Hitachi Command Suite
Administrator Guide
Contents

Preface..........................................................................................................................xxi
Intended audience........................................................................................................xxii
Product version...........................................................................................................xxii
Release notes.............................................................................................................xxii
Document revision level............................................................................................xxii
Document organization.............................................................................................xxiii
Related documents...................................................................................................xxiv
Document conventions.............................................................................................xxv
Conventions for storage capacity values....................................................................xxv
Accessing product documentation..........................................................................xxvi
Getting help...............................................................................................................xxvi
Comments...............................................................................................................xxvii

1 System configuration and requirements................................................................1-1
   System configuration..............................................................................................1-3
   Network security configuration............................................................................1-6
      Common security risks....................................................................................1-6
      Security configuration recommended for Device Manager............................................1-7
   System requirements for the management server and Host Data Collector computers. 1-8
      Maximum number of resources that can be managed...........................................1-8
      Changing the memory heap size.........................................................................1-9
      Changing the JDK of management servers........................................................1-10
      Changing the Java execution environment used by Host Data Collector..............1-11
   Hosts that can be managed by Device Manager....................................................1-12
   Host management software supported by Device Manager....................................1-13
   Prerequisites for normal hosts.............................................................................1-14
      Prerequisites for normal hosts managed by Host Data Collector ..........................1-14
      Prerequisites for normal hosts managed by Device Manager agent....................1-16
   Prerequisites for virtual machines........................................................................1-17
      Prerequisites for virtual machines managed by Host Data Collector .......................1-17
      Prerequisites for virtual machines managed by Device Manager agent...............1-20
   Operation workflow for allocating volumes to virtual machines...........................1-22
   Tasks required to change the virtual machine configuration....................................1-25
   Prerequisites for virtualization servers...............................................................1-26
      Prerequisites for virtualization servers..............................................................1-26
      Operation workflow for managing virtualization servers....................................1-27
Notes on operating virtualization servers .......................................................... 1-28
Prerequisites for mainframe hosts ....................................................................... 1-28
Operation workflow of managing a mainframe host ........................................... 1-29
Prerequisites for file servers ................................................................................ 1-29
Environment settings for Hitachi NAS Platform family ....................................... 1-29
Environment settings for Hitachi Data Ingestor and Hitachi NAS Platform F ....... 1-31
Operation workflow of managing file servers .................................................... 1-32
Notes on operating file servers ........................................................................... 1-33
Related products ................................................................................................... 1-33
System requirements for managing copy pairs .................................................. 1-34
System configuration for managing copy pairs .................................................. 1-35
System configuration for using the local management method to manage copy pairs ............................................................................................................. 1-36
System configuration for using the central management method to manage copy pairs ............................................................................................................. 1-40
System configuration for using a virtual command device server configuration to manage copy pairs ............................................................................................................. 1-44
System configuration for using an SVP configuration to manage copy pairs (when copy pairs are defined in a configuration definition file) ....................... 1-48
System configuration for using an SVP configuration to manage copy pairs (when copy pairs are defined as a device group) ................................................. 1-50
Storage system requirements for managing copy pairs ....................................... 1-53
Prerequisite version of the Device Manager agent for managing copy pairs ........ 1-58
Notes on managing copy pairs ........................................................................... 1-60
Configuring a high availability system ................................................................ 1-65
Example of a configuration for configuring a high availability system .................. 1-65
Requirements for configuring a high availability system ..................................... 1-67
Notes on executing commands ........................................................................... 1-69

2 Network configuration .................................................................................. 2-1
Ports used by Hitachi Command Suite products ................................................ 2-2
Ports used by Common Component ................................................................... 2-2
Ports used by the Device Manager server ......................................................... 2-3
Ports used by the Tiered Storage Manager server ............................................. 2-5
Ports used by Host Data Collector ..................................................................... 2-5
Ports used by the Device Manager agent ......................................................... 2-7
Ports used by storage systems ......................................................................... 2-7
Changing ports used by Common Component .................................................. 2-10
Registering firewall exceptions for Device Manager and Tiered Storage Manager 2-15
Port numbers that must be registered as firewall exceptions for Device Manager and Tiered Storage Manager ............................................................ 2-15
Registering firewall exceptions for Device Manager and Tiered Storage Manager in Windows ............................................................ 2-28
Registering firewall exceptions for Device Manager and Tiered Storage Manager in Red Hat Enterprise Linux ............................................................ 2-29
Registering firewall exceptions for Device Manager and Tiered Storage Manager in SUSE Linux Enterprise Server ............................................................ 2-29
Registering firewall exceptions for Host Data Collector (Windows) ................. 2-30
Registering an exception for the Host Data Collector service (for non-SSL communication) ............................................................ 2-30
Registering an exception for the Host Data Collector service (for SSL communication) ............................................................ 2-31
3 User account management ................................................................. 3-1
   About password policies............................................................. 3-2
      Setting password policies....................................................... 3-2
   About account locking.............................................................. 3-3
      About account locking policies............................................... 3-4
      Setting account locking policies............................................ 3-4
      Settings for automatically locking the System account........... 3-5
      Unlocking accounts............................................................. 3-6
   User management on an external authentication server.................... 3-7
      About linking to an external authentication server................... 3-7
      About linking to an external authorization server..................... 3-7
      Operating workflow for user authentication on an external authentication server.. 3-8
         Operating workflow for user authentication on an LDAP directory server........... 3-8
         Operating workflow for user authentication on a RADIUS server....................... 3-10
         Operation workflow for user authentication on a Kerberos server.................. 3-12
   Account conditions for Hitachi Command Suite products.................... 3-14
   About the data structures of user entries........................................ 3-15
      About the hierarchical structure model..................................... 3-15
      About the flat model.......................................................... 3-16
      About the BaseDN................................................................... 3-17
   Registering an external authentication server and an external authorization server3-17
      Setup items in the exauth.properties file for LDAP authentication........ 3-19
      Examples of setting the exauth.properties file for LDAP authentication...... 3-25
      Setup items in the exauth.properties file for RADIUS authentication....... 3-26
      Examples of setting the exauth.properties file for RADIUS authentication.. 3-33
      Setup items in the exauth.properties file for Kerberos authentication .... 3-34
      Examples of setting the exauth.properties file for Kerberos authentication.3-40
   About a LDAP search user account.................................................. 3-41
      Conditions for LDAP search user account.................................... 3-42
      Registering an LDAP search user account.................................... 3-43
      Deleting an LDAP search user account....................................... 3-45
      Checking the LDAP directory server that registered LDAP search user account ............... 3-45
   Registering a shared secret.......................................................... 3-46
      Deleting a shared secret......................................................... 3-46
      Checking the RADIUS server that registered a shared secret on the management server.. 3-47
Checking connections to an external authentication server and an external authorization server........................................................................................................3-47
Notes on commands for setting up a link to an external authentication server........................................................................................................3-49
Encryption types for Kerberos authentication.................................................................................................................................3-50

4 Security...............................................................................................4-1
Login warning banners.............................................................................................4-2
Conditions that apply when displaying warning banner messages..........................4-2
Creating and deleting a message displayed on a warning banner..........................4-2
Deleting a message from the warning banner..........................................................4-4
Communication security mode..................................................................................4-5
Secure communication for Device Manager and Tiered Storage Manager..............4-5
Operation workflow for secure communication between a management server and a management client (GUI)..............................................................4-9
Operation workflow for secure communication between a management server and a management client (Device Manager CLI)..........................................4-11
Operation workflow for secure communication between a management server and a management client (Tiered Storage Manager CLI)..........................4-12
Operation workflow for secure communication between an LDAP directory server and a management server .................................................................4-13
Operation workflow for secure communication between a Device Manager server and a replication manager server..............................................................4-14
Operation workflow for secure communication between a Tuning Manager server and a Device Manager server.................................................................4-16
Operation workflow for secure communication between a Host Data Collector machine and a management server...........................................................4-17
Operation workflow for secure communication between a virtualization server and a management server.........................................................................4-19
Operation workflow for secure communication between a management server and a management server and Device Manager agent........................................4-20
Operation workflow for secure communication between a storage system and a management server ..............................................................................4-22
Operation workflow for secure communication between a management server and a storage system (VSP G1000).................................................................4-22
Operation workflow for secure communication between an SMI-S provider and a management server.............................................................................4-23
Operation workflow for secure communication between a Tuning Manager Agent and a Tuning Manager server.................................................................4-24
Operation workflow for secure communication between a Tuning Manager server and a Tuning Manager API client...............................................................4-25
Operation workflow for secure communication between a storage system and a management client (GUI)..............................................................................4-25
Operation workflow for secure communication between a management server and a CIM client (object operations).................................................................4-26
Operation workflow for secure communication between a management server and a CIM client (two-way authentication for object operations)....................4-27
Operation workflow for secure communication between a management server and a CIM client (event indications).................................................................4-29
Operation workflow for secure communication between an SMI-S provider and a CIM client (two-way authentication for event indications).........................4-29
Truststores.................................................................................................................4-30
Configuring an SSL server (Common Component)....................................................4-33
Creating a secret key and a certificate signing request for Common Component .......................................................................................... 4-33
Applying to a certificate authority for a Common Component server certificate ............................................................................................................. 4-36
Editing the user_httpd.conf file......................................................................... 4-36
Closing the port for the non-SSL communication (HBase 64 Storage Mgmt Web Service)............................................................................................................. 4-39

Configuring an SSL server (Device Manager server)............................................ 4-41
Creating a key pair and a self-signed certificate for Device Manager server 4-41
Enabling SSL/TLS for the Device Manager server............................................ 4-44
Creating a certificate signing request for Device Manager server................. 4-45
Applying to a certificate authority for a Device Manager server certificate... 4-46
Importing a server certificate into the Device Manager server keystore..... 4-47
Viewing the Device Manager server key pair information in normal mode.. 4-48
Viewing the Device Manager server key pair information in verbose mode ... 4-49
Deleting a key pair from the Device Manager server keystore....................... 4-50
Changing the password of a Device Manager server key pair.................... 4-50
Changing the password of the Device Manager server key store................... 4-51
Importing a certificate into the Device Manager server truststore............. 4-52
Viewing the Device Manager server truststore information in normal mode4-53
Viewing the Device Manager server truststore information in verbose mode... 4-53

Configuring an SSL server (Host Data Collector)............................................. 4-56
Creating a key pair and a certificate signing request for Host Data Collector .... 4-56
Applying to a certificate authority for a Host Data Collector server certificate .. 4-58
Importing the Host Data Collector server certificates into the keystore...... 4-59

Configuring an SSL server (Tuning Manager Agent host)............................. 4-60
Creating a secret key and a certificate signing request for Tuning Manager Agent host.......................................................... 4-60
Applying to a certificate authority for an Tuning Manager Agent host server certificate............................................................ 4-60
Enabling SSL/TLS (Tuning Manager Agent host)........................................... 4-62

Configuring an SSL client.................................................................................. 4-65
Downloading a Device Manager server truststore file.................................... 4-65
Exporting a Device Manager server self-signed certificate............................ 4-66
Importing a server certificate into a Web browser....................................... 4-66
Changing pop-up blocker settings.................................................................. 4-67
Enabling SSL/TLS for the Device Manager CLI computer........................... 4-68
Downloading the Tiered Storage Manager server truststore files............... 4-69
Enabling SSL/TLS for the Tiered Storage Manager CLI computer.............. 4-70
Importing a certificate into the truststore for Hitachi Command Suite....... 4-71
Conditions for an LDAP directory server certificate.................................... 4-74
Checking the certificates imported into the truststore for Hitachi Command Suite ................................................................. 4-75
Changing the communication protocol between the Replication Manager server and the Device Manager server................................................ 4-75
Importing a certificate into the truststore for Host Data Collector............... 4-76
Checking the server certificate imported into the truststore for the Host Data Collector............................................................................................... 4-77
Changing the truststore password for the Host Data Collector............................................................... 4-78
Changing virtualization server information............................................................................................. 4-79
Importing a server certificate into the truststore for the Device Manager agent.................................................. 4-79
Checking the server certificate imported into the truststore for the Device Manager agent.......................... 4-81
Changing the truststore password for the Device Manager agent.............................................................. 4-81
Deleting a server certificate imported into the truststore for the Device Manager agent.......................... 4-82
Changing storage system information........................................................................................................ 4-83
Configuring an SSL server and clients (VSP G1000)......................................................................... 4-84
Notes on updating the signed certificate to the SVP.............................................................................. 4-84
Creating a private key (.key file) ................................................................................................................. 4-85
Creating a public key (.csr file) .................................................................................................................. 4-85
Acquiring a signed certificate....................................................................................................................... 4-86
Uploading the signed certificate.................................................................................................................. 4-87
Returning the certificate to default............................................................................................................ 4-88
Importing the certificate to the SVP.......................................................................................................... 4-90
Blocking HTTP communication to the storage system.............................................................................. 4-95
Releasing HTTP communication blocking.................................................................................................. 4-96
Using the SMI-S function............................................................................................................................. 4-96
Uploading a signed certificate to the SMI-S provider................................................................................. 4-97
Returning an SMI-S provider certificate to default...................................................................................... 4-99
Uploading an SMI-S provider configuration file.......................................................................................... 4-100
Returning an SMI-S provider configuration file to default........................................................................ 4-101
Sending SMI-S Artificial Indication........................................................................................................... 4-102
Array-setting-01.properties file.................................................................................................................. 4-103
Registering certificates for HCS.................................................................................................................. 4-106
Notes on registering certificates for HCS..................................................................................................... 4-107
Deleting certificates for HCS...................................................................................................................... 4-107
Configuring an SSL server and clients (CIM server)......................................................................... 4-108
Creating a keystore file for object operations............................................................................................ 4-109
Editing an MOF file for object operations.................................................................................................. 4-110
Exporting a server certificate for object operations.................................................................................... 4-111
Enabling two-way authentication for object operations............................................................................. 4-112
Importing a client certificate for object operations...................................................................................... 4-113
Creating a keystore file for event indications.............................................................................................. 4-113
Editing an MOF file for event indications.................................................................................................. 4-114
Exporting a client certificate for event indications...................................................................................... 4-116
Enabling two-way authentication for event indications................................................................................ 4-116
Importing a server certificate for event indications.................................................................................... 4-117
Checking a self-signed certificate for a CIM server..................................................................................... 4-118
Self-signed certificate for object operations supplied with the product..................................................... 4-119
Disabling two-way authentication............................................................................................................... 4-119
Configuring an SSL server and clients (CIM client)........................................................................ 4-120
Creating a key pair and self-signed certificate for a CIM client.................................................................... 4-120
Exporting a server or client certificate for a CIM client............................................................................. 4-121
Importing a server or client certificate into a CIM client............................................................................ 4-121
Controlling management client access to the management server........................................................... 4-122
Changing the password-encoding level in the Device Manager CLI and the Tiered Storage Manager CLI ................................................................. 4-124

5 Configuring Device Manager for use with related products ............... 5-1
Settings required for linking with Storage Navigator Modular 2 ............. 5-2
Notes and requirements for connecting to Storage Navigator Modular 2 .. 5-2
Settings for using Element Manager ....................................................... 5-3
Deleting the settings for using Element Manager .................................... 5-5
Settings required to collect storage system performance information .......... 5-6
System configuration for collecting storage system performance information .. 5-7
Settings to enable the Device Manager server, the Tuning Manager server, and Tuning Manager - Agent for RAID to communicate ......................... 5-9
Settings for collecting storage system performance information ................. 5-10
Settings for collecting performance information from enterprise-class storage systems and HUS VM ................................................................. 5-10
Settings for collecting performance information from midrange storage systems ................................................................................................. 5-11
Operation workflow for setting up the Device Manager server (collection of storage system performance information) ........................................ 5-11
Remote connection to the Tuning Manager server (in a non-cluster environment) ................................................................................................... 5-15
Remote connection to the Tuning Manager server (in a cluster environment) ........................................................................................................ 5-15
Specifying the settings for remote connection to the Tuning Manager server and the port number (htmsetup command) ...................................... 5-18
Setting up the config.xml and configforclient.xml files ......................... 5-19
Setting up the management client (to collect storage system performance information) ............................................................................................. 5-20
Analyzing the performance of Universal Replicator ............................... 5-20
System configuration for analyzing the performance of Universal Replicator ... 5-20
Settings on Device Manager for analyzing Universal Replicator performance .......................... 5-23
Settings on Replication Manager for analyzing Universal Replicator performance. 5-24
Settings on Tuning Manager for analyzing Universal Replicator performance .... 5-24
Settings necessary to launch Hitachi Storage Services Manager ............... 5-25
Using the Device Manager - Storage Navigator (VSP G1000) ................. 5-26
Logging in to Device Manager - Storage Navigator .................................. 5-26
Initial super-user login ............................................................................. 5-26
Normal login ............................................................................................. 5-26
Changing your password ........................................................................ 5-27
Adding your SVP to the trusted sites zone - for Windows server ............... 5-28
Setting Device Manager - Storage Navigator environmental parameters .... 5-29
Backing up and restoring HDvM - SN configuration files .......................... 5-31
Installing the report configuration tool ................................................................. 5-33
Prerequisites ........................................................................................ 5-33
Installation procedure ........................................................................... 5-34
Using the report configuration tool .............................................................. 5-34
Report Configuration Tool command reference (raidinf commands) ...... 5-34
raidinf command list and command description ...................................... 5-34
raidinf command syntax ......................................................................... 5-35
raidinf add report .................................................................................. 5-37
raidinf delete report .............................................................................. 5-38
raidinf download report ........................................................................ 5-39
6 Setting up logs and alerts.................................................................6-1
   Setting up Hitachi Command Suite common trace log files..................6-2
      Setting up Hitachi Command Suite common trace log files (Windows)...6-2
      Setting up Hitachi Command Suite common trace log files (Linux).....6-2
   Setting up alerts............................................................................6-3
      Error detection by Device Manager..............................................6-3
      Settings for displaying SNMP traps as alerts.........................6-5
      Operation flow for reporting alerts by email.............................6-6
      Setting up the SMTP server.......................................................6-7
      Registering recipients of email alerts........................................6-7
      Property settings for reporting alerts.......................................6-8
      Registering an SMTP authentication user account in Device Manager6-8
      Customizing email alert template..............................................6-9
   Sending SNMP traps to log files...................................................6-11
      Setting up Device Manager to output SNMP traps......................6-12
   Using event notification.................................................................6-13
      Setting properties for event notification..................................6-14
      Customizing event notification templates...............................6-14
      Specifying SMTP user authentication information for event notification6-19
         Format of the hdvmmmodmailuser command..........................6-19
         Format of the htsmmmodmailuser command.............................6-21
   Reporting failure information about storage systems (for VSP G1000 only)6-22
      Requirements of the new Syslog protocol (TLS1.2/RFC5424).........6-22
      Obtaining a client certificate for the new Syslog protocol...........6-22
      Setting and configuring syslog notification for SIMs..................6-23
      Configuring email notification..................................................6-24
      Setting system options...............................................................6-26

7 Configuring Device Manager for CIM/WBEM..................................7-1
   About CIM/WBEM........................................................................7-2
   CIM/WBEM functions in Device Manager.......................................7-2
   Specifying a namespace...............................................................7-4
   User account settings for using the CIM/WBEM functions...............7-4
   Enabling CIM/WBEM functions.....................................................7-5
   Changing CIM/WBEM port numbers..............................................7-6
   Settings for acquiring storage system performance information by using CIM/WBEM functions.................................7-7
      Required system configuration for acquiring performance information7-7
      Settings required to acquire performance information of enterprise-class storage systems..................................................7-9
      Preparing the storage system for acquiring performance information7-9
      Preparing the host to acquire performance information................7-9
      Preparing the Device Manager server to acquire performance information.7-10
10 Using the Device Manager agent

10-1
Prerequisites for running the Device Manager agent........................................ 10-2
Prerequisites for using a host on which multiple NICs are installed.............. 10-2
Notes on running the Device Manager agent.............................................. 10-2
Specifying the Device Manager agent environment settings....................... 10-3
Settings for changing the Java execution environment (javapath_setup command) ..................................................................................................................... 10-4
Registering the Windows Firewall exceptions for Device Manager agent
(firewall_setup command)............................................................................. 10-6
Registering a Java process in SED as an exception (AIX)............................ 10-6
Managing copy pairs.................................................................................. 10-7
Settings required for a host to manage 100 or more LUs............................. 10-8
Resident processes of the Device Manager agent....................................... 10-10
Starting and stopping the Device Manager agent service, and checking the operating status of the service (hbsasrv command)..................................................... 10-15
Changing the user who executes the Device Manager agent service (Windows).10-17
Device Manager agent operations.............................................................. 10-17
Checking the available agent functions (hbsa_modinfo command)............ 10-17
Deleting the Device Manager agent's registry entries and files (hbsa_util command) ................................................................................................................... 10-19
Displaying the version of the Device Manager agent (hdvm_info command).10-19
Setting the Device Manager server's information, HiScan command's execution period, and CCI's information (hdvmagt_setting command)..................................................... 10-20
Reporting host information to the Device Manager server manually (HiScan
command)....................................................................................................10-22
Acquiring device information (hldutil command).................................... 10-24
Information displayed by the hldutil command........................................ 10-28
Configuration definition file for managing copy pairs............................ 10-29
Prerequisite environment for using the configuration definition file.......... 10-29
Editing the configuration definition file.................................................... 10-30
Configuration definition file parameters supported Device Manager.......... 10-31
Description conventions for the configuration definition file..................... 10-32
HORCM_MON parameter description format............................................ 10-33
HORCM_CMD parameter description format............................................ 10-35
HORCM_VCMD parameter description format......................................... 10-37
HORCM_DEV parameter description format.......................................... 10-37
HORCM_LDEV parameter description format........................................... 10-40
HORCM_INST parameter description format......................................... 10-42
HORCM_INSTP parameter description format......................................... 10-44
Changing the storage location of the configuration definition file............ 10-46
Notes on using the configuration definition file....................................... 10-47

11 Troubleshooting

11-1
How to troubleshoot problems on the management server (Device Manager related).11-2
The user cannot log in to the Device Manager GUI.................................... 11-2
The services of Common Component or the Device Manager server cannot be started.......................................................... 11-2
The Device Manager server cannot be accessed after starting up the management server or Hitachi Command Suite product services .................................................. 11-3
SNMP traps of Hitachi Data Ingestor and Hitachi NAS Platform F cannot be received ..................................................................................................................... 11-3
An attempt to reconfigure or refresh a storage system failed ................................................. 11-4
How to troubleshoot problems on the management server (Tiered Storage Manager related) ........................................................................................................... 11-5
The Tiered Storage Manager server could not be started .................................................. 11-5
The Tiered Storage Manager server does not stop ............................................................. 11-5
The Tiered Storage Manager server terminates abnormally or fails over in a cluster environment ................................................................................................... 11-6
Tiered Storage Manager operations cannot be performed because an error occurred in the database .................................................................................................. 11-7
How to troubleshoot problems on a host .............................................................................. 11-8
The HiScan command cannot add host information to the Device Manager server ......................................................................................................................... 11-8
A communication error occurs, and the processing of other Hitachi Command Suite products stops ..................................................................................................... 11-9
Two copies of HBase Agent are displayed in the Programs and Features window .............. 11-9
HBase Agent is displayed in the Programs and Features window ....................................... 11-9
JavaVM terminates abnormally .......................................................................................... 11-9
An OutOfMemory error occurs on a host, and after a while the host stops responding .......... 11-10
The file system name is not displayed in the Device Manager GUI .................................... 11-10
Changes to the storage system configuration are not applied to the Device Manager server .............................................................................................................. 11-11
Errors requiring no action .................................................................................................. 11-12
Maintenance information that must be collected if a failure occurs ..................................... 11-13
Acquiring maintenance information on the management server (hcmds64getlogs command) ........................................................................................................... 11-14
Generating the Tiered Storage Manager CLI log file .......................................................... 11-14
Acquiring maintenance information for a Host Data Collector computer (hdc_getras command) ............................................................................................................ 11-16
Acquiring maintenance information on a host managed by Host Data Collector (hdc_target_getras command) ............................................................................... 11-16
Acquiring maintenance information on the Device Manager agent (TIC command) .......... 11-17
Acquiring a thread dump of the HBase 64 Storage Mgmt Common Service (Windows) .... 11-18
Acquiring a thread dump of the HCS Device Manager Web Service (Windows) ............... 11-19
Acquiring a thread dump of the HBase 64 Storage Mgmt Common Service (Linux) ......... 11-20
Acquiring a thread dump of the HCS Device Manager Web Service (Linux) .................... 11-21

A Device Manager server properties ................................................................................... A-1
Device Manager server property files .................................................................................. A-3
Changing Device Manager server properties .................................................................... A-4
Syntax rules for Device Manager server property files .................................................... A-4
Device Manager server configuration properties (server.properties file) ......................... A-5
server.http.host ............................................................................................................. A-5
server.http.port .......................................................................................................... A-6
server.https.port ......................................................................................................... A-7
<table>
<thead>
<tr>
<th>Property</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>server.rmi.port</td>
<td>A-8</td>
</tr>
<tr>
<td>server.http.entity.maxLength</td>
<td>A-8</td>
</tr>
<tr>
<td>server.base.home</td>
<td>A-8</td>
</tr>
<tr>
<td>server.horcmconfigfile.hostname</td>
<td>A-9</td>
</tr>
<tr>
<td>server.base.initialsynchro</td>
<td>A-9</td>
</tr>
<tr>
<td>server.cim.agent</td>
<td>A-9</td>
</tr>
<tr>
<td>server.cim.support</td>
<td>A-9</td>
</tr>
<tr>
<td>server.cim.support.job</td>
<td>A-10</td>
</tr>
<tr>
<td>server.cim.support.protocol</td>
<td>A-10</td>
</tr>
<tr>
<td>server.cim.http.port</td>
<td>A-10</td>
</tr>
<tr>
<td>server.cim.https.port</td>
<td>A-10</td>
</tr>
<tr>
<td>server.configchange.enabled</td>
<td>A-11</td>
</tr>
<tr>
<td>server.logicalview.initialsynchro</td>
<td>A-12</td>
</tr>
<tr>
<td>server.mail.enabled.filesystem</td>
<td>A-12</td>
</tr>
<tr>
<td>server.mail.enabled.storagesystem</td>
<td>A-12</td>
</tr>
<tr>
<td>server.mail.from</td>
<td>A-13</td>
</tr>
<tr>
<td>server.mail.smtp.host</td>
<td>A-13</td>
</tr>
<tr>
<td>server.mail.smtp.port</td>
<td>A-13</td>
</tr>
<tr>
<td>server.mail.smtp.auth</td>
<td>A-13</td>
</tr>
<tr>
<td>server.mail.errorsTo</td>
<td>A-14</td>
</tr>
<tr>
<td>server.eventNotification.mail.to</td>
<td>A-14</td>
</tr>
<tr>
<td>server.mail.alert.type.storagesystem</td>
<td>A-14</td>
</tr>
<tr>
<td>server.mail.alert.status</td>
<td>A-14</td>
</tr>
<tr>
<td>server.subsystem.ssid.availableValues</td>
<td>A-15</td>
</tr>
<tr>
<td>server.smisclient.indication.port</td>
<td>A-15</td>
</tr>
<tr>
<td>server.agent.differentialrefresh.manual.enabled</td>
<td>A-15</td>
</tr>
<tr>
<td>server.agent.differentialrefresh.periodical.enabled</td>
<td>A-16</td>
</tr>
<tr>
<td>server.dispatcher.daemon.pollingPeriod</td>
<td>A-21</td>
</tr>
<tr>
<td>server.dispatcher.message.timeout</td>
<td>A-20</td>
</tr>
<tr>
<td>server.dispatcher.message.timeout.in.processing</td>
<td>A-20</td>
</tr>
<tr>
<td>server.dispatcher.daemon.pollingPeriod</td>
<td>A-21</td>
</tr>
<tr>
<td>server.dispatcher.traps.purgePeriod</td>
<td>A-21</td>
</tr>
<tr>
<td>server.dispatcher.daemon.receiveTrap</td>
<td>A-21</td>
</tr>
<tr>
<td>server.dispatcher.snmp2.configchange.pollingPeriod</td>
<td>A-21</td>
</tr>
<tr>
<td>server.dispatcher.configchange.pollingPeriod</td>
<td>A-22</td>
</tr>
<tr>
<td>server.dispatcher.daemon.configUpdate.detection.interval</td>
<td>A-22</td>
</tr>
<tr>
<td>server.dispatcher.daemon.autoSynchro.doRefresh</td>
<td>A-23</td>
</tr>
<tr>
<td>server.dispatcher.daemon.autoSynchro.type</td>
<td>A-24</td>
</tr>
<tr>
<td>server.dispatcher.daemon.autoSynchro.dayOfWeek</td>
<td>A-24</td>
</tr>
</tbody>
</table>
Device Manager MIME type properties (mime.properties file) ........................................... A-28
Device Manager client properties (client.properties file) ........................................... A-28
Device Manager security properties (server.properties file and cimxmlscpa.properties file) .................................................. A-29
Device Manager SNMP trap log output properties (customizedsnmptrap.properties file) .................................................. A-33
Device Manager launchable applications properties (launchapp.properties file) .................................................. A-35
Properties for communicating with the host (host.properties file) .................................................. A-37
Properties for connecting to Host Data Collector (hostdatacollectors.properties file) .................................................. A-38
Properties for migrations (migration.properties file) .................................................. A-41
Properties for connecting to Tuning Manager (tuningmanager.properties file) .................................................. A-43
Properties related to Universal Replicator performance analysis (replication.properties file) ................................................................. A-46
  server.dispatcher.daemon.replication.config.doUpdate .................................. A-46
  server.dispatcher.daemon.replication.config.updateInterval .......................... A-47
  server.dispatcher.daemon.replication.config.offset ....................................... A-47
  server.dispatcher.daemon.replication.config.minute .................................... A-48
  server.dispatcher.daemon.replication.performance.rpm.updateInterval .......... A-48
  server.dispatcher.daemon.replication.performance.tnm.updateInterval .......... A-49
  server.dispatcher.daemon.replication.performance.tnm.offset ...................... A-49
  server.dispatcher.daemon.replication.performance.tnm.minute ..................... A-50
  hdvm.replication.disabled ........................................................................ A-50
Properties for connecting to Replication Manager (rpmlib.properties file) ................................................................. A-50
  rpmlib.rpm.port .......................................................................................... A-50
Properties for the CIM/WBEM functions (jserver.properties file, cimxmlcpa.properties file, cimxmlscpa.properties file) .................................................................................. A-51
  com.wbemsolutions.jserver.bindto ................................................................ A-51
  HTTPPort....................................................................................................... A-52
  HTTPSPort................................................................................................... A-52

B Tiered Storage Manager server properties ............................................. B-1
Tiered Storage Manager server property files.............................................. B-2
  Changing Tiered Storage Manager server properties ....................................... B-2
  Syntax rules for Tiered Storage Manager server property files ............................ B-3
Tiered Storage Manager server operations properties (server.properties file) .... B-3
  server.rmi.port............................................................................................. B-4
  server.rmi.security.port ............................................................................... B-4
  server.base.initialsynchro ........................................................................... B-5
  server.mail.smtp.host ................................................................................ B-5
  server.mail.from .......................................................................................... B-5
  server.mail.errorsTo ................................................................................... B-5
  server.mail.smtp.port ................................................................................. B-6
  server.mail.smtp.auth ............................................................................... B-6
  server.mail.smtp.auth ............................................................................... B-6
  server.eventNotification.mail.to .................................................................. B-6
  server.eventMonitoringIntervalInMinute ...................................................... B-6
  server.migration.multiExecution .................................................................. B-6
  server.checkOutVolumeRange ..................................................................... B-7
  server.migration.dataErase.defaultValue ..................................................... B-7
  server.migrationPlan.candidateVolumeCountLimit ....................................... B-7
  server.migrationPlan.candidateCapacityGroupDisplayMaxCount ................. B-7
  server.migration.maxRetryCount .................................................................. B-8
Tiered Storage Manager database properties (database.properties file) .......... B-8
  dbm.traceSQL ............................................................................................ B-8
Tiered Storage Manager properties for accessing Device Manager server (devicemanager.properties file) ....................................................... B-9
  hdvm.protocol ............................................................................................ B-9
  hdvm.port ................................................................................................. B-9
  hdvm.timeout ............................................................................................ B-9
  hdvm.rmi.port ............................................................................................ B-9
Tiered Storage Manager log output properties (logger.properties file) ............ B-10
  logger.messageLogLevel ........................................................................... B-10
  logger.traceLogLevel ................................................................................ B-11
  logger.syslogLevel .................................................................................... B-12
logger.serverMessageFileCount........................................................................ B-12
logger.serverTraceFileCount........................................................................ B-12
logger.guiMessageFileCount......................................................................... B-13
logger.guiTraceFileCount............................................................................. B-13
logger.serverMessageMaxFileSize................................................................ B-14
logger.serverTraceMaxFileSize..................................................................... B-14
logger.guiMessageMaxFileSize..................................................................... B-14
logger.guiTraceMaxFileSize......................................................................... B-14

Tiered Storage Manager security properties (server.properties file)................. B-15
server.rmi.secure........................................................................................ B-15
server.rmi.security.enabledCipherSuites.................................................... B-15

C Host Data Collector properties..................................................................... C-1
Host Data Collector property files................................................................. C-2
Changing Host Data Collector properties....................................................... C-2
Properties related to Host Data Collector operation (hdcbase.properties file).... C-2
    hdc.service.localport........................................................................... C-3
    hdc.adapter.adapterProcessNum......................................................... C-3
    hdc.adapter.localport....................................................................... C-3
    hdc.common.rmi.registryPort............................................................ C-3
    hdc.common.rmi.serverPort............................................................... C-4
    hdc.common.http.serverPort............................................................. C-4
    hdc.common.rmi.ssl.registryPort....................................................... C-5
    hdc.common.rmi.ssl.serverPort.......................................................... C-5
    hdc.common.https.serverPort......................................................... C-6
    hdc.service.rmi.registryIPAddress..................................................... C-6
    hdc.service.rmi.registryPort........................................................... C-7
    hdc.service.rmi.ssl.registryPort....................................................... C-7
    hdc.service.rmi.ssl.serverPort......................................................... C-7
    hdc.adapter.esx.timeout................................................................... C-7
    hdc.ssl.secure................................................................................ C-7
    hdc.ssl.esx.certCheck...................................................................... C-8

Host Data Collector logger properties (logger.properties file)........................ C-9
    logger.trace.level................................................................................ C-9
    logger.trace.maxFileSize..................................................................... C-9
    logger.trace.numOfFiles...................................................................... C-9
    logger.iotrace.maxFileSize.................................................................. C-10
    logger.iotrace.numOfFiles.................................................................. C-10

Properties related to the Host Data Collector's Java environment (javaconfig.properties file)............................................................................................................. C-10
javapathlocation..................................................................................... C-10

Host Data Collector security properties (hdcbase.properties file).................. C-11
    hdc.ssl.ciphers................................................................................ C-11

D Device Manager agent properties............................................................... D-1
Device Manager agent property files.......................................................... D-2
Changing Device Manager agent properties................................................ D-2
Device Manager agent properties for connecting to the Replication Manager server (agent.properties file).......................................................... D-3
    agent.rm.TimeOut............................................................................... D-3
    agent.rm.everytimeShutdown............................................................ D-3
    agent.rm.shutdownWait..................................................................... D-4
    agent.rm.horcmInstance................................................................. D-4
Acronyms and abbreviations
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 revision level**
- **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 SANs (Storage Area Networks)
- 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 v8.1 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.

Document revision level

<table>
<thead>
<tr>
<th>Revision</th>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MK-90HC175-00</td>
<td>October 2010</td>
<td>Initial release</td>
</tr>
<tr>
<td>MK-90HC175-01</td>
<td>October 2010</td>
<td>Revision 1, supersedes and replaces MK-90HC175-00</td>
</tr>
<tr>
<td>MK-90HC175-02</td>
<td>January 2011</td>
<td>Revision 2, supersedes and replaces MK-90HC175-01</td>
</tr>
<tr>
<td>MK-90HC175-03</td>
<td>April 2011</td>
<td>Revision 3, supersedes and replaces MK-90HC175-02</td>
</tr>
<tr>
<td>MK-90HC175-04</td>
<td>August 2011</td>
<td>Revision 4, supersedes and replaces MK-90HC175-03</td>
</tr>
<tr>
<td>MK-90HC175-05</td>
<td>November 2011</td>
<td>Revision 5, supersedes and replaces MK-90HC175-04</td>
</tr>
<tr>
<td>MK-90HC175-06</td>
<td>March 2012</td>
<td>Revision 6, supersedes and replaces MK-90HC175-05</td>
</tr>
<tr>
<td>MK-90HC175-07</td>
<td>July 2012</td>
<td>Revision 7, supersedes and replaces MK-90HC175-06</td>
</tr>
<tr>
<td>MK-90HC175-08</td>
<td>August 2012</td>
<td>Revision 8, supersedes and replaces MK-90HC175-07</td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>Chapter/Appendix</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Chapter 1, System configuration and requirements on page 1-1</strong></td>
<td>This chapter provides the system configuration and system requirements for Device Manager and Tiered Storage Manager.</td>
</tr>
<tr>
<td><strong>Chapter 2, Network configuration on page 2-1</strong></td>
<td>This chapter explains the Hitachi Command Suite product settings required for various network configurations.</td>
</tr>
<tr>
<td><strong>Chapter 3, User account management on page 3-1</strong></td>
<td>This chapter explains the settings required for managing Hitachi Command Suite product user accounts.</td>
</tr>
<tr>
<td><strong>Chapter 4, Security on page 4-1</strong></td>
<td>This chapter explains the security settings required to use Hitachi Command Suite products.</td>
</tr>
<tr>
<td><strong>Chapter 5, Configuring Device Manager for use with related products on page 5-1</strong></td>
<td>This chapter explains the settings required to link with related products.</td>
</tr>
<tr>
<td><strong>Chapter 6, Setting up logs and alerts on page 6-1</strong></td>
<td>This chapter explains the settings required for using Hitachi Command Suite products to monitor system statuses and errors.</td>
</tr>
<tr>
<td><strong>Chapter 7, Configuring Device Manager for CIM/WBEM on page 7-1</strong></td>
<td>This chapter explains how to set up CIM/WBEM.</td>
</tr>
</tbody>
</table>
Chapter 8, Starting and stopping services on page 8-1
This chapter explains how to start and stop Hitachi Command Suite product services on the management server.

Chapter 9, Managing the database on page 9-1
This chapter explains how to back up and restore Hitachi Command Suite product databases.

Chapter 10, Using the Device Manager agent on page 10-1
This chapter contains precautions regarding the management of hosts and the settings and operations for Device Manager agents.

Chapter 11, Troubleshooting on page 11-1
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.

Appendix A, Device Manager server properties on page A-1
This chapter describes the Device Manager server property files.

Appendix B, Tiered Storage Manager server properties on page B-1
This chapter describes the Tiered Storage Manager server property files.

Appendix C, Host Data Collector properties on page C-1
This chapter describes Host Data Collector property file.

Appendix D, Device Manager agent properties on page D-1
This chapter describes the Device Manager agent property files.

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

- Hitachi Command Suite Installation and Configuration Guide, MK-90HC173
- Hitachi Command Suite Tiered Storage Manager CLI Reference Guide, MK-90HC177
- Hitachi Command Suite Messages, MK-90HC178
- 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:

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bold</td>
<td>Indicates text on a window, other than the window title, including menus, menu options, buttons, fields, and labels. Example: Click OK.</td>
</tr>
<tr>
<td><em>Italic</em></td>
<td>Indicates a variable, which is a placeholder for actual text provided by the user or system. Example: <code>copy source-file target-file</code></td>
</tr>
<tr>
<td><em>Note:</em> Angled brackets (&lt; &gt;) are also used to indicate variables.</td>
<td></td>
</tr>
<tr>
<td>Monospace</td>
<td>Indicates text that is displayed on screen or entered by the user. Example: <code># pairdisplay -g oradb</code></td>
</tr>
<tr>
<td>&lt; &gt; angled brackets</td>
<td>Indicates a variable, which is a placeholder for actual text provided by the user or system. Example: <code># pairdisplay -g &lt;group&gt;</code></td>
</tr>
<tr>
<td><em>Note:</em> Italic font is also used to indicate variables.</td>
<td></td>
</tr>
<tr>
<td>[ ] square brackets</td>
<td>Indicates optional values. Example: `[ a</td>
</tr>
<tr>
<td>{ } braces</td>
<td>Indicates required or expected values. Example: `{ a</td>
</tr>
<tr>
<td></td>
<td>vertical bar</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Icon</th>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Note" /></td>
<td>Note</td>
<td>Calls attention to important or additional information.</td>
</tr>
<tr>
<td><img src="image" alt="Tip" /></td>
<td>Tip</td>
<td>Provides helpful information, guidelines, or suggestions for performing tasks more effectively.</td>
</tr>
<tr>
<td><img src="image" alt="Caution" /></td>
<td>Caution</td>
<td>Warns the user of adverse conditions or consequences (for example, disruptive operations).</td>
</tr>
<tr>
<td><img src="image" alt="WARNING" /></td>
<td>WARNING</td>
<td>Warns the user of severe conditions or consequences (for example, destructive operations).</td>
</tr>
</tbody>
</table>

Conventions for storage capacity values

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

<table>
<thead>
<tr>
<th>Physical capacity unit</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 kilobyte (KB)</td>
<td>1,000 (10^3) bytes</td>
</tr>
<tr>
<td>1 megabyte (MB)</td>
<td>1,000 KB or 1,000(^2) bytes</td>
</tr>
<tr>
<td>1 gigabyte (GB)</td>
<td>1,000 MB or 1,000(^3) bytes</td>
</tr>
<tr>
<td>1 terabyte (TB)</td>
<td>1,000 GB or 1,000(^4) bytes</td>
</tr>
<tr>
<td>1 petabyte (PB)</td>
<td>1,000 TB or 1,000(^5) bytes</td>
</tr>
<tr>
<td>1 exabyte (EB)</td>
<td>1,000 PB or 1,000(^6) bytes</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Logical capacity unit</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 block</td>
<td>512 bytes</td>
</tr>
<tr>
<td>1 KB</td>
<td>1,024 (2^{10}) bytes</td>
</tr>
<tr>
<td>1 MB</td>
<td>1,024 KB or 1,024(^2) bytes</td>
</tr>
<tr>
<td>1 GB</td>
<td>1,024 MB or 1,024(^3) bytes</td>
</tr>
<tr>
<td>1 TB</td>
<td>1,024 GB or 1,024(^4) bytes</td>
</tr>
<tr>
<td>1 PB</td>
<td>1,024 TB or 1,024(^5) bytes</td>
</tr>
<tr>
<td>1 EB</td>
<td>1,024 PB or 1,024(^6) bytes</td>
</tr>
</tbody>
</table>

### Accessing product documentation

The Device Manager and Tiered Storage Manager user documentation is available on the Hitachi Data Systems Portal: [https://portal.hds.com](https://portal.hds.com). 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 Portal is the destination for technical support of your current or previously-sold storage systems, midrange and enterprise servers, and combined solution offerings. The Hitachi Data Systems customer support staff is available 24 hours a day, seven days a week. If you need technical support, log on to the Hitachi Data Systems Support Portal for contact information: [https://portal.hds.com](https://portal.hds.com).

Hitachi Data Systems Community is a new global online community for HDS customers, partners, independent software vendors, employees, and prospects. It is an open discussion among these groups about the HDS portfolio of products and services. It is the destination to get answers, discover insights, and make connections. The HDS Community complements
our existing Support Portal and support services by providing an area where you can get answers to non-critical issues and questions. **Join the conversation today!** Go to community.hds.com, register, and complete your profile.

**Comments**

Please send us your comments on this document: 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!**
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
- Related products
- System requirements for managing copy pairs
- System configuration for managing copy pairs
- 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.

**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

---

**Figure 1-1 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.

Pair management server
- The computer for centrally managing the status and configuration 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, Universal Storage Platform V/VM, and Hitachi USP.

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.
- Enterprise-class storage system and HUS VM
General terms for the following storage systems: VSP G1000, Virtual Storage Platform, Universal Storage Platform V/VM, Hitachi USP, and HUS VM. SVP, the computer that manages these storage systems, is built-in.

Storage Navigator (a management tool for storage systems):
Used to set up storage systems and view their settings on a management client via Device Manager.

The name of the storage system management tool differs depending on the storage system.
For VSP G1000: Device Manager - Storage Navigator
For systems other than VSP G1000: Storage Navigator
This tool is referred to as "Storage Navigator" unless there is a need to distinguish Device Manager - Storage Navigator and Storage Navigator.

- Midrange storage system
  A general term for the following storage systems: HUS100, Hitachi AMS2000, Hitachi SMS, and Hitachi AMS/WMS.

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.
- 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.
- 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, Virtual Storage Platform, Universal Storage Platform V/VM, Hitachi USP and HUS VM come equipped with a service processor, which is usually abbreviated as SVP.

The following two Ethernet adapters are available for the SVP:

- Private (internal) Ethernet LAN adapter
  Used for communication only 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 1-2 Separate management LAN with a firewall configuration on page 1-7, 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.

Caution: If you use Storage Navigator to operate any of the following storage systems from the Device Manager GUI, Java Web Start and the browser on the management client directly communicate with the storage system: VSP G1000, Virtual Storage Platform, Universal Storage Platform V/VM, Hitachi USP, and HUS VM. For this reason, if the storage system and the management client are on different networks, you must set up the networks so that the storage system and the management client can communicate directly with each other.

* Device Manager does not support NAT.

