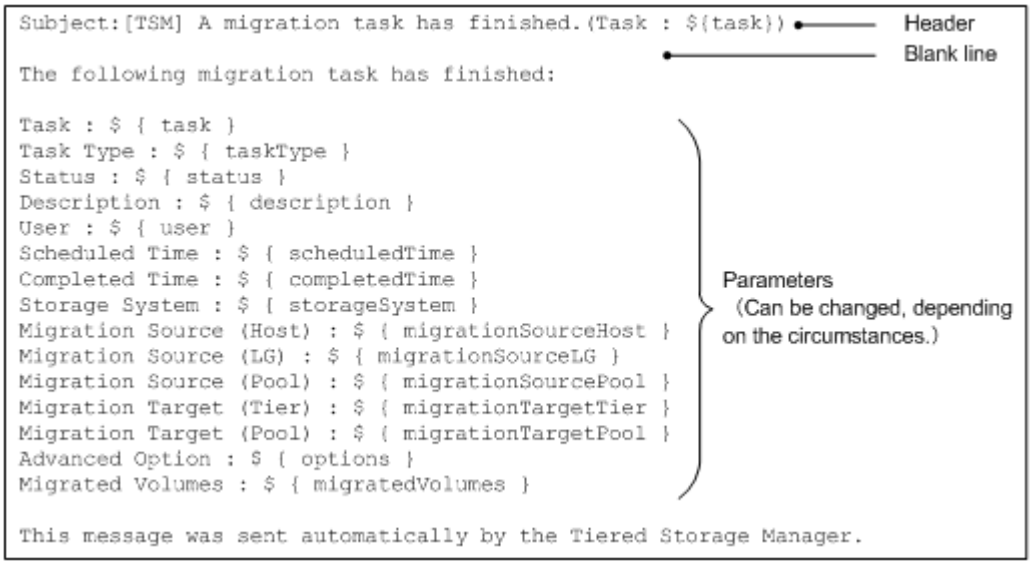
The template files are stored in the following locations:

- In Windows:
  installation-folder-for-Hitachi-Command-Suite\TieredStorageManager\template
- In Linux:
  installation-directory-for-Hitachi-Command-Suite/TieredStorageManager/template

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. For details about the parameters of each event, see the *Hitachi Command Suite Tiered Storage Manager CLI Reference Guide*.

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



Set up template files using the following format:

- Specify a header in the first line, nothing in the second line, and the email body in the third and following lines.
- Specify a header in the format `Subject: email-title`.
- Specify parameters in the format `${parameter-name}`.
- 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 1024 bytes, excluding linefeed characters.

Note:

- Do not apply the byte order mark (BOM) when saving the template file. If the byte order mark (BOM) is applied to the template file, error message KAIC18797-E is output and sending of the email will fail.
- To apply changes to the template file, restart the Hitachi Command Suite product services.

The parameters that can be specified in a template depend on the events. The parameters are listed in the following table.

Table 67 Parameters for events that occur when tasks end (migration tasks created via the Migrate data wizard)

Parameter	Description
task	Task name
taskType	Task type
status	Task status
description	Task description
user	The user ID of the user who created the task.
scheduledTime	Time the task execution was requested
completedTime	Time the task execution ended
storageSystem	Storage system name
migrationSourceHost	Migration source: Host
migrationSourceLG	Migration source: Logical Group
migrationSourcePool	Migration source: Pool
migrationTargetTier	Migration target: Tier
migrationTargetPool	Migration target: Pool
options	Options
migratedVolumes	Volume ID of the migrated volume

Table 68 Parameters for events that occur when tasks end (tasks created via the Tiered Storage Manager CLI)

Parameter	Description
taskId	Task ID
taskType	Task type
taskStatus	Task status
taskOwner	The user ID of the user who created the task.
executionRequestTime	Time that task execution was requested
endTime	Time that task execution ended
storageDomainName	Storage domain name
migrationGroupName	Migration group name
previousTargetStorageTierName	Name of the target storage tier in the previous migration
targetStorageTierName	Name of the target storage tier
eraseData	Whether data after migration is to be deleted
migratedVolumes	Device numbers of both migrated volumes and volumes whose data has been erased
shreddingMethod	Shredding method
shreddedVolumes	Device numbers of shredded volumes
guardMode	Lock mode

Parameter	Description
retentionDays	Retention period (days)
lockedVolumes	Device numbers of locked volumes
unlockedVolumes	Device numbers of unlocked volumes
moveToMigrationGroupName	Name of the target migration group after task completion

Table 69 Parameters for time-lapse events

Parameter	Description
storageDomainName	Storage domain name
migrationGroupName	Migration group name
expiredVolumes	Device numbers of expired volumes
remindAt	Scheduled time when an "elapsed time" event will occur
reminderDescription	Message that appears when an "elapsed time" event occurs

Related tasks

- Starting the Hitachi Command Suite services on page 458
- Stopping the Hitachi Command Suite services on page 460

8

Configuring Device Manager for CIM/WBEM

This chapter explains how to configure Device Manager for CIM/WBEM .

- About CIM/WBEM
- CIM/WBEM functions in Device Manager
- Specifying a namespace
- User account settings for using the CIM/WBEM functions
- Specifying the settings for using the CIM/WBEM functions
- Settings for acquiring storage system performance information by using CIM/WBEM functions
- Controlling the SLP service

About CIM/WBEM

Device Manager supports CIM and WBEM, which have been defined by the DMTF standards group. CIM is a method of managing systems in a network environment. WBEM is a standard for managing network devices, such as hosts and storage systems, over the Internet.

The CIM model that Device Manager uses complies with the SMI-S specifications advocated by SNIA, and is compatible with SNIA-CTP. CIM/WBEM functions can be used to manage the configuration and status of storage systems in a standardized manner that is independent of vendor, OS, protocol, and other environmental factors.

The CIM models of the Device Manager server are defined in MOF files provided by Device Manager.

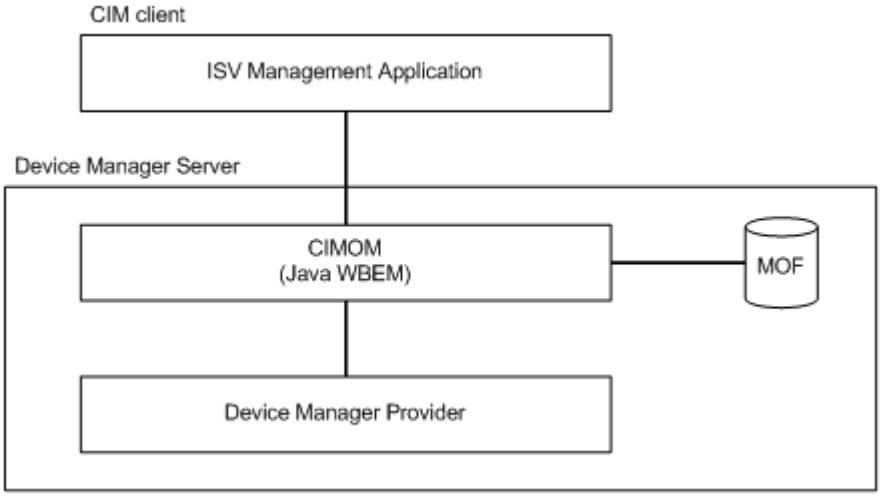


Figure 59 CIM components for Device Manager

You can acquire information about CIM at:

http://www.dmtf.org/

You can acquire information about SMI-S at:

http://www.snia.org/

CIM/WBEM functions in Device Manager

The CIM/WBEM functions in Device Manager provide the following functions that come standard in SMI-S:

Object operation function

The SMI-S specifications, which Device Manager conforms to, define the interfaces for devices that make up a storage network, such as storage

systems, virtual storage systems, switches, and hosts. The functions that need to be provided by the management service to manage the devices are grouped in a profile for each device.

The profiles used by the CIM/WBEM functions of Device Manager are the Array profile and its subprofiles. The Array profile defines the interfaces for storage systems.

Indication function

The *indication* function is the event notification function defined by CIM. When an event occurs in a CIM server, the CIM server reports the indication instance, which shows the information about the event (such as generation or deletion of a CIM instance), to CIM clients. For a CIM client to receive indications, its location and transmission conditions for indications must be registered in the CIM server beforehand. For details on how to register them, see the SNIA website.

Device Manager reports the occurrence of the following events:

- Generation of a volume
- Deletion of a volume
- Allocation of a LUN path
- Cancellation of a LUN path

Service discovery function

Device Manager provides the service discovery function based on the Service Location Protocol (SLP).

The SLP is undergoing standardization by IETF and provides a way to discover desired services available in a network. For details on the SLP, see RFC2608.

Just by specifying the type of service, SLP clients can acquire information (such as URLs) about how to access the available services, and information about service attributes.

In Device Manager, the Device Manager server uses the SLP to report information about the WBEM Service.

Performance information acquisition function

Device Manager acquires the following types of information as storage system performance information:

- Port-related information
  Total I/O count
  Data traffic
- Volume-related information
  Total I/O count
  Data traffic

Number of read I/Os
Number of read I/Os that hit the cache
Number of write I/Os
Number of write I/Os that hit the cache

Specifying a namespace

Device Manager supports versions 1.1.0 through 1.5.0 of SMI-S. The namespace that is used to connect to Device Manager (CIM server) must be specified on CIM clients.

You can specify a namespace by using the follow format:

- Specify the SMI-S version.
  Specify `root/smis/smis`*xx* (*xx* is an abbreviation for the version number).
  For example, to specify version 1.5.0, enter `root/smis/smis15`.
  The latest namespaces that complies with the specified SMI-S version is selected.
- Specify the condition `current`.
  Enter `root/smis/current`.
  The current namespace is selected.
- Specify `interop`.
  SMI-S 1.3.0 or a later version supports the namespace `interop`. If `interop` is specified as the namespace, the Server profile that stores the current management server information is specified.
  The namespace of each vendor is accessed via this Server profile to acquire information about the Array profile and its subprofiles.
  For interop namespaces, only the queries from SMI-S version 1.3.0 or later can be set for the Query property of CIM_IndicationFilter.

Table 70 Correspondence between namespaces and SMI-S versions

Namespace			SMI-S
smis*xx*	**current**	**interop**	
smis11	--	--	1.1.0
smis12	--	--	1.2.0
smis13	--	--	1.3.0
smis14	--	--	1.4.0
smis15	current	interop	1.5.0

Legend: --: N/A

User account settings for using the CIM/WBEM functions

Note that `All Resources` must be assigned for the users who use the CIM/WBEM functions. Also note that the CIM methods that can be executed differ depending on the role in Device Manager.

Table 71 Roles in Device Manager and CIM methods that can be executed

Role in Device Manager	CIM method that can be executed	
	Service methods	CIM operations
Admin or Modify	Y	Y
View or Peer	--	Y

Legend:

Y: These CIM methods can be executed.

--: These CIM methods cannot be executed.

Specifying the settings for using the CIM/WBEM functions

When Hitachi Command Suite has been installed as a new installation, the CIM/WBEM functions are enabled. If you want to enable the CIM/WBEM functions again after having disabled them, you need to specify environment settings as described below.

Before you begin

- Log in as a user with Administrator permissions (for Windows) or as a root user (for Linux)
- Register the storage system in Device Manager.
  When registering a storage system that is to be managed, use the account of an administrator for the entire storage system. Do not use the account of an administrator who only has permissions for part of the storage system.
- Check port numbers.
  Check whether any port numbers exist that are used by both the CIM/WBEM functions of Device Manager and programs other than Device Manager. If such port numbers exist, change the port number assignments so that the CIM/WBEM functions of Device Manager use unique port numbers.
- Start the SLP service or SLP daemon (if you want to use the service discovery function).
- Set the language tag (when using the service discovery function)

When starting the CIM client, set the language tag (locale) for the service discovery function to English (`en`).

Procedure

1. On the Device Manager server, in the `server.properties` file, set the `server.cim.support` property to `true`.
2. Restart the Hitachi Command Suite product services.

   When an external storage system is connected to Virtual Storage Platform or Universal Storage Platform V/VM, if there is a large number of LDEVs managed by Device Manager, it might take time for the services to start.
3. Refresh the storage systems registered in Device Manager server via the Device Manager GUI or CLI.

Caution:

- If you delete a storage system while disabling CIM/WBEM functions, perform step 3 in the following order to restart the services.
  1. In the `server.properties` file, change the `server.logicalview.initialsynchro` property to `true`.
  2. Restart the Hitachi Command Suite product services.
  3. In the `server.properties` file, change the `server.logicalview.initialsynchro` property back to `false`.
- If you use CIM/WBEM to perform an operation for resources (such as LDEVs and parity groups) that have been reserved by the setup operation from the Device Manager GUI, the setting might be changed or the resources might be deleted.

Related concepts

- Controlling the SLP service on page 450

Related tasks

- Starting the Hitachi Command Suite services on page 458
- Stopping the Hitachi Command Suite services on page 460

Related references

- Ports used by the Device Manager server on page 107
- server.cim.support on page 596
- server.logicalview.initialsynchro on page 598

Changing CIM/WBEM port numbers

To change the port numbers used by CIM/WBEM functions, edit the relevant property files on the Device Manager server.

Before you begin

Log in as a user with Administrator permissions (for Windows) or as a root user (for Linux).

Procedure

1. Stop the services of Hitachi Command Suite product.
2. Set the port numbers by editing the following Device Manager server properties:
   - For non-SSL communication:
     `server.cim.http.port` property in the `server.properties` file and `HTTPPort` property in the `cimxmlcpa.properties` file
   - For SSL communication:
     `server.cim.https.port` property in the `server.properties` file and `HTTPSPort` property in the `cimxmlscpa.properties` file
     In the `cimxmlscpa.properties` file, make sure that you also set the `Ciphers` property.
3. Start the services of Hitachi Command Suite product.

Related tasks

- Starting the Hitachi Command Suite services on page 458
- Stopping the Hitachi Command Suite services on page 460

Related references

- server.cim.http.port on page 596
- server.cim.https.port on page 597
- Ciphers on page 620
- HTTPPort on page 639
- HTTPSPort on page 639

Settings for acquiring storage system performance information by using CIM/WBEM functions

This section describes the system configuration that is required to use the performance information acquisition function, and how to specify settings for acquiring performance information.

Required system configuration for acquiring performance information

The system configuration in which the performance information of a storage system is acquired by using the CIM/WBEM functions differs depending on the model of the storage system.

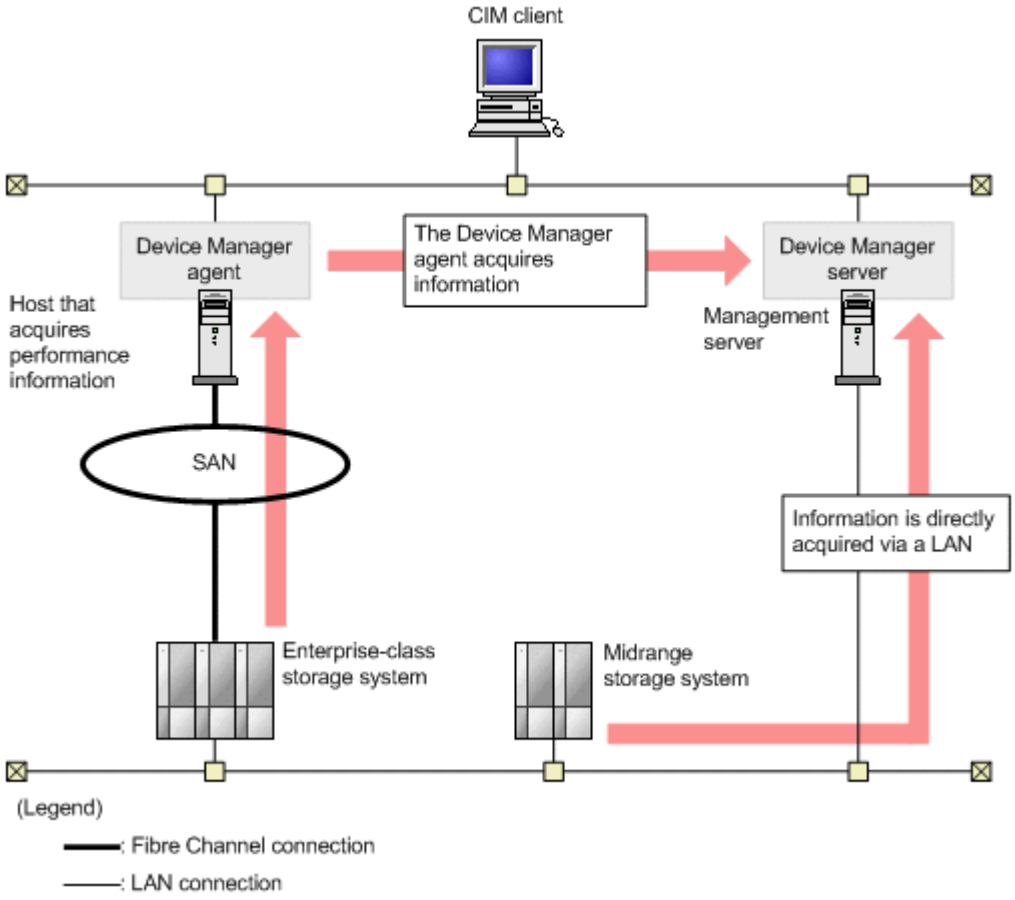


Figure 60 Example of a system configuration in which performance information of a storage system is acquired

Storage system

This is a storage system whose performance information is to be acquired.

The host that acquires performance information (the Device Manager agent) acquires the performance information about Virtual Storage Platform or Universal Storage Platform V/VM storage systems by using the command device within the storage system, and then reports it to the Device Manager server.

In midrange storage systems (HUS100, Hitachi AMS2000, Hitachi SMS, or Hitachi AMS/WMS), the Device Manager server acquires performance information directly from a storage system.

Host that acquires performance information

This host is required for acquiring performance information about Virtual Storage Platform or Universal Storage Platform V/VM storage systems. Device Manager agent version 7.0 or later is required for Virtual Storage Platform storage systems, and Device Manager agent version 5.9 or later is required for Universal Storage Platform V/VM storage systems.

We recommend that use the same computer for the management server and for the host that acquires performance information.

Even if you use different computers for the management server and for the host that acquires performance information, the OS for the host that acquires performance information must be Windows, Solaris, or Linux.

The host that acquires performance information cannot run HP-UX or AIX.

We recommend that you use the `hdvmagt_setting` command to set the Device Manager agent central management method.

Management server

Device Manager server version 5.9 or later must be installed, and the CIM/WBEM functions must be enabled.

Specifying the settings required to acquire performance information about Virtual Storage Platform or Universal Storage Platform V/VM storage systems

This section describes the settings required to acquire performance information about Virtual Storage Platform or Universal Storage Platform V/VM storage systems.

Before you begin

Log in as a user with Administrator permissions or as a root user.

Procedure

1. Prepare a command device for each storage system that is to be a target for collecting performance information.
2. Assign the command device to the host that collects the performance information, and have the hosts recognize the command devices.

   To acquire Virtual Storage Platform performance information, force hosts to recognize command devices for which authentication mode is disabled.

3. Install a Device Manager agent and CCI LIB on a host that collects performance information.

   For details on how to install a Device Manager agent, see the *Hitachi Command Suite Installation and Configuration Guide*.

   To acquire performance information, a CCI/LIB is necessary. If you install the Device Manager agent on a host, the necessary CCI/LIB is installed. However, if the host OS is UNIX, and a CCI/LIB is already installed on the host, the CCI/LIB is not overwritten. If this is the case, install the proper CCI/LIB, as shown in the following table.

Table 72 CCI/LIB required to acquire performance information

Storage system	Version
Virtual Storage Platform	01-15-03/00 or later
Universal Storage Platform V/VM	01-12-03/03 or later

4. Use the Device Manager agent `hdvmagt_setting` command to configure the central management method settings. (This is recommended.)
5. Use the `perf_findcmddev` command to register command devices.

Caution:
- If you upgrade the Device Manager agent from version 6.3 or earlier to version 6.4 or later, the settings in the `perf_cmddev.properties` file remain unchanged. If you are using a storage system in an SLPR environment, after the upgrade installation finishes, refresh the information of SLPR command devices defined in the `perf_cmddev.properties` file.
- If you are using the Device Manager agent version 6.3 or earlier and you want to use a storage system in an SLPR environment, directly edit the `perf_cmddev.properties` file to define command devices for SLPRs.

6. On the Device Manager server, in the `server.properties` file, set the `server.cim.agent` property to the host name of the host that collects performance information (the host on which the Device Manager agent is installed).

Caution: Make sure that the host name specified for the `server.cim.agent` property matches the host name registered in Device Manager for the host that acquires performance information. If these host names are different, you cannot acquire performance information.

Related tasks

- Changing Device Manager server properties on page 590

Related references

- Format of the command for registering command devices (perf_findcmddev) on page 445
- Setting the Device Manager server's information, HiScan command's execution period, and CCI's information (hdvmagt_setting command) on page 533
- server.cim.agent on page 595

Format of the command for registering command devices (perf_findcmddev)

The following shows the format of the command (`perf_findcmddev`) that registers command devices on a Device Manager agent, and displays the settings for command devices.

Format of the command

```
perf_findcmddev { write [-file file-name] | verify | view }
```

Storage directory of the command

In Windows:

installation-folder-for-the-Device-Manager-agent\bin

In Linux:

installation-directory-for-the-Device-Manager-agent/bin

In Solaris:

/opt/HDVM/HBaseAgent/bin

Options

write [-file *file-name*]

Specify this option to register command devices. This option outputs the settings of all command devices recognized by the host to the file.

You can use the `-file` *file-name* option to specify the desired file name. To specify the file name, you can use an absolute or relative path.

If you do not specify the `-file` option, the `perf_cmddev.properties` file will be overwritten.

If no command device recognized by the host is detected, nothing is output to the `perf_cmddev.properties` file.

verify

This option compares the settings for the command devices defined in the `perf_cmddev.properties` file to the settings for the command devices recognized by the host. If the host recognizes multiple command devices, the execution result is output for each.

- If the information of a command device defined in the `perf_cmddev.properties` file matches the information of the command device recognized by the host, the following message is displayed:
  `The definition of the command device is valid.`
- If the host does not recognize a command device defined in the `perf_cmddev.properties` file:
  The error message `KAIC28615-W` and information of the command device that is not recognized by the host are displayed.
- If a command device recognized by the host is not defined in the settings file:
  The error message `KAIC28616-W` and information of the command device that is not defined in the settings file are displayed.
  Note that, if the settings for a command device are defined in the `perf_cmddev.properties` file by using the format of version 6.3 or earlier, the command device is assumed to belong to SLPR0.

`view`

This parameter displays the settings for the command devices defined in the `perf_cmddev.properties` file.

In the `perf_cmddev.properties` file, `UNKNOWN` is displayed for any lines on which non-recognizable values are defined or that are not correctly formatted. Comment lines and blank lines are not displayed. In addition, if no value is specified in the `perf_cmddev.properties` file, only the header is displayed.

The following is an example of output from the command. The items that are output are the same as the items set in the `perf_cmddev.properties` file.

```
Raid ID Serial# SLPR# LDEV# Device file name
R600    14050   0     345   \\.\PhysicalDrive3
R601    44332   1     456   \\.\Volume{xxxxxxx-xxxx-xxx-
xxxxxxxx}

R600    UNKNOWN -     1045  \\.\PhysicalDrive10
```

Related references

- Format of the perf_cmddev.properties file on page 447

Format of the perf_cmddev.properties file

Edit the `perf_cmddev.properties` file to define the command device of the target storage system.

Storage directory of the perf_cmddev.properties file

In Windows:

installation-folder-for-the-Device-Manager-agent\mod\hdvm\config

In Linux:

installation-directory-for-the-Device-Manager-agent/mod/hdvm/config

In Solaris:

/opt/HDVM/HBaseAgent/mod/hdvm/config

Format of the perf_cmddev.properties file

Define one command device per line, using the following format.

When using the Device Manager agent version 6.4 or later:

RAID-ID.*serial-number*.[*SLPR-number*.]*LDEV-number*: *deviceFileName*

When using the Device Manager agent version 6.3 or earlier:

RAID-ID.*serial-number*.*LDEV-number*: *deviceFileName*

Table 73 Settings in the perf_cmddev.properties file

Setting item	Value
RAID-ID	Specify one of the following depending on the type of the target storage system: R700 for Virtual Storage Platform R600 for Universal Storage Platform V R601 for Universal Storage Platform VM
Serial-number	Specify the serial number of the storage system by using a decimal (base 10) number.
SLPR-number	Specify the number of the SLPR to which the command device belongs by using a decimal (base 10) number. If no SLPR is configured, specify 0. This item is optional. If you omit this item or define this item by using the format for version 6.3 or earlier, it is assumed that no SLPR has been configured.

Setting item	Value
LDEV-number	Specify the CU:LDEV number of the command device by using a decimal (base 10) number.

deviceFileName	Specify the command device identifier (the PhysicalDrive number, VolumeGUID, or device file name) that the host recognizes in the following format:#
	• In Windows:
	`\\.\PhysicalDrive`*X*
	`\\.\Volume{`*GUID*`}`
	• In Solaris:
	`/dev/rdsk/cxtxdxs2`
	• In Linux:
	`/dev/sd`*x*
	x is an integer.

#:

- If this item is specified using the physical drive number in Windows or Linux and you then restart the OS, the physical drive number and device file name might be changed. If this occurs, you need to execute the `perf_findcmddev` command to check and update the settings. In Windows, if you specify this item using the volume GUID, the setting is not affected even if you restart the OS.
- If you are using the Device Manager agent version 6.3 or earlier and you want to acquire performance information of all SLPRs in an SLPR environment, you need to define SLPR0 command device in the `perf_cmddev.properties` file.

  To define command devices for different SLPRs that belong to the same storage system, define the SLPR0 command device in the first line of the storage system. The following example shows how to define `PhysicalDrive5` (whose LDEV number is 345) as the SLPR0 command device of Universal Storage Platform V (whose serial number is 14050).

```
R700.44332.456: \\.\PhysicalDrive3
R600.14050.345: \\.\PhysicalDrive5
R600.14050.346: \\.\PhysicalDrive6
R600.14050.347: \\.\PhysicalDrive10
R601.89832.780: \\.\PhysicalDrive15
```

Settings required to acquire performance information of midrange storage systems

This section describes the settings required to acquire performance information from midrange storage systems (HUS100, Hitachi AMS2000, Hitachi SMS, or Hitachi AMS/WMS).

Procedure

1. On Element Manager in the Device Manager GUI, Storage Navigator Modular, or Storage Navigator Modular 2, specify the settings for acquiring performance statistics.

   For details on how to specify the settings for collecting performance statistics, see the manual for each storage system.
2. If account authentication is enabled in a storage system, create a user account that is used to collect information with only read permission.

   If account authentication or password protection is enabled in a storage system, the storage system might be locked while performance information is being acquired. If the storage system is locked, other users sometimes might not be able to log in. If account authentication is enabled, you can prevent the storage system from being locked during acquisition of performance information by registering the user account that is used to acquire performance information in both the storage system and Device Manager.

   If you want to acquire performance information from multiple storage systems, the user account registered for each of those storage systems must be the same.
3. Execute the `hdvmmodpolluser` command, and register the user account on Device Manager for collecting performance information.

Related references

- Format of the command for registering a user account to acquire performance information (hdvmmodpolluser) on page 449

Format of the command for registering a user account to acquire performance information (hdvmmodpolluser)

The following shows the format of the command (`hdvmmodpolluser`) that registers the user account that is used to acquire performance information in Device Manager. You can register only one user account in Device Manager. If you execute the `hdvmmodpolluser` command with another user account specified, the previously registered information will be overwritten.

Format of the command

In Windows:

```
hdvmmodpolluser { -u Device-Manager-user-ID -p Device-Manager-
password performance-information-acquisition-user-ID
performance-information-acquisition-password| -d }
```

Storage directory of the command

In Windows:

installation-folder-for-Hitachi-Command-Suite\DeviceManager\HiCommandServer\tools

Options

-u, -p

These options are used to specify the user ID and password of the Device Manager. Note that for the user you specify, `All Resources` must be assigned as the resource group, and `Admin` must be set as the Device Manager role.

performance-information-acquisition-user-ID, performance-information-acquisition-password

Specify the user ID and password of the view-only user account registered in the storage system.

-d

Specify this option to delete information about the user registered in Device Manager.

Controlling the SLP service

This section describes how to configure the service discovery function of Device Manager. Note that the ports used by the CIM/WBEM functions are registered in the SLP service (or SLP daemon) by default.

Software prerequisites for using the service discovery function

To use the service discovery function in Device Manager, the prerequisite software is needed:

Table 74 Software prerequisites for using the service discovery function

OS	Prerequisite software	Remarks
Windows Red Hat Enterprise Linux 5 Red Hat Enterprise Linux 6	OpenSLP 1.0.11	OpenSLP is provided with Device Manager. When you install Device Manager, the required file is copied. For details on OpenSLP, see the OpenSLP website (http://www.openslp.org/).
Red Hat Enterprise Linux 7 Oracle Linux 7	OpenSLP 2.0.0	OpenSLP is provided with each OS. For details on OpenSLP, see the OpenSLP website (http://www.openslp.org/).
SUSE Linux Enterprise Server 11	OpenSLP 1.2.0	OpenSLP is provided with the SUSE Linux Enterprise Server system. For details on OpenSLP, see the Novell website (http://www.novell.com/).
SUSE Linux Enterprise Server 12	OpenSLP 2.0.0	

Starting the SLP service (Windows)

To start the SLP service, use the Windows menu or the `slpd` command.

Before you begin

Log in as a user with Administrator permissions.

Procedure

Perform either of the following procedures:

- From **Administrative Tools**, select **Services** and then **Service Location Protocol** to start the SLP service.
- Show the command prompt, move to the folder containing the OpenSLP executable file, and execute the following command:

  ```
  slpd -start
  ```

Stopping the SLP service (Windows)

To stop the SLP service, use the Windows menu or the `slpd` command.

Before you begin

Log in as a user with Administrator permissions.

Procedure

Perform either of the following procedures:

- From **Administrative Tools**, select **Services** and then **Service Location Protocol** to stop the SLP service.
- Display the command prompt, move to the folder containing the OpenSLP executable file, and execute the following command:

  ```
  slpd -stop
  ```

Starting the SLP daemon (Red Hat Enterprise Linux or Oracle Linux)

To start the SLP daemon, use the `slpd` or `systemctl` command.

Before you begin

Log in as a user with root user.

Procedure

Execute the following command:

In Red Hat Enterprise Linux 5 or Red Hat Enterprise Linux 6:

```
installation-directory-for-Hitachi-Command-Suite/
HiCommandServer/wsi/bin/slpd.sh start
```

In Red Hat Enterprise Linux 7 or Oracle Linux 7:

```
# systemctl start slpd.service
```

Stopping the SLP daemon (Red Hat Enterprise Linux or Oracle Linux)

To stop the SLP daemon, use the `slpd` or `systemctl` command.

Before you begin

Log in as a user with root user.

Procedure

Execute the following command:

In Red Hat Enterprise Linux 5 or Red Hat Enterprise Linux 6:

```
installation-directory-for-Hitachi-Command-Suite/
HiCommandServer/wsi/bin/slpd.sh stop
```

In Red Hat Enterprise Linux 7 or Oracle Linux 7:

```
# systemctl stop slpd.service
```

Starting the SLP daemon (SUSE Linux Enterprise Server)

To start the SLP daemon, use the `rcslpd` command.

Before you begin

Log in as a user with root user.

Procedure

Execute the following command:

```
# /usr/sbin/rcslpd start
```

Stopping the SLP daemon (SUSE Linux Enterprise Server)

To stop the SLP daemon, use the `rcslpd` command.

Before you begin

Log in as a user with root user.

Procedure

Execute the following command:

```
# /usr/sbin/rcslpd stop
```

Releasing the SLP service (Windows)

You might need to release the SLP service when uninstalling Hitachi Command Suite products.

If the following message is displayed, manually release the SLP service from the Windows services.

```
Unable to release the SLP service, but the removal will
continue. After the removal, release the SLP service.
```

Before you begin

Log in as a user with Administrator permissions.

Procedure

1. Show the command prompt and move to the folder containing the OpenSLP executable file.
2. Execute the following command:

   ```
   slpd -remove
   ```

Releasing the SLP daemon (Linux)

You might need to release the SLP daemon when uninstalling Hitachi Command Suite products.

If the following message is displayed, manually release the SLP daemon.

```
Unable to release the SLP service, but the removal will
continue. After the removal, release the SLP service.
```

Before you begin

Log in as a user with root user.

Procedure

1. Stop the SLP daemon.
2. If `/etc/init.d/slpd` exists, delete it.

   ```
   # chkconfig --level 01345 slpd off
   # chkconfig --del slpd
   # rm -f /etc/init.d/slpd
   ```

Notes on OpenSLP logs

Since the SLP service log output (or SLP daemon) accumulates as time elapses, if you use the SLP service (or SLP daemon) for an extended period of time, the log output might eventually use up a lot of disk space. To prevent this, you need to periodically back up the log file and clear the disk space. By default, only the start message at SLP daemon startup is output to the log file.

In Windows:

*%WINDIR%*slpd.log

%WINDIR% is replaced by the value of the environment variable WINDIR in Windows. Normally, the value is C:\WINNT\.

In Linux:

*installation-directory-for-Hitachi-Command-Suite/*HiCommandServer/wsi/cfg/slp.log

9

Starting and stopping services

This chapter explains how to start and stop the Hitachi Command Suite product services.

- Starting and stopping services of Hitachi Command Suite
- Starting and stopping services of the Host Data Collector
- Hitachi Command Suite product services that are registered in cluster management applications

Starting and stopping services of Hitachi Command Suite

This section explains how to start and stop the services of Device Manager, Tiered Storage Manager, and Replication Manager.

Resident processes of Hitachi Command Suite

Hitachi Command Suite (Device Manager, Tiered Storage Manager, and Replication Manager) operation requires that resident processes are running on the OS.

The following table describes the resident processes of Device Manager, Tiered Storage Manager, and Replication Manager.

Table 75 Resident processes in Windows

Process name	Service name	Function
htsmService.exe	HiCommand Tiered Storage Manager	The Tiered Storage Manager server
HiCommandServer	HiCommandServer	The Device Manager server
hcmdssvctl.exe cjstartsv.exe	HBase 64 Storage Mgmt SSO Service	Hitachi Command Suite J2EE service for single sign-on
httpsd.exe rotatelogs.exe	HBase 64 Storage Mgmt Web Service	Hitachi Command Suite common web service. Multiple instances of this process might be running.
httpsd.exe rotatelogs.exe	HBase 64 Storage Mgmt Web SSO Service	Hitachi Command Suite common web service for single sign-on.
hcmdssvctl.exe cjstartsv.exe	HCS Device Manager Web Service	Device Manager J2EE service
hntr2mon.exe	Hitachi Network Objectplaza Trace Monitor 2 Hitachi Network Objectplaza Trace Monitor 2 (x64)	Hitachi Command Suite common trace log collection
hntr2srv.exe		Hitachi Command Suite common trace service (This service processes events from the Services window.)
pdservice.exe#	HiRDB/ EmbeddedEdition _HD1	HiRDB process server control

#:

This process must always be running. Do not stop it manually or register it as a cluster resource.

Table 76 Resident processes in Linux

Process name	Function
htsmservice	The Tiered Storage Manager server
hicmdserver	The Device Manager server *installation-directory-for-Hitachi-Command-Suite*/HiCommandServer/hicmdserver
hcs_hsso cjstartsv	Hitachi Command Suite J2EE service for single sign-on *installation-directory-for-Hitachi-Command-Suite*/Base64/uCPSB/CC/web/containers/HBase64StgMgmtSSOService/hcs_hsso *installation-directory-for-Hitachi-Command-Suite*/Base64/uCPSB/CC/web/bin/cjstartweb
httpsd rotatelogs	Hitachi Command Suite common web service Multiple instances of this process might be running. *installation-directory-for-Hitachi-Command-Suite*/Base64/uCPSB/httpsd/sbin/httpsd *installation-directory-for-Hitachi-Command-Suite*/Base64/uCPSB/httpsd/sbin/rotatelogs
httpsd rotatelogs	Hitachi Command Suite common web service for single sign-on. *installation-directory-for-Hitachi-Command-Suite*/Base64/uCPSB/httpsd/sbin/httpsd *installation-directory-for-Hitachi-Command-Suite*/Base64/uCPSB/httpsd/sbin/rotatelogs
hcs_dm cjstartsv	Device Manager J2EE service /bin/sh *installation-directory-for-Hitachi-Command-Suite*/Base64/uCPSB/CC/server/repository/DeviceManagerWebService/hcs_dm *installation-directory-for-Hitachi-Command-Suite*/Base64/uCPSB/CC/server/bin/cjstartsv
/opt/hitachi/HNTRLib2/bin/hntr2mon	Hitachi Command Suite common trace log collection
pdprcd#	HiRDB process server process

#:

This process must always be running. Do not stop it manually or register it as a cluster resource.

Related concepts

- Resident processes of the Host Data Collector on page 463

Related tasks

- Starting the Hitachi Command Suite services on page 458

- Stopping the Hitachi Command Suite services on page 460
- Checking the operating status of the Hitachi Command Suite services on page 462

Starting the Hitachi Command Suite services

You can start the Hitachi Command Suite services from the Windows menu or by using the `hcmds64srv` command.

Before you begin

Log in as a user with Administrator permissions (for Windows) or as a root user (for Linux).

Procedure

Perform the following operations.

In Windows:

Start the services in either of the following ways:

In Windows Server 2008 R2:

Select **Start**, **All Programs**, **Hitachi Command Suite**, **Manage Services**, and then **Start - HCS**.

In Windows Server 2012 or Windows Server 2012 R2:

From the Start window, open the application list window, select **Hitachi Command Suite**, and then **Start - HCS**.

By using the following command:

installation-folder-for-Hitachi-Command-Suite`\Base64\bin\hcmds64srv /start`

In Linux:

Execute the following command:

installation-directory-for-Hitachi-Command-Suite`/Base64/bin/hcmds64srv -start`

Note: If the system is linked with Hitachi File Services Manager or Storage Navigator Modular 2 and you use a command to start Hitachi Command Suite product services, also execute the following commands:

- In Windows:
  installation-folder-for-Hitachi-File-Services-Manager-or-Storage-Navigator-Modular-2`\Base\bin\hcmdssrv /start`
- In Linux:

installation-directory-for-Hitachi-File-Services-Manager-or-Storage-Navigator-Modular-2`/Base/bin/hcmdssrv -start`

Tip: The Storage Navigator Modular 2 service does not start even if Hitachi Command Suite product services start.

To start the Storage Navigator Modular 2 service:

In Windows:

Perform either of the following operations:

- From the Services window, select **SNM2 Server**, and then **Restart the service**.

- From the command prompt, execute the following command:

```
net start snm2server
```

In Linux:

Log in as a root user, and then execute the following command:

```
/etc/init.d/snm2srv start
```

Result

The following services are started in a batch, and the results of starting the services are displayed in the window:

- HiRDB
- HBase 64 Storage Mgmt SSO Service
- HBase 64 Storage Mgmt Web Service
- HBase 64 Storage Mgmt Web SSO Service
- HCS Device Manager Web Service
- HiCommandServer
- HiCommand Tiered Storage Manager
- All Hitachi Command Suite product services present on the same server

Stopping the Hitachi Command Suite services

You can stop the Hitachi Command Suite services from the Windows menu or by using the hcmds64srv command.

Before you begin

Log in as a user with Administrator permissions (for Windows) or as a root user (for Linux).

Procedure

Perform the following operations.

In Windows:

Stop the services in either of the following ways:

In Windows Server 2008 R2:

Select **Start**, **All Programs**, **Hitachi Command Suite**, **Manage Services**, and then **Stop - HCS**.

In Windows Server 2012 or Windows Server 2012 R2:

From the Start window, open the application list window, select **Hitachi Command Suite**, and then **Stop - HCS**.

By using the following command:

installation-folder-for-Hitachi-Command-Suite`\Base64\bin\hcmds64srv /stop`

In Linux:

Execute the following command:

installation-directory-for-Hitachi-Command-Suite`/Base64/bin/hcmds64srv -stop`

Caution: In Linux, do not stop Common Component before it has completed startup. If you do so, the service status might indicate that the service has stopped even though a resident process for the service is running, or you might be unable to stop the service. In such cases, restart the computer.

Note: If the system is linked with Hitachi File Services Manager or Storage Navigator Modular 2 and you use a command to start Hitachi Command Suite product services, also execute the following commands:

- In Windows:
  installation-folder-for-Hitachi-File-Services-Manager-or-Storage-Navigator-Modular-2`\Base\bin\hcmdssrv /stop`
- In Linux:
  installation-directory-for-Hitachi-File-Services-Manager-or-Storage-Navigator-Modular-2`/Base/bin/hcmdssrv -stop`

Tip: The Storage Navigator Modular 2 service does not stop even if Hitachi Command Suite product services stop.

To stop the Storage Navigator Modular 2 service:

In Windows:

Perform either of the following operations:

- From the Services window, select **SNM2 Server**, and then **Stop the service**.

- From the command prompt, execute the following command:

```
net stop snm2server
```

In Linux:

Log in as a root user, and then execute the following command:

```
/etc/init.d/snm2srv stop
```

Result

The following services are stopped in a batch, and the results of stopping the services are displayed in the window:

- HiRDB
- HBase 64 Storage Mgmt SSO Service
- HBase 64 Storage Mgmt Web Service
- HBase 64 Storage Mgmt Web SSO Service
- HCS Device Manager Web Service
- HiCommandServer
- HiCommand Tiered Storage Manager

- All Hitachi Command Suite product services present on the same server

Checking the operating status of the Hitachi Command Suite services

You can check the operating status of the Hitachi Command Suite services from the Windows menu or by using the hcmds64srv command.

Before you begin

Log in as a user with Administrator permissions (for Windows) or as a root user (for Linux).

Procedure

Perform the following operations:

In Windows:

Check the operating status of the services in either of the following ways:

In Windows Server 2008 R2

Select **Start**, **All Programs**, **Hitachi Command Suite**, **Manage Services**, and then **Status - HCS**.

In Windows Server 2012 or Windows Server 2012 R2

From the Start window, open the application list window, select **Hitachi Command Suite**, and then **Status - HCS**.

By using the following command:

```
installation-folder-for-Hitachi-Command-Suite\Base64\bin
\hcmds64srv /statusall
```

In Linux:

Execute the following command:

```
installation-directory-for-Hitachi-Command-Suite/
Base64/bin/hcmds64srv -statusall
```

Result

The operating status of the services are displayed in the window.

Starting and stopping services of the Host Data Collector

This section explains how to start and stop the Host Data Collector services.

Resident processes of the Host Data Collector

The resident processes of the Host Data Collector are Host Data Collector service process and JavaVM service process.

These processes are listed in Table 77 Resident processes of the Host Data Collector (Windows) on page 463 to Table 78 Resident processes of the Host Data Collector (Linux) on page 463.

Table 77 Resident processes of the Host Data Collector (Windows)

Process name	Service name	Function
HdcProcessController.exe HdcAdapter.exe# HdcRMI.exe HdcService.exe	Host Data Collector Base Service	Host Data Collector service

#:

There are as many resident Adapter processes as the value specified for the `hdc.adapter.adapterProcessNum` property in the `hdcbase.properties` file for Host Data Collector.

Table 78 Resident processes of the Host Data Collector (Linux)

Process name	Function
installation-directory-for-Host-Data-Collector/HDC/Base/internal/bin/HdcAdapter.sh	Adapter process of the Host Data Collector service#
installation-directory-for-Host-Data-Collector/HDC/Base/internal/bin/HdcService.sh	Service process of the Host Data Collector service
installation-directory-for-Host-Data-Collector/HDC/Base/internal/bin/HdcRMI.sh	RMI process of the Host Data Collector service
Java-execution-environment-installation-path/bin/java	JavaVM (Adapter)#
Java-execution-environment-installation-path/bin/java	JavaVM (Service)
Java-execution-environment-installation-path/bin/java	JavaVM (RMI)

#:

There are as many resident Adapter processes as the value specified for the `hdc.adapter.adapterProcessNum` property in the `hdcbase.properties` file for Host Data Collector.

Note: In a cluster configuration, while the Host Data Collector service on the executing node is running, the Host Data Collector service on the standby node must also be active.

Related concepts

- Resident processes of Hitachi Command Suite on page 456

Related references

- hdc.adapter.adapterProcessNum on page 659

Starting the Host Data Collector service

Use the `controlservice` command to start the Host Data Collector service.

Before you begin

Log in as a user with Administrator permissions (for Windows) or as a root user (for Linux).

Procedure

Execute the following command:

In Windows:

installation-folder-for-Host-Data-Collector\HDC\Base\bin\controlservice.exe start

In Linux:

installation-directory-for-Host-Data-Collector/HDC/Base/bin/controlservice.sh start

Related concepts

- Resident processes of the Host Data Collector on page 463

Related tasks

- Stopping the Host Data Collector service on page 464
- Checking the operating status of the Host Data Collector service on page 465

Stopping the Host Data Collector service

Use the `controlservice` command to stop the Host Data Collector service.

Before you begin

Log in as a user with Administrator permissions (for Windows) or as a root user (for Linux).

Procedure

Execute the following command:

In Windows:

installation-folder-for-Host-Data-Collector\HDC\Base\bin\controlservice.exe stop

In Linux:

installation-directory-for-Host-Data-Collector/HDC/Base/bin/controlservice.sh stop

Related concepts

- Resident processes of the Host Data Collector on page 463

Related tasks

- Starting the Host Data Collector service on page 464
- Checking the operating status of the Host Data Collector service on page 465

Checking the operating status of the Host Data Collector service

Use the `controlservice` command to check the operating status of the Host Data Collector service.

Before you begin

Log in as a user with Administrator permissions (for Windows) or as a root user (for Linux).

Procedure

Execute the following command:

In Windows:

installation-folder-for-Host-Data-Collector\HDC\Base\bin\controlservice.exe state

In Linux:

installation-directory-for-Host-Data-Collector/HDC/Base/bin/controlservice.sh state

Related concepts

- Resident processes of the Host Data Collector on page 463

Related tasks

- Starting the Host Data Collector service on page 464
- Stopping the Host Data Collector service on page 464

Hitachi Command Suite product services that are registered in cluster management applications

The following table explains the Hitachi Command Suite product services that are subject to the `hcmds64clustersrvstate` commands.

In a Windows cluster environment, all services in the table below are brought online or taken offline together if you remotely connect to the Tuning Manager server or back up the database.

Table 79 Hitachi Command Suite product services that are registered in the cluster management applications on the management server

Product name	Displayed service name	Service name	Remarks
Common Component	`HiRDB/ClusterService _HD1`	HiRDBClusterService_HD1	-
	`HBase 64 Storage Mgmt Web Service`	HBase64StgMgmtWebService	-
	`HBase 64 Storage Mgmt Web SSO Service`	HBase64StgMgmtWebSSOService	-
	`HBase 64 Storage Mgmt SSO Service`	HBase64StgMgmtSSOService	-
Device Manager	`HCS Device Manager Web Service`	DeviceManagerWebService64	-
	`HiCommandServer`	HiCommandServer	-
	`HiCommand Tiered Storage Manager`	HiCommandTieredStorageManager	-
Tuning Manager server	`HCS Tuning Manager REST Application Service`	TuningManagerRESTService	-
	`HiCommand Performance Reporter`	PerformanceReporter64	-
	`HiCommand Suite TuningManager`	HiCommandTuningManager64	-
	`PFM - Name Server [logical-host-name]`	JP1PCMGR_PN [*logical-host-name*]	-
	`PFM - Master Manager [logical-host-name]`	JP1PCMGR_PM [*logical-host-name*]	-
	`PFM - Master Store [logical-host-name]`	JP1PCMGR_PS [*logical-host-name*]	-
	`PFM - View Server [logical-host-name]`	JP1PCMGR_PP [*logical-host-name*]	-
	`PFM - Correlator [logical-host-name]`	JP1PCMGR_PE [*logical-host-name*]	-
	`PFM - Trap Generator [logical-host-name]`	JP1PCMGR_PC [*logical-host-name*]	-

Product name	Displayed service name	Service name	Remarks
	PFM - Action Handler [*logical-host-name*]	JP1PCMGR_PH [*logical-host-name*]	-
	PFM - Agent Store for HealthCheck [*logical-host-name*]	JP1PCAGT_0S [*logical-host-name*]	-
	PFM - Agent for HealthCheck [*logical-host-name*]	JP1PCAGT_0A [*logical-host-name*]	-
Compute Systems Manager	HCS Compute Systems Manager Web Service	ComputeSystemsManagerWebService64	-
	DeploymentManager PXE Management	PxeSvc	This service is available if Deployment Manager is installed.
	DeploymentManager PXE Mtftp	PxeMtftp	This service is available if Deployment Manager is installed.
	DeploymentManager Transfer Management	ftsvc	This service is available if Deployment Manager is installed.
Automation Director	HAutomation Common Event *logical-host-name*	JP1_Base_Event *logical-host-name*	-
	HAutomation Common Base *logical-host-name*	JP1_Base_*logical-host-name*	-
	HAutomation Engine Web Service	AutomationWebService64	-
	HAutomation Engine *logical-host-name*	JP1_AJS2_*logical-host-name*	-

Legend:

-: Not applicable

10

Managing the database

This chapter describes how to back up and restore the database for Hitachi Command Suite products.

- Managing databases
- Backing up databases
- Restoring databases
- Migrating databases

Managing databases

The following table describes backing up and restoring, as opposed to exporting and importing.

Table 80 Backing up and restoring as opposed to exporting and importing

Item	Backing up and restoring	Exporting and importing
Restrictions on Hitachi Command Suite product versions	No restrictions	Products of version 05-50 or later must be installed on the server to which data is imported or from which data is exported.
Main purpose	To restore the current operating environment if a failure occurs on the server	To migrate the server data from the current environment to a different environment (such as a server that has a different OS)
Target data	• Databases for Hitachi Command Suite products • The Common Component database	• Databases for Hitachi Command Suite products • User information in the Common Component database
Conditions for computers	• The installed Hitachi Command Suite products are the same between the backup-source computer and the restoration-destination computer. • The version and revision of the installed Hitachi Command Suite products are the same between the backup-source computer and the restoration-destination computer.	• The Hitachi Command Suite products to be imported are installed on the import-destination computer. • The versions and revisions of the Hitachi Command Suite products installed on the import-destination server are the same as or later than the versions and revisions of the products installed on the export-source computer.