Figure 1-2 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 1-1 Maximum number of management resources

<table>
<thead>
<tr>
<th>Resource</th>
<th>Maximum for the Device Manager server</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of LDEVs(^1)</td>
<td>1,000,000</td>
</tr>
<tr>
<td>Total of number of LDEVs and paths(^2)</td>
<td>5,000,000</td>
</tr>
</tbody>
</table>

Note:
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 topics
- Changing Device Manager server properties on page A-4
- server.cim.support.job on page A-10
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 hicommmand.sh file.

Information to collect in advance

- Number of LDEVs to be managed

<table>
<thead>
<tr>
<th>Table 1-2 Appropriate memory heap size for the Device Manager server</th>
</tr>
</thead>
<tbody>
<tr>
<td>Managed resource</td>
</tr>
<tr>
<td>-----------------------</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Number of LDEVs per storage system</td>
</tr>
</tbody>
</table>

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

Set a memory heap size according to the number of file server clusters and the number of file servers as shown below:

- When managing one file server that has one cluster or is in a non-cluster configuration
  Set the memory heap size to 1024MB.
- When managing two or more file servers that have at least two clusters or are in a non-cluster configuration
  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.

To change the memory heap size:

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.
   - In Windows: Specify an appropriate memory heap size for JVM_XOPT_HEAP_MAX using the following format: JVM_XOPT_HEAP_MAX=-Xmxnew-setting-value m
   - In Linux: 
Specify an appropriate memory heap size for the -Xmx option of the java command specified in the script for the start option.

This example shows how to change the value from 512 MB to 1024 MB:

Before: java -Xmx512m -classpath ...
After: java -Xmx1024m -classpath ...

3. Restart the Hitachi Command Suite product services.

Related topics
• Starting the Hitachi Command Suite services on page 8-4
• Stopping the Hitachi Command Suite services on page 8-5

Changing the JDK of management servers

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

Operations to complete in advance
• Check the JDK for Hitachi Command Suite products
  For details, see Hitachi Command Suite System Requirements.

To change the JDK:

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 Agent and the Tuning Manager servers (If the Tuning Manager API is used)

4. If the system is linked with Tuning Manager, edit the javavm.ini file.

5. Start the services of Hitachi Command Suite products.

6. 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.

---

**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.

---

**Related topics**

- [Importing a certificate into the truststore for Hitachi Command Suite on page 4-71](#)
- [Starting the Hitachi Command Suite services on page 8-4](#)
- [Stopping the Hitachi Command Suite services on page 8-5](#)
- How to edit the javavm.ini file: *Hitachi Command Suite Tuning Manager Server Administration Guide*

---

**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.

---

**Operations to complete in advance**

- 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).

---

**Information to collect in advance**

Installation path of the Java execution environment to be used.
To change the Java execution environment used by Host Data Collector:

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.

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 topics
- Starting the Host Data Collector service on page 8-9
- Stopping the Host Data Collector service on page 8-9
- javapathlocation on page C-11

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>
<thead>
<tr>
<th>Hosts</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Open hosts</td>
<td>Normal host: An environment in which virtualization software is not installed</td>
</tr>
<tr>
<td></td>
<td>Virtual machine#: A virtual environment created by using virtualization software</td>
</tr>
<tr>
<td></td>
<td>Virtualization server: A physical environment in which virtualization software is installed</td>
</tr>
<tr>
<td>Mainframe hosts</td>
<td>Computers that use mainframe volumes</td>
</tr>
<tr>
<td>File servers</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Hitachi NAS Platform</td>
</tr>
<tr>
<td></td>
<td>Hitachi NAS Platform F</td>
</tr>
</tbody>
</table>

#: 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 1-4 Host management software supported by Device Manager**

<table>
<thead>
<tr>
<th>Host management software</th>
<th>Open host</th>
<th></th>
<th></th>
<th>Mainframe host</th>
<th>File server</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Normal host</td>
<td>Virtual machine</td>
<td>Virtualization server</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Host Data Collector*</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>Device Manager agent*</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>Mainframe Agent</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>File server management software</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>Y</td>
</tr>
</tbody>
</table>

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 or CLI are registered in Device Manager.

- 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.

**Related topics**

- Details about the hosts to be managed by the host management software: *Hitachi Command Suite System Requirements*

**Prerequisites for normal hosts**

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

⚠️ **Note:**

- If you use Host Data Collector or 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 Host Data Collector or 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 Host Data Collector or 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 normal hosts managed by Host Data Collector**

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 performed 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.
- 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)

**Related topics**

- How to set up Host Data Collector: *Hitachi Command Suite Installation and Configuration Guide*

**Prerequisites for normal hosts managed by Device Manager agent**

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.

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)

**Related topics**

- How to set up Device Manager agent: *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 or the Device Manager agent, you must perform environment setup of the virtual machines before registering them in Device Manager.

**Prerequisites for virtual machines managed by Host Data Collector**

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

**Figure 1-3 Environment settings on virtual machines (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.

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.
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 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 VMware ESX is used as the virtualization software)

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

- SSH is enabled.
- Settings have been performed so that you can log in as root via a remote SSH login with password authentication.
- In a configuration in which 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.
• 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:

```bash
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.

• In a configuration in which a virtual HBA is allocated for each virtual machine (by using NPIV HBAs), the following operations have already been performed:
  o Registering virtualization servers that operate in the same physical environment in Device Manager
  o 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.

**Related topics**

- Chapter 11, Troubleshooting on page 11-1

**Prerequisites for virtual machines managed by Device Manager agent**

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.

Note that the environment settings that must be specified differ depending on the HBA configuration.
If a virtual HBA is allocated to each virtual machine (if an NPIV HBA is used) (recommended)
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 ESX 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.

If an HBA is allocated for each virtual machine
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.
- For virtual machines running the AIX OS, set the `ODMDIR` environment variable.

- If an HBA is shared by multiple virtual machines
  The Device Manager agent is installed and managed on only one virtual machine.
  - The Device Manager agent cannot be installed on each virtual machine.
  - For virtual machines running the AIX OS, set the `ODMDIR` environment variable.

**Related topics**

- How to set up Device Manager agent: *Hitachi Command Suite Installation and Configuration Guide*

**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)

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

Figure 1-5 Operation workflow for allocating volumes to virtual machines (when allocating a virtual HBA to each virtual machine)
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.

**Configuration in which an HBA is allocated for each virtual machine**

![Diagram of HBA allocation for each virtual machine]

**Figure 1-6 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.

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

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.
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 topics**

- How to register a virtualization server: *Hitachi Command Suite User Guide* or *Hitachi Command Suite CLI Reference Guide*

**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.

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.

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
```

**Related topics**
- How to refresh the virtualization server or virtual machine information: Hitachi Command Suite User Guide or Hitachi Command Suite CLI Reference Guide

**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 ESX 4.x, VMware ESXi 4.x or VMware ESXi 5.x is the virtualization server that can be managed by Host Data Collector.
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.

**Related topics**
- Chapter 11, Troubleshooting on page 11-1

**Operation workflow for managing virtualization servers**

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

Note the following when operating virtualization servers:

- To check the latest volume information of virtualization servers, manually refresh information for each virtualization server 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.

![Operation workflow of managing a mainframe host diagram]

**Related topics**
- How to specify environment settings from the Device Manager CLI: *Hitachi Command Suite CLI Reference Guide*
- How to specify environment settings for Mainframe Agent: *Mainframe Agent Installation and Configuration Guide*

**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 Hitachi NAS Platform family**

To manage Hitachi NAS Platform using Device Manager, the management server must be in a system configuration in which communication with SMU and Admin services EVS can be performed.
Figure 1-11 Environment settings for Hitachi NAS Platform

- Locate the management server on a network that can communicate with SMU.
  To use the Device Manager GUI to create file systems for firmware version 10.2.3071 or later of Hitachi NAS Platform, set up the system so that it can also communicate with Admin services EVS.
- Make sure that the version of SMU 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 Hitachi 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.
  - 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.

**Related topics**
- How to configure the file server using SMU: See the documentation for Hitachi NAS Platform family.

**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 1-5 Installation conditions of Hitachi File Services Manager**

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

Legend:
- **Y:** You can perform the operation.
N: You cannot perform the operation.

Related topics

- Setting up alerts on page 6-3
- How to install Hitachi File Services Manager and the environment settings: The Hitachi Data Ingestor or Hitachi NAS Platform F manual.
- Prerequisite version of Hitachi File Services Manager: Hitachi Command Suite System Requirements

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.

![Diagram showing the operation workflow of managing file servers]

Note: For details about the storage systems that can be used for file servers, see the documentation of the file servers.

Related topics

- How to specify settings from the Device Manager GUI or CLI: Hitachi Command Suite User Guide or Hitachi Command Suite CLI Reference Guide
• How to specify settings for the file server management software: Documentation for the file servers

**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 Hitachi NAS Platform, file server information is applied to the Device Manager database every day at 3:00 AM.
  
  When the SMU version is 10.2.3071 or later:
  You can perform a synchronization operation in the SMU Hitachi Device Managers window to apply the latest Hitachi 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 Hitachi NAS Platform is applied to the Device Manager database (you do not need to delete anything).

• 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.

• If Hitachi 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 Hitachi NAS Platform matches the host name of a file server or a normal host that has already been registered in Device Manager, the Hitachi NAS Platform will be registered as a file server. (The information of the database will be overwritten.)

**Related topics**

• [Changing Device Manager server properties on page A-4](#)

• [server.http.entity.maxLength on page A-8](#)

• How to specify settings for SMU: Documentation for Hitachi NAS Platform family

• How to specify settings for Hitachi File Services Manager: Documentation for Hitachi Data Ingestor or Hitachi NAS Platform F

**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.

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:

- GUI
By launching the Replication Manager GUI from the Device Manager GUI, you can define copy pairs or change pair statuses. 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.

- **CLI**
  You can use the Device Manager CLI to define copy pairs or change pair statuses.

**Tip:** In Device Manager, you can configure a high availability system by duplicating data on two units of the storage systems (VSP G1000) by using a global-active device functionality. For details on system configuration and requirements to configure high availability system, see Configuring a high availability system on page 1-65.

## System configuration for managing copy pairs

Device Manager supports the following four types of system configurations to manage copy pairs.

- **Local management method**
  In this configuration, copy pairs are managed for each host by connecting a command device to each application server via Fibre Channel.

- **Configuration that uses a pair management server (central management method)**
  In this configuration, copy pairs are centrally managed by connecting a command device to a computer other than application servers (pair management 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.

- **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, 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 machine on which you execute the CCI command 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 topics

- [Notes on managing copy pairs on page 1-60](#)
- [Operation workflow for secure communication between a management server and Device Manager agent on page 4-20](#)
- [server.agent.rm.userAuthentication on page D-20](#)

### System configuration for using the local management method to manage copy pairs

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

---

(Legend)
---: indicates that LUN security is set
#: No configuration definition file is necessary for a Thin Image copy pair defined in a snapshot group.

Figure 1-13 Example of a system configuration for managing copy pairs (local management)
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.
- 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 (application 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.
- From the P-VOL or S-VOL, LUN security must be set for the host (application 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.

**Caution:** Note the following when a command device whose authentication mode is enabled is connected to a host (application 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, 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) 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).

When a virtual storage machine is created to manage resources in VSP G1000:

- 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 topics

- Storage system requirements for managing copy pairs on page 1-53
- Prerequisite version of the Device Manager agent for managing copy pairs on page 1-58
- Changing Device Manager agent properties on page D-2
- Properties for command devices connected to Device Manager agent (rgcmddev.properties file) on page D-23
- How to install CCI: CCI documentation

System configuration for using the central management method to manage copy pairs

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

Figure 1-14 Example of a system configuration for managing copy pairs (central management method)
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.

- 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.

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, 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) 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).

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:

- 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 topics**

- [Storage system requirements for managing copy pairs on page 1-53](#)
System configuration for using a virtual command device server configuration to manage copy pairs

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

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

- A host that recognizes the P-VOL

![Diagram of system configuration]

(Legend): ------ indicates that LUN security is set.

Figure 1-15 Example of a system configuration for managing copy pairs (virtual command device server configuration)
A host that recognizes the S-VOL

Host (application 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.
- If there are multiple NICs on the host (application 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.
- 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 \((34000 + \text{instance-number+1})\) must be used for the CCI initiator port of the application 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: \text{value-specified-by-the-agent.rm.horcmInstance-property}
    
    Minimum value: \((\text{value-specified-by-the-agent.rm.horcmInstance-property}) - (\text{value-specified-by-the-agent.rm.horcmRange-property}) + 1\)
  - 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 host (virtual command device server):
  - If multiple command devices in the same storage system are connected to the host, 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 (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 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.

Resource group conditions (when managing partitioned resources in VSP G1000, 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) are connected to the host (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).

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:

○ 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 topics**

- Storage system requirements for managing copy pairs on page 1-53
- Prerequisite version of the Device Manager agent for managing copy pairs on page 1-58
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.

Management server conditions:

Figure 1-16 Example of a system configuration for managing copy pairs (when copy pairs are defined in a configuration definition file)
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 conditions:

- 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.

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.

Resource group requirements (when managing partitioned resources in VSP G1000, 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:

- 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 topics**

- [Storage system requirements for managing copy pairs on page 1-53](#)
- [Prerequisite version of the Device Manager agent for managing copy pairs on page 1-58](#)
- How to install CCI: [CCI documentation](#)

**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.
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.
- The Replication Manager server and the Device Manager server can communicate using SSL.
- Either of the conditions below is satisfied on the management server.

Figure 1-17 Example of a system configuration for managing copy pairs (when copy pairs are defined as a device group)
- 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.

Resource group requirements (when managing partitioned resources in VSP
G1000, 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:
- 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 topics**

- Storage system requirements for managing copy pairs on page 1-53
- Prerequisite version of the Device Manager agent for managing copy pairs on page 1-58
- Operation workflow for secure communication between a Device Manager server and Replication Manager server on page 4-14
- Changing Device Manager agent properties on page D-2
- server.agent.rm.centralizePairConfiguration on page D-15
- server.agent.rm.ignorePairStatus on page D-20
- How to install CCI: CCI documentation

## Storage system requirements for managing copy pairs

Set up the environment in accordance with the storage system requirements.

### Table 1-6 Storage system requirements for managing copy pairs

<table>
<thead>
<tr>
<th>Storage system</th>
<th>Function</th>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>VSP G1000 Virtual Storage</td>
<td>Universal Replicator&lt;sup&gt;1&lt;/sup&gt;</td>
<td>• Prerequisite software for Universal Replicator must be installed and the license must be enabled.</td>
</tr>
<tr>
<td>Storage system</td>
<td>Function</td>
<td>Requirements</td>
</tr>
<tr>
<td>------------------------</td>
<td>-------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Universal Storage</td>
<td></td>
<td>• There must be a fibre-channel connection between the two ports used for an MCU-RCU path.</td>
</tr>
<tr>
<td>Platform V/VM</td>
<td></td>
<td>• The MCU port for an MCU-RCU path must be an Initiator port, and the RCU port must be an RCU Target port.</td>
</tr>
<tr>
<td>Hitachi USP</td>
<td></td>
<td>• The RCU and the MCU-RCU path must be registered in the MCU.</td>
</tr>
<tr>
<td>HUS VM</td>
<td></td>
<td>• The storage system cache or non-volatile memory must be sufficient.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Journal volumes must be registered in the journal group.</td>
</tr>
<tr>
<td>Note:</td>
<td></td>
<td>After configuring the ports, you need to refresh the storage system. If you need to increase the cache, contact maintenance personnel.</td>
</tr>
<tr>
<td>TrueCopy</td>
<td></td>
<td>• Prerequisite software for TrueCopy must be installed and the license must be enabled.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• There must be a fibre-channel connection between the two ports used for an MCU-RCU path.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The MCU port for an MCU-RCU path must be an Initiator port, and the RCU port must be an RCU Target port.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The RCU and the MCU-RCU path must be registered in the MCU.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The storage system cache or non-volatile memory must be sufficient.</td>
</tr>
<tr>
<td>Note:</td>
<td></td>
<td>After configuring the ports, you need to refresh the storage system. If you need to increase the cache, contact maintenance personnel.</td>
</tr>
<tr>
<td>ShadowImage</td>
<td></td>
<td>Prerequisite software for ShadowImage must be installed and the license must be enabled.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>To be used as an S-VOL, a V-VOL (a special LU) must be prepared in advance.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Perform the preparations in the following order:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>o Create a pool.</td>
</tr>
<tr>
<td>Copy-on-Write Snapshot</td>
<td></td>
<td>• Prerequisite software for Copy-on-Write Snapshot must be installed and the license must be enabled.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• To be used as an S-VOL, a V-VOL (a special LU) must be prepared in advance.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Perform the preparations in the following order:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>o Create a pool.</td>
</tr>
<tr>
<td>Storage system</td>
<td>Function</td>
<td>Requirements</td>
</tr>
<tr>
<td>--------------------</td>
<td>------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Thin Image</td>
<td></td>
<td>• Prerequisite software for Thin Image must be installed and the license must be enabled.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• For Thin Image copy pairs defined in the snapshot group, you need to enable the authentication mode for the command devices.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• You also need to authenticate users by executing the <code>raidcom -login</code> command on the host.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• To be used as an S-VOL, a V-VOL (a special LU) must be prepared in advance.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Perform the preparations in the following order:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Create a pool.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Create a V-VOL.</td>
</tr>
<tr>
<td>HUS100</td>
<td>TrueCopy</td>
<td>• Prerequisite software for TrueCopy must be installed and the license must be enabled.</td>
</tr>
<tr>
<td>Hitachi AMS2000</td>
<td></td>
<td>• There must be a fibre-channel connection between the two ports used for a path.</td>
</tr>
<tr>
<td>Hitachi AMS/WMS</td>
<td></td>
<td>• The TrueCopy path must be configured. For HUS100 or Hitachi AMS2000, paths can be set from a storage system to multiple storage systems.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The system start attribute must be dual active mode.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• To use TrueCopy remote replication or TrueCopy Extended Distance with Hitachi AMS2000 or Hitachi AMS/WMS, or to use TrueCopy remote replication with HUS100, a DM-LU must be set up.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• To use TrueCopy Extended Distance with Hitachi AMS2000 or Hitachi AMS/WMS, a data pool must be set. The data pool can be shared with Copy-on-Write Snapshot.</td>
</tr>
<tr>
<td>Storage system</td>
<td>Function</td>
<td>Requirements</td>
</tr>
<tr>
<td>----------------</td>
<td>------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• To use TrueCopy Extended Distance with HUS100, a DP pool must be created. Specify settings so that management data and differential data are stored in the same DP pool. The DP pool can be shared with Copy-on-Write Snapshot.</td>
</tr>
<tr>
<td>ShadowImage</td>
<td></td>
<td>• Prerequisite software for ShadowImage must be installed and the license must be enabled.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The system start attribute must be dual active mode.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• For HUS100, Hitachi AMS2000, or Hitachi AMS/WMS, a DM-LU must be set up.</td>
</tr>
<tr>
<td>Copy-on-Write Snapshot</td>
<td></td>
<td>• Prerequisite software for Copy-on-Write Snapshot must be installed and the license must be enabled.</td>
</tr>
</tbody>
</table>
|                |                              | • To be used as an S-VOL, a V-VOL (a special LU) must be prepared in advance. Perform the preparations in the following order: For HUS100  
|                |                              |   a. Create a DP pool. Specify settings so that management data and differential data are stored in the same DP pool. The DP pool can be shared with TrueCopy Extended Distance DP pools.  
|                |                              |   b. Create a V-VOL.  
|                |                              |   For Hitachi AMS2000 or Hitachi AMS/WMS  
|                |                              |   a. Create a data pool. The data pool can be shared with TrueCopy Extended Distance data pools.  
|                |                              |   b. Create a V-VOL.  
|                |                              | • For Hitachi AMS2000, or Hitachi AMS/WMS, a DM-LU must be set up. |
| Hitachi SMS    | ShadowImage                  | • Prerequisite software for ShadowImage must be installed and the license must be enabled. |
|                |                              | • The system start attribute must be the dual active mode.                 |
|                |                              | • A DM-LU must be set up.                                                  |
## Storage system Function Requirements

<table>
<thead>
<tr>
<th>Storage system</th>
<th>Function</th>
<th>Requirements</th>
</tr>
</thead>
</table>
|                | Copy-on-Write Snapshot | • Prerequisite software for Copy-on-Write Snapshot must be installed and the license must be enabled.  
• To be used as an S-VOL, a V-VOL (a special LU) must be prepared in advance.  
Performance the preparations in the following order:  
- Create a data pool.  
- Create a V-VOL.  
• A DM-LU must be set up. |

### #1:
For mainframe volume copy pairs, you can only check the configuration by using the Device Manager CLI. There are no storage system requirements for checking the copy pair configuration by using the Device Manager CLI.

### #2:
The settings specified in TrueCopy can be shared with Universal Replicator. However, in Universal Replicator, the settings must be specified for both storage systems used for the P-VOL and the S-VOL.

### Caution:
- After the storage system has been configured as required, 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, Virtual Storage Platform, or HUS VM logical units to create a copy pair, do not use logical units associated with a device group.

### Related topics
- [System configuration for using the local management method to manage copy pairs](#)
- [System configuration for using the central management method to manage copy pairs](#)
- [System configuration for using a virtual command device server configuration to manage copy pairs](#)
- [System configuration for using an SVP configuration to manage copy pairs (when copy pairs are defined in a configuration definition file)](#)

---

**System configuration and requirements**  
Hitachi Command Suite Administrator Guide  
1-57
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 1-7 Device Manager agent requirements for managing copy pairs by using the GUI**

<table>
<thead>
<tr>
<th>Storage system</th>
<th>Device Manager agent version</th>
</tr>
</thead>
<tbody>
<tr>
<td>VSP G1000</td>
<td>8.0 or later</td>
</tr>
<tr>
<td>Virtual Storage Platform</td>
<td>7.0 or later</td>
</tr>
<tr>
<td>Universal Storage Platform V/VM</td>
<td>6.0 or later</td>
</tr>
<tr>
<td>Hitachi USP</td>
<td>6.0 or later</td>
</tr>
<tr>
<td>HUS VM</td>
<td>7.3.1 or later</td>
</tr>
<tr>
<td>HUS100</td>
<td>7.2.0 or later</td>
</tr>
<tr>
<td>Hitachi AMS2000</td>
<td>6.0 or later</td>
</tr>
<tr>
<td>Hitachi SMS</td>
<td>6.0 or later</td>
</tr>
<tr>
<td>Hitachi AMS/WMS</td>
<td>6.0 or later</td>
</tr>
</tbody>
</table>

**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 1-8 Device Manager agent requirements for managing copy pairs by using the CLI**

<table>
<thead>
<tr>
<th>Program</th>
<th>Operation from Device Manager</th>
<th>Device Manager agent version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Universal Replication</td>
<td>Display the status</td>
<td>4.0 or later</td>
</tr>
<tr>
<td></td>
<td>Display the status (3DR)</td>
<td>5.5 or later</td>
</tr>
<tr>
<td></td>
<td>Change the status</td>
<td>5.6 or later</td>
</tr>
<tr>
<td></td>
<td>Change the status (3DR)</td>
<td>5.5 or later</td>
</tr>
</tbody>
</table>
Program | Operation from Device Manager | Device Manager agent version#
--- | --- | ---
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
 | 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

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 1-9 Device Manager agent version required for each storage system model when managing copy pairs by using the CLI**

<table>
<thead>
<tr>
<th>Storage system model</th>
<th>Device Manager agent version</th>
</tr>
</thead>
<tbody>
<tr>
<td>VSP G1000</td>
<td>8.0 or later</td>
</tr>
<tr>
<td>Hitachi Virtual Storage Platform</td>
<td>7.0 or later</td>
</tr>
<tr>
<td>Hitachi Universal Storage Platform V</td>
<td>5.7 or later</td>
</tr>
<tr>
<td>Hitachi Universal Storage Platform VM</td>
<td>5.8 or later</td>
</tr>
<tr>
<td>Hitachi Universal Storage Platform</td>
<td>3.5 or later</td>
</tr>
<tr>
<td>Hitachi Network Storage Controller</td>
<td>4.0 or later</td>
</tr>
<tr>
<td>Hitachi Unified Storage VM</td>
<td>7.3.1 or later</td>
</tr>
<tr>
<td>Hitachi Unified Storage 150</td>
<td>7.2.0 or later</td>
</tr>
<tr>
<td>Hitachi Unified Storage 130</td>
<td></td>
</tr>
</tbody>
</table>
### Storage System Model

<table>
<thead>
<tr>
<th>Storage System Model</th>
<th>Device Manager Agent Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hitachi Unified Storage 110</td>
<td></td>
</tr>
<tr>
<td>Hitachi Adaptable Modular Storage AMS2500 (H/W Rev. 0100)</td>
<td>6.0 or later</td>
</tr>
<tr>
<td>Hitachi Adaptable Modular Storage AMS2300 (H/W Rev. 0100)</td>
<td></td>
</tr>
<tr>
<td>Hitachi Adaptable Modular Storage AMS2100 (H/W Rev. 0100)</td>
<td></td>
</tr>
<tr>
<td>Hitachi Adaptable Modular Storage AMS2500 (H/W Rev. 0200)</td>
<td>6.4 or later</td>
</tr>
<tr>
<td>Hitachi Adaptable Modular Storage AMS2300 (H/W Rev. 0200)</td>
<td></td>
</tr>
<tr>
<td>Hitachi Adaptable Modular Storage AMS2100 (H/W Rev. 0200)</td>
<td></td>
</tr>
<tr>
<td>Hitachi Adaptable Modular Storage AMS2010</td>
<td></td>
</tr>
<tr>
<td>Hitachi Simple Modular Storage 100</td>
<td>6.0 or later</td>
</tr>
<tr>
<td>Hitachi Simple Modular Storage 110</td>
<td>6.1 or later</td>
</tr>
<tr>
<td>Hitachi Adaptable Modular Storage 1000</td>
<td>5.0 or later</td>
</tr>
<tr>
<td>Hitachi Adaptable Modular Storage 500</td>
<td>4.2 or later</td>
</tr>
<tr>
<td>Hitachi Adaptable Modular Storage 200</td>
<td></td>
</tr>
<tr>
<td>Hitachi Workgroup Modular Storage 100</td>
<td>4.1 or later</td>
</tr>
</tbody>
</table>

### Related Topics

- [System configuration for using the local management method to manage copy pairs on page 1-36](#)
- [System configuration for using the central management method to manage copy pairs on page 1-40](#)
- [System configuration for using a virtual command device server configuration to manage copy pairs on page 1-44](#)
- [System configuration for using an SVP configuration to manage copy pairs (when copy pairs are defined in a configuration definition file) on page 1-48](#)
- [System configuration for using an SVP configuration to manage copy pairs (when copy pairs are defined as a device group) on page 1-50](#)

### Notes on Managing Copy Pairs

Note the following when managing copy pairs:

- [System configuration for using the local management method to manage copy pairs on page 1-36](#)
- [System configuration for using the central management method to manage copy pairs on page 1-40](#)
- [System configuration for using a virtual command device server configuration to manage copy pairs on page 1-44](#)
- [System configuration for using an SVP configuration to manage copy pairs (when copy pairs are defined in a configuration definition file) on page 1-48](#)
- [System configuration for using an SVP configuration to manage copy pairs (when copy pairs are defined as a device group) on page 1-50](#)
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 01-32-03/XX or earlier and the above rules are not followed, you need to manually recreate the existing configuration definition files.

For details about configuration definition files, see Configuration definition file for managing copy pairs on page 10-29.

In a configuration where virtual IDs are used to make serial numbers overlap among storage systems in VSP G1000

- If you are using CCI 01-32-03/XX or earlier, connect the command devices for each storage system to different hosts.
- If you are using CCI 01-32-03/XX or later, use different hosts 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

- 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.
  If the microcode version for VSP G1000 is 80-02-01-XX/XX or later, 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. However, when a command device with authentication mode enabled and a command device with authentication mode disabled both exist in VSP G1000, and are connected to the same host, authentication mode must be enabled for all the command devices recognized by the same host.
  A command device with its authentication mode enabled must be connected to the host 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.horcconfigfile.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.horcconfigfile.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.horcconfigfile.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 host that manages the P-VOL of the copy pair and the configuration definition file on the host 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 host 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 installed on the host is 05-60 or earlier:
  Each copy pair on the host must have a unique combination of the following items:
  Group name
  Pair name

• If the version of the Device Manager agent installed on the host is 05-70 or later:
  Each copy pair on the host 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 host 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 host that manages copy pairs.

Related topics

• Managing copy pairs on page 10-7
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 (VSP G1000) by using global-active device functionality and then making it possible to receive I/O from both units of the storage system.

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.
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

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

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
```

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

- Both the primary site and secondary site storage systems must be VSP G1000.
- 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, 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 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):

- Device Manager agent version 8.0.1 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 HDP volumes or HDT volumes.
- Both the P-VOL and S-VOL must be opened volumes.
- 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.

If 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.

---

**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 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.
- The volume does not have data that is being migrated by using the nondisruptive migration functionality.

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 topics**

- Properties for command devices connected to Device Manager agent *(rgcmddev.properties file)* on page D-23

**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.
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.

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 2-1 Ports used by Common Component

<table>
<thead>
<tr>
<th>Port number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>22015/tcp</td>
<td>Used for accessing the HBase 64 Storage Mgmt Web Service when communicating with management clients (GUI). This port number can be changed.</td>
</tr>
<tr>
<td>22016/tcp</td>
<td>Used for accessing the HBase 64 Storage Mgmt Web Service when performing SSL communication with management clients (GUI). This port number can be changed.</td>
</tr>
<tr>
<td>22017/tcp</td>
<td>Used internally for Common Component communication (communication with the Web server). This port number can be changed.</td>
</tr>
<tr>
<td>22018/tcp</td>
<td>Used internally for Common Component communication (receiving a termination message from the Web server). This port number can be changed.</td>
</tr>
<tr>
<td>22019/tcp to 22024/tcp</td>
<td>Used when Tuning Manager is installed. This port number can be changed.</td>
</tr>
<tr>
<td>22025/tcp</td>
<td>Used internally for Common Component communication (communication with the Web server). This port number can be changed.</td>
</tr>
<tr>
<td>22026/tcp</td>
<td>Used internally for Common Component communication (receiving a termination message from the Web server). This port number can be changed.</td>
</tr>
<tr>
<td>22027/tcp 22028/tcp</td>
<td>Used when Compute Systems Manager is installed. This port number can be changed.</td>
</tr>
<tr>
<td>22029/tcp 22030/tcp</td>
<td>Reserved by Common Component.</td>
</tr>
<tr>
<td>Port number</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>-------------</td>
</tr>
<tr>
<td>22031/tcp</td>
<td>Used internally for Common Component communication (single sign-on). This port number can be changed.</td>
</tr>
<tr>
<td>22032/tcp</td>
<td>Used internally for Common Component communication (HIRDB). This port number can be changed.</td>
</tr>
<tr>
<td>22033/tcp</td>
<td>Used internally for Common Component communication (communication with the Web server). This port number can be changed.</td>
</tr>
<tr>
<td>22034/tcp</td>
<td>Used internally for Common Component communication (receiving a termination message from the Web server). This port number can be changed.</td>
</tr>
</tbody>
</table>

#: 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 topics**
- [Changing ports used by Common Component](#)
- [Registering firewall exceptions for Device Manager and Tiered Storage Manager](#)
- [Editing the user_httpsd.conf file](#)
- How to change the ports when Tuning Manager and Compute Systems Manager are installed: The manual for each product

### 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 2-2 Ports used by the Device Manager server**

<table>
<thead>
<tr>
<th>Port number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>162/udp</td>
<td>Used for receiving SNMP traps from storage systems (VSP G1000, Virtual Storage Platform, Universal Storage Platform V/VM, Hitachi USP, and HUS VM) and file servers (Hitachi Data Ingestor and Hitachi NAS Platform F). 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.</td>
</tr>
<tr>
<td>427/tcp</td>
<td>Used for communication with a CIM client (service discovery).</td>
</tr>
<tr>
<td>Port number</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>-------------</td>
</tr>
<tr>
<td>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.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Port number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2001/tcp*</td>
<td>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.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Port number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2443/tcp</td>
<td>Used internally for Device Manager server communication and for SSL communication with management clients (via the GUI or the CLI). You can change this port number by modifying the server.https.port property in the server.properties file of the Device Manager server.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Port number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>5983/tcp</td>
<td>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.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Port number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>5988/tcp</td>
<td>Used for non-SSL communication with a CIM client (Object operation). This port number can be changed.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Port number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>5989/tcp</td>
<td>Used for SSL communication with a CIM client (Object operation). This port number can be changed.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Port number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>23055/tcp</td>
<td>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.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Port number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>24230/tcp</td>
<td>Used by HiRDB. You can change this port number by using the htmsetup command.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Port number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any/tcp</td>
<td>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.</td>
</tr>
</tbody>
</table>

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

- Registering firewall exceptions for Device Manager and Tiered Storage Manager on page 2-15
- Specifying the settings for remote connection to the Tuning Manager server and the port number (hmtsetup command) on page 5-18
- Setting up the config.xml and configforclient.xml files on page 5-19
- Changing CIM/WBEM port numbers on page 7-6
- Changing Device Manager server properties on page A-4
  - server.http.port on page A-6
  - server.https.port on page A-7
  - server.rmi.port on page A-8
  - server.smisclient.indication.port on page A-15

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>
<thead>
<tr>
<th>Port number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>20352/tcp</td>
<td>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.</td>
</tr>
<tr>
<td>24500/tcp</td>
<td>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.</td>
</tr>
</tbody>
</table>

Related topics

- Changing Tiered Storage Manager server properties on page B-2
- server.rmi.port on page B-4
- server.rmi.security.port on page B-4

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 2-4 Ports used by Host Data Collector

<table>
<thead>
<tr>
<th>Port number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>22098/tcp</td>
<td>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.</td>
</tr>
<tr>
<td>22099/tcp</td>
<td>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.</td>
</tr>
<tr>
<td>22100/tcp</td>
<td>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.</td>
</tr>
<tr>
<td>22104/tcp</td>
<td>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.</td>
</tr>
<tr>
<td>22105/tcp</td>
<td>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.</td>
</tr>
<tr>
<td>22106/tcp</td>
<td>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.</td>
</tr>
<tr>
<td>22110/tcp</td>
<td>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.</td>
</tr>
<tr>
<td>22111/tcp to 22120/tcp</td>
<td>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.</td>
</tr>
</tbody>
</table>

**Related topics**

- Changing Host Data Collector properties on page C-2
- hdc.service.localport on page C-3
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 2-5 Ports used by Device Manager agent

<table>
<thead>
<tr>
<th>Port number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>24041/tcp</td>
<td>Used for communication with the Device Manager server. You can change the port by using the <code>server.agent.port</code> property in the <code>server.properties</code> file of the Device Manager agent.</td>
</tr>
<tr>
<td>24042/tcp</td>
<td>Used for communication with the Device Manager server. You can change the port by using the <code>server.http.port</code> property in the <code>server.properties</code> file of the Device Manager agent.</td>
</tr>
<tr>
<td>24043/tcp</td>
<td>Used internally for Device Manager agent communication. You can change the port by using the <code>server.http.localPort</code> property in the <code>server.properties</code> file of the Device Manager agent.</td>
</tr>
</tbody>
</table>

Related topics

- Changing Device Manager agent properties on page D-2
- `server.agent.port` on page D-11
- `server.http.localPort` on page D-11
- `server.http.port` on page D-11

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>
<thead>
<tr>
<th>Target storage system</th>
<th>Port number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VSP G1000</td>
<td>80/tcp</td>
<td>Used for communication with management clients (GUI). This port number cannot be changed.</td>
</tr>
<tr>
<td></td>
<td>443/tcp</td>
<td>Used for starting Storage Navigator by SSL from management clients (GUI). This port number cannot be changed.</td>
</tr>
<tr>
<td></td>
<td>1099/tcp</td>
<td>Used for communication with the management server or management clients (GUI). This port number cannot be changed.</td>
</tr>
<tr>
<td></td>
<td>51099/tcp</td>
<td>Used for communication with the management server or management clients (GUI). This port number cannot be changed.</td>
</tr>
<tr>
<td></td>
<td>51100/tcp</td>
<td>Used for communication with the management server or management clients (GUI). This port number cannot be changed.</td>
</tr>
<tr>
<td>Universal Storage Platform V/VM</td>
<td>80/tcp</td>
<td>Used for communication with management clients (GUI). This port number cannot be changed.</td>
</tr>
<tr>
<td></td>
<td>443/tcp</td>
<td>Used for starting Element Manager by SSL from management clients (GUI). This port number cannot be changed.</td>
</tr>
<tr>
<td></td>
<td>1099/tcp</td>
<td>Used for communication with the management server or management clients (GUI). This port number cannot be changed.</td>
</tr>
<tr>
<td></td>
<td>51099/tcp</td>
<td>Used for communication with the management server or management clients (GUI). This port number cannot be changed.</td>
</tr>
<tr>
<td></td>
<td>51100/tcp</td>
<td>Used for communication with the management server or management clients (GUI). This port number cannot be changed.</td>
</tr>
<tr>
<td>Hitachi USP</td>
<td>80/tcp</td>
<td>Used for communication with management clients (GUI). This port number cannot be changed.</td>
</tr>
<tr>
<td></td>
<td>443/tcp</td>
<td>Used for starting Element Manager by SSL from management clients (GUI). This port number cannot be changed.</td>
</tr>
<tr>
<td>Target storage system</td>
<td>Port number</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-------------</td>
<td>-------------</td>
</tr>
<tr>
<td></td>
<td>1099/tcp</td>
<td>Used for communication with the management server or management clients (GUI). This port number cannot be changed.</td>
</tr>
<tr>
<td></td>
<td>51099/tcp</td>
<td>Used for communication with the management server or management clients (GUI). This port number cannot be changed.</td>
</tr>
<tr>
<td>HUS VM</td>
<td>80/tcp</td>
<td>Used for communication with management clients (GUI). This port number cannot be changed.</td>
</tr>
<tr>
<td></td>
<td>443/tcp</td>
<td>Used for starting Element Manager by SSL. This port number cannot be changed.</td>
</tr>
<tr>
<td></td>
<td>1099/tcp</td>
<td>Used for communication with management clients (GUI). This port number cannot be changed.</td>
</tr>
<tr>
<td></td>
<td>51099/tcp</td>
<td>Used for communication with the management server. This port number cannot be changed.</td>
</tr>
<tr>
<td></td>
<td>51100/tcp</td>
<td>Used for communication with the management server. This port number cannot be changed.</td>
</tr>
<tr>
<td>Hitachi AMS/WMS</td>
<td>2000/tcp</td>
<td>Used for communication with the management server. This port number can be changed.</td>
</tr>
<tr>
<td></td>
<td>28355/tcp</td>
<td>Used for communication with the management server. This port number can be changed.</td>
</tr>
<tr>
<td>Hitachi AMS2000</td>
<td>2000/tcp</td>
<td>Used for non-SSL communication with the management server. This port number can be changed.</td>
</tr>
<tr>
<td></td>
<td>28355/tcp</td>
<td>Used for SSL communication with the management server. This port number can be changed.</td>
</tr>
<tr>
<td>Hitachi SMS</td>
<td>2000/tcp</td>
<td>Used for non-SSL communication with the management server. This port number can be changed.</td>
</tr>
<tr>
<td></td>
<td>28355/tcp</td>
<td>Used for SSL communication with the management server. This port number can be changed.</td>
</tr>
<tr>
<td>HUS100</td>
<td>2000/tcp</td>
<td>Used for non-SSL communication with the management server.</td>
</tr>
</tbody>
</table>
### Target storage system

<table>
<thead>
<tr>
<th>Port number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>28355/tcp</td>
<td>Used for SSL communication with the management server. This port number can be changed.</td>
</tr>
</tbody>
</table>

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.

**Related topics**

- How to change the port numbers and how to specify entries in the services file: Documentation for 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.

**To change the ports used by Common Component:**

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

Table 2-7 Port number settings files for Common Component

<table>
<thead>
<tr>
<th>Default port number</th>
<th>Settings files</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>22015/tcp</td>
<td>In Windows:</td>
<td>Listen</td>
</tr>
<tr>
<td></td>
<td><code>installation-folder-for-Hitachi-Command-Suite\Base64\uCPSB\httpsd\conf\user_httpsd.conf</code>#1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>In Linux:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>installation-directory-for-Hitachi-Command-Suite/Base64/HCPSB/httpsd/conf/user_httpsd.conf</code>#1</td>
<td></td>
</tr>
<tr>
<td>22016/tcp</td>
<td>In Windows:</td>
<td>VirtualHost host-name:port-number Listen#2</td>
</tr>
<tr>
<td></td>
<td><code>installation-folder-for-Hitachi-Command-Suite\Base64\uCPSB\httpsd\conf\user_httpsd.conf</code>#1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>In Linux:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>installation-directory-for-Hitachi-Command-Suite/Base64/HCPSB/httpsd/conf/user_httpsd.conf</code>#1</td>
<td></td>
</tr>
<tr>
<td>22017/tcp</td>
<td>In Windows:</td>
<td>worker.HiCommand64.port</td>
</tr>
<tr>
<td></td>
<td><code>installation-folder-for-Hitachi-Command-Suite\Base64\uCPSB\CC\web\redirector\workers.properties</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td>In Linux:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>installation-directory-for-Hitachi-Command-Suite/Base64/uCPSB/CC/web/redirector/workers.properties</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td>In Windows:</td>
<td>webserver.connector.ajp13.port</td>
</tr>
<tr>
<td></td>
<td><code>installation-folder-for-Hitachi-Command-Suite\Base64\uCPSB\CC\web\containers\HiCommand64\usrconf\usrconf.properties</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td>In Linux:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>installation-directory-for-Hitachi-Command-Suite/Base64/uCPSB/CC/web/containers/HiCommand64/usrconf/ usrconf.properties</code></td>
<td></td>
</tr>
<tr>
<td>22018/tcp</td>
<td>In Windows:</td>
<td>webserver.shutdown.port</td>
</tr>
<tr>
<td></td>
<td><code>installation-folder-for-Hitachi-Command-Suite\Base64\uCPSB\CC\web\containers\HiCommand64\usrconf\usrconf.properties</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td>In Linux:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>installation-directory-for-Hitachi-Command-Suite/Base64/uCPSB/CC/web/containers/HiCommand64/usrconf/ usrconf.properties</code></td>
<td></td>
</tr>
</tbody>
</table>

Network configuration

Hitachi Command Suite Administrator Guide 2-11
<table>
<thead>
<tr>
<th>Default port number</th>
<th>Settings files</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>installation-folder-for-Hitachi-Command-Suite\Base64\uCPSB\CC\web\containers\HiCommand64\usrconf\usrconf.properties</td>
<td>worker.DeviceManagerWebService.port</td>
<td></td>
</tr>
<tr>
<td>installation-directory-for-Hitachi-Command-Suite/Base64/ uCPSB/CC/web/containers/ HiCommand64/ usrconf/ usrconf.properties</td>
<td>worker.DeviceManagerWebService.port</td>
<td></td>
</tr>
<tr>
<td>In Linux:</td>
<td>worker.DeviceManagerWebService.port</td>
<td></td>
</tr>
<tr>
<td>In Windows:</td>
<td>worker.DeviceManagerWebService.port</td>
<td></td>
</tr>
<tr>
<td>In Linux:</td>
<td>worker.DeviceManagerWebService.port</td>
<td></td>
</tr>
<tr>
<td>22025/tcp</td>
<td>In Windows:</td>
<td>webserver.connector.ajp13.port</td>
</tr>
<tr>
<td>installation-folder-for-Hitachi-Command-Suite\Base64\uCPSB\CC\web\containers\DeviceManagerWebService\usrconf\usrconf.properties</td>
<td>webserver.connector.ajp13.port</td>
<td></td>
</tr>
<tr>
<td>In Linux:</td>
<td>webserver.connector.ajp13.port</td>
<td></td>
</tr>
<tr>
<td>In Windows:</td>
<td>webserver.connector.ajp13.port</td>
<td></td>
</tr>
<tr>
<td>In Linux:</td>
<td>webserver.connector.ajp13.port</td>
<td></td>
</tr>
<tr>
<td>22026/tcp</td>
<td>In Windows:</td>
<td>webserver.shutdown.port</td>
</tr>
<tr>
<td>installation-folder-for-Hitachi-Command-Suite\Base64\uCPSB\CC\web\containers\DeviceManagerWebService\usrconf\usrconf.properties</td>
<td>webserver.shutdown.port</td>
<td></td>
</tr>
<tr>
<td>In Linux:</td>
<td>webserver.shutdown.port</td>
<td></td>
</tr>
<tr>
<td>In Windows:</td>
<td>webserver.shutdown.port</td>
<td></td>
</tr>
<tr>
<td>In Linux:</td>
<td>webserver.shutdown.port</td>
<td></td>
</tr>
<tr>
<td>22031/tcp</td>
<td>installation-folder-for-Hitachi-Command-Suite\Base64\uCPSB\httpsd\conf\user_hss0_httpsd.conf</td>
<td>Listen 127.0.0.1:port-number</td>
</tr>
<tr>
<td>22032/tcp</td>
<td>installation-folder-for-Hitachi-Command-Suite\Base64\HDB\CONF\emb\HiRDB.ini</td>
<td>PDNAMEPORT</td>
</tr>
<tr>
<td>Default port number</td>
<td>Settings files</td>
<td>Location</td>
</tr>
<tr>
<td>---------------------</td>
<td>----------------</td>
<td>----------</td>
</tr>
<tr>
<td></td>
<td>In Linux:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>installation-directory-for-Hitachi-Command-Suite/Base64/HDB/conf/emb/HiRDB.ini</td>
<td></td>
</tr>
<tr>
<td></td>
<td>In Windows:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>installation-folder-for-Hitachi-Command-Suite\Base64\HDB\CONF\pdsys</td>
<td></td>
</tr>
<tr>
<td></td>
<td>In Linux:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>installation-directory-for-Hitachi-Command-Suite/Base64/HDB/conf/pdsys</td>
<td></td>
</tr>
<tr>
<td></td>
<td>In Windows:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>installation-folder-for-Hitachi-Command-Suite\Base64\database\work\def_pdsys</td>
<td></td>
</tr>
<tr>
<td></td>
<td>In Linux:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>installation-directory-for-Hitachi-Command-Suite/Base64/database/work/def_pdsys</td>
<td></td>
</tr>
<tr>
<td>22033/tcp</td>
<td>In Windows:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>installation-folder-for-Hitachi-Command-Suite\Base64\uCPSB\CC\web\redirector\workers.properties</td>
<td></td>
</tr>
<tr>
<td></td>
<td>In Linux:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>installation-directory-for-Hitachi-Command-Suite/Base64\uCPSB\CC\web\redirector\workers.properties</td>
<td></td>
</tr>
<tr>
<td></td>
<td>In Windows:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>installation-folder-for-Hitachi-Command-Suite\Base64\uCPSB\CC\web\containers\HBase64StgMgmtSSOSService\usrconf\usrconf.properties</td>
<td></td>
</tr>
<tr>
<td></td>
<td>In Linux:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>installation-directory-for-Hitachi-Command-Suite/Base64\uCPSB\CC\web\containers\HBase64StgMgmtSSOSService\usrconf\usrconf.properties</td>
<td></td>
</tr>
<tr>
<td>22034/tcp</td>
<td>In Windows:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>installation-folder-for-Hitachi-Command-Suite\Base64\uCPSB\CC\web\containers\HBase64StgMgmtSSOSService\usrconf\usrconf.properties</td>
<td></td>
</tr>
<tr>
<td></td>
<td>In Linux:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>installation-directory-for-Hitachi-Command-Suite/Base64\uCPSB\CC\web\containers\HBase64StgMgmtSSOSService\usrconf\usrconf.properties</td>
<td></td>
</tr>
<tr>
<td></td>
<td>In Windows:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>installation-folder-for-Hitachi-Command-Suite\Base64\uCPSB\CC\web\redirector\workers.properties</td>
<td></td>
</tr>
<tr>
<td></td>
<td>In Linux:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>installation-directory-for-Hitachi-Command-Suite/Base64\uCPSB\CC\web\redirector\workers.properties</td>
<td></td>
</tr>
<tr>
<td></td>
<td>In Windows:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>installation-folder-for-Hitachi-Command-Suite\Base64\uCPSB\CC\web\containers\HBase64StgMgmtSSOSService\usrconf\usrconf.properties</td>
<td></td>
</tr>
<tr>
<td></td>
<td>In Linux:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>installation-directory-for-Hitachi-Command-Suite/Base64\uCPSB\CC\web\containers\HBase64StgMgmtSSOSService\usrconf\usrconf.properties</td>
<td></td>
</tr>
<tr>
<td></td>
<td>In Linux:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>installation-directory-for-Hitachi-Command-Suite/Base64\uCPSB\CC\web\containers\HBase64StgMgmtSSOSService\usrconf\usrconf.properties</td>
<td></td>
</tr>
<tr>
<td></td>
<td>In Windows:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>installation-folder-for-Hitachi-Command-Suite\Base64\uCPSB\CC\web\containers\HBase64StgMgmtSSOSService\usrconf\usrconf.properties</td>
<td></td>
</tr>
<tr>
<td></td>
<td>In Linux:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>installation-directory-for-Hitachi-Command-Suite/Base64\uCPSB\CC\web\containers\HBase64StgMgmtSSOSService\usrconf\usrconf.properties</td>
<td></td>
</tr>
<tr>
<td></td>
<td>In Linux:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>installation-directory-for-Hitachi-Command-Suite/Base64\uCPSB\CC\web\containers\HBase64StgMgmtSSOSService\usrconf\usrconf.properties</td>
<td></td>
</tr>
</tbody>
</table>

Network configuration

Hitachi Command Suite Administrator Guide
<table>
<thead>
<tr>
<th>Default port number</th>
<th>Settings files</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>installation-directory-for-Hitachi-Command-Suite/Base64/ Hayes64StgMgmtSSOService/usrconf/ usrconf.properties</td>
<td></td>
</tr>
</tbody>
</table>

#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:** 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.

**Related topics**

- [Ports used by Common Component on page 2-2](#)
- [Changing the URL for accessing Hitachi Command Suite products (hcmds64chgurl command) on page 2-41](#)
- [Editing the `user_httpsd.conf` file on page 4-36](#)
- [Changing pop-up blocker settings on page 4-67](#)
- [Settings for using Element Manager on page 5-3](#)
- [Starting the Hitachi Command Suite services on page 8-4](#)
- [Stopping the Hitachi Command Suite services on page 8-5](#)
- [Changing Device Manager server properties on page A-4](#)
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 2-8 Port numbers that must be registered as firewall exceptions between the management server and management clients on page 2-16
- Table 2-9 Port numbers that must be registered as firewall exceptions between the management server and storage systems on page 2-17
- Table 2-10 Port numbers that must be registered as firewall exceptions between the management client and storage systems on page 2-19
- Table 2-11 Port numbers that must be registered as firewall exceptions between the management server and a host on page 2-20
- Table 2-12 Port numbers that must be registered as firewall exceptions between the management server and a virtualization server on page 2-21
- Table 2-13 Port number that must be registered as an exception to a firewall between the management server and a mainframe host on page 2-21
Table 2-8 Port numbers that must be registered as firewall exceptions between the management server and management clients

<table>
<thead>
<tr>
<th>Originator Machine</th>
<th>Port number</th>
<th>Machine</th>
<th>Port number</th>
<th>Machine</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management client (GUI or Device Manager CLI)</td>
<td>any/tcp</td>
<td>Management server</td>
<td>2001/tcp#</td>
<td>2001/tcp</td>
<td>This setting is required when non-SSL communication is used.</td>
</tr>
<tr>
<td>Management client (GUI or Device Manager CLI)</td>
<td>any/tcp</td>
<td>Management server</td>
<td>2443/tcp#</td>
<td>2443/tcp</td>
<td>This setting is required when SSL communication is used.</td>
</tr>
<tr>
<td>Management client (Tiered Storage Manager CLI)</td>
<td>any/tcp</td>
<td>Management server</td>
<td>20352/tcp#</td>
<td>20352/tcp</td>
<td>This setting is required when non-SSL communication is used.</td>
</tr>
<tr>
<td>Management client (GUI)</td>
<td>any/tcp</td>
<td>Management server</td>
<td>22015/tcp#</td>
<td>22015/tcp</td>
<td>This setting is required when non-SSL communication is used.</td>
</tr>
<tr>
<td>Management client</td>
<td>any/tcp</td>
<td>Management server</td>
<td>22016/tcp#</td>
<td>22016/tcp</td>
<td>This setting is required when SSL communication is used.</td>
</tr>
</tbody>
</table>
#:
This port number can be changed.

Table 2-9 Port numbers that must be registered as firewall exceptions between the management server and storage systems

<table>
<thead>
<tr>
<th>Originator</th>
<th>Destination</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port number</td>
<td>Machine</td>
<td>Port number</td>
</tr>
<tr>
<td>(GUI)</td>
<td>Management client</td>
<td>24500/tcp#</td>
</tr>
</tbody>
</table>

#: This port number can be changed.

Table 2-9 Port numbers that must be registered as firewall exceptions between the management server and storage systems

<table>
<thead>
<tr>
<th>Originator</th>
<th>Destination</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port number</td>
<td>Machine</td>
<td>Port number</td>
</tr>
<tr>
<td>any/udp</td>
<td>• VSP G1000 • Virtual Storage Platform • Universal Storage Platform V/VM • Hitachi USP • HUS VM</td>
<td>162/udp</td>
</tr>
<tr>
<td>any/tcp</td>
<td>Management server</td>
<td>443/tcp</td>
</tr>
<tr>
<td>any/tcp</td>
<td>Management server</td>
<td>1099/tcp</td>
</tr>
<tr>
<td>any/tcp</td>
<td>Management server</td>
<td>2000/tcp#</td>
</tr>
<tr>
<td>Originator Port number</td>
<td>Machine</td>
<td>Destination Port number</td>
</tr>
<tr>
<td>------------------------</td>
<td>---------</td>
<td>-------------------------</td>
</tr>
<tr>
<td>any/tcp</td>
<td>Management server</td>
<td>2000/tcp#</td>
</tr>
<tr>
<td>any/tcp</td>
<td>• Universal Storage Platform V/VM&lt;br&gt;• Hitachi USP</td>
<td>2001/tcp#</td>
</tr>
<tr>
<td>any/tcp</td>
<td>Management server</td>
<td>28355/tcp#</td>
</tr>
<tr>
<td>any/tcp</td>
<td>Management server</td>
<td>51099/tcp</td>
</tr>
<tr>
<td>any/tcp</td>
<td>Management server</td>
<td>51100/tcp</td>
</tr>
<tr>
<td>any/tcp</td>
<td>Management server</td>
<td>51100/tcp</td>
</tr>
</tbody>
</table>

Legend:

-: Not applicable

#: This port number can be changed.
### Table 2-10 Port numbers that must be registered as firewall exceptions between the management client and storage systems

<table>
<thead>
<tr>
<th>Port number</th>
<th>Machine</th>
<th>Port number</th>
<th>Machine</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>any/tcp</td>
<td>Management client (GUI)</td>
<td>80/tcp</td>
<td>VSP G1000</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Virtual Storage Platform</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Universal Storage Platform</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>V/VM</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Hitachi USP</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>HUS VM</td>
<td></td>
</tr>
<tr>
<td>any/tcp</td>
<td>Management client (GUI)</td>
<td>443/tcp</td>
<td>VSP G1000</td>
<td>This setting is required when using SSL for Storage Navigator.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Virtual Storage Platform</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Universal Storage Platform</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>V/VM</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Hitachi USP</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>HUS VM</td>
<td></td>
</tr>
<tr>
<td>any/tcp</td>
<td>Management client (GUI)</td>
<td>1099/tcp</td>
<td>VSP G1000</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Virtual Storage Platform</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Universal Storage Platform</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>V/VM</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Hitachi USP</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>HUS VM</td>
<td></td>
</tr>
<tr>
<td>any/tcp</td>
<td>Management client (GUI)</td>
<td>51099/tcp</td>
<td>VSP G1000</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Virtual Storage Platform</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Universal Storage Platform</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>V/VM</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Hitachi USP</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>HUS VM</td>
<td></td>
</tr>
<tr>
<td>any/tcp</td>
<td>Management client</td>
<td>51100/tcp</td>
<td>VSP G1000</td>
<td>-</td>
</tr>
<tr>
<td>Originator</td>
<td>Destination</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>------------</td>
<td>-------------</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Port number</td>
<td>Machine</td>
<td>Port number</td>
<td>Machine</td>
<td></td>
</tr>
<tr>
<td>(GUI)</td>
<td>• Virtual Storage Platform</td>
<td>VSP G1000</td>
<td>This setting is required when using the management client as an SNMP manager.</td>
<td></td>
</tr>
<tr>
<td>any/tcp</td>
<td>Management client (GUI)</td>
<td>161/udp</td>
<td>VSP G1000</td>
<td>This setting is required when using SMI-S.</td>
</tr>
<tr>
<td>any/tcp</td>
<td>Management client (GUI)</td>
<td>427/tcp</td>
<td>VSP G1000</td>
<td>This setting is required when using SMI-S.</td>
</tr>
<tr>
<td>any/tcp</td>
<td>Management client (GUI)</td>
<td>5989/tcp</td>
<td>VSP G1000</td>
<td>This setting is required when using the management client as an SNMP manager.</td>
</tr>
</tbody>
</table>

Legend:
- : Not applicable

**Table 2-11 Port numbers that must be registered as firewall exceptions between the management server and a host**

<table>
<thead>
<tr>
<th>Originator</th>
<th>Destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port number</td>
<td>Machine</td>
</tr>
<tr>
<td>any/tcp</td>
<td>• Normal host</td>
</tr>
<tr>
<td>any/tcp</td>
<td>Management server</td>
</tr>
<tr>
<td>any/tcp</td>
<td>Management server</td>
</tr>
</tbody>
</table>

Legend:
- : Not applicable
This port number can be changed.

**Table 2-12 Port numbers that must be registered as firewall exceptions between the management server and a virtualization server**

<table>
<thead>
<tr>
<th>Originator</th>
<th>Destination</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port number</td>
<td>Machine</td>
<td>Port number</td>
</tr>
<tr>
<td>any/tcp</td>
<td>Management server</td>
<td>443/tcp</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>any/tcp</td>
<td>Management server</td>
<td>5988/tcp</td>
</tr>
<tr>
<td>any/tcp</td>
<td>Management server</td>
<td>5989/tcp</td>
</tr>
</tbody>
</table>

**Legend:**
- : Not applicable
#: This port number can be changed.

**Table 2-13 Port number that must be registered as an exception to a firewall between the management server and a mainframe host**

<table>
<thead>
<tr>
<th>Originator</th>
<th>Destination</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port number</td>
<td>Machine</td>
<td>Port number</td>
</tr>
<tr>
<td>any/tcp</td>
<td>Management server</td>
<td>24042/tcp#</td>
</tr>
</tbody>
</table>

**Table 2-14 Port number that must be registered as an exception to a firewall between the management server and a file server**

<table>
<thead>
<tr>
<th>Originator</th>
<th>Destination</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port number</td>
<td>Machine</td>
<td>Port number</td>
</tr>
<tr>
<td>any/tcp</td>
<td>Hitachi Data Ingestor Hitachi NAS Platform</td>
<td>2001/tcp#</td>
</tr>
<tr>
<td>Originator</td>
<td>Destination</td>
<td>Remarks</td>
</tr>
<tr>
<td>----------------------------</td>
<td>----------------------------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Port number</td>
<td>Machine</td>
<td>Port number</td>
</tr>
<tr>
<td>any/tcp</td>
<td>Management server</td>
<td>8443/tcp</td>
</tr>
</tbody>
</table>

Legend:
- #: Not applicable

#:
This port number can be changed.

**Table 2-15 Port numbers that must be registered as firewall exceptions between the Device Manager management server and the Tuning Manager management server**

<table>
<thead>
<tr>
<th>Originator</th>
<th>Destination</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port number</td>
<td>Machine</td>
<td>Port number</td>
</tr>
<tr>
<td>any/tcp</td>
<td>Device Manager management server</td>
<td>22286/tcp #1</td>
</tr>
<tr>
<td>any/tcp</td>
<td>Device Manager management server</td>
<td>22900/tcp to 22999/tcp</td>
</tr>
<tr>
<td>any/tcp</td>
<td>Tuning Manager management server</td>
<td>22015/tcp #1</td>
</tr>
<tr>
<td>any/tcp</td>
<td>Tuning Manager management server</td>
<td>24230/tcp #2</td>
</tr>
<tr>
<td>any/tcp</td>
<td>Tuning Manager management server</td>
<td>1024/tcp to 65535/tcp #3</td>
</tr>
</tbody>
</table>

Legend:
This port number can be changed.

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

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. For details on the config.xml file and the configforclient.xml file, see Setting up the config.xml file and the configforclient.xml files on page 5-19.

Table 2-16 Port number that must be registered as a firewall exception between the management server and the Host Data Collector computer

<table>
<thead>
<tr>
<th>Originator</th>
<th>Destination</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>any/tcp</td>
<td>Management server</td>
<td>22098/tcp</td>
</tr>
<tr>
<td>any/tcp</td>
<td>Management server</td>
<td>22099/tcp</td>
</tr>
<tr>
<td>any/tcp</td>
<td>Management server</td>
<td>22100/tcp</td>
</tr>
<tr>
<td>any/tcp</td>
<td>Management server</td>
<td>22104/tcp</td>
</tr>
<tr>
<td>any/tcp</td>
<td>Management server</td>
<td>22105/tcp</td>
</tr>
<tr>
<td>any/tcp</td>
<td>Management server</td>
<td>22106/tcp</td>
</tr>
</tbody>
</table>

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.

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.

#: This port number can be changed.
Table 2-17 Port number that must be registered as a firewall exception between the Host Data Collector computer and a host

<table>
<thead>
<tr>
<th>Originator</th>
<th>Destination</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>any/tcp</td>
<td>Host Data Collector computer</td>
<td>22/tcp #</td>
</tr>
<tr>
<td>any/tcp</td>
<td>Host Data Collector computer</td>
<td>80/tcp</td>
</tr>
<tr>
<td>any/tcp</td>
<td>Host Data Collector computer</td>
<td>135/tcp</td>
</tr>
<tr>
<td>any/tcp</td>
<td>Host Data Collector computer</td>
<td>139/tcp</td>
</tr>
<tr>
<td>any/tcp</td>
<td>Host Data Collector computer</td>
<td>443/tcp</td>
</tr>
<tr>
<td>any/tcp</td>
<td>Host Data Collector computer</td>
<td>445/tcp</td>
</tr>
<tr>
<td>any/udp</td>
<td>Host Data Collector computer</td>
<td>445/udp</td>
</tr>
</tbody>
</table>

#: This port number can be changed.
### Table 2-18 Port numbers that must be registered as firewall exceptions between the management server and an SMI-S provider

<table>
<thead>
<tr>
<th>Originator</th>
<th>Destination</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port number</td>
<td>Machine</td>
<td>Port number</td>
</tr>
<tr>
<td>any/tcp</td>
<td>SMI-S provider</td>
<td>5983/tcp#</td>
</tr>
<tr>
<td>any/tcp</td>
<td>Management server</td>
<td>5988/tcp#</td>
</tr>
<tr>
<td>any/tcp</td>
<td>Management server</td>
<td>5989/tcp#</td>
</tr>
</tbody>
</table>

Legend:
- : Not applicable
# : This port number can be changed.

### Table 2-19 Port numbers that must be registered as firewall exceptions between the management server and a CIM client

<table>
<thead>
<tr>
<th>Originator</th>
<th>Destination</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port number</td>
<td>Machine</td>
<td>Port number</td>
</tr>
<tr>
<td>any/tcp</td>
<td>CIM client</td>
<td>427/tcp</td>
</tr>
<tr>
<td>any/tcp</td>
<td>CIM client</td>
<td>5988/tcp#</td>
</tr>
<tr>
<td>any/tcp</td>
<td>CIM client</td>
<td>5989/tcp#</td>
</tr>
</tbody>
</table>

Legend:
- : Not applicable
# : This port number can be changed.
Table 2-20 Port numbers that must be registered as firewall exceptions between the management server and a mail server

<table>
<thead>
<tr>
<th>Originator Machine</th>
<th>Destination Machine</th>
<th>Remarks</th>
</tr>
</thead>
</table>
| 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 2-21 Port numbers that must be registered as firewall exceptions between the management server and an external authentication server

<table>
<thead>
<tr>
<th>Originator</th>
<th>Destination</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port number</td>
<td>Machine</td>
<td>Port number</td>
</tr>
<tr>
<td>any/tcp</td>
<td>Management server</td>
<td>88/tcp#</td>
</tr>
<tr>
<td>any/tcp</td>
<td>Management server</td>
<td>88/udp#</td>
</tr>
<tr>
<td>any/tcp</td>
<td>Management server</td>
<td>359/tcp#</td>
</tr>
<tr>
<td>any/tcp</td>
<td>Management server</td>
<td>1812/udp#</td>
</tr>
</tbody>
</table>

Legend:
- : Not applicable
# : This port number is generally used. However, a different port number might be used for an external authentication server.

Table 2-22 Port numbers that must be registered as firewall exceptions when you manage copy pairs by using the pair management server

<table>
<thead>
<tr>
<th>Originator</th>
<th>Destination</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port number</td>
<td>Machine</td>
<td>Port number</td>
</tr>
<tr>
<td>any/udp</td>
<td>Normal host • Virtual machine</td>
<td>31001/udp</td>
</tr>
</tbody>
</table>

Legend:
- : Not applicable

Related topics
- Registering firewall exceptions for Device Manager and Tiered Storage Manager in Windows on page 2-28
- Registering firewall exceptions for Device Manager and Tiered Storage Manager in Red Hat Enterprise Linux on page 2-29
- Registering firewall exceptions for Device Manager and Tiered Storage Manager in SUSE Linux Enterprise Server on page 2-29
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.

To add the components to the firewall exceptions list:

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
   ```

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

Table 2-23 Names added to the exceptions list and paths specified with the netsh command

<table>
<thead>
<tr>
<th>Component</th>
<th>Name added to the exceptions list</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Manager server</td>
<td>Device Manager</td>
<td><code>installation-folder-for-Hitachi-Command-Suite\DeviceManager\HiCommandServer\HiCommandServer.exe</code></td>
</tr>
<tr>
<td>Tiered Storage Manager server</td>
<td>Tiered Storage Manager(htsmService)</td>
<td><code>installation-folder-for-Hitachi-Command-Suite\TieredStorageManager\bin\htsmService.exe</code></td>
</tr>
<tr>
<td>JDK</td>
<td>Device Manager - HBase64(java)</td>
<td><code>installation-folder-for-Hitachi-Command-Suite\Base64\uCPSB\hjdk\jre\bin\java.exe</code></td>
</tr>
<tr>
<td></td>
<td>Tiered Storage Manager - HBase64(java)</td>
<td><code>installation-folder-for-Hitachi-Command-Suite\Base64\uCPSB\hjdk\bin\java.exe</code></td>
</tr>
</tbody>
</table>

#:

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.

Related topics

- [Port numbers that must be registered as firewall exceptions for Device Manager and Tiered Storage Manager on page 2-15](#)
- [Starting the Hitachi Command Suite services on page 8-4](#)
Registering firewall exceptions for Device Manager and Tiered Storage Manager in Red Hat Enterprise Linux

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

**To add the port numbers to the firewall exceptions list:**

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 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 topics**

- Port numbers that must be registered as firewall exceptions for Device Manager and Tiered Storage Manager on page 2-15

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.

**To add the port numbers to the firewall exceptions list:**

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, 22015, 22016, 22017, 22018, 161, and 162 are registered as exceptions:

```
FW_SERVICES_EXT_TCP="2001 22015:22018"
FW_SERVICES_EXT_UDP="161 162"
```

2. Execute `/sbin/SuSEfirewall2`.

**Related topics**

- [Port numbers that must be registered as firewall exceptions for Device Manager and Tiered Storage Manager on page 2-15](#)

## 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 topics

- Registering an exception for the Host Data Collector service (for SSL communication) on page 2-31
- hdc.common.rmi.registryPort on page C-3
- hdc.common.rmi.serverPort on page C-4
- hdc.common.http.serverPort on page C-4

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.

Operations to complete in advance

Log in with administrator permissions.

Information to collect in advance

- 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.http.serverPort` property (Default value: 22106/tcp)

To register a firewall exception for the Host Data Collector service:

1. Execute the following command for each port.
   ```bash
   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:
   ```bash
   netsh advfirewall firewall show rule name=all
   ```

Related topics

- Starting the Host Data Collector service on page 8-9
- Stopping the Host Data Collector service on page 8-9
- Registering an exception for the Host Data Collector service (for non-SSL communication) on page 2-30
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 2-1 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.

- Enterprise-class storage system and HUS VM, and the management client
• Enterprise-class storage system and HUS VM, and the management server
• Midrange storage systems 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 2-1 Example of a configuration in which the management server is used as a bridge between networks on page 2-32) 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 topics**
- [Changing Device Manager server properties on page A-4](#)
- [server.http.host on page A-5](#)
- [launchapp.snm2.url on page A-36](#)

**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 topics**
- [hdc.service.rmi.registryIPAddress on page C-6](#)

**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 topics
• Settings required for linking with Storage Navigator Modular 2 on page 5-2

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

To migrate Device Manager to an IPv6 environment:

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 SSLEnable.
- 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 topics

- Editing the user_httpsd.conf file on page 4-36
- Starting the Hitachi Command Suite services on page 8-4
- Stopping the Hitachi Command Suite services on page 8-5

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.

To link with storage systems that support IPv6:

1. 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 or Hitachi USP 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 topics**
- Changing Device Manager server properties on page A-4
- server.http.host on page A-5

**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.

**Information to collect in advance**
- 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.

**To change the host name of the management server:**

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`, `hsso_httpsd.conf`, and `user_hsso_httpsd.conf` files.

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.
   `installation-folder-for-Hitachi-Command-Suite\Base64\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 topics

- Required operations after changing the IP address or host name of the management server on page 2-39
- Changing the URL for accessing Hitachi Command Suite products (hcmand64chgurl command) on page 2-41
- Editing the user_httpsd.conf file on page 4-36
- Stopping the Hitachi Command Suite services on page 8-5
- Checking the operating status of the Hitachi Command Suite services on page 8-7
- Backing up a database in non-cluster configuration on page 9-3
- Backing up a database in a cluster configuration on page 9-4

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.

Information to collect in advance

Changed IP address of the management server.

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

To change the IP address of the management server:

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 topics

- Required operations after changing the IP address or host name of the management server on page 2-39
- Changing the URL for accessing Hitachi Command Suite products (hcmds64chgurl command) on page 2-41
- Editing the user_httpsd.conf file on page 4-36
- Stopping the Hitachi Command Suite services on page 8-5
- Checking the operating status of the Hitachi Command Suite services on page 8-7
- Backing up a database in non-cluster configuration on page 9-3
- Backing up a database in a cluster configuration on page 9-4

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.

- 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.

- If acquiring performance information from Tuning Manager
  Revise the `ownHost` parameter setting in the `config.xml` file and the `configforclient.xml` file.

- If receiving SNMP traps from file servers
  You must change the host name or IP address of the notification destination for SNMP traps (the SNMP manager) by using Hitachi File Services Manager.

- If user accounts are authenticated in Hitachi Command Suite when logging in to CCI or the SVP
  In 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.

**Related topics**

- [Registering an external authentication server and an external authorization server on page 3-17](#)
- [Settings for using Element Manager on page 5-3](#)
- [Setting up the config.xml and configforclient.xml files on page 5-19](#)
- [Starting the Hitachi Command Suite services on page 8-4](#)
- [Stopping the Hitachi Command Suite services on page 8-5](#)
- [Setting the Device Manager server's information, HiScan command's execution period, and CCI's information (hdvmagt_setting command) on page 10-20](#)
- [Changing Device Manager server properties on page A-4](#)
- [server.http.host on page A-5](#)
- How to register the Replication Manager information source: *Replication Manager User Guide*

- How to change the registration of the repository location: *Tuning Manager Server Administration Guide*

- How to change the SNMP trap notification destination for the file server: The file server manuals.
About settings required for products other than Device Manager, Tiered Storage Manager, and Replication Manager: The manuals for Hitachi Command Suite products.

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

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

**To change Hitachi Command Suite product URLs:**

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.
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
```

---

**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
  ```

---

**Related topics**

- Changing ports used by Common Component on page 2-10
- Changing the host name of the management server on page 2-36
- Changing the IP address of the management server on page 2-38
- Operation workflow for secure communication between a management server and a management client (GUI) on page 4-9
• How to migrate from a non-cluster configuration to a cluster configuration: *Hitachi Command Suite Installation and Configuration Guide*
User account management

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

- About password policies
- About account locking
- User management on an external authentication server
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.

To set a password policy:

1. 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>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>password.min.length</code></td>
<td>Specifies the minimum number of characters the password must contain. Specify a value from 1 to 256. Default: 4</td>
</tr>
<tr>
<td><code>password.min.uppercase</code></td>
<td>Specifies the minimum number of uppercase letters the password must contain. Specify a value</td>
</tr>
</tbody>
</table>

User account management

Hitachi Command Suite Administrator Guide
<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>from 0 to 256. If you specify 0, no restriction applies. Default: 0</td>
</tr>
<tr>
<td>password.min.lowercase</td>
<td>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</td>
</tr>
<tr>
<td>password.min.numeric</td>
<td>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</td>
</tr>
<tr>
<td>password.min.symbol</td>
<td>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</td>
</tr>
<tr>
<td>password.check.userID</td>
<td>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</td>
</tr>
</tbody>
</table>

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

**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.

**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.

**To set an account locking policy:**

1. 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:**
The following table shows the account locking policies that can be set in the `security.conf` file.

**Table 3-2 Account locking policies that can be set in the `security.conf` file**

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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         |

If you change the setting values in the `security.conf` file, the new account locking policy takes effect immediately.

**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.

**Settings for automatically locking the System account**

To apply account locking to System accounts, change the settings in the `user.conf` file.

**To apply account locking to System accounts:**

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:
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.

Account locking is applied to `System` accounts for all Hitachi Command Suite products.

**Related topics**

- [Starting the Hitachi Command Suite services on page 8-4](#)
- [Stopping the Hitachi Command Suite services on page 8-5](#)

**Unlocking accounts**

Locked user accounts can be unlocked by using the `hcmds64unlockaccount` command.

**Operations to complete in advance**

Log in as a user with Administrator permissions (for Windows) or as a root user (for Linux).

**Information to collect in advance**

- 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.

- The user ID and password of the locked user account

**To unlock a locked account:**

1. 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.

### User management on an external authentication server

Hitachi Command Suite products not only allow you to register user accounts and use them in Common Component (internal authentication), but also allow you to use the user accounts that are under the integrated management of an external authentication server or an external authorization server.

By using user accounts managed by an external authentication server or an external authorization server, you do not need to manage the operations of Hitachi Command Suite products, thereby reducing your workload.

### 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.
Figure 3-1 Operating workflow for user authentication on an LDAP directory server

Note:

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.
• 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 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 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.

Related topics

• [Account conditions for Hitachi Command Suite products on page 3-14](#)
• [About the data structures of user entries on page 3-15](#)
• [Registering an external authentication server and an external authorization server on page 3-17](#)
• [About a LDAP search user account on page 3-41](#)
• [Checking connections to an external authentication server and an external authorization server on page 3-47](#)
• [Secure communication for Device Manager and Tiered Storage Manager on page 4-5](#)

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.
Figure 3-2 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 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.

---

**Related topics**

- [Account conditions for Hitachi Command Suite products on page 3-14](#)
- [About the data structures of user entries on page 3-15](#)
- [Registering an external authentication server and an external authorization server on page 3-17](#)
- [About a LDAP search user account on page 3-41](#)
- [Registering a shared secret on page 3-46](#)
- [Checking connections to an external authentication server and an external authorization server on page 3-47](#)
- [Secure communication for Device Manager and Tiered Storage Manager on page 4-5](#)

---

**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.
Figure 3-3 Operation workflow for user authentication on a Kerberos server

Note:

- 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.

#1: This step is required if you want to change the current user authentication method.
#2: Set operation permissions according to users' job scopes.
• When a Hitachi Command Suite product is in operation, to switch to the system configuration linked to an external authorization server, delete user any ID that has the same name with 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.

Related topics

• [Account conditions for Hitachi Command Suite products on page 3-14](#)
• [About the data structures of user entries on page 3-15](#)
• [Registering an external authentication server and an external authorization server on page 3-17](#)
• [About a LDAP search user account on page 3-41](#)
• [Checking connections to an external authentication server and an external authorization server on page 3-47](#)
• [Secure communication for Device Manager and Tiered Storage Manager on page 4-5](#)
• Operations on a management client: [Hitachi Command Suite User Guide](#) or [Replication Manager User Guide](#)

**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
  ! # $ % & ' ( ) * + - . = @ \ ^ _ |

[3-14 User account management](#) Hitachi Command Suite Administrator Guide
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. Only user entries that are in the hierarchies below BaseDN are subject to authentication or authorization.

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 3-4 Example of the hierarchical structure model](image)

Legend: The user entries enclosed by the dotted line can be authenticated.

**Figure 3-4 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.

![Diagram of the flat model]

Legend: The user entities enclosed by the dotted line can be authenticated.

**Figure 3-5 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`
Example of an invalid RDN:
uid=John:123S \(\text{(A colon is used.)}\)

\(\text{cn=John Smith} \ \text{(A space is used between John and Smith.)}\)

**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.

**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.

**Operations to complete in advance**

- 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).
  
  (see [About the data structures of user entries on page 3-15](#))
- Set up the environment for the DNS server on the OS of the LDAP directory server.
  
  #: This operation is required to look up the information about the LDAP directory server by using the DNS server.
**Information to collect in advance**

- **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 managed by the LDAP directory server (when linking to an external authorization server)

- **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 name
  - 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)

**To register an external authentication server and an external authorization server:**

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 topics

- [Starting the Hitachi Command Suite services on page 8-4](#)
- [Stopping the Hitachi Command Suite services on page 8-5](#)

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 3-3 Setup items in the `exauth.properties` file for LDAP authentication (common items) on page 3-20](#)
- 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 3-4 Setup items in the `exauth.properties` file for LDAP authentication (when directly specifying information about the external authentication server) on page 3-20](#)
      - [Table 3-5 Setup items in the `exauth.properties` file for LDAP authentication (when an external authentication server and StartTLS are used for communication) on page 3-23](#)
    - When using the DNS server to look up information about the LDAP directory server:
      - [Table 3-6 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 3-23](#)

Note:

- 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 3-3 Setup items in the `exauth.properties` file for LDAP authentication
(common items)

<table>
<thead>
<tr>
<th>Property</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>auth.server.type</td>
<td>Specify an external authentication server type. Specify <code>ldap</code>. Default value: <code>internal</code> (used when not linking to an external authentication server)</td>
</tr>
<tr>
<td>auth.server.name</td>
<td>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 3-4 Setup items in the <code>exauth.properties</code> file for LDAP authentication (when directly specifying information about the external authentication server) on page 3-20 or Table 3-6 Setup items in the <code>exauth.properties</code> file for LDAP authentication (when using the DNS server to look up information about the external authentication server) on page 3-23) are applied to. ServerName has been set as the initial value. You must specify at least one name. When specifying multiple LDAP directory server identification names, separate the names with 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</td>
</tr>
<tr>
<td>auth.group.mapping</td>
<td>Specify whether to also link to an external authorization server. Specify <code>true</code> to link to an external authorization server. Specify <code>false</code> to not to link to an external authorization server. Default value: <code>false</code></td>
</tr>
</tbody>
</table>

### Table 3-4 Setup items in the `exauth.properties` file for LDAP authentication
(when directly specifying information about the external authentication server)

<table>
<thead>
<tr>
<th>Attributes</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>protocol#1</td>
<td>Specify the protocol for connecting to the LDAP directory server. This attribute is required. When communicating in plain text format, specify <code>ldap</code>. When using StartTLS communication, specify <code>tls</code>. Before specifying <code>tls</code>, make sure that one of the following encryption methods can be used on the LDAP directory server. - TLS_RSA_WITH_AES_256_CBC_SHA256 - TLS_RSA_WITH_AES_256_CBC_SHA</td>
</tr>
</tbody>
</table>

3-20 User account management 
Hitachi Command Suite Administrator Guide
<table>
<thead>
<tr>
<th>Attributes</th>
<th>Details</th>
</tr>
</thead>
</table>
| • 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)  
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.  
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 |
### Attributes

<table>
<thead>
<tr>
<th>Attributes</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td></td>
</tr>
</tbody>
</table>

- 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 # + ; , < = > \n
Default value: none

<table>
<thead>
<tr>
<th>retry.interval</th>
<th>Specify the retry interval (in seconds) for when an attempt to connect to the LDAP directory server fails.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifiable values: 1 to 60 (seconds)</td>
<td>Default value: 1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>retry.times</th>
<th>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.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifiable values: 0 to 50</td>
<td>Default value: 20</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>domain.name</th>
<th>Specify the name of a domain managed by the LDAP directory server. This item is required when an external authorization directory server is also linked to.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default value: none</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>dns_lookup</th>
<th>Specify false.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default value: false</td>
<td></td>
</tr>
</tbody>
</table>

### Note:

To specify the attributes, use the following syntax:

```text
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 3-5 Setup items in the exauth.properties file for LDAP authentication (when an external authentication server and StartTLS are used for communication)**

<table>
<thead>
<tr>
<th>Property</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>auth.ocsp.enable</td>
<td>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</td>
</tr>
<tr>
<td>auth.ocsp.responderURL</td>
<td>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</td>
</tr>
</tbody>
</table>

**Table 3-6 Setup items in the exauth.properties file for LDAP authentication (when using the DNS server to look up information about the external authentication server)**

<table>
<thead>
<tr>
<th>Attributes</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>protocol</td>
<td>Specify the protocol for connecting to the LDAP directory server. This attribute is required. Specifiable values: ldap Default value: none</td>
</tr>
<tr>
<td>port</td>
<td>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</td>
</tr>
<tr>
<td>timeout</td>
<td>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</td>
</tr>
<tr>
<td>attr</td>
<td>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</td>
</tr>
<tr>
<td>Attributes</td>
<td>Details</td>
</tr>
<tr>
<td>------------</td>
<td>---------</td>
</tr>
<tr>
<td>attribute</td>
<td>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 <code>sAMAccountName</code> in which the Windows logon ID has been defined.</td>
</tr>
<tr>
<td>basedn</td>
<td>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.</td>
</tr>
<tr>
<td>retry.interval</td>
<td>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</td>
</tr>
<tr>
<td>retry.times</td>
<td>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</td>
</tr>
<tr>
<td>domain.name</td>
<td>Specify the domain name managed by the LDAP directory server. Default value: none</td>
</tr>
<tr>
<td>dns_lookup</td>
<td>Specify <code>true</code>.</td>
</tr>
</tbody>
</table>
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

**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 3-7 Setup items in the exauth.properties file for RADIUS authentication (common items) on page 3-27

- **Properties for an external authentication server**
  Specify these property values for each RADIUS server.
  Table 3-8 Setup items in the exauth.properties file for RADIUS authentication (settings for the external authentication server) on page 3-28

- **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 3-9: Setup items in the exauth.properties file for RADIUS authentication (common settings for the external authorization server) on page 3-29

Table 3-10: Setup items in the exauth.properties file for RADIUS authentication (when directly specifying information about the external authorization server) on page 3-30

Table 3-11: Setup items in the exauth.properties file for RADIUS authentication (when an external authorization server and StartTLS are used for communication) on page 3-32

- When using the DNS server to look up the information about the LDAP directory server
  Table 3-9: Setup items in the exauth.properties file for RADIUS authentication (common settings for the external authorization server) on page 3-29
  Table 3-12: 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 3-32

---

**Note:**

- 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 3-7: Setup items in the exauth.properties file for RADIUS authentication (common items)

<table>
<thead>
<tr>
<th>Property names</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>auth.server.type</td>
<td>Specify an external authentication server type. Specify <code>radius</code>. Default value: <code>internal</code> (used when not linking to an external authentication server)</td>
</tr>
<tr>
<td>auth.server.name</td>
<td>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 3-8: Setup items in the exauth.properties file for RADIUS authentication (settings for the external authentication server) on page 3-28) are applied to. <code>ServerName</code> has been set as the initial value. You must specify at least one name. When specifying multiple RADIUS server identification names, separate the names with 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 ! # ( ) + - . = [ ] ^ _ <code>{ </code> ~</td>
</tr>
</tbody>
</table>
### 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>
<thead>
<tr>
<th>Property names</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>auth.group.mapping</td>
<td>Specify whether to also link to an external authorization server.</td>
</tr>
<tr>
<td></td>
<td>Specify <code>true</code> to link to an external authorization server.</td>
</tr>
<tr>
<td></td>
<td>Specify <code>false</code> to not to link to an external authorization server.</td>
</tr>
<tr>
<td></td>
<td>Default value: <code>false</code></td>
</tr>
</tbody>
</table>

### Table 3-8 Setup items in the exauth.properties file for RADIUS authentication (settings for the external authentication server)

<table>
<thead>
<tr>
<th>Attributes</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>protocol</td>
<td>Specify the protocol for RADIUS server authentication. This attribute is required. Specifiable values: PAP or CHAP Default value: none</td>
</tr>
<tr>
<td>host</td>
<td>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</td>
</tr>
<tr>
<td>port</td>
<td>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</td>
</tr>
<tr>
<td>timeout</td>
<td>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</td>
</tr>
<tr>
<td>retry.times</td>
<td>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</td>
</tr>
<tr>
<td>attr.NAS-Identifier</td>
<td>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</td>
</tr>
</tbody>
</table>
**attr.NAS-IP-Address**

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

**attr.NAS-IPv6-Address**

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 3-9 Setup items in the exauth.properties file for RADIUS authentication (common settings for the external authorization server)**

<table>
<thead>
<tr>
<th>Attributes</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>domain.name</td>
<td>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</td>
</tr>
<tr>
<td>dns_lookup</td>
<td>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 <code>exauth.properties</code> file, specify <code>false</code>.</td>
</tr>
</tbody>
</table>
### Attributes

<table>
<thead>
<tr>
<th>Attributes</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>If you want to use the DNS server to look up the information, specify <code>true</code>. 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.</td>
</tr>
<tr>
<td></td>
<td>- <code>auth.group.domain-name.host</code></td>
</tr>
<tr>
<td></td>
<td>- <code>auth.group.domain-name.port</code></td>
</tr>
<tr>
<td>Default value:</td>
<td><code>false</code></td>
</tr>
</tbody>
</table>

Note:

To specify the attributes, use the following syntax:

```
auth.radius.auth.server.name-property-value.attribute=value
```

#### Table 3-10 Setup items in the `exauth.properties` file for RADIUS authentication (when directly specifying information about the external authorization server)

<table>
<thead>
<tr>
<th>Attributes</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>protocol</strong>&lt;sup&gt;#1&lt;/sup&gt;</td>
<td>Specify the protocol for connecting to the LDAP directory server. When communicating in plain text format, specify <code>ldap</code>. When using StartTLS communication, specify <code>tls</code>. Before specifying <code>tls</code>, make sure that one of the following encryption methods can be used on the LDAP directory server.</td>
</tr>
<tr>
<td></td>
<td>- <code>TLS_RSA_WITH_AES_256_CBC_SHA256</code></td>
</tr>
<tr>
<td></td>
<td>- <code>TLS_RSA_WITH_AES_256_CBC_SHA</code></td>
</tr>
<tr>
<td></td>
<td>- <code>TLS_RSA_WITH_AES_128_CBC_SHA256</code></td>
</tr>
<tr>
<td></td>
<td>- <code>TLS_RSA_WITH_AES_128_CBC_SHA</code></td>
</tr>
<tr>
<td></td>
<td>- <code>SSL_RSA_WITH_3DES_EDE_CBC_SHA</code></td>
</tr>
<tr>
<td>Specifiable values:</td>
<td><code>ldap</code> or <code>tls</code></td>
</tr>
<tr>
<td>Default value:</td>
<td><code>ldap</code></td>
</tr>
</tbody>
</table>

| **host**<sup>#2</sup> | 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 |
### Attributes

<table>
<thead>
<tr>
<th>Attributes</th>
<th>Details</th>
</tr>
</thead>
</table>
| **basedn** | Default value: 389  
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.  
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 3-11 Setup items in the exauth.properties file for RADIUS authentication (when an external authorization server and StartTLS are used for communication)

<table>
<thead>
<tr>
<th>Property</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>auth.ocsp.enable</td>
<td>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</td>
</tr>
<tr>
<td>auth.ocsp.responderURL</td>
<td>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</td>
</tr>
</tbody>
</table>

Table 3-12 Setup items in the exauth.properties file for RADIUS authentication (when using the DNS server to look up information about the external authorization server)

<table>
<thead>
<tr>
<th>Attributes</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>protocol</td>
<td>Specify the protocol for connecting to the LDAP directory server. Specifiable values: ldap Default value: ldap</td>
</tr>
<tr>
<td>port</td>
<td>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</td>
</tr>
<tr>
<td>basedn</td>
<td>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 # + ; , &lt; = &gt; \</td>
</tr>
</tbody>
</table>
### Attributes

<table>
<thead>
<tr>
<th>Attributes</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>timeout</strong></td>
<td>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</td>
</tr>
<tr>
<td><strong>retry.interval</strong></td>
<td>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</td>
</tr>
<tr>
<td><strong>retry.times</strong></td>
<td>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</td>
</tr>
</tbody>
</table>

**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**
When using the DNS server to look up an external authorization server

**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 3-13 Setup items in the exauth.properties file for Kerberos authentication (common items) on page 3-35

- **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 3-14 Setup items in the exauth.properties file for Kerberos authentication (when directly specifying information about the external authentication server) on page 3-35
When using the DNS server to look up information about the Kerberos server:

Table 3-15 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 3-37

- 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 3-16 Setup items in the exauth.properties file for Kerberos authentication (settings for the external authorization server) on page 3-38

Table 3-17 Setup items in the exauth.properties file for Kerberos authentication (when an external authorization server and StartTLS are used for communication) on page 3-40

Note:
- 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 3-13 Setup items in the exauth.properties file for Kerberos authentication (common items)

<table>
<thead>
<tr>
<th>Property names</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>auth.server.type</td>
<td>Specify an external authentication server type. Specify kerberos.</td>
</tr>
<tr>
<td></td>
<td>Default value: internal (used when not linking to an external authentication server)</td>
</tr>
<tr>
<td>auth.group.mapping</td>
<td>Specify whether to also link to an external authorization server.</td>
</tr>
<tr>
<td></td>
<td>Specify true to link to an external authorization server.</td>
</tr>
<tr>
<td></td>
<td>Specify false to not link to an external authorization server.</td>
</tr>
<tr>
<td></td>
<td>Default value: false</td>
</tr>
</tbody>
</table>

Table 3-14 Setup items in the exauth.properties file for Kerberos authentication (when directly specifying information about the external authentication server)

<table>
<thead>
<tr>
<th>Attributes</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>default_realm</td>
<td>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.</td>
</tr>
<tr>
<td>Attributes</td>
<td>Details</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>dns_lookup_kdc</td>
<td>Specify false. Default value: false</td>
</tr>
</tbody>
</table>
| 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) 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:                                                                 |

3-36 User account management Hitachi Command Suite Administrator Guide
### Attributes and Details

<table>
<thead>
<tr>
<th>Attributes</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>host-name-or-IP-address[::port-number]</code></td>
<td>This attribute is required.</td>
</tr>
<tr>
<td><code>host-name-or-IP-address</code></td>
<td>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).</td>
</tr>
<tr>
<td><code>port-number</code></td>
<td>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 specifying multiple Kerberos servers, separate them with commas as follows: <code>host-name-or-IP-address[::port-number],host-name-or-IP-address[:port-number],...</code></td>
</tr>
</tbody>
</table>

### Note:

To specify the attributes, use the following syntax:

```
auth.kerberos.attribute=value
```

If 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 3-15 Setup items in the exauth.properties file for Kerberos authentication (when using the DNS server to look up information about the external authentication server)

<table>
<thead>
<tr>
<th>Attributes</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>default_realm</code></td>
<td>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</td>
</tr>
<tr>
<td><code>dns_lookup_kdc</code></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>• <code>realm_name</code></td>
</tr>
</tbody>
</table>
## Attributes

<table>
<thead>
<tr>
<th>Attributes</th>
<th>Details</th>
</tr>
</thead>
</table>
|                  | • 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) 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 3-16 Setup items in the exauth.properties file for Kerberos authentication (settings for the external authorization server)

<table>
<thead>
<tr>
<th>Attributes</th>
<th>Details</th>
</tr>
</thead>
</table>
| 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.  