The following sections describe the procedure for each operation separately.

Backing up databases

If an error occurs in the database, the management server might not be able to be used. As a preparatory measure, therefore, back up the database regularly.

To back up a database, a directory for storing backup files is required. This directory requires space equal to the formula below. In addition to the estimate below, space is required for the temporary files created during backup.

Required space:

(*total-size-of-all-Hitachi-Command-Suite-product-databases-to-be-backed-up* + 4.6 GB) x 2

As an example, in an environment in which Device Manager, Tiered Storage Manager, and Replication Manager are used, estimate the required space by taking into consideration the sizes of the following directories:

- The directory of the Device Manager database
- The directory of the Tiered Storage Manager database
- The directory of the Replication Manager database
- The directories of the Common Component database#

#: As the directories of Common Component database, the `BASE` directory and the `SYS` directory exist.

If other Hitachi Command Suite products are used, add the sizes of the product directories to the estimate.

Caution:

- If Tuning Manager is remotely connected, stop the Tuning Manager services on the computer where the Tuning Manager server is installed. After the database is backed up, restart the Tuning Manager services. For details about how to start and stop the Tuning Manager services, see the manual for the installed version of Tuning Manager.
- During database backup, Hitachi Command Suite services stop. Therefore, do not access Hitachi Command Suite while the backup is in progress.

Note: If you access a database-related file used by Hitachi Command Suite products by using the backup software, an error might occur due to an I/O delay or file exclusion.

If you want to perform a backup that includes the Hitachi Command Suite installation directory by using the backup software, stop all the services of Hitachi Command Suite products, and then perform the backup.

Backing up a database in non-cluster configuration

To back up a database when management servers are not clustered, perform the procedure below.

Procedure

1. Log on to the management server as a user with Administrator permissions or root permissions.
2. Execute the `hcmds64backups` command to back up the database.

   In Windows:

   installation-folder-for-Hitachi-Command-Suite\Base64\bin\hcmds64backups /dir *folder-for-storing-backup-files* /auto

   In Linux:

*installation-directory-for-Hitachi-Command-Suite/*Base64/bin/hcmds64backups -dir *directory-for-storing-backup-files* -auto

dir

Specify the absolute path of the directory on the local disk in which the database backup files are stored. In Linux, do not specify a path that includes a space.

Make sure that no files or subdirectories are in the directory specified for the `dir` option.

auto

Automatically starts or stops Hitachi Command Suite services.

When you execute the `hcmds64backups` command, the directory `database` will be created in the directory for storing backup files, specified with the `dir` option, and these files will be combined and stored as the file `backup.hdb`.

Note: The setting files for Hitachi Command Suite products are backed up in locations other than the `database` directory created in the directory for storing backup files, specified with the `dir` option. If an error occurs in the management server and you need to re-install Hitachi Command Suite products, you can use the backed up setting files to check the previous settings.

Backing up a database in a Windows cluster configuration

To back up a database when the OSs of the management servers are Windows and are clustered, perform the procedure below.

Caution: Use the executing node (a machine that has `online` set for `mode` in the `cluster.conf` file) to make backups of databases.

Before you begin

Log in as a user with Administrator permissions

Procedure

1. Execute the following command to take the Hitachi Command Suite product services offline.

   installation-folder-of-Hitachi-Command-Suite\Base64\ClusterSetup\hcmds64clustersrvstate /soff /r *resource-group-name*

soff

Use this option to suppress failover by taking the following offline: the Hitachi Command Suite product services registered to the resource group of the cluster management application. A group of clustered services (the set of services for which failover is performed) is called a resource group.

r

Specify the name of the resource group.

2. Execute the `hcmds64backups` command to back up the database.

   installation-folder-for-Hitachi-Command-Suite\Base64\bin\hcmds64backups /dir *folder-for-storing-backup-files* /auto

   dir

   Specify the absolute path of the folder on the shared disk in which the database backup files are stored.

   Make sure that no files or subfolders are in the folder specified for the `dir` option.

   auto

   Automatically starts or stops Hitachi Command Suite services.

   When you execute the `hcmds64backups` command, the folder `database` will be created in the folder for storing backup files, specified with the `dir` option, and these files will be combined and stored as the file `backup.hdb`.

3. Execute the `hcmds64srv /stop` command to stop the Hitachi Command Suite product services.

   Then, execute the `hcmds64srv /statusall` command to make sure that the services have stopped or that the return code of the command is 0.

4. Execute the command below to bring the following online: the resource group of the cluster management application and the Hitachi Command Suite product services.

   installation-folder-of-Hitachi-Command-Suite\Base64\ClusterSetup\hcmds64clustersrvstate /son /r *resource-group-name*

   son

   Use this option to enable failover by bringing the following online: the resource group set for the cluster management application.

   r

   Specify the name of the resource group.

Related tasks

- Stopping the Hitachi Command Suite services on page 460
- Checking the operating status of the Hitachi Command Suite services on page 462

Related references

- Hitachi Command Suite product services that are registered in cluster management applications on page 466

Backing up a database in a Red Hat Enterprise Linux cluster configuration

To back up a database when the OSs for the management servers are Red Hat Enterprise Linux and are clustered, perform the procedure below.

Caution: Use the executing node (a machine that has `online` set for `mode` in the `cluster.conf` file) to make backups of databases.

Before you begin

- Log in as a user with root permissions
- Check the following information:
  - The file name of the script created to register services into a service group
    For details about how to register the Hitachi Command Suite product services to a service group, see *Hitachi Command Suite Installation and Configuration Guide*.

Procedure

1. Remove the Hitachi Command Suite product services from the service group.

   For details, see *Hitachi Command Suite Installation and Configuration Guide*.
2. Confirm that the service group was moved to the executing node.

   If the service group has not been moved, move the service group to the executing node.
3. Execute the `hcmds64srv -statusall` command to make sure that the services have stopped or that the return code of the command is 0.
4. Execute the `hcmds64backups` command to back up the database.

   installation-directory-for-Hitachi-Command-Suite/Base64/bin/hcmds64backups -dir *directory-for-storing-backup-files* -auto

   dir

Specify the absolute path of the directory on the shared disk in which the database backup files are stored.

Make sure that no files or subfolders are in the directory specified for the `dir` option.

`auto`

Automatically starts or stops Hitachi Command Suite services.

When you execute the `hcmds64backups` command, the folder `database` will be created in the folder for storing backup files, specified with the `dir` option, and these files will be combined and stored as the file `backup.hdb`.

5. Execute the `hcmds64srv -stop` command to stop the Hitachi Command Suite product services.

   Then, execute the `hcmds64srv -statusall` command to make sure that the services have stopped or that the return code of the command is 0.
6. Re-register the Hitachi Command Suite product services removed in step 1 to the service group.
7. Start the service group to which the Hitachi Command Suite product services were registered.

   For details, see *Hitachi Command Suite Installation and Configuration Guide*.

Related tasks

- Stopping the Hitachi Command Suite services on page 460
- Checking the operating status of the Hitachi Command Suite services on page 462

Restoring databases

If an error occurs with a database, use the following methods, depending on the situation, to restore the database:

- When a database inconsistency occurs:
  The database can be restored by using a database that has been backed up via the `hcmds64backups` command.
  All of the following must be same between the management server when the database was backed up and the management server when the database is restored:
  - Type, version, and revision of the installed Hitachi Command Suite products
  - Installation destination of the Hitachi Command Suite products
  - Installation destination of Common Component

- Installation destination of the Hitachi Command Suite product databases
- Installation destination of the Common Component database
- IP address and host name of the computer

- When a database is corrupted:
  The database can be restored by using a database exported via the `hcmds64dbtrans` command.
  The type, version, and revision of the installed Hitachi Command Suite products must be the same between the management server when the database was exported and the management server when the database is restored.
  When the `hcmds64dbrepair` command is executed, all of the Hitachi Command Suite databases installed on the management server are forcibly deleted and then replaced by the exported databases.

Restoring a database when a data inconsistency occurs in a non-cluster configuration

To restore a database when management servers are not clustered, perform the procedure below.

Caution:

- The `hcmds64db` command, which is used in the procedure below, creates temporary files during execution. Make sure that the directory to which the backup file is to be restored satisfies the following conditions:
  - The write permission is granted to the user who executes the `hcmds64db` command.
  - There is enough free capacity for the stored backup file.
- If Tuning Manager is remotely connected, stop the Tuning Manager services on the computer where the Tuning Manager server is installed. After the database is restored, restart the Tuning Manager services. For details about how to start and stop the Tuning Manager services, see the manual for the installed version of Tuning Manager.
  If Tuning Manager is remotely connected and was using the Alert function of Tuning Manager, you need to restore the database, and then synchronize the alert definition information. For details about synchronizing alert definition information, see the *Hitachi Command Suite Tuning Manager API Reference Guide*.
- During database restoration, Hitachi Command Suite services stop. Therefore, do not access Hitachi Command Suite while restoration is in progress.

Procedure

1. Log on to the management server as a user with Administrator permissions or root permissions.
2. Execute the `hcmds64db` command to restore the database.

   In Windows:

   installation-folder-for-Hitachi-Command-Suite\Base64\bin\hcmds64db /restore *backup-file* /type *name-of-the-Hitachi-Command-Suite-product-to-be-restored* /auto

   In Linux:

   installation-directory-for-Hitachi-Command-Suite/Base64/bin/hcmds64db -restore *backup-file* -type *name-of-the-Hitachi-Command-Suite-product-to-be-restored* -auto

   restore

   Specify the absolute path to the database backup file (`backup.hdb`) that was created by using the `hcmds64backups` command. In Linux, do not specify a path that includes a space.

   type

   As a rule, specify `ALL`. If you specify `ALL`, the databases of all Hitachi Command Suite products that are installed on the management server are restored at once.

   To restore the database of only a specific Hitachi Command Suite product because of a failure or other reasons, specify the name of the product to be restored as listed in the following table.

   Table 81 Values to specify for the type option when restoring databases (In a non-cluster configuration)

Product	Value
Device Manager	`DeviceManager`
Tiered Storage Manager	`TieredStorageManager`
Replication Manager	`ReplicationManager`
Other products	Refer to the manual for each product.

   auto

   Automatically starts or stops Hitachi Command Suite services.

3. If `DeviceManager` is specified for the `type` option, specify `true` for the `server.base.initialsynchro` property on the Device Manager server.
4. If `TieredStorageManager` is specified for the `type` option, specify `true` for the `server.base.initialsynchro` property on the Tiered Storage Manager server.

5. If Tuning Manager is remotely connected, the remote connection setting is re-initialized during a database restoration. Execute the `htmsetup` command to specify the setting again.
6. Start the Hitachi Command Suite product services.
7. Change the value of the `server.base.initialsynchro` property on the Device Manager server back to `false`.
8. Change the value of the `server.base.initialsynchro` property on the Tiered Storage Manager server back to `false`.
9. If you specified `ALL` or `DeviceManager` for the `type` option, refresh the storage system from the Device Manager GUI or CLI.
10. If you restored the management server database at the Replication Manager secondary site, refresh the configuration information by using the Replication Manager GUI to synchronize the Replication Manager database at the primary site and the Device Manager database at the secondary site.
11. Check the status of Device Manager tasks from the Device Manager GUI.

    If a Device Manager task is not completed or has failed, re-create the task or change the execution schedule of the task as necessary.
12. See the message log of Tiered Storage Manager.

    When Tiered Storage Manager is started for the first time after a database is restored, make sure that the message KATS50354-E is output to a log file. The task IDs of Tiered Storage Manager tasks whose status was changed to **Failure** are output to KATS50354-E.
13. 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.
14. If a Tiered Storage Manager task is not completed, create and execute the task again as necessary.

Related tasks

- Starting the Hitachi Command Suite services on page 458

Related references

- Specifying the settings for remote connection to the Tuning Manager server and the port number (htmsetup command) on page 352

Restoring a database when a data inconsistency occurs in a Windows cluster configuration

To restore a database when the OSs for the management servers are Windows and are clustered, perform the procedure below.

Caution:

- Use the executing node (a machine that has `online` set for `mode` in the `cluster.conf` file) to restore databases.
- The `hcmds64db` command, which is used in the procedure below, creates temporary files during execution. Make sure that the directory to which the backup file is to be restored satisfies the following conditions:
  - The write permission is granted to the user who executes the `hcmds64db` command.
  - There is enough free capacity for the stored backup file.
- If Tuning Manager is remotely connected, stop the Tuning Manager services on the computer where the Tuning Manager server is installed. After the database is restored, restart the Tuning Manager services. For details about how to start and stop the Tuning Manager services, see the manual for the installed version of Tuning Manager.
  If Tuning Manager is remotely connected and was using the Alert function of Tuning Manager, you need to restore the database, and then synchronize the alert definition information. For details about synchronizing alert definition information, see the *Hitachi Command Suite Tuning Manager API Reference Guide*.
- During database restoration, Hitachi Command Suite services stop. Therefore, do not access Hitachi Command Suite while restoration is in progress.

Before you begin

Log in as a user with Administrator permissions

Procedure

1. Execute the following command to take the Hitachi Command Suite product services offline.

   installation-folder-of-Hitachi-Command-Suite`\Base64\ClusterSetup\hcmds64clustersrvstate /soff /r` *resource-group-name*

   soff

   Use this option to suppress failover by taking the following offline: the Hitachi Command Suite product services registered to the resource group of the cluster management application. A group of clustered services (the set of services for which failover is performed) is called a resource group.

   r

   Specify the name of the resource group.

2. Execute the `hcmds64db` command to restore the database.

   installation-folder-for-Hitachi-Command-Suite\Base64\bin\hcmds64db /restore *backup-file* /type *name-of-the-Hitachi-Command-Suite-product-to-be-restored*

   restore

   Specify the absolute path to the database backup file (`backup.hdb`) that was created by using the `hcmds64backups` command. Use a backup file saved on the shared disk.

   type

   As a rule, specify `ALL`. If you specify `ALL`, the databases of all Hitachi Command Suite products that are installed on the management server are restored at once.

   To restore the database of only a specific Hitachi Command Suite product because of a failure or other reasons, specify the name of the product to be restored as listed in the following table.

   Table 82 Values to specify for the type option when restoring databases (For a Windows cluster configuration)

Product	Value
Device Manager	`DeviceManager`
Tiered Storage Manager	`TieredStorageManager`
Replication Manager	`ReplicationManager`
Other products	Refer to the manual for each product.

3. If you specified `DeviceManager` for the `type` option, set the `server.base.initialsynchro` property of the Device Manager server to `true` on the executing node and the standby node.
4. If you specified `TieredStorageManager` for the `type` option, set the `server.base.initialsynchro` property of the Tiered Storage Manager server to `true` on the executing node and the standby node.
5. Execute the command below to bring the following online: the resource group of the cluster management application and the Hitachi Command Suite product services.

   installation-folder-of-Hitachi-Command-Suite\Base64\ClusterSetup\hcmds64clustersrvstate /son /r *resource-group-name*

   son

   Use this option to enable failover by bringing the following online: the resource group set for the cluster management application.

   r

Specify the name of the resource group.

6. On the executing node and standby node, change the value of the `server.base.initialsynchro` property on the Device Manager server back to `false`.
7. On the executing node and standby node, change the value of the `server.base.initialsynchro` property on the Tiered Storage Manager server back to `false`.
8. If you specified `ALL` or `DeviceManager` for the `type` option, refresh the storage system from the Device Manager GUI or CLI.
9. If you restored the management server database at the Replication Manager secondary site, refresh the configuration information by using the Replication Manager GUI to synchronize the Replication Manager database at the primary site and the Device Manager database at the secondary site.
10. Check the status of Device Manager tasks from the Device Manager GUI.

    If a Device Manager task is not completed or has failed, re-create the task or change the execution schedule of the task as necessary.
11. See the message log of Tiered Storage Manager.

    When Tiered Storage Manager is started for the first time after a database is restored, make sure that the message KATS50354-E is output to a log file. The task IDs of Tiered Storage Manager 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 Tiered Storage Manager task is not completed, create and execute the task again as necessary.
14. If Tuning Manager is remotely connected, the remote connection setting is re-initialized during a database restoration. Specify the setting again.

Related tasks

- Remote connection to the Tuning Manager server (in a Windows cluster environment) on page 349

Related references

- Hitachi Command Suite product services that are registered in cluster management applications on page 466

Restoring a database when a data inconsistency occurs in a Red Hat Enterprise Linux cluster configuration

To restore a database when the OSs for the management servers are Red Hat Enterprise Linux and are clustered, perform the procedure below.

Caution:

- Use the executing node (a machine that has `online` set for `mode` in the `cluster.conf` file) to restore databases.
- The `hcmds64db` command, which is used in the procedure below, creates temporary files during execution. Make sure that the directory to which the backup file is to be restored satisfies the following conditions:
  - The write permission is granted to the user who executes the `hcmds64db` command.
  - There is enough free capacity for the stored backup file.
- If Tuning Manager is remotely connected, stop the Tuning Manager services on the computer where the Tuning Manager server is installed. After the database is restored, restart the Tuning Manager services. For details about how to start and stop the Tuning Manager services, see the manual for the installed version of Tuning Manager.
  If Tuning Manager is remotely connected and was using the Alert function of Tuning Manager, you need to restore the database, and then synchronize the alert definition information. For details about synchronizing alert definition information, see the *Hitachi Command Suite Tuning Manager API Reference Guide*.
- During database restoration, Hitachi Command Suite services stop. Therefore, do not access Hitachi Command Suite while restoration is in progress.

Before you begin

- Log in as a user with root permissions
- Check the following information:
  - The file name of the script created to register services into a service group
    For details about how to register the Hitachi Command Suite product services to a service group, see *Hitachi Command Suite Installation and Configuration Guide*.

Procedure

1. Remove the Hitachi Command Suite product services from the service group.

   For details, see *Hitachi Command Suite Installation and Configuration Guide*.
2. Confirm that the service group was moved to the executing node.

If the service group has not been moved, move the service group to the executing node.

3. Execute the `hcmds64db` command to restore the database.

   installation-directory-for-Hitachi-Command-Suite`/Base64/bin/hcmds64db -restore` *backup-file* `-type` *name-of-the-Hitachi-Command-Suite-product-to-be-restored*

   restore

   Specify the absolute path to the database backup file (`backup.hdb`) that was created by using the `hcmds64backups` command. Use a backup file saved on the shared disk.

   type

   As a rule, specify `ALL`. If you specify `ALL`, the databases of all Hitachi Command Suite products that are installed on the management server are restored at once.

   To restore the database of only a specific Hitachi Command Suite product because of a failure or other reasons, specify the name of the product to be restored as listed in the following table.

   Table 83 Values to specify for the type option when restoring databases (For a Red Hat Enterprise Linux cluster configuration)

Product	Value
Device Manager	`DeviceManager`
Tiered Storage Manager	`TieredStorageManager`
Replication Manager	`ReplicationManager`
Other products	Refer to the manual for each product.

4. If you specified `DeviceManager` for the `type` option, set the `server.base.initialsynchro` property of the Device Manager server to `true` on the executing node and the standby node.
5. If you specified `TieredStorageManager` for the `type` option, set the `server.base.initialsynchro` property of the Tiered Storage Manager server to `true` on the executing node and the standby node.
6. Start the Hitachi Command Suite product services.
7. On the executing node and standby node, change the value of the `server.base.initialsynchro` property on the Device Manager server back to `false`.
8. On the executing node and standby node, change the value of the `server.base.initialsynchro` property on the Tiered Storage Manager server back to `false`.
9. Restart the Hitachi Command Suite product services.

10. Re-register the Hitachi Command Suite product services removed in step 1 to the service group.
11. Start the service group to which the Hitachi Command Suite product services were registered.

    For details, see *Hitachi Command Suite Installation and Configuration Guide*.
12. If you specified `ALL` or `DeviceManager` for the `type` option, refresh the storage system from the Device Manager GUI or CLI.
13. If you restored the management server database at the Replication Manager secondary site, refresh the configuration information by using the Replication Manager GUI to synchronize the Replication Manager database at the primary site and the Device Manager database at the secondary site.
14. Check the status of Device Manager tasks from the Device Manager GUI.

    If a Device Manager task is not completed or has failed, re-create the task or change the execution schedule of the task as necessary.
15. See the message log of Tiered Storage Manager.

    When Tiered Storage Manager is started for the first time after a database is restored, make sure that the message KATS50354-E is output to a log file. The task IDs of Tiered Storage Manager tasks whose status was changed to **Failure** are output to KATS50354-E.
16. 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.
17. If a Tiered Storage Manager task is not completed, create and execute the task again as necessary.
18. If Tuning Manager is remotely connected, the remote connection setting is re-initialized during a database restoration. Specify the setting again.

Related tasks

- Remote connection to the Tuning Manager server (in a Red Hat Enterprise Linux cluster environment) on page 351
- Starting the Hitachi Command Suite services on page 458
- Stopping the Hitachi Command Suite services on page 460

Restoring a database when it is corrupted in a non-cluster configuration

To restore a database when management servers are not clustered, perform the procedure below.

Caution:
- If Tuning Manager is remotely connected, stop the Tuning Manager services on the computer where the Tuning Manager server is installed.

After the database is restored, restart the Tuning Manager services. For details about how to start and stop the Tuning Manager services, see the manual for the installed version of Tuning Manager.
If Tuning Manager is remotely connected and was using the Alert function of Tuning Manager, you need to restore the database, and then synchronize the alert definition information. For details about synchronizing alert definition information, see the *Hitachi Command Suite Tuning Manager API Reference Guide*.

- During database restoration, Hitachi Command Suite services stop. Therefore, do not access Hitachi Command Suite while restoration is in progress.

Procedure

1. Log on to the management server as a user with Administrator permissions or root permissions.
2. Stop the Hitachi Command Suite product services.
3. Execute the `hcmds64dbrepair` command to restore the database.

   In Windows:

   installation-folder-for-Hitachi-Command-Suite\Base64\bin\hcmds64dbrepair /trans *exported-file*

   In Linux:

   installation-directory-for-Hitachi-Command-Suite/Base64/bin/hcmds64dbrepair -trans *exported-file*

   trans

   Specify the absolute path to the archive file of the database exported via the `hcmds64dbtrans` command. In Linux, do not specify a path that includes a space.
4. Specify `true` for the `server.base.initialsynchro` property on the Device Manager server.
5. Specify `true` for the `server.base.initialsynchro` property on the Tiered Storage Manager server.
6. If Tuning Manager is remotely connected, the remote connection setting is re-initialized during a database restoration. Execute the `htmsetup` command to specify the setting again.
7. Start the Hitachi Command Suite product services.
8. Change the value of the `server.base.initialsynchro` property on the Device Manager server back to `false`.
9. Change the value of the `server.base.initialsynchro` property on the Tiered Storage Manager server back to `false`.
10. Refresh the storage system from the Device Manager GUI or CLI.

11. If you restored the management server database at the Replication Manager secondary site, refresh the configuration information by using the Replication Manager GUI to synchronize the Replication Manager database at the primary site and the Device Manager database at the secondary site.
12. Check the status of Device Manager tasks from the Device Manager GUI.

    If a Device Manager task is not completed or has failed, re-create the task or change the execution schedule of the task as necessary.
13. See the message log of Tiered Storage Manager.

    When Tiered Storage Manager is started for the first time after a database is restored, make sure that the message KATS50354-E is output to a log file. The task IDs of Tiered Storage Manager 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 those tasks are completed.

    Check for completion of not only migration tasks but also shredding tasks and locking tasks.
15. If a Tiered Storage Manager task is not completed, create and execute the task again as necessary.
16. The password for the `System` account is re-initialized during a database restoration. If necessary, specify the password again.

    For details on how to change the password for the `System` account, see the *Hitachi Command Suite User Guide*.

Related tasks

- Starting the Hitachi Command Suite services on page 458
- Stopping the Hitachi Command Suite services on page 460

Related references

- Specifying the settings for remote connection to the Tuning Manager server and the port number (htmsetup command) on page 352

Restoring a database when it is corrupted in a Windows cluster configuration

To restore a database when the OSs for the management servers are Windows and are clustered, perform the procedure below.

Caution:

- Use the executing node (a machine that has `online` set for `mode` in the `cluster.conf` file) to restore databases.
- If Tuning Manager is remotely connected, stop the Tuning Manager services on the computer where the Tuning Manager server is installed. After the database is restored, restart the Tuning Manager services. For

details about how to start and stop the Tuning Manager services, see the manual for the installed version of Tuning Manager.
If Tuning Manager is remotely connected and was using the Alert function of Tuning Manager, you need to restore the database, and then synchronize the alert definition information. For details about synchronizing alert definition information, see the *Hitachi Command Suite Tuning Manager API Reference Guide*.

- During database restoration, Hitachi Command Suite services stop. Therefore, do not access Hitachi Command Suite while restoration is in progress.

Before you begin

Log in as a user with Administrator permissions

Procedure

1. Execute the following command to take the Hitachi Command Suite product services offline.

   installation-folder-of-Hitachi-Command-Suite\Base64\ClusterSetup\hcmds64clustersrvstate /soff /r *resource-group-name*

   soff

   Use this option to suppress failover by taking the following offline: the Hitachi Command Suite product services registered to the resource group of the cluster management application. A group of clustered services (the set of services for which failover is performed) is called a resource group.

   r

   Specify the name of the resource group.

2. Execute the `hcmds64dbrepair` command to restore the database.

   installation-folder-for-Hitachi-Command-Suite\Base64\bin\hcmds64dbrepair /trans *exported-file*

   trans

   Specify the absolute path to the archive file of the database exported via the `hcmds64dbtrans` command.

3. On the executing node and standby node, specify `true` for the `server.base.initialsynchro` property on the Device Manager server.
4. On the executing node and standby node, specify `true` for the `server.base.initialsynchro` property on the Tiered Storage Manager server.

5. Stop the Hitachi Command Suite product services.
6. Execute the command below to bring the following online: the resource group of the cluster management application and the Hitachi Command Suite product services.

   installation-folder-of-Hitachi-Command-Suite\Base64\ClusterSetup\hcmds64clustersrvstate /son /r *resource-group-name*

   son

   Use this option to enable failover by bringing the following online: the resource group set for the cluster management application.

   r

   Specify the name of the resource group.
7. On the executing node and standby node, change the value of the `server.base.initialsynchro` property on the Device Manager server back to `false`.
8. On the executing node and standby node, change the value of the `server.base.initialsynchro` property on the Tiered Storage Manager server back to `false`.
9. Refresh the storage system from the Device Manager GUI or CLI.
10. If you restored the management server database at the Replication Manager secondary site, refresh the configuration information by using the Replication Manager GUI to synchronize the Replication Manager database at the primary site and the Device Manager database at the secondary site.
11. Check the status of Device Manager tasks from the Device Manager GUI.

    If a Device Manager task is not completed or has failed, re-create the task or change the execution schedule of the task as necessary.
12. See the message log of Tiered Storage Manager.

    When Tiered Storage Manager is started for the first time after a database is restored, make sure that the message KATS50354-E is output to a log file. The task IDs of Tiered Storage Manager tasks whose status was changed to **Failure** are output to KATS50354-E.
13. 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.
14. If a Tiered Storage Manager task is not completed, create and execute the task again as necessary.
15. If Tuning Manager is remotely connected, the remote connection setting is re-initialized during a database restoration. Specify the setting again.
16. The password for the `System` account is re-initialized during a database restoration. If necessary, specify the password again.

For details about how to change the password for the `System` account, see the *Hitachi Command Suite User Guide*.

Related tasks

- Remote connection to the Tuning Manager server (in a Windows cluster environment) on page 349
- Stopping the Hitachi Command Suite services on page 460

Related references

- Hitachi Command Suite product services that are registered in cluster management applications on page 466

Restoring a database when it is corrupted in a Red Hat Enterprise Linux cluster configuration

To restore a database when the OSs for the management servers are Red Hat Enterprise Linux and are clustered, perform the procedure below.

Caution:

- Use the executing node (a machine that has `online` set for `mode` in the `cluster.conf` file) to restore databases.
- If Tuning Manager is remotely connected, stop the Tuning Manager services on the computer where the Tuning Manager server is installed. After the database is restored, restart the Tuning Manager services. For details about how to start and stop the Tuning Manager services, see the manual for the installed version of Tuning Manager.
  If Tuning Manager is remotely connected and was using the Alert function of Tuning Manager, you need to import the database, and then synchronize the alert definition information. For details about synchronizing alert definition information, see the *Hitachi Command Suite Tuning Manager API Reference Guide*.
- During database restoration, Hitachi Command Suite services stop. Therefore, do not access Hitachi Command Suite while restoration is in progress.

Before you begin

- Log in as a user with root permissions
- Check the following information:
  - The file name of the script created to register services into a service group
    For details about how to register the Hitachi Command Suite product services to a service group, see *Hitachi Command Suite Installation and Configuration Guide*.

Procedure

1. Remove the Hitachi Command Suite product services from the service group.

   For details, see *Hitachi Command Suite Installation and Configuration Guide*.
2. Confirm that the service group was moved to the executing node.

   If the service group has not been moved, move the service group to the executing node.
3. Execute the `hcmds64dbrepair` command to restore the database.

   installation-directory-for-Hitachi-Command-Suite`/Base64/bin/hcmds64dbrepair -trans` *exported-file*

   `trans`

   Specify the absolute path to the archive file of the database exported via the `hcmds64dbtrans` command.
4. On the executing node and standby node, specify `true` for the `server.base.initialsynchro` property on the Device Manager server.
5. On the executing node and standby node, specify `true` for the `server.base.initialsynchro` property on the Tiered Storage Manager server.
6. Start the Hitachi Command Suite product services.
7. On the executing node and standby node, change the value of the `server.base.initialsynchro` property on the Device Manager server back to `false`.
8. On the executing node and standby node, change the value of the `server.base.initialsynchro` property on the Tiered Storage Manager server back to `false`.
9. Restart the Hitachi Command Suite product services.
10. Re-register the Hitachi Command Suite product services removed in step 1 to the service group.
11. Start the service group to which the Hitachi Command Suite product services were registered.

    For details, see *Hitachi Command Suite Installation and Configuration Guide*.
12. Refresh the storage system from the Device Manager GUI or CLI.
13. If you restored the management server database at the Replication Manager secondary site, refresh the configuration information by using the Replication Manager GUI to synchronize the Replication Manager database at the primary site and the Device Manager database at the secondary site.
14. Check the status of Device Manager tasks from the Device Manager GUI.

If a Device Manager task is not completed or has failed, re-create the task or change the execution schedule of the task as necessary.

15. See the message log of Tiered Storage Manager.

    When Tiered Storage Manager is started for the first time after a database is restored, make sure that the message KATS50354-E is output to a log file. The task IDs of Tiered Storage Manager tasks whose status was changed to **Failure** are output to KATS50354-E.
16. 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.
17. If a Tiered Storage Manager task is not completed, create and execute the task again as necessary.
18. If Tuning Manager is remotely connected, the remote connection setting is re-initialized during a database restoration. Specify the setting again.
19. The password for the `System` account is re-initialized during a database restoration. If necessary, specify the password again.

    For details about how to change the password for the `System` account, see the *Hitachi Command Suite User Guide*.

Related tasks

- Remote connection to the Tuning Manager server (in a Red Hat Enterprise Linux cluster environment) on page 351
- Starting the Hitachi Command Suite services on page 458
- Stopping the Hitachi Command Suite services on page 460

Migrating databases

If you use Hitachi Command Suite products for an extended period of time, you might need a higher performance computer to run an upgraded product or to handle an increased number of managed objects. In such a case, you have to migrate the current databases to your new computer.

You can migrate Hitachi Command Suite product databases by using the `hcmds64dbtrans` command. This command migrates both the data stored in the databases of Hitachi Command Suite products and the user information managed by Common Component.

You can also use the `hcmds64dbtrans` command to migrate a database to a server whose environment differs from the current one. There are the following three cases:

- Migration to a server of a different platform
- Migration to a server on which installation locations for Hitachi Command Suite products differ from the ones on the migration source server

- Migration to a server on which versions of Hitachi Command Suite products are later than the ones on the migration source server

Note: If you are using the Replication tab, note that when you move the management server environment to a new machine, you must perform the procedure for handing over the collected performance information. If you do not perform the procedure correctly, the collected performance information might be lost. For details, see *Hitachi Command Suite Release Notes*.

Prerequisites and restrictions on migrating databases

The following are notes on the databases, product types, versions, and user information of Hitachi Command Suite products on the migration source and destination servers.

Notes on databases, product types, and versions of Hitachi Command Suite products:

- If the following products are installed on the migration source server, before exporting the database, upgrade the products to version 6.0 or later on both the migration source and destination servers:
  Replication Monitor 5.*x* or earlier
  Tuning Manager 5.*x* or earlier
  If these products cannot be upgraded to version 6.0 or later or if migrating the database is not required, remove these products from the products whose databases are to be imported.
- The following restrictions apply when migrating the Tuning Manager database.
  Specify the same capacity for the Tuning Manager database on both the migration source and destination servers. For details about how to change the capacity of the database, see the *Tuning Manager Server Administration Guide*.
  The database can be migrated if the database configuration (Small or Medium) is the same on both the migration source and destination servers, or if the database configuration on the migration destination server is larger than that on the source server.
  On the migration source server, if the number of managed resources exceeds 70% of the number of manageable resources, the database data cannot be migrated to a database that has the same configuration.
- If Global Link Manager is installed on the migration source management server, remove it from the products whose databases are to be imported. If you need it to be migrated, migrate the database by following the manual that corresponds to the version of Global Link Manager that is installed on the migration destination server.

- Databases that are exported from an environment where Device Manager 6.*x* or earlier is installed can be imported to an environment where Device Manager 7.0 or later is installed. This can be done just once, only after Device Manager 7.0 or later is newly installed. After the product is installed and overwritten to version 7.0 or later or when operation has started on the migration destination server, do not import the database of 6.*x* or earlier again.

Notes on user information:

- If there is user information on the migration destination server, this user information will be replaced with the user information from the migration source server. Therefore, do not perform a migration to a server on which user information for Hitachi Command Suite products already exists.
- Do not migrate the databases of Hitachi Command Suite products that were running on different management servers to one management server because user information will be overwritten.

Procedure for migrating databases

Procedure

1. On the migration destination server, install the Hitachi Command Suite products whose databases will be migrated.
2. Export the databases from the migration source server by using the `hcmds64dbtrans` command.
3. Transfer the archive file from the source server to the destination server.
4. Import the databases into the destination server by using the `hcmds64dbtrans` command.

The following sections describe each step.

Installing Hitachi Command Suite products on the migration destination server

On the migration destination server, install the Hitachi Command Suite products whose databases will be migrated. Databases of Hitachi Command Suite products that do not exist on the migration destination server cannot be migrated. Install necessary products on the migration destination server before migration.

The versions of the Hitachi Command Suite products installed on the migration destination server must be the same as or later than the ones on the migration source server. If any of the versions of the Hitachi Command Suite products installed on the migration destination server are earlier than the ones on the migration source server, no databases can be migrated.

Exporting databases on the migration source server (for a non-cluster configuration)

This section explains how to export databases from the migration source server when the management server is not in a cluster configuration.

To export the databases of Hitachi Command Suite products, a directory for temporarily storing the database data and a directory for storing archive files are required. For each directory, ensure that a comparable capacity to the total size of the following directories is available.

- Storage directory of each database for the installed Hitachi Command Suite products
- Storage directory of the Common Component database (excluding the `SYS` directory and its subdirectories)

Caution:

- Databases are exported as archive files. If the capacity of a disk where archive files are created is insufficient, creation of the archive file fails when the database data is exported. In this case, instead of using the archive file, manually transfer the exported database data to the migration destination.
- If Tuning Manager is remotely connected, stop the Tuning Manager services on the computer where the Tuning Manager server is installed. After the database is exported, restart the Tuning Manager services. For details about how to start and stop the Tuning Manager services, see the manual for the installed version of Tuning Manager.
- During database export, Hitachi Command Suite services stop. Therefore, do not access Hitachi Command Suite while the export is in progress.

Procedure

1. Log on to the management server as a user with Administrator permissions or root permissions.
2. Execute the `hcmds64dbtrans` command to export the databases.

   In Windows:

   ```
   installation-folder-for-Hitachi-Command-Suite\Base64\bin
   \hcmds64dbtrans /export /workpath working-folder /file
   archive-file /auto
   ```

   In Linux:

```
installation-directory-for-Hitachi-Command-Suite/
Base64/bin/hcmds64dbtrans -export -workpath working-
directory -file archive-file -auto
```

workpath

Specify the absolute path to the working directory where you want to temporarily store database data. In Linux, do not specify a path that includes a space. Specify a directory on your local disk.

Make sure that no files or subdirectories are in the directory specified for the `workpath` option.

file

Using an absolute path, specify the name of the archive file to be output. In Linux, do not include a space in this path.

auto

Automatically starts or stops Hitachi Command Suite services.

3. Transfer the archive files to the migration destination server.

   If the archive file cannot be created, transfer all the files created in the directory specified by the `workpath` option. In this case, do not change the structure of the files.

Exporting databases on the migration source server (for a Windows cluster configuration)

This section explains how to export the databases on the migration source server when the OS of the management server is in a Windows cluster configuration.

To export the databases of Hitachi Command Suite products, a directory for temporarily storing the database data and a directory for storing archive files are required. For each directory, ensure that a comparable capacity to the total size of the following directories is available.

- Storage directory of each database for the installed Hitachi Command Suite products
- Storage directory of the Common Component database (excluding the `SYS` directory and its subdirectories)

Caution:

- Use the executing node (a machine that has `online` set for `mode` in the `cluster.conf` file) to export databases.
- Databases are exported as archive files. If the capacity of a disk where archive files are created is insufficient, creation of the archive file fails

when the database data is exported. In this case, instead of using the archive file, manually transfer the exported database data to the migration destination.

- If Tuning Manager is remotely connected, stop the Tuning Manager services on the computer where the Tuning Manager server is installed. After the database is exported, restart the Tuning Manager services. For details about how to start and stop the Tuning Manager services, see the manual for the installed version of Tuning Manager.
- During database export, Hitachi Command Suite services stop. Therefore, do not access Hitachi Command Suite while the export is in progress.

Before you begin

Log in as a user with Administrator permissions

Procedure

1. Execute the following command to take the Hitachi Command Suite product services offline.

   installation-folder-of-Hitachi-Command-Suite\Base64\ClusterSetup\hcmds64clustersrvstate /soff /r *resource-group-name*

   soff

   Use this option to suppress failover by taking the following offline: the Hitachi Command Suite product services registered to the resource group of the cluster management application. A group of clustered services (the set of services for which failover is performed) is called a resource group.

   r

   Specify the name of the resource group.

2. Execute the `hcmds64dbtrans` command to export the databases.

   installation-folder-for-Hitachi-Command-Suite\Base64\bin\hcmds64dbtrans /export /workpath *working-folder* /file *archive-file* /auto

   workpath

   Specify the absolute path to the working folder where you want to temporarily store database data. Specify a folder on your local disk. Make sure that no files or subfolders are in the folder specified for the `workpath` option.

   file

Using an absolute path, specify the name of the archive file to be output.

auto

Automatically starts or stops Hitachi Command Suite services.

3. Transfer the archive files to the migration destination server.

   If the archive file cannot be created, transfer all the files created in the folder specified by the `workpath` option. In this case, do not change the structure of the files.
4. Execute the `hcmds64srv` command to stop the Hitachi Command Suite product services.
5. Execute the command below to bring the following online: the resource group of the cluster management application and the Hitachi Command Suite product services.

   installation-folder-of-Hitachi-Command-Suite`\Base64\ClusterSetup\hcmds64clustersrvstate /son /r` *resource-group-name*

   son

   Use this option to enable failover by bringing the following online: the resource group set for the cluster management application.

   r

   Specify the name of the resource group.

Related tasks

- Stopping the Hitachi Command Suite services on page 460

Related references

- Hitachi Command Suite product services that are registered in cluster management applications on page 466

Exporting databases on the migration source server (for a Red Hat Enterprise Linux cluster configuration)

This section explains how to export the databases on the migration source server when the OS of the management server is in a Red Hat Enterprise Linux cluster configuration.

To export the databases of Hitachi Command Suite products, a directory for temporarily storing the database data and a directory for storing archive files are required. For each directory, ensure that a comparable capacity to the total size of the following directories is available.

- Storage directory of each database for the installed Hitachi Command Suite products

- Storage directory of the Common Component database (excluding the `SYS` directory and its subdirectories)

Caution:

- Use the executing node (a machine that has `online` set for `mode` in the `cluster.conf` file) to export databases.
- Databases are exported as archive files. If the capacity of a disk where archive files are created is insufficient, creation of the archive file fails when the database data is exported. In this case, instead of using the archive file, manually transfer the exported database data to the migration destination.
- If Tuning Manager is remotely connected, stop the Tuning Manager services on the computer where the Tuning Manager server is installed. After the database is exported, restart the Tuning Manager services. For details about how to start and stop the Tuning Manager services, see the manual for the installed version of Tuning Manager.
- During database export, Hitachi Command Suite services stop. Therefore, do not access Hitachi Command Suite while the export is in progress.

Before you begin

- Log in as a user with root permissions
- Check the following information:
  - The file name of the script created to register services into a service group
    For details about how to register the Hitachi Command Suite product services to a service group, see *Hitachi Command Suite Installation and Configuration Guide*.

Procedure

1. Remove the Hitachi Command Suite product services from the service group.

   For details, see *Hitachi Command Suite Installation and Configuration Guide*.
2. Confirm that the service group was moved to the executing node.

   If the service group has not been moved, move the service group to the executing node.
3. Execute the `hcmds64dbtrans` command to export the databases.

installation-directory-for-Hitachi-Command-Suite/Base64/bin/hcmds64dbtrans -export -workpath *working-folder* -file *archive-file* -auto

workpath

Specify the absolute path to the working directory where you want to temporarily store database data. Specify a directory on your local disk. Make sure that no files or subdirectories are in the directory specified for the `workpath` option.

file

Using an absolute path, specify the name of the archive file to be output.

auto

Automatically starts or stops Hitachi Command Suite services.

4. Transfer the archive files to the migration destination server.

   If the archive file cannot be created, transfer all the files created in the folder specified by the `workpath` option. In this case, do not change the structure of the files.
5. Execute the `hcmds64srv` command to stop the Hitachi Command Suite product services.
6. Re-register the Hitachi Command Suite product services removed in step 1 to the service group.
7. Start the service group to which the Hitachi Command Suite product services were registered.

   For details, see *Hitachi Command Suite Installation and Configuration Guide*.

Related tasks

- Stopping the Hitachi Command Suite services on page 460

Importing databases on the migration destination server (for a non-cluster configuration)

This section explains how to import databases to the migration destination server when the management server is not in a cluster configuration.

Caution:

- If Tuning Manager is remotely connected, stop the Tuning Manager services on the computer where the Tuning Manager server is installed. After the database is imported, restart the Tuning Manager services. For details about how to start and stop the Tuning Manager services, see the manual for the installed version of Tuning Manager.

If Tuning Manager is remotely connected and was using the Alert function of Tuning Manager, you need to import the database, and then synchronize the alert definition information. For details about synchronizing alert definition information, see the *Hitachi Command Suite Tuning Manager API Reference Guide*.

- During database import, Hitachi Command Suite services stop. Therefore, do not access Hitachi Command Suite while the import is in progress.

Procedure

1. Log on to the management server as a user with Administrator permissions or root permissions.
2. If you specified a value other than the default value for a property on the migration source management server, check and review the property value set on the migration destination server as required.

   The property file will not be migrated to the migration destination server even if the database is imported.
3. Execute the `hcmds64dbtrans` command to import the databases.

   In Windows:

   installation-folder-for-Hitachi-Command-Suite\Base64\bin\hcmds64dbtrans /import /workpath *working-folder* [/file *archive-file*] /type {ALL|*name-of-Hitachi-Command-Suite-product-whose-database-is-to-be-migrated*} /auto

   In Linux:

   installation-directory-for-Hitachi-Command-Suite/Base64/bin/hcmds64dbtrans -import -workpath *working-directory* [-file *archive-file*] -type {ALL|*name-of-Hitachi-Command-Suite-product-whose-database-is-to-be-migrated*} -auto

   workpath

   When using the archive file for the import:

   Specify the absolute path to the directory used to extract the archive file. In Linux, do not specify a path that includes a space. Specify a directory on your local disk. If you want to use the archive file, the `file` option must be specified.

   Make sure that no files or subdirectories are in the directory specified for the `workpath` option.

   When not using the archive file for the import:

Specify the directory that stores the database data files transferred from the migration source server. Do not change the structure of those files in the transferred directory. Also, do not specify the `file` option.

`file`

Specify the absolute path to the archive file of the databases transferred from the migration source server. In Linux, do not specify a path that includes a space. If the database data files transferred from the migration source server are stored in the directory specified by `workpath`, you do not need to specify this option.

`type`

As a rule, specify `ALL`. If you specify `ALL`, the databases of Hitachi Command Suite products that are installed on the migration destination server are automatically selected and migrated.

When migrating the database of only a specific Hitachi Command Suite product because of the difference in program configurations of management servers, specify the name of the product to be migrated as listed in the following table. To specify multiple product names, use a comma to separate the names.

You can use the `type` option to migrate databases only if the database data of all the specified products is contained in the archive file or in the directory specified by the `workpath` option, and all the specified products exist on the migration destination server. If any of the products do not meet the above conditions, data cannot be migrated.

Table 84 Values to specify for the type option when migrating databases (In a non-cluster configuration)

Product	Value
Device Manager#1#2	`DeviceManager`
Tiered Storage Manager#1	`TieredStorageManager`
Replication Manager#2	`ReplicationManager`
Other products	Refer to the manual for each product.

#1: When importing databases that were exported from an environment of version 7.0 or later, regardless of whether you have registered a Tiered Storage Manager license, import both the Device Manager and Tiered Storage Manager databases at the same time.

#2: To import the Replication Manager database, you must also import the Device Manager database at the same time.

`auto`

Automatically starts or stops Hitachi Command Suite services.

4. Specify `true` for the `server.base.initialsynchro` property on the Device Manager server.

   Because, other than user information, the `hcmds64dbtrans` command does not migrate the Common Component repository, you need to synchronize the repository information with the imported Device Manager database data.
5. Specify `true` for the `server.base.initialsynchro` property on the Tiered Storage Manager server.
6. If Tuning Manager is remotely connected, the remote connection setting is re-initialized during a database import. Execute the `htmsetup` command to specify the setting again.
7. Start the Hitachi Command Suite product services on the migration destination server as follows.
8. Change the value of the `server.base.initialsynchro` property on the Device Manager server back to `false`.
9. Change the value of the `server.base.initialsynchro` property on the Tiered Storage Manager server back to `false`.
10. In the following cases, use the Device Manager GUI or CLI to refresh the storage systems:
    - If the configuration of the storage system was changed between the time databases were exported and the time they were imported:
      Refresh the storage system whose configuration was changed.
    - If the versions of Hitachi Command Suite products that are installed on the migration source and destination management servers are different:
      Refresh all the storage systems that are registered in Device Manager.
11. If you imported the management server database at the Replication Manager secondary site, refresh the configuration information by using the Replication Manager GUI to synchronize the Replication Manager database at the primary site and the Device Manager database at the secondary site.
12. Back up the databases.

    After resuming operations, you cannot import the archive file that was exported in version 6.4 or earlier. In preparation for a failure, we recommend that you back up the databases immediately after importing them.

Related tasks

- Starting the Hitachi Command Suite services on page 458
- Backing up a database in non-cluster configuration on page 471

Related references

- Specifying the settings for remote connection to the Tuning Manager server and the port number (htmsetup command) on page 352

Importing databases on the migration destination server (for a Windows cluster configuration)

This section explains how to import the databases on the migration destination server when the OS of the management server is in a Windows cluster configuration.

Caution:

- Use the executing node (a machine that has `online` set for `mode` in the `cluster.conf` file) to import databases.
- If Tuning Manager is remotely connected, stop the Tuning Manager services on the computer where the Tuning Manager server is installed. After the database is imported, restart the Tuning Manager services. For details about how to start and stop the Tuning Manager services, see the manual for the installed version of Tuning Manager.
  If Tuning Manager is remotely connected and was using the Alert function of Tuning Manager, you need to import the database, and then synchronize the alert definition information. For details about synchronizing alert definition information, see the *Hitachi Command Suite Tuning Manager API Reference Guide*.
- During database import, Hitachi Command Suite services stop. Therefore, do not access Hitachi Command Suite while the import is in progress.

Before you begin

- Log in as a user with Administrator permissions
- Revise the setting value of the property file (for executing and the standby nodes of the migration destination).
  The property file will not be migrated to the migration destination server even if the database is imported. Therefore, if a value other than the default was specified for the property in the management server of the migration source, revise the value as necessary.

Procedure

1. Execute the following command to take the Hitachi Command Suite product services offline.

   ```
   installation-folder-of-Hitachi-Command-Suite
   \Base64\ClusterSetup\hcmds64clustersrvstate /soff /r resource-
   group-name
   ```

soff

Use this option to suppress failover by taking the following offline: the Hitachi Command Suite product services registered to the resource group of the cluster management application. A group of clustered services (the set of services for which failover is performed) is called a resource group.

r

Specify the name of the resource group.

2. Execute the `hcmds64dbtrans` command to import the databases.

installation-folder-for-Hitachi-Command-Suite\Base64\bin\hcmds64dbtrans /import /workpath *working-folder* [/file *archive-file*] /type {ALL|*name-of-Hitachi-Command-Suite-product-whose-database-is-to-be-migrated*} /auto

workpath

When using the archive file for the import:

Specify the absolute path to the folder used to extract the archive file. Specify a folder on your local disk. If you want to use the archive file, the `file` option must be specified.

Make sure that no files or subdirectories are in the folder specified for the `workpath` option.

When not using the archive file for the import:

Specify the folder that stores the database data files transferred from the migration source server. Do not change the structure of those files in the transferred directory. Also, do not specify the `file` option.

file

Specify the absolute path to the archive file of the databases transferred from the migration source server. If the database data files transferred from the migration source server are stored in the folder specified by `workpath`, you do not need to specify this option.

type

As a rule, specify `ALL`. If you specify `ALL`, the databases of Hitachi Command Suite products that are installed on the migration destination server are automatically selected and migrated.

When migrating the database of only a specific Hitachi Command Suite product because of the difference in program configurations of management servers, specify the name of the product to be

migrated as listed in the following table. To specify multiple product names, use a comma to separate the names.