### Attributes

<table>
<thead>
<tr>
<th>Attributes</th>
<th>Details</th>
</tr>
</thead>
</table>
| **TLS_RSA_WITH_AES_256_CBC_SHA256** | Specifiable values: ldap or tls  
Default value: ldap |
| **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** |  |

**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.  
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 3-17 Setup items in the exauth.properties file for Kerberos authentication (when an external authorization server and StartTLS are used for communication)**

<table>
<thead>
<tr>
<th>Property</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>auth.ocsp.enable</td>
<td>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</td>
</tr>
<tr>
<td>auth.ocsp.responderURL</td>
<td>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</td>
</tr>
</tbody>
</table>

**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.timeout=3
  auth.kerberos.clockskew=300
  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
  ```
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.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
```

### 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.

Operations to complete in advance

Register an LDAP search user on the LDAP directory server.

Information to collect in advance

- DN and password of the LDAP search user
- Server identification name 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.
- 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.
To register an LDAP search user account:

1. 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 topics

- Notes on commands for setting up a link to an external authentication server on page 3-49

Deleting an LDAP search user account

Use the hcmds64ldapuser command to delete the LDAP search user account from the management server.

Information to collect in advance

- Server identification name 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)

To delete an LDAP search user account:

1. 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 topics

- Notes on commands for setting up a link to an external authentication server on page 3-49

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.

To check the LDAP directory server that registered the LDAP search user account:

1. 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.

**Information to collect in advance**

- 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.

**To register a shared secret:**

1. 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 topics**

- Notes on commands for setting up a link to an external authentication server on page 3-49

Deleting a shared secret

Use the `hcmds64radiussecret` command to delete the shared secret.

**Information to collect in advance**

RADIUS server indication name.

**To delete a shared secret:**

1. Execute the `hcmds64radiussecret` command.

   In Windows:
   ```
   installation-folder-for-Hitachi-Command-Suite\Base64\bin\hcmds64radiussecret /delete /name RADIUS-server-indication-name
   ```
   
   In Linux:
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.

**To check the RADIUS server that registered a shared secret on the management server:**

1. 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
     ```

   The server identification name of the RADIUS server is displayed.

Related topics

- [Notes on commands for setting up a link to an external authentication server on page 3-49](#)

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.

**Operations to complete in advance**

Register an external authentication server and an external authorization server (see [Registering an external authentication server and an external authorization server on page 3-17](#)).
Information to collect in advance

- 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.

  Note that you cannot specify a user account whose user-ID or password begins with a forward slash (/) in Windows, or hyphen (-) in Linux.

To check connections to an external authentication server and an external authorization server:

1. 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 by realm name. In addition, specify user IDs according to the following:

- If you specify a user who belongs to a realm other than the realm set for default_realm in the exauth.properties file:
  Specify a character string that contains the realm name.
• If you specify a user who belongs to the realm set for `default_realm` in the `exauth.properties` file:
  You can omit the realm name.

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 topics**

- [Notes on commands for setting up a link to an external authentication server on page 3-49](#)

**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
This chapter describes the security settings required to operate Hitachi Command Suite products.

- Login warning banners
- Communication security mode
- Controlling management client access to the management server
- Changing the password-encoding level in the Device Manager CLI and the Tiered Storage Manager CLI
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 `&amp;` 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.

Operations to complete in advance

Log in as a user with Administrator permissions (for Windows) or as a root user (for Linux).

To create and register a message displayed on a warning banner:

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:
     `installation-folder-for-Hitachi-Command-Suite\Base64\sample\resource`
   - In Linux:
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:

```html
<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.

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.

**Operations to complete in advance**

Log in as a user with Administrator permissions (for Windows) or as a root user (for Linux).

**Information to collect in advance**

The locale of the message to be deleted (en for English or ja for Japanese).

To delete a message:

1. 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.
Communication security mode

Hitachi Command Suite products can enhance communication security between computers in networks by using SSL or TLS. SSL/TLS has the following main functions:

- Verifies the identities of connecting applications
- Encrypts data transferred between servers and clients
- Detects data that was tampered with during transfers

Secure communication for Device Manager and Tiered Storage Manager

Device Manager and Tiered Storage Manager can use SSL/TLS for the inter-machine communications listed below.
Figure 4-1 Secure communication routes for Device Manager and Tiered Storage Manager
• Between a management server and a management client (GUI) 
SSL/TLS can be used for communication between the components listed 
below.
  ○ Common Component and a Web browser
  ○ The Device Manager server and a Web browser
• Between a management server and a management client (Device 
Manager CLI) 
SSL/TLS can be used for communication between the Device Manager 
server and the Device Manager CLI.
• Between a management server and a management client (Tiered Storage 
Manager CLI) 
SSL/TLS can be used for communication between the Tiered Storage 
Manager server and the Tiered Storage Manager CLI.
• Between an LDAP directory server and a management server 
StartTLS can be used for communication between an LDAP directory 
server and Common Component.
• Between the Device Manager server and Replication Manager server 
SSL/TLS can be used for communication between the Device Manager 
server and Replication Manager server. 
Even in a multi-site configuration, SSL/TLS can be used for 
communication between each of the secondary sites (Device Manager 
server) and each of the primary sites (Replication Manager server).
• Between the Tuning Manager server and Device Manager server 
SSL/TLS can be used for communication between the Tuning Manager 
server and Device Manager server when both are on the same 
management server. The Tuning Manager server communicates with the 
Device Manager server via the Common Component using SSL/TLS. 
If the Tuning Manager server and Device Manager server are installed on 
different management servers, SSL/TLS communication between those 
management servers is not possible.
• Between a Host Data Collector machine and a management server 
SSL/TLS can be used for communication between Host Data Collector and 
the Device Manager server.
• Between a virtualization server and Host Data Collector 
If Host Data Collector is used to manage a virtualization server, SSL/TLS 
can be used for communication between a virtualization server and Host 
Data Collector.
• Between a management server and a Device Manager agent computer 
SSL/TLS can be used for communication between the Device Manager 
server and a Device Manager agent.
• Between a storage system and a management server 
If the Device Manager server is used as an SSL client, SSL/TLS can be 
used for communication between the following storage systems and the 
Device Manager server:
SSL/TLS is always used for communication with VSP G1000, Virtual Storage Platform, Universal Storage Platform V/VM, Hitachi USP, or HUS VM.

- VSP G1000
- Virtual Storage Platform
- Universal Storage Platform V/VM
- Hitachi USP
- HUS VM
- HUS100
- Hitachi AMS2000
- Hitachi SMS
- SMI-S enabled storage systems (SMI-S provider)

#: If the Device Manager server is used as the SSL server (if user accounts are authenticated in Hitachi Command Suite when logging in to CCI or the SVP), you need to configure settings to use SSL/TLS for communication between the Device Manager server and the storage system (VSP G1000).

- Between a storage system and a management client (GUI)
  SSL/TLS can be used for communication between the Web browser of a management client and a storage system if Storage Navigator or Storage Navigator Modular 2 is used from the Device Manager GUI.

- Between a Tuning Manager Agent and a Tuning Manager server
  SSL/TLS can be used for communication, triggered by use of the Tuning Manager API, between the Tuning Manager server and a Tuning Manager Agent
  Note that the Tuning Manager Agent REST API component in Figure 4-1 Secure communication routes for Device Manager and Tiered Storage Manager on page 4-6 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.

- Between a Tuning Manager server and a Tuning Manager API client
  SSL/TLS can be used for communication between the Tuning Manager server and a Tuning Manager API client if the Tuning Manager API is used. A Tuning Manager server communicates with a Tuning Manager API client by using SSL/TLS via the Common Component.

- Between a management server and a CIM client
  The Device Manager server that acts as the CIM server of CIM/WBEM can use SSL/TLS to communicate with a CIM client for object operations or event indications.
    - Object operations
      The Device Manager server acts as an SSL server, and a CIM client acts as an SSL client.
- Event indications
  The Device Manager server acts as an SSL client and a CIM client acts as an SSL server.
  
  To further improve security, you can enable two-way authentication.

**Note:** Hitachi Command Suite products support SSL version 3 and TLS version 1.2. However, for the following communication routes where the Device Manager server acts as an SSL client, SSL version 3 or TLS version 1.0 is used.

- Between HUS100, Hitachi AMS2000, or Hitachi SMS and a management server
- Between Tiered Storage Manager CLI and a management server (If the JDK bundled with Hitachi Command Suite is used)

For the following communication routes where the Device Manager server acts as an SSL client, if Oracle JDK7 (1.7.0) is used, SSL version 3 or TLS version 1.0 is used:

- Between VSP G1000, Virtual Storage Platform, Universal Storage Platform V/VM, Hitachi USP, HUS VM, or SMI-S enabled storage system (SMI-S provider) and a management server
- Between a CIM client and a management server

**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 4-2 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.
- 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 topics

- Changing the URL for accessing Hitachi Command Suite products (hcmds64chgurl command) on page 2-41
- Configuring an SSL server (Common Component) on page 4-33
- Configuring an SSL server (Device Manager server) on page 4-41
- Configuring an SSL client on page 4-65
- Settings for using Element Manager on page 5-3
- Changing Device Manager server properties on page A-4
- `server.https.enabledCipherSuites` on page A-32

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 4-3 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 topics**

- Configuring an SSL server (Device Manager server) on page 4-41
- Configuring an SSL client on page 4-65
- Changing Device Manager server properties on page A-4
- `server.https.enabledCipherSuites` on page A-32

**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 4-4 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 topics
- Configuring an SSL client on page 4-65
- Changing Tiered Storage Manager server properties on page B-2
- server.rmi.secure on page B-15
- server.rmi.security.port on page B-4
- server.rmi.security.enabledCipherSuites on page B-15

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 4-5 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 topics
- User management on an external authentication server on page 3-7
- Configuring an SSL client on page 4-65

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 4-6 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 (jssecaerts). 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 topics

- Configuring an SSL server (Device Manager server) on page 4-41
- Configuring an SSL client on page 4-65
- Changing Device Manager server properties on page A-4
- server.https.enabledCipherSuites on page A-32

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 4-7 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 topics

- Configuring an SSL server (Common Component) on page 4-33
- Configuring an SSL client on page 4-65
- Changing Device Manager server properties on page A-4
- htnm.servers on page A-44
- htnm.server.n.host on page A-44
- htnm.server.n.protocol on page A-45
- htnm.server.n.port on page A-45

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 4-8 Operation workflow for secure communication between a Host Data Collector machine and a management server

Note: 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.

Related topics
- Registering firewall exceptions for Host Data Collector (Windows) on page 2-30
- Configuring an SSL server (Host Data Collector) on page 4-56
- Configuring an SSL client on page 4-65
- Changing Device Manager server properties on page A-4
- hdc.rmiregistry on page A-39
- hdc.rmiserver on page A-39
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 4-9 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 ESX 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 the following, 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.
    - VMware ESX 4.x
    - VMware ESXi 4.x
    - VMware vCenter Server 4.x
    - VMware ESXi 5.0, 5.0 Update 1, 5.1
    - VMware vCenter Server 5.0, 5.0 Update 1b, 5.1, 5.1.0a
  Replace the obtained server certificate with the self-signed certificate that is imported to the virtualization server. For details, see VMware manuals.

**Related topics**

- [Importing a certificate into the truststore for Host Data Collector on page 4-76](#)
- [Changing virtualization server information on page 4-79](#)
- [Changing Host Data Collector properties on page C-2](#)
- [hdc.ssl.esx.certCheck on page C-8](#)

**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 4-10 Operation workflow for secure communication between a management server and Device Manager agent

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 topics

- Configuring an SSL server (Device Manager server) on page 4-41
- Configuring an SSL client on page 4-65
- Changing Device Manager server properties on page A-4
- server.https.enabledCipherSuites on page A-32
- server.server.serverPort on page D-15
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, Virtual Storage Platform, Universal Storage Platform V/VM, Hitachi USP, or HUS VM because such communication always uses SSL/TLS.

![Figure 4-11 Operation workflow for secure communication between a storage system and a management server](image)

**Related topics**

- Changing storage system information on page 4-83

Operation workflow for secure communication between a management server and a storage system (VSP G1000)

To authenticate user accounts in Hitachi Command Suite when logging in to CCI or the SVP, create a server certificate for the Device Manager server, and then import the certificate into SVP.
Figure 4-12 Operation workflow for secure communication between a management server and a storage system (VSP G1000)

Related topics
• Configuring an SSL server (Device Manager server) on page 4-41
• Downloading a Device Manager server truststore file on page 4-65
• Registering certificates for HCS on page 4-106

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 4-13 Operation workflow for secure communication between an SMI-S provider and a management server

Related topics
- Configuring an SSL client on page 4-65

Operation workflow for secure communication between a Tuning Manager Agent and a Tuning Manager server

You need to create a server certificate on the Tuning Manager Agent host, and then import it into the truststore (`jssecacerts`).

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`). In this case, you do not need to import a certificate.
Related topics

- Configuring an SSL server (Tuning Manager Agent host) on page 4-60
- Configuring an SSL client on page 4-65

Operation workflow for secure communication between a Tuning Manager server and a Tuning Manager API client

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/TLS settings by performing the operations appropriate for the environment on each client.

![Diagram]

Figure 4-15 Operation workflow for secure communication between a Tuning Manager server and a Tuning Manager API client

Related topics

- Configuring an SSL server (Common Component) on page 4-33

Operation workflow for secure communication between a storage system and a management client (GUI)

To operate VSP G1000, Virtual Storage Platform, or HUS VM by using Storage Navigator from the Device Manager GUI, you need to re-create a server certificate for VSP G1000, Virtual Storage Platform, or HUS VM. You do not need to change the setting when operating other Hitachi storage systems.

When using the server certificate bundled with VSP G1000, Virtual Storage Platform, or HUS VM, if you launch Storage Navigator from the Device Manager GUI, an error message is displayed in the Web browser. To avoid this, you need to create a server certificate in which the IP address of VSP G1000, Virtual Storage Platform, or HUS VM is specified for Common Name.
Figure 4-16 Operation workflow for secure communication between a storage system and a management client (GUI)

**Note:** The IP address of VSP G1000, Virtual Storage Platform, or HUS VM to be specified for **Common Name** in a server certificate must be the same as the storage system IP address specified when a storage system is registered by using the Device Manager GUI or CLI.

**Related topics**
- Configuring an SSL server and clients (VSP G1000) on page 4-84
- How to create and import a server certificate (for Virtual Storage Platform or HUS VM): See the documentation for Storage Navigator.

**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 4-17 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 topics

- Configuring an SSL server and clients (CIM server) on page 4-108
- Configuring an SSL server and clients (CIM client) on page 4-120
- Changing Device Manager server properties on page A-4
- Ciphers on page A-33

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 4-18 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 topics
- Configuring an SSL server and clients (CIM server) on page 4-108
- Configuring an SSL server and clients (CIM client) on page 4-120
- Changing Device Manager server properties on page A-4
- Ciphers on page A-33
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.

![Operation workflow for secure communication between a management server and a CIM client (event indications)](image)

**Figure 4-19 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 `cimxmlscpaproperties` file, and then specify a value for the `Ciphers` property.

**Related topics**
- Configuring an SSL server and clients (CIM server) on page 4-108
- Configuring an SSL server and clients (CIM client) on page 4-120
- Changing Device Manager server properties on page A-4
- Ciphers on page A-33

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 4-20 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 topics

- Configuring an SSL server and clients (CIM server) on page 4-108
- Configuring an SSL server and clients (CIM client) on page 4-120
- Changing Device Manager server properties on page A-4
- Ciphers on page A-33

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
- Between a Tuning Manager Agent and the Tuning Manager server (when the Tuning Manager API is used)

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 topics
• Changing Device Manager server properties on page A-4
• server.https.security.truststore on page A-32

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.

A certificate signing request and self-signed certificate are created with a
private key size of 2,048 bits. 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.
Operations to complete in advance

Log in as a user with Administrator permissions (for Windows) or as a root user (for Linux).

Information to collect in advance

- 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)

Format of the 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]
```

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]
```

Options

- **key**
  Specify the path to the location to which a private key will be output. The size of a private key is 2,048 bits (fixed).

- **csr**
  Specify the path to the location to which the certificate signing request will be output.

- **cert**
  Specify the path to the location to which the self-signed certificate will be output.

- **certtext**
  Specify the path to the location to which the contents of the self-signed certificate will be output in text format.

- **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.
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>
<thead>
<tr>
<th>Attribute type</th>
<th>Full name of attribute type</th>
<th>Attribute value</th>
</tr>
</thead>
<tbody>
<tr>
<td>CN</td>
<td>Common Name</td>
<td>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.</td>
</tr>
<tr>
<td>OU</td>
<td>Organizational Unit Name</td>
<td>Specify the name of the organizational unit.</td>
</tr>
<tr>
<td>O</td>
<td>Organization Name</td>
<td>Specify the organizational name. This attribute is required.</td>
</tr>
<tr>
<td>L</td>
<td>Locality Name</td>
<td>Specify the name of the city, town, or other locality.</td>
</tr>
<tr>
<td>ST</td>
<td>State or Province Name</td>
<td>Specify the name of the state or province.</td>
</tr>
<tr>
<td>C</td>
<td>Country Name</td>
<td>Specify the two-letter country code.</td>
</tr>
</tbody>
</table>

Specify a signature algorithm. You can specify SHA256withRSA, SHA1withRSA, or MD5withRSA. If you omit this specification, SHA256withRSA is used as the signature algorithm.
Caution: When you execute the `hcems64ssltool` command, if a file with the same name already exists in the output location, the existing file will be overwritten. Therefore, when you recreate a private key, certificate signing request, or self-signed certificate, we recommend you to output them to a directory other than existing storage directories.

**Applying to a certificate authority for a Common Component server certificate**

Usually, you can apply to a certificate authority for a server certificate online. Send the Common Component certificate signing request (CSR) that you created to a certificate authority to be digitally signed.

**Operations to complete in advance**

Create a certificate signing request for Common Component.

**Information to collect in advance**

- 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.

**To apply to a certificate authority for a Common Component server certificate:**

1. Send the created certificate signing request to a certificate authority.

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.

**Editing the user_httpsd.conf file**

To enable SSL/TLS for Common Component or change the host name or port number of a management server, edit the `user_httpsd.conf` file.

**Operations to complete in advance**

- 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.
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

Information to collect in advance

- Host name specified for Common Name in the certificate signing request (required for enabling SSL/TLS).

To edit the user_httpsd.conf file:

1. Stop the services of the Hitachi Command Suite product.
2. Edit the user_httpsd.conf file.
3. Start the services of Hitachi Command Suite product.

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)

```
ServerName host-name
Listen 22015
*Listen [::]:22015
*Listen 127.0.0.1:22015
SSL:Disable
*Listen 22016
*Listen [::]:22016
*ServerName host-name
SSL:Enable
SSL:Protocol SSLv3 TLSv1 TLSv11 TLSv12
SSL:RequiredCiphers AES256-SHA256:AES256-SHA:AES128-SHA256:AES128-SHA:DES-CBC3-SHA
SSL:RequireSSL
SSL:CertificateKeyFile "installation-folder-for-Hitachi-Command-
Suite/Base64/uCPSB/httpsd/conf/server/httpskey.pem"
SSL:CertificateFile "installation-folder-for-Hitachi-Command-
Suite/Base64/uCPSB/httpsd/conf/server/https.pem"
SSL:CACertificateFile "installation-folder-for-Hitachi-Command-
Suite/Base64/uCPSB/httpsd/conf/cacert/anycert.pem"
</VirtualHost>
```
Settings required for enabling SSL/TLS

- Remove the hash mark (#) at the beginning of the following lines:

```bash
ServerName host-name
Listen 22015
#Listen [::]:22015
#Listen 127.0.0.1:22015
SSLDisable
Listen 22016
#Listen [::]:22016
<VirtualHost *:22016>
  ServerName host-name
  SSLEnable
  SSLProtocol SSLv3 TLSv1 TLSv11 TLSv12
  SSLRequiredCiphers AES256-SHA256:AES256-SHA:AES128-SHA256:AES128-SHA
  SSLRequireSSL
  SSLCertificateKeyFile "installation-folder-for-Hitachi-Command-Suite/Base64/uCP5B/https/conf/ssl/server/httpskey.pem"
  SSLCertificateFile "installation-folder-for-Hitachi-Command-Suite/Base64/uCP5B/https/conf/ssl/server/https.pem"
  # SSLCACertificateFile "installation-folder-for-Hitachi-Command-Suite/Base64/uCP5B/https/conf/ssl/cacert/anycert.pem"
</VirtualHost>
```

- Remove the hash mark (#) from the beginning of each of these 10 lines.

- 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. Do not specify a symbolic link and junction for the path.

- For the `SSLCertificateFile` directive, specify the absolute path of the server certificate for Common Component. For the server certificate, both a signed certificate issued by the certificate authority and a self-signed certificate exist.

- To use the certificate of the chained certificate authority, remove the hash mark (#) from the beginning of the line for the `SSLCACertificateFile` directive, and then specify the absolute path of the certificate of the chained certificate authority. Multiple certificates can be contained in one file by chaining multiple PEM format certificates by using a text editor. Note that you must not specify a symbolic link or junction for the path.

- For an IPv6 environment, remove the hash mark (#) at the beginning of the lines `Listen [::]:22016`.

**Note:**

- Do not edit the `httpsd.conf` file, the `hsso_httpsd.conf` file or the `user_hsso_httpsd.conf` file.

- Even if you enable SSL or use Device Manager in an IPv6 environment, do not remove or comment out the line `Listen 22015`.

4-38 Security
Hitachi Command Suite Administrator Guide
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, make sure that the host name that is set to the `ServerName` directive can be resolved to 127.0.0.1.

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.

- 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).

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 `<VirtualHost>` to comment them out.

**Related topics**

- [Starting the Hitachi Command Suite services on page 8-4](#)
- [Stopping the Hitachi Command Suite services on page 8-5](#)

**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`).

**Operations to complete in advance**

- 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`

(see `htnm.server.n.host` on page A-44, `htnm.server.n.protocol` on page A-45, `htnm.server.n.port` on page A-45)

To close the port of the non-SSL communication for HBase 64 Storage Mgmt Web Service:

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.

   ```
   ServerName host-name
   #Listen 22015
   #Listen [::]:22015
   #Listen 127.0.0.1:22015
   SSLDisable
   Listen 22016
   #Listen [::]:22016
   #<VirtualHost *:22016>
   #  ServerName host-name
   SSLEnable
   SSLProtocol SSLv3 TLSv1 TLSv11 TLSv12
   SSLRequiredCiphers AES256-SHA256:AES256-SHA:AES128-SHA256:AES128-
   SHA:DES-CBC3-SHA
   SSLRequireSSL
   SSLCertificateKeyFile "installation-folder-for-Common-
   Component/uCPSB/https/conf/ssl/server/httpdkey.pem"
   SSLCertificateFile "installation-folder-for-Common-
   Component/uCPSB/https/conf/ssl/server/httpsd.pem"
   # SSLCACertificateFile "installation-folder-for-Common-
   Component/uCPSB/https/conf/ssl/cacert/anycert.pem"
   </VirtualHost>
   ```

   Add the leading hash mark (#).

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

In Windows:
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 topics:

- [Importing a certificate into the truststore for Hitachi Command Suite on page 4-71](#)
- [Checking the certificates imported into the truststore for Hitachi Command Suite on page 4-75](#)
- [Starting the Hitachi Command Suite services on page 8-4](#)
- [Stopping the Hitachi Command Suite services on page 8-5](#)

### 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.

#### Operations to complete in advance

- 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.
Information to collect in advance

- 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).

To create a key pair and a self-signed certificate for Device Manager server:

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.

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.

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 keystore in server properties...
   Saving new keypass to disk...

All done.

Related topics

- Changing Device Manager server properties on page A-4
- server.https.security.keystore on page A-31

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.

Operations to complete in advance

- 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.

To enable SSL/TLS for the Device Manager server:

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.

>2
Current Device Manager Server Security Level = User Logon (Basic Security

Hitachi Command Suite Administrator Guide
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.

Operations to complete in advance

- 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

To create a certificate signing request for Device Manager server:

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).

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-----
MIIC0zCCAbgsCAAwg0CzA/BJgMVBAYTAkIqQReWdYDvQQ1EwLya8hLyW5h22F3YTERRMABgAIUEBxM1MW9
rb2hbbwExEjAQgSMBwMDC3zEwMC4GA1UEcMxM2N4DB21tYyw5kIER1dmjLZSBNYW5h22
V1IEFkU1uaXNOcmF0aW9uMRIwEAYDVQQDeD9TMTAxODQ3NzMwggEiMA0GCSqGSIb3DQEB
...
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.

Operations to complete in advance

Create a certificate signing request for the Device Manager server.

Information to collect in advance

- 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.

To apply to a certificate authority for a Device Manager server certificate:

1. Send the created certificate signing request to a certificate authority.

Usually, server certificates issued by a certificate authority are sent via email. We recommend that you save the server certificate as a file named `hostname.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.
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-----
MIIDMDCCApmgAwIBAgIDOBcYMA0GCSqGSIb3DQEBAUAAMIGHMQswCQYDVQQGEwJa
QTEiMCAGA1UECBMZRk9SIFRFU1RJTkcgUFVSUE9TRVMgT05MTWEdMBsGA1UEChMU
VGhhd3RlIENlcnRpZmljYXRpb24xFzAVBgNVBAsTDlRFU1QgVEVTVCBURVNUMRww
...
...
...
ADANBgkqhkiG9w0BAQQFAAOBgQBtzeFG4IfvpPnA7G/khD4rrT1TvjbK4Y1pcROM
cel43uFkqNYgI35UukoNtjd120XoudLwKvJu5JK7846zW1bEjmCr5BYlwzuaq
MQdXMyyPUnqcgq44/JGzF27x9p4atWE2z nlj5R7XGG14RPAO5YbbvMJD0QR
yV00rw==
-----END CERTIFICATE-----
```

**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**.

**Operations to complete in advance**

- 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.

**To import a server certificate into the Device Manager server keystore:**

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.

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.

```plaintext
>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 topics**
- [Changing Device Manager server properties on page A-4](#)
- [server.https.security.keystore on page A-31](#)

**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.

**Operations to complete in advance**

Log in as a user with Administrator permissions (for Windows) or as a root user (for Linux).
To view the Device Manager server key pair information in normal mode:

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).

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
```

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.

Operations to complete in advance

Log in as a user with Administrator permissions (for Windows) or as a root user (for Linux).

To view the Device Manager server key pair information in verbose mode:

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).

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
```
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.

Operations to complete in advance

Log in as a user with Administrator permissions (for Windows) or as a root user (for Linux).

To delete a key pair from the Device Manager server keystore:

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.

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.
Operations to complete in advance

Log in as a user with Administrator permissions (for Windows) or as a root user (for Linux).

Information to collect in advance

- Password of the Device Manager server keystore
- Current password of the Device Manager server key pair

To change the password of a Device Manager server key pair:

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.

Information to collect in advance

Current password of the Device Manager server keystore.

To change the password of the Device Manager server keystore:

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**.

**Operations to complete in advance**

- 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.

**To import a certificate into the Device Manager server truststore:**

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 topics**

- [Truststores on page 4-30](#)
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**.

**Operations to complete in advance**

Log in as a user with Administrator permissions (for Windows) or as a root user (for Linux).

**To view the Device Manager server truststore information in normal mode:**

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**).

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
2) verisignclass3g2ca, Fri Nov 25 12:04:37 JST 2005
3) verisignclass3g2ca, Fri Nov 25 12:04:35 JST 2005
4) verisignclass1g2ca, Fri Nov 25 12:04:34 JST 2005
5) verisignclass3g3ca, Fri Nov 25 12:04:37 JST 2005
6) verisignclass2g3ca, Fri Nov 25 12:04:36 JST 2005
7) verisignclass1g3ca, Fri Nov 25 12:04:34 JST 2005
8) verisignclass1ca, Fri Nov 25 12:04:35 JST 2005
9) verisignserverca, Fri Nov 25 12:04:38 JST 2005
10) verisignclass2ca, Fri Nov 25 12:04:36 JST 2005
```

Related topics

- **Truststores** on page 4-30

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 Security**.
configuration for Device Manager Server, and then Display verbose contents of Device Manager Server TrustStore.

Operations to complete in advance

Log in as a user with Administrator permissions (for Windows) or as a root user (for Linux).

To view the Device Manager server truststore information in verbose mode:

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).

The verbose information of a server certificate is displayed as follows:

```bash
>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
```

Related topics

- Truststores on page 4-30

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.

Operations to complete in advance

Log in as a user with Administrator permissions (for Windows) or as a root user (for Linux).
To delete a server certificate from the Device Manager server truststore:

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.

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
2) verisignclass3g2ca, Fri Nov 25 12:04:37 JST 2005
3) verisignclass2g2ca, Fri Nov 25 12:04:35 JST 2005
4) verisignclass1g2ca, Fri Nov 25 12:04:34 JST 2005
5) verisignclass3g3ca, Fri Nov 25 12:04:37 JST 2005
6) verisignclass2g3ca, Fri Nov 25 12:04:36 JST 2005
7) verisignclass1g3ca, Fri Nov 25 12:04:34 JST 2005
8) verisignclass1ca, Fri Nov 25 12:04:35 JST 2005
9) verisignserverca, Fri Nov 25 12:04:38 JST 2005
10) verisignclass2ca, Fri Nov 25 12:04:36 JST 2005

Enter number of alias to delete (0 to abort) [default=0]:1
Delete verisignclass3ca [1] ? [default=No]:
```

Related topics

- Truststores on page 4-30
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.

Operations to complete in advance

Log in as a user with Administrator permissions (for Windows) or as a root user (for Linux).

Information to collect in advance

Current password of the Device Manager server truststore.

To change the password of the Device Manager server truststore:

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 topics

- Truststores on page 4-30

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.

**Operations to complete in advance**

- 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.

**Format of the 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 topics
- For details about DN: Creating a secret key and a certificate signing request for Common Component on page 4-33

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.

Operations to complete in advance
Create a certificate signing request for Host Data Collector.

Information to collect in advance
- 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.

To apply to a certificate authority for a Host Data Collector server certificate:
1. Send the created certificate signing request to a certificate authority.

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.
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.

Operations to complete in advance

- 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.

Information to collect in advance

- Information of the keystore file
  You need the information of the keystore file prepared when creating a self-signed certificate.
  - Absolute path
  - Access password

To import the Host Data Collector server certificates into the keystore:

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.

### Configuring an SSL server (Tuning Manager Agent host)

To use a Tuning Manager Agent host as an SSL server, you need to prepare a private key and a server certificate, and then specify their storage locations in the `htnm_httpsd.conf` file of the Tuning Manager Agent host.

### Creating a secret key and a certificate signing request for Tuning Manager Agent host

To create a private key and a certificate signing request (CSR) for a Tuning Manager Agent host, use the `htmsltool` command.

A certificate signing request and self-signed certificate are created with a private key size of 2,048 bits and the signature algorithm SHA256withRSA. 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.

### 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

Requirements for the certificate signing request (ask the certificate authority)

### Format of the command

In Windows:

```
installation-folder-for-Tuning-Manager-Agent\htnm\bin\htmsltool l -key private-key-file -csr certificate-signing-request-file -cert self-signed-certificate-file -certtext
```

4-60 Security
Hitachi Command Suite Administrator Guide
In Unix:

installation-directory-for-Tuning-Manager-Agent/htnm/bin/htmssltool 1 -key private-key-file -csr certificate-signing-request-file -cert self-signed-certificate-file -certtext contents-of-self-signed-certificate [-validity number-of-valid-days] [-dname DN]

**Options**

**key**
Specify the absolute path of the location to which a private key will be output. The size of a private key is 2,048 bits (fixed).

**csr**
Specify the absolute path of the location to which a certificate signing request will be output.

**cert**
Specify the absolute path of the location to which a self-signed certificate will be output.

**certtext**
Specify the absolute path of the location to which the contents of the self-signed certificate will be output in text format.

**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.

For Common Name, specify the host name of the Tuning Manager Agent host. (You can use the FQDN format to specify the host name.) When specifying the Common Name, note the following:

- To detect HTTP I/F information per Tuning Manager Agent host
  Specify the host name that was specified for the following property in the user.properties file for the Tuning Manager server:
  HostNamen in the rest.discovery.agent.host.HostNamen.host
  property

- To detect HTTP I/F information for all Tuning Manager Agent hosts
  Confirm that host names can be resolved by using either the hosts file on the Tuning Manager server or DNS.
Related topics

- For details about DN: Creating a secret key and a certificate signing request for Common Component on page 4-33

Applying to a certificate authority for an Tuning Manager Agent host server certificate

Usually, you can apply to a certificate authority for a server certificate online. Send the Tuning Manager Agent host certificate signing request (CSR) that you created to a certificate authority to be digitally signed.

Operations to complete in advance

Create a certificate signing request for the Tuning Manager Agent host.

Information to collect in advance

- How to apply to the certificate authority and what they support
  You need to have a server certificate issued in 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.

To apply to a certificate authority for an Tuning Manager Agent host server certificate:

1. Send the created certificate signing request to a certificate authority.

   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.

Enabling SSL/TLS (Tuning Manager Agent host)

To enable SSL/TLS for the Tuning Manager Agent host, edit the htnm_httpsd.conf file.

Operations to complete in advance

- Create a private key for the Tuning Manager Agent host.
- Prepare a server certificate for the Tuning Manager Agent host.
  Prepare the server certificate sent back from the certificate authority. When testing encrypted communications, you can use a self-signed certificate.

#: We recommend that you copy the files into the following location.
For a private key file and server certificate for a Tuning Manager Agent
In Windows:
installation-folder-for-Tuning-Manager-Agent\htnm\HBasePSB \httpsd\conf\ssl\server
In Unix:
installation-directory-for-Tuning-Manager-Agent/htnm/ HBasePSB/httpsd/conf/ssl/server

For a certificate file of the certificate authority (when using a certificate issued by the certificate authority)
In Windows:
installation-folder-for-Tuning-Manager-Agent\htnm\HBasePSB \httpsd\conf\ssl\cacert
In Unix:
installation-directory-for-Tuning-Manager-Agent/htnm/ HBasePSB/httpsd/conf/ssl/cacert

Information to collect in advance
• Host name specified for Common Name in the certificate signing request

To enable SSL/TLS:
1. Execute the following command to stop the service of the Tuning Manager Agent REST Web Service:
   In Windows:
   installation-folder-for-Tuning-Manager-Agent\htnm\bin \htmsrv stop -webservice
   In UNIX:
   installation-directory-for-Tuning-Manager-Agent/htnm/bin/ htmsrv stop -webservice
2. Edit the htm_httpsd.conf file.
3. Execute the following command to start the service of the Tuning Manager Agent REST Web Service:
   In Windows:
   installation-folder-for-Tuning-Manager-Agent\htnm\bin \htmsrv start -webservice
   In UNIX:
   installation-directory-for-Tuning-Manager-Agent/htnm/bin/ htmsrv start -webservice

Storage location of the htm_httpsd.conf file
In Windows:
installation-folder-for-Tuning-Manager-Agent\htnm\Rest\config \htnm_httpsd.conf
In UNIX:

installation-directory-for-Tuning-Manager-Agent/htnm/Rest/config/htnm_httpsd.conf

**Settings required for enabling SSL/TLS**

Make the following settings:

```plaintext
ServerName HostA
#Listen 127.0.0.1:24221
#Listen [::]:24221
#SSLDisable
Listen 24222
Listen [::]:24222
SSLEnable
SSLProtocol TLSv12
SSLRequiredCiphers AES256-SHA256:AES128-SHA256
SSLRequireSSL
SSLCertificateFile "C:/Program Files (x86)/HiCommand/TuningManager/jp1pc/htnm/HBasePSB/httpsd/conf/server/httpsd.pem"
SSLCertificateKeyFile "C:/Program Files (x86)/HiCommand/TuningManager/jp1pc/htnm/HBasePSB/httpsd/conf/server/httpsdkey.pem"
SSLCACertificateFile "C:/Program Files (x86)/HiCommand/TuningManager/jp1pc/htnm/HBasePSB/httpsd/conf/ssl/cacert/anycert.pem"
HWSLogSSLVerbose On
```

- Enter hash marks (#) as shown in the examples, and remove the hash marks (#) from other lines.
- For the `SSLCertificateFile` directive, specify the absolute path to the server certificate for Tuning Manager Agent host. For the server certificate, both a signed certificate issued by the certificate authority and a self-signed certificate exist.
- For the `SSLCertificateKeyFile` directive, specify the absolute path to the private key file for Tuning Manager Agent host. Do not specify a symbolic link or a junction for the path.
- To use the certificate of the chained certificate authority, remove the hash mark (#) from the beginning of the line for the `SSLCACertificateFile` directive, and then specify the absolute path of the certificate of the chained certificate authority. Multiple certificates can be contained in one file by chaining multiple PEM format certificates by using a text editor. Note that you must not specify a symbolic link or junction for the path.
- For an IPv6 environment, remove the hash mark (#) at the beginning of the line `#Listen [::]:24222`.

**Settings required for disabling SSL/TLS**

To disable SSL/TLS, enter hash marks (#) as shown in the examples, and remove the hash marks (#) from other lines.
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.

Operations to complete in advance

- 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 (see Importing a certificate into the Device Manager server truststore on page 4-52).
  - Import a server certificate into the keystore (see Importing a server certificate into the Device Manager server keystore on page 4-47).
- 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. (see Creating a key pair and a self-signed certificate for Device Manager server on page 4-41)

Information to collect in advance

- Host name or IP address for the management server
- 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**

**To download a Device Manager server truststore file:**

1. Start a Web browser and access the following URL:
   
   ```
   http://management-server-IP-address-or-host-name:DeviceManager-server-port-number/service/HiCommandCerts
   ```

2. Specify a user account, and download the truststore file.

**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 `hcems64keytool` utility (for Windows) or the `keytool` utility (for Linux).

**Operations to complete in advance**

Download the Device Manager server truststore file.

**Information to collect in advance**

- Alias name for the Device Manager server key pair.
  
  You can use the HiKeytool to check the alias.
  
  (see Viewing the Device Manager server key pair information in normal mode on page 4-48)

**To export a Device Manager server self-signed certificate:**

1. Execute the following command.

   **In Windows:**
   ```
   installation-folder-for-Hitachi-Command-Suite\Base64\bin
   \hcems64keytool -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.

2. Press the **Enter** key without entering the password of the Device Manager server truststore file.

**Importing a server certificate into a Web browser**

To use the GUI, you first need to import a server certificate created in the management server into the Web browser for the management client (GUI).
Operations to complete in advance

- Obtain a server certificate
  Obtain server certificates created by the management server in a secure method.
  - Server certificate of Common Component (see Creating a secret key and a certificate signing request for Common Component on page 4-33, Applying to a certificate authority for a Common Component server certificate on page 4-36)
  - Server certificate of Device Manager server (see Applying to a certificate authority for a Device Manager server certificate on page 4-46)
  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).

To import a server certificate into Internet Explorer®:

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 server certificate into the browser.

To import a server certificate into Firefox®:

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 server certificate into the browser.

Changing pop-up blocker settings

If you change the Hitachi Command Suite product URL to the SSL version of the URL, in Internet Explorer, you must register the SSL version of the URL in the pop-up blocker settings.

Operations to complete in advance

Change the Hitachi Command Suite product URL (see Changing the URL for accessing Hitachi Command Suite products (hcmds64chgurl command) on page 2-41).
**Information to collect in advance**

- IP address or host name of the management server

**To change pop-up blocker settings:**

1. Start Internet Explorer, select **Tools, Pop-up Blocker**, and then **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. Use the following format to specify the URL of each Hitachi Command Suite product in the **Address of website to allow** text box, and then click the **Add** button.
   ```
   https://management-server-IP-address-or-host-name
   ```

**Enabling SSL/TLS for the Device Manager CLI computer**

Set the environment variable `HDVM_CLI_CERTS_PATH` for the storage location of the Device Manager server truststore file (`HiCommandCerts`).

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` option when using the Device Manager CLI.

**Operations to complete in advance**

- Obtain a Device Manager server truststore file.
  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*

**Information to collect in advance**

- 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.
  (see *server.https.port on page A-7*)
To enable SSL/TLS for the Device Manager CLI computer:

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
     ```

---

**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.

**Operations to complete in advance**
- Set the server.properties file for the Tiered Storage Manager server.
  - server.rmi.secure property
  - server.rmi.security.port property
    (see Changing Tiered Storage Manager server properties on page B-2, server.rmi.secure on page B-15, server.rmi.security.port on page B-4)

**Information to collect in advance**
- Host name or IP address for the management server
- 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.
    (see Changing ports used by Common Component on page 2-10)
- User account for Tiered Storage Manager

**To download the Tiered Storage Manager server truststore files:**

1. Start a Web browser and access the following URL:
2. Specify a user account, and download the truststore file.

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 htmscli.properties file, change the settings for the htmsserver.location and option.secure properties.

If you set the htmsserver.location property or option.secure property in the htmscli.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.

Operations to complete in advance

- Obtain a truststore file for the Tiered Storage Manager server. Obtain the file from the management server using a secure way.
- Copy the htmscli.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 htmscli.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.

### Information to collect in advance

- 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.
  
  (see Changing ports used by Common Component on page 2-10, `server.rmi.security.port` on page B-4)

### To enable SSL/TLS for the Tiered Storage Manager CLI computer:

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.
   
   ○ `htmsserver.location` property
     
     Specify the location of the Tiered Storage Manager server in the following format:
     
     ```
     htmsserver.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
     ```

### Importing a certificate into the truststore for Hitachi Command Suite

To import a certificate to the truststore (`ldapcacerts`, `jssecacerts` or `dvmcacerts`), use the `hcmds64keytool` utility (for Windows) or the `keytool` utility (for Linux).

### Operations to complete in advance

- Prepare a certificate
  
  Obtain the certificate using a secure way.

  ○ For communication with an LDAP directory server
    
    The communication requires an LDAP server certificate. 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.
(see Applying to a certificate authority for a Device Manager server
certificate on page 4-46)

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.
(see Creating a secret key and a certificate signing request for
Common Component on page 4-33, Applying to a certificate authority
for a Common Component server certificate on page 4-36)

For communication with Host Data Collector
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.
(see Creating a key pair and a certificate signing request for Host
Data Collector on page 4-56, Applying to a certificate authority for a
Host Data Collector server certificate on page 4-58)

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.
(see Creating a secret key and a certificate signing request for
Common Component on page 4-33, Applying to a certificate authority
for a Common Component server certificate on page 4-36)

Information to collect in advance
• Path of the truststore file (see Truststores on page 4-30)
• Password to access the truststore, if the truststore already exists
To import a certificate into the truststore:

1. Execute the following command.

   In Windows:
   
   \installation-folder-for-Hitachi-Command-Suite\Base64\bin
   \hcems64keytool -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

   o 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.

   o file: Specify the certificate file.

   o 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 Manager 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.

   Import a certificate used for communication between Host Data Collector and the Device Manager server into dvmcacerts.

   o storepass: Specify the password used to access the truststore.

---

**Note:**

- 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 topics
- Starting the Hitachi Command Suite services on page 8-4
- Stopping the Hitachi Command Suite services on page 8-5

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 topics
- Registering an external authentication server and an external authorization server on page 3-17
Checking the certificates imported into the truststore for Hitachi Command Suite

To check the certificates imported into the truststore (ldapcacerts, jssecacerts or dvmcacerts), use the hcmds64keytool utility (for Windows) and the keytool utility (for Linux).

**Information to collect in advance**

- Path of the truststore file (see Truststores on page 4-30)
- Password to access the truststore

**To check the certificates imported into the truststore:**

1. Execute the following command.

   In Windows:
   ```batch
   installation-folder-for-Hitachi-Command-Suite\Base64\bin
   \hcmds64keytool -list -v -keystore truststore-file-name -storepass password-to-access-the-truststore
   ```

   In Linux:
   ```bash
   installation-directory-for-Hitachi-Command-Suite/Base64/
   uCPSB/jdk/bin/keytool -list -v -keystore truststore-file-name
   -storepass password-to-access-the-truststore
   ```

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.

**Operations to complete in advance**

- 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).

**Information to collect in advance**

- 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. (see server.https.port on page A-7)
To change the communication protocol between the Replication Manager server and the Device Manager server:

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.

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.

Operations to complete in advance

- 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 the following, 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.
  - VMware ESX 4.x
  - VMware ESXi 4.x
  - VMware vCenter Server 4.x
  - VMware ESXi 5.0, 5.0 Update 1, 5.1
  - VMware vCenter Server 5.0, 5.0 Update 1b, 5.1, 5.1.0a
  Replace the obtained server certificate with the self-signed certificate that is imported to the virtualization server. For details, see VMware manuals.

To import a certificate into the truststore:

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 topics
• Truststores on page 4-30

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.

Information to collect in advance
• Password for accessing the truststore

To check the certificate imported into the truststore:
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:
Changing the truststore password for the Host Data Collector

To change the truststore password for the Host Data Collector, use the keytool utility.

Operations to complete in advance

• Password for accessing the truststore

To change the truststore password:

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.

Related topics

• Truststores on page 4-30
Specify a new password (minimum of 6 characters).
4. Specify the new truststore password again.

Related topics
• Truststores on page 4-30

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.

Operations to complete in advance
• Configure an SSL server on a virtual server. For details, see VMware manuals.

To change a virtualization server information:
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.

Related topics
• ModifyVirtualizationServer command syntax: Hitachi Command Suite CLI Reference Guide

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 hbsa_keytool utility (for Windows) or the keytool utility (for UNIX).

Operations to complete in advance
• Obtain a server certificate.
  Obtain server certificates created by the management server by using a secure method.
  • Server certificate for the Device Manager server (see Applying to a certificate authority for a Device Manager server certificate on page 4-46)
    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).
To import a server certificate into the truststore:

1. Execute the following command:

In Windows:

```
installation-folder-for-Device-Manager-agent\bin
\hbsa_keytool -import -alias hdvm -file server-certificate
-keystore truststore-file-name -storepass password-for-accessing-truststore
```

In Linux:

```
installation-directory-for-Device-Manager-agent/agent/
JRE1.5/bin/keytool -import -alias hdvm -file server-certificate
-keystore truststore-file-name -storepass password-for-accessing-truststore
```

In Solaris, AIX, and HP-UX:

```
installation-directory-for-JDK-or-JRE/bin/keytool -import -
alias hdvm -file server-certificate -keystore truststore-file-name -storepass
password-for-accessing-truststore
```

- **alias**: Specify `hdvm` as the name that is used to identify the server certificate within the truststore.
- **file**: Specify the absolute path of the server certificate.
- **keystore**: Specify the following path as the truststore file of the import destination.
  - **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. The default password is `changeit`.

**Note:** Note the following when you use the `hbsa_keytool` utility to specify the truststore file name or password:

- Specify a forward slash (/) as a path delimiter.
- To specify a space in the path, enclose the path in double quotation marks (").
- 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 password in the truststore.

**Related topics**

- [Truststores on page 4-30](#)
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).

Information to collect in advance

- Password for accessing the truststore

To check the server certificate imported into the truststore:

1. Execute the following command:

   In Windows:
   
   ```
   installation-folder-for-Device-Manager-agent\bin
   hbsa_keytool -list -alias hdvm -keystore truststore-file-name -storepass password-for-accessing-truststore
   ```

   In Linux:
   
   ```
   installation-directory-for-Device-Manager-agent/agent/JRE1.5/bin/keytool -list -alias hdvm -keystore truststore-file-name -storepass password-for-accessing-truststore
   ```

   In Solaris, AIX, and HP-UX:
   
   ```
   installation-directory-for-JDK-or-JRE/bin/keytool -list -alias hdvm -keystore truststore-file-name -storepass password-for-accessing-truststore
   ```

   - **alias**: Specify hdvm as the name that is used to identify the server certificate within the truststore.
   - **storepass**: Specify the password for accessing the 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
     ```

Related topics

- Truststores on page 4-30

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).
Operations to complete in advance

- Password for accessing the truststore

To change the truststore password:

1. Execute the following command:

   In Windows:
   
   `installation-folder-for-Device-Manager-agent\bin\hbsa_keytool -storepass -keystore truststore-file-name`

   In Linux:
   
   `installation-directory-for-Device-Manager-agent/agent/JRE1.5/bin/keytool -storepass -keystore truststore-file-name`

   In Solaris, AIX, and HP-UX:
   
   `installation-directory-for-JDK-or-JRE/bin/keytool -storepass -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 topics

- Truststores on page 4-30

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).

Information to collect in advance

- Password for accessing the truststore
To delete a server certificate imported into the truststore:

1. Execute the following command:

In Windows:

```
installation-folder-for-Device-Manager-agent\bin\hbsa_keytool -delete -alias hdvm -keystore truststore-file-name -storepass password-for-accessing-truststore
```

In Linux:

```
installation-directory-for-Device-Manager-agent/agent/JRE1.5/bin/keytool -delete -alias hdvm -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 hdvm -keystore truststore-file-name -storepass password-for-accessing-truststore
```

- **alias**: Specify hdvm as the name that is used to identify the server certificate within the truststore.
- **storepass**: Specify the password for accessing the 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
    ```

Related topics

- Truststores on page 4-30

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.

Operations to complete in advance

- Configure an SSL server in the storage system. For details, see Storage Navigator Modular 2 manuals.
- Refresh the storage system
Information to collect in advance (for SMI-S enabled storage systems)

Port to communicate with the SMI-S provider (default: 5989).

To change a storage system information:

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.

Related topics

- AddStorageArray command syntax: Hitachi Command Suite CLI Reference Guide

Configuring an SSL server and clients (VSP G1000)

To improve security of remote operations from a management client to a storage system, configure SSL communication. By configuring SSL communication, the Device Manager - Storage Navigator User ID and Password are encrypted.

If you enable SSL, you must make sure that the key pair and associated server certificate do not expire. If either the key pair or the server certificate expires, users will be unable to connect to the SVP.

Notes on updating the signed certificate to the SVP

Read the following notes about uploading the signed certificate to the SVP:

- While the SVP server certificate is being updated, tasks that are being executed or scheduled for execution on Device Manager - Storage Navigator are not executed.
- Certificates for RMI communication are updated asynchronously (within approximately two minutes).
- If an SVP certificate is updated during Hitachi Command Suite setup operation, the Hitachi Command Suite setup operation will result in an error.
- Update of the SSL certificate gives a great influence to the system and may lead to SVP failure. Therefore take sufficient care about the content of the certificate and private key to be set.
- After the certificate update is complete, depending on the environment, the SVP web server can take 30 to 60 minutes to restart. When it takes that long, an internal server error occurs, and the update completion dialog box does not display. However, the certificate update is complete.
Creating a private key (.key file)

A private key is required to create an SSL keypair. The following procedure is for the Windows Vista® operating system.

Before you begin, download openssl.exe from the OpenSSL website.

To create a private key (.key file) in a Windows Vista environment:

1. If the read-only attribute is set, release it from the c:\openssl folder.
2. Open a command prompt.
3. Move the current directory to the folder to which the key file is output (such as c:\key), and execute the following command:
   
   ```
   c:\key > c:\openssl\bin\openssl genrsa -out server.key 2048
   ```

   This procedure creates a file called server.key in the c:\key folder. This file becomes the private key.

Creating a public key (.csr file)

A public key is required to create an SSL keypair. The following procedure is for the Windows Vista operating system.

Before you begin, download openssl.exe from the OpenSSL website.

To create a public key in a Windows Vista environment:

1. Open a command prompt.
2. Move the current directory to the folder to which the key file is output (such as c:\key). Execute the following command:
   
   ```
   c:\key > c:\openssl req -sha256 -new -key server.key -config c:\openssl\bin\openssl.cfg -out server.csr
   ```

3. Enter the following information in the prompt:
   - Country Name (two-letter code)
   - State or Province Name
   - Locality Name
   - Organization Name
   - Organization Unit Name
   - Common Name
     To create a self-signed certificate, enter the IP address of the web server (SVP). The name you entered here is used as the server name (host name). To obtain a signed and trusted certificate, ensure that the server name is the same as the host name of the SVP.
   - Email Address
   - Challenge password (optional)
   - Company name (optional)

The following example shows the contents of a command window when you create a public key.
is 65537 (0x10001)
C:\key>c:\openssl\bin\openssl req -sha256 -new -key server.key -config c
There are quite a few fields but you can leave some blank.
You are about to be asked to enter information that will be incorporated into
your certificate request. What you are about to enter is what is called a
Distinguished Name or a DN.
\openssl\bin\openssl.cfg -out server.csr
For some fields there will be a default value.
If you enter ".", the field will be left blank.

Country Name (2 letter code) [AU]:JP
State or Province Name (full name) [Some-State]:Kanagawa
Locality Name (eg, city) []:Odawara
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Hitachi
Organization Unit Name (eg, section) []:ITPD
Common Name (eg, YOUR name) []:192.168.0.1
Email Address []:

-----

Acquiring a signed certificate

After creating private key and public key, please acquire signed certificate file
of public key. Below are the three ways to acquire signed certificate file.

- Create a certificate by self-signing.
- Acquire a certificate of certificate authority which is used within your
  company.
- Acquire an official certificate by requesting one from a certificate authority
  such as VeriSign.

When you send a request to a certificate authority, specify SVP as the
host name. There will be an extra charge.

Note: Hitachi recommend that self-signed certificates be used only for
testing encrypted communication.

Acquiring a self-signed certificate

To acquire a self-signed certificate, open the command prompt and execute
the following command:

c:\key>c:\openssl\bin\openssl x509 -req -sha256 -days 10000 -in
server.csr -signkey server.key -out server.crt

Note: This command uses SHA-256 as a hash algorithm. MD5 or SHA-1 is
not recommended for a hash algorithm due to its low security level.

This creates a server.crt file in the c:\key folder, which is valid for 10,000
days. This is the signed private key, which is also referred to as a self-signed
certificate.
Acquiring a signed and trusted certificate

To acquire a signed and trusted certificate, you must acquire a certificate signing request (CSR), send that file to a Certificate Authority (CA), and request that the CA issue a signed and trusted certificate. Each certificate authority has its own procedures and requirements, and there is generally a cost for doing so. The signed and trusted certificate is the signed Public Key.

Uploading the signed certificate

To use SSL-encrypted communication, you must update and upload the private key and the signed Server Certificate (Public Key) to the SVP.

Prerequisites

- A private key (.key file) has been created. Change the file name to server.key unless the file is already named that.
- A signed public key certificate (.crt file) has been acquired. Change the file name to server.crt unless the file is already named that.
- The private key (.key file) and the signed public key certificate (.crt file) are in X509 PEM format.

Related information

- Notes on updating the signed certificate to the SVP on page 4-84

Procedure

To upload the signed SSL certificate:

1. Close all Device Manager - Storage Navigator sessions on the SVP.
2. Start the web browser.
3. In the browser of your Device Manager - Storage Navigator computer, specify the following URL:
   http://IP-address-or-host-name-of-SVP/cgi-bin/utility/toolpanel.cgi
4. In the **Tool Panel** dialog box, click **Update Certificate Files**. If SSL communication has been established, the Security Alert dialog box opens before the login dialog box opens. In the Security Alert dialog box, click **OK**. The Security Alert dialog box closes and the Login dialog box opens.

5. In the **Login** dialog box, enter the administrator user ID and password, and click **login**. The Upload dialog box opens.

6. In the **Upload** dialog box, enter the public key certificate file name in the Certificate file box and the private Key file name (server.key file) in the Key file box. You can enter the file names directly or by clicking **Browse**.

7. In the **Upload** dialog box, click **Upload**. A confirmation dialog box opens.

8. Click **OK** to begin the certificate update. When the update is complete, the SVP web server restarts. Depending on the environment, the SVP web server can take 30 to 60 minutes to restart. When it takes that long, an internal server error occurs, and the update completion dialog box does not display. However, the certificate update is complete. It can take 30 to 60 minutes for the web server to restart. After the SVP restarts, the Completion dialog box does **not** appear. Instead, an "internal server error" message is displayed. However, the setting is actually completed.

9. In the error message box, click **OK**. If the Security Alert dialog box for the certificate opens, click **View Certificate** to display the certificate. Confirm that the certificate is correct, and click **Yes**.

---

**Note:** If an error occurs during the certificate update, an error message displays. Resolve the problem described in the error message and then repeat this procedure, starting with Step 5 (log in) above.

---

**Returning the certificate to default**

You can return the certificate updated in **Uploading the signed certificate on page 4-87** to default.
To return the certificate to default:

1. Close all Device Manager - Storage Navigator sessions on the SVP.
2. Start the web browser.
3. Specify the following URL to open the Tool Panel dialog box
   http://IP-address-or-host-name-of-SVP/cgi-bin/utility/toolpanel.cgi

4. In the Tool Panel dialog box, click Update Certificate Files. The Update Certificate Files login dialog box opens.
   If SSL communication has been established, the Security Alert dialog box opens before the login dialog box. In the Security Alert dialog box, click OK.

5. In the Login dialog box, enter the administrator user ID and password, and click login. The Upload dialog box opens.

6. In the Upload dialog box, click Return to Default. A confirmation dialog box opens.

7. Click Yes to confirm and close the dialog box.
   When the certificate update is complete, the SVP Web server restarts to show the update. When the restart is complete, the Update Completion dialog box opens.

8. In the Update Completion dialog box, click OK. The dialog box closes and the display returns to the Login dialog box.

---

**Note:** If an error occurs during the certificate update, an error message appears. Resolve the problem described in the error message and then repeat this procedure, starting with Step 5 (log in) above.

**Note:** If the Security Alert dialog box for the certificate opens at other times, click View Certificate to confirm that the certificate is correct and then click Yes.
Importing the certificate to the SVP

If the public key certificate uploaded to SVP is self-signed or not signed by certificate authority which is in the browser by default, the browser displays a warning message when it connects to an SSL-enabled SVP. You can disable this by importing the certificate to the browser.

To import the certificate to the browser:

1. Log on to the Device Manager - Storage Navigator SVP using a secure connection (specify the URL using https).
   The Security Alert dialog box opens.

2. In the Security Alert dialog box, click Continue to this website (not recommended).

   The Certificate Invalid dialog box opens.

4. Click View certificates.
5. In the **Certificate** window, click the **General** tab.

![Certificate window](image)

**Figure 4-23 Certificate window (example)**

6. Click **Install Certificate**....
   
The welcome window of the Certificate Import Wizard opens.
Figure 4-24 Certificate Import Wizard dialog box (Welcome to the Certificate Import Wizard)

7. Click **Next**.
   The Certificate Store window of the wizard opens.
8. Select **Automatically select the certificate store based on the type of certificate** and click **Next**. The completion window opens.
9. Click **Finish**. If the import was successful, the confirmation window opens.

![Figure 4-27 Certificate Import wizard dialog box](image)

**Figure 4-27 Certificate Import wizard dialog box**

10. Click **OK**.

**Related topics**

- Normal login on page 5-26
Blocking HTTP communication to the storage system

If the web server supports SSL (HTTPS), the HTTP setting tool allows you to block access to port 80. This setting forces communication between the Web client and SVP to use only port 443 (HTTPS).

If you are using Device Manager - Hitachi Command Suite to access Device Manager - Storage Navigator, blocking HTTP communication might interfere with that access. Make sure the Hitachi Command Suite can use SSL communication to access Device Manager - Storage Navigator.

To block HTTP communication:

1. Close all Device Manager - Storage Navigator sessions on the SVP.
2. Start the web browser.
3. Specify the URL as follows:
   https://IP-address-or-host-name-of-SVP/cgi-bin/utility/toolpanel.cgi

4. In the Tool Panel dialog box, click Set up HTTP Blocking. A login dialog box opens.
5. In the Login dialog box, Enter the storage administrator User ID and Password, then click Login. The Set up HTTP Blocking dialog box opens.
6. In the dialog box, click OK. A confirmation dialog box opens.
7. In the confirmation dialog box, click OK to implement HTTP blocking. When the configuration change is complete, the SVP web server restarts. When the restart is complete, the HTTP Communications Blocked dialog box opens.

   Depending on the environment, it can take 30 to 60 minutes for the web server to restart. If it does, after the SVP restarts, the Completion dialog box does not appear. Instead, an "internal server error" message appears. However, the setting is actually completed.
8. Click **OK** to continue the operation and return to the Login dialog box, or click **Cancel** to cancel the operation and return to the Login dialog box.

### Releasing HTTP communication blocking

To release the HTTP communication blocking:

1. Close all Device Manager - Storage Navigator sessions on the SVP.
2. Start the web browser.
3. Specify the URL as follows:  
   https://IP-address-or-host-name-of-SVP/cgi-bin/utility/toolpanel.cgi

   ![Tool Panel](image)

   - Control Panel
   - Download Dump Files
   - Update Certificate Files
   - Set Up HTTP Blocking
   - Release HTTP Blocking
   - Update Certificate Files for SMI-S
   - Upload Configuration Files for SMI-S
   - SMI-S Artificial Indication
   - Set or Delete Certificate for HCS

4. In the Tool Panel dialog box, click **Release HTTP Blocking**.
5. Enter the User ID and Password for the root storage administrator, then click **Login**.
   The Release HTTP Blocking dialog box opens.
6. Click **OK**.
   A configuration dialog box opens.
7. Click **OK** to release HTTP blocking. When the configuration change is complete, the SVP web server reboots. Once the reboot is complete, the Release HTTP Blocking Complete dialog box opens.
   Depending on the environment, it can take 30 to 60 minutes for the web server to restart. After the SVP restarts, the Completion dialog box does **not** appear. Instead, an "internal server error" message is displayed. However, the setting is actually completed
8. Click **OK** to continue the operation and return to the Login dialog box, or click **Cancel** to cancel the operation and return to the Login dialog box.

### Using the SMI-S function

VSP G1000 storage systems support the SMI-S function developed by SNIA. Storage administrators can use the SMI-S function by using SMI-S compliant management software.
To use the SMI-S function, create a Device Manager - Storage Navigator user account and specify a storage system as the access destination from the management software.

**Prerequisites**
- SMI-S Provider software application must be installed.

**Procedure**

1. Create a Device Manager - Storage Navigator user account in the management software. The user account must belong to one of the following built-in user groups:
   - **Storage Administrator (View & Modify) User Group.** Users have full permissions to access the SMI-S function from the management software.
   - **Storage Administrator (View Only) User Group.** Users have read-only permissions to access the SMI-S function from the management software.

2. In the management software program, enter the following storage system information:
   - **IP Address** of the storage system
   - **Protocol:** specify HTTPS
   - **Port:** 5989
   - **Namespace:** root/hitachi/smis or interop

**Troubleshooting**

If you cannot access the SMI-S function, check the network environment and access destination.

**Uploading a signed certificate to the SMI-S provider**

To use certificates in SSL communication with the SMI-S provider, you must update and upload the private key and the signed server certificate (public key) to the SMI-S provider to update the certificate. Use the following procedure to upload and update certificates using a certificate update tool.

**Prerequisites**

Ensure that the following items have been completed:
- A private key (.key file) has been created. Change the file name to server.key unless the file is already named that.
- A signed public key certificate (.crt file) has been acquired. Change the file name to server.crt unless the file is already named that.
- The private key (server.key file) and the signed public key certificate (server.crt file) are in X509 PEM format.
Procedure

1. Close all Device Manager - Storage Navigator sessions on the SVP.
2. Start the web browser.
3. Specify the following URL to open the Tool Panel dialog box.
   \[http://IP-address-or-host-name-of-SVP/cgi-bin/utility/toolpanel.cgi\]

   ![Tool Panel](image)

4. In the Tool Panel dialog box, click **Update Certificate Files for SMI-S**. The login dialog box for **Update Certificate Files for SMI-S** opens. If SSL communication has been established, the Security Alert dialog box opens before the login dialog box. In the Security Alert dialog box, click **OK**.

5. In the login dialog box for Update Certificate Files for SMI-S, enter the administrator's user ID and password, and click **Login**. The upload dialog box for Update Certificate Files for SMI-S opens.

6. In the upload dialog box for Update Certificate Files for SMI-S, enter both the public key certificate file name in the Certificate file (server.crt file) box and the Private Key file (server.key file) box. You can enter the file names directly or by clicking **Browse**.

7. Click **Upload**. The execution confirmation dialog box for Update Certificate Files for SMI-S opens.

8. Click **OK** to update the certificate. Update of the certificate starts. Upon completion of the certificate update, the SMI-S provider restarts to reflect the update.

   Upon completion of the restart of the SMI-S provider, the update completion dialog box for Update Certificate Files for SMI-S opens

9. In the update completion dialog box for Update Certificate Files for SMI-S, click **OK**. The display returns to the login dialog box.

   **Note:** If an error occurs during update of the certificate, an error message displays. Resolve the problem and then run the procedure again, starting with logging in, to upload configuration files for SMI-S.
Note: If the Security Alert dialog box for the certificate opens at other times, click View Certificate to confirm that the certificate is correct and then click Yes.

Returning an SMI-S provider certificate to default

You can return a certificate updated in Uploading a signed certificate to the SMI-S provider on page 4-97 to default.

To return a certificate to default:

1. Close all Device Manager - Storage Navigator sessions on the SVP.
2. Start the web browser.
3. Specify the following URL to open the Tool Panel dialog box.
   http://IP-address-or-host-name-of-SVP/cgi-bin/utility/toolpanel.cgi

   ![Tool Panel](image)

4. In the Tool Panel dialog box, click Upload Configuration Files for SMI-S. The Upload Configuration Files Login dialog box opens.

   If SSL communication has been established, the Security Alert dialog box opens before the login dialog box. In the Security Alert dialog box, click OK.

5. In the Login dialog box, enter the administrator’s user ID and password, and click Login. The upload dialog box for Update Certificate Files for SMI-S opens.

6. In the upload dialog box for Update Certificate Files for SMI-S, click Return to the default configuration. The execution confirmation dialog box for Update Certificate Files for SMI-S opens.

7. Click OK to update the certificate. Update of the certificate starts.

   Upon completion of the certificate update, the SMI-S provider restarts to reflect the update. Upon completion of the restart of the SMI-S provider, the update completion dialog box for Update Certificate Files for SMI-S opens.
8. In the update completion dialog box for Update Certificate Files for SMI-S, click **OK**. The display returns to the login dialog box.

**Note:** If an error occurs during update of the certificate, an error message displays. Resolve the problem and then run the procedure again, starting with logging in, to update certificate files for SMI-S.

**Note:** If the Security Alert dialog box for the certificate opens at other times, click **View Certificate** to confirm that the certificate is correct and then click **Yes**.

### Uploading an SMI-S provider configuration file

You can control the SMI-S function using the SMI-S provider configuration file that you create.

#### Prerequisites

- Ensure that the SMI-S provider configuration file has already been created. If the configuration is not already named array-setting-01.properties, rename it to that name.

#### Procedure

**To upload the SMI-S provider configuration file:**

1. Close all Device Manager - Storage Navigator sessions on the SVP.
2. Start the web browser.
3. Specify the following URL to open the Tool Panel dialog box.
   
   ```
   http://IP-address-or-host-name-of-SVP/cgi-bin/utility/toolpanel.cgi
   ```

4. In the Tool Panel dialog box, click **Upload Configuration Files for SMI-S**. The Login dialog box opens.
If SSL communication has been established, the Security Alert dialog box opens before the Login dialog box. In the Security Alert dialog box, click OK to confirm and open the Login dialog box.

5. In the Login dialog box, enter the administrator user ID and password, and click Login. The Upload dialog box opens.

6. In the Upload dialog box, enter the SMI-S provider configuration file (array-setting-01.properties).
   Enter a file name in Configuration file or click Browse and then select a file in the displayed dialog box.

7. Click Upload. The execution confirmation dialog box opens.

8. Click OK to update the configuration file. Update of the configuration file starts.
   Upon completion of the configuration file update, the SMI-S provider restarts to reflect the update. Upon completion of the restart of the SMI-S provider, the update completion dialog box for Upload Configuration Files for SMI-S opens.

9. In the Upload Configuration Files for SMI-S dialog box, click OK. The display returns to the login dialog box.

   **Note:** If an error occurs during update of the certificate, an error message displays. Resolve the problem and then run the procedure again, starting with logging in, to upload configuration files for SMI-S.

   **Note:** If the Security Alert dialog box for the certificate opens at other times, click View Certificate to confirm that the certificate is correct and then click Yes.

### Returning an SMI-S provider configuration file to default

You can return the configuration file updated in Uploading an SMI-S provider configuration file on page 4-100.

**To return the configuration file to default:**

1. Close all Device Manager - Storage Navigator sessions on the SVP.
2. Start the web browser.
3. Specify the following URL to open the Tool Panel dialog box.
   `http://IP-address-or-host-name-of-SVP/cgi-bin/utility/toolpanel.cgi`
4. In the Tool Panel dialog box, click **Upload Configuration Files for SMI-S**. The Login dialog box opens. If SSL communication has been established, the Security Alert dialog box opens before the Login dialog box. In the Security Alert dialog box, click **OK** to confirm and open the Login dialog box.

5. In the **Login** dialog box, enter the administrator user ID and password, and click **Login**. The Upload dialog box opens.

6. In the **Upload** dialog box, click **Return to the default configuration**. A confirmation dialog box opens.

7. In the confirmation dialog box, Click **OK** to update the configuration file. The update process starts. When the file has been updated, the SMI-S provider restarts to include the update. When the SMI-S provider restarts, the update completion dialog box opens.

8. In the update completion dialog box, click **OK** to confirm and return to the Login dialog box.

---

**Note:** If an error occurs during update of the SMI-S provider configuration file, an error message appears. Resolve the problem described in the error message and then run the procedure again, starting with Step 5.

**Note:** If the Security Alert dialog box for the certificate opens at other times, click **View Certificate** to confirm that the certificate is correct and then click **Yes**.

---

**Sending SMI-S Artificial Indication**

You can send an SMI-S artificial indication to determine whether the communication between the listeners and the SMI-S provider succeeds or fails.

**Prerequisites**

- SMI-S Provider software application must be installed.
• The network environment is configured so that the computer on which the listener application operates is connected to the SVP.
• The listeners are subscribed to the SMI-S provider.

**Procedure**

To send an SMI-S artificial indication:

1. Close all Device Manager - Storage Navigator sessions connected to the related SMI-S provider.
2. On the Device Manager - Storage Navigator computer, open a web browser and enter the following URL to open the Tool Panel dialog box.
   
   
   \[ http://IP-address-or-host-name-of-SVP/cgi-bin/utility/toopanel.cgi \]

   ![](Tool_Panel.png)

3. In the Tool Panel dialog box, click SMI-S Artificial Indication. The SMI-S Artificial Indication dialog box opens.
4. In the SMI-S Artificial Indication dialog box, enter the user ID and password, and click Test. The testing begins.
5. When the test communication is completed, SMI-S Artificial Indication Result window opens.

   In the SMI-S Artificial Indication Result window, click OK. The dialog box closes and the display returns to the SMI-S Artificial Indication dialog box.

---

**Note:** If the SMI-S artificial indication fails, an error message and a code display. Resolve the problem described in the error message.

**Array-setting-01.properties file**

This section describes the description format and organization format of SMI-S provider user configuration files and parameters to be defined. The array-setting-01.properties file is an SMI-S provider user configuration file.
File description format
The format of the array-setting-01.properties file includes the following items:

- File format: text
- Character code: ISO 8859-1
- Line-end symbol: \n, \r, or \r\n
Comment: Line on which # or ! is the first non-space character

File organization format
The organization of the array-setting-01.properties file is shown here:

# comment line
parameter1= parameter1_setting_value
parameter2= parameter2_setting_value
# comment line

Parameters defined in user configuration files

<table>
<thead>
<tr>
<th>Parameter name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VVolForSnapshot</td>
<td>Use the VVolForSnapshot parameter to specify virtual volumes that the SMI-S provider can use when you operate Thin Image from CreateElementReplica of HITACHI_ReplicationService. Optional item. If no value is specified, the default value applies. If you specify this item, be sure to specify PoolIDForSnapshot as well. All virtual volumes are specified by default. Setting up the VVolForSnapshot parameter Set up the parameter by using &lt;RangeOfVVol&gt; and &lt;SingleVVol&gt; with a comma (,) as a delimiter: - &lt;RangeOfVVol&gt;: Specifies a range of virtual volumes - &lt;SingleVVol&gt;: Specifies a single virtual volume &lt;RangeOfVVol&gt; format &lt;S2HexLDKC&gt;:&lt;S2HexCU&gt;:&lt;S2HexLDEV&gt;to&lt;E2HexLDKC&gt;:&lt;E2HexCU&gt;:&lt;E2HexLDEV&gt; - &lt;S2HexLDKC&gt;: LDKC number (two-digit hexadecimal) of the first virtual volume in the specified range - &lt;S2HexCU&gt;: CU number (two-digit hexadecimal) of the first virtual volume in the specified range - &lt;S2HexLDEV&gt;: LDEV number (two-digit hexadecimal) of the first virtual volume in the specified range - &lt;E2HexLDKC&gt;: LDKC number (two-digit hexadecimal) of the last virtual volume in the specified range - &lt;E2HexCU&gt;: CU number (two-digit hexadecimal) of the last virtual volume in the specified range - &lt;E2HexLDEV&gt;: LDEV number (two-digit hexadecimal) of the last virtual volume in the specified range</td>
</tr>
<tr>
<td>Parameter name</td>
<td>Description</td>
</tr>
<tr>
<td>----------------</td>
<td>-------------</td>
</tr>
<tr>
<td>&lt;E2HexCU&gt;: CU number (two-digit hexadecimal) of the last virtual volume in the specified range</td>
<td></td>
</tr>
<tr>
<td>&lt;E2HexLDEV&gt;: LDEV number (two-digit hexadecimal) of the last virtual volume in the specified range</td>
<td></td>
</tr>
<tr>
<td><strong>SingleVVol</strong> format</td>
<td></td>
</tr>
<tr>
<td>&lt;2HexLDKC&gt;:&lt;2HexCU&gt;:&lt;2HexLDEV&gt;</td>
<td></td>
</tr>
<tr>
<td>- &lt;2HexLDKC&gt;: LDKC number (two-digit hexadecimal) of the single virtual volume to be specified</td>
<td></td>
</tr>
<tr>
<td>- &lt;2HexCU&gt;: CU number (two-digit hexadecimal) of the single virtual volume to be specified</td>
<td></td>
</tr>
<tr>
<td>- &lt;2HexLDEV&gt;: LDEV number (two-digit hexadecimal) of the single virtual volume to be specified</td>
<td></td>
</tr>
<tr>
<td><strong>Example</strong></td>
<td></td>
</tr>
<tr>
<td>VVolForSnapshot=00:00:00to00:00:FF, 00:02:00,00:04:00to00:04:FF</td>
<td></td>
</tr>
<tr>
<td>In this example, a virtual volume having one of the following LDEV IDs is used as the snapshot target:</td>
<td></td>
</tr>
<tr>
<td>- From 00:00:00 (LDKC=0,CU=0,LDEV=0) to 00:00:FF (LDKC=0,CU=0,LDEV=255)</td>
<td></td>
</tr>
<tr>
<td>- 00:02:00 (LDKC=0,CU=2,LDEV=0)</td>
<td></td>
</tr>
<tr>
<td>- From 00:04:00 (LDKC=0,CU=4,LDEV=0) to 00:04:FF (LDKC=0,CU=4,LDEV=255)</td>
<td></td>
</tr>
</tbody>
</table>

**PoolIDForSnapshot**

Use the PoolIDForSnapshot parameter to specify pools that the SMI-S provider can use when you run Thin Image from CreateElementReplica of HITACHI_ReplicationService.

Specifies pools that can be used by the SMI-S provider.

Optional item. If no value is specified, the default value applies. If you specify this item, be sure to specify VVolForSnapshot as well.

All pools are specified by default.

Setting up the PoolIDForSnapshot parameter

Set up the parameter by using <RangeOfPoolID> and <SinglePoolID> with a comma (,) as a delimiter:

- <RangeOfPoolID>: Specifies a range of pool IDs
- <SinglePoolID>: Specifies a single pool ID

**<RangeOfPoolID> format**

<Start PoolID>to<End PoolID>

- <Start PoolID>: ID of the first pool in the specified range
- <End PoolID>: ID of the last pool in the specified range

**<SinglePoolID> format**

<PoolID>

- <PoolID>: ID of the pool to be specified

**Example**

PoolIDForSnapshot=1to2,4,6to8

In this example, pools having one of the following pool IDs are used as snapshot pools:
Registering certificates for HCS

To check the server reliability at the time of SSL communication for HCS external authentication, upload an HCS public key certificate to the web server to register the certificate. Complete the steps in the following procedure to upload and register a certificate using the certificate update tool.

Prerequisites

- You must have Security Administrator (View & Modify) role to perform this task.
- If the certificate to be registered has an extension other than ".crt", change it to ".crt".
- The certificate to be registered must be in X509 format.

To register certificates for HCS:

1. Close all Device Manager - Storage Navigator sessions on the SVP.
2. On the Device Manager - Storage Navigator computer, open a web browser and enter the following URL to open the Tool Panel dialog box.

   http://IP-address-or-host-name-of-SVP/cgi-bin/utility/toolpanel.cgi

3. In the Tool Panel dialog box, click Set or Delete Certificate File for HCS. The Login dialog box opens. If SSL communication has been established, the Security Alert dialog box opens before the Login dialog box. In the Security Alert dialog box, click OK.
4. When the Login dialog box opens, enter the administrator user ID and password, and click **Login**. The Login dialog box opens.

5. In the dialog box, enter the certificate file for HCS (.crt file) in the Certificate file (.crt file) box. You can enter the file name directly or by clicking **Browse** and searching for the file name.

6. Click **Register**. The execution confirmation dialog for **Set or Delete Certificate File for HCS** opens.

7. Click **Register**. The execution confirmation dialog for **Set or Delete Certificate File for HCS** opens.

8. In the registration completion dialog box for **Set or Delete Certificate File for HCS**, click **OK**. The display returns to the login dialog box.

**Note:** If an error occurs during registration of the HCS certificate, an error message displays. Resolve the problem and then run the procedure again, starting with logging in, to Set or Delete HCS Certificate.

**Note:** If the Security Alert dialog box for the certificate opens at other times, click **View Certificate** to confirm that the certificate is correct and then click **Yes**.

**Related Topics**

- [Deleting certificates for HCS on page 4-107](#)

**Notes on registering certificates for HCS**

Read the following notes about registering certificates for HCS:

- Ensure that the certificate to be registered is the right one. If you register a wrong certificate, HCS external authentication is not performed.
- Only with registration or deletion of the correct certificate, HCS external authentication operates normally.

**Deleting certificates for HCS**

You can delete the certificates you registered in the procedure of the "Registering certificates for HCS" section. Once you delete a certificate, server, reliability for that certificate is not checked by SSL communication for HCS external authentication.

**Prerequisites**

- You must have Security Administrator (View & Modify) role to perform this task.

To delete certificates for HCS:

1. Close all Device Manager - Storage Navigator sessions on the SVP.
2. On the Device Manager - Storage Navigator computer, open a web browser and enter the following URL to open the Tool Panel dialog box.
In the Tool Panel dialog box, click **Set or Delete Certificate File for HCS**. The login dialog box opens. If SSL communication has been established, the Security Alert dialog box opens before the login dialog box. In the Security Alert dialog box, click **OK**.

4. In the login dialog box, enter the administrator user ID and password, and click **Login**. The **Set or Delete Certificate File for HCS** dialog box opens.

5. In the dialog box, click **Delete**. A confirmation dialog box opens.

6. Click **OK** to delete the certificate. Deletion of the certificate starts. When the certificate has been deleted, a completion dialog box opens.

7. In the completion dialog box click **OK**. The display returns to the login dialog box.

---

**Note:** If an error occurs during deletion of the certificate for HCS, an error message displays. Resolve the problem and then run the procedure again, starting with logging in, to Set or Delete Certificate for HCS.

---

**Note:** If the Security Alert dialog box for the certificate opens at other times, click **View Certificate** to confirm that the certificate is correct and then click **Yes**.

### 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.
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 `hcms64keytool` utility (for Windows) or the `keytool` utility (for Linux).

**Operations to complete in advance**

- 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
  ```

**To create a keystore file for object operations:**

1. Execute the following command to create a keystore file for object operations.

   In Windows:
   
   ```
   installation-folder-for-Hitachi-Command-Suite\Base64\bin\hcms64keytool -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
   ```

   o **keystore**: Specify the keystore file for object operations (.keystore).
   
   o **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\WSIEncryptString.jar
   ```
In Linux:

```
installation-directory-for-Hitachi-Command-Suite/
HiCommandServer/wsi/server/jserver/lib/
```

```
> java -jar WSIEncryptString.jar keystore-password
```

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.

**Operations to complete in advance**

Create a keystore file for object operations.

**Information to collect in advance**

Keystore password encrypted by WSIEncryptString.jar.

**To edit an MOF file for object operations:**

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 topics
• Starting the Hitachi Command Suite services on page 8-4
• Stopping the Hitachi Command Suite services on page 8-5

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.

Operations to complete in advance
Edit the MOF file for object operations.

Information to collect in advance
• Keystore password for object operations
• Alias name of the server certificate for object operations

To export a server certificate for object operations:
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.
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.

**To enable two-way authentication for object operations:**

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 topics**

- [Starting the Hitachi Command Suite services on page 8-4](#)
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.

Operations to complete in advance

- Obtain the client certificate for object operations from a CIM client (see Exporting a server or client certificate for a CIM client on page 4-121).
- Delete the existing truststore file for object operations (.truststore). (see Truststores on page 4-30)

To import a client certificate for object operations:

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:trustssl
   Enter authentication-filename(absolute path):c:\tmp\client.cer

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).

Operations to complete in advance

- 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

To create a keystore file for event indications:

1. Execute the following command to create a keystore file for event indications:

In Windows:
installation-folder-for-Hitachi-Command-Suite\Base64\bin
\hcmds64\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

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
> java -jar WSIEncryptString.jar keystore-password
```

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.
Operations to complete in advance

Create a keystore file for event indications.

To edit an MOF file for event indications:

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 xxxxxxxx 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\jservlet\logr ..\server\jserver\mof\wbemserver\CIMXMLSOMATLSSettingData_instances.mof
```

4. Start the Hitachi Command Suite product services.

Related topics

- Starting the Hitachi Command Suite services on page 8-4
- Stopping the Hitachi Command Suite services on page 8-5
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.

**Operations to complete in advance**

Edit the MOF file for event indications.

**Information to collect in advance**

- Keystore password for event indications
- Alias name of the client certificate for event indications

**To export a client certificate for event indications:**

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.

**To enable two-way authentication for event indications:**

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 topics

- Starting the Hitachi Command Suite services on page 8-4
- Stopping the Hitachi Command Suite services on page 8-5

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.

Operations to complete in advance

- Obtain a CIM client server certificate for event indications (see Exporting a server or client certificate for a CIM client on page 4-121).
- Delete the existing truststore file for event indications (indtruststore). (see Truststores on page 4-30)
To import a server certificate for event indications:

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 into 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
   ```

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).

Information to collect in advance

- Keystore password

To check a self-signed certificate for a CIM server:

1. 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.

**To disable two-way authentication:**

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\nIn Linux:
installation-directory-for-Hitachi-Command-Suite/
HiCommandServer/wsi/server/jserver/mof/

Related topics

- Starting the Hitachi Command Suite services on page 8-4
- Stopping the Hitachi Command Suite services on page 8-5

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.

Operations to complete in advance

Install Java onto a CIM client.

To create a key pair and self-signed certificate for a CIM client:

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:
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.

**Operations to complete in advance**
- Install Java onto the CIM client.
- Create a CIM client server certificate.

**Information to collect in advance**
- 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

**To export a server or client certificate for a CIM client:**

1. Execute the following command to export the server or client certificate for a CIM client:
   ```bash
   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:
   ```bash
   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.

**Operations to complete in advance**
- Install Java onto the CIM client.
- Obtain a Device Manager server certificate (see Exporting a server certificate for object operations on page 4-111, Exporting a client certificate for event indications on page 4-116).

**Information to collect in advance**
- CIM client truststore password

**To import a server or client certificate into a CIM client:**

1. Execute the following command to import a server or client certificate for the Device Manager:
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.

Information to collect in advance

- 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)

To control management client access to the management server:

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**

```xml
<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**

```xml
<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>
```


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 topics**

- [Starting the Hitachi Command Suite services on page 8-4](#)
- [Stopping the Hitachi Command Suite services on page 8-5](#)
- [server.http.security.clientIP on page A-30](#)
- [server.http.security.clientIPv6 on page A-30](#)
Changing the password-encoding level in the Device Manager CLI and the Tiered Storage Manager CLI

If a password is specified in advance, you do not need to enter your password when you execute commands by using the Device Manager CLI or the Tiered Storage Manager CLI.

If you want to specify a password in advance, we recommend that you encode the password character string before specifying it.

There are two levels for encoding passwords, NORMAL and HIGH. In the NORMAL level, a password is encoded with a 128-bit key length. In the HIGH level, it is encoded with a 256-bit key length.

If you want to change the encoding level to HIGH, you need to download and install the Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files for the JRE version you are using. Download the Jurisdiction Policy files from the Oracle corporation website (if the management client OS is Windows, Solaris, HP-UX, or Linux) or the IBM website (if the management client OS is AIX). For details about how to install the files, see the documentation provided with the Jurisdiction Policy files.

Related topics

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
- Analyzing the performance of Universal Replicator
- Settings necessary to launch Hitachi Storage Services Manager
- Using the Device Manager - Storage Navigator (VSP G1000)
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 from Element Manager of 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 on how to use Storage Navigator Modular 2 to register user accounts, see the documentation for Storage Navigator Modular 2. For details on how to assign a resource group, 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.

Related topics:

- How to assign resource groups: *Hitachi Command Suite User Guide*

Settings for using Element Manager

To operate a Hitachi AMS/WMS storage system from Element Manager, you must use launchapptool to specify environment settings.

To use Element Manager:

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 1.
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 launachapptool.

---

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 topics**

- [Starting the Hitachi Command Suite services on page 8-4](#)
- [Stopping the Hitachi Command Suite services on page 8-5](#)

### 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.

**To delete the settings for using Element Manager:**

1. Execute the following command from the command prompt or terminal window:
   - In Windows:
     ```
     installation-folder-for-Hitachi-Command-Suite\DeviceManager \HiCommandServer\tools\launachapptool.bat
     ```
   - In Linux:
     ```
     installation-directory-for-Hitachi-Command-Suite/
     HiCommandServer/tools/launachapptool.sh
     ```

2. The main menu appears. Select 2.
   A list of the launch environment settings appears.

   A deletion confirmation message appears.
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 topics
- Starting the Hitachi Command Suite services on page 8-4
- Stopping the Hitachi Command Suite services on page 8-5

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.

The following shows the settings that are prerequisite for storage systems and machines.

Figure 5-1 Example of a system configuration for collecting storage system performance information

This might be installed on a different computer than Device Manager.
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
- 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.

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.

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 topics
- Changing Device Manager server properties on page A-4
- How to set up Tuning Manager server and Tuning Manager - Agent for RAID: Tuning Manager Installation Guide
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.
- Tuning Manager - Agent for RAID is configured so that the Tuning Manager API can be used.
- 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 Tuning Manager API is used, specify a resolvable host name of Tuning Manager - Agent for RAID in the `user.properties` file on the Tuning Manager server.
- 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.

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 topics**

- Registering firewall exceptions for Device Manager and Tiered Storage Manager on page 2-15
- Operation workflow for secure communication between a Tuning Manager server and a Device Manager server on page 4-16
- Changing Device Manager server properties on page A-4
- `server.dispatcher.daemon.autoSynchro.performance.startTime` on page A-27
- Port numbers used by the Tuning Manager server, and how to set up the Tuning Manager server and Tuning Manager - Agent for RAID: *Tuning Manager Installation Guide*
- Port numbers used by Tuning Manager - Agent for RAID: *Tuning Manager Agent Administration Guide*
- About the `user.properties` file on the Tuning Manager server: *Hitachi Command Suite Tuning Manager Server Administration Guide*

**Settings for collecting storage system performance information**

This subsection describes settings for collecting performance information from enterprise-class storage systems (VSP G1000, Virtual Storage Platform, Universal Storage Platform V/VM, and Hitachi USP) and HUS VM, and from midrange storage systems (HUS100, Hitachi AMS2000, Hitachi SMS, and Hitachi AMS/WMS).

**Settings for collecting performance information from enterprise-class storage systems and HUS VM**

Before Tuning Manager - Agent for RAID can collect performance information from enterprise-class storage systems (VSP G1000, Virtual Storage Platform, Universal Storage Platform V/VM, and Hitachi USP) and HUS VM, specify the necessary settings in the enterprise-class storage systems with HUS VM:

- The microcode versions of the storage systems to be monitored are supported by Tuning Manager - Agent for RAID.
- 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.
- When the storage system to be monitored is Hitachi USP, settings are configured for the `PI_RGS` record so that performance information is collected by Performance Monitor.
- When performing a health check, the record storage period must be set to the records below. For details on the record storage period to be set, see...
Table 5-1 Record storage period to be set when performing a health check (for enterprise-class storage systems and HUS VM) on page 5-11.