You can use the `type` option to migrate databases only if the database data of all the specified products is contained in the archive file or in the folder specified by the `workpath` option, and all the specified products exist on the migration destination server. If any of the products do not meet the above conditions, data cannot be migrated.

Table 85 Values to specify for the type option when migrating databases (For a Windows cluster configuration)

Product	Value
Device Manager#1#2	`DeviceManager`
Tiered Storage Manager#1	`TieredStorageManager`
Replication Manager#2	`ReplicationManager`
Other products	Refer to the manual for each product.

#1: When importing databases that were exported from an environment of version 7.0 or later, regardless of whether you have registered a Tiered Storage Manager license, import both the Device Manager and Tiered Storage Manager databases at the same time.

#2: To import the Replication Manager database, you must also import the Device Manager database at the same time.

auto

Automatically starts or stops Hitachi Command Suite services.

3. On the executing node and standby node, specify `true` for the `server.base.initialsynchro` property of the Device Manager server. Because, other than user information, the `hcmds64dbtrans` command does not migrate the Common Component repository, you need to synchronize the repository information with the imported Device Manager database data.
4. On the executing node and standby node, specify `true` for the `server.base.initialsynchro` of the Tiered Storage Manager server.
5. Execute the command below to bring the following online: the resource group of the cluster management application and the Hitachi Command Suite product services.

   installation-folder-of-Hitachi-Command-Suite`\Base64\ClusterSetup\hcmds64clustersrvstate /son /r` *resource-group-name*

   son

Use this option to enable failover by bringing the following online: the resource group set for the cluster management application.

r

Specify the name of the resource group.

6. On the executing node and standby node, change the value of the `server.base.initialsynchro` property of the Device Manager server back to `false`.
7. On the executing node and standby node, change the value of the `server.base.initialsynchro` property of the Tiered Storage Manager server back to `false`.
8. In the following cases, use the Device Manager GUI or CLI to refresh the storage systems:
   - If the configuration of the storage system was changed between the time databases were exported and the time they were imported:
     Refresh the storage system whose configuration was changed.
   - If the versions of Hitachi Command Suite products that are installed on the migration source and destination management servers are different:
     Refresh all the storage systems that are registered in Device Manager.
9. If you imported the management server database at the Replication Manager secondary site, refresh the configuration information by using the Replication Manager GUI to synchronize the Replication Manager database at the primary site and the Device Manager database at the secondary site.
10. Back up the databases.
11. If Tuning Manager is remotely connected, the remote connection setting is re-initialized during a database import. Specify the setting again.

Related tasks

- Remote connection to the Tuning Manager server (in a Windows cluster environment) on page 349
- Starting the Hitachi Command Suite services on page 458
- Backing up a database in a Windows cluster configuration on page 472

Related references

- Hitachi Command Suite product services that are registered in cluster management applications on page 466

Importing databases on the migration destination server (for a Red Hat Enterprise Linux cluster configuration)

This section explains how to import the databases on the migration destination server when the OS of the management server is in a Red Hat Enterprise Linux cluster configuration.

Caution:

- Use the executing node (a machine that has `online` set for `mode` in the `cluster.conf` file) to import databases.
- If Tuning Manager is remotely connected, stop the Tuning Manager services on the computer where the Tuning Manager server is installed. After the database is imported, restart the Tuning Manager services. For details about how to start and stop the Tuning Manager services, see the manual for the installed version of Tuning Manager.
  If Tuning Manager is remotely connected and was using the Alert function of Tuning Manager, you need to import the database, and then synchronize the alert definition information. For details about synchronizing alert definition information, see the *Hitachi Command Suite Tuning Manager API Reference Guide*.
- During database import, Hitachi Command Suite services stop. Therefore, do not access Hitachi Command Suite while the import is in progress.

Before you begin

- Log in as a user with root permissions
- Revise the setting value of the property file (for executing and the standby nodes of the migration destination).
  The property file will not be migrated to the migration destination server even if the database is imported. Therefore, if a value other than the default was specified for the property in the management server of the migration source, revise the value as necessary.
- Check the following information:
  - The file name of the script created to register services into a service group
    For details about how to register the Hitachi Command Suite product services to a service group, see *Hitachi Command Suite Installation and Configuration Guide*.

Procedure

1. Remove the Hitachi Command Suite product services from the service group.

   For details, see *Hitachi Command Suite Installation and Configuration Guide*.
2. Confirm that the service group was moved to the executing node.

   If the service group has not been moved, move the service group to the executing node.

3. Execute the `hcmds64dbtrans` command to import the databases.

   installation-directory-for-Hitachi-Command-Suite`/Base64/bin/hcmds64dbtrans -import -workpath` *working-directory* `[-file` *archive-file*`] -type {ALL|`*name-of-Hitachi-Command-Suite-product-whose-database-is-to-be-migrated*`} -auto`

   workpath

   When using the archive file for the import:

   Specify the absolute path to the directory used to extract the archive file. Specify a directory on your local disk. If you want to use the archive file, the `file` option must be specified.

   Make sure that no files or subdirectories are in the directory specified for the `workpath` option.

   When not using the archive file for the import:

   Specify the directory that stores the database data files transferred from the migration source server. Do not change the structure of those files in the transferred directory. Also, do not specify the `file` option.

   file

   Specify the absolute path to the archive file of the databases transferred from the migration source server. If the database data files transferred from the migration source server are stored in the directory specified by `workpath`, you do not need to specify this option.

   type

   As a rule, specify `ALL`. If you specify `ALL`, the databases of Hitachi Command Suite products that are installed on the migration destination server are automatically selected and migrated.

   When migrating the database of only a specific Hitachi Command Suite product because of the difference in program configurations of management servers, specify the name of the product to be migrated as listed in the following table. To specify multiple product names, use a comma to separate the names.

   You can use the `type` option to migrate databases only if the database data of all the specified products is contained in the archive file or in the directory specified by the `workpath` option, and all the specified products exist on the migration destination server. If any of the products do not meet the above conditions, data cannot be migrated.

Table 86 Values to specify for the type option when migrating databases (For a Red Hat Enterprise Linux cluster configuration)

Product	Value
Device Manager#1#2	`DeviceManager`
Tiered Storage Manager#1	`TieredStorageManager`
Replication Manager#2	`ReplicationManager`
Other products	Refer to the manual for each product.

#1: When importing databases that were exported from an environment of version 7.0 or later, regardless of whether you have registered a Tiered Storage Manager license, import both the Device Manager and Tiered Storage Manager databases at the same time.

#2: To import the Replication Manager database, you must also import the Device Manager database at the same time.

`auto`

Automatically starts or stops Hitachi Command Suite services.

4. On the executing node and standby node, specify `true` for the `server.base.initialsynchro` property of the Device Manager server. Because, other than user information, the `hcmds64dbtrans` command does not migrate the Common Component repository, you need to synchronize the repository information with the imported Device Manager database data.
5. On the executing node and standby node, specify `true` for the `server.base.initialsynchro` of the Tiered Storage Manager server.
6. Start the Hitachi Command Suite product services.
7. On the executing node and standby node, change the value of the `server.base.initialsynchro` property of the Device Manager server back to `false`.
8. On the executing node and standby node, change the value of the `server.base.initialsynchro` property of the Tiered Storage Manager server back to `false`.
9. Restart the Hitachi Command Suite product services.
10. Re-register the Hitachi Command Suite product services removed in step 1 to the service group.
11. Start the service group to which the Hitachi Command Suite product services were registered.

    For details, see *Hitachi Command Suite Installation and Configuration Guide*.
12. In the following cases, use the Device Manager GUI or CLI to refresh the storage systems:

- If the configuration of the storage system was changed between the time databases were exported and the time they were imported:
  Refresh the storage system whose configuration was changed.
- If the versions of Hitachi Command Suite products that are installed on the migration source and destination management servers are different:
  Refresh all the storage systems that are registered in Device Manager.

13. If you imported the management server database at the Replication Manager secondary site, refresh the configuration information by using the Replication Manager GUI to synchronize the Replication Manager database at the primary site and the Device Manager database at the secondary site.
14. Back up the databases.
15. If Tuning Manager is remotely connected, the remote connection setting is re-initialized during a database import. Specify the setting again.

Related tasks

- Remote connection to the Tuning Manager server (in a Red Hat Enterprise Linux cluster environment) on page 351
- Starting the Hitachi Command Suite services on page 458
- Stopping the Hitachi Command Suite services on page 460
- Backing up a database in a Red Hat Enterprise Linux cluster configuration on page 474

11

Using the Device Manager agent

This chapter explains the settings that must be specified to run the Device Manager agent. This chapter also explains Device Manager agent operations.

- Prerequisites for running the Device Manager agent
- Specifying the Device Manager agent environment settings
- Device Manager agent operations
- Configuration definition file for managing copy pairs

Prerequisites for running the Device Manager agent

This section provides the prerequisites for running the Device Manager agent. This section also provides notes on using the Device Manager agent.

Note:

- If the host OS is Linux and you want to use the Device-Mapper Multipath feature (DM-Multipath), to set the alias for a multipath device for the `alias` attribute in the `multipaths` section of the `/etc/multipath.conf` file, use the following characters:

  `A` to `Z`

  `a` to `z`

  `0` to `9`

  `- _ . @`
- If you use the Device Manager agent to register Linux hosts that recognize 256 or more logical unit numbers in a storage system, the KAIC03006-E error message is output and the operation fails. For Linux hosts managed by the Device Manager agent, specify a value of 256 or less as the number of LUs per port of storage systems recognized by a host. Specify a logical unit number in the range from 0 to 255.
- For Solaris hosts with the Solaris multi-pathing feature (MPxIO) enabled that are managed by the Device Manager agent, specify a logical unit number for storage systems recognized by a host in the range from 0 to 255. If the logical unit number is 256 or more, the following problems occur:

  - The information of the LDEVs whose logical unit number is 256 or more is not collected.

  - When the logical unit number of the command device is 256 or more, if you perform an operation related to the copy-pair configuration definition by using Replication Manager, the operation fails and the error message KAVN00451-E is output.

Prerequisites for using the Device Manager agent to manage normal hosts

To use the Device Manager agent to manage normal hosts, you need to install the Device Manager agent on each normal host and set information such as the management server information and the execution cycle of the `HiScan` command.

For details on how to set up Device Manager agent, see the *Hitachi Command Suite Installation and Configuration Guide*.

In addition, on normal hosts running the AIX OS, set the `ODMDIR` environment variable.

Note: Do not use a name that contains a semicolon (;) for the following host items:

- If managing a Windows host:
  - Network connection name
  - Comment field for the shared disk
- If managing a UNIX host:
  - Mount-destination directory name
  - Disk group name (volume group name and disk set name)
  - Logical volume name
  - Network name
  - Shared disk directory name
  - Device name of the network drive (directory name of the shared disk that has been set up on the reference destination host)

Prerequisites for using the Device Manager agent to manage virtual machines

To use the Device Manager agent to manage virtual machines, install the Device Manager agent on each virtual machine. After installation, specify the environment settings such as the management server information and the execution interval of the `HiScan` command.

The following three configurations are available for each method for allocating HBA to a virtual machine. The prerequisite environment differs depending on the configuration.

- A configuration where a virtual HBA is allocated to each virtual machine (if an NPIV HBA is used) (recommended)
- A configuration where an HBA is allocated for each virtual machine
- A configuration where an HBA is shared among multiple virtual machines

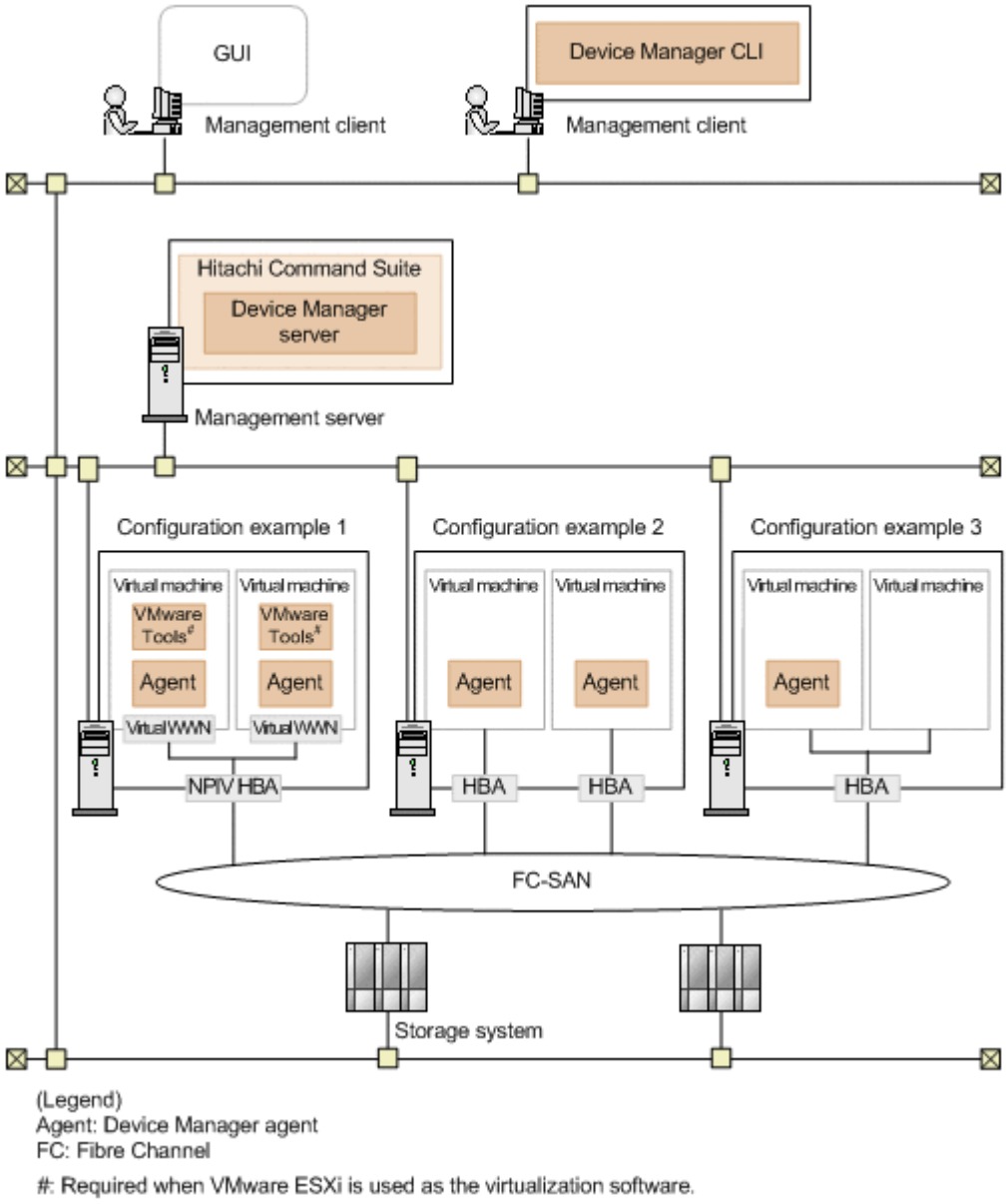


Figure 61 Environment settings on virtual machines (when the Device Manager agent is used for management)

If a virtual HBA is allocated to each virtual machine (if an NPIV HBA is used) (recommended): Configuration example 1 in the figure

The Device Manager agent is installed and managed in each virtual machine as an independent HBA configuration.

- Install a Device Manager agent on each virtual machine.
- When VMware ESXi is used as the virtualization software, install a VMware Tools on each virtual machine.
- Register the virtualization server that runs in the same physical environment in Device Manager.

- For virtual machines running the AIX OS, set the `ODMDIR` environment variable.

For details on how to set up Device Manager agent, see the *Hitachi Command Suite Installation and Configuration Guide*.

If an HBA is allocated for each virtual machine: Configuration example 2 in the figure

The Device Manager agent is installed and managed in each virtual machine in which an HBA is allocated.

- Install a Device Manager agent on each virtual machine.
- Do not register a virtualization server that operates on the same physical environment as Device Manager.
- For virtual machines running the AIX OS, set the `ODMDIR` environment variable.

For details on how to set up Device Manager agent, see the *Hitachi Command Suite Installation and Configuration Guide*.

If an HBA is shared by multiple virtual machines: Configuration example 3 in the figure

The Device Manager agent is installed and managed on only one virtual machine.

- The Device Manager agent cannot be installed on each virtual machine.
- Do not register a virtualization server that operates on the same physical environment as Device Manager.
- For virtual machines running the AIX OS, set the `ODMDIR` environment variable.

For details on how to set up Device Manager agent, see the *Hitachi Command Suite Installation and Configuration Guide*.

Prerequisites for using a host on which multiple NICs are installed

You must perform the following before running the Device Manager agent on a host on which multiple NICs are installed:

- Open the `server.properties` file of the Device Manager agent, and then set the `server.http.socket.agentAddress` property to the IP address of the NIC that is used by the Device Manager agent.
- If the OSs of the host that recognizes the P-VOL and the host that recognizes the S-VOL are Windows, check and, if necessary, revise the priority of NICs on each of the hosts so that the IP address assigned to the priority NIC of the local host matches the IP address obtained when the host name of the local host is resolved from the remote host. In an environment in which name resolution cannot be performed, an error might occur when an operation is performed on copy pairs from the Device Manager CLI or from Replication Manager.

To change the priority of NICs:

1. From Control Panel, click Network and Sharing Center, and then click Change adapter settings.
2. From the Advanced menu, click Advanced Settings, and then click the Adapters and Bindings tab to change the priority of NICs.
   If the Advanced menu is not displayed, press the **Alt** key to display the menu bar and then perform the above operation.

Related tasks

- Changing Device Manager agent properties on page 670

Related references

- server.http.socket.agentAddress on page 680

Notes on running the Device Manager agent

The following notes apply when running the Device Manager agent.

- If you have installed the Device Manager agent and then upgraded the host OS under any of the following conditions, perform an overwrite installation of the Device Manager agent:
  - Upgrading Solaris from a version earlier than 10 to version 10 or later
  - Upgrading AIX from a version earlier than 6.1 to version 6.1 or later
- If the OS of the host is Windows, the Device Manager agent will not acquire data from devices assigned the drive letter A or B. Assign a drive letter from C to Z for a device managed by the Device Manager agent.
- If you change a device file name by using the `rendev` command on a host whose OS is AIX 7.1 or AIX 6.1 TL6 or later, the new device name must be specified by using printable ASCII characters only. If a character other than a printable ASCII character is included in the name, the Device Manager agent will not work properly.
- To execute Device Manager agent commands other than `hdvm_info`, you must be a member of the Administrators group or a superuser.
- When using one of the following OSs on the host, execute Device Manager agent commands from the WOW64 command prompt:
  Windows Server 2008 (x64 and IPF)
  Windows Server 2008 R2 (x64 and IPF)
  Windows Server 2012 (x64)
  Windows Server 2012 R2 (x64)
  The following shows an example of executing from the command prompt:
  `C:\WINDOWS\SysWOW64\cmd.exe`
- In Windows, the folder in which the Device Manager agent commands are installed is automatically added to the environment variable `PATH`. When you execute a command, you do not need to change the current folder to the folder that contains commands.

Specifying the Device Manager agent environment settings

Before you can start running the Device Manager agent, you must specify the necessary environment settings.

Specify the following settings as necessary:

- Settings for changing the Java execution environment (Windows or Linux)
  You must specify these settings if you change the Java execution environment used by the Device Manager agent.
- Registering firewall exceptions (Windows)
  You must specify these settings if you enable Windows Firewall after the Device Manager agent has been installed or if you change the port used by the Device Manager agent.
- Registering a Java process in SED as an exception (AIX)
  You must perform this registration if you change the SED mode to `all` after the Device Manager agent has been installed.
- Settings for managing copy pairs
  You must specify these settings if you use Device Manager or Replication Manager to manage copy pairs.
- Settings required when 100 or more LUs are managed for a host
  You must specify these settings if a host recognizes 100 or more LUs that are managed by Device Manager.
- Settings for changing the user of the Device Manager agent service (Windows)
  You must specify these settings to change the user of the Device Manager agent service to an Administrators group member to enable operations on HORCM instances activated by the Device Manager agent (default: `LocalSystem`).

If the following settings were not specified during a new installation of the Device Manager agent, execute the `hdvmagt_setting` command to specify the required settings.

- Settings for Device Manager server information (required)
- Settings for the interval for reporting host information to the Device Manager server (optional)
- Settings for using CCI information (optional)

Settings for changing the Java execution environment (javapath_setup command)

If the OS of the host is Windows or Linux, execute the `javapath_setup` command to change the Java execution environment used by the Device Manager agent.

Operations to complete in advance

- Check the Java execution environment required for a Device Manager agent.
  For details, see *Hitachi Command Suite System Requirements*.
- Log in as a user with Administrator permissions (for Windows) or as a root user (for Linux).
- Install the Jurisdiction Policy files (when security communication is established between a Device Manager server and Device Manager agent).
  You need to download and install the Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files for the version of the Java execution environment to be used.
  Download the Jurisdiction Policy files from the Website of Oracle corporation or IBM corporation. For details about how to install the files, see the documentation provided with the Jurisdiction Policy files.

Information to collect in advance

Installation path of the Java execution environment to be used (if you are using a specific Java execution environment).

Command format

```
javapath_setup {-set [new|bundle|Java-execution-environment-installation-path]|-check}
```

Location of the command

In Windows:

installation-folder-for-Device-Manager-agent\bin

In Linux:

installation-directory-for-Device-Manager-agent/bin

Options

-set

Specify this option to switch the Java execution environment. If you do not specify an argument for this option, the command assumes that you have specified `new` as an argument.

- `new`
  Specify this argument to select the latest version of the Java execution environment from Oracle JDK and Oracle JRE installed on the host.
  If the versions of the installed JDK and JRE are the same, the JDK takes precedence.
- `bundle`

Specify this argument to select the Java execution environment bundled with the Device Manager agent.

- *Java-execution-environment-installation-path*
  If you want to use a specific Java execution environment, specify the absolute path of the installation path.

-check

Specify this option to check the latest version of the Java execution environment from Oracle JDK and Oracle JRE installed on the host.

Caution:

- After you execute this command, you must restart the Device Manager agent service.
- In the following cases, use a 32-bit Java execution environment:
  - If the host OS is Windows
  - If the host OS is Linux, and performance information about Virtual Storage Platform or Universal Storage Platform V/VM storage systems is acquired by using the CIM/WBEM function

  If the host OS is Red Hat Enterprise Linux 7 or later, Oracle Linux 7 or later, or SUSE Linux Enterprise Server 12 or later, use a 64-bit Java execution environment.
- For details on Java execution environments that can be specified when Dynamic Link Manager is installed on the host, see the Dynamic Link Manager documentation.
- After upgrading from version 7.0.1 or earlier, if you changed the Java execution environment from the JRE bundled with the Device Manager agent to Oracle JDK or Oracle JRE, you need to register the Device Manager agent as an exception with the Windows firewall.

Related references

- Registering the Windows Firewall exceptions for Device Manager agent (firewall_setup command) on page 519
- Starting and stopping the Device Manager agent service, and checking the operating status of the service (hbsasrv command) on page 528

Registering the Windows Firewall exceptions for Device Manager agent (firewall_setup command)

Use the `firewall_setup` command to add ports used by the Device Manager agent to the Windows Firewall exceptions list.

A firewall exception is registered for the ports set for the following Device Manager agent properties:

- Port set for the `server.agent.port` property (default: 24041/tcp)
- Port set for the `server.http.port` property (default: 24042/tcp)
- Port set for the `server.http.localPort` property (default: 24043/tcp)

Operations to complete in advance

Log in as a user with Administrator permissions.

Command format

```
firewall_setup {-set|-unset}
```

Location of the command

installation-folder-for-Device-Manager-agent\bin

Options

-set

Adds firewall exceptions.

-unset

Removes firewall exceptions.

Related references

- server.agent.port on page 679
- server.http.localPort on page 679
- server.http.port on page 679

Registering a Java process in SED as an exception (AIX)

If the OS of the host is AIX and you change the SED mode to `all` after installing the Device Manager agent, you must execute the `sedmgr` command to register the Java process used by the Device Manager agent in SED as an exception.

Before you begin

Check the following information:

- Installation path for the Java execution environment used by the Device Manager agent
  You can check this information with the `server.agent.JRE.location` property in the `server.properties` file of the Device Manager agent.

Procedure

1. Execute the following command to register the Java process to be used by the Device Manager agent as an SED exception:

   ```
   # sedmgr -c exempt Java-execution-environment-installation-path/bin/java
   ```

   If this command execution succeeds, no execution results are output.

2. Execute the following command to ensure that the Java process to be used by the Device Manager agent has been registered as an SED exception:

   ```
   # sedmgr -d Java-execution-environment-installation-path/bin/java
   ```

   If the Java process has been registered as an SED exception, the following information will be displayed:

   ```
   Java-execution-environment-installation-path/bin/java : exempt
   ```

3. Restart the host.

Related references

- server.agent.JRE.location on page 682

Managing copy pairs

If you use Device Manager or Replication Manager to manage copy pairs, depending on the environment, you must change property settings on the Device Manager agent or the Replication Manager server.

- If CCI is installed in a location other than the default location, or if the host OS is Windows and the CCI installation drive is different from the Device Manager agent installation drive:
  For the `server.agent.rm.location` property in the `server.properties` file of the Device Manager agent, set the installation directory of CCI.
- If you want to centrally manage copy pairs in the storage system managed by the Device Manager server from the management target host:
  For the `server.agent.rm.centralizePairConfiguration` property in the `server.properties` file of the Device Manager agent, set `enable`.

  Caution: To create or add a copy pair definition for a mainframe volume to the configuration definition file, the copy pair management method must be central management.

- If the host that recognizes copy pairs is a virtual machine:
  For the `server.agent.rm.ignorePairStatus` property in the `server.properties` file of the Device Manager agent, set `true`.

  Caution: If you want to check the latest copy pair information by using the GUI or CLI, take either of the following actions depending on the copy pair management method.

  If central management is used: Refresh the pair management server.

  If copy pairs are managed at each host: Refresh the storage systems.

- To use an SVP as a virtual command device to manage copy pairs defined as a device group:
  When P-VOLs and S-VOLs are assigned to the management server, the following property must be set:
  For the `server.agent.rm.ignorePairStatus` property in the `server.properties` file of the Device Manager agent, set `true`.
  To check the latest copy pair information via the GUI or CLI, refresh the storage systems.
- If copy pairs are managed that have been defined by using a device group or a virtual command device
  Because responses to CCI commands take more time than when managing copy pairs in a configuration using physical command devices, processing by the Device Manager agent might terminate in an error. We recommend that you change the following property values in advance:
  - `server.agent.rm.moduleTimeOut` property in the `server.properties` file of the Device Manager agent
    Set the value to `1800` or greater.
  - `agent.rm.TimeOut` property in the `agent.properties` file of the Device Manager agent
    Set the value to `1800` or greater.
  - `hdvmagtif.MaxPollingCount` property in the `agentif.properties` file of the Replication Manager server
    Set the value to `100`.
  - `hdvmagtif.PollingInterval` property in the `agentif.properties` file of the Replication Manager server
    Set the value to `60` or greater.

  For details about the `hdvmagtif.MaxPollingCount` property and the `hdvmagtif.PollingInterval` property in the Replication Manager server `agentif.properties` file, see the *Replication Manager Configuration Guide*.

- If you want to unify the coding format of pair volume information into the `HORCM_DEV` or `HORCM_LDEV` format when creating pairs:
  For the `server.agent.rm.pairDefinitionForm` property in the `server.properties` file of the Device Manager agent, set `HORCM_DEV` or `HORCM_LDEV`.

Caution: If a HUS100, Hitachi AMS2000, Hitachi SMS, or Hitachi AMS/WMS storage system manages copy pairs, and pair volume information is written in `HORCM_DEV` format, the following operations might take a long time:

- Refreshing hosts
- Refreshing storage systems

In this case, we recommend that you change the format of pair volume information to `HORCM_LDEV`. Note that before you change to the `HORCM_LDEV` format, CCI 01-17-03/04 or later needs to be installed.

- If you want to exclude pair volume that is already managed by CCI from Device Manager operations
  For the `server.agent.rm.exclusion.instance` property in the `server.properties` file of the Device Manager agent, set the instance number of CCI that you want to exclude from Device Manager operations.
- If you want to optimize a user-created CCI configuration definition file so that it can be used in Device Manager
  For the `server.agent.rm.optimization.userHorcmFile` property in the `server.properties` file of the Device Manager agent, set `true`.
- If the host (pair management server) has multiple IP addresses
  For the `server.http.socket.agentAddress` property in the `server.properties` file of the Device Manager agent, set the IP address that the Device Manager agent notifies the Device Manager server of.

In addition, to use Replication Manager to manage copy pairs, you need to specify the properties below. If the properties are not set to appropriate values, the memory heap size might be insufficient or a timeout might occur during the Replication Manager processing.

- `agent.rm.TimeOut` property in the `agent.properties` file of the Device Manager agent
  Adjust this value as necessary, while running Replication Manager and checking for timeouts during processing.
- `server.agent.maxMemorySize` property in the `server.properties` file of the Device Manager agent
  Specify a value based on the number of pairs managed by a host (pair management server). By default, the heap runs in a 64 MB memory area. If the number of managed pairs exceeds 5,000, increase the memory heap size by 64 MB, and increase by another 64 MB for every 2,500 pairs above that. For example, if a host manages 6,000 pairs, set the `server.agent.maxMemorySize` property to `128`. Also, if a host manages the configuration definition files for both a primary and secondary site, specify a value based on having twice as many managed pairs.

Related tasks

- Changing Device Manager agent properties on page 670

Related references

- agent.rm.TimeOut on page 671
- server.http.socket.agentAddress on page 680
- server.agent.maxMemorySize on page 681

- server.agent.rm.centralizePairConfiguration on page 684
- server.agent.rm.exclusion.instance on page 685
- server.agent.rm.location on page 685
- server.agent.rm.optimization.userHorcmFile on page 685
- server.agent.rm.pairDefinitionForm on page 687
- server.agent.rm.ignorePairStatus on page 689
- server.agent.rm.moduleTimeOut on page 690

Settings required for a host to manage 100 or more LUs

If you want a host to manage 100 or more LUs, you must change the property settings (such as the length of data that can be received by the Device Manager server and the timeout value for the Device Manager agent) according to the number of LUs to be managed.

You must change the properties below. Note that the values set for these items differ depending on whether the host is using a volume manager.

- The maximum length of data that can be received by the Device Manager server
  `server.http.entity.maxLength` property in the `server.properties` file of the Device Manager server
- The timeout value for the processing to register information in a server
  `server.http.server.timeOut` property and
  `server.util.processTimeOut` property in the `server.properties` file of the Device Manager server
- The memory heap size
  `server.agent.maxMemorySize` property in the `server.properties` property file of the Device Manager agent

Note:

- Depending on the environment, this issue might not be solved by setting the guide values. Make sure that you adjust the values to suit your environment.
- In the following cases, set a value two to three times larger than the guide value.
  When executing the `HiScan` command shortly after restarting the Device Manager agent.
  When executing the `hldutil` command and `HiScan` command at the same time.
  When executing multiple `HiScan` commands at the same time.

When the host is not using a volume manager

The following table lists the recommended property values for hosts that do not use a volume manager.

Table 87 Recommended property values for a host that will manage 100 or more LUs (when the host is not using a volume manager)

Number of LUs managed by Device Manager, and recognized by the host	server.http.entity.maxLength (units: bytes)	server.http.server.timeOut (units: seconds)	server.util.processTimeOut (units: milliseconds)
100	131,072 or more	600 (Default value)	600,000 (Default value)
256	153,600 or more	600	600,000
512	307,200 or more	600	600,000
1,024	614,400 or more	1,200	1,200,000

When the host is using a volume manager

Table 88 Recommended property values for a host that will manage 100 or more LUs (when the host is using a volume manager in Windows) on page 525 through Table 92 Recommended property values for a host that will manage 100 or more LUs (when the host is using a volume manager in HP-UX) on page 527 indicate the recommended property values for each OS when the volume manager is used.

These tables also list the setting values when the execution of the `HiScan` command finishes within an hour. Using a configuration where the number of LUs or logical volumes is more than the number shown in the tables is not recommended. It will take more than one hour for the `HiScan` operation to complete, and the operation might fail.

Table 88 Recommended property values for a host that will manage 100 or more LUs (when the host is using a volume manager in Windows)

Number of LUs and logical volumes managed by Device Manager and recognized by the host	server.http.entity.maxLength (units: bytes)	server.http.server.timeOut (units: seconds)	server.util.processTimeOut (units: milliseconds)	server.agent.maxMemorySize (units: MB)
88/10	230,000 or more	600 (Default value)	600,000 (Default value)	64
88/20	750,000 or more	600	600,000	64
100/200	12,000,000 or more	600	600,000	128
100/500	30,000,000 or more	600	600,000	384

Table 89 Recommended property values for a host that will manage 100 or more LUs (when the host is using a volume manager in Solaris)

Number of LUs and logical volumes managed by Device Manager and recognized by the host	server.http.entity.maxLength (units: bytes)	server.http.server.timeOut (units: seconds)	server.util.processTimeOut (units: milliseconds)	server.agent.maxMemorySize (units: MB)
100/200	3,100,000 or more	600 (Default value)	600,000 (Default value)	128
100/500	7,200,000 or more	600	600,000	384
150/500	12,000,000 or more	600	600,000	512
250/500	18,000,000 or more	600	600,000	768
500/1,000	36,000,000 or more	600	600,000	768
1,000/1,000	72,000,000 or more	1,200	600,000	768

Table 90 Recommended property values for a host that will manage 100 or more LUs (when the host is using a volume manager in AIX)

Number of LUs and logical volumes managed by Device Manager and recognized by the host	server.http.entity.maxLength (units: bytes)	server.http.server.timeOut (units: seconds)	server.util.processTimeOut (units: milliseconds)	server.agent.maxMemorySize (units: MB)
100/200	2,500,000 or more	600 (Default value)	600,000 (Default value)	128
100/500	6,000,000 or more	600	600,000	384
175/500	11,000,000 or more	600	600,000	640
250/500	15,000,000 or more	600	600,000	768
500/1,000	19,000,000 or more	600	600,000	768
1,000/1,000	38,000,000 or more	600	600,000	768

Table 91 Recommended property values for a host that will manage 100 or more LUs (when the host is using a volume manager in Linux)

Number of LUs and logical volumes managed by Device Manager and recognized by the host	server.http.entity.maxLength (units: bytes)	server.http.server.timeOut (units: seconds)	server.util.processTimeOut (units: milliseconds)	server.agent.maxMemorySize (units: MB)
100/50	748,000 or more	600 (Default value)	600,000 (Default value)	64
100/100	1,420,000 or more	600	600,000	64
100/256	3,600,000 or more	600	600,000	192
200/256	7,100,000 or more	600	600,000	512

Table 92 Recommended property values for a host that will manage 100 or more LUs (when the host is using a volume manager in HP-UX)

Number of LUs and logical volumes managed by Device Manager and recognized by the host	server.http.entity.maxLength (units: bytes)	server.http.server.timeOut (units: seconds)	server.util.processTimeOut (units: milliseconds)	server.agent.maxMemorySize (units: MB)
100/50	745,000 or more	600 (Default value)	600,000 (Default value)	64
100/100	1,400,000 or more	600	600,000	64
100/256	3,500,000 or more	600	600,000	192
200/256	7,000,000 or more	600	600,000	512
500/1,000	40,000,000 or more	600	600,000	896
1,000/100	8,000,000 or more	600	600,000	192
1,000/500	42,000,000 or more	600	1,200,000	896

Related tasks

- Changing Device Manager server properties on page 590
- Changing Device Manager agent properties on page 670

Related references

- server.http.entity.maxLength on page 594
- server.agent.maxMemorySize on page 681
- server.http.server.timeOut on page 691
- server.util.processTimeOut on page 691

Resident processes of the Device Manager agent

The Device Manager agent's resident processes must run on the OS.

The following describes the resident processes of the Device Manager agent.

Table 93 Resident processes of the Device Manager agent (Windows)

Process name	Service name	Function
hbsa_service.exe	HBsA Service	Device Manager agent service

Table 94 Resident processes of the Device Manager agent (UNIX)

Process name	Function
hbsa_service	Device Manager agent service

Immediately after Device Manager agent installation is completed, the Device Manager agent service is enabled. The Device Manager agent service needs to be restarted in the following cases:

- When the IP address of a host in which the Device Manager agent is installed is changed
- When the HBA driver or HBA API library is installed on a host in which the Device Manager agent is installed
- When the contents of the property files of the Device Manager agent are modified
- When a new installation of Hitachi Command Suite is performed after the OS is re-installed on the management server
- When CCI is installed or removed
- When Dynamic Link Manager is installed or removed on AIX or Linux
- When the execution of the `hdvmagt_setting` command is interrupted
- When the Java execution environment used by the Device Manager agent is changed

Starting and stopping the Device Manager agent service, and checking the operating status of the service (hbsasrv command)

The `hbsasrv` command can be used to start and stop the Device Manager agent service. The command can also be used to check the operating status of the service.

Operations to complete in advance

Log in as a user with Administrator permissions (for Windows) or as a root user (for UNIX).

Command format

```
hbsasrv [start|stop [-f]|status]
```

Location of the command

In Windows:

installation-folder-for-Device-Manager-agent\bin

In Linux:

installation-directory-for-Device-Manager-agent/bin

In Solaris or HP-UX:

/opt/HDVM/HBaseAgent/bin

In AIX:

/usr/HDVM/HBaseAgent/bin

Options

start

Specify this option to start the Device Manager agent service.

stop

Specify this option to stop the Device Manager agent service.

If the -f option is also specified, the command forces the Device Manager agent service to stop. In such a case, all processing is forced to terminate, thus ongoing processing of jobs is not guaranteed.

status

Specify this option to check the operating status of the Device Manager agent service.

Caution:

- Depending on the performance or the load status of the host computer, the Device Manager agent service might not stop immediately, even if the hbsasrv command finishes.
- If any add-on module or version 5.8 or later of Dynamic Link Manager is still running, you might not be able to stop the Device Manager agent service. In such a case, the error message KAIE62604-E is output. Wait until the add-on module or Dynamic Link Manager completes its operation, and then execute the command again.

- The version information displayed when the command is executed with the `status` option specified is not the version information for the Device Manager agent. You must use `hdvm_info` commands to check the Device Manager agent version.

Related references

- Displaying the version of the Device Manager agent (hdvm_info command) on page 533

Changing the user who executes the Device Manager agent service (Windows)

This section explains how to change the user who executes the Device Manager agent service to a member of the Administrators group.

Before you begin

Check the following information:

- User name and password of the new user (a member of the Administrators group).

Procedure

1. Stop the Device Manager agent service.
2. Open the Services window by selecting **Administrative Tools**, and then **Services**.
3. Select **HBsA Service**, **Operations**, and then **Properties**.
   The HBsA Service property window opens.
4. Click the **Logon** tab, and then select **Account**.
5. Set up the user and password, and then click **OK**.
6. From the Services window, select **HBsA Service**, and then start it.

Related references

- Starting and stopping the Device Manager agent service, and checking the operating status of the service (hbsasrv command) on page 528

Device Manager agent operations

This section explains Device Manager agent operations.

Checking the available agent functions (hbsa_modinfo command)

Use the `hbsa_modinfo` command to display the names and versions of available add-on modules.

The names and versions of add-on modules are displayed in *V.R1.R2-MM* format (*V*: version number, *R1* and *R2*: revision number, *MM*: modification

version number). You can also use the command to display whether a specific add-on module is ready for use by specifying the name of that module.

If applicable add-on modules are not found, a message appears indicating that the system was unable to find the add-on modules. However, the `hbsa_modinfo` command completes normally.

Note that if the version of Global Link Manager agent is 6.2, `HGLM Agent` is displayed for the add-on module name in the command execution results.

Also note that `hdlm` is displayed for the add-on module name only if the OS is Windows and the version of Dynamic Link Manager agent is 6.0 or later.

Operations to complete in advance

Log in as a user with Administrator permissions (for Windows) or as a root user (for UNIX).

Command format

`hbsa_modinfo [`*`name-of-the-addon-module`*`]`

Location of the command

In Windows:

`installation-folder-for-Device-Manager-agent``\bin`

In Linux:

`installation-directory-for-Device-Manager-agent``/bin`

In Solaris or HP-UX:

`/opt/HDVM/HBaseAgent/bin`

In AIX:

`/usr/HDVM/HBaseAgent/bin`

Options

name-of-the-addon-module

Specifies the following abbreviations for add-on modules whose availability you wish to check:

`hdlm`: Dynamic Link Manager agent

`hdvm`: Device Manager agent

`hglm`: Global Link Manager agent

`hptm`: Protection Manager agent

`hrpm`: Replication Manager agent

`hrpmap`: Replication Manager Application agent

The following describes add-on modules that can be checked by the `hbsa_modinfo` command and provides a functional overview.

- Dynamic Link Manager agent
  Monitors and adjusts the access route between the host and storage systems.
- Device Manager agent
  Collects host and storage system usage.
- Global Link Manager agent
  Monitors the DMP path route between the host and storage systems.
- Protection Manager agent
  Simplifies backup operations using the high-speed copy function of the storage system.
- Replication Manager agent
  Monitors the status of storage system replication.
- Replication Manager Application agent
  Centrally manages backup operations on a unit basis using the high-speed copy function of the storage system.

Deleting the Device Manager agent's registry entries and files (hbsa_util command)

If the OS of the host is Windows, you can use the `hbsa_util` command to delete the Device Manager agent's registry entries and files.

Operations to complete in advance

Log in as a user with Administrator permissions.

Command format

```
hbsa_util -cleanup
```

Location of the command

installation-folder-for-Device-Manager-agent\bin

Tip: The `hbsa_util.exe` file is also stored in the following folder of the integrated installation media:

DVD-ROM-drive\AGENTS\HDVM\Windows\HBsA

Options

`-cleanup`

Deletes the files and registry entries of the Device Manager agent.

Displaying the version of the Device Manager agent (hdvm_info command)

Use the `hdvm_info` command to display the version of the Device Manager agent.

The `hdvm_info` command displays the version of the Device Manager agent in *V.R1.R2-MM* format, where *V* is the version number, *R1.R2* is the revision number, *MM* is the modified version.

Command format

```
hdvm_info
```

Location of the command

In Windows:

installation-folder-for-Device-Manager-agent\bin

In Linux:

installation-directory-for-Device-Manager-agent/bin

In Solaris or HP-UX:

/opt/HDVM/HBaseAgent/bin

In AIX:

/usr/HDVM/HBaseAgent/bin

Setting the Device Manager server's information, HiScan command's execution period, and CCI's information (hdvmagt_setting command)

Use the `hdvmagt_setting` command to set the Device Manager server's information, the `HiScan` command's automatic execution period, and the information necessary for using CCI.

If the version of the Device Manager agent is 8.2.0 or later, you can use the `hdvmagt_setting` command to specify the following settings if secure communications are used between the Device Manager server and the Device Manager agent:

- Importing a server certificate of the Device Manager server into the truststore of the Device Manager agent
- Specifying settings in the property file of the Device Manager agent
  - `server.server.ssl.hdvm`
    Set `true`.
  - `server.server.serverPort`
    Set the port number for SSL communication.

This command lets you interactively set the items listed in the following table.

Table 95 Items that can be set by using the hdvmagt_setting command

Item	Details
Information for the Device Manager server	**IP address or host name** If you specify the IP address, you can use either an IPv4 or IPv6 address. Abbreviation can be used. The host name must satisfy the following conditions: Host name length: 50 bytes or less Available characters: `A-Z a-z 0-9 - _ . @` **SSL communication settings** If SSL communications are used between the Device Manager server and the Device Manager agent, specify the following information: • Directory to which a server certificate of the Device Manager server is to be stored All certificate files in the specified directory will be imported, but subdirectories will not be imported. Values to be specified must satisfy the following conditions: Absolute path length: 64 bytes or less Available characters (Windows): `A-Z a-z 0-9 . ( )` spaces Available characters (UNIX): `A-Z a-z 0-9 _ /` • Access password for the truststore of the Device Manager agent The password is case sensitive. The default password is `changeit`. **Port number** Specify the port number of the Device Manager server. The default value is 2001 for non-SSL communications and is 2443 for SSL communications. If a value other than the default is set, the currently set value is displayed. **User ID and password** Enter the user ID and password for the Device Manager agent registered with the Device Manager server. For a built-in account for use with the Device Manager agent, the user ID is `HaUser` and the default password is `haset`.
Execution period for the `HiScan` command	One of the following three automatic execution periods can be selected for the `HiScan` command: • Hourly • Daily • Weekly Note that any execution time can be specified.

Item	Details
	If you do not specify the execution time, for the hourly execution period, the `HiScan` command is executed at the 30th minute of every hour. For the daily or weekly period, the command is executed at 2:30 AM. If the Device Manager agent has been installed on multiple hosts, select the daily or weekly time period to reduce the load on the Device Manager server. Also, adjust the command execution times on those hosts so that information about multiple hosts is not reported to the Device Manager server at the same time.
Information for using CCI	**Installation location** Specify the drive or directory where CCI is installed. **Central management method** Specify whether to perform central management of copy pairs on the target hosts.

Operations to complete in advance

- Log in as a user with Administrator permissions (for Windows) or as a root user (for UNIX).
- Obtain server certificates (if you specify settings for SSL communication)
  Obtain server certificates created by the management server by using a secure method.
  - Server certificate for the Device Manager server
    When you use a self-signed certificate for testing encrypted communication or any temporary use, you first need to export the server certificate from the truststore file (`HiCommandCerts`).

Note: The default certificate of the Device Manager server is a self-signed certificate that is used to encrypt communication routes when user account authentication is linked between the storage system (VSP G1000, G1500, VSP F1500, VSP Gx00 models, or VSP Fx00 models) and Hitachi Command Suite. To use SSL communications between the Device Manager server and the Device Manager agent, use another self-signed certificate or a certificate signed by a certificate authority.

Information to collect in advance

- IP address or host name of the Device Manager server
- Access password for the truststore of the Device Manager agent (if the default password is changed)
- Port number of the Device Manager server
  You can check this value by using the `server.http.port` property (for non-SSL communication with the Device Manager server) or the `server.https.port` property (for SSL communication with the Device

Manager server) in the `server.properties` file for the Device Manager server.
- User ID and password for the Device Manager agent
  The relevant user account must belong to the Device Manager `PeerGroup`.
- Installation location of CCI

Command format

```
hdvmagt_setting
```

Location of the command

In Windows:

installation-folder-for-Device-Manager-agent\bin

In Linux:

installation-directory-for-Device-Manager-agent/bin

In Solaris or HP-UX:

/opt/HDVM/HBaseAgent/bin

In AIX:

/usr/HDVM/HBaseAgent/bin

Tip:
- The currently set execution time can be checked from KAIC22805-I messages and KAIC22804-I messages in the `HiScan.log` file, which is stored in the following locations:
  In Windows:
  installation-folder-for-Device-Manager-agent\bin\logs
  In Linux:
  installation-directory-for-Device-Manager-agent/bin/logs
  In Solaris or HP-UX:
  /opt/HDVM/HBaseAgent/bin/logs
  In AIX:
  /usr/HDVM/HBaseAgent/bin/logs
- In Windows, specifying an execution period registers `exeHiScan.bat` as a Windows task.
- The alias of the server certificate imported into the truststore will be: hdvm*yyyymmddhhmmssxxxxx.*(xxxxx : processing number)

Related concepts

- Operation workflow for secure communication between a management server and Device Manager agent on page 237

Related references

- Truststores on page 250
- Applying to a certificate authority for a Device Manager server certificate on page 271
- server.http.port on page 592
- server.https.port on page 593
- server.server.serverPort on page 683
- server.server.ssl.hdvm on page 691

Reporting host information to the Device Manager server manually (HiScan command)

Use the `HiScan` command to send host information (such as the host name, HBA WWN, file system, mount-point directory, and LUs connected to the host) to the Device Manager server.

If the configuration of the host's storage systems or file system is changed, the change can be applied to the Device Manager server by executing the `HiScan` command manually.

Operations to complete in advance

Log in as a user with Administrator permissions (for Windows) or as a root user (for UNIX).

Information to collect in advance

- IP address or host name of the Device Manager server
- Port number of the Device Manager server
- User ID and password for the Device Manager agent
  If you want to use another account with the Device Manager agent, you must register the user ID in the `PeerGroup` user group in advance.

Command format

To send host information:

```
HiScan -s server-destination [-u user-id -p password] [{-c
sec|-t output-file-name}]
```

To output the sent host information to a file:

```
HiScan -t output-file-name
```

Location of the command

In Windows:

```
installation-folder-for-Device-Manager-agent\bin
```

In Linux:

installation-directory-for-Device-Manager-agent/bin

In Solaris or HP-UX:

/opt/HDVM/HBaseAgent/bin

In AIX:

/usr/HDVM/HBaseAgent/bin

Options

-s

Specify the Device Manager server destination.

server-destination can be specified in the following format:

IP-address[:*port-number*]

host-name[:*port-number*]

localhost[:*port-number*]

If the port number is omitted, the port number set in the server.server.serverPort property of the server.properties file of the Device Manager agent is used. In addition, when you specify an IPv6 format IP address and port number at the same time, enclose the IPv6 address in square brackets ([]).

-u, -p

Specify the user ID and password of an account that is registered on the destination Device Manager server and in the PeerGroup user group.

If these options are omitted, the command will use the user ID and password defined by the server.server.authorization property in the server.properties file of the Device Manager agent.

-c

Specifies the interval (in seconds) at which host information is sent to the Device Manager server. Host information is continuously sent to the Device Manager server at the specified interval, until a forced termination occurs. Values of less than ten seconds are recognized as invalid. Specify a value in the range from 10 to 2147483647.

-t

Specify this option if you want to output the host information that was sent to the Device Manager server to an XML file. The file is output to the current directory.

The following characters cannot be used in the file name:

\ / : , ; * ? " < > | $ % & ' ` ^

If the -s option is also specified, response messages from the Device Manager server, as well as the information sent from the Device Manager agent, are output to the file.

Tip: Information about the host on which a Device Manager agent is installed is automatically reflected to the Device Manager server in the following cases:

- When the HiScan command is automatically executed
- When the host is started
- When host information is updated from the Device Manager GUI

Related references

- server.server.authorization on page 683
- server.server.serverPort on page 683

Acquiring device information (hldutil command)

Use the hldutil command to acquire device information such as storage system LDEVs and file systems.

The acquired device information can be displayed in a specific format or output to an execution log file. Device information acquired in the past can also be displayed. If all options are omitted when this command is used, the command displays information about all LDEVs recognized by the host.