- PI_CLPS record
- PI_LDA record
- PI_PLS record (No settings are required for Hitachi USP.)
- PI_PRCS record
- PI_PTS record
- PI_RGS record

Table 5-1 Record storage period to be set when performing a health check (for enterprise-class storage systems and HUS VM)

<table>
<thead>
<tr>
<th>Store database version</th>
<th>Property name</th>
<th>Setting value</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>Product Interval - Hour Drawer</td>
<td>Month</td>
</tr>
<tr>
<td></td>
<td>Product Interval - Day Drawer</td>
<td>Year</td>
</tr>
<tr>
<td>2.0</td>
<td>Period - Hour Drawer (Day)</td>
<td>9 or more</td>
</tr>
<tr>
<td></td>
<td>Period - Day Drawer (Week)</td>
<td>5 or more</td>
</tr>
</tbody>
</table>

Related topics

- Prerequisite microcode versions of storage systems monitored by Tuning Manager - Agent for RAID, how to setup of command devices, and how to setup of records for collection performance information: *Tuning Manager Installation Guide*
- How to set the record retention period: *Hitachi Command Suite Tuning Manager Agent Administration Guide*

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.
- 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.
- 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
When performing a health check, the record storage period must be set to the records below. For details on the record storage period to be set, see Table 5-2 Record storage period be set when performing a health check (for midrange storage systems) on page 5-12.

### Table 5-2 Record storage period be set when performing a health check (for midrange storage systems)

<table>
<thead>
<tr>
<th>Store database version</th>
<th>Property name</th>
<th>Setting value</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>Product Interval - Hour Drawer</td>
<td>Month</td>
</tr>
<tr>
<td>1.0</td>
<td>Product Interval - Day Drawer</td>
<td>Year</td>
</tr>
<tr>
<td>2.0</td>
<td>Period - Hour Drawer (Day)</td>
<td>9 or more</td>
</tr>
<tr>
<td>2.0</td>
<td>Period - Day Drawer (Week)</td>
<td>5 or more</td>
</tr>
</tbody>
</table>

### Related topics

- Prerequisite microcode versions of storage systems monitored by Tuning Manager - Agent for RAID, how to create accounts only for Tuning Manager - Agent for RAID, how to setup of records for collection performance information, and checking for duplicated serial numbers (device IDs): Tuning Manager Installation Guide
- How to set the record retention period: Tuning Manager Agent Administration Guide
- How to set the record retention period: Hitachi Command Suite Tuning Manager Agent Administration Guide

### Operation workflow for setting up the Device Manager server (collection of storage system performance information)

Before you can collect storage system performance information, you must set the Device Manager server properties related to linkage with Tuning Manager,
and then you must 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.

Figure 5-2 Operation workflow for setting up the Device Manager server (collection of 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 topics**

- [Registering an SMTP authentication user account in Device Manager](#)
- [Starting the Hitachi Command Suite services](#)
- [Stopping the Hitachi Command Suite services](#)
- [server.mail.enabled.storagesystem](#)
- [server.mail.from](#)
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.

**Operations to complete in advance**

- 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)

**To remotely connect to the Tuning Manager server:**

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 topics**

- Port numbers that must be registered as firewall exceptions for Device Manager and Tiered Storage Manager on page 2-15
- Stopping the Hitachi Command Suite services on page 8-5

Remote connection to the Tuning Manager server (in a cluster environment)

In a 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.

**Operations to complete in advance**

- **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**

**To remotely connect to the Tuning Manager server:**

1. In the cluster application, take the following services offline:
   - HiCommand Tiered Storage Manager
   - HiCommandServer
   - HCS Device Manager Web Service
   - HBase 64 Storage Mgmt Web Service
   - HBase 64 Storage Mgmt Common Service
   - HBase 64 Storage Mgmt SSO Service
   - HBase 64 Storage Mgmt Web SSO Service
   - Hitachi Command Suite product resources other than the above
2. Stop the Hitachi Command Suite product services.
3. In the cluster application, take the following service offline:
   - HiRDB/ClusterService _HD1
4. Use the cluster management application to disable failover of the following resource groups:
   - HiCommand Tiered Storage Manager
   - HBase 64 Storage Mgmt Common Service
   - HBase 64 Storage Mgmt Web Service
   - HBase 64 Storage Mgmt SSO Service
   - HBase 64 Storage Mgmt Web SSO Service
   - HCS Device Manager Web Service
   - HiCommandServer
   - HiRDB/ClusterService _HD1
   - Services that were taken offline in step 1
   - Right-click a resource name, and select **Properties**. Then, click the **Policies** tab, and select **If resource fails, do not restart**.
5. Execute the `htmsetup` command.
6. When a menu is displayed, select 1 (Configure the settings for remote connection).
7. 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.

8. Stop the Hitachi Command Suite product services.

9. Move the group in which the Hitachi Command Suite product services have been registered to the standby node.

10. On the standby node, execute the `htmsetup` command. Specify the same settings as those on the executing node.

11. Stop the Hitachi Command Suite product services.

12. In the Services window, open the properties for the following services, and then change **Startup Type** from **Automatic** to **Manual**:

  - HBase 64 Storage Mgmt Common Service
  - HBase 64 Storage Mgmt Web Service
  - HBase 64 Storage Mgmt SSO Service
  - HBase 64 Storage Mgmt Web SSO Service
  - HCS Device Manager Web Service
  - HiCommandServer
  - HiCommand Tiered Storage Manager

13. In the cluster management application, enable failover of the following resource groups:

  - HBase 64 Storage Mgmt Common Service
  - HBase 64 Storage Mgmt Web Service
  - HBase 64 Storage Mgmt SSO Service
  - HBase 64 Storage Mgmt Web SSO Service
  - HCS Device Manager Web Service
  - HiCommandServer
  - HiCommand Tiered Storage Manager
  - HiRDB/ClusterService _HD1
  - Hitachi Command Suite product resources other than the above

   Right-click a resource name, and select **Properties**. Then, open the **Policies** tab, and select the following items: **If resource fails, attempt restart on current node** and **If restart is unsuccessful, fail over all resources in this Role** (or **If restart unsuccessful, fail over all resources in this service or application**)

14. In the cluster application, bring online the group in which the Hitachi Command Suite product services have been registered.

**Related topics**

- [Stopping the Hitachi Command Suite services on page 8-5](#)
- For services and resource groups that need to be removed from cluster management targets other than Device Manager and Tiered Storage Manager: The documentation for each Hitachi Command Suite product.
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 (see Stopping the Hitachi Command Suite services on page 8-5)
- 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:
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 topics

- Port numbers that must be registered as firewall exceptions for Device Manager and Tiered Storage Manager on page 2-15
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 AnalyticsReportDefV810. 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.

Related topics

- 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: Hitachi Command Suite User Guide
- How to register licenses and specify permission settings in Tuning Manager: Tuning Manager Server Administration Guide
- How to import report definitions into Performance Reporter of Tuning Manager: Tuning Manager Server User Guide

Analyzing the performance of Universal Replicator

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

To analyze the performance of Universal Replicator, either an open system that is configured to manage Universal Replicator copy groups or an open system that uses Tuning Manager is required.
Before the management client can connect to the Device Manager servers at the primary and secondary sites, all of the following conditions must be satisfied:

- The Tuning Manager server is installed at the same site as the Device Manager server that is connected from the management client (the site on the Replication tab side).
- Replication Manager at the site not on the Replication tab side is in maintenance mode.
- Tuning Manager - Agent for RAID is set up at both sites.

The following figures are examples of systems that are configured to analyze Universal Replicator performance by connecting the management client to the Device Manager server at the primary site.
Figure 5-3 Example of a system that is configured to analyze performance by connecting to the Device Manager server at the primary site

**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 topics
- About the maintenance mode of Replication Manager: Replication Manager Configuration Guide

Settings on Device Manager for analyzing Universal Replicator performance

To analyze Universal Replicator performance, check the following settings:
- The property settings in the replication.properties file of the Device Manager server
  You can periodically collect information required for analysis from Replication Manager and Tuning Manager. 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.
- The rpmlib.rpm.port property settings in the rpmlib.properties file of the Device Manager server
  If you change the base.rmi.port property in the base.properties file of the Replication Manager server to change the port number used for communication between Replication Manager and the RMI registry, you must also change the rpmlib.rpm.port property in the rpmlib.properties file of the Device Manager server.

Note: If you change the locale of the Device Manager server while managing copy groups by using the Replication tab, graphs might not be displayed correctly in the Replication tab. For this reason, we do not recommend that you change the locale.

Tip: When daylight saving time applies, the information collection time required for analysis is coordinated according to the daylight saving time.

Related topics
- Changing Device Manager server properties on page A-4
- Properties related to Universal Replicator performance analysis (replication.properties file) on page A-46
- rpmlib.rpm.port on page A-50
• About the `base.rmi.port` property in the Replication Manager `base.properties` file: *Replication Manager Configuration Guide*

**Settings on Replication Manager for analyzing Universal Replicator performance**

To analyze Universal Replicator performance, the settings for copy groups to be analyzed must be completed in Replication Manager and the settings for the Replication Manager properties must be completed.

Make sure that the following Replication Manager settings are completed.

- C/T Delta alerts are set for the copy groups to be analyzed.
- In the Replication Manager `base.properties` file, the `base.rmi.enabled` property is set to `true`.

**Related topics**

- Settings on Replication Manager: *Replication Manager User Guide*
- About the `base.rmi.enabled` property in the Replication Manager `base.properties` file: *Replication Manager Configuration Guide*

**Settings on Tuning Manager for analyzing Universal Replicator performance**

Before you can analyze Universal Replicator performance, you must specify the Tuning Manager settings for collecting storage system performance information.

In addition, to collect performance information for the following metrics, you must change settings from the default so that performance data is recorded.

**Table 5-3 Records that must be specified for analyzing Universal Replicator performance information**

<table>
<thead>
<tr>
<th>Metric</th>
<th>Record</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cache Write Pending Rate</td>
<td>PI_CLMS</td>
</tr>
<tr>
<td>Host Write Transfer Rate to M-JNL</td>
<td>PI_JNLs</td>
</tr>
<tr>
<td>M-JNL Async Transfer Rate to RCU</td>
<td></td>
</tr>
<tr>
<td>Host Write IOPS to M-JNL</td>
<td></td>
</tr>
<tr>
<td>Read M-JNL Process Time</td>
<td></td>
</tr>
<tr>
<td>End-to-End Journal Copy Time</td>
<td></td>
</tr>
</tbody>
</table>

To specify the records above, use either of the following methods to change the method for recording performance data for the records:

To change the method for recording performance data in the GUI
Change the method in the Properties window of the Agent Collector service in Performance Reporter.

In the Properties window of the Agent Collector service, expand the **Interval Records** node in **Service Properties**, select a record (CLMS or JNLS) to be specified, and then set the **Log** property to **Yes**.

For details, see the *Hitachi Command Suite Tuning Manager Agent Administration Guide*.

To change the method for recording performance data by using a command

Execute the Performance Reporter `jpcasrec update` command.

For the parameter file to be specified for an option of the `jpcasrec update` command, specify the `log` parameter and set the value to **Yes**.

For details about the `jpcasrec update` command, see the *Hitachi Command Suite Tuning Manager CLI Reference Guide*.

**Related topics**

- [Settings required to collect storage system performance information on page 5-6](#)

**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.

**Operations to complete in advance**

Log in as a user with Administrator permissions (for Windows) or as a root user (for Linux).

**Information to collect in advance**

- Hitachi Storage Services Manager startup URL
  
  For details, see the applicable Hitachi Storage Services Manager manual.

**To launch the Hitachi Storage Services Manager GUI:**

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:
Using the Device Manager - Storage Navigator (VSP G1000)

This section explains Device Manager - Storage Navigator operations.

Logging in to Device Manager - Storage Navigator

There are two types of logins to Device Manager - Storage Navigator:

- One-time only initial login by the administrator or super-user who logs in first to create other user accounts
- Normal login allows users to perform only tasks related to initial settings such as account management or software application management. When the initial settings are complete, use Hitachi Command Suite to configure the storage system.

Initial super-user login

This login procedure is for the super-user who logs into Device Manager - Storage Navigator for the first time and sets up the user accounts. The super-user has a built-in ID which includes all permissions, and a default password.

To log in to Device Manager - Storage Navigator as the super-user:

1. Call your local service representative to obtain the super-user ID and default password.
2. In your web browser, specify the URL for your SVP:
   https://IP-address-or-host-name-of-SVP/sanproject/
3. Log in with the superuser ID and password.
4. To prevent unauthorized use of the superuser account, change the password immediately after you log in. Click Settings > User Management > Change Password to change your password.

Normal login

Normal login allows you to perform only the following:

- User management
- License management
- Creating a login message
- Editing system options

When the initial settings are complete, use Hitachi Command Suite to configure the storage system.

To log in to a Device Manager - Storage Navigator:

1. In your web browser, specify the following URL:
2. The following actions might be required to open the login dialog box, depending on your environment:

- If a message indicates that the enhanced security configuration is enabled on the computer, select **In the future, do not show this message** and click **OK**.
- If the SVP is set to support SSL-encrypted communication and security messages appear, make sure the certificate is correct and follow the instructions in the dialog box.
- If a message indicates that certain web sites are blocked, follow instructions in **Adding your SVP to the trusted sites zone - for Windows server on page 5-28**.

3. Type the user ID and password.
4. Click **Login**.
5. If the Security Information dialog box appears, click **Yes**.
6. If a local storage area pop-up dialog box of Adobe Flash Player Setting appears, click **Allow** to open the Device Manager - Storage Navigator main window. The cache function of Flash Player optimizes the process of Device Manager - Storage Navigator. Denial of the request might delay the processing speed of Device Manager - Storage Navigator.

![Figure 5-4 Flash Player local storage area dialog box](image)

**Note:** The roles and resource groups for each user are set up ahead of time and will be available to you when you log in to Device Manager - Storage Navigator. If the roles or resource allocations for your username are changed after you log in, the changes will not be effective until you log out and log back in again.

**Note:** If login fails three times with the same user ID, Device Manager - Storage Navigator stops responding for one minute. This is for security purposes and is not a system failure. Wait, then try again.

### Changing your password

After the administrator gives you a user ID and password, you should change the password.
To change your user account password:

1. Log in to Device Manager - Storage Navigator with the user ID and password given to you by the administrator.
2. Click **Settings > User Management > Change Password** to change your password.

**Related topics**

- [Normal login on page 5-26](#)

**Adding your SVP to the trusted sites zone - for Windows server**

If you are using Device Manager - Storage Navigator on a Windows Server 2003/2008 computer, the following message may appear during login. If it does, you must add the SVP to the trusted sites zone.

![Figure 5-5 Trusted sites message](image)

**Figure 5-5 Trusted sites message**

**To add the SVP to the trusted sites zone:**

1. Click **Add** in the message dialog box. The Trusted Sites dialog box opens.
2. In **Add this web site to the zone**, enter the URL of the SVP that you want to log in to. For example, if the host name is **host01**, the URL is **http://host01**. If the IP address is **127.0.0.1**, the URL is **http://127.0.0.1**.
3. Click **Add** to add the URL of the SVP to the **web sites** list.
4. Click **Close** to close the dialog box.
Setting Device Manager - Storage Navigator environmental parameters

You can set the following Device Manager - Storage Navigator environmental parameters:

- Polling period for monitoring who is changing information while others are viewing
- Time interval for monitoring disk controller and disk array unit status
- Time period that a user is logged out of the SVP because of a network error
- Time period when no changes are made that access the RMI server and the user is released from Modify mode as a result

You can also specify whether to show or hide the Alerts tab.

Prerequisites

You must have the Storage Administrator (Initial Configuration) role to perform this task.

To set time periods:

1. Start a web browser and enter the following URL to open the tool panel.
   http://IP-address-or-host-name-of-SVP/cgi-bin/utility/toolpanel.cgi
2. Click Control Panel to open the Control Panel.
3. Enter the user ID and password and click Login.
4. Click the Set Env. tab to open the Environment Parameter window.
5. Specify the Device Manager - Storage Navigator parameters as required.
6. Click Submit.
7. Click Exit to close the Control Panel.
8. Log out of the Device Manager - Storage Navigator SVP and then log in again to make the new parameters take effect.
9. Back up the Device Manager - Storage Navigator configuration file by
downloading the file from the SVP.

Device Manager - Storage Navigator environment parameters are described
in the following table:

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RMI time-out period</td>
<td>If the user cannot access the SVP for a certain period of time because of a network error, the RMI time-out logs the user out of the SVP.</td>
</tr>
</tbody>
</table>
|                                   | • The value of the RMI time-out period must be greater than the value set for the smallest polling period, either for checking exclusive lock or for checking obstacles (see below for those parameters). For example, specify a value of the RMI time-out period to satisfy the following condition: RMI time-out period > min \([A, B]\)
<p>|                                   | where (A) = Polling period for checking exclusive lock (B) = Polling period for checking obstacles, and min ([A, B]) indicates the minimum value selected from (A) and (B). |
|                                   | • The default is 1 minute. You can specify 1 minute, 5 – 60 minutes in 5-minute increments, 70 to 120 minutes in 10-minute increments, or one day (24 hours). |
|                                   | • This parameter cannot be disabled.                                                                                                          |
| RMI time-out period for Modify    | If a user is in Modify mode but does not make any changes that access the RMI server for a specified period of time, Modify mode is released, and the View mode appears. |
|                                   | • The default time period is 30 minutes. You can specify between 10 and 60 minutes in 10-minute increments, or between 120 and 360 minutes in 60-minute increments. |
|                                   | • Specify NO to disable this parameter.                                                                                                      |
| Polling period for checking       | Using Device Manager - Storage Navigator's secondary window, specify the polling period for monitoring who is changing information while in Modify mode when other users are viewing the storage system information in View mode. The Locked and Unlocked icons are automatically updated either when a user who is in Modify mode either logs out from Device Manager - Storage Navigator or changes to View mode. |
| exclusive lock                    | • The shorter the time period you specify, the more frequently the Lock/Unlock status is updated, but this does increase network traffic. |
|                                   | • The default time period is 35 seconds. You can specify 5 to 60 seconds in 5-second increments, or 70 to 120 in 10-second increments. |
|                                   | • Specify NO to disable this parameter.                                                                                                      |
| Polling period for checking       | Specify a time interval to monitor the Disk Controller and Disk Array Unit status, which is indicated by the Alerts window or the Device Manager - Storage Navigator secondary window. |
| obstacles                         |                                                                                                                                              |</p>
<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
</table>
|      | • The default time period is 110 seconds. You can specify 5 to 60 seconds in 5-second increments, and 70 to 120 seconds in 10-second increments for the parameter.  
|      | • Specify NO to disable this parameter.  
|      | • We recommend that you select NO when Option to hide Alerts window check box is selected. |

### Backing up and restoring HDvM - SN configuration files

You can make backup copies of the various Device Manager - Storage Navigator configuration files by downloading them to a folder that you specify. You can then use the backup copies to restore one or more configuration files if it becomes necessary.

#### Prerequisites

You must have one of the following roles, depending on the configuration you are backing up or restoring.

#### Table 5-5 Roles required to back up and restore configuration files

<table>
<thead>
<tr>
<th>Configuration file</th>
<th>Description</th>
<th>Required role to back up a file</th>
<th>Required role to restore a file</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Account Information</td>
<td>User account information registered to the Device Manager - Storage Navigator.</td>
<td>Security Administrator (View Only)</td>
<td>Security Administrator (View &amp; Modify)</td>
</tr>
<tr>
<td>Environment Parameter List</td>
<td>The parameters settings in the Set Env. window.</td>
<td>Storage Administrator (Initial Configuration)</td>
<td>Storage Administrator (Initial Configuration)</td>
</tr>
<tr>
<td>Log Transfer Information</td>
<td>Settings made in the Edit Audit Log Settings window and the Edit Alert Settings wizard</td>
<td>Audit log Administrator (View Only)</td>
<td>Audit log Administrator (View &amp; Modify)</td>
</tr>
<tr>
<td>SIMSyslog Transfer Information</td>
<td>Settings made in the Edit Alert Settings wizard</td>
<td>Storage Administrator (Initial Configuration)</td>
<td>Storage Administrator (Initial Configuration)</td>
</tr>
<tr>
<td>External Authentication</td>
<td>Connection to the authentication server.</td>
<td>Security Administrator (View &amp; Modify)</td>
<td>Security Administrator (View &amp; Modify)</td>
</tr>
<tr>
<td>Key Management Server</td>
<td>Connection to the Key Management Server(^1)</td>
<td>Security Administrator (View &amp; Modify)</td>
<td>Security Administrator (View &amp; Modify)</td>
</tr>
<tr>
<td>Password Policy</td>
<td>Password policy for backing up encryption keys on the Device Manager - Storage Navigator computer</td>
<td>Security Administrator (View &amp; Modify)</td>
<td>Security Administrator (View &amp; Modify)</td>
</tr>
</tbody>
</table>

---

Note 1. The client certificate in use when the key management (KMIP) server is connected cannot be backed up or restored by Device Manager - Storage Navigator. Consult the administrator of the key management server to determine the best way to use the server to manage and back up the certificate.
To back up configuration files:

1. Start a web browser and enter the following URL to open the tool panel:
   http://IP-address-or-host-name-of-SVP/cgi-bin/utility/toolpanel.cgi

2. Click Control Panel to open the Control Panel.
3. Enter the user ID and password and click Login.
4. Click the Download tab to open the Download file window.
5. Click the files to be downloaded. You can download only the files for which you have permission.
6. Click Submit. The Download File dialog box shows the list of the files to be downloaded.
7. Click Download. The File Download dialog box opens.
8. Click Save. The Save As dialog box opens.
9. Specify the name of a folder to save the compressed file, and then click Save to start downloading.
10. Decompress the downloaded *.tgz file as required. To decompress the *.tgz file, use a tool supporting tar and gzip.

To restore the configuration files:

1. Start a web browser and enter the following URL to open the tool panel:
   http://IP-address-or-host-name-of-SVP/cgi-bin/utility/toolpanel.cgi
2. Click **Control Panel** to open the Control Panel.
3. Enter the user ID and password and click **Login**.
4. Click the **Restore** tab to open the **Restore** file window.
5. Click the files and click **Browse** to specify the directory of the file. You can restore only the files for which you have permission.
6. Click **Next**.
7. Click the configuration files to restore.
8. Click **Submit**.
9. If the **Password check** dialog box opens, enter **User ID**, **Password**, and **Re-enter Password** of the storage administrator on the backup user list, and click **Submit** on the **Password check** dialog box. The **Restore File** dialog box opens.
10. Confirm the restoring process has been completed successfully.
11. Click **Close** to close the dialog box.

**Installing the report configuration tool**

Complete the following instructions to install the report configuration tool.

**Prerequisites**

You need the following items to install the report configuration tool:

  
You can use either an IPv4 address or an IPv6 address to connect the SVP to the windows computer. You can also connect the computer to the SVP over an IPv4 proxy server. When you use the proxy server, specify a name and a port number of the proxy server as the **HTTP_PROXY** environment variable on the Windows computer. For example:

```bash
SET HTTP_PROXY=http://proxy.xx.co.jp:8080
```
• **A user account** for exclusive use of the report configuration tool.

To use the report configuration tool, you must create a user account that is used exclusively for the report configuration tool. Assign the storage administrator role (initial configuration) to this user account.

• **The report configuration tool** installation software

The Report Configuration Tool is located on the CD-ROM Disc 2, which is named *Host PP*. The installation procedure is located in Installation procedure on page 5-34.

### Installation procedure

To install the report configuration tool:

1. Insert the Report Configuration Tool installation CD into the CD-ROM drive.
2. On the CD, navigate to the `/program/Config_Report_CLI/Win32` folder and double-click `setup.exe`. Follow the instructions on the screen.
3. When prompted, enter the name of the directory in which to install the report configuration tool. The installer continues until the tool is installed.

**Note:** The directory where the report configuration tool is installed is not specified as an application path. When necessary, specify the directory as the application path.

### Using the report configuration tool

You can use the report configuration tool to create up to 20 configuration reports and then view or download them.

### Report Configuration Tool command reference (raidinf commands)

This section describes the `raidinf` commands, symbols, and reports used in Device Manager - Storage Navigator.

### raidinf command list and command description

The following lists the `raidinf` commands and symbols.

#### Table 5-6 raidinf command list

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>raidinf add report</td>
<td>Creates a report.</td>
</tr>
<tr>
<td>raidinf delete report</td>
<td>Deletes a report.</td>
</tr>
<tr>
<td>raidinf download report</td>
<td>Downloads a report.</td>
</tr>
<tr>
<td>raidinf get reportinfo</td>
<td>Displays a list of reports.</td>
</tr>
</tbody>
</table>
Table 5-7 Conventions of the command format

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt; &gt;</td>
<td>The item enclosed in this symbol is variable.</td>
</tr>
<tr>
<td></td>
<td>Vertical bar</td>
</tr>
<tr>
<td>]</td>
<td>Symbol is placed between multiple items to indicate &quot;or&quot;. For example: -A</td>
</tr>
<tr>
<td>[ ]</td>
<td>Specifies -A or -B.</td>
</tr>
<tr>
<td>]</td>
<td>Square brackets</td>
</tr>
<tr>
<td>{ }</td>
<td>The enclosed item can be omitted. If some items are delimited by the vertical bar, specify one or omit all items. For example: [ -A ]</td>
</tr>
<tr>
<td>{ }</td>
<td>Specifies nothing or specifies -A.</td>
</tr>
<tr>
<td>{ }</td>
<td>[ -a</td>
</tr>
<tr>
<td>{ }</td>
<td>Specifies nothing or specifies -a or -b.</td>
</tr>
<tr>
<td>{ }</td>
<td>Curly brackets</td>
</tr>
<tr>
<td>{ }</td>
<td>The meaning differs depending on the enclosed item.</td>
</tr>
<tr>
<td>{}</td>
<td>If items in curly brackets are delimited by vertical bars, one of the items must be specified. For example: { -A</td>
</tr>
<tr>
<td>{}</td>
<td>Specifies -A, -B, or -C.</td>
</tr>
<tr>
<td>{}</td>
<td>If curly brackets enclose items enclosed by square brackets, at least one of the items must be specified. For example: { [ -A ] [ -B ] [ -C ] }</td>
</tr>
<tr>
<td>{}</td>
<td>Specifies one or more items from -A, -B, or -C.</td>
</tr>
</tbody>
</table>

raidinf command syntax

The syntax of the raidinf commands and the basic format of the options and parameters are described next.

Syntax


raidinf [-h] -login <user_name> <password> -servername <hostname/ipaddress>

raidinf [-h] -logout -servername <hostname/ipaddress>
Options and parameters

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>[-h]</td>
<td>Displays help for raidinf.</td>
</tr>
<tr>
<td>&lt;action&gt;</td>
<td>Specifies command operation. You can specify the following commands.</td>
</tr>
<tr>
<td></td>
<td>• get: Displays a list of reports.</td>
</tr>
<tr>
<td></td>
<td>• add: Creates a report.</td>
</tr>
<tr>
<td></td>
<td>• delete: Deletes a report.</td>
</tr>
<tr>
<td></td>
<td>• download: Downloads a report.</td>
</tr>
<tr>
<td>&lt;object&gt;</td>
<td>Specifies an operation target object. You can specify the following objects.</td>
</tr>
<tr>
<td></td>
<td>• reportinfo to display a list of reports.</td>
</tr>
<tr>
<td></td>
<td>• report to create, delete, or download a report.</td>
</tr>
<tr>
<td>-servername &lt;hostname/ ipaddress&gt;</td>
<td>Specifies the host name or the IP address of the SVP.</td>
</tr>
<tr>
<td>[-report &lt;report_name&gt;</td>
<td>[-]report_id &lt;report_id&gt;}]</td>
</tr>
<tr>
<td></td>
<td>• -report_id specifies a report ID displayed by the report list. Because a report ID is a unique ID to each of the reports, a specific report can be identified even if reports of the same name exist.</td>
</tr>
<tr>
<td>[-targetfolder &lt;folder&gt;]</td>
<td>Specifies a folder name to which a report is downloaded. The folder whose name you specify must already exist and you must have permissions to the folder.</td>
</tr>
<tr>
<td>[-fill]</td>
<td>Deletes a report only if the number of created reports is 20.</td>
</tr>
<tr>
<td>-login [&lt;user_name&gt; &lt;password&gt;]</td>
<td>Executes a user authentication for Device Manager - Storage Navigator. Specifies a user name and a password. The user is logged out automatically three minutes (180 seconds) after the last command is entered.</td>
</tr>
<tr>
<td>-logout</td>
<td>Logs out of Device Manager - Storage Navigator.</td>
</tr>
</tbody>
</table>

Examples

This example authenticates user01 using the password xxxxxx.
# raidinf -login user01 xxxxxx -servername svp.xxx.co.jp

This example executes a logout.
# raidinf -logout -servername svp.xxx.co.jp

Displays help.
# raidinf -h
Model : RAIDINF/WindowsNT
VerandRev: 01-00-03/00

Usage: raidinf [options]
        raidinf <action> <object> [parameters]
Options:
- \( \text{h} \)                                   Help/Usage
- login \(<\text{user\_name}>\) <password>        Specify LOGIN explicitly
- logout                                      Specify LOGOUT

<User authentification>
<option>       <parameters>
- login         \(<\text{user\_name}>\) <password> -servername <hostname/ipaddress>
- logout        -servername <hostname/ipaddress>

<Report management>
<action> <object>    <parameters>
get    reportinfo -servername <hostname/ipaddress>
add    report     -servername <hostname/ipaddress>    [-report <report\_name>]
download report   -servername <hostname/ipaddress>    [-report <report\_name> | -report_id <report\_id>] -targetfolder <folder>
delete report    -servername <hostname/ipaddress> [-report <report\_name> | -report_id <report_id>] [-fill]

Parameters:
- servername     <hostname/ipaddress>  Specify the SVP hostname or IP address.
- report          <report\_name>        Specify the Report Name.
- report_id       <report\_id>          Specify the ReportID.
- targetfolder    <folder>             Specify the download folder.
- fill            Report is deleted only full of the server reports.

raidinf add report

The raidinf add report command creates a report.

If other users have created 20 reports, the logged in user cannot create a report and will receive an error.

Syntax
raidinf add report -servername <hostname/ipaddress> [-report <report_name>]

Options and parameters

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-servername &lt;hostname/ipaddress&gt;</td>
<td>Specifies the host name or the IP address of the SVP.</td>
</tr>
<tr>
<td>[-report &lt;report_name&gt;]</td>
<td>Specifies a report name, up to 32 characters. If you specify more than 32 characters, the 33rd and subsequent characters are ignored. If the report name is omitted, the default report name YYMMDD-CreateConfigurationReport is specified. The hyphen (-) cannot be specified at the beginning of the report name.</td>
</tr>
</tbody>
</table>

Configuring Device Manager for use with related products
Hitachi Command Suite Administrator Guide
Examples

This example creates a report with the default report name.

```
# raidinf add report -servername 10.213.74.121
ReportName   UserName   CreateTime
101009-CreateConfigurationReport user01  2010/10/09-12:43:10
```

This example specifies the report name 101009-CreateConfigurationReport and creates a report.

```
# raidinf add report -servername 10.213.74.121 -report 101009-
CreateConfigurationReport
ReportName   UserName
CreateTime
101009-CreateConfigurationReport user01  2010/10/09-12:43:10
```

The respective items of the output example are explained next.

- **ReportName**
  - The report name is displayed (up to 32 characters).

- **UserName**
  - The user name is displayed (up to 16 characters). If the user name exceeds 16 characters, an ellipsis (...) is displayed.

- **CreateTime**
  - The time of creating a report is displayed (up to 19 characters).

raidinf delete report

The `raidinf delete report` command deletes a report.

If multiple reports of the same name exist, the command deletes the oldest report. If the specified report does not exist, the command does not do anything and is normally terminated.

Reports created using Device Manager - Storage Navigator can also be deleted.

Syntax

```
raidinf delete report -servername <hostname/ipaddress>
{ -report<report_name> | -report_id <report_id> } [-fill]
```

Options and parameters

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-servername &lt;hostname/ipaddress&gt;</td>
<td>Specifies the host name or the IP address of the SVP.</td>
</tr>
<tr>
<td></td>
<td>• -report specifies a report name (up to 32 characters).</td>
</tr>
<tr>
<td></td>
<td>If you specify more than 32 characters, the 33rd and subsequent characters are ignored.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------</td>
</tr>
<tr>
<td>-servername &lt;hostname/ipaddress&gt;</td>
<td>Specifies the host name or the IP address of the Web server (SVP).</td>
</tr>
<tr>
<td>{ -report &lt;report_name&gt;</td>
<td>Specifies either -report or -report_id.</td>
</tr>
<tr>
<td></td>
<td>If you specify more than 32 characters, the 33rd and subsequent characters are ignored.</td>
</tr>
<tr>
<td></td>
<td>If a special name LatestReport is specified as a report name, the report created on the newest date is downloaded.</td>
</tr>
</tbody>
</table>

### Examples

This example specifies the report name 101009-CreateConfigurationReport and deletes the report.

```bash
# raidinf delete report -servername 10.213.74.121 -report 101009-CreateConfigurationReport
```

101009-CreateConfigurationReport is deleted in the SVP.

### raidinf download report

The `raidinf download report` command downloads a report.

Reports created by Device Manager - Storage Navigator can also be downloaded. The report in process of creation cannot be downloaded.

The name of the downloaded file is `Report_<report name>.tgz`. Note that the files are overwritten if reports of the same name has already existed.

Example: the name of the downloaded file when the report name is 110309-CreateConfigurationReport

`Report_110309-CreateConfigurationReport.tgz`

#### Syntax

```bash
raidinf download report -servername <hostname/ipaddress>  
{ -report <report_name> | -report_id <report_id> }  
-targetfolder <folder>
```

### Options and parameters

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-servername &lt;hostname/ipaddress&gt;</td>
<td>Specifies the host name or the IP address of the Web server (SVP).</td>
</tr>
<tr>
<td>{ -report &lt;report_name&gt;</td>
<td>Specifies either -report or -report_id.</td>
</tr>
<tr>
<td></td>
<td>If you specify more than 32 characters, the 33rd and subsequent characters are ignored.</td>
</tr>
<tr>
<td></td>
<td>If a special name LatestReport is specified as a report name, the report created on the newest date is downloaded.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>-report_id</td>
<td>specifies a report ID displayed by the report list. As a report ID is a unique ID to each of the reports, a specific report can be identified even if reports of the same name exist.</td>
</tr>
<tr>
<td>-targetfolder &lt;folder&gt;</td>
<td>Specifies a folder name to which a report is downloaded. The folder whose name you specify must already exist and you have permissions to the folder.</td>
</tr>
</tbody>
</table>

### Examples

Downloads the most recently created report.

```bash
# raidinf download report -servername 10.213.74.121
-report LatestReport -targetfolder C:\tmp
```

Report_101009-CreateConfigurationReport.tgz is downloaded to C:\tmp.

This example specifies the report name 101009-CreateConfigurationReport and downloads the report.

```bash
# raidinf download report -servername 10.213.74.121
-report 101009-CreateConfigurationReport -targetfolder C:\tmp
```

Report_101009-CreateConfigurationReport.tgz is downloaded to C:\tmp.

**raidinf get reportinfo**

The **raidinf get reportinfo** command displays a list of reports.

Reports created using Device Manager - Storage Navigator are also displayed. A report currently being created cannot be downloaded.

**Syntax**

*raidinf get reportinfo* -servername <hostname/ipaddress>

**Options and parameters**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-servername &lt;hostname/ipaddress&gt;</td>
<td>Specifies the host name or the IP address of the Web server (SVP).</td>
</tr>
</tbody>
</table>

**Examples**

Displays a list of reports.

```bash
# raidinf get reportinfo -servername 10.213.74.121
```

ReportName   UserName   CreateTime   ReportID
---          ---          ---           ---

The respective items of the output example are explained next.

- **ReportName**
  The report name is displayed (up to 32 characters).

- **UserName**
  The user name is displayed (up to 16 characters). If the user name exceeds 16 characters, an ellipsis (...) is displayed.

- **CreateTime**
  The time of creating a report is displayed (up to 19 characters).

- **ReportID**
  The report ID is displayed.

### Creating a configuration report using the Report Configuration Tool

You can create a configuration report by using a command prompt when you use the Report Configuration Tool. By preparing a script file that contains a series of commands and scheduling a task in Windows to execute the script at regular intervals, you can automate the creation and the deletion of the configuration report.

### Preparing a script file

Before creating the configuration report, you will need to write a series of commands in a script file. When you run the Report Configuration Tool, the commands in the script files execute sequentially and then create or delete a configuration report. See Report Configuration Tool command reference (raidinf commands) on page 5-34 for a list of commands.

Two examples of scripts are shown below. Refer to these examples as needed to create a script file that suits your needs.

- [Example script for creating a configuration report on page 5-41](#)
- [Example script for downloading a configuration report on page 5-43](#)

### Example script for creating a configuration report

This script logs the user in, deletes a configuration report, creates a configuration report, and logs the user out, using the Report Configuration Tool.

For each command except the logout command, this example performs three retries at intervals of 2 minutes, assuming that communication errors and other errors can occur. In addition, the delete report command is executed with the -fill option before the add report command, so that the script does not terminate when 20 configuration reports accumulate in the SVP.
REM Create Report Script (CreateReport.bat)
REM
SET USER=<Username for Device Manager - Storage Navigator>
SET PASS=<Password for Device Manager - Storage Navigator>
SET SERVER=<Hostname or IP address of SVP>
SET REPORT_NAME=DailyConfigurationReport
SET LOOP=2
REM LOOP: 0-2 3Times
SET TIMEOUT=121
REM TIMEOUT 2[minutes]=120[s]
SET RAIDINF_PATH="C:\Program Files\raidinf"
SET /a CNT_LOGIN=0

:LOGIN_RETRY
REM ############################# LOGIN %CNT_LOGIN%
SET /a CNTLOGIN=%CNTLOGIN% + 1
%RAIDINF_PATH%\raidinf -login %USER% %PASS% -servername %SERVER%
if ERRORLEVEL 1 (
   if %CNT_LOGIN% GTR %LOOP% GOTO :ABEND
   CALL :SLEEP
   GOTO LOGIN_RETRY
)

SET /a CNT_DEL=0

:DEL_RETRY
REM ############################# DELETE %CNT_DEL%
SET /a CNT_DEL=%CNT_DEL% + 1
%RAIDINF_PATH%\raidinf delete report -servername %SERVER% ^
-report %REPORT_NAME% -fill
if ERRORLEVEL 1 (  
   IF %CNT_DEL% GTR %LOOP% GOTO :ABEND
   CALL :SLEEP
   GOTO :DEL_RETRY
)

SET /a CNT_ADD=0

:ADD_RETRY
REM ############################# ADD %CNT_ADD%
SET /a CNT_ADD=%CNT_ADD% + 1
%RAIDINF_PATH%\raidinf add report -servername %SERVER% -report ^
%REPORT_NAME%
if ERRORLEVEL 1 (  
   IF %CNT_ADD% GTR %LOOP% GOTO :ABEND
   CALL :SLEEP
   GOTO ADD_RETRY
)

GOTO :END
EXIT /B

:SLEEP
REM
REM ############################# SLEEP with %TIMEOUT% sec
REM
ping 127.0.0.1 -n %TIMEOUT% > NUL
EXIT /B

:ABEND
REM ############################# ABEND
ECHO "Create Report Script was ABEND"
Example script for downloading a configuration report

This script logs the user in, downloads a configuration report, and logs the user out, using the Report Configuration Tool.

For each command except the logout command, this example performs 3 retries at intervals of 2 minutes, assuming that communication errors and other errors can occur. The downloaded configuration report is accumulated for 3 generations in the C:\Reports folder by names from Report_DailyConfigurationReport_1.tgz to Report_DailyConfigurationReport_3.tgz. In addition, if the script for creating a configuration report fails, generation copy is terminated so that the past configuration reports may not be overwritten.

REM Download Report Script(DownloadReport.bat)
REM
SET USER=<Username for Device Manager - Storage Navigator>
SET PASS=<Password for Device Manager - Storage Navigator>
SET SERVER=<Hostname or IP Address of SVP>
SET REPORT_NAME=DailyConfigurationReport
SET LOOP=2
REM LOOP:0-2 3Times
SET TIMEOUT=121
REM TIMEOUT 2[minutes]=120[s]
SET TARGETFOLDER=C:\Reports\tmp
SET REPORTFOLDER=C:\Reports
SET RAIDINF_PATH="C:\Program Files\raidinf"
REM
REM Create Report Folder
REM
IF NOT EXIST %REPORTFOLDER% ( 
    MKDIR %REPORTFOLDER%
    IF NOT EXIST %TARGETFOLDER% ( 
        MKDIR %TARGETFOLDER%
    )
)

SET /a CNT_LOGIN=0
:LOGIN_RETRY
REM ####### Login %CNT_LOGIN%
SET /a CNT_LOGIN=%CNT_LOGIN% + 1
%RAIDINF_PATH%\raidinf -login %USER% %PASS% -servername %SERVER%
if ERRORLEVEL 1 ( 
    IF %CNT_LOGIN% GTR %LOOP% GOTO :ABEND
    CALL :SLEEP
    GOTO LOGIN_RETRY
)

SET /a CNT_DL=0
:DL_RETRY
REM ####### Download %CNT_DL%
SET /a CNT_DL=%CNT_DL% + 1
%RAIDINF_PATH%\raidinf download report -servername %SERVER% ^
-report %REPORT_NAME% -targetfolder %TARGETFOLDER%
if ERRORLEVEL 1 (
    IF %CNT_DL% GTR %LOOP% GOTO :ABEND
    CALL :SLEEP
    GOTO :DL_RETRY
)
REM ####################################### Create Error Check
IF EXIST %REPORTFOLDER%\Report_%REPORT_NAME%_1.tgz (
    IF EXIST %TARGETFOLDER%\Report_%REPORT_NAME%.tgz ( 
      GOTO :FC_CHECK
    ) else ( 
      GOTO :CHECK_END
    )
) else ( 
    GOTO :CHECK_END
)
:FC_CHECK
FC /B %REPORTFOLDER%\Report_%REPORT_NAME%_1.tgz ^
%TARGETFOLDER%\Report_%REPORT_NAME%.tgz > NUL
if ERRORLEVEL 1 ( 
    REM
) else ( 
    DEL %TARGETFOLDER%\Report_%REPORT_NAME%.tgz
    GOTO :END
)
:CHECK_END
REM ####################################### Migrate Reports
IF EXIST %TARGETFOLDER%\Report_%REPORT_NAME%.tgz ( 
    IF EXIST %REPORTFOLDER%\Report_%REPORT_NAME%_2.tgz ( 
        COPY %REPORTFOLDER%\Report_%REPORT_NAME%_2.tgz ^
        %REPORTFOLDER%\Report_%REPORT_NAME%_3.tgz
    ) 
    IF EXIST %REPORTFOLDER%\Report_%REPORT_NAME%_1.tgz ( 
        COPY %REPORTFOLDER%\Report_%REPORT_NAME%_1.tgz ^
        %REPORTFOLDER%\Report_%REPORT_NAME%_2.tgz
    )
    IF EXIST %TARGETFOLDER%\Report_%REPORT_NAME%.tgz ( 
        COPY %TARGETFOLDER%\Report_%REPORT_NAME%.tgz ^
        %REPORTFOLDER%\Report_%REPORT_NAME%_1.tgz
        DEL %TARGETFOLDER%\Report_%REPORT_NAME%.tgz
    )
) 
GOTO :END
EXIT /B
:SLEEP
REM ####################################### SLEEP with %TIMEOUT%
ping 127.0.0.1 -n %TIMEOUT% > NUL
EXIT /B
:ABEND
REM ####################################### ABEND
ECHO "Download Report Script was ABEND"
:END
REM ####################################### Logout
%RAIDINF_PATH%\raidinf -logout -servername %SERVER%

5-44
Configuring Device Manager for use with related products
Hitachi Command Suite Administrator Guide
Example execution and explanation of script files

- The first time you execute the script files to create a configuration report and download a configuration file, the `Report_DailyConfigurationReport_1.tgz` file is created in the `C:\Reports` folder.

- On the second day:
  `Report_DailyConfigurationReport_1.tgz` is renamed
  `Report_DailyConfigurationReport_2.tgz`, and
  `Report_DailyConfigurationReport_1.tgz` is newly created.

- From the third day on:
  `Report_DailyConfigurationReport_1.tgz` and
  `Report_DailyConfigurationReport_2.tgz` are renamed
  `Report_DailyConfigurationReport_2.tgz`, and
  `Report_DailyConfigurationReport_1.tgz` are newly created. Because
  `Report_DailyConfigurationReport_3.tgz` is overwritten, the reports for
  three days are always accumulated in the `C:\Reports` folder.

C:\Reports
  CreateReport.bat
  DownloadReport.bat
  Report_DailyConfigurationReport_1.tgz <-Generated today
  Report_DailyConfigurationReport_2.tgz <-Generated yesterday
  Report_DailyConfigurationReport_3.tgz <-Generated two days ago

Error in executing Report Configuration Tool

When using the Report Configuration Tool, you may see Device Manager - Storage Navigator error codes and other error codes that are unique to the Report Configuration Tool. For Device Manager - Storage Navigator error codes, see Hitachi Command Suite Messages. The error codes unique to the Report Configuration Tool and the corresponding actions are as follows.

<table>
<thead>
<tr>
<th>Error code</th>
<th>Error message</th>
<th>Cause of error and action</th>
<th>Return value</th>
</tr>
</thead>
<tbody>
<tr>
<td>EW_COMERR</td>
<td>A certificate does not become effective. Please login again.</td>
<td>A certain period of time elapsed after a login. Log in again.</td>
<td>131</td>
</tr>
<tr>
<td>EW_COMERR</td>
<td>Login is necessary. Please login again.</td>
<td>A command was entered before logging in. Log in and then enter the command.</td>
<td>131</td>
</tr>
<tr>
<td>EW_ENFILE</td>
<td>No such folder. Please refer to the help.</td>
<td>The specified folder to download to is not found. See Report Configuration Tool command reference (raidinf commands) on page 5-34 and specify the parameter again.</td>
<td>131</td>
</tr>
<tr>
<td>EW_ENOMEM</td>
<td>Memory allocate error. Please other program terminate.</td>
<td>Allocation of internal memory fails. Close unnecessary programs or reboot the server.</td>
<td>245</td>
</tr>
<tr>
<td>Error code</td>
<td>Error message</td>
<td>Cause of error and action</td>
<td>Return value</td>
</tr>
<tr>
<td>--------------</td>
<td>---------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------</td>
<td>--------------</td>
</tr>
<tr>
<td>EW_INVOPA</td>
<td>Report name reserved. Please check input '-report' parameter.</td>
<td>You cannot use the report name specified by the <code>-report</code> option. Check the report name and specify a new one.</td>
<td>131</td>
</tr>
<tr>
<td>EW_INVOPT</td>
<td>Invalid option. Please refer to the help.</td>
<td>The hyphen (-) is not added to the option parameter. See Report Configuration Tool command reference (raidinf commands) on page 5-34 and revise the parameters.</td>
<td>131</td>
</tr>
<tr>
<td>EW_LNGARG</td>
<td>Argument too long. Please refer to the help.</td>
<td>Either of the following causes is possible.</td>
<td>131</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The length of a parameter of the command exceeds 256 bytes.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The length of all the parameters of the command exceeds 1,021 bytes.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>See Report Configuration Tool command reference (raidinf commands) on page 5-34 and revise the parameters.</td>
<td></td>
</tr>
<tr>
<td>EW_MAXAPP</td>
<td>Maximum application start. Please check starting application.</td>
<td>The maximum number of SVPs that you can connect simultaneously is exceeded. Log out of unnecessary SVPs and reconnect.</td>
<td>131</td>
</tr>
<tr>
<td>EW_MAXARG</td>
<td>Maximum argument. Please refer to the help.</td>
<td>The number of parameters of the command exceeds 10. See Report Configuration Tool command reference (raidinf commands) on page 5-34 and revise the parameters.</td>
<td>131</td>
</tr>
<tr>
<td>EW_REQOPT</td>
<td>Required option list. Please refer to the help.</td>
<td>The required option and parameters were not entered. See Report Configuration Tool command reference (raidinf commands) on page 5-34 and specify a valid option and parameters.</td>
<td>131</td>
</tr>
<tr>
<td>EW_SYSERR</td>
<td>System error. Please call to service center.</td>
<td>An internal error occurred. Contact Hitachi Data Systems Support Center.</td>
<td>131</td>
</tr>
<tr>
<td>EW_SYSERR</td>
<td>Install path is too long. Specify the install path with up to 240 bytes.</td>
<td>The installation path exceeds 240 bytes. Specify no more than 240 bytes.</td>
<td>131</td>
</tr>
<tr>
<td>EW_SYSERR</td>
<td>Certificate file invalid.</td>
<td>Updating certificate file fails. Contact Hitachi Data Systems Support Center.</td>
<td>131</td>
</tr>
<tr>
<td>Error code</td>
<td>Error message</td>
<td>Cause of error and action</td>
<td>Return value</td>
</tr>
<tr>
<td>------------</td>
<td>-------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------</td>
<td>--------------</td>
</tr>
<tr>
<td>EW_SYSERR</td>
<td>The file is illegal. Please move 'raidinfcer' file from the installation directory.</td>
<td>The installation directory includes a file that will overlap with another file to be created by the Report Configuration Tool and the Report Configuration Tool cannot start. Remove the overlapping file from the installation directory.</td>
<td>131</td>
</tr>
<tr>
<td>EW_SYSERR</td>
<td>Log file invalid. Please call to service center.</td>
<td>The log file cannot be accessed. Contact Hitachi Data Systems Support Center.</td>
<td>131</td>
</tr>
<tr>
<td>EW_UNWCMD</td>
<td>Unknown command. Please refer to the help.</td>
<td>The syntax of the command is not valid. See Report Configuration Tool command reference (raidinf commands) on page 5-34 and input a valid parameter.</td>
<td>230</td>
</tr>
<tr>
<td>EW_UNWOPT</td>
<td>Unknown option. Please refer to the help.</td>
<td>The option and parameter are not valid. See Report Configuration Tool command reference (raidinf commands) on page 5-34 and input a new option and parameter.</td>
<td>252</td>
</tr>
<tr>
<td>EW_UNWOPT</td>
<td>Invalid environment value. Please confirm the setting of HTTP_PROXY.</td>
<td>Unable to connect to the proxy server specified by the environment variable. Check the proxy server name.</td>
<td>252</td>
</tr>
<tr>
<td>EW_WEBERR</td>
<td>Web access error. Please confirm the setting of server.</td>
<td>An internal error occurred while connecting to the server. Check the setting of the server.</td>
<td>131</td>
</tr>
<tr>
<td>EW_WEBERR</td>
<td>Server name can not be resolved. Please check the setting of server name.</td>
<td>The server specified by the -servername option does not exist. Check the server name and specify a new server.</td>
<td>131</td>
</tr>
</tbody>
</table>
| EW_WEBERR  | Server is no response. Input argument server is incorrect or server is not ready. | No response from the server specified by the -servername option. Make sure that:  
  • The correct server name is specified.  
  • The settings of the server are correct. | 131          |
| EW_WEBERR  | Web access error. Please check your network equipment and cables.            | An internal error occurred while connecting to the server. Check the network devices and cables. | 131          |
### Executing a regularly scheduled script file

To execute the created script file on a regular basis, register it as a scheduled task in Windows.

The following procedure uses the Windows `schtasks` command to register the script files created in the example shown in [Preparing a script file on page 5-41](#) as tasks of Windows.

#### Registration example

- Create a configuration report at 21:00 every day (`CreateReport.bat`).
- Download a configuration report at 22:00 every day (`DownloadReport.bat`).

#### Procedure

1. Store the two script files in the `C:\Reports` folder.

   ```
   C:\Reports
   CreateReport.bat
   DownloadReport.bat
   ```

2. Run the Windows `schtasks` command to register the two script files as a task of Windows.

   Make sure that the `<Username for Windows>` parameter of this command is a user who has write permissions to the following two folders.

   - `C:\Reports` folder
   - The log folder in the installation folder of the Report Configuration Tool.

   ```
schtasks /create /tn CreateReport /tr "C:\Reports \CreateReport.bat" /sc DAILY /st. 21:00:00 /ru <Username for Windows> /rp <Password for Windows> schtasks /
   ```
create /tn DownloadReport /tr "C:\Reports\DownloadReport.bat" /sc DAILY /st 22:00:00 /ru <Username for Windows> /rp <Password for Windows>

3. Run the `schtasks /Query` command to confirm that the Windows task is registered.

C:\>schtasks /Query
Task name       Time of next execution       Status
============= =========== ===============
CreateReport    21:00:00, 2011/05/17          **********
DownloadReport  22:00:00, 2011/05/17          **********

**Downloading dump files using the Dump tool**

Use the Dump tool to download dump files onto a web client. The downloaded dump files can be used to:

- troubleshoot the system. Use the Dump tool to download dump files from the SVP and give it to the HDS support personnel.

- check system configuration. First click **File > Refresh All** to refresh the configuration information, and then use the Dump tool to download dump files.

**Prerequisites**

- All other users (including the SVP user) must stop using the Dump tool.

- Stop all maintenance operations.

- You must have Support Personnel role to log in.

**To download dump files from the SVP:**

1. Start a web browser and specify the following URL to open the Tool Panel:
   
   https://IP-address-or-host-name-of-SVP/cgi-bin/utility/toolpanel.cgi

   ![](Tool_Panel.png)

   2. Click **Download Dump Files**. The Login dialog box opens.
3. Enter the user ID and password and click **Login**. The Download Dump Files dialog box opens.

4. Select a file that you want to download.
   - **Existing Dump Files** indicates the last dump file that you downloaded. Select this when you want to re-download a previously downloaded dump file. If you have not downloaded any dump files from the Tool Panel, this item does not display even if you have acquired a dump file via SVP.
   - **Normal Dump** includes all information about the SVP and the minimum information about the storage system. Select this when you have a less serious problem such as incorrect display.
   - **Detail Dump** includes all information about the SVP and the storage system. Select this when Device Manager - Storage Navigator has a serious problem (for example, Device Manager - Storage Navigator does not start) or when you need to determine if the storage system has a problem.
   - **Detail Dump (for DKC Performance)** contains the I/O-performance-related information. This includes performance monitor collection information, in addition to information applicable to Detail Dump. Choose **Detail Dump (for DKC Performance)** to check for I/O performance problems.
     Note that while processing takes place, DKC I/O performance may be affected. During processing, you cannot use Device Manager - Storage Navigator to change the system configuration or perform SVP maintenance operations.

5. Click **Next**. A message appears confirming the execution of compression of the dump files.

6. Click **OK**. File compression processing starts. When the file is compressed, the Download Dump Files dialog box opens for the download.

7. Click **Download**. The File Download dialog box opens.

8. On the File Download dialog box, click **Save this file to disk**, and then click **OK**. The Save As dialog box opens.

9. Specify the download destination, and then click **Save**. When the file is downloaded successfully, the Download complete dialog box opens.
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
- Using event notification
- Reporting failure information about storage systems (for VSP G1000 only)
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.

**Operations to complete in advance**

Log in to the system as a member of the Administrators group.

**To set up trace log files:**

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.

**Operations to complete in advance**

Log in to the system as a root user.

**To set up trace log files:**

1. Execute the utility program stored in the following location:
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 6-1 Alerts that can be displayed by Device Manager

<table>
<thead>
<tr>
<th>Management target</th>
<th>Polling</th>
<th>SNMP traps</th>
<th>Email notification of alerts</th>
</tr>
</thead>
<tbody>
<tr>
<td>Storage system</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VSP G1000</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Virtual Storage Platform</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Universal Storage Platform V/VM</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Hitachi USP</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>HUS VM</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>HUS100</td>
<td>Y</td>
<td>--</td>
<td>Y</td>
</tr>
<tr>
<td>Hitachi AMS2000</td>
<td>Y</td>
<td>--</td>
<td>Y</td>
</tr>
<tr>
<td>Hitachi SMS</td>
<td>Y</td>
<td>--</td>
<td>Y</td>
</tr>
<tr>
<td>Hitachi AMS/WMS</td>
<td>Y</td>
<td>--</td>
<td>Y</td>
</tr>
<tr>
<td>SMI-S enabled storage systems</td>
<td>--</td>
<td>--</td>
<td>--</td>
</tr>
<tr>
<td>File server</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hitachi Data Ingestor</td>
<td>--</td>
<td>Y</td>
<td>--</td>
</tr>
<tr>
<td>Hitachi NAS Platform</td>
<td>Y#</td>
<td>Y#</td>
<td>Y#</td>
</tr>
<tr>
<td>Hitachi NAS Platform F</td>
<td>--</td>
<td>Y</td>
<td>--</td>
</tr>
</tbody>
</table>

**Legend**

- **Y:** Supported
- **--:** Not supported

- **#:** For Hitachi NAS Platform, both of the following conditions must be satisfied to detect error information:
  - The version of Hitachi NAS Platform is 12.0 or later.
  - Admin services EVS is set.

**Note:** For Hitachi NAS Platform, 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 topics**

- Settings for displaying SNMP traps as alerts on page 6-5
- Changing Device Manager server properties on page A-4
- server.dispatcher.daemon.pollingPeriod on page A-21
Settings for displaying SNMP traps as alerts

To display SNMP traps as alerts, the following settings are required:

- **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.

- **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.
  - For Hitachi NAS Platform, the host name or IP address of the management server and a port number (162/udp) must be set from SMU or the Hitachi 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 6-2 IP address format for the management server to be set (setting SNMP traps for Hitachi NAS Platform)**

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

- 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.

After the above settings finish, the Device Manager server receives SNMP traps from all communities and displays them as alerts.

**Related topics**

- [Changing Device Manager server properties on page A-4](#)
- [server.dispatcher.daemon.receiveTrap on page A-21](#)
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.

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. Registering recipients of email alerts
   In the Device Manager GUI, register the users who will receive emails.

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.filesystem` property of the Device Manager server.
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.

Registering recipients of email alerts

Use the Device Manager GUI to set an email destination user.

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.

**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).

Related topics

- How to register users in the Device Manager GUI: *Hitachi Command Suite User Guide*
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 topics

- Changing Device Manager server properties on page A-4
- `server.mail.enabled.storagesystem` on page A-12
- `server.mail.enabled.fileserver` on page A-12
- `server.mail.from` on page A-13
- `server.mail.smtp.host` on page A-13
- `server.mail.smtp.port` on page A-13
- `server.mail.smtp.auth` on page A-13
- `server.mail.errorsTo` on page A-14
- `server.eventNotification.mail.to` on page A-14
- `server.mail.alert.type.storagesystem` on page A-14
- `server.mail.alert.status` on page A-14

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.

Operations to complete in advance

- 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`. 
Information to collect in advance

- 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.

To register an SMTP authentication user account in Device Manager:

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:
   

2. Restart the Hitachi Command Suite product services.

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.

Related topics

- Starting the Hitachi Command Suite services on page 8-4
- Stopping the Hitachi Command Suite services on page 8-5
- Changing Device Manager server properties on page A-4
- server.mail.smtp.auth on page A-13

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:

```
Subject:[DVM] Alert Notification
The following alert occurred.
MessageID: ${messageID}
Alert Type: ${alertType}
Source: ${source}
Status: ${status}
Component: ${component}
Description: ${description}
Recommended Action: ${recommendedAction}
Additional Info: ${additionalInfo}
Occurrence Time: ${occurrenceTime}
```

This message was sent automatically by the Device Manager server.

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.

The following table shows the specifiable parameters:

<table>
<thead>
<tr>
<th>Parameter name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>messageID</code></td>
<td>Alert ID</td>
</tr>
<tr>
<td><code>alertType</code></td>
<td>Alert type</td>
</tr>
<tr>
<td><code>source</code></td>
<td>Alert source</td>
</tr>
<tr>
<td>Parameter name</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>status</td>
<td>Alert severity</td>
</tr>
<tr>
<td>component</td>
<td>Component on which the problem occurred</td>
</tr>
<tr>
<td>description</td>
<td>Alert description</td>
</tr>
<tr>
<td>recommendedAction</td>
<td>Action to be taken for the alert</td>
</tr>
<tr>
<td>additionalInfo</td>
<td>Supplementary information</td>
</tr>
<tr>
<td>occurrenceTime</td>
<td>For storage systems, the time at which the Device Manager server acquired alert information. For Hitachi NAS Platform, the time at which an error occurred in Hitachi NAS Platform. Display format: yyyy/mm/dd hh:mm:ss hh is displayed by using 24-hour display.</td>
</tr>
</tbody>
</table>

**Related topics**

- [Starting the Hitachi Command Suite services on page 8-4](#)
- [Stopping the Hitachi Command Suite services on page 8-5](#)

**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 version1 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 topics**

- Setting up Device Manager to output SNMP traps on page 6-12
- Changing Device Manager server properties on page A-4
- customizedsnmptrap.customizelist on page A-34

### 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.

- **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.

- **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.

After the above settings finish, the Device Manager server receives SNMP traps from all communities and outputs them to log files.

**Related topics**

- Changing Device Manager server properties on page A-4
Using 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 6-4 Tiered Storage Manager events that can be reported via email**

<table>
<thead>
<tr>
<th>Event</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Migration task ended</td>
<td>This event occurs when a migration task ends successfully, ends due to a failure, or is canceled.</td>
</tr>
<tr>
<td>Shredding task ended</td>
<td>This event occurs when a shredding task created via the Tiered Storage Manager CLI ends successfully, ends due to a failure, or is canceled.</td>
</tr>
<tr>
<td>Locking task ended</td>
<td>This event occurs when a locking task created via the Tiered Storage Manager CLI ends successfully, ends due to a failure, or is canceled.</td>
</tr>
<tr>
<td>Unlocking task ended</td>
<td>This event occurs when an unlocking task created via the Tiered Storage Manager CLI ends successfully, ends due to a failure, or is canceled.</td>
</tr>
<tr>
<td>Volume lock period expired</td>
<td>This event occurs when the volume lock period has expired for a volume in a migration group created via the Tiered Storage Manager CLI.</td>
</tr>
<tr>
<td>Specified time elapsed</td>
<td>This event occurs when a period specified by a user for a migration group created via the Tiered Storage Manager CLI has elapsed (the period is a specified number of days).</td>
</tr>
</tbody>
</table>

The range of events to be reported varies depending on the settings for the notification-destination email addresses, as follows:

- **Setting when creating tasks**  
  If an email address is set when creating tasks such as migration and shredding, the results of the tasks are reported to the user.

- **Setting in the server.properties file**  
  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.

### Setting properties for 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`

### Customizing event notification templates

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>
<thead>
<tr>
<th>Type</th>
<th>Event</th>
<th>Template file</th>
</tr>
</thead>
<tbody>
<tr>
<td>Task ended</td>
<td>Migration task ended</td>
<td>• For migration tasks created by using the <strong>Migrate data</strong> wizard(^1)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>In Windows:</td>
</tr>
</tbody>
</table>
### Type

<table>
<thead>
<tr>
<th>Event</th>
<th>Template file</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><code>installation-folder-for-Hitachi-Command-Suite\DeviceManager\HiCommandServer\config\mail-migrationtask-end.txt</code></td>
</tr>
<tr>
<td></td>
<td><strong>In Linux:</strong> <code>installation-directory-for-Hitachi-Command-Suite/HiCommandServer/config/mail-migrationtask-end.txt</code></td>
</tr>
<tr>
<td></td>
<td>• For migration tasks created by using the Tiered Storage Manager CLI**#2**</td>
</tr>
<tr>
<td></td>
<td><strong>In Windows:</strong> <code>installation-folder-for-Hitachi-Command-Suite\TieredStorageManager\conf\mail-migrationtask-end.txt</code></td>
</tr>
<tr>
<td></td>
<td><strong>In Linux:</strong> <code>installation-directory-for-Hitachi-Command-Suite/TieredStorageManager/conf/mail-migrationtask-end.txt</code></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Event</th>
<th>Template file</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Shredding task ended</strong></td>
<td><strong>#2</strong></td>
</tr>
<tr>
<td></td>
<td><strong>In Windows:</strong> <code>installation-folder-for-Hitachi-Command-Suite\TieredStorageManager\conf\mail-shreddingtask-end.txt</code></td>
</tr>
<tr>
<td></td>
<td><strong>In Linux:</strong> <code>installation-directory-for-Hitachi-Command-Suite/TieredStorageManager/conf/mail-shreddingtask-end.txt</code></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Event</th>
<th>Template file</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Locking task ended</strong></td>
<td><strong>#2</strong></td>
</tr>
<tr>
<td></td>
<td><strong>In Windows:</strong> <code>installation-folder-for-Hitachi-Command-Suite\TieredStorageManager\conf\mail-lockingtask-end.txt</code></td>
</tr>
<tr>
<td></td>
<td><strong>In Linux:</strong> <code>installation-directory-for-Hitachi-Command-Suite/TieredStorageManager/conf/mail-lockingtask-end.txt</code></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Event</th>
<th>Template file</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Unlocking task ended</strong></td>
<td><strong>#2</strong></td>
</tr>
<tr>
<td></td>
<td><strong>In Windows:</strong> <code>installation-folder-for-Hitachi-Command-Suite\TieredStorageManager\conf\mail-unlockingtask-end.txt</code></td>
</tr>
<tr>
<td></td>
<td><strong>In Linux:</strong> <code>installation-directory-for-Hitachi-Command-Suite/TieredStorageManager/conf/mail-unlockingtask-end.txt</code></td>
</tr>
<tr>
<td>Type</td>
<td>Event</td>
</tr>
<tr>
<td>----------------------</td>
<td>------------------------------------------------</td>
</tr>
<tr>
<td>Time lapse</td>
<td>Volume lock period expired^2</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Specified time elapsed^2</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

\^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.

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

![Template example](image)

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:** 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 [Table 6-6 Parameters for events that occur when tasks end (migration tasks created via the Migrate data wizard)] on page 6-17 to [Table 6-8 Parameters for time-lapse events] on page 6-19.

### Table 6-6 Parameters for events that occur when tasks end (migration tasks created via the Migrate data wizard)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>task</td>
<td>Task name</td>
</tr>
<tr>
<td>taskType</td>
<td>Task type</td>
</tr>
</tbody>
</table>

---

Setting up logs and alerts 6-17

Hitachi Command Suite Administrator Guide
### Table 6-7 Parameters for events that occur when tasks end (tasks created via the Tiered Storage Manager CLI)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>taskId</td>
<td>Task ID</td>
</tr>
<tr>
<td>taskType</td>
<td>Task type</td>
</tr>
<tr>
<td>taskStatus</td>
<td>Task status</td>
</tr>
<tr>
<td>taskOwner</td>
<td>The user ID of the user who created the task.</td>
</tr>
<tr>
<td>executionRequestTime</td>
<td>Time that task execution was requested</td>
</tr>
<tr>
<td>endTime</td>
<td>Time that task execution ended</td>
</tr>
<tr>
<td>storageDomainName</td>
<td>Storage domain name</td>
</tr>
<tr>
<td>migrationGroupName</td>
<td>Migration group name</td>
</tr>
<tr>
<td>previousTargetStorageTierName</td>
<td>Name of the target storage tier in the previous migration</td>
</tr>
<tr>
<td>targetStorageTierName</td>
<td>Name of the target storage tier</td>
</tr>
<tr>
<td>eraseData</td>
<td>Whether data after migration is to be deleted</td>
</tr>
<tr>
<td>migratedVolumes</td>
<td>Device numbers of both migrated volumes and volumes whose data has been erased</td>
</tr>
<tr>
<td>shreddingMethod</td>
<td>Shredding method</td>
</tr>
<tr>
<td>shreddedVolumes</td>
<td>Device numbers of shredded volumes</td>
</tr>
<tr>
<td>guardMode</td>
<td>Lock mode</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>retentionDays</td>
<td>Retention period (days)</td>
</tr>
<tr>
<td>lockedVolumes</td>
<td>Device numbers of locked volumes</td>
</tr>
<tr>
<td>unlockedVolumes</td>
<td>Device numbers of unlocked volumes</td>
</tr>
<tr>
<td>moveToMigrationGroupName</td>
<td>Name of the target migration group after task completion</td>
</tr>
</tbody>
</table>

### Table 6-8 Parameters for time-lapse events

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>storageDomainName</td>
<td>Storage domain name</td>
</tr>
<tr>
<td>migrationGroupName</td>
<td>Migration group name</td>
</tr>
<tr>
<td>expiredVolumes</td>
<td>Device numbers of expired volumes</td>
</tr>
<tr>
<td>remindAt</td>
<td>Scheduled time when an &quot;elapsed time&quot; event will occur</td>
</tr>
<tr>
<td>reminderDescription</td>
<td>Message that appears when an &quot;elapsed time&quot; event occurs</td>
</tr>
</tbody>
</table>

### Related topics
- [Starting the Hitachi Command Suite services on page 8-4](#)
- [Stopping the Hitachi Command Suite services on page 8-5](#)
- For details about the parameters of each event: [Tiered Storage Manager CLI Reference Guide](#)

### Specifying SMTP user authentication information for event notification

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.

**Tip:** To send notifications about 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.

### Format of 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/
```

**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 topics**

- [Starting the Hitachi Command Suite services on page 8-4](#)
- [Stopping the Hitachi Command Suite services on page 8-5](#)
Format of 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 topics**

- [Starting the Hitachi Command Suite services on page 8-4](#)
- [Stopping the Hitachi Command Suite services on page 8-5](#)
Reporting failure information about storage systems (for VSP G1000 only)

This topic explains how to report storage system failure though Syslog or email.

You can report failure information (SIM) about storage systems through Syslog, SNMP trap, and email. Failure information reported through email is the same as SIM displayed on the Alert window or reported through SNMP trap. For SNMP trap, the user needs to access the SNMP Manager to check for failure. However, for report through Syslog or email, the user has only to check Syslog or email to know about the occurrence of failure. See the Hitachi SNMP Agent User Guide for methods of notification with SNMP traps.

Requirements of the new Syslog protocol (TLS1.2/RFC5424)

The new Syslog protocol (TLS1.2/RFC5424) requires the following:

- Operation confirmed Syslog server (rsyslog version 4.6.2)
- Syslog server certificate. The IP address of the Syslog server in "Subject Alternative Name: IP Address" of the Syslog server certificate.
- Client certificate. Upload the following:

<table>
<thead>
<tr>
<th>Certificate type</th>
<th>Format</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syslog server root certificate</td>
<td>X.509</td>
<td>Obtain the Syslog server root certificate from the server administrator.</td>
</tr>
<tr>
<td>Client certificate</td>
<td>PKCS#12</td>
<td>Convert the Syslog server client certificate that is signed by a Certificate Authority (CA) to PKCS#12 format. (See Obtaining a client certificate for the new Syslog protocol on page 6-22.)</td>
</tr>
</tbody>
</table>

Each certificate has an expiry date, after which you are prevented from connecting to the Syslog server. Note the expiration dates when preparing certificates.

Contact the Syslog server administrator for the following:

- Password set up in the PKCS#12-format client certificate
- More information about the certificates

 Obtaining a client certificate for the new Syslog protocol

 To obtain a client certificate:

1. Download the program to create the certificate from the following website: OpenSSL website, http://www.openssl.org/.
2. Install the OpenSSL program in the C:\openssl folder.
3. Convert the client certificate to the PKCS#12 format.
Example

The following example to obtain a client certificate, Windows Vista is the operating system. Both a private key and a public key are created. The client.p12 file is the client certificate in PKCS#12 format. This file is created in the c:\key folder.

1. Create a private key (.key file). See Creating a private key (.key file) on page 4-85.
2. Create a public key (.csr file). See Creating a public key (.csr file) on page 4-85.
3. Send the new key to the Syslog server Certificate Authority for signature to obtain a certificate. The certificate is used as the client certificate.

When preparing a certificate, note its expiration date. If the expiration date passes, you will not be able to connect to the Syslog server.

Setting and configuring syslog notification for SIMs

You can be notified in syslog format when storage system failures occur.

Prerequisites

- You must have the Storage Administrator (Initial Configuration) role to perform this task.
- You must have a server that supports syslogs.
- If a firewall is used, a port must be opened to transfer syslogs.

To configure settings for syslog notification:

1. Click Settings > Environmental Settings > Edit Alert Settings.
2. In Notification Alert, select the destination of the alert notification.
   - Host Report: Reports alerts only to the host(s) for which SIM report setting is made.
   - All: Reports alerts to all hosts.
3. In Transfer Protocol, select the protocol for Syslog transfer.
4. To transfer Syslog to the primary server, select Enable and set the following items:
   - IP Address
   - Port Number
   - Client Certificate File Name, Password, and Root Certificate File Name
   Use this field only when you select New Syslog Protocol (TLS1.2/RFC5424) in Transfer Protocol.
5. To transfer Syslog to the alternate server (secondary server), select Enable and set the following items:
   - IP Address
   - Port Number
   - Client Certificate File Name, Password, and Root Certificate File Name
Use this field only when you select New Syslog Protocol (TLS1.2/RFC5424) in Transfer Protocol.

6. Enter a name in Location Identification Name for identification for the storage system.

7. If you select New Syslog Protocol (TLS1.2/RFC5424) in Transfer Protocol, also specify timeout, retry interval, and number of retries.

8. As necessary, click Test Send to Syslog Server to test the settings.

9. Check that the Syslog server has received log (Detailed data: "RefCode: 7FFFFFF, This is Test Report.").


11. In the Confirm window, check the settings and enter a task name in Task Name.

12. Click Apply. The task is registered. If the Go to tasks window for status check box is checked, the Task window opens.

Related topics
- Normal login on page 5-26

Configuring email notification

Prerequisites
- You must have a Security Administrator account with an Initial Configuration role to perform this task.
- You must have a mail server that supports the Simple Mail Transfer Protocol (SMTP).
- If a firewall is used, port 25 must be used.

To configure settings for email notices:

1. Click Settings > Environmental Settings > Edit Alert Settings. The E-mail Information window opens.

2. In Notification Alert, select the destination of the alert notification.
   - Host Report: Reports alerts only to the host(s) for which SIM report setting is made.
   - All: Reports alerts to all hosts.
   Alert notification destination is common to Syslog, SNMP, and Email.

3. Select Enable in Mail Notice on the Email tab.

4. In the Email Settings table, set the email destination address and attributes (To, Cc, Bcc).
   - To add an email address, click Add. On the Add Address window, set the email address and attributes.
   - To change an email address and attributes, select the line for the email address to be changed, and click Change. In the Change Settings window, change the email address and attributes.
You can select more than one email address. When you selected more than one email address, you can change only attributes.

- To delete an email address, select the line for the email address to be deleted and click **Delete**. You can select more than one email address.

This field is mandatory when you select Enable in Mail Notice.

5. Enter the email source address (mandatory) and return address (optional).
   You can use up to 255 alphanumeric characters (ASCII codes) and symbols (! # $ % & ` + - * / ^ { } _ .)

6. Enter the following email server information:
   - **Identifier**. To specify a host name, select Identifier. You can use up to 63 alphanumeric characters (ASCII codes) and symbols ('! # $ % & ` + - * / ^ { } _ .).
   - **IPv4**. To set an IPv4 address, select IPv4, and enter four numbers within the range of 0 to 255.
     Example: XXX.XXX.XXX.XXX (X indicates a numeral)
   - **IPv6**. To set an IPv6 address, select IPv6, and enter eight hexadecimal alphanumeric characters within the range of 0 to FFFF.
     You can also use an abbreviated-format IPv6 address.
     Example: YYYY:YYYY:YYYY:YYYY:YYYY:YYYY:YYYY:YYYY (Y indicates a hexadecimal digit)

7. In **SMTP Authentication**, select **Enable** to use SMTP authentication. Select **Disable** to not use SMTP authentication. If you select Enable, enter an account and password for SMTP authentication.
   You can use up to 255 alphanumeric characters (ASCII codes) and symbols ('! # $ % & ` + - * / ^ { } _ .).
   This field is mandatory when you selected Enable in Mail Notice.

8. If necessary, click **Email Test Send** to test the settings.

9. Check that the test email has been received.
   For a test email example and explanation, see **Example of test email**, below.

10. Click **Finish**. The **Confirm** window opens.

11. In the **Confirm** window, check the settings and enter a **task name** in Task Name.

12. Click **Apply**. The task is registered. If the **Go to tasks window for status** check box is checked, the **Task** window opens.

### Example of test email
Date: FRI 25 OCT 2013 10:10:10 +9000 (JST)
To: VSP G1000 alarm@example.com
From: xxxx@itg.example.com
Reply-To: xxxx@itg.example.com
Subject: VSP G1000 Report
Date : 25/10/2013
Time : 10:09:30
The field definitions in the test email are listed in the following table:

<table>
<thead>
<tr>
<th>#</th>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Date</td>
<td>Date and time when the email was sent. This time stamp is set by the mail server.</td>
</tr>
<tr>
<td>2</td>
<td>To</td>
<td>Email address of the receiver.</td>
</tr>
<tr>
<td>3</td>
<td>From</td>
<td>Email address of the sender.</td>
</tr>
<tr>
<td>4</td>
<td>Reply-To</td>
<td>Email address to which replies from the receivers will be sent. Optional.</td>
</tr>
<tr>
<td>5</td>
<td>Subject</td>
<td>Email title (Name of the storage system) + (Report)</td>
</tr>
<tr>
<td>6</td>
<td>Date</td>
<td>Date when a system failure occurred.</td>
</tr>
<tr>
<td>7</td>
<td>Time</td>
<td>Time when a system failure occurred.</td>
</tr>
<tr>
<td>8</td>
<td>Machine</td>
<td>Name and serial number of the storage system.</td>
</tr>
<tr>
<td>9</td>
<td>RefCode</td>
<td>Reference code. The same code as the one reported by SNMP traps.</td>
</tr>
<tr>
<td>10</td>
<td>Detail</td>
<td>Failure details. The same information as the one reported by SNMP traps.</td>
</tr>
</tbody>
</table>

See the *Hitachi SNMP Agent User Guide* for reference codes and failure details.

**Related topics**

- [Normal login on page 5-26](#)

**Setting system options**

You can change settings about alert display and data acquisition by setting system options. Log off and log in again when you enabled or disabled a system option.

**Prerequisites**

- You must have the Storage Administrator (Initial Configuration) role to perform this task.

To set system options:

1. Click **Settings > Environmental Settings > Edit System Options**.
2. Select the system option to set and click **Enable**.
   
   - **Hide alert information**. If you enable this system option, the **Alert** window does not open.
- **Refresh forcibly after Apply.** If you enable this system option, after settings changes are applied to the storage system, the configuration information for the storage system is forcibly updated.

- **Disable data polling.** If you enable this system option, polling stops.

- **Disable retry of data updating.** If you enable this system option, retry does not occur even if data cannot be acquired.

- **Enable Device Manager - Storage Navigator 2 All Function.** If you enable this system option, the restrictions on login from Device Manager - Storage Navigator's login window are cleared, including the restrictions on the users who can log in and on the functions available after login. When enabling or disabling the system option, log in again.

3. Click **Finish**. The **Confirm** window opens.

4. In the confirmation window, check the settings and enter a task name in **Task Name**.

5. Click **Apply**. The task is registered. If the **Go to tasks window for status** check box is checked, the **Task** window opens.

**Related topics**

- [Normal login on page 5-26](#)
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
- Enabling 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.

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 \texttt{root/smis/smisxx} (\texttt{xx} is an abbreviation for the version number).
  For example, to specify version 1.5.0, enter \texttt{root/smis/smis15}.
  The latest namespaces that complies with the specified SMI-S version is selected.

- Specify the condition \texttt{current}.
  Enter \texttt{root/smis/current}.
  The current namespace is selected.

- Specify \texttt{interop}.
  SMI-S 1.3.0 or a later version supports the namespace \texttt{interop}. If \texttt{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.

\begin{table}[h]
\centering
\begin{tabular}{|c|c|c|c|}
\hline
Namespace & \texttt{smisxx} & \texttt{current} & \texttt{interop} & SMI-S \\
\hline
\texttt{smis11} & -- & -- & -- & 1.1.0 \\
\texttt{smis12} & -- & -- & -- & 1.2.0 \\
\texttt{smis13} & -- & -- & -- & 1.3.0 \\
\texttt{smis14} & -- & -- & -- & 1.4.0 \\
\texttt{smis15} & \texttt{current} & \texttt{interop} & -- & 1.5.0 \\
\hline
\end{tabular}
\caption{Correspondence between namespaces and SMI-S versions}
\end{table}

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 7-2 Roles in Device Manager and CIM methods that can be executed

<table>
<thead>
<tr>
<th>Role in Device Manager</th>
<th>CIM method that can be executed</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Service methods</td>
</tr>
<tr>
<td>Admin or Modify</td>
<td>Y</td>
</tr>
<tr>
<td>View or Peer</td>
<td>--</td>
</tr>
</tbody>
</table>

Legend:

Y: These CIM methods can be executed.
--: These CIM methods cannot be executed.

Enabling 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.

Operations to complete in advance

- 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.
- 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).

To enable the CIM/WBEM functions:

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, Universal Storage Platform V/VM or Hitachi USP, 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 topics**

- [Ports used by the Device Manager server on page 2-3](#)
- [Starting and stopping the SLP service on page 7-16](#)
- [Starting the Hitachi Command Suite services on page 8-4](#)
- [Stopping the Hitachi Command Suite services on page 8-5](#)
- [server.cim.support on page A-9](#)
- [server.logicalview.initialsynchro on page A-12](#)

**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.

**Operations to complete in advance**

Log in as a user with Administrator permissions (for Windows) or as a root user (for Linux).

**To change a port number:**

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 topics**

- Starting the Hitachi Command Suite services on page 8-4
- Stopping the Hitachi Command Suite services on page 8-5
- `server.cim.http.port` on page A-10
- `server.cim.https.port` on page A-11
- Ciphers on page A-33
- `HTTPPort` on page A-52
- `HTTPSPort` on page A-52

**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 7-2 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 information of enterprise-class storage systems (Virtual Storage Platform, Universal Storage Platform V/VM, and Hitachi USP) 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 when acquiring performance information of enterprise-class storage systems (Virtual Storage Platform, Universal Storage Platform V/VM or Hitachi USP). 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 or Hitachi USP 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.

**Settings required to acquire performance information of enterprise-class storage systems**

This section describes the settings required to acquire performance information for enterprise-class storage systems (Virtual Storage Platform, Universal Storage Platform V/VM, or Hitachi USP).

**Preparing the storage system for acquiring performance information**

Prepare a command device for each storage system from which you want to acquire performance information, and then assign a LUN path to the host that will acquire the performance information so that the host can recognize the command device.

To acquire Virtual Storage Platform performance information, force hosts to recognize command devices for which authentication mode is disabled.

**Preparing the host to acquire performance information**

Install the Device Manager agent, and then register command devices.

**To collect performance information:**

1. Install the Device Manager agent.
   
   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 7-3 CCI/LIB required to acquire performance information**

<table>
<thead>
<tr>
<th>Storage system</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Storage Platform</td>
<td>01-15-03/00 or later</td>
</tr>
<tr>
<td>Universal Storage Platform V/VM</td>
<td>01-12-03/03 or later</td>
</tr>
<tr>
<td>Hitachi USP</td>
<td>01-12-03/03 or later</td>
</tr>
</tbody>
</table>

2. Use the Device Manager agent `hdvmagt_setting` command to configure the central management method settings. (This is recommended.)
3. 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.

**Related topics**

- [Defining the command device (perf_findcmddev command) on page 7-10](#)
- [Setting the Device Manager server's information, HiScan command's execution period, and CCI's information (hdvmagt_setting command) on page 10-20](#)
- [How to install Device Manager agent: Hitachi Command Suite Installation and Configuration Guide](#)

**Preventing the Device Manager server to acquire performance information**

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 topics**

- [Changing Device Manager server properties on page A-4](#)
- [server.cim.agent on page A-9](#)

**Defining the command device (perf_findcmddev command)**

To register a command device on a Device Manager agent, execute the `perf_findcmddev` command with the `write` option specified.

**Operations to complete in advance**

Log in as a user with Administrator permissions or as a root user.
**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]`

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.
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.

<table>
<thead>
<tr>
<th>Raid ID</th>
<th>Serial#</th>
<th>SLPR#</th>
<th>LDEV#</th>
<th>Device file name</th>
</tr>
</thead>
<tbody>
<tr>
<td>R500</td>
<td>14050</td>
<td>0</td>
<td>345</td>
<td><code>\\PhysicalDrive3</code></td>
</tr>
<tr>
<td>R601</td>
<td>44332</td>
<td>1</td>
<td>456</td>
<td><code>\\Volume{xxxxxxx-xxxx-xxx-xxxxxxxx}</code></td>
</tr>
<tr>
<td>R501</td>
<td>UNKNOWN</td>
<td>-</td>
<td>1045</td>
<td><code>\\PhysicalDrive10</code></td>
</tr>
</tbody>
</table>

**Related topics**

- Format of the `perf_cmddev.properties` file on page 7-12

**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 7-4 Settings in the perf_cmddev.properties file

<table>
<thead>
<tr>
<th>Setting item</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>RAID-ID</strong></td>
<td>Specify one of the following depending on the type of the target storage system:&lt;br&gt; R700 for Virtual Storage Platform&lt;br&gt; R600 for Universal Storage Platform V&lt;br&gt; R601 for Universal Storage Platform VM&lt;br&gt; R500 for Hitachi USP&lt;br&gt; R501 for Hitachi NSC55</td>
</tr>
<tr>
<td><strong>Serial-number</strong></td>
<td>Specify the serial number of the storage system by using a decimal (base 10) number.</td>
</tr>
<tr>
<td><strong>SLPR-number</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>LDEV-number</strong></td>
<td>Specify the CU:LDEV number of the command device by using a decimal (base 10) number.</td>
</tr>
<tr>
<td><strong>deviceFileName</strong></td>
<td>Specify the command device identifier (the PhysicalDrive number, VolumeGUID, or device file name) that the host recognizes in the following format:#&lt;br&gt; - In Windows: \PhysicalDriveX \Volume{GUID}&lt;br&gt; - In Solaris: /dev/rdsk/cxt.xdxdxs2&lt;br&gt; - In Linux: /dev/sdx&lt;br&gt; x is an integer.</td>
</tr>
</tbody>
</table>

#:  
- 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 Hitachi USP (whose serial number is 14050).

\[
\begin{align*}
R600.44332.456: & \text{ \textbackslash \textbackslash .PhysicalDrive3} \\
R500.14050.345: & \text{ \textbackslash \textbackslash .PhysicalDrive5} \\
R500.14050.346: & \text{ \textbackslash \textbackslash .PhysicalDrive6} \\
R500.14050.347: & \text{ \textbackslash \textbackslash .PhysicalDrive10} \\
R501.89832.780: & \text{ \textbackslash \textbackslash .PhysicalDrive15}
\end{align*}
\]

**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).

**Preparing the storage system**

Before you use the function for acquiring performance information, you need to use Element Manager in the Device Manager GUI, Storage Navigator Modular, or Storage Navigator Modular 2 to specify the settings for acquiring performance statistics for each relevant storage system.

**Related topics**

- How to specify the settings for collecting performance statistics: The manual for each storage system

**Setting up a user account to acquire performance information (hdvmmodpolluser command)**

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 cannot 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.

To register the user account that is used to acquire performance information in Device Manager, execute the `hdvmmodpolluser` command.

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.

**Operations to complete in advance**

- Register a user account that has only the read permission for each storage system
If you want to acquire performance information from multiple storage systems, the user account registered for each of those storage systems must have the same user ID and password.

**Format of the command**

In Windows:

```bash
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**

In Windows or Red Hat Enterprise Linux:

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/](http://www.openslp.org/)).

In SUSE Linux Enterprise Server:
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/).

Starting and stopping the SLP service
This section describes how to start and stop the SLP service.

Starting and stopping the SLP service (Windows)

Operations to complete in advance
Log in as a user with Administrator permissions.

To start the SLP service:
1. 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
   ```

To stop the SLP service:
1. Perform either of the following procedures:
   - From Administrative Tools, select Services and then Service Location Protocol.
   - Display the command prompt, move to the folder containing the OpenSLP executable file, and execute the following command:

   ```
   slpd -stop
   ```

Starting and stopping the SLP daemon (Red Hat Enterprise Linux)

Operations to complete in advance
Log in as a user with root user.

To start the SLP daemon:
1. Execute the following command:

   ```
   installation-directory-for-Hitachi-Command-Suite/HiCommandServer/wsi/bin/
   slpd.sh start
   ```

To stop the SLP daemon:
1. Execute the following command:
Starting and stopping the SLP daemon (SUSE Linux Enterprise Server)

**Operations to complete in advance**

Log in as a user with root user.

**To start the SLP daemon:**

1. Execute the following command:

```
#/usr/sbin/rcslpd start
```

**To stop the SLP daemon:**

1. Execute the following command:

```
#/usr/sbin/rcslpd stop
```

Releasing the SLP service

You might need to release the SLP service (or SLP daemon) 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.
```

Releasing the SLP service (Windows)

**Operations to complete in advance**

Log in as a user with Administrator permissions.

**To release the SLP service:**

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)

Operations to complete in advance

Log in as a user with root user.