This command can also be used to manage device information by copying or deleting execution log files.

Operations to complete in advance

Log in as a user with Administrator permissions (for Windows) or as a root user (for UNIX).

Command format

To display device information:

```
hldutil [-d [device-number-or-device-file-name]|-g [drive-
group-name]|-l ldev-number.serial-number] [-p] [-q] [-nolog]
[-s sort-key...] [-serdec] [-k|-hf log-file-name|-h log-
number]
```

To manage device information:

```
hldutil {-h log-number -hb log-file-name | -hrm {log-number |
all } | -history number-of-log-file-generations }
```

Location of the command

In Windows:

installation-folder-for-Device-Manager-agent\util\bin

In Linux:

installation-directory-for-Device-Manager-agent/util/bin

In Solaris or HP-UX:

/opt/HDVM/HBaseAgent/util/bin

In AIX:

/usr/HDVM/HBaseAgent/util/bin

Options

-d

Specify this option to display information about the LDEV specified as an argument of this option. (The argument is either a drive number (in Windows) or device special file name (in UNIX).) If the argument is omitted, the command displays information about all LDEVs that are currently recognized.

-g

Specify this option to display information about the drive group specified by a drive group name as an argument of this option. If the argument is omitted, the command displays information about all drive groups that are currently defined.

-l

Specify this option to display the information about the LDEV specified by an LDEV number and serial number as arguments. The LDEV number and serial number must be specified in the indicated order. If either argument (or both) is omitted, the command does not display LDEV information.

If you specify the `-l` option, only the following items are output:

- `Ldev#` (LDEV number)
- `Ser#` (storage system serial number)
- `Device` (device special file name or drive number)
- `Dg name` (drive group name)
- `fs` (file system)

-p

Specify this option to add the P-VOL and S-VOL information (that you set up by using ShadowImage, TrueCopy, Copy-on-Write Snapshot, Thin

Image, Universal Replicator or global-active device) to the drive information to be output. When this option specified, if no P-VOL or S-VOL information is assigned to an LDEV, nothing is output.

-q

Specify this option to output the command execution results only to the execution log file without sending them to the standard output (quiet mode). Typically, you specify this option when you want to run a background job to output the latest LDEV information to the execution-result log file. However, error messages are sent to the standard error output.

-nolog

Specify this option to send the command execution results only to the standard output without updating the execution log file.

-s

Specify this option to display LDEV information in ascending ASCII order.

If the sort key is specified, the LDEV information acquired by the command can be sorted based on the specified sort key.

When specifying multiple sort keys, place a one-byte space between sort keys.

If you specify multiple sort keys, the command sorts information using the sort keys in the order in which they are specified. If you specify the file system name as the sort key, the command sorts LDEV information using the file system name that is included in each logical device and assigned the lowest ASCII code.

If you do not specify the `-s` option, the command outputs LDEV information in the order in which it has processed the information.

The following table lists the sort keys that can be specified for the `hldutil` command.

Table 96 hldutil sort keys that can be specified for the hldutil command

Sort key	Descriptions
`dg`	Drive group name
`fs`	File system name
`iscsin`	iSCSI name for the iSCSI initiator
`ldev`	LDEV number
`lun`	LU number
`port`	Port number

Sort key	Descriptions
prod	Product name
rg	Parity Group number
rid	Character string representing a storage system model
ser	Serial number of a storage system
tid	Target ID
vend	Vendor name
wwnn	Node WWN name
wwnp	Port WWN name

-serdec

Specify this option to display the serial number of the storage system in decimal format.

-k

Specify this option to send the contents of the latest execution log file to the standard output.

This processing involves no hardware access. Note that if no drive information is recorded in an execution log file, the drive information is acquired and then output to the standard output and an execution log file.

-hf

Specify this option to output the contents of a specific execution log file to the standard output.

This processing involves no hardware access.

-h

Specify this option to output the contents of the execution log file identified by a specific log number to the standard output. This processing involves no hardware access.

If this option is specified together with the -hb option, the command creates a copy of the execution log file. For the -h option, specify the log number of the copy source execution log file. For the -hb option, specify the copy destination.

-hb

Specify this option to create a copy of an execution log file. This option must always be specified together with the -h option.

Specify the log number of the copy source execution log file for the `-h` option, and specify the copy destination for the `-hb` option. The copy destination file can be specified with an absolute path or relative path.

`-hrm`

Specify this option to delete the execution log file specified by a log number. If you specify `all` instead of a log number, the command deletes all execution log files from the default log storage directory.

`-history`

Specify this option to set the maximum number of generations of execution log files to be kept. Specify a number from `1` to `64`. The default value is `32`. The specified value takes effect when the next execution log file is created.

Caution: If you execute the `hldutil` command immediately after the host environment is changed (for example, after an LU is added or deleted), the command might not be able to recognize the changed contents of the host. In this case, wait a while, and then re-execute the `hldutil` command.

Information displayed by the hldutil command

The following table lists and describes the information output when you execute the `hldutil` command. The information items are output in the order shown in the table.

The items displayed differ depending on the OS and the specified options.

Table 97 Information displayed when the hldutil command is executed

Item	Description
`Dg name`	Drive group name
`Device`	Drive number (for Windows)
	Device special file name (for UNIX)
`fs`	File system name
`P/S`[#1]	Identification of the P-VOL or S-VOL
`Vend.`	Vendor name
`Prod.`	Product name
`Port#`	Port number (on the DKC)
`Tid#`[#2]	Target ID (SCSI interface on the host)
`Lun#`[#2]	LU number (SCSI interface on the host)
`Ldev#`	LDEV number (on the DKC)
`Ser#`	Serial number of the storage system
`RaidID`	Character string indicating the model of the storage system

Item	Description
	For details, see Table 98 Correspondence between RaidID values displayed by the hldutil command and storage system models on page 544.
RG#	Parity Group number
PortWWN#3	Port WWN
NodeWWN#3	Node WWN
iSCSIName	iSCSI name for the iSCSI initiator

#1:

If the host is a virtual machine and you execute the `hldutil` command after changing the configuration of the P-VOL or S-VOL, this information might not be displayed correctly. In this case, restart the virtualization server to display the information correctly.

#2:

In the case of HP-UX 11i v3, this item is not displayed for a persistent special device (persistent device special file).

#3:

If the virtual WWN is assigned to the virtual machine by using NPIV, the physical WWN of the virtualization server is displayed.

Table 98 Correspondence between RaidID values displayed by the hldutil command and storage system models

RaidID	Storage system model
71	Hitachi WMS 100
73	Hitachi AMS 200
75	Hitachi AMS 500
77	Hitachi AMS 1000
81	Hitachi SMS 100
82	Hitachi SMS 110
83	Hitachi AMS2100
85	Hitachi AMS2300
87	Hitachi AMS2500
91	HUS110
92	HUS130
93	HUS150
HM70	HUS VM
HM82	VSP G200
HM84	VSP G400, VSP G600, VSP F400 or VSP F600

RaidID	Storage system model
HM86	VSP G800 or VSP F800
R600	Universal Storage Platform V
R601	Universal Storage Platform VM
R700	Virtual Storage Platform
R800	VSP G1000, G1500, or VSP F1500

Configuration definition file for managing copy pairs

In Device Manager, you can use a user-created CCI configuration definition file to manage copy pairs.

Prerequisite environment for using the configuration definition file

To use the configuration definition file, you need to set up the environment as follows on the host on which CCI is installed.

- Installing a Device Manager agent
- Setting the Device Manager server information
- Specifying the settings required for using Device Manager to manage copy pairs

Related concepts

- Managing copy pairs on page 521

Related tasks

- Editing the configuration definition file on page 545

Related references

- Setting the Device Manager server's information, HiScan command's execution period, and CCI's information (hdvmagt_setting command) on page 533

Editing the configuration definition file

Edit the `horcm`*XX*`.conf` file, and then refresh the storage system.

Procedure

1. Open the `horcm`*XX*`.conf` file.

   The configuration definition file is stored in the directory specified by the `server.agent.rm.horcmSource` property of the `server.properties` file in the Device Manager agent.

   The default storage location is as follows:

   In Windows:

System folder (represented by the environment variable `%windir%`)

In UNIX:

`/etc` directory

If the `horcm`*XX*`.conf` file does not exist, create it.

2. Specify the parameters according to the description conventions.

Note:

- If a parameter not supported by Device Manager is used, the configuration definition file is assumed to be invalid and the system does not execute normal processing. Even though a parameter is supported, Device Manager might not support certain description formats. Note that the configuration definition file is assumed to be invalid if an item is specified using an unsupported format.
- Do not specify the following instance numbers and UDP port numbers in the configuration definition file, because the Device Manager agent temporarily uses these values to acquire copy pair information:
  - Instance number: 900 to 998 (default)
  - UDP port number: 53232 to 53330 (default)

  If these instance numbers or UDP port numbers are used, CCI error information might be output to the system log or event log.

Tip: To change the instance numbers and UDP port numbers that are temporarily used by the Device Manager agent, use the `server.agent.rm.temporaryInstance` and `server.agent.rm.temporaryPort` properties in the `server.properties` file.

3. Use the Device Manager GUI or CLI to refresh the storage system that contains the copy pair volumes for which the configuration definition file was created.

Related references

- Prerequisite environment for using the configuration definition file on page 545
- Notes on using the configuration definition file on page 562
- agent.rm.horcmInstance on page 672
- agent.rm.horcmService on page 673
- server.agent.rm.temporaryInstance on page 686

- server.agent.rm.temporaryPort on page 686
- server.agent.rm.horcmSource on page 690

Configuration definition file parameters supported Device Manager

If you use a parameter not supported by Device Manager, the configuration definition file is assumed to be invalid and processing is not performed normally.

Device Manager supports the following parameters:

- HORCM_MON
- HORCM_CMD
- HORCM_VCMD
- HORCM_DEV
- HORCM_LDEV
- HORCM_INST
- HORCM_INSTP
- HORCM_CTQM#

#

This parameter is supported by Device Manager agent version 6.2 or later. Note that when you create or use a copy pair, even if HORCM_CTQM information is defined in the configuration definition file, the Device Manager agent will operate while ignoring the definition. The Device Manager agent does not add the HORCM_CTQM definitions to the configuration definition file, nor does it add a pair group to the existing definitions. However, when you delete a pair, any definitions of that pair group that exist in the HORCM_CTQM definitions will also be deleted.

Related references

- Description conventions for the configuration definition file on page 547
- HORCM_MON parameter description format on page 548
- HORCM_CMD parameter description format on page 550
- HORCM_VCMD parameter description format on page 552
- HORCM_DEV parameter description format on page 553
- HORCM_LDEV parameter description format on page 556
- HORCM_INST parameter description format on page 558
- HORCM_INSTP parameter description format on page 560

Description conventions for the configuration definition file

If a configuration definition file is not created in accordance with the description conventions, Device Manager assumes that the configuration definition file is invalid.

Create a configuration definition file in accordance with the following conventions.

- A configuration definition file cannot include a line that consists only of space characters.
- If the version of Device Manager agent is 5.5 or earlier, a line that starts with H and includes any of the following character strings cannot be included (except in the starting line of the parameter):
  HORCM_MON, HORCM_CMD, HORCM_VCMD, HORCM_DEV, HORCM_LDEV, HORCM_INST, HORCM_INSTP, HORCM_CTQM, HORCM_LDEVG, HORCM_ALLOW_INST
- If the version of the Device Manager agent is from 7.0.0 to 7.0.1, a virtual command device must not be defined for the HORCM_CMD parameter in the configuration definition file.
- The configuration definition file must be created in accordance with the following conditions:
  - HORCM_MON must be defined.
  - At a minimum, either HORCM_DEV or HORCM_LDEV must be defined.
  - At a minimum, either HORCM_INST or HORCM_INSTP must be defined.
  - HORCM_ALLOW_INST must not be defined.
- A virtual ID must not be defined for the HORCM_DEV parameter in the configuration definition file.
- If you use CCI 01-32-03/*XX* or later, the HORCM_DEV parameter or a copy pair definition for storage systems that do not support virtual storage machines must not be defined in the configuration definition file in which the HORCM_VCMD parameter is defined.
- If you use CCI 01-32-03/*XX* or later, the configuration definition file in which the HORCM_VCMD parameter is specified must not include command device definitions for multiple storage systems.

Related references

- Configuration definition file parameters supported Device Manager on page 547
- HORCM_MON parameter description format on page 548
- HORCM_CMD parameter description format on page 550
- HORCM_VCMD parameter description format on page 552
- HORCM_DEV parameter description format on page 553
- HORCM_LDEV parameter description format on page 556
- HORCM_INST parameter description format on page 558
- HORCM_INSTP parameter description format on page 560

HORCM_MON parameter description format

Use the HORCM_MON parameter to specify the machine information for the local host and the interval for monitoring errors in copy pair volumes.

- ip_address
  Specify the IP address (the Device Manager agent whose version is 5.9 or later supports the IPv6 protocol), host name, NONE, or NONE6.

- Specify the information for the host managed by the Device Manager server.
- Match the IP address version (IPv6 or IPv4) to the one specified for `HORCM_INST` or `HORCM_INSTP`.
- If an IPv6 environment is being used, specify an IP address. If you specify a host name, an IPv4 environment is used.
- The table below lists the values that can be specified for `ip_address`. Note that some formats cannot be specified for `ip_address` because they cannot identify a host.

Table 99 Values that can be specified for the ip_address of HORCM_MON parameter

Value	Device Manager agent version		
	5.9 or later	05-80	05-70 or earlier
IP address	Yes	Yes	Yes
Host name	Yes	Yes	Yes
`NONE`	Yes#	Yes#	No
`"__NONE__"`	No	No	No
`NONE6`	Yes#	No	No
`"__NONE6__"`	No	No	No
Loopback IP addresses (127.0.0.1 to 127.255.255.254)	Yes#	Yes#	No
Loopback host name (`localhost`)	Yes#	Yes#	No
Cluster virtual IP address	No	No	No
Cluster virtual machine name	No	No	No

Legend:
Yes: Can be specified.
No: Cannot be specified.
#: Can be specified when the copy pair is managed from the Device Manager CLI. However, this item cannot be specified when copy pair operations are performed from the Device Manager GUI or Replication Manager.

- `service`
  Specify the port name or port number.
  - Specify the port name using 1 to 15 single-byte characters. The environment must support the conversion of port names to port numbers.
  - Specify the port number as a numeric value from 0 to 65535.
- `poll`
  Specify a value (in ten millisecond units) or `-1`.
- `timeout`
  Specify the timeout period in ten millisecond units.

Table 100 Support status of HORCM_MON parameter description format

Version	Item			
	ip_address	service	poll	timeout
6.1 or later	Yes	Yes	Yes	Yes
5.9 to 6.0	Yes	Only supports port number specification.	Yes	Yes
05-80	Supports IP address, host name, and NONE.	Only supports port number specification.	Yes	Yes
05-70 or earlier	Supports IP address and host name.	Only supports port number specification.	Yes	Yes

Legend:

Yes: Supports all description formats.

Related tasks

- Editing the configuration definition file on page 545

Related references

- Description conventions for the configuration definition file on page 547
- HORCM_INST parameter description format on page 558
- HORCM_INSTP parameter description format on page 560
- Notes on using the configuration definition file on page 562

HORCM_CMD parameter description format

Specify a command device for the storage system in the HORCM_CMD parameter.

- dev_name

  Specify a command device that is recognized by the host. You can specify more than one command device in the same system, and you can specify a command device in more than one system.

  In Windows, you can specify a command device in IPCMD format, PhysicalDrive format, GUID format, or CMD format.

  IPCMD format

  \\.\IPCMD-*IP-address-of-the-virtual-command-device-port-number*[-*unit-ID-of-the-storage-system*]

  PhysicalDrive format

  \\.\PhysicalDrive*disc-number-defined-by-Windows*

  For the Device Manager agent 4.3 or earlier, this item is case sensitive.

GUID format

\\.\Volume{*GUID*}

CMD format

\\.\CMD-*serial-number*[-*logical-device-number*[-*port-name*[-*host-group-number*]]]

You must use base-10 numbers to specify the serial number and logical device number. For the host group number, if the version of the Device Manager agent is 5.6 or later, specify a value from 0 to 254. If the version of the Device Manager agent is 5.5 or earlier, specify a value from 0 to 127.

In UNIX, you can specify a command device in IPCMD or CMD format, or in a special file.

IPCMD format

\\.\IPCMD-*IP-address-of-the-virtual-command-device-port-number*[-*unit-ID-of-the-storage-system*]

CMD format

\\.\CMD-*serial-number*[-*logical-device-number*[-*port-name*[-*host-group-number*]]]*HINT*

You must use base-10 numbers to specify the serial number and logical device number. For the host group number, if the version of the Device Manager agent is 5.6 or later, specify a value from 0 to 254. If the version of the Device Manager agent is 5.5 or earlier, specify a value from 0 to 127.

Specify the HINT as follows.

Solaris: /dev/rdsk/

AIX: /dev/rhdisk

Linux: /dev/sd

HP-UX: /dev/rdsk/ or /dev/rdisk/disk

Table 101 Support status of HORCM_CMD parameter description format

Version		Item
		dev_name
7.4.1 or later	Windows	Yes
	UNIX	Yes
7.1 to 7.4.0	Windows	Yes

Version		Item
		dev_name
	UNIX	Only supports specification using a special file or specification using IPCMD format.
05-10 to 7.0	Windows	Supports description formats other than IPCMD format.
	UNIX	Only supports specification using a special file.
05-00	Windows	Supports description formats other than IPCMD and CMD format.
	UNIX	Only supports specification using a special file.
04-30 or earlier	Windows	Supports description formats other than IPCMD, CMD and GUID formats.
	UNIX	Only supports specification using a special file.

Legend:

Yes: Supports all description formats.

Related tasks

- Editing the configuration definition file on page 545

Related references

- Description conventions for the configuration definition file on page 547
- Notes on using the configuration definition file on page 562

HORCM_VCMD parameter description format

Use the `HORCM_VCMD` parameter to specify the serial number of the target virtual storage machine.

- `Serial#`
  Specify the serial number of the virtual storage machine.

Table 102 Support status of HORCM_VCMD parameter description format

Version	Item
	Serial#
8.0.1 or later	Yes#1
8.0	Yes#2
7.6.1 or earlier	No

Legend:

Yes: Supports all description formats.

No: Cannot be specified.

#1

If you use CCI 01-32-03/*XX* or later, you can change the `HORCM_VCMD` definition from the Device Manager agent.

#2

You cannot change the `HORCM_VCMD` definition from the Device Manager agent.

Related tasks

- Editing the configuration definition file on page 545

Related references

- Description conventions for the configuration definition file on page 547
- Notes on using the configuration definition file on page 562

HORCM_DEV parameter description format

Use the `HORCM_DEV` parameter to specify information about the storage system that contains volumes to be used as copy pairs.

- `dev_group`
  Specify the group name.
  - The combination of the `dev_group` and `dev_name` values must not be duplicated in the configuration definition file for a host.
  - Specify no more than 31 single-byte characters. A hyphen (`-`) cannot be specified at the beginning of the character string.
- `dev_name`
  Specify the name of the pair volume.
  - The same `dev_name` value must not be duplicated in a configuration definition file.
  - Specify no more than 31 single-byte characters. A hyphen (`-`) cannot be specified at the beginning of the character string.
- `port#`
  Specify the port name.
  If you specify the host group number immediately after specifying the port name for `port#`, the range of values that you can specify differs depending on the version of the Device Manager agent. When the version of the Device Manager agent is 5.6 or later, specify a value from `0` to `254`. When the version of the Device Manager agent is 5.5 or earlier, specify a value from `0` to `127`.
- `targetID`
  Specify the target ID of SCSI/Fibre.
- `LU#`
  Specify the LU number of SCSI/Fibre.
- `MU#`
  Specify the mirror descriptor using a numeric value or the `h` addition. You can omit this by leaving it blank.

The value that can be specified for `MU#` differs depending on the Device Manager agent version being used and the copy type.

When the version of the Device Manager agent is 8.0.1 or later:

ShadowImage: `0` to `2`

Copy-on-Write Snapshot: `0` to `63`

Thin Image: `0` to `63`

TrueCopy: Not specified

Universal Replicator: Not specified#, `0`#, `h0`#, `h1`, `h2`, or `h3`

global-active device: Not specified, `h0`, `h1`, `h2`, or `h3`

#:

If no value is specified or if 0 or h0 is specified, multi-target configuration pairs cannot be created with TrueCopy.

When the version of the Device Manager agent is from 7.4.0 to 8.0:

ShadowImage: `0` to `2`

Copy-on-Write Snapshot: `0` to `63`

Thin Image: `0` to `63`

TrueCopy: Not specified

Universal Replicator: Not specified#, `0`#, `h1`, `h2`, or `h3`

#:

If no value is specified or 0 is specified, multi-target configuration pairs cannot be created with TrueCopy.

When the version of the Device Manager agent is from 6.0 to 7.3.1:

ShadowImage: `0` to `2`

Copy-on-Write Snapshot: `0` to `63`

TrueCopy: Not specified

Universal Replicator: Not specified#, `0`#, `h1`, `h2`, or `h3`

#:

If no value is specified or 0 is specified, multi-target configuration pairs cannot be created with TrueCopy.

When the version of the Device Manager agent is from 04-20 to 5.9:

ShadowImage: `0` to `2`

Copy-on-Write Snapshot: `0` to `31`

TrueCopy: Not specified

Universal Replicator: `h1`, `h2`, or `h3`

When the version of the Device Manager agent is 4.0 or 4.1

ShadowImage: `0` to `2`

Copy-on-Write Snapshot: `0` to `13`

TrueCopy: Not specified

Universal Replicator: `h1`, `h2`, or `h3`

When the version of the Device Manager agent is 3.5 or earlier

ShadowImage: `0` to `2`

Copy-on-Write Snapshot: `0` to `13`

TrueCopy: Not specified

Table 103 Support status of HORCM_DEV parameter description format

Version	Item					
	dev_group	dev_name	port#	targetID	LU#	MU#
04-00 or later	Yes	Yes	Yes	Yes	Yes	Yes
03-50 or earlier	Yes	Yes	Yes	Yes	Yes	Supports specification using mirror descriptors, omissions (blank), and numeric values.

Legend:

Yes: Supports all description formats.

Related tasks

- Editing the configuration definition file on page 545

Related references

- Description conventions for the configuration definition file on page 547
- Notes on using the configuration definition file on page 562

HORCM_LDEV parameter description format

Use the HORCM_LDEV parameter to specify information about the storage system that contains copy pairs, and the volume information.

- dev_group
  Specify the group name.
  - The combination of the dev_group and dev_name values must not be duplicated in the configuration definition file for a host.
  - Specify no more than 31 single-byte characters. A hyphen (-) cannot be specified at the beginning of the character string.
- dev_name
  Specify the name of the pair volume.
  - The same dev_name value must not be duplicated in a configuration definition file.
  - Specify no more than 31 single-byte characters. A hyphen (-) cannot be specified at the beginning of the character string.
- Serial#
  Specify the system number of the storage system using the decimal number or *serial-number:journal-ID* format.
- CU:LDEV(LDEV#)
  Specify the LDEV number using the decimal number, hexadecimal number, or *CU:LDEV* format.
  The following are examples of LDEV#:

  Base-10 numbers

  260

  Hexadecimal numbers

  0x104

  ***CU:LDEV* format**

  01:04
- MU#
  Specify the mirror descriptor using a numeric value or h addition. You can omit this by leaving it blank.
  The value that can be specified for MU# differs depending on the version and copy type of the Device Manager agent, as shown below.

  When the version of the Device Manager agent is 8.0.1 or later:

  ShadowImage: 0 to 2

  Copy-on-Write Snapshot: 0 to 63

  Thin Image: 0 to 63

TrueCopy: Not specified

Universal Replicator: Not specified#, 0#, h0#, h1, h2, or h3

global-active device: Not specified, h0, h1, h2, or h3

#:

If no value is specified or if 0 or h0 is specified, multi-target configuration pairs cannot be created with TrueCopy.

When the version of the Device Manager agent is from 7.4.0 to 8.0:

ShadowImage: 0 to 2

Copy-on-Write Snapshot: 0 to 63

Thin Image: 0 to 63

TrueCopy: Not specified

Universal Replicator: Not specified#, 0#, h1, h2, or h3

#:

If no value is specified or 0 is specified, multi-target configuration pairs cannot be created with TrueCopy.

When the version of the Device Manager agent is from 6.0 to 7.3.1:

ShadowImage: 0 to 2

Copy-on-Write Snapshot: 0 to 63

TrueCopy: Not specified

Universal Replicator: Not specified#, 0#, h1, h2, or h3

#:

If no value is specified or 0 is specified, multi-target configuration pairs cannot be created with TrueCopy.

When the version of the Device Manager agent is 5.9 or earlier:

ShadowImage: 0 to 2

Copy-on-Write Snapshot: 0 to 31

TrueCopy: Not specified

Universal Replicator: h1, h2, or h3

Table 104 Support status of HORCM_LDEV parameter description format

Version	Item				
	dev_group	dev_name	Serial#	CU:LDEV(LDEV#)	MU #
6.4 or later	Yes	Yes	Yes	Yes	Yes
6.3 to 6.2	Yes	Yes	Yes	Yes#	Yes
6.1 to 05-60	Yes	Yes	Supports description formats other than the *serial-number:journal-ID* format.	Yes#	Yes
05-50 or earlier	No	No	No	No	No

Legend:

Yes: Supports all description formats.

No: Does not support any description formats.

#: If the LDEV number is specified by using a hexadecimal number or the *CU:LDEV* format, you can only view or delete the LDEV number.

Related tasks

- Editing the configuration definition file on page 545

Related references

- Description conventions for the configuration definition file on page 547
- Notes on using the configuration definition file on page 562

HORCM_INST parameter description format

Use the `HORCM_INST` parameter to specify machine information for the remote host.

- `dev_group`
  Specify the contents specified for `dev_group` of the `HORCM_DEV` parameter or `HORCM_LDEV` parameter.
  - You cannot specify `ip_address` more than once for the same host for a single `dev_group`.
  - Specify no more than 31 single-byte characters. A hyphen (-) cannot be specified at the beginning of the character string.
- `ip_address`
  Specify the IP address (a Device Manager agent whose version is 5.9 or later also supports the IPv6 protocol), or the host name.
  - Specify the information for the host managed by the Device Manager server.

- Match the IP address version (IPv6 or IPv4) to the one specified for `HORCM_MON`.
- When an IPv6 environment is being used, you cannot specify a host name. If you specify a host name, an IPv4 environment is used.
- The table below lists the values that can be specified for `ip_address`. Note that some formats cannot be specified for `ip_address` because they cannot identify a host.

Table 105 Values that can be specified for the ip_address of HORCM_INST parameter

Value	Device Manager agent version	
	05-80 or later	05-70 or earlier
IP address	Yes	Yes
Host name	Yes	Yes
Loopback IP addresses (127.0.0.1 to 127.255.255.254)	Yes#	No
Loopback host name (`localhost`)	Yes#	No
Cluster virtual IP address	No	No
Cluster virtual machine name	No	No

Legend:
Yes: Can be specified.
No: Cannot be specified.
#: Can be specified when the copy pair is managed from the Device Manager CLI. However, this item cannot be specified when copy pair operations are performed from the Device Manager GUI or Replication Manager.

- `service`
  Specify the port name or port number.
  - Specify the port name using 1 to 15 single-byte characters. The environment must support the conversion of port names to port numbers.
  - Specify the port number as a numeric value from 0 to 65535.

Table 106 Support status of HORCM_INST parameter description format

Version	Item		
	dev_group	ip_address	service
7.0 or later	Yes	Yes	Yes
6.1 to 6.4	Yes	Supports IP address and host name.	Yes
6.0 or earlier	Yes	Supports IP address and host name.	Only supports port number specification.

Legend:

Yes: Supports all description formats.

Related tasks

- Editing the configuration definition file on page 545

Related references

- Description conventions for the configuration definition file on page 547
- HORCM_MON parameter description format on page 548
- HORCM_DEV parameter description format on page 553
- HORCM_LDEV parameter description format on page 556
- Notes on using the configuration definition file on page 562

HORCM_INSTP parameter description format

Use the `HORCM_INSTP` parameter to specify the machine information and path group ID of the remote host.

- `dev_group`
  Specify the contents specified for `dev_group` of the `HORCM_DEV` parameter or `HORCM_LDEV` parameter.
  - You cannot specify `ip_address` more than once for the same host for a single `dev_group`.
  - Specify no more than 31 single-byte characters. A hyphen (-) cannot be specified at the beginning of the character string.
- `ip_address`
  Specify the IP address, or the host name.
  - Specify the information for the host managed by the Device Manager server.
  - Match the IP address version (IPv6 or IPv4) to the one specified for `HORCM_MON`.
  - When an IPv6 environment is being used, you cannot specify a host name. If you specify a host name, an IPv4 environment is used.
  - The table below lists the values that can be specified for `ip_address`. Note that some formats cannot be specified for `ip_address` because they cannot identify a host.

Table 107 Values that can be specified for the ip_address of HORCM_INSTP parameter

Value	Device Manager agent version
	7.6.0 or later
IP address	Yes
Host name	Yes

Value	Device Manager agent version
	7.6.0 or later
Loopback IP addresses (127.0.0.1 to 127.255.255.254)	Yes#
Loopback host name (`localhost`)	Yes#
Cluster virtual IP address	No
Cluster virtual machine name	No

Legend:
Yes: Can be specified.
No: Cannot be specified.
#: Can be specified when the copy pair is managed from the Device Manager CLI. However, this item cannot be specified when copy pair operations are performed from the Device Manager GUI or Replication Manager.

- `service`
  Specify the port name or port number.
  - Specify the port name using 1 to 15 single-byte characters. The environment must support the conversion of port names to port numbers.
  - Specify the port number as a numeric value from 0 to 65535.
- `pathID`
  Specify the path group ID as a decimal number from 1 to 255.
  - You cannot specify multiple path group IDs for a single copy group.
  - If you omit path group ID specification (that is, if you select CU Free), use the `HORCM_INST` parameter instead of the `HORCM_INSTP` parameter.

Table 108 Support status of HORCM_INSTP parameter description format

Version	Item
	All parameters
7.6.0 or later	Yes
6.2 to 7.5.0	Yes#
6.1 or earlier	No

Legend:

Yes: Supports all description formats.

No: Does not support any description formats.

#: The `HORCM_INSTP` parameter is ignored during copy pair creation or manipulation. During copy pair deletion, if the `HORCM_INSTP` definition

includes a group that has the same name as the copy pair group to be deleted, that group is deleted from the definition.

Related tasks

- Editing the configuration definition file on page 545

Related references

- Description conventions for the configuration definition file on page 547
- HORCM_MON parameter description format on page 548
- HORCM_DEV parameter description format on page 553
- HORCM_LDEV parameter description format on page 556
- HORCM_INST parameter description format on page 558
- Notes on using the configuration definition file on page 562

Changing the storage location of the configuration definition file

To change the storage location of the CCI configuration definition file, set the path of the storage location in the `server.agent.rm.horcmSource` property of the `server.properties` file of the Device Manager agent.

Before you begin

Log in as a user with Administrator permissions (for Windows) or as a root user (for UNIX).

Procedure

1. Execute the `hbsasrv` command to stop the Device Manager agent service.
2. Execute a CCI command to stop all HORCM instances that were manually started by users.

   For details on how to stop an HORCM instance, see the CCI manual.
3. Change the storage location of the configuration definition file.
4. Specify the new storage location that was changed in step 3 in the `server.agent.rm.horcmSource` property of the `server.properties` file of the Device Manager agent.
5. Execute the `hbsasrv` command to start the Device Manager agent service.

Related references

- Starting and stopping the Device Manager agent service, and checking the operating status of the service (hbsasrv command) on page 528
- server.agent.rm.horcmSource on page 690

Notes on using the configuration definition file

The following provides notes on using a configuration definition file for CCI to manage copy pairs.

When editing the configuration definition file:

When you use Device Manager to create or change a configuration definition file, the information that is defined in the file is automatically reported to the Device Manager server.

However, if you create or change a configuration definition file without using the Device Manager, for example, by using the Replication Manager instead or by directly editing the file, you need to manually report the file information to the Device Manager server.

If you refresh the storage system via the Device Manager GUI or CLI, information about the configuration definition file is reported to the Device Manager server. Refresh all storage systems associated with copy pair volumes that are specified in the configuration definition file.

When optimizing the configuration definition file:

If `true` is specified for the `server.agent.rm.optimization.userHorcmFile` property of the `server.properties` file, when the Device Manager agent service starts, or when you operate copy pairs, the Device Manager agent optimizes the contents of the CCI configuration definition file. In this case, note the following:

- For backing up the configuration definition file:
  In the optimization processing, the original configuration definition file `horcm`*`XX`*`.conf` is backed up as `horcm`*`XX`*`.conf.bk`. If the optimization is performed more than once, the original user-created configuration definition file will be lost because only one generation of backup file is made. Therefore, back up as necessary.
- About a comment added to the command device definition:
  When the CCI configuration definition file is optimized, the unit ID, logical device number, and serial number for the command device are added as comments on the line before the line on which the command device is defined. In this case, note the following:
  - Do not change the contents of the comment because the Device Manager agent references it.
  - When you copy the CCI configuration definition file that the Device Manager agent is already managing, and then create a new CCI configuration definition file, delete this comment.

When deleting copy pairs:

When you delete copy pairs from a management client, if all the definitions of the copy pairs in a configuration definition file are deleted, that configuration definition file will also be deleted. If you do not want the configuration definition file to be deleted, back up of the configuration definition file before you delete the copy pairs.

Related tasks

- Editing the configuration definition file on page 545

Related references

- server.agent.rm.optimization.userHorcmFile on page 685

12

Troubleshooting

This chapter describes how to resolve problems that occur during Device Manager and Tiered Storage Manager operation, and how to collect maintenance information.

If you need technical support, see Getting help on page 26.

- How to troubleshoot problems on the management server (Device Manager related)
- How to troubleshoot problems on the management server (Tiered Storage Manager related)
- How to troubleshoot problems on a host
- Maintenance information that must be collected if a failure occurs

How to troubleshoot problems on the management server (Device Manager related)

This section describes how to troubleshoot problems that occur due to Device Manager.

The user cannot log in to the Device Manager GUI

If a user cannot log in to the Device Manager GUI, unlock the user account.

Cause

The user account might have been locked.

Countermeasure

For a user without `Admin` (user management) permission:

Ask a user with `Admin` (user management) permission to unlock the account.

For a user with `Admin` (user management) permission:

Ask another user with `Admin` (user management) permission to unlock the account. Alternatively, execute the `hcmds64unlockaccount` command to unlock your own account.

Related tasks

- Unlocking accounts on page 162

The services of Common Component or the Device Manager server cannot be started

If the Common Component or Device Manager server services cannot be started, you need to change the desktop heap area.

Cause

The desktop heap might be insufficient.

Countermeasure

Edit the registry to change the area of the desktop heap.

For details on how to change the area of the desktop heap, see the Microsoft website.

The Device Manager server cannot be accessed after starting up the management server or Hitachi Command Suite product services

If Device Manager cannot be accessed from the GUI or CLI after starting the management server or Hitachi Command Suite product services, increase the retry count and the interval for connections to the Device Manager database.

Cause

If the KAIC03100-E error message is output to the Device Manager trace log file, the communication process from Device Manager server to the database has timed out.

Countermeasure

Increase the maximum number of times an attempt to connect to the Device Manager database can be retried and the interval at which connection attempts are retried.

In the `database.properties` file on the Device Manager server, change the values of the following properties:

- `dbm.startingCheck.retryCount`
- `dbm.startingCheck.retryPeriod`

Related tasks

- Changing Device Manager server properties on page 590

Related references

- dbm.startingCheck.retryCount on page 603
- dbm.startingCheck.retryPeriod on page 603

SNMP traps of Hitachi Data Ingestor and Hitachi NAS Platform F cannot be received

If SNMP traps of Hitachi Data Ingestor and Hitachi NAS Platform F cannot be received, make sure that the management server settings, such as the IP address and host name, match between Hitachi File Services Manager and Device Manager.

Cause

The following settings might not match between Hitachi File Services Manager and Device Manager.

- The IP address or host name of the management server
- The port number of the management server
- The file server name (the IP address or host name of the node)

Countermeasure

Check and, if necessary, revise the following settings:

- Whether the IP address or host name of the management server is registered in the notification destination of SNMP traps.
- Whether the SNMP trap reception port of Device Manager is registered in the notification destination of SNMP traps.
- Whether the file server name registered in Device Manager matches the IP address or host name of the node registered in Hitachi File Services Manager
  Format of the file server name: *host-name-of-the-node@IP-address-of-the-node*

An attempt to reconfigure or refresh a storage system failed

If an attempt to reconfigure or refresh a midrange storage system fails and the message KAIC05310-E or KAIC06299-E is output, increase the timeout value for communication between the midrange storage system and the Device Manager server.

Cause

Connection processing from the Device Manager server to the storage system might have timed out.

Countermeasure

Extend the timeout interval for communication between the storage system and the Device Manager server by using the following procedure.

Note that the smaller of the following values is used as the timeout value:

- The value set in the management server OS
- The value of the `ConnectionTimeout` property in the `lanconf.inf` file

1. In the `lanconf.inf`, change the value of the `ConnectionTimeout` property according to the operation environment.
   The specifiable values range from 1 to 60 seconds.

   In Windows:

   installation-folder-for-Hitachi-Command-Suite
   `\DeviceManager\HiCommandServer\lib\HSNMAPI\lanconf.inf`

   In Linux:

   installation-directory-for-Hitachi-Command-Suite/
   `HiCommandServer/lib/HSNMAPI/lanconf.inf`
2. Restart Hitachi Command Suite product services.

Related tasks

- Starting the Hitachi Command Suite services on page 458

- Stopping the Hitachi Command Suite services on page 460

How to troubleshoot problems on the management server (Tiered Storage Manager related)

This section describes how to troubleshoot problems that occur due to Tiered Storage Manager.

Note that operations from the management client here refer to operations from the Tiered Storage Manager CLI only.

The Tiered Storage Manager server could not be started

If an attempt to start the Tiered Storage Manager server fails, take the action appropriate for the cause.

Cause

- Device Manager or Common Component has not started.
- The user who attempted the operation does not have administrator permissions.
- The property file is invalid.

Countermeasure

If Device Manager or Common Component has not started:

Start Device Manager and Common Component.

If the user who attempted the operation does not have administrator permissions:

Perform the operation again as a user who has administrator permissions for the OS.

If the property file is invalid:

Revise the property file in accordance with the command logs or the message logs.

The Tiered Storage Manager server does not stop

If the Tiered Storage Manager server does not stop, take the action appropriate for the cause.

Cause

- An error occurred in the Tiered Storage Manager server during processing to stop it.
- The user who attempted the operation does not have administrator permissions.

Countermeasure

If a failure occurs on the server while it is being stopped:

If 10 minutes have passed since the stop request, and the Tiered Storage Manager server is still not stopping, execute the following command:

In Windows:

installation-folder-for-Hitachi-Command-Suite
\TieredStorageManager\bin\htsmserver forcestop

In Linux:

installation-directory-for-Hitachi-Command-Suite/
TieredStorageManager/bin/htsmserver forcestop

If the user does not have administrator permissions:

Perform the operation again through a user who has administrator permissions for the OS.

The Tiered Storage Manager server terminates abnormally or fails over in a cluster environment

If forced shutdown or another unexpected error causes the Tiered Storage Manager server to terminate abnormally or to fail over in an a cluster environment, you must restore the consistency between the database information and the storage system status.

Cause

An inconsistency exists between the database information and the storage system status.

Countermeasure

Perform the following procedure to restore the consistency between the database information and the storage system status:

1. After restarting the Hitachi Command Suite product services, refresh all storage systems by using Device Manager.
2. If the Tiered Storage Manager server terminated abnormally when a migration task was being created or canceled, perform the creation or cancellation again. If an error occurred while a migration was being canceled, refresh the storage system.
3. If a migration task that is being executed has failed, refresh the storage system again. After that, take action as described below according to the task status.

If the task status is DATA ERASURE FAILURE:

The migration is complete, and the LDEV numbers of the migration source and destination have been reversed. Check the status of the source volume that has the destination volume LDEV number, and then take the appropriate action depending on the status. If data was not deleted, the original data remains on the source volume that has the destination volume LDEV number.

- If the volume that has the destination LDEV number is blocked, use Storage Navigator to format the volume.
- If the volume that has the destination LDEV number is not blocked, the data on the volume might not have been deleted.
  The data on the volume might not have been deleted. If the data must be deleted, either format the volume or use the procedure below to delete the data. Note that the following procedure assumes that LDEV `10:01` has been migrated to LDEV `20:01` (Also note that the LDEV numbers of the volumes have been reversed.):
  1. Set a LUN path to LDEV `20:01`, and allocate it to a host.
  2. From the host, enter `0` for the size of the volume to delete any data remaining on LDEV `20:01`.
  3. Remove the LUN path to LDEV `20:01`.

If the task status is MIGRATION FAILURE:

Depending on the cause of the error, even if migration processing has been completed in the storage system, Tiered Storage Manager or Device Manager might treat the processing as having failed. As such, do the following:

1. Use Device Manager to refresh all the storage systems, and update the management information in Tiered Storage Manager and Device Manager.
   If reserved volumes remain, their reservation is canceled during the refresh processing.
2. For the migration task that is in the failed status, display the volume information and check whether the volumes have already been migrated.
   Also, check the parity group names and storage system names for all LDEVs at the migration source.
3. If there are LDEVs that have not been migrated yet, remove the cause of the error, and then re-create and execute the migration task.

Related tasks

- Starting the Hitachi Command Suite services on page 458
- Stopping the Hitachi Command Suite services on page 460

Tiered Storage Manager operations cannot be performed because an error occurred in the database

If Tiered Storage Manager has become inoperable due to a database error, restore the database from a previously-created backup.

Cause

The repository cannot be accessed because an error occurred in the database.

Countermeasure

Restore a backed up database.

Related concepts

- Restoring databases on page 475

How to troubleshoot problems on a host

This section describes how to troubleshoot problems that occur due to Device Manager agent.

The HiScan command cannot add host information to the Device Manager server

If the `HiScan` command fails to add host information to the Device Manager server and causes an error message to be output, take the action appropriate for the cause.

Cause

If the KAIC22019-E error message is output:

Possible causes of the error are as follows:

- The LUN path to the volume managed by the Device Manager recognized by the host has been disabled, possibly due to a lost connection.
- This problem might occur if a host recognizes 100 or more LUs that are managed by Device Manager.

If the KAIC22009-E, KAIC22014-E, or KAIC22048-E error message is output:

This problem might occur if a host recognizes 100 or more LUs that are managed by Device Manager.

Countermeasure

If the LUN path to a volume that is managed by Device Manager and is recognized by the host is disabled:

Either restore the disabled LUN path, or change the OS settings so that the disabled LUN path is no longer recognized.

If the number of LUs that are managed by Device Manager and are recognized by the host exceeds 100:

Change the host settings so that the host can manage 100 or more LUs per host.

Related concepts

- Settings required for a host to manage 100 or more LUs on page 524

A communication error occurs, and the processing of other Hitachi Command Suite products stops

If processing of another Hitachi Command Suite product stops due to a communication error, wait a few minutes and then restart the processing.

Cause

Another Hitachi Command Suite product might have attempted to access the Device Manager agent either immediately after the installation of the Device Manager agent was complete, or immediately after the Device Manager agent services started.

Countermeasure

Wait a few minutes, and then retry the operation.

Two copies of HBase Agent are displayed in the Programs and Features window

In a Windows environment, two instances of HBase Agent are sometimes displayed in the Programs and Features windows on machines where the Device Manager agent or Dynamic Link Manager is installed. If two instances of HBase Agent are displayed, execute the `hbsa_util` command to delete the registry entries and files for the Device Manager agent.

Related references

- Deleting the Device Manager agent's registry entries and files (hbsa_util command) on page 532

HBase Agent is displayed in the Programs and Features window

In a Windows environment, HBase Agent sometimes remains in the Programs and Features window after uninstalling both the Device Manager agent and Dynamic Link Manager. If HBase Agent remains, execute the `hbsa_util`

command to delete the registry entries and files for the Device Manager agent.

Related references

- Deleting the Device Manager agent's registry entries and files (hbsa_util command) on page 532

JavaVM terminates abnormally

In a Windows (x64 or IPF) environment, if JavaVM terminates abnormally, edit the `Server.cmd` file.

Cause

Another program linked with Device Manager might be frequently accessing the Device Manager agent that is running.

Countermeasure

To edit the `Server.cmd` file:

1. Open the `Server.cmd` file with a text editor. The location of this file is as follows:
   installation-folder-for-Device-Manager-agent`\agent\bin\Server.cmd`
2. Add `-Djava.compiler=NONE` as a Java startup option.
   The following shows an example of editing the `Server.cmd` file:

```
.java -Dalet.msglang -Djava.compiler=NONE %1 %2 -classpath
"C:\Program Files\HITACHI\HDVM\HBaseAgent\agent\jar
\agent4.jar;C:\Program Files\HITACHI\HDVM\HBaseAgent\agent
\jar\jdom.jar;C:\Program Files\HITACHI
\HDVM\HBaseAgent\agent\jar\xerces.jar;C:\Program Files
\HITACHI\HDVM\HBaseAgent\agent
\jar\servlet.jar;C:\Program Files\HITACHI\HDVM\HBaseAgent
\agent\jar
\log4j-1.2.3.jar" com.Hitachi.soft.HiCommand.DVM.agent4.as.
export.Server %*
exit /b %ERRORLEVEL%
```

An OutOfMemory error occurs on a host, and after a while the host stops responding

An OutOfMemory error sometimes occurs on a host when, for example, a host is refreshed. In this kind of case, if after a while the host stops responding, take the action appropriate for the cause.

Cause

- This problem might occur if a host recognizes 100 or more LUs that are managed by Device Manager.
- This problem might occur due to high load on the Device Manager server. If so, the following error message will have been output to the log file

specified by the -t option of the HiScan command or to the HiScan.msg file:

```
<html><head><title>400 Bad request</title>
<meta http-equiv="Content-Type" content="text/html;
charset=ISO-8859-1">
</head><body>
<h1>400 Bad request</h1>
<p><strong>ServiceConnection#0: java.lang.OutOfMemoryError</
strong>
</body></html>
```

The HiScan.msg file is stored in the following locations:

In Windows:

installation-folder-for-the-Device-Manager-agent\bin\logs\

In Linux:

installation-directory-for-the-Device-Manager-agent/bin/logs/

In Solaris or HP-UX:

/opt/HDVM/HBaseAgent/bin/logs/

In AIX:

/usr/HDVM/HBaseAgent/bin/logs/

Countermeasure

- If one host recognizes 100 or more LUs that are managed by Device Manager, change the host settings so that the host can manage 100 or more LUs.
- If the Device Manager server is highly loaded, take action as follows:
  - Change the memory heap size on the Device Manager server.
  - If multiple hosts concurrently execute the HiScan command, use the hdvmagt_setting command to adjust the HiScan command execution schedule of those hosts.

Related concepts

- Settings required for a host to manage 100 or more LUs on page 524

Related tasks

- Changing the memory heap size on page 36

Related references

- Setting the Device Manager server's information, HiScan command's execution period, and CCI's information (hdvmagt_setting command) on page 533

- Reporting host information to the Device Manager server manually (HiScan command) on page 537

The file system name is not displayed in the Device Manager GUI

In a Solaris environment, if the file system name is not displayed in the Device Manager GUI, use VxVM 4.0 or later.

Cause

When using a version of VxVM earlier than 4.0, the Device Manager agent does not notify the Device Manager server of correspondence between the file system and LUN if device names are set based on the enclosure.

Countermeasure

To check the correspondence between the file system and LUN, use VxVM version 4.0 or later.

Changes to the storage system configuration are not applied to the Device Manager server

If changes to the storage system configuration are not applied to the Device Manager server, use the `hldutil` command or the `HiScan` command to apply the latest information to the Device Manager server.

Cause

The OS might not recognize the modified contents immediately after the storage system configuration is changed (for example, when an LU is registered or deleted). In this case, the Device Manager agent reports the old information to the Device Manager server.

Countermeasure

1. Execute the `hldutil` command to check the latest information.
2. Restart the host OS.
3. Execute the `HiScan` command.

Related references

- Reporting host information to the Device Manager server manually (HiScan command) on page 537
- Acquiring device information (hldutil command) on page 539

Errors requiring no action

For errors listed below, no action is required.

- The following messages are output to the event log or system log when multiple instances of the `HiScan` command are executed simultaneously:
  - `[HORCM_005] Could not create endpoint for remote connection.`

    - `[HORCM_007] Illegal parameter values in HORCM configuration file.`
- When a S-VOL in the pair status is being mounted, one of the following messages for event ID 51 or 57 is output to the Windows event log:
    - Event ID: 51

      `An error was detected on device \Device\Harddisk`*nn*`\DR`*n* `during a paging operation.`
    - Event ID: 57

      `The system failed to flush data to the transaction log. Corruption may occur.`
- If the same `HiScan` command execution interval is set on the active and standby nodes of the Device Manager agent, `SC_DISK_ERR2` (Device Busy) or `HSDRV_RSV_CONFLICT` is output to the AIX error log for the secondary node.

  This problem sometimes occurs if the I/O load on the shared disk is high. The active node is providing disk reserve normally for the shared disk, and therefore there is no problem with the system. Shared disk information is acquired from the Device Manager agent running on the active node, and therefore there is no problem with the operation of Device Manager.
- The `rpm -V` command executed in a Linux environment fails.

Maintenance information that must be collected if a failure occurs

If you cannot identify the cause of a failure or recover from a failure, collect the maintenance information, and then contact our support center.

If a failure occurs, you need to collect the following information to determine the cause of the failure:

- System status after the failure
- Date and time when the failure occurred
- Situation in which the failure occurred
- Network configurations of the management server and the host
- OSs of the management server and the host
- Maintenance information for the computers where the failure occurred
    - Maintenance information for the management server
    - Maintenance information for Host Data Collector

      If you are using Host Data Collector installed on a computer other than the management server, you also need to collect maintenance information for the Host Data Collector computer. If Host Data Collector is installed on the management server, executing the `hcmds64getlogs` command automatically acquires maintenance information for Host Data Collector.
    - Maintenance information for the host
- Java VM thread dump

If any of the following problems occurs, you need to acquire the thread dumps of HCS Device Manager Web Service to locate the cause of the problem.
  - The Device Manager logon window is not displayed when you start the GUI.
  - The Device Manager main window is not displayed after logging on to Device Manager.
  - The Device Manager main window is not displayed when you start a Device Manager server from Tuning Manager.

Note: Depending on the system configuration and where a failure occurs, the log files of other programs might be required for failure analysis.

- When performance information is viewed from the Mobility tab or the Analytics tab:
  The log files of the Tuning Manage server and Tuning Manager - Agent for RAID are required.
- When performance information is viewed from the Replication tab:
  The log files of the Replication Manager server, Tuning Manager server, and Tuning Manager - Agent for RAID are required.
- When virtualization servers are managed via Device Manager:
  The log files of the virtualization software and VMware vCenter Server are required.
- When Hitachi Data Ingestor or Hitachi NAS Platform F is managed via Device Manager:
  The Hitachi File Services Manager log file is required.
- When application server (host) information is synchronized between Device Manager and Compute Systems Manager:
  The Compute Systems Manager log file is required.

For details on how to acquire log files for any program other than Device Manager and Tiered Storage Manager, the manual for that program.

Acquiring maintenance information on the management server (hcmds64getlogs command)

Execute the `hcmds64getlogs` command to acquire maintenance information on the management server.

Operations to complete in advance

Log in as a user with Administrator permissions (for Windows) or as a root user (for Linux).

Command format

In Windows:

installation-folder-for-Hitachi-Command-Suite\Base64\bin\hcmds64getlogs /dir *folder-name* [/types *Hitachi-Command-Suite-product-name*[*Hitachi-Command-Suite-product-name* ...]] [/arc *archive-file-name*] [/logtypes *log-file-type*[*log-file-type* ...]]

In Linux:

installation-directory-for-Hitachi-Command-Suite/Base64/bin/hcmds64getlogs -dir *directory-name* [-types *Hitachi-Command-Suite-product-name*[*Hitachi-Command-Suite-product-name* ...]] [-arc *archive-file-name*] [-logtypes *log-file-type*[*log-file-type* ...]]

Caution: Do not execute more than one `hcmds64getlogs` command simultaneously.

Note: If Hitachi File Services Manager or Storage Navigator Modular 2 is linked, you can also collect maintenance information for Hitachi File Services Manager or Storage Navigator Modular 2 by omitting the `types` and `logtypes` options when you execute the command.

Options

dir

Specify the absolute path to the directory on a local disk that contains collected maintenance information. If the directory has already been created, empty the directory.

The maximum length of a path name that can be specified is 41 bytes. You can specify any printable ASCII character excluding certain special characters. You cannot specify the following characters:

`\ / : , ; * ? " < > | $ % & ' ` `

However, you can specify backslashes (`\`), colons (`:`), and forward slashes (`/`) in Windows, or forward slashes (`/`) in Linux as a path delimiter. Do not specify a path delimiter at the end of a path name.

In Windows, to specify a space character in a path name, enclose the path name in double quotation marks (`"`). In Linux, you cannot specify a space character in a path name.

types

Specify the names of the products to be acquired by using the table below if the maintenance information for only specific Hitachi Command Suite products can be collected. To specify multiple product names, separate them by a space.

Table 109 Values specified for the type option when collecting maintenance information

Product	Value
Device Manager	`DeviceManager`
Tiered Storage Manager	`TieredStorageManager`
Replication Manager	`ReplicationManager`
Other products	Refer to the manual for each product.

When specifying this option, also specify the log file type `log` for the `logtypes` option.

If this option is not specified, the maintenance information for all Hitachi Command Suite products installed on the same management server is collected.

arc

Specify the name of the archive files to be created. If you do not specify this option, the default file name is `HiCommand_log_64`.

For the file name, you can specify any printable ASCII character excluding certain special characters. You cannot specify the following characters:

`\ / : , ; * ? " < > | $ % & ' ``

In Linux, you cannot specify a space character in a file name.

logtypes

Specify the types of log files to acquire when log files of a particular type cannot be collected due to a failure.

`log`: Specify this to acquire `.jar` files and `.hdb.jar` files only.

`db`: Specify this to acquire `.db.jar` files only.

`csv`: Specify this to acquire `.csv.jar` files only.

To specify multiple types, separate them by a space.

If you omit this option, all log files will be acquired.

Note: If the Replication tab is used in a large-scale system environment, obtaining maintenance information takes time, and the maintenance information files are large. Therefore, to execute the `hcmds64getlogs` command, we recommend that you specify the following option to obtain the maintenance information.

In Windows:

installation-folder-for-Hitachi-Command-Suite\Base64\bin
\hcmds64getlogs /dir *folder-name* /logtypes log csv

In Linux:

installation-directory-for-Hitachi-Command-Suite/Base64/bin/
hcmds64getlogs -dir *directory-name* -logtypes log csv

When this command is executed, the KAPM05318-I or KAPM05319-E message is output. In addition, maintenance information (log file and database file) is acquired and four archive files (.jar, .hdb.jar, .db.jar, and .csv.jar) are output in the directory specified in the dir option.

Tip: If the KAPM05318-I or KAPM05319-E message is not output, the hcmds64getlogs command did not complete because sufficient free space was not available for the directory specified in the dir option. Free up sufficient space in the directory, and then re-execute the hcmds64getlogs command.

Generating the Tiered Storage Manager CLI log file

If the Tiered Storage Manager CLI is installed on the management server, you can use the hcmds64getlogs command to collect Tiered Storage Manager CLI log files with the other log files. To acquire both log files by using one operation, you must specify the environment settings in the HtsmgetTI.properties file.

Procedure

Set the necessary properties in the HtsmgetTI.properties file stored in the following location.

In Windows:

installation-folder-for-Hitachi-Command-Suite
\TieredStorageManager\SupportTools\CollectTool\

In Linux:

installation-directory-for-Hitachi-Command-Suite/
TieredStorageManager/SupportTools/CollectTool/

Table 110 Properties set in the HtsmgetTI.properties file

Property	Description
CLI_DIR	Specify the directory in which Tiered Storage Manager CLI is installed. The following are the default installation directories: • In Windows: *installation-folder-for-Hitachi-Command-Suite* \TieredStorageManager\CLI • In Linux:

Property	Description
	*installation-directory-for-Hitachi-Command-Suite/*TieredStorageManager/CLI
SYSLOG	In Linux, specify the absolute path to syslog. The default directory is: /var/log/messages

Acquiring maintenance information for a Host Data Collector computer (hdc_getras command)

Execute the hdc_getras command to acquire maintenance information for a Host Data Collector computer that manages virtualization servers.

Operations to complete in advance

Log in as a user with Administrator permissions (for Windows) or as a root user (for Linux).

Command format

In Windows:

installation-folder-for-Host-Data-Collector\HDC\Base\bin\hdc_getras.bat -o *folder-name* [-f]

In Linux:

installation-directory-for-Host-Data-Collector/HDC/Base/bin/hdc_getras.sh -o *directory-name* [-f]

- o
  Use the absolute path or a relative path from the current directory to specify the output destination for the maintenance information.
  You can specify any printable ASCII character other than the following special characters:
  \ / : , ; * ? " < > | $ % & ' ` ^
  However, you can specify backslashes (\), colons (:), and forward slashes (/) in Windows, or forward slashes (/) in Linux as a path delimiter.
- f
  Use this option to forcibly overwrite the directory if the directory specified by the o option already exists.

Maintenance information is output to the following location:

In Windows:

folder-specified-for-the-o-option\hdcResult

In Linux:

directory-specified-for-the-o-option/hdcResult

Acquiring maintenance information on a host managed by Host Data Collector (hdc_target_getras command)

Execute the `hdc_target_getras` command to acquire maintenance information on a normal host or virtual machine managed by Host Data Collector.

Operations to complete in advance

- Copy a file to the host
  Copy the following file to the target managed host from the computer on which Host Data Collector is installed:

  In Windows:

  installation-folder-for-Host-Data-Collector\Base\bin\hdc_target_getras.bat

  In UNIX:

  installation-directory-for-Host-Data-Collector/Base/bin/hdc_target_getras.sh

- Log in as a user with Administrator permissions (for Windows) or as a root user (for UNIX)

Command format

In Windows:

```
hdc_target_getras.bat -o folder-name [-f]
```

In UNIX:

```
hdc_target_getras.sh -o directory-name [-f]
```

- o
  Use the absolute path or a relative path from the current directory to specify the output destination for the maintenance information.
  You can specify any printable ASCII character other than the following special characters:
  \ / : , ; * ? " < > | $ % & ' ` ^
  However, you can specify backslashes (\), colons (:), and forward slashes (/) in Windows, or forward slashes (/) in UNIX as a path delimiter.
- f
  Use this option to forcibly overwrite the directory if the directory specified by the o option already exists.

Maintenance information is output to the following location:

In Windows:

folder-specified-for-the-o-option\target_hdcResult

In UNIX:

directory-specified-for-the-o-option/target_hdcResult

Acquiring maintenance information on the Device Manager agent (TIC command)

Execute the TIC command to acquire maintenance information on a normal host or virtual machine managed by the Device Manager agent.

Operations to complete in advance

Log in as a user with Administrator permissions (for Windows) or as a root user (for UNIX).

Command format

In Windows:

TIC.bat [-outdir *folder-name* [-f] [-d [*addon-module-name*]]]

In Solaris or HP-UX:

TIC.sh [-outdir *directory-name* [-f] [-d [*addon-module-name*]]]

In AIX or Linux:

TIC.sh [-outdir *directory-name* [-f]]

Location of the command

In Windows:

installation-folder-for-Device-Manager-agent\bin

In Linux:

installation-directory-for-Device-Manager-agent/bin

In Solaris or HP-UX:

/opt/HDVM/HBaseAgent/bin

In AIX:

/usr/HDVM/HBaseAgent/bin

Options

-outdir

Use the absolute path or a relative path from the current directory to specify the output destination for the maintenance information.

Note that you cannot use the following characters for any elements other than path separators:

\ / : , ; * ? " < > | $ % & ' ` ^

If this option is omitted, the directory that contains the TIC command will be used as the output destination.

-f

Specify this option to forcibly overwrite the directory specified by the –outdir option if the specified directory already exists.

-d

Specify the following abbreviations for add-on modules whose error information you wish to remove from the acquisition target:

hglm: Global Link Manager agent (Windows, Solaris, or HP-UX only)

hrpmap: Replication Manager Application agent

If you specify multiple parameters, separate them with commas (,). If the name of the add-on module is omitted, the error information for the Global Link Manager agent and Replication Manager Application agent is not acquired.

Maintenance information is output to the following location:

In Windows:

folder-specified-for-the-outdir-option\resultDir

In UNIX:

directory-specified-for-the-outdir-option/resultDir

Acquiring a thread dump of the HCS Device Manager Web Service (Windows)

To acquire a thread dump of HCS Device Manager Web Service, create a file called dump, and then restart HCS Device Manager Web Service.

Procedure

1. In *installation-folder-for-Hitachi-Command-Suite*\Base64\uCPSB\CC\server\public\ejb\DeviceManagerWebService, create a file called dump.
2. Access the Windows Services window.
3. Stop the HCS Device Manager Web Service.
4. From the Services window, start the HCS Device Manager Web Service.

Result

The `javacore`*`xxx`*`.`*`xxx`*`.txt` file is output when using JDK bundled with Hitachi Command Suite, or the `DeviceManagerWebService.log` file is output when using Oracle JDK, to the following folder:

`installation-folder-for-Hitachi-Command-Suite``\Base64\uCPSB\CC\server\public\ejb\DeviceManagerWebService`

If you are using the Oracle JDK, the `DeviceManagerWebService.log` file is overwritten each time it is output. We recommend saving the file by using a different name after the file is output.

Acquiring a thread dump of the HCS Device Manager Web Service (Linux)

To acquire a thread dump of HCS Device Manager Web Service, execute the `kill` command, and then restart the Hitachi Command Suite product services.

Procedure

1. Execute the following command:

   `# kill -3 `*`PID`*

   PID is a process ID written in the *`installation-directory-for-Hitachi-Command-Suite`*`/Base64/uCPSB/CC/server/public/ejb/DeviceManagerWebService/logs/CC/maintenance/cjstdout.log` file.

   Multiple process IDs are written to the `cjstdout.log` file. Specify the last process ID written to the file.
2. Restart the Hitachi Command Suite product services.

Result

The `javacore`*`xxx`*`.`*`xxx`*`.txt` file is output when using JDK bundled with Hitachi Command Suite, or the `DeviceManagerWebService.log` file is output when using Oracle JDK, to the following directory:

`installation-directory-for-Hitachi-Command-Suite``/Base64/uCPSB/CC/server/public/ejb/DeviceManagerWebService`

If you are using the Oracle JDK, the `DeviceManagerWebService.log` file is overwritten each time it is output. We recommend saving the file by using a different name after the file is output.

Related tasks

- Starting the Hitachi Command Suite services on page 458
- Stopping the Hitachi Command Suite services on page 460

A

Device Manager server properties

This section describes the property files of a Device Manager server.

- Device Manager server property files
- Device Manager server configuration properties (server.properties file)
- Device Manager database properties (database.properties file)
- Device Manager log output properties (logger.properties file)
- Device Manager dispatcher properties (dispatcher.properties file)
- Device Manager MIME type properties (mime.properties file)
- Device Manager client properties (client.properties file)
- Device Manager security properties (server.properties file and cimxmlscpa.properties file)
- Device Manager SNMP trap log output properties (customizedsnmptrap.properties file)
- Device Manager launchable applications properties (launchapp.properties file)
- Properties for communicating with the host (host.properties file)
- Properties for connecting to Host Data Collector (hostdatacollectors.properties file)
- Properties for migrations (migration.properties file)

- Properties for connecting to Tuning Manager (tuningmanager.properties file)
- Properties related to the Replication tab (replication.properties file)
- Properties for connecting to Replication Manager (rpmlib.properties file)
- Properties for the CIM/WBEM functions (jserver.properties file, cimxmlcpa.properties file, cimxmlscpa.properties file)

Device Manager server property files

Device Manager server property files include property files related to Device Manager configuration information and the Device Manager database.

The following table describes the contents of property files of a Device Manager server.

Table 111 Property files of a Device Manager server

Property file	Description
`server.properties` file	This property file contains the Device Manager server configuration information. ***Warning:*** Do not attempt to optimize these attributes unless you are an expert, because even minor changes could severely impact the performance of the Device Manager server.
`database.properties` file	This property file is related to the Device Manager database. ***Warning:*** Do not attempt to optimize these attributes unless you are an expert, because even minor changes could severely impact the performance of the Device Manager server.
`logger.properties` file	This property file is related to the Device Manager log output.
`dispatcher.properties` file	This property file is related to Device Manager threads.
`mime.properties` file	This property file is related to MIME (Multipurpose Internet Mail Extensions) types for Device Manager.
`client.properties` file	This property file is related to the Device Manager GUI. | • `server.properties` file • `cimxmlscpa.properties` file	This property file is related to Device Manager security.
`customizedsnmptrap.properties` file	This property file is related to the log output of the SNMP traps received by Device Manager.
`launchapp.properties` file	This property file is related to the applications that can be launched from Device Manager.
`host.properties` file	This property file is related to communicating with hosts.
`hostdatacollectors.properties` file	This property file is related to the connection to Host Data Collector.
`migration.properties` file	This property file is related to migrations.
`tuningmanager.properties` file	This property file is related to the connection to Tuning Manager.
`replication.properties` file	This property file is related to the Replication tab.
`rpmlib.properties` file	This property file is related to the connection to Replication Manager.
• `jserver.properties` file	This property file is related to the CIM/WBEM functions.

Property file	Description
• `cimxmlcpa.properties` file • `cimxmlscpa.properties` file	

Caution:
- For ordinary use, you do not need to change the values set in the property files of a Device Manager server.
  Use extreme caution when you are modifying the values, because you can cause the server to fail or to function incorrectly. Do not modify the values unless you have sufficient expertise.
- The default values are set during a new installation.
- If you perform an overwrite or upgrade installation, values set in the property files of a Device Manager server before the installation are inherited.

Changing Device Manager server properties

Use a text editor to edit the property files of a Device Manager server.

Before you begin

Log in as a user with Administrator permissions (for Windows) or as a root user (for Linux).

Procedure

1. Stop the services of Hitachi Command Suite product.
2. Use a text editor to specify the appropriate values in the Device Manager server property files.
3. Start the services of Hitachi Command Suite product.

Related tasks

- Starting the Hitachi Command Suite services on page 458
- Stopping the Hitachi Command Suite services on page 460

Syntax rules for Device Manager server property files

The property files are in the Java property file format.

Property files must be created according to the following description conventions:
- Each property must be entered as a combination of a property name and value separated by an equals sign (=). For example, `foo.bar=12345`.
- Each property must be separated by a line delimiter (a line feed character).
- A line beginning with a hash mark (#) is a comment line.

- You do not need to insert quotation marks around literals (text strings or numerical values).
- 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\docroot\foo.bar` should be entered as `C:\\HiCommand\\docroot\\foo.bar`. When you specify properties, there is no need to precede other characters with the escape character `\`.
- If two or more entries in a property file have the same property name, the value of the last such property specified in the file will take effect.
- If a line ends with a backslash (\), the next line is a continuation of the current line.

Device Manager server configuration properties (server.properties file)

The `server.properties` file contains the server configuration properties.

- In Windows:
  installation-folder-for-Hitachi-Command-Suite\DeviceManager\HiCommandServer\config\server.properties
- In Linux:
  installation-directory-for-Hitachi-Command-Suite/HiCommandServer/config/server.properties

server.http.host

Specify host names or IP addresses of the management server (Device Manager server).

To specify the IP address, use one of the following formats:

IPv4 format:

x.*x*.*x*.*x* (*x*: integer from 0 to 255)

IPv6 format:

Specify hexadecimal numbers by using colons (:). You can also use a short format. You can only use global IPv6 addresses.

A value specified for the host name or IP address must be accessible from clients (GUI, CLI, and storage systems).

Default: The host name or IP address of the management server specified during installation (if an error occurs when registering the URL, `localhost` is set).

Caution:

- If multiple NICs are installed on the server computer on which Device Manager is installed, specify the IP address of the NIC that belongs to the network to which the clients (GUI, CLI, and storage systems) connect. Do not specify the host name.
- In a cluster environment, the IP address of the cluster manager should be specified.
- If Device Manager manages SMI-S enabled storage systems and the setting value of this property has been changed, you must refresh any SMI-S enabled storage system that is a management target.
- In the following cases, if you have changed the setting value for this property, reconfigure user account authentication in the Edit Storage Systems window for the Device Manager GUI:
  - For VSP G1000, G1500 or VSP F1500, when Hitachi Command Suite is used to authenticate user accounts to log in to CCI and the SVP
  - When you operate VSP Gx00 models or VSP Fx00 models

server.http.port

Specify the port to be used for non-SSL communication by the Device Manager server.

The conventional port number used for a standard web server is 80, but there might already be an intranet server running on this port. Moreover, you should avoid low-numbered ports because these could conflict with other services installed on the server. As a general rule, you can pick any port between `1024` and `49151`.

`80` is used for the port number when this property is set to a space character.

Default: `2001`

Caution: If you change the value of this property, you also need to change the following settings:

- The port number for Device Manager registered in the Device Manager agent (the `hdvmagt_setting` command)
- The `hdvm.port` property of the Tiered Storage Manager server
- The port number for the Device Manager server of the information source registered in Replication Manager (for non-SSL communication with the Device Manager server)
- The port number for the Device Manager server registered in the file server management software

  For details on how to change the port number in the file server management software, see the file server manuals.

- The `HiCommandCLI.serverurl` property of the `HiCommandCLI.properties` file in the Device Manager CLI (for non-SSL communication with the Device Manager server)

Related tasks

- Changing pop-up blocker settings on page 293
- Enabling SSL/TLS for the Device Manager CLI computer on page 294
- Changing the communication protocol between the Replication Manager server and the Device Manager server on page 303
- Changing Tiered Storage Manager server properties on page 642

Related references

- Setting the Device Manager server's information, HiScan command's execution period, and CCI's information (hdvmagt_setting command) on page 533
- hdvm.port on page 649

server.https.port

Specify the port to be used for SSL communication by the Device Manager server.

The conventional port number for a secure web server is `443`, but there might already be a secure intranet server running on this port. As noted above, it is better practice to utilize a port number between 1024 and 49151 for a specialized (middleware) HTTP server. Make sure that it has a different value than the port designated for the HTTP listener.

Default: `2443`

Caution: If you change the value of this property, you also need to change the following settings:

- The port number for Device Manager registered in the Device Manager agent (the `hdvmagt_setting` command)
- The port number for the Device Manager server of the information source registered in Replication Manager (for SSL communication with the Device Manager server)
- The `HiCommandCLI.serverurl` property of the `HiCommandCLI.properties` file in the Device Manager CLI (for SSL communication with the Device Manager server)

In the following cases, if you have changed the setting value for this property, reconfigure user account authentication in the Edit Storage Systems window for the Device Manager GUI:

- For VSP G1000, G1500 or VSP F1500, when Hitachi Command Suite is used to authenticate user accounts to log in to CCI and the SVP
- When you operate VSP Gx00 models or VSP Fx00 models

Related tasks

- Changing pop-up blocker settings on page 293
- Enabling SSL/TLS for the Device Manager CLI computer on page 294
- Changing the communication protocol between the Replication Manager server and the Device Manager server on page 303

Related references

- Setting the Device Manager server's information, HiScan command's execution period, and CCI's information (hdvmagt_setting command) on page 533

server.rmi.port

Specify the port used for the Device Manager RMI server.

You should avoid low-numbered ports because these could conflict with other services installed on the server. As a general rule, you can pick any port between `1024` and `65535`.

Default: `23055`

Caution: If you change the value of this property, you must also change the values of the Device Manager server `client.rmi.port` property and the Tiered Storage Manager `hdvm.rmi.port` property to the same value.

Related references

- client.rmi.port on page 615
- hdvm.rmi.port on page 649

server.http.entity.maxLength

Specify in bytes the maximum length of an HTTP request entity to be permitted by the Device Manager server.

Under normal conditions, you do not need to change the default value of this property. It helps prevent certain types of denial of service and attempted buffer overflow attacks by restricting the effect of malicious requests that contain unusually large payload entities. If the server detects a posted request longer than this value, it sends an error response to the client and logs details of the attempted request.

Default: `3000000`

Note: If you register a file server that has many file systems and storage pools into Device Manager, information sent from the file server might not be applied to Device Manager properly. In this case, change the property value to a value greater than the default.

server.base.home

This property contains the installation directory of Common Component, which is set by the Device Manager installer.

Under normal conditions, you do not need to change the default value of this property.

Default: Value set by the installer

server.horcmconfigfile.hostname

Specify whether to use the IP address (`ipaddress`) or the host name (`hostname`) when Device Manager edits the configuration definition file.

Default: `ipaddress`

Caution:

- Changing the IP address or host name specified when a copy pair was created might disable operations on the copy pair. If this is the case, you need to modify the configuration definition file and refresh the storage systems.
- The setting for this property is ignored in Replication Manager.

Related references

- Notes on managing copy pairs on page 88

server.base.initialsynchro

Specify whether to synchronize the management information database and the displayed information (Common Component repository) when you start Device Manager.

A setting of `true` will synchronize the information. A setting of `false` will not synchronize the information.

Default: `false`

Caution: If this property is set to `true`, synchronization of the information will take several minutes. If you change the property and then log in to Device Manager right away, an error might occur. In such a case, wait until the synchronization has finished, and then log in.

server.cim.agent

Specify the name of the host on which the Device Manager agent is installed when the function for acquiring storage system performance information is used.

Performance information can be acquired only when this property is specified.

Default: None

server.cim.support

Specify whether CIM support is enabled.

Specify whether to enable the CIM function.

To enable the CIM function, set this property to `true`. To disable the CIM function, set this property to `false`.

Default: `true`

server.cim.support.job

Specify whether a method for creating or deleting a volume, setting or releasing a LUN path, setting or canceling security for a LUN, or creating or deleting a LUSE volume is executed asynchronously or synchronously.

If you set this property to `true`, the method is executed asynchronously. If you set this property to `false`, the method is executed synchronously. If the CIM client does not support the job control subprofile, specify `false`.

If you specify any values other than `true` or `false`, or if this property does not exist, the method is executed asynchronously.

Default: `true`

server.cim.support.protocol

Specify whether to open or close the ports used by the CIM function.

A value of `1` to `3` can be specified. The value specified for this property determines whether to open or close the non-SSL communication ports (default: 5988/tcp) and SSL communication ports (default: 5989/tcp).

`1`: The non-SSL communication ports are open, and the SSL communication ports are closed.

`2`: The non-SSL communication ports are closed and the SSL communication ports are open.

`3`: Both the non-SSL communication ports and the SSL communication ports are open.

Default: `3`

Related references

- server.cim.http.port on page 596
- server.cim.https.port on page 597

server.cim.http.port

Specify the port for non- SSL transmission for the CIM function.

Default: `5988`

Caution: If you change the value of this property, also change the `HTTPPort` property of the Device Manager server to the same value.

Related references

- server.cim.support.protocol on page 596
- HTTPPort on page 639

server.cim.https.port

Specify the port for SSL transmission, for the CIM function.

Default: `5989`

Caution: If you change the value of this property, also change the `HTTPSPort` property of the Device Manager server to the same value.

Related references

- server.cim.support.protocol on page 596
- HTTPSPort on page 639

server.configchange.enabled

Specify whether to automatically update (refresh) storage system information in the database when the storage system configuration is changed by a storage management tool (Element Manager) launched from the GUI.

For Universal Storage Platform V/VM, if you specify `true`, storage system information in the database is automatically refreshed immediately after the configuration change. For HUS100, Hitachi AMS2000, Hitachi SMS, or Hitachi AMS/WMS, if you specify `true`, whether the configuration has been changed is checked at the interval specified in the following properties, and storage system information in the database is automatically refreshed if the configuration has been changed:

For HUS100, Hitachi AMS2000 or Hitachi SMS

`server.dispatcher.snm2.configchange.pollingPeriod` property

For Hitachi AMS/WMS

`server.dispatcher.configchange.pollingPeriod` property

If you specify `false`, it is not automatically refreshed.

Default: `true`

Related references

- server.dispatcher.snm2.configchange.pollingPeriod on page 607
- server.dispatcher.configchange.pollingPeriod on page 608

server.logicalview.initialsynchro

Specify whether to forcibly synchronize the storage system information in the database with the information displayed in the GUI or CIM/WBEM functions when Device Manager server is started.

If you specify `true`, the information will be synchronized. If you specify `false`, the information will not be synchronized.

Default: `false`

server.mail.enabled.storagesystem

Specify whether to send the following content to users by email.

- Storage system alerts
- Device Manager GUI and Tiered Storage Manager events
- Health check results

To enable this email notification function, set this property to `true`. To disable this function, set this property to `false`.

Default: `true`



Caution: If this property is set to `true`, set the `server.mail.smtp.host` property.

Related references

- server.mail.smtp.host on page 599

server.mail.enabled.fileserver

Specify whether to send file server or NAS module alerts to users by email.

To enable this email notification function, set this property to `true`. To disable this function, set this property to `false`.

For a file server or NAS module, the timing of when polls and SNMP traps detect errors is different, but the same information is displayed in their alerts. Therefore, if you specify `true`, alerts for both the polls and SNMP traps are sent by email.

Default: `true`



Caution: If this property is set to `true`, set the `server.mail.smtp.host` property.

Related references

- server.mail.smtp.host on page 599

server.mail.from

Specify the email address of the notification source (sender) used to send alerts, events, and health check results to users by email.

Depending on the operating environment, users might not receive email from an address that does not include a domain name. In this case, change the value of this property or the email settings (including the SMTP server and receiver filter settings).

If no value is specified or the specified value is invalid, the default value is set.

Default: `hdvmserver`

server.mail.smtp.host

Specify the host name or IP address of the SMTP server.

To send alerts, events, and health check results to users by email, you must specify this property. The IP address can be specified in either IPv4 or IPv6 format.

Default: None



Caution: If you set this property, specify `true` for the `server.mail.enabled.storagesystem` or `server.mail.enabled.fileserver` property.

Related references

- server.mail.enabled.storagesystem on page 598
- server.mail.enabled.fileserver on page 598

server.mail.smtp.port

Specify the port number of the SMTP server.

To send alerts, events, and health check results to users by email, you must specify this property.

Specifiable range: `0` to `65535`.

Default: `25`

server.mail.smtp.auth

Specify whether to use SMTP authentication to send alerts, events, and health check results to users by email.

To use SMTP authentication, set this property to `true`. To not use SMTP authentication, set this property to `false`.

Default: `false`

server.mail.errorsTo

Specify the address to which an undeliverable notification email will be sent when alert email notifications, event email notifications, and health check results email notifications cannot be delivered.

If this property is not specified, notifications for undeliverable emails are sent to the email address specified in `server.mail.from` in the `server.properties` file of the Device Manager server. Note that the conditions for sending undeliverable notification emails vary according to the SMTP server settings. Make sure to review these settings.

Default: None

Related references

- server.mail.from on page 599

server.eventNotification.mail.to

Specify the send destination address for alert and event notification emails.

All alerts and events are sent to the email address specified in this property.

Default: None

server.mail.alert.type.storagesystem

Specify the type of storage system alerts that are sent to users by email.

The following values can be specified:

- `Trap`: Reports only the alerts detected by SNMP traps.
- `Server`: Reports only the alerts detected by the polls that Device Manager conducts.
- `All`: Reports the alerts detected by both SNMP traps and the polls that Device Manager conducts. Alerts are reported from both SNMP traps and the polls conducted by Device Manager even if these alerts refer to the same error information.

Default: `Trap`

server.mail.alert.status

Specify the severity of alerts that are sent to users by email.

The Device Manager server reports alerts whose severity is equal to or higher than the severity specified for this property. The following values (listed in ascending order of severity) can be specified:

`Normal`, `Service`, `Moderate`, `Serious`, `Acute`

Default: `Moderate`

server.subsystem.ssid.availableValues

When creating volumes in Device Manager, specify the range of the SSIDs that can be assigned automatically to storage systems registered in Device Manager.

This property is valid for VSP G1000, G1500, VSP F1500, VSP Gx00 models, VSP Fx00 models, Virtual Storage Platform, Universal Storage Platform V/VM, and HUS VM.

The values that can be specified for this property are as follows:

- Hexadecimal numbers in the range from 4 to FFFD: To specify consecutive numbers, use a hyphen (–) to specify the range. To specify non-consecutive numbers, use commas as separators. The values are not case sensitive. If multiple values and ranges that include duplicated numbers are specified, the logical union of all specified values is used.
- `All`: The string `All` specifies that the entire range of values can be specified. This value is not case sensitive.

Automatic SSID assignment can be performed only when a value or values are specified in this property.

Default: `All`

server.smisclient.indication.port

Specify the port number used to receive event indications from SMI-S providers.

Specifiable range: 1024 to 49151.

If the setting value of this property has been changed, you must refresh any SMI-S enabled storage system that is managed by Device Manager.

Default: `5983`

server.agent.differentialrefresh.manual.enabled

Specify whether to update the database information only for resources whose configuration has changed since the last refresh when manually refreshing a storage system.

This property is valid only for VSP G1000, G1500, VSP F1500, VSP Gx00 models, VSP Fx00 models, Virtual Storage Platform or HUS VM storage systems.

If you specify `true` for this property, refresh processing is more efficient because database updates are skipped for resources whose configuration has not changed since the last refresh.

Specify `false` to update all storage system resource information in the database regardless of whether the configuration has changed.

Default: `true`

server.agent.differentialrefresh.periodical.enabled

Specify whether to update the database information only for resources whose configuration has changed since the last refresh when automatically refreshing a storage system.

This property is valid only for VSP G1000, G1500, VSP F1500, VSP Gx00 models, VSP Fx00 models, Virtual Storage Platform or HUS VM storage systems.

If you specify `true` for this property, refresh processing is more efficient because database updates are skipped for resources whose configuration has not changed since the last refresh.

Specify `false` to update all storage system resource information in the database regardless of whether the configuration has changed.

Default: `true`

server.logicalGroupMapping.updateInterval

When using Health Check, to omit the processing to obtain configuration information about the volumes of logical groups, specify the interval during which the processing is to be omitted (in minutes).

By default, Health Check reports for logical groups are always created based on the most recent volume configuration information. If Device Manager is managing many volumes, the processing to obtain configuration information about the volumes of logical groups might take a long time. In an environment in which the configuration of the volumes in a logical group does not change frequently, the processing to obtain configuration information can be omitted, and Health Check can be performed based on the last volume configuration information obtained. By doing so, you can shorten the time required to create reports.

Because this property is not present by default, specify it as follows:

`server.logicalGroupMapping.updateInterval=`*`time-in-minutes`*

After a Health Check is performed, for any Health Check performed from that time until the specified interval has elapsed, reports will be created based on the last volume configuration information obtained.

Device Manager database properties (database.properties file)

The `database.properties` file contains the database properties.

- In Windows:

installation-folder-for-Hitachi-Command-Suite\DeviceManager\HiCommandServer\config\database.properties

- In Linux:
  installation-directory-for-Hitachi-Command-Suite/HiCommandServer/config/database.properties

This property file contains the directives that pertain to establishing a connection with the Device Manager server's database. Before the Device Manager server can run you need to correctly enter these settings and start the Database Management System (DBMS). If the server cannot connect to its DBMS, an entry is written to the error log (the default location is in the `logs` directory). This information can help considerably when you are troubleshooting a new installation.

dbm.traceSQL

Specify whether to output SQL to trace log.

Set `true` to output SQL. Set `false` not to output SQL.

Default: `false`

dbm.startingCheck.retryCount

Specify the number of times that the Device Manager server (at startup) retries checking of whether the DBMS has started.

The specifiable values are from 0 to 100. Under normal conditions, you do not need to change the default value of this property.

Default: `18`

dbm.startingCheck.retryPeriod

Specify the interval (in seconds) that the Device Manager server (at startup) retries checking of whether the DBMS has started.

The specifiable values are from 0 to 60 (seconds). Under normal conditions, you do not need to change the default value of this property.

Default: `10` (seconds)

Device Manager log output properties (logger.properties file)

The `logger.properties` file contains the log output properties.

- In Windows:
  installation-folder-for-Hitachi-Command-Suite\DeviceManager\HiCommandServer\config\logger.properties
- In Linux:

installation-directory-for-Hitachi-Command-Suite/
HiCommandServer/config/logger.properties

This property file contains a set of directives that configure the Device Manager server's logging module, including the names, locations and verbosity level of the various operation and error log files. You can also use this file to configure trace logging for debugging and diagnostic purposes.

logger.loglevel

Specify the verbosity level for the `trace.log`, `error.log`, `CIMOMTrace.log`, and `SMISClientTrace.log`.

The values accepted in this field are (in decreasing order of detail): `DEBUG`, `INFO`, `WARN`, `ERROR`, and `FATAL`. If this property is set to the default, entries whose verbosity level is either `INFO`, `WARN`, `ERROR`, or `FATAL` are written into the `trace.log`. In this case, entries whose verbosity level is `DEBUG` are not written into the logs.

Default: `INFO`

logger.MaxBackupIndex

Specify the maximum number of backups for the `access.log`, `cim_access.log`, `error.log`, `service.log`, `stdout.log`, `stderr.log`, `statuscheck.log`, `trace.log`, `CIMOMTrace.log`, and `SMISClientTrace.log`.

When a log file reaches its maximum size (as specified in the `logger.MaxFileSize` property), the file is renamed and a counter is added into the file name (for example, `access.log.1`). As more backup log files are created, their counters or version suffixes are incremented (for example, `access.log.1` becomes `access.log.2`), until the specified number of backups have been created. After that, the oldest backup log file is deleted each time a new backup is created.

Specifiable values are from 1 to 20.

Default: `10`

Related references

- logger.MaxFileSize on page 604

logger.MaxFileSize

Specify the maximum size for the `access.log`, `cim_access.log`, `error.log`, `service.log`, `stdout.log`, `stderr.log`, `statuscheck.log`, `trace.log`, `CIMOMTrace.log`, and `SMISClientTrace.log`.

If the maximum size is exceeded, a new log file is created. Unless `KB` is specified for kilobytes or `MB` for megabytes, the specified size is interpreted to mean bytes.

Specifiable range: from 512 KB to 32 MB

Default: `1 MB`

logger.hicommandbase.loglevel

Specify the verbosity level for each operation (trace) log file and error log file written by Common Component. The log files are `HDvMtracen.log`, `HDvMGuiTracen.log`, and `HDvMGuiMessagen.log`, where *n* is an integer that represents the backup number for the file.

Each logging event has its own importance level independent from its type (error, warning, and information). The levels, in increasing order of importance, are: `30`, `20`, `10`, and `0`. The default logging level for production systems is `20`, which means that messages for logging event levels `20`, `10`, and `0` are written to `HDvMtrace1.log`, but messages for logging event level `30` are not.

Default: `20`

logger.hicommandbase.sysloglevel

Specify the verbosity level for the operation (trace) log data and error log data written to the event log (in Windows) or to syslog (in Linux) by Common Component.

Each logged event has its own importance level independent from its type (error, warning, and information). The levels, in increasing order of importance, are: `30`, `20`, `10` and `0`. The default logging level for production systems is `0`, which means that only messages for the logging event level `0` are written to the event log (in Windows) or to syslog (in Linux), but messages for the logging event level `30`, `20`, and `10` are not. The default value is recommended.

Default: `0`

logger.hicommandbase.MaxBackupIndex

Specify the maximum number of backups for each trace and error log file that is written by Common Component. The log files are `HDvMtracen.log`, `HDvMGuiTracen.log`, and `HDvMGuiMessagen.log` (the *n* in the file name indicates the backup generation number of the file).

When a log file reaches the size specified in the `logger.hicommandbase.MaxFileSize` property, a new log file is created with a counter added to the file name, for example `HDvMtrace2.log`. If the number of log files reaches the value specified in this property, log files are overwritten starting from the oldest file.

Valid values are from `1` to `16`.

Default: `10`

Related references

- logger.hicommandbase.MaxFileSize on page 606

logger.hicommandbase.MaxFileSize

Specify the maximum size of each operation (trace) log file and error log file that is written by Common Component. The log files are `HDvMtracen.log`, `HDvMGuiTracen.log`, and `HDvMGuiMessagen.log` (the *n* in the file name indicates the backup generation number of the file).

The specified size is assumed to be in bytes unless you specify `KB` for kilobytes, `MB` for megabytes or `GB` for gigabytes.

Valid values are from 4096 to 2147483647 (less than 2 GB).

Default: `5 MB`

Device Manager dispatcher properties (dispatcher.properties file)

The `dispatcher.properties` file contains the dispatcher properties.

- In Windows:
  installation-folder-for-Hitachi-Command-Suite\DeviceManager\HiCommandServer\config\dispatcher.properties
- In Linux:
  installation-directory-for-Hitachi-Command-Suite/HiCommandServer/config/dispatcher.properties

This property file contains a set of configurable directives pertaining to the operation of the Device Manager server's dispatcher layer, including properties that allow the fine-tuning of various background processes (daemons) and the optimization of the thread-priority for service agents.

server.dispatcher.message.timeout

Specify the timeout (in minutes) for pending response messages before they are expired (purged).

A pending message contains a response from a process that has been running for a long time (such as the addition of a storage system) but has not yet been polled by the client or has not yet been sent to the client via the Device Manager notification service.

Default: `15` (minutes)

server.dispatcher.message.timeout.in.processing

Specify the timeout period (in minutes) for the GUI processing and CLI processing that does not complete for some reason.

Default: `720` (minutes)

server.dispatcher.daemon.pollingPeriod

Specify the polling interval (in minutes) for the background threads responsible for checking component status and the configuration version.

A value of `0` will disable these pollings.

Default: `5` (minutes)



Caution: When polling is executed in HUS100, Hitachi AMS2000, or in Hitachi SMS, the I/O performance of the storage system might be affected. If you want to reduce the affect, set a larger polling interval or disable polling.

server.dispatcher.traps.purgePeriod

Specify the purging interval for stale SNMP traps or alerts (in minutes).

A value of `0` will disable the purging of traps from the server.

Default: `5` (minutes)

server.dispatcher.daemon.receiveTrap

Specify whether Device Manager receives SNMP traps generated by network resources such as storage systems and switches.

To receive SNMP traps, set this property to `true`. To not receive SNMP traps, set this property to `false`.

The port `162/udp` is used for receiving SNMP traps. When a new installation of Hitachi Command Suite is performed, if this port is not used by another product, this property is automatically set to `true`.

Default: `true`

server.dispatcher.snm2.configchange.pollingPeriod

Specify the interval (in seconds) at which the Device Manager server checks whether the configuration of HUS100, Hitachi AMS2000 or Hitachi SMS is changed by Storage Navigator Modular 2 launched from the GUI.

If the `server.configchange.enabled` property is set to `true` and the Device Manager server detects changes in the storage system configuration, storage system information in the database is automatically updated (refreshed).

You can specify a value from `0` to `3600`. If you specify `0`, storage system information in the database is not refreshed when the storage system configuration is changed because the Device Manager server does not detect the change.

Default: `300` (seconds)

Related references

- server.configchange.enabled on page 597

server.dispatcher.configchange.pollingPeriod

Specify the interval (in seconds) at which the Device Manager server checks whether the configuration of Hitachi AMS/WMS is changed by Element Manager.

If the `server.configchange.enabled` property is set to `true` and the Device Manager server detects changes in the storage system configuration, storage system information in the database is automatically updated (refreshed).

You can specify a value from `0` to `3600`. If you specify `0`, storage system information in the database is not updated when the storage system configuration is changed because the Device Manager server does not detect the change.

Default: `60` (seconds)

Related references

- server.configchange.enabled on page 597

server.dispatcher.daemon.configUpdate.detection.interval

Specify the interval (in minutes) at which the Device Manager server checks whether the configuration of VSP G1000, G1500, VSP F1500, VSP Gx00 models, VSP Fx00 models, Virtual Storage Platform, Universal Storage Platform V/VM, or HUS VM is changed by a storage management tool other than Device Manager (such as CCI or SVP).

If the Device Manager server detects changes in the configuration of VSP G1000, G1500, VSP F1500, VSP Gx00 models, VSP Fx00 models, Virtual Storage Platform, Universal Storage Platform V/VM, or HUS VM, the Device Manager GUI displays a warning message.

You can specify a value from `0` to `1440`. If you specify `0`, the Device Manager server does not check whether the configuration of VSP G1000, G1500, VSP F1500, VSP Gx00 models, VSP Fx00 models, Virtual Storage Platform, Universal Storage Platform V/VM, or HUS VM is changed.

Default: `10` (minutes)

Caution:

- If the GUI displays a warning message, manually refresh the corresponding storage system information.
  You can also specify the settings so that information in the database is automatically updated in case a user forgets to perform a manual refresh after changing the storage system configuration. To do so, set up the following properties:
  `server.dispatcher.daemon.autoSynchro.doRefresh` property

`server.dispatcher.daemon.autoSynchro.type` property

- The Device Manager server cannot detect the following configuration changes:
  - Changes in the LDEV status (such as normal, blocked, or being copied).
  - Creating, changing, or deleting copy pairs

  In addition, the Device Manager server cannot detect changes to the access attribute of LDEVs (such as Read/Write, Read Only, or Protect) that are performed on Universal Storage Platform V/VM.
- In the Device Manager server the configurations of storage system are treated as changed for the following triggers:
  - Restarting SVP (only for Universal Storage Platform V/VM)
  - Refreshing the configuration information of storage system displayed in Storage Navigator.
  - Switching the SVP in a cluster configuration from the executing node to the standby node, or vice versa (only for VSP G1000, G1500, VSP F1500, Virtual Storage Platform, or Universal Storage Platform V/VM)
  - Turning on the DKC
  - The configuration of a DP pool is changed#

  The configuration of the Copy-on-Write Snapshot data pool or the Thin Image data pool is changed#

  #:

  For VSP G1000, G1500, VSP F1500, VSP Gx00 models, VSP Fx00 models, Virtual Storage Platform or HUS VM, if you specify `false` for the `server.dispatcher.daemon.configUpdate.detection.variable.enabled` property, you can prevent a warning message from being displayed in the Device Manager GUI when the pool configuration is changed.

Related references

- server.dispatcher.daemon.autoSynchro.doRefresh on page 609
- server.dispatcher.daemon.autoSynchro.type on page 610
- server.dispatcher.daemon.configUpdate.detection.variable.enabled on page 611

server.dispatcher.daemon.autoSynchro.doRefresh

Specify whether to automatically refresh the storage system information in the database if the Device Manager server detects that the configuration of a VSP G1000, G1500, VSP F1500, VSP Gx00 models, VSP Fx00 models, Virtual Storage Platform, Universal Storage Platform V/VM, or HUS VM storage system has changed.

If `true` is specified for this property and a user does not perform a manual refresh after the Device Manager server detects a change, the information of VSP G1000, G1500, VSP F1500, VSP Gx00 models, VSP Fx00 models, Virtual Storage Platform, Universal Storage Platform V/VM, or HUS VM in the database is automatically refreshed at the interval specified in the

server.dispatcher.daemon.autoSynchro.type property. If false is specified, the database is not automatically refreshed.

Default: true

Caution: If you specify true, only the information about the VSP G1000, G1500, VSP F1500, VSP Gx00 models, VSP Fx00 models, Virtual Storage Platform, Universal Storage Platform V/VM, or HUS VM is updated in the database. The information in the configuration file of a host that recognizes the command device of VSP G1000, G1500, VSP F1500, VSP Gx00 models, VSP Fx00 models, Virtual Storage Platform, Universal Storage Platform V/VM, or HUS VM is not updated in the database.

Related references

- server.dispatcher.daemon.autoSynchro.type on page 610

server.dispatcher.daemon.autoSynchro.type

Specify the interval at which storage system information in the database is automatically updated (refreshed) using one of the following values:

H: Specify this format to automatically refresh the information at regular intervals. Specify the interval in the server.dispatcher.daemon.autoSynchro.interval property.

D: Specify this format to automatically refresh the information once a day at a specific time. Specify the time in the server.dispatcher.daemon.autoSynchro.startTime property.

W: Specify this format to automatically refresh the information once a week at a specific time on a specific day. Specify the day in the server.dispatcher.daemon.autoSynchro.dayOfWeek property, and the time in the server.dispatcher.daemon.autoSynchro.startTime property.

This property is enabled only if the server.dispatcher.daemon.autoSynchro.doRefresh property is set to true.

Default: D

Related references

- server.dispatcher.daemon.autoSynchro.doRefresh on page 609
- server.dispatcher.daemon.autoSynchro.dayOfWeek on page 610
- server.dispatcher.daemon.autoSynchro.startTime on page 611
- server.dispatcher.daemon.autoSynchro.interval on page 611

server.dispatcher.daemon.autoSynchro.dayOfWeek

Specify the day on which storage system information in the database is automatically updated (refreshed) using one of the following values:

`Sun Mon Tue Wed Thu Fri Sat`

This property is enabled only if the `server.dispatcher.daemon.autoSynchro.type` property is set to `W`. In addition, storage system information is automatically refreshed (updated) according to the time zone setting for the management server.

Default: `Fri`

Related references

- server.dispatcher.daemon.autoSynchro.type on page 610

server.dispatcher.daemon.autoSynchro.startTime

Specify the time at which storage system information is automatically refreshed (updated) in the database starts in the format *hh*:*mm*.

Specify a value from `00` to `23` for *hh*, and `00` to `59` for *mm*. This property is enabled only if the `server.dispatcher.daemon.autoSynchro.type` property is set to `D` or `W`. In addition, storage system information is automatically refreshed (updated) according to the time zone setting for the management server.

Default: `23:00`

Related references

- server.dispatcher.daemon.autoSynchro.type on page 610

server.dispatcher.daemon.autoSynchro.interval

Specify the interval (in hours) at which storage system information in the database is automatically updated (refreshed).

You can specify a value from `1` to `24`.

This property is enabled only if the `server.dispatcher.daemon.autoSynchro.type` property is set to `H`.

Default: `24` (hours)

Related references

- server.dispatcher.daemon.autoSynchro.type on page 610

server.dispatcher.daemon.configUpdate.detection.variable.enabled

Specify whether to monitor items with values that change sequentially, such as the usage rate of DP pools and the usage rate of Copy-on-Write Snapshot data pools, when the Device Manager server checks if the configuration of VSP G1000, G1500, VSP F1500, VSP Gx00 models, VSP Fx00 models, Virtual Storage Platform or HUS VM has been changed.

If `true` is specified, then the items are monitored. The Device Manager GUI displays a warning message when the Device Manager server detects

changes in the values. If `false` is specified, the following changes are not monitored, and the Device Manager GUI does not display a warning message.

- A change in the usage rate of the following volumes:
  - HDP volume
  - HDP pool
  - HDT pool
  - Data pool of Copy-on-Write Snapshot
  - Data pool of Thin Image
- A change in the threshold value for the usage rate of the following volumes:
  - HDP pool
  - HDT pool
  - Data pool of Copy-on-Write Snapshot
  - Data pool of Thin Image
- A change in the maximum reservation amount of the following volumes:
  - HDP pool
  - HDT pool
  - Data pool of Copy-on-Write Snapshot
  - Data pool of Thin Image
- A change in the monitoring mode for the HDT pool
- A change in the settings regarding performance monitoring and hierarchical relocation of the HDT pool
- A change in the settings regarding tiering policy for the HDT volume. The HDT volume is a virtual volume created from the HDT pool (associated with the HDT pool).

This property is enabled only if values other than `0` are specified for the `server.dispatcher.daemon.configUpdate.detection.interval` property.

Default: `false`

Related references

- server.dispatcher.daemon.configUpdate.detection.interval on page 608

server.dispatcher.daemon.autoSynchro.performance.doRefresh

Specify whether to automatically update (refresh) the performance information displayed in the Mobility tab.

If `true` is specified for this property, the storage system performance information is automatically refreshed at the time specified in the `server.dispatcher.daemon.autoSynchro.performance.startTime` property over the interval specified in the `htnm.infoAcquirePeriod` property.

If `false` is specified for this property, the storage system performance information is not automatically refreshed. To refresh the performance information, use either of the following methods:

- When using the GUI:
  In the Refresh Storage Systems window, select the Refresh Performance data check box, and then refresh the storage system.
- When using the CLI:
  Execute the `RefreshPerformanceData` command.

Default:`true`

Related references

- server.dispatcher.daemon.autoSynchro.performance.startTime on page 613
- htnm.infoAcquirePeriod on page 630

server.dispatcher.daemon.autoSynchro.performance.startTime

Specify the time at which performance information displayed in the Mobility tab is automatically updated in the format *hh*:*mm*.

Specify a value from `00` to `23` for *hh*, and `00` to `59` for *mm*. This property is enabled only if the `server.dispatcher.daemon.autoSynchro.performance.doRefresh` property is set to `true`.

Default:`00:10`

Related references

- server.dispatcher.daemon.autoSynchro.performance.doRefresh on page 612

server.dispatcher.daemon.autoSynchro.logicalGroup.doRefresh

Specify whether to automatically update logical group information when any of the operations below occur.

If this property is set to `true`, logical group information is automatically updated each time one of the events below occurs.

- Registering a storage system
- Refreshing a storage system
- Deleting a storage system
- Automatically updating performance information (over the interval specified in `htnm.infoAcquirePeriod`)
- Creating and editing a logical group
- Creating, editing, and deleting a user group
- Editing and deleting a resource group

Note that logical group information is automatically updated only when the above operations are performed from the GUI.

If the above operations are executed from the CLI when this property is set to `true` or if this property is set to `false`, logical group information is not

automatically updated. To update the information, select a logical group from Logical Groups under the Mobility tab, and then click the Refresh Data button.

Default:`true`

Related references

- htnm.infoAcquirePeriod on page 630

server.dispatcher.daemon.logicalGroupMappingUpdate.startTime

In the *hh*:*mm* format, specify the time to start executing the task that collects logical groups in the background. The logical groups to be collected are those that have volumes belong to them and appear in the Analyze MP Blade/Unit window of the Analytics tab.

Specify a value in the range from 00 to 23 for *hh* and a value in the range from 00 to 59 for *mm*.

The default value is `02:00`.

Device Manager MIME type properties (mime.properties file)

The `mime.properties` file contains the MIME type properties.

- In Windows:
  installation-folder-for-Hitachi-Command-Suite`\DeviceManager\HiCommandServer\config\mime.properties`
- In Linux:
  installation-directory-for-Hitachi-Command-Suite`/HiCommandServer/config/mime.properties`

This property file contains the translation and lookup table for all MIME types recognized by the Device Manager server. Each property in this lookup table maps a particular extension suffix to the MIME type for that file. Under normal conditions, you do not need to change the default values in this file. In any event, only expert system administrators should make any additions to this file.

Device Manager client properties (client.properties file)

The `client.properties` file contains the client properties.

- In Windows:
  installation-folder-for-Hitachi-Command-Suite`\DeviceManager\HiCommandServer\config\client.properties`
- In Linux:

installation-directory-for-Hitachi-Command-Suite/
HiCommandServer/config/client.properties

This property file contains the settings related to display and operation of Device Manager GUI.

client.rmi.port

Specify the port number for the Device Manager RMI server.

You must specify the same value as the one specified for the `server.rmi.port` property of the Device Manager server.

Default: `23055`

Related references

- server.rmi.port on page 594

client.launch.em.secure

When performing operations on VSP G1000, G1500, VSP F1500, VSP Gx00 models , or VSP Fx00 models , specify whether to simplify the information to be sent to Storage Navigator to improve security when launching Storage Navigator from the Device Manager GUI.

If you specify `true`, the information to be sent to Storage Navigator is simplified. To specify `true`, you must also configure the following settings:

- Enable the security communication between the storage system and the management client (GUI).
  Use a self-signed certificate or a server certificate signed by a certificate authority.
- Register the host name of the storage system when registering the storage system by using the Device Manager GUI.
  Register the host name that is set for Common Name in the server certificate. For details on how to register a storage system, see the *Hitachi Command Suite User Guide*.

If you specify `false`, the information to be sent to Storage Navigator is not simplified.

Default: `false`

Related concepts

- Operation workflow for secure communication between a storage system and a management client (GUI) on page 244

Device Manager security properties (server.properties file and cimxmlscpa.properties file)

The `server.properties` and `cimxmlscpa.properties` file contains the security properties.

- `server.properties` file
  - In Windows:
    installation-folder-for-Hitachi-Command-Suite\DeviceManager\HiCommandServer\config\server.properties
  - In Linux:
    installation-directory-for-Hitachi-Command-Suite/HiCommandServer/config/server.properties
- `cimxmlscpa.properties` file
  - In Windows:
    installation-folder-for-Hitachi-Command-Suite\DeviceManager\HiCommandServer\wsi\server\jserver\bin\cimxmlscpa.properties
  - In Linux:
    installation-directory-for-Hitachi-Command-Suite/HiCommandServer/wsi/server/jserver/bin/cimxmlscpa.properties

server.http.security.clientIP

Specify IP addresses, in IPv4 format, that can be used to connect to the Device Manager server.

The `server.http.security.clientIP` property is in the `server.properties` file.

This setting limits the IP addresses permitted for connection, thus preventing denial-of-service attacks or other attacks that intend to overflow buffers.

The following shows a specification example when the Device Manager server accepts connections from `172.16.0.1` and IP addresses in the range from `192.168.0.0` to `192.168.255.255`:

```
server.http.security.clientIP=172.16.0.1,192.168.*.*
```

You can use asterisks as a wildcard character when specifying multiple connection sources by using a single IP address. To specify multiple IP addresses, separate them with commas. Invalid IP addresses and spaces are ignored.

Default: `*.*.*.*` (Any IP address can be used to connect to the Device Manager server.)

Caution:

- You do not need to specify the IP address (the local loopback address) of the computer on which the Device Manager server is installed. In this property, it is assumed that the Device Manager server can always be connected to using the local loopback address.
- You also need to register the IP addresses to the environment definition file `user_httpsd.conf` for Common Component.

Related tasks

- Controlling management client access to the management server on page 699

server.http.security.clientIPv6

Specify IP addresses, in IPv6 format, that can be used to connect to the Device Manager server.

The `server.http.security.clientIPv6` property is in the `server.properties` file.

This setting limits the IP addresses permitted for connection, thus preventing denial-of-service attacks or other attacks that intend to overflow buffers.

The following shows a specification example when the Device Manager server accepts connections from IP addresses in the range from `12AB:0:0:CD30::` to `12AB:0:0:CD3F:FFFF:FFFF:FFFF:FFFF`.

```
server.http.security.clientIPv6=12AB:0:0:CD30::/60
```

You can specify a range of IP addresses in CIDR format. To specify multiple IP addresses, separate them with commas. Invalid IP addresses and spaces are ignored.

Default: `::` (Any IP address can be used to connect to the Device Manager server.)

Caution:

- You do not need to specify the IP address (the local loopback address) of the computer on which the Device Manager server is installed. In this property, it is assumed that the Device Manager server can always be connected to using the local loopback address.
- You also need to register the IP addresses to the environment definition file `user_httpsd.conf` for Common Component.

Related tasks

- Controlling management client access to the management server on page 699

server.https.security.keystore

Specify the name of the keystore file that contains the keypair and associated server certificate used for establishing encrypted communications via SSL or TLS.

The `server.https.security.keystore` property is in the `server.properties` file.

For Device Manager 8.1.3 or later, if you perform a new installation of Device Manager or perform an upgrade installation in an environment where the Device Manager server certificate does not exist, the default certificate used to authenticate user accounts for VSP G1000, G1500, VSP F1500, VSP Gx00 models, and VSP Fx00 models is stored in the Device Manager server keystore. If you want to improve security of communication with VSP G1000, G1500, VSP F1500, VSP Gx00 models, and VSP Fx00 models, or if you want to use secure communication for other purposes, re-import the keypair and associated self-signed certificate or trusted certificate into the keystore.

Default: `keystore`

Related concepts

- Default certificate for Device Manager on page 224

server.http.security.unprotected

Specify a comma-delimited list of any non-protected file resources under the server's document root.

The `server.http.security.unprotected` property is in the `server.properties` file.

To specify multiple file resources, separate them with commas. Spaces are ignored. When files or directories are designated as `unprotected`, they are not subject to Access Control List checks (user authentication), regardless of the security mode setting for the server. Entire directories (including nested sub-directories) can be flagged as unprotected by using an asterisk as a wildcard character. If you specify a space, all resources are protected, so that every request to the Device Manager server will require user authentication.

This property allows anyone to view the `index.html` front page via a browser, without user authentication being required. More importantly, it allows the Java Web Start application to update its JAR file and deploy (via the `HiCommand.jnlp` file) to the end-user's system without the appearance of a series of logon dialog boxes. Similarly, the GUI's help files (and certain client installation information) can be viewed via a web browser without separate authentication being required at each step. Under normal conditions, you do not need to change the default value of this property.

Default: `index.html, HiCommand/*, webstart/*, images/*, style/*, docs/*, favicon.ico, vasa/*`

server.https.security.truststore

Specify the truststore file of the Device Manager server.

The `server.https.security.truststore` property is in the `server.properties` file.

Default: `dvmcacerts`

Note: This property cannot be modified with HiKeytool. If you want to change the value, you must do so by editing the value in the `server.properties` file.

server.https.enabledCipherSuites

Specify the cipher suites to be used for the following SSL/TLS communication. Use commas (,) to separate multiple cipher suites.

- Between the Device Manager server and a Web browser
- Between the Device Manager server and the Device Manager CLI
- Between the Device Manager server and a Device Manager agent
- Between the Device Manager server and Replication Manager server

The `server.https.enabledCipherSuites` property is in the `server.properties` file.

The specifiable cipher suites are as follows:

- TLS_RSA_WITH_AES_256_CBC_SHA256
- `TLS_RSA_WITH_AES_256_CBC_SHA`
- `TLS_RSA_WITH_AES_128_CBC_SHA256`
- `TLS_RSA_WITH_AES_128_CBC_SHA`
- `SSL_RSA_WITH_3DES_EDE_CBC_SHA`

Default: `TLS_RSA_WITH_AES_256_CBC_SHA256, TLS_RSA_WITH_AES_256_CBC_SHA, TLS_RSA_WITH_AES_128_CBC_SHA256, TLS_RSA_WITH_AES_128_CBC_SHA, SSL_RSA_WITH_3DES_EDE_CBC_SHA`

server.https.protocols

Specify the protocols to be used for the following SSL/TLS communication. Use commas (,) to separate multiple protocols.

- Between the Device Manager server and the Device Manager GUI (web browser)
- Between the Device Manager server and the Device Manager CLI
- Between the Device Manager server and a Device Manager agent
- Between the Device Manager server and Replication Manager server

The `server.https.protocols` property is in the `server.properties` file.

The specifiable protocols are as follows:

- `TLSv1`
- `TLSv1.1`
- `TLSv1.2`

The specified protocols are used in order of their cipher strength, from highest to lowest.

Default: `TLSv1,TLSv1.1,TLSv1.2`

Ciphers

Specify the cipher suites to be used for SSL/TLS communication between the Device Manager server and a CIM client (object operations and indication notifications). Use commas (,) to separate multiple cipher suites.

The specifiable cipher suites are as follows:

- `TLS_RSA_WITH_AES_256_CBC_SHA256`
- `TLS_RSA_WITH_AES_256_CBC_SHA`
- `TLS_RSA_WITH_AES_128_CBC_SHA256`
- `TLS_RSA_WITH_AES_128_CBC_SHA`
- `SSL_RSA_WITH_3DES_EDE_CBC_SHA`

The `cimxmlscpa.properties` file and `Ciphers` property are not present by default. To limit the cipher suites that are used, create a new `cimxmlscpa.properties` file, and add the `Ciphers` property as follows:

`Ciphers = `*`cipher-suite`*`,`*`cipher-suite`*`,...`

Caution: The `cimxmlscpa.properties` file is deleted when the service for the Device Manager server starts. For this reason, we recommend noting down the specified values elsewhere.

Device Manager SNMP trap log output properties (customizedsnmptrap.properties file)

The `customizedsnmptrap.properties` file contains the SNMP trap log output properties.

- In Windows:
  `installation-folder-for-Hitachi-Command-Suite``\DeviceManager\HiCommandServer\config\customizedsnmptrap.properties`
- In Linux:
  `installation-directory-for-Hitachi-Command-Suite/``HiCommandServer/config/customizedsnmptrap.properties`

customizedsnmptrap.customizedSNMPTrapEnable

Specify whether to output SNMP traps received by Device Manager to log files.

To output SNMP traps to log files, set this property to `true`. To not output SNMP traps to log files, set this property to `false`.

If you set this property to `true`, also set the `customizedsnmptrap.customizelist` property.

Default: `false`

Note: If the `server.dispatcher.daemon.receiveTrap` property is set to `true`, SNMP traps from storage systems might be output to log files two times for the same event.

Related references

- server.dispatcher.daemon.receiveTrap on page 607

customizedsnmptrap.customizelist

Specify the format and severity used when outputting SNMP traps received by Device Manager to log files.

The following shows the syntax of the `customizedsnmptrap.customizelist` property:

```
customizedsnmptrap.customizelist = \
enterprise-ID-1:generic-trap-number-1:specific-trap-number-1:
severity-1:content-to-be-output-1, \
enterprise-ID-2:generic-trap-number-2:specific-trap-number-2:
severity-2:content-to-be-output-2, \
...
enterprise-ID-n:generic-trap-number-n:specific-trap-number-n:
severity-n:content-to-be-output-n
```

Table 112 Items specified in the customizedsnmptrap.customizelist property

Item	Format	Remarks
enterprise-ID	Specify by using dots (for example, . `1.3.6.1.4.116.3.11.1.2`)	Required
generic-trap-number	Numeric value, from 0 to 6	Required
specific-trap-number	Numeric value	Required
severity	Specify the severity of each trap by using one of the character strings below.	This item is optional. If you omit this item, `Null` is assumed.

Item	Format	Remarks
	You cannot use character strings other than the following: • `Information` • `Warning` • `Error` • `Critical` • `Alert` • `Null`	The severity indicators in the message IDs are output as follows: • `-I` for `Information` • `-W` for `Warning` • `-E` for `Error`, `Critical`, and `Alert` • No log data is output for `Null`
content-to-be-output	Specify the content to be output by using the character strings (variables) below. You cannot use character strings other than the following: • `$a` • `$e` • `$g` • `$s` • `$`*n* (where *n* indicates an integer, which is 1 or larger)	Optional. If you omit this item, the `$a$e$g$s` content is output. If you specify `Null` for the severity, specification for this item is disabled. Information output for each variable is as follows: • `$a`: Agent address (dotted format) • `$e`: Enterprise ID (dotted format) • `$g`: Generic trap number • `$s`: Specific trap number • `$`*n* (where *n* indicates an integer, which is 1 or larger): The value of the *n*th variable is binding

- You can omit some items, but you cannot omit the colon delimiter.
- To specify more than one customization definition, use a comma as a delimiter, but do not enter a comma at the end of the last entry.
- To move to a new line in the customization list, enter a back slash (`\`) at the end of that line. The line feed following the back slash (`\`) is ignored.

The following shows an example of specifying the `customizedsnmptrap.customizelist` property:

```
customizedsnmptrap.customizelist = \
.1.2.3:6:1:Information:$a$e$g$s$1$2, \
.1.3.6.1.4.1.2854:6:1:Warning:$e$a$s$3$2$1$g, \
.1.3.6.1.4.1.116.3.11.4.1.1:6:1:Error:$a$s, \
.1.3.6.1.4.1.116.3.11.4.1.1:6:100:Information:$a$s
```

Default: None

Caution: If you do not specify this property, the SNMP trap data will not be output to the log even if you specify `true` for the `customizedsnmptrap.customizedSNMPTrapEnable` property.

Related references

- customizedsnmptrap.customizedSNMPTrapEnable on page 621

Device Manager launchable applications properties (launchapp.properties file)

The `launchapp.properties` file contains the launchable applications properties.

- In Windows:
  installation-folder-for-Hitachi-Command-Suite\DeviceManager\HiCommandServer\config\launchapp.properties
- In Linux:
  installation-directory-for-Hitachi-Command-Suite/HiCommandServer/config/launchapp.properties

This property file contains information for the server that contains launchable applications.

launchapp.snm2.url

Specify the URL of the web server for Storage Navigator Modular 2 to be launched from the web browser in a client.

Specify this property when the target storage system is Hitachi AMS/WMS.

The following shows an example of specifying the URL of the web server for Storage Navigator Modular 2:

```
launchapp.snm2.url=http://192.168.17.235:23015/program/StorageNavigatorModular/applet
```

Default: None

Caution:
- You cannot use an IP address in IPv6 format. In IPv6 environments, specify a host name.
- If the management server has multiple NICs, use the IP address of the network that connects to the management client (GUI) to set the URL IP address. Do not specify the host name.

launchapp.snm2.rmi.port

If you change the port number used for RMI communication in Storage Navigator Modular 2, specify the new port number in this property.

If you do not do this, Device Manager cannot link with Storage Navigator Modular 2. Valid values are from `1` to `65535`.

Specify this property when the target storage system is Hitachi AMS/WMS.

If you want to run Storage Navigator Modular 2 on a computer also running Storage Navigator Modular (for Web), do not specify the same number for

the port numbers that are used for RMI communication in Storage Navigator Modular (for Web) and Storage Navigator Modular 2.

Default: None

launchapp.elementmanager.role.mode

Specify the permissions of Device Manager users who can manage storage system user accounts and audit log data by using Element Manager.

You can specify `0` or `1`. The permissions of Device Manager users who can manage storage system user accounts and audit log data by using Element Manager vary depending on the specified value as follows:

`0`: Only users who have the `Admin` or `Modify` permission can manage them.

`1`: Only users who have the `Admin` permission can manage them.

Default: `0`

Caution: For HUS100, Hitachi AMS2000, Hitachi SMS, or Hitachi AMS/WMS, Account Authentication must be enabled.

launchapp.elementmanager.usehostname

Specify whether a host name is to be displayed in the Storage Navigator URL when you are using Storage Navigator from the Device Manager GUI to connect to an enterprise-class storage system, VSP Gx00 models, VSP Fx00 models, or HUS VM.

If you specify `true`, when you register a storage system in Device Manager by specifying a host name, the host name is displayed in the Storage Navigator URL. If you specify `false`, an IP address is displayed in the Storage Navigator URL.

Default: `true`

Properties for communicating with the host (host.properties file)

The `host.properties` file contains the properties for communicating with the host.

- In Windows:
  installation-folder-for-Hitachi-Command-Suite\DeviceManager\HiCommandServer\config\host.properties
- In Linux:
  installation-directory-for-Hitachi-Command-Suite/HiCommandServer/config/host.properties

host.mf.agent.connection.timeout

Specify the timeout value (in seconds) for communication processing between the Device Manager server and Mainframe Agent.

Valid values are 0 and from 30 to 3600 (seconds). If you specify `0`, no timeout applies. Modify this property only if you are an expert system administrator and you want to fine-tune the performance of Mainframe Agent.

Default: `300`

host.agent.access.timeoutForRpm

Specify the communication timeout value (in minutes) for the Replication Manager server obtaining the host information from the Device Manager agent via the Device Manager server.

Valid values are from 1 to 1440 (minutes).

Default: `15`

Properties for connecting to Host Data Collector (hostdatacollectors.properties file)

The `hostdatacollectors.properties` file contains properties for connecting to Host Data Collector.

- In Windows:
  installation-folder-for-Hitachi-Command-Suite\DeviceManager\HiCommandServer\config\hostdatacollectors.properties
- In Linux:
  installation-directory-for-Hitachi-Command-Suite/HiCommandServer/config/hostdatacollectors.properties

hdc.request.timeout

Specify the timeout value for request processing from the Device Manager server to Host Data Collector (in milliseconds).

You can specify a value from `1000` to `86400000`.

If the Device Manager server communicates with multiple Host Data Collectors, the timeout value will be applied to communication with all the Host Data Collectors.

Default: `1800000`

hdc.rmiregistry

Specify the IP address or host name of the computer where Host Data Collector is installed and the port number of the RMI registry in the following format:

IP-address-or-host-name:[*port-number*],*IP-address-or-host-name*:[*port-number*],...

For the IP address, you can use either an IPv4 address or IPv6 address. If you use an IPv6 address, you must enclose the IP address with square brackets (`[` and `]`).

The port number must match the value specified for the property `hdc.common.rmi.registryPort` or `hdc.common.rmi.ssl.registryPort` of the `hdcbase.properties` file. If you omit the port number, it is assumed to be 22098 if the value of the `hdc.usessl` property is `false`, and 22104 if the value is `true`.

If there are multiple computers where Host Data Collector is installed, you must specify the Host Data Collector information for all the computers.

Default:

If the management server OS is a prerequisite OS for Host Data Collector: `127.0.0.1:22098`

If the management server OS is not a prerequisite OS for Host Data Collector: None



Caution: The IP address or host name of the computer where Host Data Collector is installed must be the same for the properties `hdc.rmiregistry`, `hdc.rmiserver`, and `hdc.classloader`. In addition, if multiple IP addresses are assigned to the computer where Host Data Collector is installed, specify the same values for the `hdc.service.rmi.registryIPAddress` property in the `hdcbase.properties` file of Host Data Collector.

Related references

- hdc.rmiserver on page 626
- hdc.classloader on page 627
- hdc.usessl on page 628
- hdc.common.rmi.registryPort on page 659
- hdc.common.rmi.ssl.registryPort on page 661
- hdc.service.rmi.registryIPAddress on page 662

hdc.rmiserver

Specify the IP address or host name of the computer where Host Data Collector is installed and the port number of the RMI server in the following format:

IP-address-or-host-name:[*port-number*],*IP-address-or-host-name*:[*port-number*],...

For the IP address, you can use either an IPv4 address or IPv6 address. If you use an IPv6 address, you must enclose the IP address with square brackets ([and]).

The port number must match the value specified for the property `hdc.common.rmi.serverPort` or `hdc.common.rmi.ssl.serverPort` of Host Data Collector. If you omit the port number, it is assumed to be 22099 if the value of the `hdc.usessl` property is `false`, and 22105 if the value is `true`.

If there are multiple computers where Host Data Collector is installed, you must specify the Host Data Collector information for all the computers.

Default:

If the management server OS is a prerequisite OS for Host Data Collector: `127.0.0.1:22099`

If the management server OS is not a prerequisite OS for Host Data Collector: None

Caution: The IP address or host name of the computer where Host Data Collector is installed must be the same for the properties `hdc.rmiregistry`, `hdc.rmiserver`, and `hdc.classloader`. In addition, if multiple IP addresses are assigned to the computer where Host Data Collector is installed, specify the same values for the `hdc.service.rmi.registryIPAddress` property in the `hdcbase.properties` file of Host Data Collector.

Related references

- hdc.rmiregistry on page 626
- hdc.classloader on page 627
- hdc.usessl on page 628
- hdc.common.rmi.serverPort on page 660
- hdc.common.rmi.ssl.serverPort on page 661
- hdc.service.rmi.registryIPAddress on page 662

hdc.classloader

Specify the IP address or host name of the machine where Host Data Collector is installed and the port number of the class loader in the following format:

IP-address-or-host-name:[*port-number*],*IP-address-or-host-name*:[*port-number*],...

For the IP address, you can use either an IPv4 address or IPv6 address. If you use an IPv6 address, you must enclose the IP address with square brackets ([and]).

The port number must match the value specified for the properties `hdc.common.http.serverPort` or `hdc.common.https.serverPort` of Host Data Collector. If you omit the port number, it is assumed to be 22100 if the value of the `hdc.usessl` property is `false`, and 22106 if the value is `true`.

If there are multiple computers with Host Data Collector installed, you must specify the Host Data Collector information for all the computers.

Default:

If the management server OS is a prerequisite OS for Host Data Collector: `127.0.0.1:22100`

If the management server OS is not a prerequisite OS for Host Data Collector: None

Caution: The IP address or host name of the computer where Host Data Collector is installed must be the same for the properties `hdc.rmiregistry`, `hdc.rmiserver`, and `hdc.classloader`. In addition, if multiple IP addresses are assigned to the computer where Host Data Collector is installed, specify the same values for the `hdc.service.rmi.registryIPAddress` property in the `hdcbase.properties` file of Host Data Collector.

Related references

- hdc.rmiregistry on page 626
- hdc.rmiserver on page 626
- hdc.usessl on page 628
- hdc.common.http.serverPort on page 660
- hdc.common.https.serverPort on page 662
- hdc.service.rmi.registryIPAddress on page 662

hdc.usessl

Specify whether to use SSL to communicate between the Host Data Collector machine and the Device Manager server.

If SSL is used for communication, specify `true`. If SSL is not used for communication, specify `false`,

If there are multiple computers where Host Data Collector is installed, this property setting applies to communication with all of the Host Data Collector machines.

Default: `false`

Properties for migrations (migration.properties file)

The `migration.properties` file contains properties for migrations.

- In Windows:

installation-folder-for-Hitachi-Command-Suite\DeviceManager\HiCommandServer\config\migration.properties

- In Linux:
  installation-directory-for-Hitachi-Command-Suite/HiCommandServer/config/migration.properties

migration.dataErase.defaultValue

Specify the status of the Shredding check box when the Migrate Data wizard starts.

When `true` is set:

The Shredding check box is selected.

When `false` is set:

The Shredding check box is not selected.

To prevent data leaks, we recommend that you delete the data on migration source volumes after migration.

Default: `false`

migration.plan.candidateVolumeCountLimit

Specify whether to limit the number of candidate volumes that are displayed when creating a migration plan.

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`

migration.plan.candidateCapacityGroupDisplayMaxCount

Specify 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`

Caution:

- 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 re-created, the free capacity of the parity 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 parity 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.

migration.multiExecution

Specify the number of migration pairs that can be executed simultaneously in a storage system.

The range for specifiable values is from `1` to `64`.

Default: `8`

migration.volumeDelete.defaultValue

Specify the status of the Deleting check box when the Migrate Data wizard starts.

When `true` is set:

The Deleting check box is selected.

When `false` is set:

The Deleting check box is not selected.

Default: `false`

Properties for connecting to Tuning Manager (tuningmanager.properties file)

The `tuningmanager.properties` file contains properties for connecting to Tuning Manager.

- In Windows:
  installation-folder-for-Hitachi-Command-Suite\DeviceManager\HiCommandServer\config\tuningmanager.properties
- In Linux:
  installation-directory-for-Hitachi-Command-Suite/HiCommandServer/config/tuningmanager.properties

htnm.infoAcquirePeriod

Specify the period for which performance information, such as the parity group usage rate and the volume IOPS, is collected and summarized.

The following three time periods can be specified:

- `day`: Collects and summarizes performance information on a daily basis.

- `week`: Collects and summarizes performance information on a weekly basis. In Tuning Manager, a week is from Monday to Sunday.
- `month`: Collects and summarizes performance information on a monthly basis. In Tuning Manager, a month is from the first day to the last day of the month.

The information displayed is the performance information from when summarization was last completed. As such, if `day` is specified, performance information from the previous day is displayed, if `week` is specified, from the previous week, and if `month` is specified, from the previous month. Even if you refresh the storage system during the week or the month, the same information is displayed.

Default: `day`

htnm.servers

Specify the number of Tuning Manager servers to be connected.

The range of specifiable values is from `0` to `50`.

Default: `0`

htnm.server.*n*.host

Specify the host name or IP address of a Tuning Manager server to access.

For *n* in the property name, specify a value in the range from `0` to *value-specified-in-htnm.servers-property* - 1.

- If the Device Manager server and the Tuning Manager server are installed on the same computer:
  Values to be specified depend on the communication method used between the Tuning Manager server and Common Component.
  - Communicating with HTTP:
    Specify the loopback address (`127.0.0.1` or `localhost`).
  - Communicating with HTTPS:
    Specify the same host name as the value of CN in the server certificate of Common Component. The value is case-sensitive.
- If the Device Manager server and the Tuning Manager server are installed on different computers:
  Specify the host name or IPv4 address of the Tuning Manager server to be accessed. Note that an IPv6 address cannot be used.

Default: None

htnm.server.*n*.protocol

Specify either `http` or `https`, depending to the communication method used between the Tuning Manager server and Common Component.

Default:`http`

For *n* in the property name, specify a value in the range from `0` to *value-specified-in-htnm.servers-property* - 1.

htnm.server.*n*.port

Specify the port number to access of a HBase 64 Storage Mgmt Web Service for a Tuning Manager server.

If `http` is specified for `htnm.server.n.protocol`, specify the port number for the non-SSL HBase 64 Storage Mgmt Web Service. If `https` is specified for `htnm.server.n.protocol`, specify the port number for the SSL HBase 64 Storage Mgmt Web Service.

Default: None

For *n* in the property name, specify a value in the range from `0` to *value-specified-in-htnm.servers-property* - 1.

Related references

- htnm.server.n.protocol on page 631

htnm.flashMode

When launching the history report for Tuning Manager from the Analytics tab, specify the chart display type in the history report.

Specifying `true` displays the chart by using Adobe Flash Player. Specifying `false` displays the chart with an image (in PNG format).

Default: `true`

hdvm.analytics.report.pdf.showLogo

Specify whether to output the logo and copyrights on the cover and in the contents of the PDF file, which will be exported by using the Analytics tab.

Specify `true` to output the items below. Specify `false` to not to output the items.

- Cover
  - Hitachi logo
  - Hitachi Data Systems logo
  - Copyrights
  - "Hitachi" at the beginning of product names
- Contents
  - "Hitachi" at the beginning of product names

Default: `true`

hdvm.analytics.disabled

Hides the Analytics tab.

This property is not present by default.

To hide the Analytics tab, specify the following in the `tuningmanager.properties` file:

```
hdvm.analytics.disabled=true
```

hdvm.analytics.healthcheck.notification.exportreport.locale

When sending health check results by email, specify a locale for the PDF file to be used to attach the health check report.

By default, the locale of the Device Manager server is specified. If a language other than Japanese is specified for the locale of the Device Manager server, English will be specified.

Use this property to specify a locale for PDF files that differs from the locale of the Device Manager server. If you specify `ja` for this property, the Japanese locale will be specified. If you specify `en`, the English locale will be specified.

Because this property is not present by default, specify it by using the following syntax:

```
hdvm.analytics.healthcheck.notification.exportreport.locale=locale-value
```

Properties related to the Replication tab (replication.properties file)

The `replication.properties` file contains properties related to the Replication tab.

- In Windows:
  installation-folder-for-Hitachi-Command-Suite\DeviceManager\HiCommandServer\config\replication.properties
- In Linux:
  installation-directory-for-Hitachi-Command-Suite/HiCommandServer/config/replication.properties

server.dispatcher.daemon.replication.config.doUpdate

Specify whether to periodically collect configuration information for primary site and secondary site storage systems, copy groups, copy pairs, and pair management servers.

If you specify `true`, configuration information is periodically collected.

By default, configuration information is collected every day at 2:00.

If the time of collection is specified so that the collection coincides with the health check or the polling of Tuning Manager, we recommend that the time of collection be changed.

We also recommend that you specify the time of collection so that, after the configuration information of Replication Manager is refreshed, the configuration information is collected. You can check the time that the refresh of the configuration information of Replication Manager was completed in the event log. For details about the event log for Replication Manager, see the *Hitachi Command Suite Replication Manager User Guide*.

If you want to change the interval or time of collection, edit the following properties:

- `server.dispatcher.daemon.replication.config.updateInterval` property: Collection interval
- `server.dispatcher.daemon.replication.config.offset` property: Collection start time (hours)
- `server.dispatcher.daemon.replication.config.minute` property: Collection start time (minutes)

If you specify `false`, configuration information is not periodically collected. In this case, use the Device Manager GUI/CLI to collect the configuration information.

Default: `true`

Related references

- server.dispatcher.daemon.replication.config.updateInterval on page 634
- server.dispatcher.daemon.replication.config.offset on page 634
- server.dispatcher.daemon.replication.config.minute on page 635

server.dispatcher.daemon.replication.config.updateInterval

Specify a time period for the interval at which to collect configuration information for primary site and secondary site storage systems, copy groups, copy pairs, and pair management servers.

You can specify the values 8, 12, or 24 (hours).

This property is enabled only if the `server.dispatcher.daemon.replication.config.doUpdate` property is set to `true`.

Default: `24` (hours)

Related references

- server.dispatcher.daemon.replication.config.doUpdate on page 633

server.dispatcher.daemon.replication.config.offset

Specify the start time (in hours) at which to collect configuration information for primary site and secondary site storage systems, copy groups, copy pairs, and pair management servers.

If you specify `8` or `12` for the `server.dispatcher.daemon.replication.config.updateInterval` property, configuration information is collected multiple times a day, so you must specify the first collection start time of the day.

For example, if you specify `3` for this property, configuration information is collected as follows:

- If you specified `8` for the `server.dispatcher.daemon.replication.config.updateInterval` property:
  Information is collected every day, at 3:00, 11:00, and 19:00.
- If you specified `12` for the `server.dispatcher.daemon.replication.config.updateInterval` property:
  Information is collected every day, at 3:00 and 15:00.
- If you specified `24` for the `server.dispatcher.daemon.replication.config.updateInterval` property:
  Information is collected every day, at 3:00.

Specify a smaller value for this property than the value specified for the `server.dispatcher.daemon.replication.config.updateInterval` property in the range from 0 to 23.

This property is enabled only if the `server.dispatcher.daemon.replication.config.doUpdate` property is set to `true`.

Default: `2`

Related references

- server.dispatcher.daemon.replication.config.doUpdate on page 633
- server.dispatcher.daemon.replication.config.updateInterval on page 634

server.dispatcher.daemon.replication.config.minute

Specify the start time (in minutes) at which to collect configuration information for primary site and secondary site storage systems, copy groups, copy pairs, and pair management servers.

You can specify a value from `0` to `59` (minutes).

This property is enabled only if the `server.dispatcher.daemon.replication.config.doUpdate` property is set to `true`.

Default: `0` (minutes)

Related references

- server.dispatcher.daemon.replication.config.doUpdate on page 633

server.dispatcher.daemon.replication.performance.rpm.updateInterval

Specify the interval (in minutes) at which to collect performance information such as C/T Delta or journal volume usage rates from Replication Manager.

Specify a factor of 60, in the range 3 through 60.

Default: `5` (minutes)

server.dispatcher.daemon.replication.performance.tnm.updateInterval

Specify a time period for the interval at which to collect performance information from Tuning Manager, such as the ratios of storage system processor usage or data in storage system cache memory that is waiting to be written.

You can specify the values 4, 8, 12, or 24 (hours).

Default: `4` (hours)

server.dispatcher.daemon.replication.performance.tnm.offset

Specify the start time (in hours) at which to collect performance information from Tuning Manager, such as the ratios of storage system processor usage or data in storage system cache memory that is waiting to be written.

If you specify `4`, `8`, or `12` for the `server.dispatcher.daemon.replication.performance.tnm.updateInterval` property, performance information is collected multiple times a day, so you must specify the first collection start time of the day.

For example, if you specify `2` for this property, performance information is collected as follows:

- If you specified `4` for the `server.dispatcher.daemon.replication.performance.tnm.updateInterval` property:
  Information is collected every day, at 2:00, 6:00, 10:00, 14:00, 18:00, and 22:00.
- If you specified `8` for the `server.dispatcher.daemon.replication.performance.tnm.updateInterval` property:
  Information is collected every day, at 2:00, 10:00, and 18:00.
- If you specified `12` for the `server.dispatcher.daemon.replication.performance.tnm.updateInterval` property:
  Information is collected every day, at 2:00, and 14:00.

- If you specified `24` for the `server.dispatcher.daemon.replication.performance.tnm.updateInterval` property:
  Information is collected every day, at 2:00.

Specify a smaller value for this property than the value specified for the `server.dispatcher.daemon.replication.performance.tnm.updateInterval` property in the range from 0 to 23.

If the time of collection is specified so that the collection coincides with the health check or the polling of Tuning Manager, we recommend that the time of collection be changed.

Default: `3`

Related references

- server.dispatcher.daemon.replication.performance.tnm.updateInterval on page 636

server.dispatcher.daemon.replication.performance.tnm.minute

Specify the start time (in minutes) at which to collect performance information from Tuning Manager, such as the ratios of storage system processor usage or data in storage system cache memory that is waiting to be written.

You can specify a value from `0` to `59` (minutes).

Default: `5` (minutes)

hdvm.replication.disabled

Hides the Replication tab.

This property is not present by default.

To hide the Replication tab, specify the following in the `replication.properties` file:

```
hdvm.replication.disabled=true
```

Properties for connecting to Replication Manager (rpmlib.properties file)

The `rpmlib.properties` file contains properties for connecting to Replication Manager.

- In Windows:
  installation-folder-for-Hitachi-Command-Suite`\DeviceManager\HiCommandServer\config\rpmlib.properties`
- In Linux:

installation-directory-for-Hitachi-Command-Suite/
HiCommandServer/config/rpmlib.properties

rpmlib.rpm.port

Specify the port number used for connecting to Replication Manager servers.

Match the port number to the value set for the base.rmi.port property in the Replication Manager server's base.properties file.

For details about the base.rmi.port property in the Replication Manager server's base.properties file, see the *Replication Manager Configuration Guide*.

Default: 25200

Properties for the CIM/WBEM functions (jserver.properties file, cimxmlcpa.properties file, cimxmlscpa.properties file)

The jserver.properties file, cimxmlcpa.properties file, and cimxmlscpa.properties file contain properties related to the CIM/WBEM functions.

- Location of the jserver.properties file
  - In Windows:
    installation-folder-for-Hitachi-Command-Suite\DeviceManager\HiCommandServer\config
  - In Linux:
    *installation-directory-for-Hitachi-Command-Suite/*HiCommandServer/config
- Location of the cimxmlcpa.properties file and the cimxmlscpa.properties file
  - In Windows:
    installation-folder-for-Hitachi-Command-Suite\DeviceManager\HiCommandServer\wsi\server\jserver\bin
  - In Linux:
    *installation-directory-for-Hitachi-Command-Suite/*HiCommandServer/wsi/server/jserver/bin

com.wbemsolutions.jserver.bindto

Specify the IP address to be registered in the SLP, when multiple IP addresses are assigned to one management server.

IP addresses that can be accessed from a CIM client must be specified.

Specify this property in the jserver.properties file. The com.wbemsolutions.jserver.bindto property does not exist by default, so specify the property in the following format:

com.wbemsolutions.jserver.bindto=*IP-address*

HTTPPort

In the case of non-SSL communication, specify the port number to be used by the CIM/WBEM functionality.

Specify this property in the `cimxmlcpa.properties` file. The `cimxmlcpa.properties` file does not exist by default, so create a new file and specify the property in the following format:

`HTTPPort=`*`port-number`*

Caution:

- If you change the value of this property, you must also change the values of the Device Manager server `server.cim.http.port` property to the same value.
- The `cimxmlcpa.properties` file is deleted when the service for the Device Manager server starts. Create a new `cimxmlcpa.properties` file every time the port is changed.

Related references

- server.cim.http.port on page 596

HTTPSPort

In the case of SSL communication, specify the port number to be used by the CIM/WBEM functionality.

Specify this property in the `cimxmlscpa.properties` file. The `cimxmlscpa.properties` file does not exist by default, so create a new file and specify the property in the following format:

`HTTPSPort=`*`port-number`*

Caution:

- Be sure to also specify the `Ciphers` property in the `cimxmlscpa.properties` file.
- If you change the value of this property, you must also change the values of the Device Manager server `server.cim.https.port` property to the same value.
- The `cimxmlscpa.properties` file is deleted when the service for the Device Manager server starts. Create a new `cimxmlscpa.properties` file every time the port is changed.

Related references

- server.cim.https.port on page 597
- Ciphers on page 620

B

Tiered Storage Manager server properties

This section describes the property files of the Tiered Storage Manager server.

- Tiered Storage Manager server property files
- Tiered Storage Manager server operations properties (server.properties file)
- Tiered Storage Manager database properties (database.properties file)
- Tiered Storage Manager properties for accessing Device Manager server (devicemanager.properties file)
- Tiered Storage Manager log output properties (logger.properties file)
- Tiered Storage Manager security properties (server.properties file)

Tiered Storage Manager server property files

There is a Tiered Storage Manager server property file for Tiered Storage Manager server operations and another property file for accessing the Device Manager server. These property files apply only to operations (processes) from the Tiered Storage Manager CLI.

The following table lists the Tiered Storage Manager server property files.

Table 113 Tiered Storage Manager server property files

Property file	Description
`server.properties` file	This property file is related to the Tiered Storage Manager server operations.
`database.properties` file	This property file is related to the Tiered Storage Manager database.
`devicemanager.properties` file	This property file is related to access from Tiered Storage Manager to the Device Manager server.
`logger.properties` file	This property file is related to Tiered Storage Manager log output.
`server.properties` file	This property file is related to Tiered Storage Manager security.



Caution:

- 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.
- The default values are set during a new installation.

Changing Tiered Storage Manager server properties

Use a text editor to edit Tiered Storage Manager server properties.

To reset the Tiered Storage Manager server properties to the default values, use the template stored in the following location.

In Windows:

installation-folder-for-Hitachi-Command-Suite`\TieredStorageManager\template`

In Linux:

installation-directory-for-Hitachi-Command-Suite`/TieredStorageManager/template`

Before you begin

Log in as a user with Administrator permissions (for Windows) or as a root user (for Linux).

Procedure

1. Stop the services of Hitachi Command Suite product.
2. Use a text editor to set appropriate values in the Tiered Storage Manager server property files.
3. Start the services of Hitachi Command Suite product.

Related tasks

- Starting the Hitachi Command Suite services on page 458
- Stopping the Hitachi Command Suite services on page 460

Syntax rules for Tiered Storage Manager server property files

The property files are in the Java property file format.

The following syntax rules must be followed for property files:

- Each property must be entered as a combination of a property name and value separated by an equals sign (=). For example, `foo.bar=12345`.
- Each property must be separated by a line delimiter (a line feed character).
- A line beginning with a hash mark (#) is a comment line.
- Literals (character strings or numeric values) do not need to be surrounded 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\docroot\foo.bar` should be entered as `C:\\HiCommand\\docroot\\foo.bar`. When you specify properties, there is no need to precede other characters with the escape character \.
- If two or more entries in a property file have the same property name, the value of the last such property specified in the file will take effect.
- If a line ends with a backslash (\), the next line is a continuation of the current line.

Tiered Storage Manager server operations properties (server.properties file)

The `server.properties` file contains properties related to Tiered Storage Manager server operations.

- In Windows:

installation-folder-for-Hitachi-Command-Suite
\TieredStorageManager\conf\server.properties

- In Linux:
installation-directory-for-Hitachi-Command-Suite/
TieredStorageManager/conf/server.properties

server.rmi.port

For configurations not using SSL communication, specify the RMI port number used by Tiered Storage Manager to accept processing requests.

The range of specifiable values is from `1` to `65535`.

This property takes effect when `1` is specified for the `server.rmi.secure` property.

Default: `20352`

Caution: If you change the value of this property, revise the `htsmserver.location` property in the `htsmcli.properties` file of the Tiered Storage Manager CLI.

Related tasks

- Enabling SSL/TLS for the Tiered Storage Manager CLI computer on page 296

Related references

- server.rmi.secure on page 655

server.rmi.security.port

For configurations using SSL communication, specify the RMI port number used by Tiered Storage Manager to accept processing requests.

The range of specifiable values is from `1` to `65535`.

This property takes effect when `2`, `3`, or `4` is specified for the `server.rmi.secure` property.

Default: `24500`

Caution: If you change the value of this property, revise the `htsmserver.location` property in the `htsmcli.properties` file of the Tiered Storage Manager CLI.

Related tasks

- Enabling SSL/TLS for the Tiered Storage Manager CLI computer on page 296

Related references

- server.rmi.secure on page 655

server.base.initialsynchro

Specify whether the Tiered Storage Manager configuration information contained in the navigation tree is synchronized with the Common Component database when the Tiered Storage Manager server starts.

Specify `true` to synchronize information. Specify `false` if you do not want to synchronize information.

If you restore Tiered Storage Manager database individually, inconsistencies may arise between the storage configuration information in Tiered Storage Manager and the Common Component database when the Tiered Storage Manager server is restarted. In such a case, set this property to `true`.

Default: `false`

server.mail.smtp.host

Specify the host name or IP address of the SMTP server to access when sending an event notification email.

When entering an IPv6 address, enclose it with `[` and `]`.

Default: None

server.mail.from

Specify the email address of the sender of event notification emails.

Depending on the operating environment, users might not receive email from an address that does not include a domain name. In this case, change the value of this property or the SMTP server environment settings.

Default: `htsmserver`

server.mail.errorsTo

Specify the address to which an undeliverable notification email will be sent when an 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 emails vary according to the SMTP server settings. Make sure to review these settings.

Default: None

Related references

- server.mail.from on page 645

server.mail.smtp.port

Specify the SMTP server port number to use when sending an event notification email.

The range of specifiable values is from `1` to `65535`.

Default: `25`

server.mail.smtp.auth

Specify whether to enable SMTP authentication when sending an event notification email.

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

Specify the send destination address for an event notification email.

Notification emails for all events are sent to the email address specified in this property.

Default: None

server.eventMonitoringIntervalInMinute

Specify 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 `35,791`.

Default: `720`

server.migration.multiExecution

Specify the number of migration pairs that can be simultaneously executed in a storage system.

The range for specifiable values is from `1` to `64`.

Default: `8`

server.checkOutVolumeRange

Specify whether filter conditions used for searching volumes or defining storage tiers have their values checked for validity.

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.migration.dataErase.defaultValue

Specify the status of the Erase remaining data on source volumes. check box when the Migration wizard is started, and the action to be taken when the `erasedata` parameter of the `CreateMigrationTask` command is omitted.

If `true` is specified:

The Migration wizard starts with the Erase remaining data on source volumes. check box selected. Also, if the `erasedata` parameter of the `CreateMigrationTask` command is omitted, the command is executed assuming that `Yes` is specified.

If `false` is specified:

The Migration wizard starts with the Erase remaining data on source volumes. check box cleared in the initial display. Also, if the `erasedata` parameter of the `CreateMigrationTask` command is omitted, the command is executed assuming that `No` is specified.

To prevent data leaks, we recommend that you delete the data on migration source volumes after migration.

Default: `false`

server.migrationPlan.candidateVolumeCountLimit

Specify whether to limit the number of candidate volumes that are displayed when creating a migration plan.

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

Specify 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`

Caution:

- 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 re-created, the free capacity of the parity 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 parity 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

Specify the maximum number of retries to be sent by the Tiered Storage Manager server when requesting that the storage system retry task execution.

If the storage system is temporarily unable to receive such requests because the user has modified the configuration of the storage system or the storage system is operating in Modify mode, requests to the storage system 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`

Tiered Storage Manager database properties (database.properties file)

The `database.properties` file contains properties related to databases.

- In Windows:
  installation-folder-for-Hitachi-Command-Suite
  `\TieredStorageManager\conf\database.properties`
- In Linux:
  installation-directory-for-Hitachi-Command-Suite/
  `TieredStorageManager/conf/database.properties`

dbm.traceSQL

Specify whether SQL should be output to a trace log.

Specifying `true` outputs SQL. If you specify `false`, SQL is not output.

Default: `false`

Tiered Storage Manager properties for accessing Device Manager server (devicemanager.properties file)

The `devicemanager.properties` file contains properties related to access to the Device Manager server.

- In Windows:
  installation-folder-for-Hitachi-Command-Suite
  `\TieredStorageManager\conf\devicemanager.properties`
- In Linux:
  installation-directory-for-Hitachi-Command-Suite/
  `TieredStorageManager/conf/devicemanager.properties`

hdvm.protocol

Specify the protocol to be used when accessing the Device Manager server.

Default: `http`

hdvm.port

Specify the port number of the Device Manager server you are accessing.

You must specify the same value as the one specified for the `server.http.port` property of the Device Manager server.

Default: `2001`

Related references

- server.http.port on page 592

hdvm.timeout

Specify 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`

hdvm.rmi.port

Specify the port number for the Device Manager RMI server.

You must specify the same value as the one specified for the `server.rmi.port` property of the Device Manager server.

Default: `23055`

Related references

- server.rmi.port on page 594

Tiered Storage Manager log output properties (logger.properties file)

The `logger.properties` file contains properties related to log output.

- In Windows:
  installation-folder-for-Hitachi-Command-Suite
  `\TieredStorageManager\conf\logger.properties`
- In Linux:
  installation-directory-for-Hitachi-Command-Suite/
  `TieredStorageManager/conf/logger.properties`

The following figure shows the relationship between the threshold value of the output levels and the output messages.

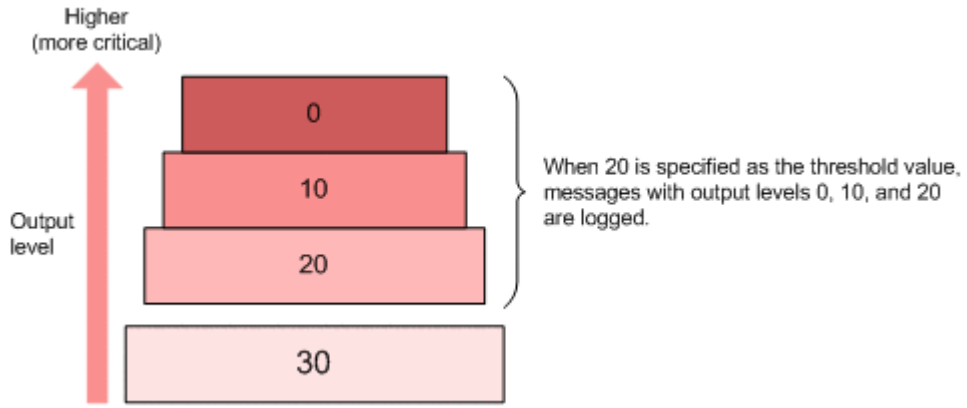


Figure 62 Relationship between the threshold value of the output levels and the output messages

logger.messagelogLevel

Specify an output level for the log data that is output to the `HTSMServerMessage*n*.log` file and the `HTSMGuiMessage*n*.log` file.

The output levels are based on the contents of the logged messages. 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: `20`

Table 114 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 GUI.
	20	Information has been produced about the processing for an operation.

logger.tracelogLevel

Specify an output level for the log data that is output to the`HTSMServerTracen.log` file and the `HTSMGuiTracen.log` file.

This property applies to the Tiered Storage Manager server trace log (`HTSMServerTracen.log`) and the GUI trace log (`HTSMGuiTracen.log`).

Output levels are based on the contents of the logged messages. 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`

Table 115 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.

logger.syslogLevel

Specify an output level for the event log data that is output by Tiered Storage Manager or for the log data that is output to syslog.

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`

logger.serverMessageFileCount

Specify the maximum number of backups of the `HTSMServerMessage`*n*`.log` file.

The range of specifiable values is from `2` to `16`.

When a log file reaches the maximum size specified in the `logger.serverMessageMaxFileSize` property, the file is renamed by adding a counter to the file name (for example, `HTSMServerMessage2.log`). The log files are used and written to in the order of the counter. 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`

Related references

- logger.serverMessageMaxFileSize on page 653

logger.serverTraceFileCount

Specify the maximum number of backups of the `HTSMServerTrace`*n*`.log` file.

The range of specifiable values is from `2` to `16`.

When a log file reaches the maximum size specified in the `logger.serverTraceMaxFileSize` property, the file is renamed by adding a counter to the file name (for example, `HTSMServerTrace2.log`). The log files are used and written to in the order of the counter. 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`

Related references

- logger.serverTraceMaxFileSize on page 654

logger.guiMessageFileCount

Specify the maximum number of backups of the `HTSMGuiMessage`*n*`.log` file.

The range of specifiable values is from `2` to `16`.

When a log file reaches the maximum size specified in the `logger.guiMessageMaxFileSize` property, the file is renamed by adding a counter to the file name (for example, `HTSMGuiMessage2.log`). The log files are used and written to in the order of the counter. 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`

Related references

- logger.guiMessageMaxFileSize on page 654

logger.guiTraceFileCount

Specify the maximum number of backups of the `HTSMGuiTrace`*n*`.log` file.

The range of specifiable values is from `2` to `16`.

When a log file reaches the maximum size specified in the `logger.guiTraceMaxFileSize` property, the file is renamed by adding a counter to the file name (for example, `HTSMGuiTrace2.log`). The log files are used and written to in the order of the counter. 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`

Related references

- logger.guiTraceMaxFileSize on page 654

logger.serverMessageMaxFileSize

Specify the maximum size of the `HTSMServerMessage`*n*`.log` file.

The range of specifiable values is from 32,768 bytes (32 KB) to 2,147,483,647 bytes (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

Specify the maximum size of the `HTSMServerTracen.log` file.

The range of specifiable values is from 32,768 bytes (32 KB) to 2,147,483,647 bytes (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 the `HTSMGuiMessagen.log` file.

The range of specifiable values is from 32,768 bytes (32 KB) to 2,147,483,647 bytes (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.guiTraceMaxFileSize

Specify the maximum size of the `HTSMGuiTracen.log` file.

The range of specifiable values is from 32,768 bytes (32 KB) to 2,147,483,647 bytes (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)

Tiered Storage Manager security properties (server.properties file)

The `server.properties` file contains properties related to Tiered Storage Manager security.

- In Windows:
  installation-folder-for-Hitachi-Command-Suite
  `\TieredStorageManager\conf\server.properties`
- In Linux:

installation-directory-for-Hitachi-Command-Suite/
TieredStorageManager/conf/server.properties

server.rmi.secure

Specify whether to use SSL for communications between the Tiered Storage Manager server and the management client (Tiered Storage Manager CLI).

Specify a value from 1 to 4 for this property.

1: Use non-SSL.

2: Use SSL. MD5withRSA is used as the signature algorithm.

3: Use SSL in advanced security mode. SHA256withRSA is used as the signature algorithm.

4: Use SSL in a restricted state, by using SHA256withRSA as the signature algorithm and using cipher suites in conformance with the security policy. Specify the cipher suites to be used in the server.rmi.security.enabledCipherSuites property.

Default: 1

Related references

- server.rmi.security.enabledCipherSuites on page 655

server.rmi.security.enabledCipherSuites

To use SSL/TLS communication between the Tiered Storage Manager server and the management client (Tiered Storage Manager CLI), specify cipher suites. Use commas (,) to separate multiple cipher suites.

This property takes effect only when the server.rmi.secure property in the server.properties file is set to 4.

Specifiable cipher suites are as follows:

- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA
- SSL_RSA_WITH_3DES_EDE_CBC_SHA

Default: TLS_RSA_WITH_AES_256_CBC_SHA256, TLS_RSA_WITH_AES_256_CBC_SHA, TLS_RSA_WITH_AES_128_CBC_SHA256, TLS_RSA_WITH_AES_128_CBC_SHA, SSL_RSA_WITH_3DES_EDE_CBC_SHA

Related references

- server.rmi.secure on page 655

server.rmi.security.protocols

To use SSL/TLS communication between the Tiered Storage Manager server and the management client (Tiered Storage Manager CLI), specify protocols. Use commas (,) to separate multiple protocols.

The specifiable protocols are as follows:

- `TLSv1`
- `TLSv1.1`
- `TLSv1.2`

The specified protocols are used in order of their cipher strength, from highest to lowest.

Default: `TLSv1,TLSv1.1,TLSv1.2`

C

Host Data Collector properties

This section describes the Host Data Collector property file.

- Host Data Collector property files
- Properties related to Host Data Collector operation (hdcbase.properties file)
- Host Data Collector logger properties (logger.properties file)
- Properties related to the Host Data Collector's Java environment (javaconfig.properties file)
- Host Data Collector security properties (hdcbase.properties file)

Host Data Collector property files

The Host Data Collector property files include a property file related to Host Data Collector operation and a property file related to log output.

The following table describes the Host Data Collector property files .

Table 116 Host Data Collector property files

Property file	Description
`hdcbase.properties` file	This property file is related to Host Data Collector operation.
`logger.properties` file	This property file is related to log output by Host Data Collector.
`javaconfig.properties` file	This property file is related to a Java environment for Host Data Collector.
`hdcbase.properties` file	This property file is related to Host Data Collector security.

Changing Host Data Collector properties

Use a text editor to edit the property files of Host Data Collector.

Before you begin

Log in as a user with Administrator permissions (for Windows) or as a root user (for Linux).

Procedure

1. Stop the Host Data Collector service.
2. Use a text editor to set the appropriate values in the Host Data Collector property files.
3. Start the Host Data Collector service.

Related tasks

- Starting the Host Data Collector service on page 464
- Stopping the Host Data Collector service on page 464

Properties related to Host Data Collector operation (hdcbase.properties file)

The `hdcbase.properties` file contains properties related to Host Data Collector operation.

- In Windows:

installation-folder-for-Host-Data-Collector\HDC\Base\config\hdcbase.properties

- In Linux:
  installation-directory-for-Host-Data-Collector/HDC/Base/config/hdcbase.properties

hdc.service.localport

Specify the port number on the Service process side that is used when the Service process and the Adapter process communicate each other.

Specifiable range: 1 to 65535.

Default: 22110

hdc.adapter.adapterProcessNum

Specify the number of Adapter processes that can start on the same host.

Specifiable range: 1 to 10.

Default: 1

hdc.adapter.localport

Specify the port number on the Adapter process side that is used when the Service process and the Adapter process communicate each other.

When you start multiple Adapter processes, specify the port numbers delimited by a comma (,). No more than 10 port numbers can be specified. If the number of port numbers is more than the number of Adapter processes to be started, only as many port numbers as Adapter processes to be started are enabled.

Specifiable range: 1 to 65535.

Default:
22111,22112,22113,22114,22115,22116,22117,22118,22119,22120

Related references

- hdc.adapter.adapterProcessNum on page 659

hdc.common.rmi.registryPort

Specify the non-SSL communication port number of the RMI registry.

Specifiable range: 1 to 65535. This port is also used for internal communication by Host Data Collector.

Default: 22098

Note: If you changed the value of this property, the following settings must be performed:

- Use the `firewall_setup` command to reset the firewall exemptions (when the value of the `hdc.ssl.secure` property is `1` or `2`).
- Set the same value as the `hdc.rmiregistry` property of the Device Manager server (when non-SSL communication is used by Host Data Collector and the Device Manager server).

Related tasks

- Registering an exception for the Host Data Collector service (for non-SSL communication) on page 141

Related references

- hdc.rmiregistry on page 626
- hdc.ssl.secure on page 663

hdc.common.rmi.serverPort

Specify the non-SSL communication port number of the RMI server.

Specifiable range: `1` to `65535`.

Default: `22099`

Note: If you changed the value of this property, the following settings must be performed:

- Use the `firewall_setup` command to reset the firewall exemptions (when the value of the `hdc.ssl.secure` property is `1` or `2`).
- Set the same value as the `hdc.rmiserver` property of the Device Manager server (when non-SSL communication is used by Host Data Collector and the Device Manager server).

Related tasks

- Registering an exception for the Host Data Collector service (for non-SSL communication) on page 141

Related references

- hdc.rmiserver on page 626
- hdc.ssl.secure on page 663

hdc.common.http.serverPort

Specify the non-SSL communication port number of the class loader.

Specifiable range: `1` to `65535`.

Default: `22100`

Note: If you changed the value of this property, the following settings must be performed:

- Use the `firewall_setup` command to reset the firewall exemptions (when the value of the `hdc.ssl.secure` property is `1` or `2`).
- Set the same value as the `hdc.classloader` property of the Device Manager server (when non-SSL communication is used by Host Data Collector and the Device Manager server).

Related tasks

- Registering an exception for the Host Data Collector service (for non-SSL communication) on page 141

Related references

- hdc.classloader on page 627
- hdc.ssl.secure on page 663

hdc.common.rmi.ssl.registryPort

Specify the SSL communication port number of the RMI registry.

Specifiable range: `1` to `65535`.

Default: `22104`

Note: If you changed the value of this property, the following settings must be performed:

- Use the `netsh` command to reset the firewall exemptions (when the value of the `hdc.ssl.secure` property is `2` or `3`).
- Set the same value as the `hdc.rmiregistry` property of the Device Manager server (when SSL communication is used by Host Data Collector and the Device Manager server).

Related tasks

- Registering an exception for the Host Data Collector service (for SSL communication) on page 142

Related references

- hdc.rmiregistry on page 626
- hdc.ssl.secure on page 663

hdc.common.rmi.ssl.serverPort

Specify the SSL communication port number of the RMI server.

Specifiable range: `1` to `65535`.

Default: `22105`

Note: If you changed the value of this property, the following settings must be performed:

- Use the `netsh` command to reset the firewall exemptions (when the value of the `hdc.ssl.secure` property is `2` or `3`).
- Set the same value as the `hdc.rmiserver` property of the Device Manager server (when SSL communication is used by Host Data Collector and the Device Manager server).

Related tasks

- Registering an exception for the Host Data Collector service (for SSL communication) on page 142

Related references

- hdc.rmiserver on page 626
- hdc.ssl.secure on page 663

hdc.common.https.serverPort

Specify the SSL communication port number of the class loader.

Specifiable range: `1` to `65535`.

Default: `22106`

Note: If you changed the value of this property, the following settings must be performed:

- Use the `netsh` command to reset the firewall exemptions (when the value of the `hdc.ssl.secure` property is `2` or `3`).
- Set the same value as the `hdc.classloader` property of the Device Manager server (when SSL communication is used by Host Data Collector and the Device Manager server).

Related tasks

- Registering an exception for the Host Data Collector service (for SSL communication) on page 142

Related references

- hdc.classloader on page 627
- hdc.ssl.secure on page 663

hdc.service.rmi.registryIPAddress

If the machine that is running Host Data Collector has multiple IP addresses, specify the IP address to be used for communication with the Device Manager server.

For the IP address, you can use either an IPv4 address or IPv6 address.

Make sure that the IP address you specify is the same as the value specified for the following properties in the `hostdatacollectors.properties` file on the Device Manager server:

- `hdc.rmiregistry`
- `hdc.rmiserver`
- `hdc.classloader`

Default: None#

#: If you do not specify an IP address, the IP address acquired by Host Data Collector will be used.

Related references

- hdc.rmiregistry on page 626
- hdc.rmiserver on page 626
- hdc.classloader on page 627

hdc.service.fileCleanup.startTime

Specify the time at which host information files that Host Data Collector collected from managed hosts are deleted, in the format *hhmm*.

Specify a value from `00` to `23` for *hh*, and `00` to `59` for *mm*.

Default: `2300`

hdc.adapter.esx.timeout

Specify the timeout value, in seconds, for Host Data Collector to acquire information from a managed virtualization server.

Specifiable range: `0` to `2147483647`.

Default: `1200`

hdc.ssl.secure

Specify the port to be opened for communication between Host Data Collector and the Device Manager server.

Specifiable range: `1` to `3`.

`1`: Only the non-SSL communication ports are open.

`2`: Both the non-SSL communication ports and the SSL communication ports are open.

`3`: Only the SSL communication ports are open.

The correspondences between the `hdc.ssl.secure` property values and the port numbers to be opened are as follows:

Table 117 Correspondences between the hdc.ssl.secure property values and the port numbers to be opened

hdc.ssl.secure property value	Port numbers to be opened (Default)	
1	RMI registry	22098/tcp
	RMI server	22099/tcp
	Class loader	22100/tcp
2	RMI registry	22098/tcp, 22104/tcp
	RMI server	22099/tcp, 22105/tcp
	Class loader	22100/tcp, 22106/tcp
3	RMI registry	22098/tcp, 22104/tcp
	RMI server	22105/tcp
	Class loader	22106/tcp

#

The non-SSL communication port for the RMI registry (22098/tcp by default) is always open because it is also used for internal communication by Host Data Collector.

Default: 1

Related references

- hdc.common.rmi.registryPort on page 659
- hdc.common.rmi.serverPort on page 660
- hdc.common.http.serverPort on page 660
- hdc.common.rmi.ssl.registryPort on page 661
- hdc.common.rmi.ssl.serverPort on page 661
- hdc.common.https.serverPort on page 662

hdc.ssl.esx.certCheck

If you are using the server certificate issued by a certificate authority for SSL communication between a virtualization server and Host Data Collector, specify whether to check the validity of the certificate.

Host Data Collector can perform the following to check the validity of a certificate:

- Check whether the server certificate is valid
- Verify the server certificate's chain
- Check the Subject Alternative Names of the server certificate

To check the validity of the certificate, specify 1. If you do not want to check the validity of the certificate, specify 0.

Default: 0

Host Data Collector logger properties (logger.properties file)

The `logger.properties` file contains properties related to Host Data Collector log output.

- In Windows:
  installation-folder-for-Host-Data-Collector\HDC\Base\config\logger.properties
- In Linux:
  installation-directory-for-Host-Data-Collector/HDC/Base/config/logger.properties

logger.trace.level

Specify the output level for the Host Data Collector trace log.

Messages whose output level is equal to or smaller than the value of this property will be output to the trace log.

Table 118 Trace log output level

Message type	Output level	Description
ERROR	0	error
WARNING	10	warning
INFO	30	information
-	40	debug

You can specify `0`, `10`, `30`, or `40`.

Default: `30`

logger.trace.maxFileSize

Specify the maximum size of the Host Data Collector trace log.

The specified size is assumed to be in bytes unless you specify `KB` for kilobytes, `MB` for megabytes or `GB` for gigabytes.

Specifiable range: `4096` to `2147483647`.

Default: `5242880`

logger.trace.numOfFiles

Specify the maximum number of backup files for the Host Data Collector log.

If a log file reaches the maximum size specified by the `logger.trace.maxFileSize` property, the file is renamed by adding a counter (which represents the version) to the file name. If additional backup

log files are created, the counter increases until the specified number of backup log files is generated. After the specified number of backup log files is created, each time a new backup file is created, the oldest backup file is deleted.

Specifiable range: `2` to `16`.

Default: `10`

Related references

- logger.trace.maxFileSize on page 665

logger.iotrace.maxFileSize

Specify the maximum size of the Host Data Collector communication trace log.

The specified size is assumed to be in bytes unless you specify `KB` for kilobytes, `MB` for megabytes or `GB` for gigabytes.

Specifiable range: `4096` to `2147483647`.

Default: `5242880`

logger.iotrace.numOfFiles

Specify the maximum number of backup files for the Host Data Collector communication trace log.

If a log file reaches the maximum size specified by the `logger.iotrace.maxFileSize` property, the file is renamed by adding a counter (which represents the version) to the file name. If additional backup log files are created, the counter increases until the specified number of backup log files is generated. After the specified number of backup log files is created, each time a new backup file is created, the oldest backup file is deleted.

Specifiable range: `2` to `16`.

Default: `10`

Related references

- logger.iotrace.maxFileSize on page 666

Properties related to the Host Data Collector's Java environment (javaconfig.properties file)

The `javaconfig.properties` file contains properties related to the Java environment of the Host Data Collector.

- In Windows:

installation-folder-for-Host-Data-Collector\HDC\Base\config\javaconfig.properties

- In Linux:
  installation-directory-for-Host-Data-Collector/HDC/Base/config/javaconfig.properties

javapathlocation

Use the absolute path to specify the location of the Java execution environment to be used by Host Data Collector.

If the path contains a space, you do not need to enclose the path with quotation marks (").

Default:

None (The Java execution environment that comes with Host Data Collector is used.)

Host Data Collector security properties (hdcbase.properties file)

The `hdcbase.properties` file contains the security properties.

- In Windows:
  installation-folder-for-Host-Data-Collector\HDC\Base\config\hdcbase.properties
- In Linux:
  installation-directory-for-Host-Data-Collector/HDC/Base/config/hdcbase.properties

hdc.ssl.ciphers

If SSL/TLS is in use for communication between the Device Manager server and Host Data Collector, specify the cipher suites. Use commas (,) to separate multiple cipher suites.

The specifiable cipher suites are as follows:

- `TLS_RSA_WITH_AES_256_CBC_SHA256`
- `TLS_RSA_WITH_AES_128_CBC_SHA256`
- `TLS_RSA_WITH_AES_256_CBC_SHA`
- `TLS_RSA_WITH_AES_128_CBC_SHA`

Default: `TLS_RSA_WITH_AES_256_CBC_SHA256, TLS_RSA_WITH_AES_128_CBC_SHA256, TLS_RSA_WITH_AES_256_CBC_SHA, TLS_RSA_WITH_AES_128_CBC_SHA`

hdc.ssl.esx.enabledTLSv1

Specify whether to allow the use of TLS version 1.0 when using SSL/TLS communication between a virtualization server and Host Data Collector.

You can specify `0`, or `1`.

`0`: Suppresses the use of TLS version 1.0.

`1`: Allows the use of TLS version 1.0.

Default: `1`

D

Device Manager agent properties

This section describes the property files of a Device Manager agent.

- Device Manager agent property files
- Device Manager agent properties for connecting to the Replication Manager server (agent.properties file)
- Device Manager agent properties for hldutil command operations (hldutil.properties file)
- Device Manager agent log output properties (logger.properties file)
- Device Manager agent properties for program information (programproductinfo.properties file)
- Device Manager agent operations properties (server.properties file)
- Properties for command devices connected to Device Manager agent (rgcmddev.properties file)

Device Manager agent property files

There is a Device Manager agent property file for Device Manager agent operations and a property file for settings related to the connection between the Device Manager agent and the Replication Manager server.

The following table describes the Device Manager agent property files.

Table 119 Device Manager agent property files

Property file	Description
`agent.properties` file	This property file is related to the connection between the Device Manager agent and the Replication Manager server.
`hldutil.properties` file	This property file is related to the Device Manager agent operations performed when executing the `hldutil` command.
`logger.properties` file	This property file is related to the Device Manager agent log output.
`programproductinfo.properties` file	This property file is related to the program information of the Device Manager agent.
`server.properties` file	This property file is related to Device Manager agent operations.
`rgcmddev.properties` file	This property file is related to the command devices that Device Manager agent connects to.

Caution: The default values are set during a new installation.

Changing Device Manager agent properties

Use a text editor to edit Device Manager agent property files.

Before you begin

Log in as a user with Administrator permissions (for Windows) or as a root user (for UNIX).

Procedure

1. Execute the `hbsasrv` command to stop the Device Manager agent service.
2. Use a text editor to set appropriate values in the Device Manager agent property files.
3. Execute the `hbsasrv` command to start the Device Manager agent service.

Related references

- Starting and stopping the Device Manager agent service, and checking the operating status of the service (hbsasrv command) on page 528

Device Manager agent properties for connecting to the Replication Manager server (agent.properties file)

The `agent.properties` file contains properties related to connecting to the Replication Manager server.

- In Windows:
  installation-folder-for-Device-Manager-agent\mod\hrpm\config\agent.properties
- In Linux:
  installation-directory-for-Device-Manager-agent/mod/hrpm/config/agent.properties
- In Solaris or HP-UX:
  /opt/HDVM/HBaseAgent/mod/hrpm/config/agent.properties
- In AIX:
  /usr/HDVM/HBaseAgent/mod/hrpm/config/agent.properties

Note: The Device Manager agent uniquely creates and manages the configuration definition files and instances for monitoring to monitor the statuses of copy pairs in Replication Manager. The *HORCM instance for monitoring* is the instance of CCI used by the Device Manager agent. The *HORCM file for monitoring* is the CCI configuration definition file of that instance.

agent.rm.TimeOut

Specify the time limit for a response from the CCI command used by the Device Manager agent (in seconds).

Specify a value from 0 to 86,400. Specify `0` for no time-out.

Default: `600`

Normally, the values set for these parameters do not need to be changed. To change their values, you need expert knowledge of the Device Manager agent.

agent.rm.everytimeShutdown

Specify whether to stop the HORCM instance for monitoring every time.

Specify `true` or `false`. If `true` is specified, the instance stops every time. If `false` is specified, the instance does not stop.

Default: `false`

Normally, the values set for these parameters do not need to be changed. To change their values, you need expert knowledge of the Device Manager agent.

agent.rm.shutdownWait

Specify the wait time when stopping the HORCM instance for monitoring (in seconds).

Specify a value from 1 to 60.

Default: `5`

agent.rm.horcmInstance

Specify the maximum value for an instance number of the HORCM file for monitoring.

Specify a value from 1 to 2047. This value must be different from the instance number of other CCI configuration definition files.

Default: `2047`

The instance numbers of the HORCM file for monitoring differ depending on the version of CCI.

If the version of CCI is 01-32-03/*XX* or later

Instance numbers in the following range, calculated from the values of this property and the `agent.rm.horcmRange` property, are used. The default is the range from 1948 to 2047.

Maximum value for an instance number: *value-specified-by-this-property*

Minimum value for an instance number: (*value-specified-by-this-property*) - (*value-specified-by-the-agent.rm.horcmRange-property*) + 1

If the version of CCI is earlier than 01-32-03/*XX*

The value specified by this property and the *value-specified-by-this-property* - 1 are used as the instance numbers. The defaults are 2046 and 2047.

Do not set a value from 990 to 998 because Device Manager agent uses these values by default.



Tip: The instance numbers for use by the Device Manager agent can be changed by using the `server.agent.rm.temporaryInstance` property in the `server.properties` file.

Related references

- agent.rm.horcmRange on page 673
- server.agent.rm.temporaryInstance on page 686

agent.rm.horcmService

Specify the maximum value for a port number of the HORCM file for monitoring.

Specify a value from 2 to 65535. This value must be different from the port number of other applications.

Default: `54323`

The port numbers of the HORCM file for monitoring differ depending on the version of CCI.

If the version of CCI is 01-32-03/*XX* or later

Port numbers in the following range, calculated from the values of this property and the `agent.rm.horcmRange` property, are used. The default is the range from 54224 to 54323.

Maximum value for a port number: *value-specified-by-this-property*

Minimum value for a port number: (*value-specified-by-this-property*) - (*value-specified-by-the-agent.rm.horcmRange-property*) + 1

If the version of CCI is earlier than 01-32-03/*XX*

The value specified by this property and the *value-specified-by-this-property* - 1 are used as the port number. The defaults are 54322 and 54323.

Do not set a value from 53232 to 53330 because the Device Manager agent uses these values by default.

Tip: The UDP port numbers for use by the Device Manager agent can be changed by using the `server.agent.rm.temporaryPort` property in the `server.properties` file.

Related references

- agent.rm.horcmRange on page 673
- server.agent.rm.temporaryPort on page 686

agent.rm.horcmRange

Specify the number of instance numbers of the HORCM file for monitoring, and the number of UDP port numbers.

This property is enabled only when the version of CCI is 01-32-03/*XX* or later.

You can specify a value in the range from 10 to 1000. Specify a value greater than the value calculated by the following formula:

2 x (2 + *number-of-storage-systems-that-comprise-the-virtual-storage-machine*)

Default: `100`

Related references

- agent.rm.horcmInstance on page 672
- agent.rm.horcmService on page 673

agent.logger.loglevel

Specify the output level of the log file for the Replication Manager agent functionality.

Log data that has a level equal to or higher than the specified value is output. Specify one of the following values (listed in ascending order of importance):

`DEBUG`, `INFO`, `WARN`, `ERROR`, `FATAL`

Default: `INFO`

agent.logger.MaxBackupIndex

Specify the maximum number of log files for the Replication Manager agent functionality.

Specify a value from 1 to 20. When the number of log files generated reaches this value, the log files are reused, beginning with the oldest file.

Default: `5`

The size of an output log file depends on the number of copy pairs managed by Replication Manager. You can use the following formula to determine the log file output size:

amount-of-information-output-to-log-file (MB/week) = 0.75 x *number-of-copy-pairs* + 4

Set the values of `agent.logger.MaxBackupIndex` and `agent.logger.MaxFileSize` taking into account the amount of information that is output and the retention period. To check the number of copy pairs managed by the target host (pair management server), use Replication Manager's *copy-group-name* subwindow.

Related references

- agent.logger.MaxFileSize on page 674

agent.logger.MaxFileSize

Specify the maximum size of log files for the Replication Manager agent functionality.

Specify a value from 512 KB to 32 MB. You can specify the value in bytes, kilobytes, or megabytes. If `KB` or `MB` is not specified for the number, bytes is assumed.

Default: `5 MB`

The size of an output log file depends on the number of copy pairs managed by Replication Manager. You can use the following formula to determine the log file output size:

amount-of-information-output-to-log-file (MB/week) = 0.75 x *number-of-copy-pairs* + 4

Set the values of `agent.logger.MaxBackupIndex` and `agent.logger.MaxFileSize` taking into account the amount of information that is output and the retention period. To check the number of copy pairs managed by the target host (pair management server), use Replication Manager's *copy-group-name* subwindow.

Related references

- agent.logger.MaxBackupIndex on page 674

Device Manager agent properties for hldutil command operations (hldutil.properties file)

The `hldutil.properties` file contains properties related to `hldutil` command operations.

- In Windows:
  installation-folder-for-Device-Manager-agent\util\bin\hldutil.properties
- In Linux:
  installation-directory-for-Device-Manager-agent/util/bin/hldutil.properties
- In Solaris or HP-UX:
  /opt/HDVM/HBaseAgent/util/bin/hldutil.properties
- In AIX:
  /usr/HDVM/HBaseAgent/util/bin/hldutil.properties

agent.util.hpux.displayDsf

Specify the format of the device file name displayed when the `hldutil` command is executed on a host on whose OS is HP-UX 11i v3.

If `disk` is specified:

When the `hldutil` command is executed, disk device file names are displayed.

If `ctd` is specified:

When the `hldutil` command is executed, ctd device file names are displayed.

If `mix` is specified:

When the `hldutil` command is executed, both disk and ctd device file are displayed.

If any value other than the above is specified, `mix` is assumed.

Default: `mix`

Device Manager agent log output properties (logger.properties file)

The `logger.properties` file contains properties related to the Device Manager agent log output.

- In Windows:
  installation-folder-for-Device-Manager-agent\agent\config\logger.properties
- In Linux:
  installation-directory-for-Device-Manager-agent/agent/config/logger.properties
- In Solaris or HP-UX:
  /opt/HDVM/HBaseAgent/agent/config/logger.properties
- In AIX:
  /usr/HDVM/HBaseAgent/agent/config/logger.properties

Note: The files `access.log`, `error.log`, `service.log`, and `trace.log` are output to the following locations:

In Windows:

installation-folder-for-the-Device-Manager-agent\agent\logs\

In Linux:

installation-directory-for-the-Device-Manager-agent/agent/logs/

In Solaris or HP-UX:

/opt/HDVM/HBaseAgent/agent/logs/

In AIX:

/usr/HDVM/HBaseAgent/agent/logs/

---

logger.loglevel

Specify the minimum level of log data that the Device Manager agent outputs to the files `error.log` and `trace.log`.

The values can be specified (in increasing order of importance) are `DEBUG`, `INFO`, `WARN`, `ERROR`, and `FATAL`. For example, if the default value is specified, `INFO`, `WARN`, `ERROR`, and `FATAL` data is output to the log files, but `DEBUG` data is not output.

Default: `INFO`

logger.MaxBackupIndex

Specify the maximum number of backup files for the files `access.log`, `error.log`, `service.log`, and `trace.log`.

When a log file reaches the maximum size specified in the `logger.MaxFileSize` property, the file is renamed by adding a counter to the file name (for example, `access.log.1`). If additional backup log files are created, the counter increases until the specified number of backup log files is generated (for example, `access.log.1` becomes `access.log.2`). After the specified number of backup log files is created, each time a new backup file is created, the oldest backup file is deleted.

Specify a value from 1 to 20.

Default: `10`

The size of an output log file depends on the number of copy pairs managed by Replication Manager. You can use the following formula to determine the log file output size:

amount-of-information-output-to-log-file (MB/week) = 0.8 x *number-of-copy-pairs* + 25

Set the values of `logger.MaxBackupIndex` and `logger.MaxFileSize` taking into account the amount of information that is output and the retention period. To check the number of copy pairs managed by the target host (pair management server), use Replication Manager's *copy-group-name* subwindow.

Related references

- logger.MaxFileSize on page 677

logger.MaxFileSize

Specify the maximum size of the files `access.log`, `error.log`, `service.log`, and `trace.log`.

If a log file becomes larger than this value, the Device Manager agent creates a new file and writes log data to it. Unless `KB` is specified for kilobytes or `MB`

for megabytes, the specified size is interpreted to mean bytes. Specify a value from 512 KB to 32 MB.

Default: `5 MB`

The size of an output log file depends on the number of copy pairs managed by Replication Manager. You can use the following formula to determine the log file output size:

amount-of-information-output-to-log-file (MB/week) = 0.8 x *number-of-copy-pairs* + 25

Set the values of `logger.MaxBackupIndex` and `logger.MaxFileSize` taking into account the amount of information that is output and the retention period. To check the number of copy pairs managed by the target host (pair management server), use Replication Manager's *copy-group-name* subwindow.

Related references

- logger.MaxBackupIndex on page 677

Device Manager agent properties for program information (programproductinfo.properties file)

The `programproductinfo.properties` file contains properties related to the program information of the Device Manager agent.

This file exists only when the host OS is Windows.

installation-folder-for-Device-Manager-agent`\agent\config\programproductinfo.properties`

veritas.volume.manager.version

Specify the version of VxVM installed in Windows.

If VxVM is installed in a Windows environment, specify the VxVM version in this property, in the format *x.x*.

Default: None

Device Manager agent operations properties (server.properties file)

The `server.properties` file contains properties related to Device Manager agent operations.

- In Windows:
  installation-folder-for-Device-Manager-agent`\agent\config\server.properties`

- In Linux:
  installation-directory-for-Device-Manager-agent/agent/config/server.properties
- In Solaris or HP-UX:
  /opt/HDVM/HBaseAgent/agent/config/server.properties
- In AIX:
  /usr/HDVM/HBaseAgent/agent/config/server.properties

server.agent.port

Specify the port number for the Device Manager agent's daemon process (or service).

Avoid specifying small port numbers because such numbers might conflict with other applications. The normal range is 1024 to 49151. If a version of Dynamic Link Manager earlier than 5.8 is installed, specify 23013.

Note that if the host OS is Windows and you have changed the port, you must use the `firewall_setup` command to specify the firewall exception settings again.

Default: `24041`

server.http.localPort

Specify the port number for communication between the Device Manager agent's daemon process and the Web server process.

Avoid specifying small port numbers because such numbers might conflict with other applications. The normal range is 1024 to 49151.

Note that if the host OS is Windows and you have changed the port, you must use the `firewall_setup` command to specify the firewall exception settings again.

Default: `24043`

server.http.port

Specify the port number that the Device Manager agent's Web server uses.

Avoid specifying small port numbers because such numbers might conflict with other applications. The normal range is 1024 to 49151. If a version of Dynamic Link Manager earlier than 5.8 is installed, specify 23011.

Note that if the host OS is Windows and you have changed the port, you must use the `firewall_setup` command to specify the firewall exception settings again.

Default: `24042`

server.http.host

Specify the host that executes the Device Manager agent's Web server.

Make sure the specified host name can be resolved to an IP address.

Default: `localhost`

Caution: In the following cases, if the host before the change and the host after the change are both registered as hosts to be managed by Device Manager, delete the host before the change:

- If the service of the Device Manager agent was restarted after the value of this property was changed
- If an upgrade installation of the Device Manager agent to version 8.5.0 or later was performed in the environment in which the value of this property is being changed

server.http.socket.agentAddress

Specify the IP address that Device Manager agent reports to the Device Manager server.

In order to limit the IP addresses that Device Manager agent reports to the Device Manager server, specify the IP address to be reported.

For the IP address, you can specify either an IPv4 address or an IPv6 address.

If you specify an IPv4 address, both the specified IPv4 address and the IPv6 address[#1] set for the same NIC are reported. If you specify an IPv6 address, both the specified IPv6 address and the IPv4 address[#1] set for the same NIC are reported.

For operation in an IPv6 environment, specify a global address. If you specify a site-local address or link-local address, the IPv4 address will be used.

It is necessary to match the IP address version to the one specified in `server.http.socket.bindAddress`.

The IP address that you specified in this property can also be used when creating or editing the CCI configuration definition file. If CCI is used with the Device Manager agent, make sure that communication between CCI instances is possible using the specified IP address.

Default: None[#2]

#1: The first IP address acquired by the Device Manager agent will be reported.

#2: If no IP address is specified, the IP address acquired by the Device Manager agent will be used. If there are multiple IP addresses, the first IP address acquired by the Device Manager agent will be used.

Related references

- server.http.socket.bindAddress on page 681

server.http.socket.bindAddress

In situations in which the Device Manager agent runs on a platform on which two or more NICs are installed, specify the NIC through which the Device Manager agent can accept requests.

If you want to restrict the interface to be accepted, specify the IP address to be accepted with the Device Manager agent.

For operation in an IPv6 environment, specify a global address. If you specify a site-local address or link-local address, the default value will be used.

It is necessary to match the IP address version to the one specified in `server.http.socket.agentAddress`.

Default: None. (The Device Manager agent accepts all NIC requests.)

Related references

- server.http.socket.agentAddress on page 680

server.agent.maxMemorySize

Specify the maximum memory heap size for the Web server function processes of the Device Manager agent (in MB).

Specifiable range (MB): 32 to 4096.

Default: None#

#: The heap runs in a 64 MB memory area. In Solaris (x64 Edition (AMD64)) , the heap runs in a memory area that is 1/4 of the physical memory area or a 1 GB memory area, whichever is smaller.

Caution: If you are using both Device Manager and Replication Manager, for each product, specify the required memory size.

Related concepts

- Settings required for a host to manage 100 or more LUs on page 524
- Managing copy pairs on page 521

server.agent.shutDownTime

Specify the period to shutdown the Device Manager agent's Web server after it receives or sends the last HTTP/XML message (in milliseconds).

Specify a value from 1 to 9223372036854775807.

Do not edit this property without current knowledge of the Device Manager agent's performance.

Default: `600000`

server.agent.JRE.location

Specify the absolute path to the installation destination of the software that provides the Java execution environment for the Device Manager agent.

For Windows, use a forward slash (/) as the path delimiter.

Default: Installation path for the Java execution environment used on the Device Manager agent



Caution:

- If the host OS is Windows or Linux and this property is omitted, the Java execution environment bundled with the Device Manager agent is used.
- In the following cases, use a 32-bit Java execution environment:
  - If the host OS is Windows or Solaris
  - If the host OS is Linux, and performance information about Virtual Storage Platform or Universal Storage Platform V/VM storage systems is acquired by using the CIM/WBEM function

  If the host OS is Red Hat Enterprise Linux 7 or later, Oracle Linux 7 or later, or SUSE Linux Enterprise Server 12 or later, use a 64-bit Java execution environment.
- For details on the Java execution environment that can be specified when Dynamic Link Manager is installed on the host, see the Dynamic Link Manager documentation.

server.http.entity.maxLength

Specify the maximum size of HTTP request entities permitted by the Web server function of the Device Manager agent (in bytes).

Normally, the default value of this property need not be changed. By limiting the impact of malicious requests with an entity that has an abnormally large data size, this setting can be useful in repelling attacks that are intended to impair services or cause a buffer overflow. When detecting a post request larger than the specified limit, the Device Manager agent sends a remote error response and records details of the request in the log.

Default: `262144`

server.http.security.clientIP

Specify an IPv4 or IPv6 address that can be used to connect to the Device Manager agent.

This setting limits the IP addresses permitted for connection, thus preventing denial-of-service attacks or other attacks that intend to overflow buffers.

You can use an asterisk (*) as a wildcard character when you use IPv4 addresses. To specify multiple IP addresses, separate them with commas (,).

In the following example, the specification permits the address `191.0.0.2` and addresses from `192.168.0.0` to `192.168.255.255` to connect to the Device Manager agent:

```
server.http.security.clientIP=191.0.0.2, 192.168.*.*
```

In the following example, the specification permits the addresses `2001::203:baff:fe36:109a` and `2001::203:baff:fe5b:7bac` to connect to the Device Manager agent:

```
server.http.security.clientIP=2001::203:baff:fe36:109a,
2001::203:baff:fe5b:7bac
```

Default: None (All IP addresses can connect to the Device Manager agent.)

server.server.authorization

This property stores the ID and password of the user for Device Manager server authorization.

This property is encoded, so you cannot edit it using a text editor. To edit this property, use the `hdvmagt_setting` command.

Default: None

server.server.serverIPAddress

Specify the IP address or host name of the Device Manager server.

When specifying an IP address:

For IPv4, specify the IP address in dotted-decimal format.

For IPv6, specify the IP address using hexadecimal numbers with colons. Abbreviation can be used. The following example shows how to specify an IPv6 address:

```
server.server.serverIPAddress=2001::214:85ff:fe02:e53b
```

When specifying a host name:

Use a character string of 50 bytes or fewer to specify the host name. The following characters can be used:

```
a-z A-Z 0-9 - . @ _
```

Default: `255.255.255.255`

server.server.serverPort

Specify the port number of the Device Manager server to which the Device Manager agent is going to connect.

As a general rule, you can specify a value from 1024 to 49151. You must specify the same value specified for the `server.http.port` property (for non-SSL communication with the Device Manager server) or the

`server.https.port` property (for SSL communication with the Device Manager server) of Device Manager server.

Default: `2001`

Related references

- server.http.port on page 592
- server.https.port on page 593

server.agent.rm.centralizePairConfiguration

Specify whether to manage copy pairs for each host or to centrally manage all copy pairs on a single host.

disable

Specify this value to manage copy pairs at each host (pair management server).

enable

When the system uses the central management method, specify this value to manage all copy pairs with a single host (pair management server) .

Default: `disable`

Related concepts

- System configuration for managing copy pairs (other than the central management method) on page 67

Related references

- System configuration for managing copy pairs (central management method) on page 63

server.agent.rm.cuLdevForm

Specify the output format for LDEV numbers when pair volume information is written in `HORCM_LDEV` format in the configuration definition file when creating pairs.

If omitted, the information will be output in decimal format.

DECIMAL

Specify to output in decimal format.

CULDEV

Specify to output in *CU:LDEV* format.

HEXA

Specify to output in hexadecimal format.

This property is enabled only when creating copy pairs for VSP G1000, G1500, VSP F1500, VSP Gx00 models, VSP Fx00 models, Virtual Storage Platform, Universal Storage Platform V/VM, or HUS VM. In addition, if a virtual command device is used for the target copy pair command device (if a command device is set for the `HORCM_CMD` parameter in IPCMD format), LDEV numbers will be output in decimal format regardless of the value specified for this parameter.

Default value: `CULDEV`

server.agent.rm.exclusion.instance

On the host where the Device Manager agent is installed, to exclude a pair volume that is already being managed by CCI from Device Manager operations, specify the applicable CCI instance numbers.

The volume pairs excluded from Device Manager operations are also excluded from Replication Manager operations. To specify multiple instance numbers, separate the individual numbers with commas (`,`). From the Device Manager agent, you cannot operate a CCI whose instance number is specified in this property.

Default: None

server.agent.rm.location

Specify the CCI installation directory if CCI is installed in a location other than the default or if the host OS is Windows and the CCI installation drive is different from the Device Manager agent installation drive.

For Windows, use a forward slash (`/`) as the path delimiter.

Default for Windows: *drive-where-Device-Manager-agent-is-installed*`/HORCM`

Default for UNIX: `/HORCM`

server.agent.rm.optimization.userHorcmFile

Specify whether to optimize the user-created CCI configuration definition files.

To optimize the file, specify `true`. If you do this, the file is updated so that Device Manager can use it. Also, when the Device Manager agent starts or when the configuration definition file is updated by pair operations, the following optimizations are performed:

- The unit ID, LDEV number, and serial number of a command device are added as comments.
- If the above command device becomes unavailable due to, for example, a change to the volume name, the configuration definition file information is updated so that the command device can be used.

- If the host is connected to multiple command devices in a storage system and only some of those command devices are specified, the rest of the command devices are specified as reserved command devices.
- Command devices that are not being used are deleted.
- The CU and LDEV numbers of a command device and pair volume are added as a comment in the format *cu*:*ldev*.
- If there are multiple definitions for a command device of the same storage system in an SLPR environment, rearrange the order of the command device definitions.
- Apply the value specified in the `server.agent.rm.horcm.poll` property to `poll` of the `HORCM_MON` parameter in the configuration definition file.

Default: `false`

server.agent.rm.horcm.poll

Specify the value defined for `poll` of the `HORCM_MON` parameter in the configuration definition file (the monitoring interval for copy pairs) in hundredths of a second.

If monitoring is not being performed, specify `-1`.

The value specified for this property is applied to the configuration definition file at the following times:

- When a pair is created or added
- When the configuration definition file is optimized

Default: None#

#: In a newly created configuration definition file, `poll` is set to `1000`. When a pair is added to an existing configuration definition file or when a configuration definition file is optimized, the existing settings are used.

server.agent.rm.temporaryInstance

Specify the instance number of the configuration definition file that the Device Manager agent temporarily uses to acquire copy pair information.

Specify a value from 0 to 3997.

An instance number in the range *specified-value* to *specified-value* `+98` is used.

Default: `900`

server.agent.rm.temporaryPort

Specify the UDP port number of the configuration definition file that the Device Manager agent temporarily uses to acquire copy pair information.

Specify a value from 1 to 65437.

A UDP port number in the range *specified-value* to *specified-value* +98 is used.

Default: 53232

server.agent.rm.pairDefinitionForm

Specify which format should be used to specify pair volume information in the configuration definition file when creating a pair: HORCM_DEV format or HORCM_LDEV format.

If you want to unify the format into the HORCM_DEV format, specify HORCM_DEV. If you want to unify the format into the HORCM_LDEV format, specify HORCM_LDEV. We recommend that you use the HORCM_LDEV format.

Note that in the following cases, the HORCM_LDEV format is used to specify information in the configuration definition file, irrespective of the format specified in this property:

- If you create a copy pair for a mainframe volume
- If you create a copy pair by using a volume in a virtual storage machine on VSP G1000, G1500, VSP F1500, VSP Gx00 models, or VSP Fx00 models
- If you create a global-active device copy pair on VSP G1000, G1500, VSP F1500, VSP Gx00 models, or VSP Fx00 models

Default: HORCM_LDEV

The Device Manager agent decides which format should be used in the configuration definition file when creating a pair according to the following conditions:

- Which format is used in the existing configuration definition file: HORCM_DEV format or HORCM_LDEV format.
- A pair is created for a new copy group or existing copy group.

The following table describes the conditions under which the Device Manager agent decides whether to use the HORCM_DEV or HORCM_LDEV format in the configuration definition file.

Table 120 Conditions on which the Device Manager agent decides which format should be used in the configuration definition file

Which format is used in the existing configuration definition file	Pair operation	Format to be used in the configuration definition file
No format is used.	Creating a pair for a new copy group.	**If a format is specified in the property:** The format specified in the property

Which format is used in the existing configuration definition file	Pair operation	Format to be used in the configuration definition file
		If a format is not specified in the property: The format HORCM_DEV
HORCM_DEV format is used.	Adding a pair to an existing copy group.	HORCM_DEV format, regardless of the format specified in the property
	Creating a pair for a new copy group.	**If a format is specified in the property:** The format specified in the property **If a format is not specified in the property:** The format HORCM_DEV
HORCM_LDEV format is used.	Adding a pair to an existing copy group.	HORCM_LDEV format, regardless of the format specified in the property
	Creating a pair for a new copy group.	**If a format is specified in the property:** The format specified in the property **If a format is not specified in the property:** The format HORCM_LDEV
Both HORCM_DEV format and HORCM_LDEV format are used.	Adding a pair to an existing copy group that uses HORCM_DEV format.	HORCM_DEV format, regardless of the format specified in the property
	Adding a pair to an existing copy group that uses HORCM_LDEV format.	HORCM_LDEV format, regardless of the format specified in the property
	Adding a pair to an existing copy group that uses both HORCM_DEV format and HORCM_LDEV format.	**If a format is specified in the property:** The format specified in the property **If a format is not specified in the property:** The format HORCM_DEV

Which format is used in the existing configuration definition file	Pair operation	Format to be used in the configuration definition file
	Creating a pair for a new copy group.	**If a format is specified in the property:** The format specified in the property **If a format is not specified in the property:** The format `HORCM_DEV`

Caution: Before you specify `HORCM_LDEV`, make sure that CCI 01-17-03/04 (or later) has been installed. If you specify `HORCM_LDEV` when CCI is a version earlier than 01-17-03/04, volume pair creation will fail. If this happens, the following error message will be displayed:

`An attempt to create a pair has failed. Error detail, host "`*`host-name`*`" : "`*`error-detail`*`"`

server.agent.rm.userAuthentication

Specify whether to check that the authentication mode for command devices is enabled.

Specify `true` to check that the authentication mode for command devices is enabled. Specify `false` if you do not want to do so.

Default:`true`

Caution: If you specify `false`, make sure that no command devices whose authentication mode is enabled are connected to the host where the Device Manager agent is installed. If you specify `false` when the authentication mode for command devices is enabled, you cannot obtain the pair status or perform pair operations properly.

server.agent.rm.ignorePairStatus

Specify whether to omit copy pair information when sending host information from the Device Manager agent to the management server.

Specify `true` to omit copy pair information. Specify `false` if you do not want to omit the information.

In the following environments, make sure that you always specify `true`:

- Virtual machine for which a copy pair is assigned

- An SVP is used as a virtual command device to manage copy pairs defined as a device group.
  When P-VOLs and S-VOLs are assigned to the management server, this property must be specified.

Default: `false`

Note: When the Device Manager agent is installed on a virtual machine where a VMware Tools service or process is running, the value of the `server.agent.rm.ignorePairStatus` property will be changed to `true`.

server.agent.rm.horcmSource

If the CCI configuration definition file is stored in a location other than the default, use the absolute path to specify the storage location of the configuration definition file.

Specify the path according the following rules:

- In Windows, use a forward slash (`/`) as a path delimiter.
- In Windows, if a space is included in the path, you do not need to enclose the path with quotation marks (").
- Do not use symbolic links.

Default: None#

#: If you do not specify a path, the path for the following default storage location is used:

In Windows:

System folder (represented by the environment variable `%windir%`)

In UNIX:

`/etc` directory

Related tasks

- Changing the storage location of the configuration definition file on page 562

server.agent.rm.moduleTimeOut

Specify a timeout value for receiving command execution results when the Device Manager agent executes a CCI command (in seconds).

When a command takes longer to execute than the specified value, the Device Manager agent concludes that an error occurred during command execution.

This property should be changed only by a system administrator who has expert knowledge, when performance of the Device Manager agent's pair configuration functionality needs to be fine-tuned.

Default: `600` (seconds)

server.server.ssl.hdvm

Specify whether to use SSL to communicate between the Device Manager agent and the Device Manager server.

If SSL is used for communication, specify `true`. If SSL is not used for communication, specify `false`,

Default: `false`



Note: If `true` is specified and the execution environment for Java in Device Manager agent was changed, you need to download and install the Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files for the version of the Java execution environment to be used.

Download the Jurisdiction Policy files from the Website of Oracle corporation or IBM corporation. For details about how to install the files, see the documentation provided with the Jurisdiction Policy files.

server.http.server.timeOut

Specify a timeout value for receiving a response from the Device Manager server, for example, when registering host information by executing the `HiScan` command, restarting the service, refreshing the host (in seconds).

If no response is received from the Device Manager server within the specified time, the Device Manager agent concludes that an error has occurred and the `HiScan` command terminates abnormally.

Specify a value from 100 to 3,600. If the specified value is less than 100, the timeout is assumed to be 100. If the specified value is more than 3,600, the timeout is assumed to be 3,600.

Default: `600`

server.util.processTimeOut

Specify the Device Manager agent's normal execution time for external programs (in milliseconds).

If an external program takes longer than the specified time, the Device Manager agent concludes that an error has occurred and terminates the program. If you specify too short a time period, the Device Manager agent might stop execution of external programs that are running regularly. Do not edit this property without current knowledge of the Device Manager agent's performance.

Default: `600000`

server.agent.evtwait.timeout

Specify the waiting time until the status becomes PAIR when a remote pair is restored (in seconds).

If the specified time has elapsed, the processing ends with an error.

Specify a value from 1 to 1999999.

Default: `3600`

server.agent.snapshotEvtwait.timeout

Specify the waiting time (in seconds) until the status becomes PAIR when a Copy-on-Write Snapshot or Thin Image pair is created, resynced, or restored.

If the specified time has elapsed, the processing ends with an error.

Specify a value from 1 to 1999999.

Default: `3600`

Properties for command devices connected to Device Manager agent (rgcmddev.properties file)

If the storage system is VSP G1000, G1500, VSP F1500, VSP Gx00 models, VSP Fx00 models, Virtual Storage Platform, or HUS VM, and resources in the storage system are partitioned, in the `rgcmddev.properties` file, specify a command device whose storage system resource group ID is 0. (For VSP G1000, G1500, VSP F1500, VSP Gx00 models, or VSP Fx00 models, specify the command device of the resource pools of the default virtual storage machine.)

- In Windows:
  installation-folder-for-Device-Manager-agent`\mod\hdvm\config\rgcmddev.properties`
- In Linux:
  installation-directory-for-Device-Manager-agent`/mod/hdvm/config/rgcmddev.properties`
- In Solaris or HP-UX:
  `/opt/HDVM/HBaseAgent/mod/hdvm/config/rgcmddev.properties`
- In AIX:
  `/usr/HDVM/HBaseAgent/mod/hdvm/config/rgcmddev.properties`

Define the command device in the following format. If you define multiple command devices whose resource group ID is 0 (the resource pool of the default virtual storage machine for VSP G1000, G1500, VSP F1500, VSP Gx00 models, or VSP Fx00 models) in the same system, only the command device defined in the last line becomes valid.

RAID-ID.serial-number.LDEV-number

RAID-ID

Specify the storage system in the following format:

- `R800` for VSP G1000, G1500 or VSP F1500
- `HM82` for VSP G200
- `HM84` for VSP G400, VSP G600, VSP F400 or VSP F600
- `HM86` for VSP G800 or VSP F800
- `R700` for Virtual Storage Platform
- `HM70` for HUS VM

serial-number

Specify the serial number of the storage system by using a decimal (base 10) number. For VSP G1000, G1500, VSP F1500 or Virtual Storage Platform, specify a 5-digit number. For VSP Gx00 models, VSP Fx00 models or HUS VM, specify a 6-digit number including the model name.

LDEV-number

Specify the CU:LDEV number of the command device by using a hexadecimal number. Specify a command device whose storage system resource group ID is 0. (For VSP G1000, G1500, VSP F1500, VSP Gx00 models, or VSP Fx00 models, specify the command device of the resource pools of the default virtual storage machine.)

If multiple command devices in the same system are connected to the pair management server, in the configuration definition file, you can specify multiple command devices in the same line for the `HORCM_CMD` parameter. If you specify multiple command devices in the same line, CCI uses the first specified command device.

Because the Device Manager agent can perform operations on all resources within the system, the command device of a storage system whose resource group ID is 0 (in the case of VSP G1000, G1500, VSP F1500, VSP Gx00 models, or VSP Fx00 models, this is the resource pool of the default virtual storage machine) must be used. Therefore, if the pair management server recognizes multiple command devices, the Device Manager agent sorts the command devices so that devices whose LDEV numbers are specified in the file `rgcmddev.properties` are listed first in the specification of the `HORCM_CMD` parameter.

Example:

Below is an example when the command devices PhysicalDrive1 (LDEV number: 00:01) and PhysicalDrive2 (LDEV number: 00:02) for VSP G1000 (serial number: 310051) are recognized by the pair management server.

Normally, based on the physical drive number and the device file name, the HORCM_CMD parameter is defined as follows:

```
HORCM_CMD
#dev_name                dev_name                dev_name
#UnitID 0 (LDEV# 00:01 00:02 Serial# 310051)
\\.\PhysicalDrive1  \\.\PhysicalDrive2
```

However, if R800.310051.00:02 is specified in the file rgcmddev.properties, the command device whose LDEV number is 00:02 is defined first in the specification of the HORCM_CMD parameter.

```
HORCM_CMD
#dev_name                dev_name                dev_name
#UnitID 0 (LDEV# 00:02 00:01 Serial# 310051)
\\.\PhysicalDrive2  \\.\PhysicalDrive1
```

Security settings for management clients

This section describes the security settings for management clients.

- About Login warning banners
- Controlling management client access to the management server

About Login warning banners

A warning banner is a field for security messages displayed in the Login window of Hitachi Command Suite products.

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

Conditions that apply when displaying warning banner messages

When you use the `hcmds64banner` command to register a message to be displayed on a warning banner, there are restrictions on the number of characters and character codes.

- Use HTML tags to create a message. In addition to the usual characters, you can use HTML tags to change font attributes or place line breaks in desired locations.
  The following conditions apply to the use of HTML tags:
  - To use line breaks in a desired location, use the HTML tag `<BR>`.
  - To display a character used in HTML syntax (for example, `< > " ' &`), use the HTML escape sequence. For example, to display an ampersand (&) in the Login window, write `&` in the HTML file.
- No more than 1,000 characters can be used. (HTML tag characters are also counted in the number of characters.)
- Usable characters are from the Unicode UTF-8 encoding.

Creating and registering a message displayed on a warning banner

Use a text editor to create a message displayed on a warning banner for Hitachi Command Suite programs, and execute the `hcmds64banner` command to register it.

Before you begin

Log in as a user with Administrator permissions (for Windows) or as a root user (for Linux).

Procedure

1. Use a text editor to create a message.

   Sample messages in English (`bannermsg.txt`) and Japanese (`bannermsg_ja.txt`) are provided in the following locations: In Windows:
   - In Windows:
     installation-folder-for-Hitachi-Command-Suite`\Base64\sample\resource`
   - In Linux:

installation-directory-for-Hitachi-Command-Suite/Base64/sample/resource

These sample files are overwritten at installation so, if you wish to use a sample file, copy it and then edit it.

The following shows the default 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.
```

2. Execute the `hcmds64banner` command to register the message:
   - In Windows:
     installation-folder-for-Hitachi-Command-Suite\Base64\bin\hcmds64banner /add /file *file-name* [/locale *locale-name*]
   - In Linux:
     installation-directory-for-Hitachi-Command-Suite/Base64/bin/hcmds64banner -add -file *file-name* [-locale *locale-name*]

file-name

Using an absolute path, specify the file that stores the message. In Linux, do not specify a path that includes a space.

locale-name

Specify the locale of the language used for the message (for example, `en` for English, or `ja` for Japanese). If this setting is omitted, the registered message will always be displayed in the warning banner regardless of the locale (the message is registered as a message of the default locale).

When the GUI is used in multiple locales, if you register a message with the same contents in a different language for each locale, the message can be automatically switched to match the locale of the web browser.

When multiple languages are specified on one web browser, the locale of the warning banner is determined by the language priority settings of the web browser.

Note: If you execute the `hcmds64banner` command and a message for the specified locale is already registered, it will be updated by being overwritten.

Tip: You can also use the GUI to perform the following operations:

- Registering a message without the locale specified
- Editing a message that has been registered by the `hcmds64banner` command with the `locale` option omitted

When you use the GUI to perform operations, the following restrictions apply:

- Available HTML tags are limited.
- If the system is in a cluster configuration, the message is registered only to the executing node. To register the message to the standby node, switch the nodes, and then perform the same operations.

Result

The message is registered in the management server and displayed in the Login window of Hitachi Command Suite products.

Deleting a message from the warning banner

Execute the `hcmds64banner` command to delete a message displayed in the warning banner of Hitachi Command Suite products.

Before you begin

- Log in as a user with Administrator permissions (for Windows) or as a root user (for Linux).
- Check the following information:
  - The locale of the message to be deleted (`en` for English or `ja` for Japanese).

Procedure

Execute the `hcmds64banner` command:

- In Windows:

installation-folder-for-Hitachi-Command-Suite\Base64\bin\hcmds64banner /delete [/locale *locale-name*]

- In Linux:
  installation-directory-for-Hitachi-Command-Suite/Base64/bin/hcmds64banner -delete [-locale *locale-name*]

locale-name

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

Tip: You can also use the GUI to delete the following messages:
- A message registered from the GUI
- A message registered by the hcmds64banner command with the locale option omitted

If the system is in a cluster configuration, operations from the GUI are applied only to the executing node. To apply the operation to the standby node, switch the nodes and then perform the same operations.

Controlling management client access to the management server

In Hitachi Command Suite products, you can control which management clients can access the management server through the GUI or CLI. To restrict the management clients that can access the management server, edit the user_httpsd.conf file and the properties file for the Device Manager server.

Before you begin

Check the following information:
- Information about the management clients that can access the management server
  Use either of the following formats to specify the management clients that can access the management server:
  - The domain name (example: hitachi.datasystem.com)
  - Part of the domain name (example: hitachi)
  - The IPv4 or IPv6 address (example: 10.1.2.3 127.0.0.1 2001::123:4567:89ab:cdef)
  - Part of the IPv4 address (example: 10.1 which, in this case, means 10.1.0.0/16)

- IPv4 Network/Netmask format (dot notation) (example: `10.1.0.0/255.255.0.0`)
- IPv4 or IPv6 Network/*c* (CIDR notation: *c* is a decimal integer that indicates the number of bits for identifying a network) (example: `10.1.0.0/16 2001:0:0:1230::/64`)

Procedure

1. Stop the services of Hitachi Command Suite product.
2. Add information about the management clients that can access the management server to the last line of the `user_httpsd.conf` file.

   Location of the `user_httpsd.conf` file
   - In Windows:
     installation-folder-for-Hitachi-Command-Suite\Base64\uCPSB\httpsd\conf\user_httpsd.conf
   - In Linux:
     installation-directory-for-Hitachi-Command-Suite/Base64/uCPSB/httpsd/conf/user_httpsd.conf

   Format for specifying clients in the `user_httpsd.conf` file

   ```
   <Location /DeviceManagerWebService>
           order allow,deny
           allow from management-client [management-client...]
   </Location>
   ```

   - Be sure to specify `order` in accordance with the specified format. If extra spaces or tabs are inserted, operation will fail.
   - Multiple lines can be used to specify hosts for `allow from`.
   - If you want to specify multiple management clients in a command line for `allow from`, delimit the hosts with a space.
   - If the GUI or CLI of Hitachi Command Suite products is used on the management server, you must also specify the local loopback address (`127.0.0.1` or `localhost`).

   Example of adding information to the `user_httpsd.conf` file

   ```
   <Location /DeviceManagerWebService>
           order allow,deny
           allow from 127.0.0.1 10.0.0.1
   2001::123:4567:89ab:cdef
           allow from 10.1.0.0/16 2001:0:0:1230::/64
   </Location>
   ```

3. Add information about the management clients to the `server.http.security.clientIP` property or the `server.http.security.clientIPv6` property in the `server.properties` file for the Device Manager server.
4. Start the services of Hitachi Command Suite product.

Caution: If you log on to a Hitachi Command Suite product from a management client that is not registered in the `user_httpsd.conf` file, the GUI cannot be started from that Hitachi Command Suite product.

Related tasks

- Starting the Hitachi Command Suite services on page 458
- Stopping the Hitachi Command Suite services on page 460

Related references

- server.http.security.clientIP on page 616
- server.http.security.clientIPv6 on page 617

F

Migrating copy pair definitions

This section describes how to migrate the copy pair definitions managed in configuration definition files to device group definitions on storage systems.

- About migrating of copy pair definitions
- Prerequisites for migrating copy pair definitions
- Migrating copy pair definitions to device group definitions
- Properties used by the pair definition migration command

About migrating of copy pair definitions

Migrate the copy pair definitions managed in configuration definition files to device group definitions on storage systems.

When copy pairs are managed by using configuration definition files, if the information in a configuration definition file on the pair management server is lost or the pair management server becomes unavailable, you might no longer be able to manage those copy pairs. To prevent this from happening, you can centrally manage both copy pairs themselves and copy pair definitions on storage systems, instead of defining copy pairs in configuration definition files. By using device groups to define copy pairs, you can retain copy pair definitions on storage systems.

If a user who uses Device Manager, Replication Manager, or CCI wants to use the Configuration Manager REST API function for managing copy pairs by using device groups, copy pair definitions must be migrated to device group definitions.

To migrate copy pair definitions to device group definitions, execute the pair definition migration command (`PairCfgMigration`) on the pair management server storing the configuration definition files. When you execute the pair definition migration command, copy pair information will be obtained from the configuration definition files on the migration source, and device groups and copy groups will be created on the applicable storage systems.

To perform operations on a copy group whose copy pair definition has been migrated to a device group definition, you can use the function for creating a configuration definition file that contains `HORCM_LDEVG`. (Optional)

The following figure shows an example of a system configuration before and after pair definitions are migrated.

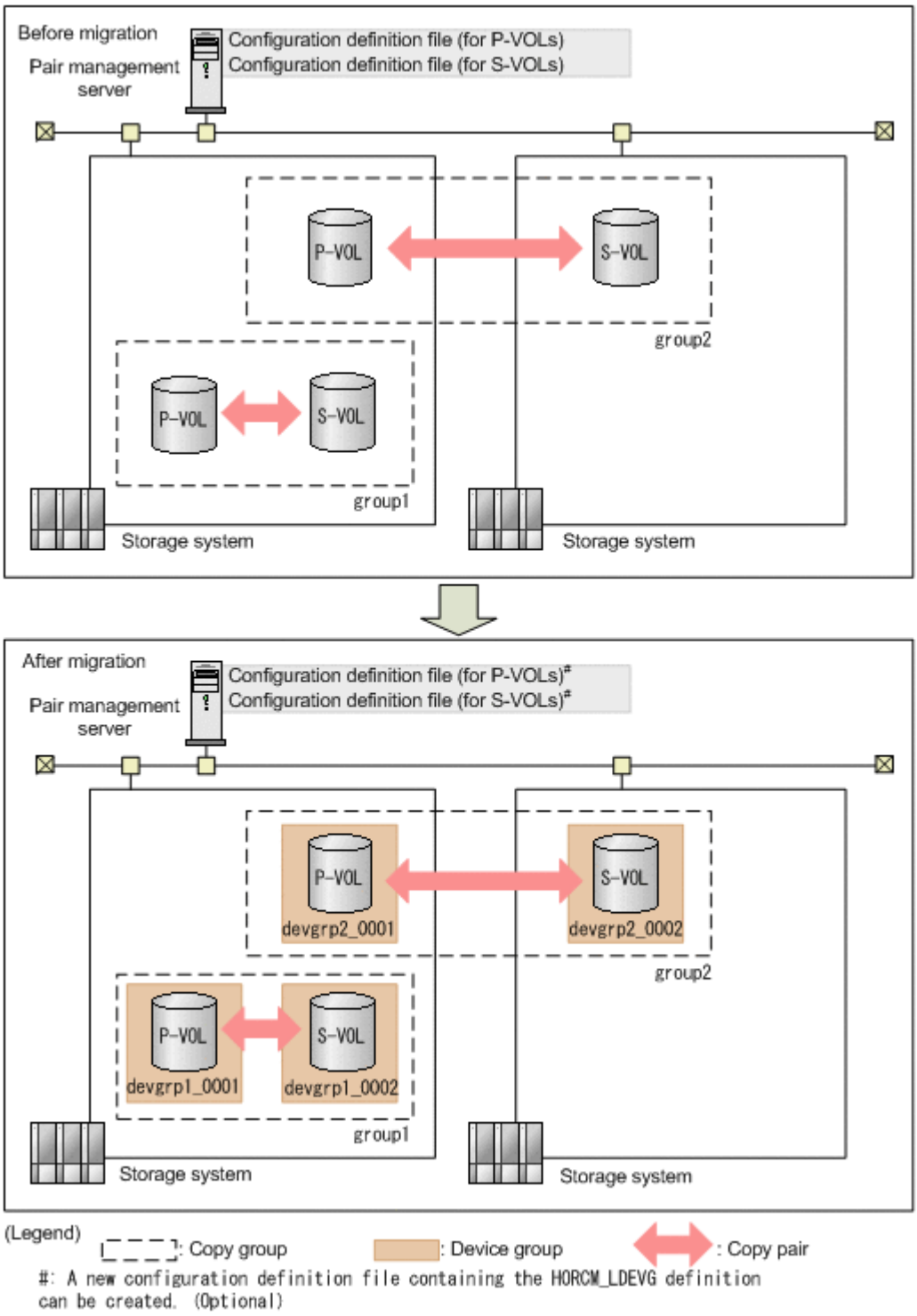


Figure 63 Example of a system configuration before and after pair definitions are migrated

Device group names are set based on the prefix that was specified when the pair definition migration command was executed. The copy group names that

were defined in the configuration definition files before migration will continue to be used after migration.

The following table describes the configuration after migration.

Table 121 Configuration after copy pair definitions are migrated to device group definitions

Type of copy pair for which definitions are to be migrated	Configuration after migration
ShadowImage	**Device group** If both the configuration definition file for P-VOLs and the configuration definition file for S-VOLs exist on the target pair management server, one device group will be created for each P-VOL and each S-VOL. If only the configuration definition file for P-VOLs exists on the target pair management server, one device group for the P-VOL, and one device group for S-VOL will be created. You do not need to execute the pair definition migration command on another pair management server storing the configuration definition file for S-VOLs. **Copy group** One copy group will be created for each copy group definition.
TrueCopy Universal Replicator High Availability Manager global-active device	**Device group** If both the configuration definition file for P-VOLs and the configuration definition file for S-VOLs exist on the target pair management server (server on which the pair definition migration command is executed), one device group for the P-VOL will be created on the primary storage system, and one device group for the S-VOL will be created on the secondary storage system. If only the configuration definition file for P-VOLs (or S-VOLs) exists on the target pair management server, one device group for the P-VOL (or S-VOL) will be created on the primary storage system (or secondary storage system). Execute the pair definition migration command on the pair management server storing the configuration definition file for S-VOLs (or P-VOLs). **Copy group** For each copy group definition, one copy group for the P-VOL will be created on the primary storage system, and one copy group for the S-VOL will be created on the secondary storage system.

Caution: When migrating copy pair definitions to device group definitions, note the following:

- In Replication Manager, you can perform operations on or view copy pairs by using the configuration definition file that uses device groups and was

re-created for a device group when the pair definition migration command was executed. However, you will no longer be able to create copy pairs.
- You will no longer be able to manage copy pairs by using the Replication tab or the Device Manager CLI.

Prerequisites for migrating copy pair definitions

This section describes the prerequisites for migrating copy pair definitions.

Storage system:

The following storage systems support the use of device groups:
- VSP G1000
- VSP G1500
- VSP F1500
- VSP Gx00 models
- VSP Fx00 models
- Virtual Storage Platform
- HUS VM

Pair management server:

The pair management server must satisfy the following conditions:
- A JDK or JRE (1.5.0_22 or later) must be installed on the pair management server on which the pair definition migration command is to be executed.
  The installation destination of the Java execution environment must be specified in the PATH environment variable or the `paircfgmigration.properties` file.
- CCI must be installed on the pair management server on which the pair definition migration command is to be executed.
  For VSP G1000, G1500, VSP F1500, VSP Gx00 models, or VSP Fx00 models, CCI 01-32-03/01 or later must be installed.

Types of copy pairs to be migrated

The following types of copy pairs can be migrated:
- ShadowImage
- TrueCopy
- Universal Replicator
- High Availability Manager
- global-active device

Copy pair definitions of Copy-on-Write Snapshot or Thin Image copy pairs cannot be migrated to device group definitions.

Configuration definition files to be migrated

Configuration definition files to be migrated must satisfy the following conditions:

- The configuration definition file must be stored in the directory specified in the `paircfgmigration.horcmFilePath` property of the `paircfgmigration.properties` file.
- The name of a configuration definition file must be `horcm`*XX*`.conf`.
  The instance number *XX* must be in the range from 0 to 4094. Files whose names contain an instance number starting with 0 (such as 01 or 001) will not be migrated.
- The file must contain configuration definition information, including a copy pair definition (`HORCM_LDEV` or `HORCM_DEV`).
- The CCI instance must be able to be started.
- The copy pair defined in the configuration definition file must have already been created.
- For a configuration definition file that defines ShadowImage copy pairs, a configuration definition file for P-VOLs must exist.
- For a configuration definition file that defines ShadowImage copy pairs, definitions of P-VOLs and S-VOLs must not exist in the same configuration definition file.
- MU numbers must be unique in each copy group.
- For the MU number 0, `MU#` must be specified in the configuration definition file as follows:
  For ShadowImage: `0`
  For TrueCopy, Universal Replicator, High Availability Manager, or global-active device: Not specified
- Journal IDs must be unique in each copy group.
- Copy pair definitions must be defined using physical IDs.
- The configuration definition file must not contain a `HORCM_VCMD` definition.

Migrating copy pair definitions to device group definitions

To migrate copy pair definitions to device group definitions, execute the pair definition migration command (`PairCfgMigration`).

Before you begin

- The authentication mode for the command device is enabled.
- Log in as a user with Administrator permissions (for Windows) or as a root user (for UNIX).
- User authentication for the applicable storage system must have been performed.
  If the OS of the pair management server is Windows, user authentication must have been performed for the user who will execute the pair definition

migration command. Furthermore, this user must have been assigned the Storage Administrator (Provisioning) role.
- The CCI instance of the configuration definition files to be migrated must not be running.

Procedure

1. Obtain the archive file of the pair definition migration command from the integrated installation media, and then decompress the file in a location of your choice on the pair management server.

   The archive file is stored in the following locations:

   In Windows:

   DVD-ROM-drive\AGENTS\MigCmd\Windows\PairCfgMigration.zip

   In UNIX:

   DVD-ROM-mount-directory/AGENTS/MigCmd/Unix/PairCfgMigration.tar

2. Specify, in the properties file (paircfgmigration.properties), the storage location of configuration definition files, the prefix to be used for device group names, and other properties.

   The properties file is stored in the following locations:

   In Windows:

   archive-file-decompression-folder\PairCfgMigration\paircfgmigration.properties

   In UNIX:

   archive-file-decompression-directory/PairCfgMigration/paircfgmigration.properties

3. Execute the following command to migrate copy pair definitions.

   In Windows:

   archive-file-decompression-folder\PairCfgMigration\PairCfgMigration.bat [/s]

   In UNIX:

   archive-file-decompression-directory/PairCfgMigration/PairCfgMigration.sh [-s]

   Options

   s

   Executes the command without requiring user response.

   If you execute the command without specifying the s option, you can display a list of the configuration definition files to be migrated and execute migration processing in an interactive format.

Note: Make sure that, while the pair definition migration command is running, other users do not lock any storage system resource on which operations will be performed.

Tip: If a failure occurs while a copy pair definition is being migrated, obtain the following log files.

Log file for the pair definition migration command

archive-file-decompression-directory/PairCfgMigration/log

Log file for CCI

CCI-installation-destination/HORCM/log*XX*

Configuration definition file

horcm*XX*.conf at the location where the configuration destination file is placed

XX is an instance number.

Related references

- Properties used by the pair definition migration command on page 710

Properties used by the pair definition migration command

Specify, in the properties file (paircfgmigration.properties), the storage locations of the configuration definition files to be migrated, the prefix to be used for device group names, and other properties.

The following table describes the properties to be specified in the paircfgmigration.properties file.

Table 122 Properties to be specified in the paircfgmigration.properties file

Property name	Description
paircfgmigration.horcmFilePath	Specify the absolute path of the directory containing the configuration definition files to be migrated. When specifying this property, use only single-byte alphanumeric characters. In Windows, use a forward slash (/) as the path delimiter. If you omit this property, one of the following storage locations will be set: **In Windows:**

Property name	Description
	System folder (represented by the environment variable `%windir%`) **In UNIX:** `/etc` directory Default: None
`paircfgmigration.ignoreInstanceNumber`	Of the configuration definition files in the directory specified for the `paircfgmigration.horcmFilePath` property, specify the instance numbers of any configuration definition files to be excluded from migration. When specifying this property, use only single-byte alphanumeric characters. To specify multiple instance numbers, delimit the numbers by using commas (,). For example, if you are executing the pair definition migration command multiple times in a row, you can specify to exclude configuration definition files for which pair definitions have already been migrated. A list of the instance numbers of configuration definition files that have been successfully migrated will be output to the log file of the pair definition migration command. You can specify these numbers by copying them from the log file to this property. Example: `paircfgmigration.ignoreInstanceNumber=101,102,103` The configuration definition files specified in this property will not appear in the list of configuration definition files that is displayed when the pair definition migration command is executed in an interactive format. If you omit this property, all configuration definition files will be migrated. Default: None
`paircfgmigration.rm.location`	Specify the absolute path of the drive or directory in which CCI is installed. When specifying this property, use only single-byte alphanumeric characters. For Windows, use a forward slash (/) as the path delimiter. If you omit this property, the following drive or directory will be set: **In Windows:** *drive-where-the-PairCfgMigration-command-is-stored*/HORCM **In UNIX:** /HORCM

Property name	Description
	Default: None
paircfgmigration.deviceGroupPrefix	Specify the prefix to be used in the names of the device groups to be created. The prefix must consist of 26 or fewer characters. You cannot specify a character string that starts with a hyphen (-). You can use the following characters: A to Z a to z 0 to 9 . @ _ : , - Device group names are created in the following format: *prefix*_*xxxx* (where *xxxx* is a four-digit number between 0001 and 9999). If you omit this property, the prefix devgrp will be set. Default: None
paircfgmigration.updateHorcmFile	Specify whether configuration definition files for the newly created device groups are to be re-created after all pair definition information in the configuration definition files on the migration source has been migrated. **disable** Do not re-create configuration definition files for device groups. **enable** Re-create configuration definition files for device groups. Configuration definition files will be re-created by replacing the HORCM_DEV and HORCM_LDEV definitions in the configuration definition files on the migration source with HORCM_LDEVG definitions. Other definitions will remain unchanged. The names of migrated configuration definition files will be the same as the names of the configuration definition files on the migration source. The extension .old will be added to migrated configuration definition files. Default: disable
paircfgmigration.java.location	Specify the absolute path of the installation destination of a program that provides a Java execution environment. When specifying this property, use only single-byte alphanumeric characters. In Windows, use a forward slash (/) as the path delimiter.

Property name	Description
	If you omit this property, the Java execution environment installation destination that is specified in the PATH environment variable will be set. Default: None

Glossary

A

AES

Advanced Encryption Standard

API

Application Program Interfaces

ASCII

American Standard Code for Information Interchange

C

CHA

Channel Adapter

CHAP

Challenge Handshake Authentication Protocol

CIDR

Classless Inter-Domain Routing

CIM

Common Information Model

CIMOM

CIM Object Manager

CLI

Command Line Interface

CLPR

Cache Logical PaRtition

CN

Common Name

CPU

Central Processing Unit

CSR

Certificate Signing Request

CSV

Comma Separated Value

CU

Control Unit

CVS

Custom Volume Size

D

DBMS

DataBase Management System

DCR

Dynamic Cache Residency

DER

Distinguished Encoding Rules

DKC

DisK Controller

DM-LU

Differential Management LU

DMP

Dynamic MultiPathing

DMTF

Distributed Management Task Force

DN

Distinguished Name

DNS

Domain Name System

DoS

Denial of Services

E

EVS

Enterprise Virtual Server

F

FQDN

Fully Qualified Domain Name

FTP

File Transfer Protocol

G

GUI

Graphical User Interface

H

HBA

Host Bus Adapter

HTTP

HyperText Transfer Protocol

HTTPS

HyperText Transfer Protocol Secure

I

I/O

Input/Output

ID

IDentifier

IETF

Internet Engineering Task Force

IOPS

Input Output Per Second

IP

Internet Protocol

IP-SAN

Internet Protocol Storage Area Network

IPF

Itanium® Processor Family

IPv4

Internet Protocol Version 4

IPv6

Internet Protocol Version 6

iSCSI

Internet Small Computer System Interface

J

JAR

Java ARchiver

L

LAN

local-area network

LBA

Logical Block Addressing

LDAP

Lightweight Directory Access Protocol

LDEV

logical device

LDKC

Logical DisK Controller

LU

Logical Unit

LUN

Logical unit number

LUSE

Logical Unit Size Expansion

M

MCU

Main Control Unit

MOF

Managed Object Format

MU

Multiple Unit

N

NAS

Network Attached Storage

NAT

Network Address Translation

NIC

Network Interface Card

NPIV

N Port ID Virtualization

NTP

Network Time Protocol

O

OS

Operating System

P

P-VOL

Primary VOLume

PAP

Password Authentication Protocol

PDEV

Physical Device

PEM

Privacy Enhanced Mail

PID

Process ID

PNG

Portable Network Graphics

PP

Program Product

R

RADIUS

Remote Authentication Dial-In User Service

RAID

Redundant Array of Independent Disks

RCU

Remote Control Unit

RDN

Relative Distinguished Name

RFC

Request For Comments

RMI

Remote Method Invocation

S

S-VOL

Secondary VOLume

SAN

Storage Area Network

SCSI

Small Computer System Interface

SED

Stack Execution Disable

SIM

Service Information Message

SLP

Service Location Protocol

SLPR

Storage Logical PaRtition

SMI-S

Storage Management Initiative - Specification

SMTP

Simple Mail Transfer Protocol

SNIA

Storage Networking Industry Association

SNIA-CTP

SNIA Conformance Testing Program

SNMP

Simple network management Protocol

SP

Service Pack

SRV

SeRVice

SSH

Secure SHell

SSID

Storage Subsystem ID

SSL

Secure Sockets Layer

SSO

Single Sign - On

SVP

Service Processor

T

TCP

Transmission Control Protocol

TLS

Transport Layer Security

U

UDP

User Datagram Protocol

URL

Uniform Resource Locator

V

V-VOL

Virtual VOLume

W

WAN

Wide Area Network

WBEM

Web - Based Enterprise Management

WWN

Worldwide name

X

XML

eXtensible Markup Language

Index

Symbols
.truststore 250

A
account
conditions 172
acquiring
maintenance information on management server 578
agent.logger.loglevel 674
agent.logger.MaxBackupIndex 674
agent.logger.MaxFileSize 674
agent.properties file 671
agent.rm.everytimeShutdown 671
agent.rm.horcmInstance 672
agent.rm.horcmRange 673
agent.rm.horcmService 673
agent.rm.shutdownWait 672
agent.rm.TimeOut 671
agent.util.hpux.displayDsf 675
alerts 405
SNMP traps 407
applying
certificate authority for Common Component server certificate 257
certificate authority for Device Manager server certificate 271
certificate authority for Host Data Collector server certificate 286
authorization group 166
Automation Director 60

B
backing up
database 470
BaseDN 173
bridge
network settings 143

C
C/T Delta
analyzing 354
central management method 684
certificate
checking 301, 305
checking for Host Data Collector 306
deleting 302
importing into Common Component 298
importing into Device Manager server 303
importing into Device Manager server truststore 278
importing into Host Data Collector 305
importing into web browser 291, 292
certificate signing request
creating for Common Component 253
creating for Device Manager server 270
creating for Host Data Collector 284
checking connections
external authentication server 212
external authorization server 212
CIM/WBEM 436
enabling 439
user account settings 439
cimxmlcpa.properties 638
cimxmlscpa.properties 616, 638
Ciphers 620
client certificate
exporting for CIM client 328
exporting for event indications 322
importing for object operations 319
importing into CIM client 329
client.launch.em.secure 615
client.properties 614
client.rmi.port 615
com.wbemsolutions.jserver.bindto 638
Common Component
log output 404
ports 106
communication protocol
changing between Replication Manager server and Device Manager server 303
Compute Systems Manager 60
condition
message (warning banner) 696

conditions
account 172
LDAP search user account 206
config.xml file 353
configforclient.xml file 353
configuration definition file
changing storage location 562
description conventions 547
editing 545
notes 562
prerequisite environment 545
supported parameter 547
configuring
networks 33
configuring instance environment 360
connecting
notes and requirements for Storage Navigator Modular 2 332
copy pair
prerequisite version of Device Manager agent 85
storage system requirements 84
copy pair definition
migrating 704
copy pairs
managing (Device Manager agent) 521
system requirements 62
virtual command device server method 67
creating a truststore file
Device Manager CLI 289
customizedsnmptrap.customizedSNMPTrapEnable 621
customizedsnmptrap.customizelist 621
customizedsnmptrap.properties 620

D

database
backing up 470
exporting 494, 495, 497
importing 499, 503, 506
migrating 491
database.properties file 602, 648
dbm.startingCheck.retryCount 603
dbm.startingCheck.retryPeriod 603
dbm.traceSQL 603, 648
device group
migrating 708
Device Manager
IPv6 environments 145
Device Manager agent 29
acquiring maintenance information (host) 584
environment settings 517
firewall 519
ports 111
prerequisite version 85
property files 670
reinstalling after host OS upgrade 516
resident process 528
Device Manager agent service
checking operating status 528
starting 528
stopping 528
Device Manager CLI 29
enabling SSL/TLS 294
Device Manager server 29
enabling SSL/TLS 269
ports 107
property files 589
devicemanager.properties file 649
dispatcher.properties 606
downloading
Device Manager server truststore file 288
Tiered Storage Manager server truststore file 295
dvmcacerts 250
Dynamic Link Manager 60

E

Element Manager
deleting settings for using 335
settings 333
email alerts
customizing templates 416
receiving 412
setting up recipients 413
setting up SMTP server 413
email notification
customizing templates (events) 423
events 420, 425
enabling
SSL/TLS for Device Manager server 269
two-way authentication for event indications 323
two-way authentication for object operations 317
enabling SSL/TLS
Device Manager CLI computer 294
Tiered Storage Manager CLI computer 296
encryption types
Kerberos authentication 216
environment settings
Device Manager agent 517
event notification
customizing template 430
customizing templates 423
setting properties 421, 427
specifying SMTP user authentication information 422, 428
exauth.properties file
Kerberos server 198
LDAP directory server 180
RADIUS server 189
exception registration
Host Data Collector service 141, 142
exporting
client certificate for a CIM client 328

client certificate for event indications 322
databases 494, 495, 497
Device Manager server self-signed certificate 290
server certificate for a CIM client 328
server certificate for object operations 317
external authentication server 166
checking connections 212
registering 178
external authorization server 166
checking connections 212
registering 178

F

file servers 40
firewall
Device Manager agent 519
Host Data Collector 141
registering exceptions 121
registering exceptions in Linux 121
registering exceptions in Windows 121
settings 121
flat model 174

G

Global Link Manager 60
global-active device 93
GUI 29

H

hbsa_modinfo command 530
hbsa_util command 532
hbsasrv command 528
hcmds64banner command 696, 698
hcmds64getlogs command 578
hcmds64unlockaccount command 162
hdc.adapter.adapterProcessNum 659
hdc.adapter.esx.timeout 663
hdc.adapter.localport 659
hdc.classloader 627
hdc.common.http.serverPort 660
hdc.common.https.serverPort 662
hdc.common.rmi.registryPort 659
hdc.common.rmi.serverPort 660
hdc.common.rmi.ssl.registryPort 661
hdc.common.rmi.ssl.serverPort 661
hdc.request.timeout 625
hdc.rmiregistry 626
hdc.rmiserver 626
hdc.service.fileCleanup.startTime 663
hdc.service.localport 659
hdc.service.rmi.registryIPAddress 662
hdc.ssl.ciphers 667
hdc.ssl.esx.certCheck 664
hdc.ssl.esx.enabledTLSv1 668
hdc.ssl.secure 663
hdc.usessl 628
hdcbase.properties 667
hdcbase.properties file 658
Host Data Collector 667
hdccacerts 250
hdvm_info command 533
hdvm.analytics.disabled 632
hdvm.analytics.healthcheck.notification.exportre port.locale 633
hdvm.analytics.report.pdf.showLogo 632
hdvm.port 649
hdvm.protocol 649
hdvm.replication.disabled 637
hdvm.rmi.port 649
hdvm.timeout 649
hdvmagt_setting command 533
hdvmcacerts 250
hdvmmodmailuser command 415, 422
hdvmmodpolluser command 449
hdvmsnmpuser 409
hierarchical structure model 173
HiScan command 537
Hitachi Command Suite common trace log setting up 404
Hitachi Command Suite for VVols 370
virtual appliance 373
Hitachi File Services Manager 60
Hitachi Storage Services Manager 60
launching 400
hldutil command 539
hldutil.properties file 675
HORCM_CMD 550
HORCM_DEV 553
HORCM_INST 558
HORCM_INSTP 560
HORCM_LDEV 556
HORCM_MON 548
HORCM_VCMD 552
host 29
that can be managed by Device Manager 40
Host Data Collector 29
acquiring maintenance information 582, 583
firewall 141
acquiring maintenance information 582, 583
ports 109
property files 658
resident process 462
Host Data Collector service
checking operating status 465
exception registration 141, 142
starting 464
stopping 464
host management software 40
host.agent.access.timeoutForRpm 625
host.mf.agent.connection.timeout 625
host.properties file 624
hostdatacollectors.properties 625
htmsetup command 352
in cluster environment 349, 351

in non-cluster environment 348
htnm.flashMode 632
htnm.infoAcquirePeriod 630
htnm.server.n.host 631
htnm.server.n.port 632
htnm.server.n.protocol 631
htnm.servers 631
HtsmgetTI.properties file 581
htsmmodmailuser command 428
HTTPPort 639
HTTPSPort 639

I

importing
certificate into Common Component 298
certificate into Device Manager server 303
certificate into Device Manager server truststore 278
certificate into Host Data Collector 305
certificate into web browser 291, 292
client certificate into CIM client 329
databases 499, 503, 506
Host Data Collector server certificate into keystore 287
server certificate for event indications 324
server certificate for object operations 319
server certificate into CIM client 329
server certificate into Device Manager agent 308
server certificate into Device Manager server keystore 273
indtruststore 250
IPv6
global address 145
global-unique local address 145
link-local address 145
linking with storage systems that support IPv6 147
migrating Device Manager server 145
site-local address 145

J

Java
changing (Device Manager agent) 517
changing (Host Data Collector) 39
javaconfig.properties file 666
javapath_setup command 517
javapathlocation 667
JDK
changing 37
jserver.properties 638
jssecacerts 250

K

Kerberos authentication
encryption types 216
Kerberos server
exauth.properties file 198
key pair
changing password of Device Manager server 277
creating for CIM client 327
creating for Device Manager server 266
creating for Host Data Collector 284
deleting from Device Manager server keystore 276
viewing in normal mode (Device Manager server) 274
viewing in verbose mode (Device Manager server) 275
keystore
changing password of Device Manager server 278
Importing a Host Data Collector server certificate 287
keystore file
creating for event indications 319
creating for object operations 314

L

launchapp.elementmanager.role.mode 624
launchapp.elementmanager.usehostname 624
launchapp.properties 623
launchapp.snm2.rmi.port 623
launchapp.snm2.url 623
launching
Hitachi Storage Services Manager 400
LDAP directory server
condition for server certificate 300
exauth.properties file 180
LDAP search user
registering 207
LDAP search user account 205
checking 210
conditions 206
deleting 209
ldapcacerts 250
Linux
registering firewall exceptions 121
locking
System account 162
unlocking accounts 162
user accounts 161
logger.guiMessageFileCount 653
logger.guiMessageMaxFileSize 654
logger.guiTraceFileCount 653
logger.guiTraceMaxFileSize 654
logger.hicommandbase.loglevel 605
logger.hicommandbase.MaxBackupIndex 605
logger.hicommandbase.MaxFileSize 606
logger.hicommandbase.sysloglevel 605

logger.iotrace.maxFileSize 666
logger.iotrace.numOfFiles 666
logger.loglevel 604, 677
logger.MaxBackupIndex 604, 677
logger.MaxFileSize 604, 677
logger.messagelogLevel 650
logger.properties 603, 665
logger.properties file 650, 676
logger.serverMessageFileCount 652
logger.serverMessageMaxFileSize 653
logger.serverTraceFileCount 652
logger.serverTraceMaxFileSize 654
logger.syslogLevel 652
logger.trace.level 665
logger.trace.maxFileSize 665
logger.trace.numOfFiles 665
logger.tracelogLevel 651
logs
  setup 403

M

mail-alert-detection.txt file 416
mainframe hosts 40
mainframe volumes 54
maintenance information
  acquiring on management server 578
  Host Data Collector 582
  host managed by Device Manager agent 584
  host managed by Host Data Collector 583
Management client 29
management server
  changing host name 148
  changing IP address 150
Management server 29
management server for VVols 373
managing
  host 40
memory heap size
  changing 36
migrating
  copy pair definition 704
  databases 491
  device group 708
  Device Manager to IPv6 environment 145
migration.dataErase.defaultValue 629
migration.multiExecution 630
migration.plan.candidateCapacityGroupDisplayMaxCount 629
migration.plan.candidateVolumeCountLimit 629
migration.properties 628
migration.volumeDelete.defaultValue 630
mime.properties 614
MOF file
  editing for event indications 321
  editing for object operations 315
multi-domain configuration 175

N

namespace 438
network
  bridge 143
NIC
  network settings multiple NICs 143
normal host 40
  prerequisites (Device Manager agent) 512
  prerequisites (Host Data Collector) 43

O

open hosts 40
OutOfMemory error 574

P

Pair management server 29
PairCfgMigration command 708
paircfgmigration.properties file 710
parameter
  configuration definition file 547
password
  truststore for Device Manager agent 311
  truststore for Host Data Collector 307
password.check.userID 158
password.min.length 158
password.min.lowercase 158
password.min.numeric 158
password.min.symbol 158
password.min.uppercase 158
perf_cmddev.properties file 447
perf_findcmddev command 445
performance information
  settings for acquiring 443, 448
  storage system (CIM/WBEM functions) 441
  storage systems 336
  system configuration 442
pop-up blocker
  changing settings 293
ports
  changing 114
  changing (CIM/WBEM) 441
  registering exceptions 121
  used by Common Component 106
  used by Device Manager agent 111
  used by Device Manager server 107
  used by Host Data Collector 109
  used by storage systems 111
  used by Tiered Storage Manager server 109
prerequisite environment
  using configuration definition file 545
prerequisites
  normal host (Device Manager agent) 512
  normal host (Host Data Collector) 43
  virtual machine (Device Manager agent) 513
  virtual machine (Host Data Collector) 45
  virtualization server 53
programproductinfo.properties file 678

properties
changing (Host Data Collector) 658
Device Manager server, changing 590
properties (Device Manager agent)
changing 670
properties (Tiered Storage Manager server)
changing 642
property files
agent.properties 671
cimxmlscpa.properties 616
client.properties 614
customizedsnmptrap.properties 620
database.properties 602, 648
Device Manager agent 670
Device Manager server 589
devicemanager.properties 649
dispatcher.properties 606
hdcbase.properties 658
hldutil.properties 675
Host Data Collector 658
hostdatacollectors 625
javaconfig.properties 666
launchapp.properties 623
logger.properties 603, 650, 665, 676
migration.properties 628
mime.properties 614
programproductinfo.properties 678
server.properties 591, 643, 654
syntax rules 590, 643
Tiered Storage Manager server 642
tuningmanager.properties 630

R

RADIUS server
exauth.properties file 189
receiving
email alerts 412
redundant configuration 175
remote connection
Tuning Manager (in a non-cluster environment) 348
Tuning Manager (in Red Hat Enterprise Linux cluster environment) 351
Tuning Manager (in Windows cluster environment) 349
Replication Manager 60
Replication Manager server 29
Replication tab 354
replication management 365
system configuration 355, 366
replication.properties file 633
requirements
connecting to Storage Navigator Modular 2 332
resident process 456
Device Manager agent 528
Host Data Collector 462
rgcmddev.properties file 692
RMI communication
Device Manager 360, 369
rpmlib.properties file 637
rpmlib.rpm.port 638

S

secret key
creating for Common Component 253
security
configuring networks (common security risks) 33
self-signed certificate
checking for CIM server 325
creating for CIM client 327
creating for Common Component 253
creating for Device Manager server 266
exporting 290
for object operations 326
sending
SNMP traps to log files 418
server certificate
applying to certificate authority for Common Component 257
applying to certificate authority for Device Manager 271
applying to certificate authority for Host Data Collector 286
checking for Device Manager agent 310
conditions for LDAP directory 300
deleting from Device Manager server truststore 281
deleting from truststore for Device Manager agent 312
exporting for CIM client 328
exporting for object operations 317
importing for event indications 324
importing into CIM client 329
importing into Device Manager agent 308
importing into Device Manager server keystore 273
importing into keystore for Host Data Collector 287
server.agent.differentialrefresh.manual.enabled 601
server.agent.differentialrefresh.periodical.enabled 602
server.agent.evtwait.timeout 692
server.agent.JRE.location 682
server.agent.maxMemorySize 681
server.agent.port 679
server.agent.rm.centralizePairConfiguration 684
server.agent.rm.cuLdevForm 684
server.agent.rm.exclusion.instance 685
server.agent.rm.horcm.poll 686
server.agent.rm.horcmSource 690
server.agent.rm.ignorePairStatus 689
server.agent.rm.location 685
server.agent.rm.moduleTimeOut 690

server.agent.rm.optimization.userHorcmFile 685
server.agent.rm.pairDefinitionForm 687
server.agent.rm.temporaryInstance 686
server.agent.rm.temporaryPort 686
server.agent.rm.userAuthentication 689
server.agent.shutDownTime 681
server.agent.snapshotEvtwait.timeout 692
server.base.home 595
server.base.initialsynchro 595, 645
server.checkOutVolumeRange 646
server.cim.agent 595
server.cim.http.port 596
server.cim.https.port 597
server.cim.support 596
server.cim.support.job 596
server.cim.support.protocol 596
server.configchange.enabled 597
server.dispatcher.configchange.pollingPeriod 608
server.dispatcher.daemon.autoSynchro.dayOfWee
k 610
server.dispatcher.daemon.autoSynchro.doRefresh
609
server.dispatcher.daemon.autoSynchro.interval
611
server.dispatcher.daemon.autoSynchro.logicalGro
up.doRefresh 613
server.dispatcher.daemon.autoSynchro.performan
ce.doRefresh 612
server.dispatcher.daemon.autoSynchro.performan
ce.startTime 613
server.dispatcher.daemon.autoSynchro.startTime
611
server.dispatcher.daemon.autoSynchro.type 610
server.dispatcher.daemon.configUpdate.detection
.interval 608
server.dispatcher.daemon.configUpdate.detection
.variable.enabled 611
server.dispatcher.daemon.logicalGroupMappingUp
date.startTime 614
server.dispatcher.daemon.pollingPeriod 607
server.dispatcher.daemon.receiveTrap 607
server.dispatcher.daemon.replication.config.doUp
date 633
server.dispatcher.daemon.replication.config.minut
e 635
server.dispatcher.daemon.replication.config.offset
634
server.dispatcher.daemon.replication.config.updat
eInterval 634
server.dispatcher.daemon.replication.performanc
e.rpm.updateInterval 636
server.dispatcher.daemon.replication.performanc
e.tnm.minute 637
server.dispatcher.daemon.replication.performanc
e.tnm.offset 636
server.dispatcher.daemon.replication.performanc
e.tnm.updateInterval 636
server.dispatcher.message.timeout 606
server.dispatcher.message.timeout.in.processing
606
server.dispatcher.snm2.configchange.pollingPerio
d 607
server.dispatcher.traps.purgePeriod 607
server.eventMonitoringIntervalInMinute 646
server.eventNotification.mail.to 600, 646
server.horcmconfigfile.hostname 595
server.http.entity.maxLength 594, 682
server.http.host 591, 679
server.http.localPort 679
server.http.port 592, 679
server.http.security.clientIP 616, 682
server.http.security.clientIPv6 617
server.http.security.unprotected 618
server.http.server.timeOut 691
server.http.socket.agentAddress 680
server.http.socket.bindAddress 681
server.https.enabledCipherSuites 619
server.https.port 593
server.https.protocols 619
server.https.security.keystore 618
server.https.security.truststore 619
server.logicalGroupMapping.updateInterval 602
server.logicalview.initialsynchro 598
server.mail.alert.status 600
server.mail.alert.type.storagesystem 600
server.mail.enabled.fileserver 598
server.mail.enabled.storagesystem 598
server.mail.errorsTo 600, 645
server.mail.from 599, 645
server.mail.smtp.auth 599, 646
server.mail.smtp.host 599, 645
server.mail.smtp.port 599, 646
server.migration.dataErase.defaultValue 647
server.migration.maxRetryCount 648
server.migration.multiExecution 646
server.migrationPlan.candidateCapacityGroupDisp
layMaxCount 647
server.migrationPlan.candidateVolumeCountLimit
647
server.properties 616
server.properties file
  Device Manager agent 678
  Device Manager server 591, 616
  Tiered Storage Manager server 643, 654
server.rmi.port 594, 644
server.rmi.secure 655
server.rmi.security.enabledCipherSuites 655
server.rmi.security.port 644
server.rmi.security.protocols 656
server.server.authorization 683
server.server.serverIPAddress 683
server.server.serverPort 683
server.server.ssl.hdvm 691
server.smisclient.indication.port 601
server.subsystem.ssid.availableValues 601
server.util.processTimeOut 691
service
  changing user (Device Manager agent) 530
setting up
  SMTP server for email alerts 413

settings
IPv6 145
properties for event notification 427
shared secret
checking 212
deleting 211
registering 210
SLP daemon
releasing 453
starting 451, 452
stopping 452
SLP service
releasing 453
starting 451
stopping 451
SLU 390
SMTP server
setting up for email alerts 413
SNMP traps
alerts 407
sending to log files 418
specifying
SMTP user authentication information for event notification 422, 428
starting instances (Tuning Manager - Agent for RAID) 361
storage location
configuration definition file, changing 562
Storage Navigator Modular 2
linking 332
storage system 29
acquiring performance information (by using CIM/WBEM functions) 441
changing 313
configuring instance environment 360
requirements for managing copy pairs 84
storage systems
collecting performance information 336
ports 111
SVP 33
System account
automatically lock 162
system configuration 29
central management method 63
for acquiring performance information 442
SVP configuration 77, 80
virtual command device server configuration 73
system requirements
managing copy pairs 62

T

TIC command 584
Tiered Storage Manager CLI 29
enabling SSL/TLS 296
generating log file 581
log file 581
Tiered Storage Manager server 29
ports 109
property files 642
truststore
changing password for Device Manager agent 311
changing password for Host Data Collector 307
deleting server certificate for Device Manager agent 312
viewing in normal mode (Device Manager server) 279
viewing in verbose mode (Device Manager server) 280
truststore file
downloading (Device Manager server) 288
downloading (Tiered Storage Manager server) 295
truststores 250
Tuning Manager 60
remote connection (in a non-cluster environment) 348
remote connection (in Red Hat Enterprise Linux cluster environment) 351
remote connection (in Windows cluster environment) 349
Tuning Manager - Agent for RAID
starting instances 361
Tuning Manager server
setting up properties 362
tuningmanager.properties file 630
two-way authentication
disabling 326
enabling for event indications 323
enabling for object operations 317

U

user accounts
account locking 160
account locking policies 160
password policies 158
setting account locking policies 161
setting password policies 158
unlocking accounts 162
user authentication
email alerts 415
event notification 422, 428
user who receives SNMP traps 409
user_httpsd.conf file 258

V

VASA Provider 370
veritas.volume.manager.version 678
virtual command device server 67
virtual machine 40
prerequisites (Device Manager agent) 513
prerequisites (Host Data Collector) 45
tasks for changing configuration 52

virtualization server 40
changing 308
prerequisites 53
VMware VVol
flow of tasks for setting Hitachi Command Suite products 377
SLU 390
system configuration for using VVol functionality 370
VASA Provider 370
vvoladaptersetup tool 382, 383, 385
vvoladaptersetup tool 382, 383, 385

W

warning banner 696
creating and registering a message 696
deleting message 698
message display condition 696
Windows
registering firewall exceptions 121

Hitachi Data Systems

MK-90HC175-25