To release the SLP daemon:

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
```
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
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>
<thead>
<tr>
<th>Process name</th>
<th>Service name</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>htmservice.exe</td>
<td>HiCommand Tiered Storage Manager</td>
<td>The Tiered Storage Manager server</td>
</tr>
<tr>
<td>HiCommandServer</td>
<td>HiCommandServer</td>
<td>The Device Manager server</td>
</tr>
<tr>
<td>hcmdssvctl.exe cjstartweb.exe</td>
<td>HBase 64 Storage Mgmt Common Service</td>
<td>Hitachi Command Suite servlet service. If the Device Manager server and other Hitachi Command Suite products are installed on the same computer, a process of a service other than HBase 64 Storage Mgmt Common Service might be started by using the name hcmdssvctl.exe and cjstartweb.exe.</td>
</tr>
<tr>
<td>hcmdssvctl.exe cjstartweb.exe</td>
<td>HBase 64 Storage Mgmt SSO Service</td>
<td>Hitachi Command Suite servlet service for single sign-on</td>
</tr>
<tr>
<td>httpsd.exe rotatelogs.exe</td>
<td>HBase 64 Storage Mgmt Web Service</td>
<td>Hitachi Command Suite common web service. Multiple instances of this process might be running.</td>
</tr>
<tr>
<td>httpsd.exe rotatelogs.exe</td>
<td>HBase 64 Storage Mgmt Web SSO Service</td>
<td>Hitachi Command Suite common web service for single sign-on.</td>
</tr>
<tr>
<td>hcmdssvctl.exe cjstartweb.exe</td>
<td>HCS Device Manager Web Service</td>
<td>Device Manager servlet service</td>
</tr>
<tr>
<td>hntr2mon.exe</td>
<td>Hitachi Network Objectplaza Trace Monitor 2</td>
<td>Hitachi Command Suite common trace log collection</td>
</tr>
<tr>
<td>hntr2srv.exe</td>
<td>Hitachi Network Objectplaza Trace Monitor 2 (x64)</td>
<td>Hitachi Command Suite common trace service (This service processes events from the Services window.)</td>
</tr>
<tr>
<td>Process name</td>
<td>Service name</td>
<td>Function</td>
</tr>
<tr>
<td>--------------------</td>
<td>---------------------------------------------------</td>
<td>----------------------------------------------------</td>
</tr>
<tr>
<td>pdservice.exe#</td>
<td>HiRDB/EmbeddedEdition_HD1</td>
<td>HiRDB process server control</td>
</tr>
</tbody>
</table>

#: This process must always be running. Do not stop it manually or register it as a cluster resource.

Table 8-2 Resident processes in Linux

<table>
<thead>
<tr>
<th>Process name</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>htsmservice</td>
<td>The Tiered Storage Manager server</td>
</tr>
<tr>
<td>hicmdserver</td>
<td>The Device Manager server</td>
</tr>
<tr>
<td></td>
<td>installation-directory-for-Hitachi-Command-Suite/HiCommandServer/hicmdserver</td>
</tr>
<tr>
<td>hcs_sso</td>
<td>Hitachi Command Suite servlet service</td>
</tr>
<tr>
<td></td>
<td>/bin/sh installation-directory-for-Hitachi-Command-Suite/Base64/uCPSB/CC/web/containers/HiCommand64/hcs_sso</td>
</tr>
<tr>
<td></td>
<td>installation-directory-for-Hitachi-Command-Suite/Base64/uCPSB/CC/web/bin/cjstartweb</td>
</tr>
<tr>
<td>hcs_hsso</td>
<td>Hitachi Command Suite servlet service for single sign-on</td>
</tr>
<tr>
<td></td>
<td>installation-directory-for-Hitachi-Command-Suite/Base64/uCPSB/CC/web/containers/HiBase64StgMgmtSSOService/hcs_hsso</td>
</tr>
<tr>
<td></td>
<td>installation-directory-for-Hitachi-Command-Suite/Base64/uCPSB/CC/web/bin/cjstartweb</td>
</tr>
<tr>
<td>httpsd</td>
<td>Hitachi Command Suite common web service</td>
</tr>
<tr>
<td>rotatelogs</td>
<td>Multiple instances of this process might be running.</td>
</tr>
<tr>
<td></td>
<td>installation-directory-for-Hitachi-Command-Suite/Base64/uCPSB/httpsd/sbin/httpsd</td>
</tr>
<tr>
<td></td>
<td>installation-directory-for-Hitachi-Command-Suite/Base64/uCPSB/httpsd/sbin/rotatelogs</td>
</tr>
<tr>
<td>httpsd</td>
<td>Hitachi Command Suite common web service for single sign-on.</td>
</tr>
<tr>
<td>rotatelogs</td>
<td>installation-directory-for-Hitachi-Command-Suite/Base64/uCPSB/httpsd/sbin/httpsd</td>
</tr>
<tr>
<td></td>
<td>installation-directory-for-Hitachi-Command-Suite/Base64/uCPSB/httpsd/sbin/rotatelogs</td>
</tr>
<tr>
<td>hcs_dm</td>
<td>Device Manager servlet service</td>
</tr>
<tr>
<td>cjstartweb</td>
<td>/bin/sh installation-directory-for-Hitachi-Command-Suite/Base64/uCPSB/CC/web/containers/DeviceManagerWebService/hcs_dm</td>
</tr>
<tr>
<td></td>
<td>installation-directory-for-Hitachi-Command-Suite/Base64/uCPSB/CC/web/bin/cjstartweb</td>
</tr>
</tbody>
</table>
### Process name | Function
--- | ---
`/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 topics**
- [Starting the Hitachi Command Suite services on page 8-4](#)
- [Stopping the Hitachi Command Suite services on page 8-5](#)
- [Checking the operating status of the Hitachi Command Suite services on page 8-7](#)
- [Resident processes of the Host Data Collector on page 8-8](#)

## Starting the Hitachi Command Suite services

You can start the Hitachi Command Suite services from the Windows menu or by using the `hcmds64srv` command.

### Operations to complete in advance

Log in as a user with Administrator permissions (for Windows) or as a root user (for Linux).

### To start the services:

1. 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`
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 Common Service
- 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

**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`

**Stopping the Hitachi Command Suite services**

You can stop the Hitachi Command Suite services from the Windows menu or by using the `hcmdssrv` command.

**Operations to complete in advance**

Log in as a user with Administrator permissions (for Windows) or as a root user (for Linux).
To stop the services:

1. 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:
   
   ```plaintext
   installation-folder-for-Hitachi-Command-Suite\Base64\bin
   \hcmands64srv /stop
   ```
   
   In Linux:
   
   Execute the following command:
   
   ```plaintext
   installation-directory-for-Hitachi-Command-Suite/
   Base64/bin/hcmands64srv -stop
   ```
   
   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 Common Service
   - 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

   **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 stop Hitachi Command Suite product services, also execute the following commands:
   
   - In Windows:
     
     ```plaintext
     installation-folder-for-Hitachi-File-Services-Manager-or-
     Storage-Navigator-Modular-2\Base\bin\hcmandsrv /stop
     ```
   
   - In Linux:
     
     ```plaintext
     installation-directory-for-Hitachi-File-Services-Manager-or-
     Storage-Navigator-Modular-2/Base/bin/hcmandsrv -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
```

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.

Operations to complete in advance

Log in as a user with Administrator permissions (for Windows) or as a root user (for Linux).

To check the operating status of the services:

1. 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
   ```

   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 8-3 Resident processes of the Host Data Collector (Windows) on page 8-8 to Table 8-4 Resident processes of the Host Data Collector (Linux) on page 8-8.

Table 8-3 Resident processes of the Host Data Collector (Windows)

<table>
<thead>
<tr>
<th>Process name</th>
<th>Service name</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>HdcProcessController.exe</td>
<td>Host Data Collector Base</td>
<td>Host Data Collector</td>
</tr>
<tr>
<td></td>
<td>Service</td>
<td>service</td>
</tr>
</tbody>
</table>

Table 8-4 Resident processes of the Host Data Collector (Linux)

<table>
<thead>
<tr>
<th>Process name</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>installation-directory-for-Host-Data-Collector</td>
<td>Adapter process of the Host Data Collector service#</td>
</tr>
<tr>
<td>/HDC/Base/internal/bin/HdcAdapter.sh</td>
<td></td>
</tr>
<tr>
<td>installation-directory-for-Host-Data-Collector</td>
<td>Service process of the Host Data Collector service</td>
</tr>
<tr>
<td>/HDC/Base/internal/bin/HdcService.sh</td>
<td></td>
</tr>
<tr>
<td>installation-directory-for-Host-Data-Collector</td>
<td>RMI process of the Host Data Collector service</td>
</tr>
<tr>
<td>/HDC/Base/internal/bin/HdcRMI.sh</td>
<td></td>
</tr>
<tr>
<td>Java-execution-environment-installation-path/bin</td>
<td>JavaVM (Adapter)#</td>
</tr>
<tr>
<td>java</td>
<td></td>
</tr>
<tr>
<td>Java-execution-environment-installation-path/bin</td>
<td>JavaVM (Service)</td>
</tr>
<tr>
<td>java</td>
<td></td>
</tr>
<tr>
<td>Java-execution-environment-installation-path/bin</td>
<td>JavaVM (RMI)</td>
</tr>
<tr>
<td>java</td>
<td></td>
</tr>
</tbody>
</table>

#: 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 topics

- Resident processes of Hitachi Command Suite on page 8-2
Starting the Host Data Collector service

Use the `controlservice` command to start the Host Data Collector service.

**Operations to complete in advance**

Log in as a user with Administrator permissions (for Windows) or as a root user (for Linux).

**To start the Host Data Collector service:**

1. 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 topics**

- Resident processes of the Host Data Collector on page 8-8
- Stopping the Host Data Collector service on page 8-9
- Checking the operating status of the Host Data Collector service on page 8-10

Stopping the Host Data Collector service

Use the `controlservice` command to stop the Host Data Collector service.

**Operations to complete in advance**

Log in as a user with Administrator permissions (for Windows) or as a root user (for Linux).

**To stop the Host Data Collector service:**

1. 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 topics**

- Resident processes of the Host Data Collector on page 8-8
- Starting the Host Data Collector service on page 8-9
• Checking the operating status of the Host Data Collector service on page 8-10

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.

Operations to complete in advance

Log in as a user with Administrator permissions (for Windows) or as a root user (for Linux).

To check the operating status of the Host Data Collector service:

1. 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 topics

• Resident processes of the Host Data Collector on page 8-8
• Starting the Host Data Collector service on page 8-9
• Stopping the Host Data Collector service on page 8-9
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>
<thead>
<tr>
<th>Item</th>
<th>Backing up and restoring</th>
<th>Exporting and importing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Restrictions on Hitachi Command Suite product versions</td>
<td>No restrictions</td>
<td>Products of version 05-50 or later must be installed on the server to which data is imported or from which data is exported.</td>
</tr>
<tr>
<td>Main purpose</td>
<td>To restore the current operating environment if a failure occurs on the server</td>
<td>To migrate the server data from the current environment to a different environment (such as a server that has a different OS)</td>
</tr>
</tbody>
</table>
| 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:

\[(\text{total-size-of-all-Hitachi-Command-Suite-product-databases-to-be-backed-up} + 4.6 \text{ GB}) \times 2\]
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.

**To back up a database:**

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 cluster configuration

To back up a database when Windows management servers 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.

To back up a database:
1. Log on to the management server as a user with Administrator permissions.
2. Use the cluster management application to select the following services, and then from the right-click menu, take the services offline:
   - HiCommand Tiered Storage Manager
   - HiCommandServer
   - HCS Device Manager Web Service
   - HBase 64 Storage Mgmt Web Service
   - HBase 64 Storage Mgmt Common Service
   - Hitachi Command Suite product resources other than the above
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. Use the cluster management application to take the following service offline:
5. Use the cluster management application to suppress failover of the resource group.
   Change the settings of the resources listed below.
   - HiCommand Tiered Storage Manager
   - HiCommandServer
   - HCS Device Manager Web Service
   - HBase 64 Storage Mgmt Web Service
   - HBase 64 Storage Mgmt Common Service
   - HiRDBClusterService _HD1
   - Hitachi Command Suite product resources other than the above
   Right-click the resource name, and select Properties, the Policies tab, and then If resource fails, do not restart.

6. Execute the \hs MutableList command to back up the database.
   \installation-folder-for-Hitachi-Command-Suite\Base64\bin\hs MutableList /dir \folder-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 \hs MutableList 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.

7. Execute the \hs MutableList /stop command to stop the Hitachi Command Suite product services.
   Then, execute the \hs MutableList /statusall command to make sure that the services have stopped or that the return code of the command is 0.

8. Use the cluster management application to enable failover of the resource group.
   Change the settings of the resources listed below.
   - HiCommand Tiered Storage Manager
   - HiCommandServer
   - HCS Device Manager Web Service
   - HBase 64 Storage Mgmt Web Service
   - HBase 64 Storage Mgmt Common Service
   - HiRDBClusterService _HD1
   - Hitachi Command Suite product resources other than the above
Right-click the resource name, select Properties, the Policies tab, and then the following items:

- **If resource fails, attempt restart on current node**
- **If restart is unsuccessful, fail over all resources in this Role** (or **If restart unsuccessful, fail over all resources in this service or application**)

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

**Related topics**
- Starting the Hitachi Command Suite services on page 8-4
- Stopping the Hitachi Command Suite services on page 8-5

**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.
- During database restoration, Hitachi Command Suite services stop. Therefore, do not access Hitachi Command Suite while restoration is in progress.

To restore a database:

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 9-2 Values to specify for the type option when restoring databases (In a non-cluster configuration)

<table>
<thead>
<tr>
<th>Product</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Manager</td>
<td>DeviceManager</td>
</tr>
<tr>
<td>Tiered Storage Manager</td>
<td>TieredStorageManager</td>
</tr>
<tr>
<td>Replication Manager</td>
<td>ReplicationManager</td>
</tr>
<tr>
<td>Other products</td>
<td>Refer to the manual for each product.</td>
</tr>
</tbody>
</table>

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 topics**

- Specifying the settings for remote connection to the Tuning Manager server and the port number (htmsetup command) on page 5-18
- Starting the Hitachi Command Suite services on page 8-4

**Restoring a database when a data inconsistency occurs in a cluster configuration**

To restore a database when Windows management servers 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.
- During database restoration, Hitachi Command Suite services stop. Therefore, do not access Hitachi Command Suite while restoration is in progress.

To restore a database:

1. Log on to the management server as a user with Administrator permissions.
2. Use the cluster management application to select the following services, and then from the right-click menu, take the services offline:
   - HiCommand Tiered Storage Manager
   - HiCommandServer
   - HCS Device Manager Web Service
   - HBase 64 Storage Mgmt Web Service
   - HBase 64 Storage Mgmt Common Service
   - Hitachi Command Suite product resources other than the above
3. Execute the `hcmds64srv` command to stop the Hitachi Command Suite product services.

4. Use the cluster management application to take the following services offline:
   - `HiRDBClusterService _HD1`

5. Use the cluster management application to suppress failover of the resource group. Change the settings of the resources listed below.
   - `HiCommand Tiered Storage Manager`
   - `HiCommandServer`
   - `HCS Device Manager Web Service`
   - `HBase 64 Storage Mgmt Web Service`
   - `HBase 64 Storage Mgmt Common Service`
   - `HiRDBClusterService _HD1`
   - `Hitachi Command Suite product resources other than the above`

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

6. 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 9-3 Values to specify for the type option when restoring databases (For a cluster configuration)

<table>
<thead>
<tr>
<th>Product</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Manager</td>
<td>DeviceManager</td>
</tr>
<tr>
<td>Tiered Storage Manager</td>
<td>TieredStorageManager</td>
</tr>
<tr>
<td>Replication Manager</td>
<td>ReplicationManager</td>
</tr>
<tr>
<td>Other products</td>
<td>Refer to the manual for each product.</td>
</tr>
</tbody>
</table>
7. 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.

8. 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.

9. Use the cluster management application to enable failover of the resource group.
   Change the settings of the resources listed below.
   - HiCommand Tiered Storage Manager
   - HiCommandServer
   - HCS Device Manager Web Service
   - HBase 64 Storage Mgmt Web Service
   - HBase 64 Storage Mgmt Common Service
   - HiRDBClusterService _HD1
   - Hitachi Command Suite product resources other than the above
   Right-click the resource name, select Properties, the Policies tab, and then the following items:
   - If resource fails, attempt restart on current node
   - If restart is unsuccessful, fail over all resources in this Role (or If restart unsuccessful, fail over all resources in this service or application)

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

11. On the executing node and standby node, change the value of the server.base.initialsynchro property on the Device Manager server back to false.

12. 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.

13. If you specified ALL or DeviceManager for the type option, refresh the storage system from the Device Manager GUI or CLI.

14. 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.

15. 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.

16. 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
The task IDs of Tiered Storage Manager tasks whose status was changed to **Failure** are output to KATS50354-E.

17. 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.

18. If a Tiered Storage Manager task is not completed, create and execute the task again as necessary.

19. If Tuning Manager is remotely connected, the remote connection setting is re-initialized during a database restoration. Specify the setting again. Specify the remote connection setting with Tuning Manager again by following [Remote connection to the Tuning Manager server (in a cluster environment) on page 5-15](#).

**Related topics**

- [Stopping the Hitachi Command Suite services on page 8-5](#)

## 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.
- During database restoration, Hitachi Command Suite services stop. Therefore, do not access Hitachi Command Suite while restoration is in progress.

**To restore a database:**

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.

Related topics

- Specifying the settings for remote connection to the Tuning Manager server and the port number (htmssetup command) on page 5-18
- Starting the Hitachi Command Suite services on page 8-4
- Stopping the Hitachi Command Suite services on page 8-5
Restoring a database when it is corrupted in a cluster configuration

To restore a database when Windows management servers 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.
- During database restoration, Hitachi Command Suite services stop. Therefore, do not access Hitachi Command Suite while restoration is in progress.

**To restore a database:**

1. Log on to the management server as a user with Administrator permissions.
2. Use the cluster management application to select the following services, and then from the right-click menu, take the services offline:
   - HiCommand Tiered Storage Manager
   - HiCommandServer
   - HCS Device Manager Web Service
   - HBase 64 Storage Mgmt Web Service
   - HBase 64 Storage Mgmt Common Service
   - Hitachi Command Suite product resources other than the above
3. Execute the `hcmds64srv` command to stop the Hitachi Command Suite product services.
4. Use the cluster management application to take the following services offline:
   - HiRDBClusterService _HD1
5. Use the cluster management application to suppress failover of the resource group. Change the settings of the resources listed below:
   - HiCommand Tiered Storage Manager
   - HiCommandServer
   - HCS Device Manager Web Service
   - HBase 64 Storage Mgmt Web Service
- HBase 64 Storage Mgmt Common Service
- HiRDBClusterService _HD1
- Hitachi Command Suite product resources other than the above
Right-click the resource name, and select **Properties**, the **Policies** tab, and then **If resource fails, do not restart**.

6. **Execute** the `hcmds64dbrepair` command to restore the database.

   ```
   installation-folder-for-Hitachi-Command-Suite\Base64\bin
   \hcmds64dbrepair /trans exported-file
   ```

   Specify the absolute path to the archive file of the database exported via the `hcmds64dbtrans` command.

7. On the executing node and standby node, specify `true` for the `server.base.initialsynchro` property on the Device Manager server.

8. On the executing node and standby node, specify `true` for the `server.base.initialsynchro` property on the Tiered Storage Manager server.

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

   Change the settings of the resources listed below.
   - HiCommand Tiered Storage Manager
   - HiCommandServer
   - HCS Device Manager Web Service
   - HBase 64 Storage Mgmt Web Service
   - HBase 64 Storage Mgmt Common Service
   - HiRDBClusterService _HD1
   - Hitachi Command Suite product resources other than the above
Right-click the resource name, select **Properties**, the **Policies** tab, and then the following items:

   - **If resource fails, attempt restart on current node**
   - **If restart is unsuccessful, fail over all resources in this Role** (or **If restart unsuccessful, fail over all resources in this service or application**)

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

11. On the executing node and standby node, change the value of the `server.base.initialsynchro` property on the Device Manager server back to `false`.

12. 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`.

13. Refresh the storage system from the Device Manager GUI or CLI.
14. 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.

15. 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.

16. 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.

17. 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.

18. If a Tiered Storage Manager task is not completed, create and execute the task again as necessary.

19. If Tuning Manager is remotely connected, the remote connection setting is re-initialized during a database restoration. Specify the setting again. Specify the remote connection setting with Tuning Manager again by following [Remote connection to the Tuning Manager server (in a cluster environment)] on page 5-15.

20. The password for the **System** account is re-initialized during a database restoration. If necessary, specify the password again.

**Related topics**
- [Stopping the Hitachi Command Suite services](#) on page 8-5
- How to change the password for the **System** account: *Hitachi Command Suite User Guide*

**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

To migrate databases:

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 the databases from the migration source server when the OS of 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 total capacity of databases exceeds 2 GB, creation of the archive file fails when the database data is exported. In this case, instead of using the archive file, 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.

**To export databases:**

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.
Using an absolute path, specify the name of the archive file to be output. In Linux, do not include a space in this path.

Automatically starts or stops Hitachi Command Suite services.

3. Transfer the exported 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 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 total capacity of databases exceeds 2 GB, creation of the archive file fails when the database data is exported. In this case, instead of using the archive file, 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.

To export databases:

1. Log on to the management server as a user with Administrator permissions.
2. Use the cluster management application to select the following services, and then from the right-click menu, take the services offline:
3. Execute the `hcmsds64srv` command to stop the Hitachi Command Suite product services.

4. Use the cluster management application to take the following service offline:
   - HiRDBClusterService _HD1

5. Use the cluster management application to suppress failover of the resource group.
   Change the settings of the resources listed below.
   - HiCommand Tiered Storage Manager
   - HiCommandServer
   - HCS Device Manager Web Service
   - HBase 64 Storage Mgmt Web Service
   - HBase 64 Storage Mgmt Common Service
   - HiRDBClusterService _HD1
   - Hitachi Command Suite product resources other than the above
   Right-click the resource name, and select Properties, the Policies tab, and then **If resource fails, do not restart.**

6. Execute the `hcmsds64srv` command to start the Hitachi Command Suite product services.

7. Execute the `hcmsds64dbtrans` command to export the databases.

   ```
   installation-folder-for-Hitachi-Command-Suite\Base64\bin \hcmsds64dbtrans /export /workpath working-folder /file archive-file
   ```

   **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.

8. Transfer the exported 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.
9. Execute the `hcmds64srv` command to stop the Hitachi Command Suite product services.

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

    Change the settings of the resources listed below.

    - HiCommand Tiered Storage Manager
    - HiCommandServer
    - HCS Device Manager Web Service
    - HBase 64 Storage Mgmt Web Service
    - HBase 64 Storage Mgmt Common Service
    - HiRDBClusterService _HD1
    - Hitachi Command Suite product resources other than the above

    Right-click the resource name, select **Properties**, the **Policies** tab, and then the following items:

    - If resource fails, attempt restart on current node
    - If restart is unsuccessful, fail over all resources in this Role (or If restart unsuccessful, fail over all resources in this service or application)

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

### Related topics

- [Starting the Hitachi Command Suite services on page 8-4](#)
- [Stopping the Hitachi Command Suite services on page 8-5](#)

### Importing databases on the migration destination server (for a non-cluster configuration)

This section explains how to import the databases on the migration destination server when the OS of 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.

- During database import, Hitachi Command Suite services stop. Therefore, do not access Hitachi Command Suite while the import is in progress.

#### To import databases:

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|Hitachi-Command-Suite-products-whose-databases-will-be-migrated} /auto
   ```

   **In Linux:**
   ```
   \installation-directory-for-Hitachi-Command-Suite/\Base64/bin/hcmds64dbtrans -import -workpath working-directory [-file archive-file] -type {ALL|Hitachi-Command-Suite-products-whose-databases-will-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 9-4 Values to specify for the `type` option when migrating databases (In a non-cluster configuration)

<table>
<thead>
<tr>
<th>Product</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Manager#1#2</td>
<td>DeviceManager</td>
</tr>
<tr>
<td>Tiered Storage Manager#1</td>
<td>TieredStorageManager</td>
</tr>
<tr>
<td>Replication Manager#2</td>
<td>ReplicationManager</td>
</tr>
<tr>
<td>Other products</td>
<td>Refer to the manual for each product.</td>
</tr>
</tbody>
</table>

#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 topics
- Specifying the settings for remote connection to the Tuning Manager server and the port number (htmsetup command) on page 5-18
- Starting the Hitachi Command Suite services on page 8-4
- Backing up a database in non-cluster configuration on page 9-3

Importing databases on the migration destination server (for a 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.
- During database import, Hitachi Command Suite services stop. Therefore, do not access Hitachi Command Suite while the import is in progress.

To import databases:
1. Log on to the management server as a user with Administrator 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 executing node and standby node of 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. Use the cluster management application to select the following services, and then from the right-click menu, take the services offline:
   - HiCommand Tiered Storage Manager
   - HiCommandServer
   - HCS Device Manager Web Service
   - HBase 64 Storage Mgmt Web Service
   - HBase 64 Storage Mgmt Common Service
   - Hitachi Command Suite product resources other than the above

4. Execute the `hcms64srv` command to stop the Hitachi Command Suite product services.

5. Use the cluster management application to take the following services offline:
   - HiRDBClusterService _HD1

6. Use the cluster management application to suppress failover of the resource group.
   Change the settings of the resources listed below.
   - HiCommand Tiered Storage Manager
   - HiCommandServer
   - HCS Device Manager Web Service
   - HBase 64 Storage Mgmt Web Service
   - HBase 64 Storage Mgmt Common Service
   - HiRDBClusterService _HD1
   - Hitachi Command Suite product resources other than the above
   Right-click the resource name, and select Properties, the Policies tab, and then If resource fails, do not restart.

7. Start HiRDB.
   `installation-folder-for-Hitachi-Command-Suite\Base64\bin \hcms64dbsrv /start`

8. Execute the `hcms64dbtrans` command to import the databases.
   `installation-folder-for-Hitachi-Command-Suite\Base64\bin \hcms64dbtrans /import /workpath working-folder [/file archive-file] /type {ALL|Hitachi-Command-Suite-products-whose-databases-will-be-migrated}

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>
<thead>
<tr>
<th>Product</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Manager</td>
<td>DeviceManager</td>
</tr>
<tr>
<td>Tiered Storage Manager</td>
<td>TieredStorageManager</td>
</tr>
<tr>
<td>Replication Manager</td>
<td>ReplicationManager</td>
</tr>
<tr>
<td>Other products</td>
<td>Refer to the manual for each product.</td>
</tr>
</tbody>
</table>

#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.

9. 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 hcmd64dbtrans command does not migrate the Common Component repository, you need to...
synchronize the repository information with the imported Device Manager database data.

10. On the executing node and standby node, specify true for the server.base.initialsynchro of the Tiered Storage Manager server.

11. Execute the hcmds64srv command to start the Hitachi Command Suite product services.

12. Use the cluster management application to enable failover of the resource group. Change the settings of the resources listed below.
   - HiCommand Tiered Storage Manager
   - HiCommandServer
   - HCS Device Manager Web Service
   - HBase 64 Storage Mgmt Web Service
   - HBase 64 Storage Mgmt Common Service
   - HiRDBClusterService _HD1
   - Hitachi Command Suite product resources other than the above
   Right-click the resource name, select Properties, the Policies tab, and then the following items:
     - If resource fails, attempt restart on current node
     - If restart is unsuccessful, fail over all resources in this Role (or If restart unsuccessful, fail over all resources in this service or application)

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

14. On the executing node and standby node, change the value of the server.base.initialsynchro property of the Device Manager server back to false.

15. 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.

16. 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.

17. 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.
18. 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.

19. If Tuning Manager is remotely connected, the remote connection setting is re-initialized during a database import. Specify the setting again. Specify the remote connection setting with Tuning Manager again by following Remote connection to the Tuning Manager server (in a cluster environment) on page 5-15.

Related topics

- Starting the Hitachi Command Suite services on page 8-4
- Stopping the Hitachi Command Suite services on page 8-5
- Backing up a database in a cluster configuration on page 9-4
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.

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:

a. From Control Panel, click Network and Sharing Center, and then click Change adapter settings.

b. 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 topics

• Changing Device Manager agent properties on page D-2
• server.http.socket.agentAddress on page D-11

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
  ○ Upgrading HP-UX from a version earlier than 11i v2 to version 11i v2 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:
  ```cmd
  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).

#### 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 an enterprise-class storage system is acquired by using the CIM/WBEM function

  If the host OS is Red Hat Enterprise Linux 7 or later, or Oracle Linux 7 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 topics**

- [Registering the Windows Firewall exceptions for Device Manager agent (firewall_setup command) on page 10-6](#)

- [Starting and stopping the Device Manager agent service, and checking the operating status of the service (hbsasrv command) on page 10-15](#)
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 topics**

- `server.agent.port` on page D-11
- `server.http.localPort` on page D-11
- `server.http.port` on page D-11

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.

**Information to collect in advance**

- 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.

To register a Java process in SED as an exception:

1. Execute the following command to register the Java process to be used by the Device Manager agent as an SED exception:

   ```bash
   # 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:

   ```bash
   # 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 topics

- `server.agent.JRE.location` on page D-13

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:
  `server.agent.rm.location` property in the `server.properties` file of the Device Manager agent

- If you want to centrally manage copy pairs in the storage system managed by the Device Manager server from the management target host:
  `server.agent.rm.centralizePairConfiguration` property in the `server.properties` file of the Device Manager agent

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:
  `server.agent.rm.ignorePairStatus` property in the `server.properties` file of the Device Manager agent
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 local management is used: Refresh the storage systems.
If central management is used: Refresh the pair management server.

- 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:
  `server.agent.rm.ignorePairStatus` property in the `server.properties` file of the Device Manager agent
  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.

- If you want to unify the coding format of pair volume information into the `HORCM_DEV` or `HORCM_LDEV` format when creating pairs:
  `server.agent.rm.pairDefinitionForm` property in the `server.properties` file of the Device Manager agent

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 \texttt{HORCM\_LDEV}. Note that before you change to the \texttt{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
  
  \texttt{server.agent.rm.exclusion.instance} property in the \texttt{server.properties} file of the Device Manager agent

- If you want to optimize a user-created CCI configuration definition file so that it can be used in Device Manager
  
  \texttt{server.agent.rm.optimization.userHorcmFile} property in the \texttt{server.properties} file of the Device Manager agent

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.

- \texttt{agent.rm.TimeOut} property in the \texttt{agent.properties} file of the Device Manager agent
  
  Adjust this value as necessary, while running Replication Manager and checking for timeouts during processing.

- \texttt{server.agent.maxMemorySize} property in the \texttt{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 \texttt{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 topics

- \textbf{Changing Device Manager agent properties on page D-2}
- \texttt{agent.rm.TimeOut} on page D-3
- \texttt{server.agent.maxMemorySize} on page D-12
- \texttt{server.agent.rm.centralizePairConfiguration} on page D-15
- \texttt{server.agent.rm.exclusion.instance} on page D-16
- \texttt{server.agent.rm.location} on page D-16
- \texttt{server.agent.rm.optimization.userHorcmFile} on page D-17
- \texttt{server.agent.rm.pairDefinitionForm} on page D-18
- \texttt{server.agent.rm.ignorePairStatus} on page D-20
- \texttt{server.agent.rm.moduleTimeOut} on page D-21
• About the `hdvmagtif.MaxPollingCount` property and the `hdvmagtif.PollingInterval` property in the Replication Manager server `agentif.properties` file: *Replication Manager Configuration Guide*

**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 10-1 Recommended property values for a host that will manage 100 or more LUs (when the host is not using a volume manager)

<table>
<thead>
<tr>
<th>Number of LUs managed by Device Manager, and recognized by the host</th>
<th>server.http.entity.maxLength (units: bytes)</th>
<th>server.http.server.timeOut (units: seconds)</th>
<th>server.util.processTimeOut (units: milliseconds)</th>
</tr>
</thead>
<tbody>
<tr>
<td>100</td>
<td>131,072 or more</td>
<td>600 (Default value)</td>
<td>600,000 (Default value)</td>
</tr>
<tr>
<td>256</td>
<td>153,600 or more</td>
<td>600</td>
<td>600,000</td>
</tr>
<tr>
<td>512</td>
<td>307,200 or more</td>
<td>600</td>
<td>600,000</td>
</tr>
<tr>
<td>1,024</td>
<td>614,400 or more</td>
<td>1,200</td>
<td>1,200,000</td>
</tr>
</tbody>
</table>

When the host is using a volume manager

Table 10-2 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 10-11 through Table 10-6 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 10-14 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 10-2 Recommended property values for a host that will manage 100 or more LUs (when the host is using a volume manager in Windows)

<table>
<thead>
<tr>
<th>Number of LUs and logical volumes managed by Device Manager and recognized by the host</th>
<th>server.http.entity.maxLength (units: bytes)</th>
<th>server.http.server.timeOut (units: seconds)</th>
<th>server.util.processTimeOut (units: milliseconds)</th>
<th>server.agent.maxMemorySize (units: MB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>88/10</td>
<td>230,000 or more</td>
<td>600 (Default value)</td>
<td>600,000 (Default value)</td>
<td>64</td>
</tr>
<tr>
<td>88/20</td>
<td>750,000 or more</td>
<td>600</td>
<td>600,000</td>
<td>64</td>
</tr>
</tbody>
</table>
### Table 10-3 Recommended property values for a host that will manage 100 or more LUs (when the host is using a volume manager in Solaris)

<table>
<thead>
<tr>
<th>Number of LUs and logical volumes managed by Device Manager and recognized by the host</th>
<th>server.http.entity.maxLength (units: bytes)</th>
<th>server.http.server.timeout (units: seconds)</th>
<th>server.util.processTimeOut (units: milliseconds)</th>
<th>server.agent.maxMemorySize (units: MB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>100/200</td>
<td>12,000,000 or more</td>
<td>600</td>
<td>600,000</td>
<td>128</td>
</tr>
<tr>
<td>100/500</td>
<td>30,000,000 or more</td>
<td>600</td>
<td>600,000</td>
<td>384</td>
</tr>
<tr>
<td>150/500</td>
<td>12,000,000 or more</td>
<td>600</td>
<td>600,000</td>
<td>512</td>
</tr>
<tr>
<td>250/500</td>
<td>18,000,000 or more</td>
<td>600</td>
<td>600,000</td>
<td>768</td>
</tr>
<tr>
<td>500/1,000</td>
<td>36,000,000 or more</td>
<td>600</td>
<td>600,000</td>
<td>768</td>
</tr>
<tr>
<td>1,000/1,000</td>
<td>72,000,000 or more</td>
<td>1,200</td>
<td>600,000</td>
<td>768</td>
</tr>
</tbody>
</table>
### Table 10-4 Recommended property values for a host that will manage 100 or more LUs (when the host is using a volume manager in AIX)

<table>
<thead>
<tr>
<th>Number of LUs and logical volumes managed by Device Manager and recognized by the host</th>
<th>server.http.entity.maxLength (units: bytes)</th>
<th>server.http.server.timeOut (units: seconds)</th>
<th>server.util.processTimeOut (units: milliseconds)</th>
<th>server.agent.maxMemorySize (units: MB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>100/200</td>
<td>2,500,000 or more (Default value)</td>
<td>600</td>
<td>600,000 (Default value)</td>
<td>128</td>
</tr>
<tr>
<td>100/500</td>
<td>6,000,000 or more</td>
<td>600</td>
<td>600,000</td>
<td>384</td>
</tr>
<tr>
<td>175/500</td>
<td>11,000,000 or more</td>
<td>600</td>
<td>600,000</td>
<td>640</td>
</tr>
<tr>
<td>250/500</td>
<td>15,000,000 or more</td>
<td>600</td>
<td>600,000</td>
<td>768</td>
</tr>
<tr>
<td>500/1,000</td>
<td>19,000,000 or more</td>
<td>600</td>
<td>600,000</td>
<td>768</td>
</tr>
<tr>
<td>1,000/1,000</td>
<td>38,000,000 or more</td>
<td>600</td>
<td>600,000</td>
<td>768</td>
</tr>
</tbody>
</table>

### Table 10-5 Recommended property values for a host that will manage 100 or more LUs (when the host is using a volume manager in Linux)

<table>
<thead>
<tr>
<th>Number of LUs and logical volumes managed by Device Manager and recognized by the host</th>
<th>server.http.entity.maxLength (units: bytes)</th>
<th>server.http.server.timeOut (units: seconds)</th>
<th>server.util.processTimeOut (units: milliseconds)</th>
<th>server.agent.maxMemorySize (units: MB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>100/50</td>
<td>748,000 or more (Default value)</td>
<td>600</td>
<td>600,000 (Default value)</td>
<td>64</td>
</tr>
<tr>
<td>100/100</td>
<td>1,420,000 or more</td>
<td>600</td>
<td>600,000</td>
<td>64</td>
</tr>
<tr>
<td>100/256</td>
<td>3,600,000 or more</td>
<td>600</td>
<td>600,000</td>
<td>192</td>
</tr>
</tbody>
</table>
### Table 10-6 Recommended property values for a host that will manage 100 or more LUs (when the host is using a volume manager in HP-UX)

<table>
<thead>
<tr>
<th>Number of LUs and logical volumes managed by Device Manager and recognized by the host</th>
<th>server.http.entity.maxLength (units: bytes)</th>
<th>server.http.server.timeOut (units: seconds)</th>
<th>server.util.processTimeOut (units: milliseconds)</th>
<th>server.agent.maxMemorySize (units: MB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>200/256</td>
<td>7,100,000 or more</td>
<td>600</td>
<td>600,000</td>
<td>512</td>
</tr>
</tbody>
</table>

### Related topics
- [Changing Device Manager server properties on page A-4](#)
- [server.http.entity.maxLength on page A-8](#)
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 10-7 Resident processes of the Device Manager agent (Windows)

<table>
<thead>
<tr>
<th>Process name</th>
<th>Service name</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>hbsa_service.exe</td>
<td>HBsA Service</td>
<td>Device Manager agent service</td>
</tr>
</tbody>
</table>

### Table 10-8 Resident processes of the Device Manager agent (UNIX)

<table>
<thead>
<tr>
<th>Process name</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>hbsa_service</td>
<td>Device Manager agent service</td>
</tr>
</tbody>
</table>

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 `hdvmagts_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.
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.

Information to collect in advance

User name and password of the new user (a member of the Administrators group).

To change the user who executes the service:

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 topics

• Starting and stopping the Device Manager agent service, and checking the operating status of the service (hbsasrv command) on page 10-15

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, and **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.

This command lets you interactively set the items listed in the following table.

| Table 10-9 Items that can be set by using the hdvmagt_setting command

<table>
<thead>
<tr>
<th>Item</th>
<th>Details</th>
</tr>
</thead>
</table>
| 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 to Z a to z 0 to 9 - _ . @  
Port number  
The default port is 2001.  
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 |
Note that any execution time can be specified.
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).

### Information to collect in advance

- IP address or host name of the Device Manager server
- 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.

**Related topics**
- [server.http.port on page A-6](#)
- [server.https.port on page A-7](#)

**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 topics
- server.server.authorization on page D-14
- server.server.serverPort on page D-15

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:

To manage device information:

```
hdutil {-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>
<thead>
<tr>
<th>Sort key</th>
<th>Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>dg</td>
<td>Drive group name</td>
</tr>
<tr>
<td>fs</td>
<td>File system name</td>
</tr>
<tr>
<td>iscsin</td>
<td>iSCSI name for the iSCSI initiator</td>
</tr>
<tr>
<td>ldev</td>
<td>LDEV number</td>
</tr>
<tr>
<td>lun</td>
<td>LU number</td>
</tr>
<tr>
<td>port</td>
<td>Port number</td>
</tr>
<tr>
<td>prod</td>
<td>Product name</td>
</tr>
<tr>
<td>rg</td>
<td>Parity Group number</td>
</tr>
<tr>
<td>rid</td>
<td>Character string representing a storage system model</td>
</tr>
<tr>
<td>ser</td>
<td>Serial number of a storage system</td>
</tr>
</tbody>
</table>
```
<table>
<thead>
<tr>
<th>Sort key</th>
<th>Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>tid</td>
<td>Target ID</td>
</tr>
<tr>
<td>vend</td>
<td>Vendor name</td>
</tr>
<tr>
<td>wwnn</td>
<td>Node WWN name</td>
</tr>
<tr>
<td>wwnp</td>
<td>Port WWN name</td>
</tr>
</tbody>
</table>

- `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 10-11 Information displayed when the hldutil command is executed**

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dg name</td>
<td>Drive group name</td>
</tr>
<tr>
<td>Device</td>
<td>Drive number (for Windows)</td>
</tr>
<tr>
<td></td>
<td>Device special file name (for UNIX)</td>
</tr>
<tr>
<td>fs</td>
<td>File system name</td>
</tr>
<tr>
<td>P/s#1</td>
<td>Identification of the P-VOL or S-VOL</td>
</tr>
<tr>
<td>Vend.</td>
<td>Vendor name</td>
</tr>
<tr>
<td>Prod.</td>
<td>Product name</td>
</tr>
<tr>
<td>Port#</td>
<td>Port number (on the DKC)</td>
</tr>
<tr>
<td>Tid#2</td>
<td>Target ID (SCSI interface on the host)</td>
</tr>
<tr>
<td>Lun#2</td>
<td>LU number (SCSI interface on the host)</td>
</tr>
<tr>
<td>Ldev#</td>
<td>LDEV number (on the DKC)</td>
</tr>
<tr>
<td>Ser#</td>
<td>Serial number of the storage system</td>
</tr>
<tr>
<td>RaidID</td>
<td>Character string indicating the model of the storage system</td>
</tr>
<tr>
<td></td>
<td>For details, see Table 10-12 Correspondence between RaidID values displayed by the hldutil command and storage system models on page 10-29.</td>
</tr>
<tr>
<td>RG#</td>
<td>Parity Group number</td>
</tr>
<tr>
<td>PortWWn#3</td>
<td>Port WWN</td>
</tr>
<tr>
<td>NodeWWn#3</td>
<td>Node WWN</td>
</tr>
<tr>
<td>iSCSIName</td>
<td>iSCSI name for the iSCSI initiator</td>
</tr>
</tbody>
</table>

#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 10-12 Correspondence between RaidID values displayed by the hldutil command and storage system models**

<table>
<thead>
<tr>
<th>RaidID</th>
<th>Storage system model</th>
</tr>
</thead>
<tbody>
<tr>
<td>71</td>
<td>Hitachi WMS 100</td>
</tr>
<tr>
<td>73</td>
<td>Hitachi AMS 200</td>
</tr>
<tr>
<td>75</td>
<td>Hitachi AMS 500</td>
</tr>
<tr>
<td>77</td>
<td>Hitachi AMS 1000</td>
</tr>
<tr>
<td>81</td>
<td>Hitachi SMS 100</td>
</tr>
<tr>
<td>82</td>
<td>Hitachi SMS 110</td>
</tr>
<tr>
<td>83</td>
<td>Hitachi AMS2100</td>
</tr>
<tr>
<td>85</td>
<td>Hitachi AMS2300</td>
</tr>
<tr>
<td>87</td>
<td>Hitachi AMS2500</td>
</tr>
<tr>
<td>91</td>
<td>HUS110</td>
</tr>
<tr>
<td>92</td>
<td>HUS130</td>
</tr>
<tr>
<td>93</td>
<td>HUS150</td>
</tr>
<tr>
<td>HM70</td>
<td>HUS VM</td>
</tr>
<tr>
<td>R500</td>
<td>Hitachi USP 100, Hitachi USP 600 or Hitachi USP 1100</td>
</tr>
<tr>
<td>R501</td>
<td>Hitachi NSC 55</td>
</tr>
<tr>
<td>R600</td>
<td>Universal Storage Platform V</td>
</tr>
<tr>
<td>R601</td>
<td>Universal Storage Platform VM</td>
</tr>
<tr>
<td>R700</td>
<td>Virtual Storage Platform</td>
</tr>
<tr>
<td>R800</td>
<td>VSP G1000</td>
</tr>
</tbody>
</table>

**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 topics
• Managing copy pairs on page 10-7
• Setting the Device Manager server’s information, HiScan command’s execution period, and CCI’s information (hdvmaqt_setting command) on page 10-20
• Editing the configuration definition file on page 10-30

Editing the configuration definition file

Edit the horcmXX.conf file, and then refresh the storage system.

To edit the configuration definition file:

1. Open the horcmXX.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 horcmXX.conf file does not exist, create it.
2. Specify the parameters according to the description conventions.
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.

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.

**Related topics**
- Prerequisite environment for using the configuration definition file on page 10-29
- Notes on using the configuration definition file on page 10-47
- `agent.rm.horcmInstance` on page D-4
- `agent.rm.horcmService` on page D-5
- `server.agent.rm.temporaryInstance` on page D-18
- `server.agent.rm.temporaryPort` on page D-18
- `server.agent.rm.horcmSource` on page D-21

**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 topics

- Description conventions for the configuration definition file on page 10-32
- HORCM_MON parameter description format on page 10-33
- HORCM_CMD parameter description format on page 10-35
- HORCM_VCMD parameter description format on page 10-37
- HORCM_DEV parameter description format on page 10-37
- HORCM_LDEV parameter description format on page 10-40
- HORCM_INST parameter description format on page 10-42
- HORCM_INSTP parameter description format on page 10-44

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 topics**

- Configuration definition file parameters supported Device Manager on page 10-31
- `HORCM_MON` parameter description format on page 10-33
- `HORCM_CMD` parameter description format on page 10-35
- `HORCM_VCMD` parameter description format on page 10-37
- `HORCM_DEV` parameter description format on page 10-37
- `HORCM_LDEV` parameter description format on page 10-40
- `HORCM_INST` parameter description format on page 10-42
- `HORCM_INSTP` parameter description format on page 10-44

**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`. Note that if you use Replication Manager to generate a configuration definition file, this item will always be specified for the host name (Replication Manager uses a Device Manager agent to view the configuration definition file).
  
  - 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>
<thead>
<tr>
<th>Value</th>
<th>Device Manager agent version</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>5.9 or later</td>
</tr>
<tr>
<td>IP address</td>
<td>Yes</td>
</tr>
<tr>
<td>Host name</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Using the Device Manager agent

Hitachi Command Suite Administrator Guide

10-33
<table>
<thead>
<tr>
<th>Value</th>
<th>Device Manager agent version</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>5.9 or later</td>
</tr>
<tr>
<td>NONE</td>
<td>Yes#</td>
</tr>
<tr>
<td>&quot;<strong>NONE</strong>&quot;</td>
<td>No</td>
</tr>
<tr>
<td>NONE6</td>
<td>Yes#</td>
</tr>
<tr>
<td>&quot;<strong>NONE6</strong>&quot;</td>
<td>No</td>
</tr>
<tr>
<td>Loopback IP addresses (127.0.0.1 to 127.255.255.254)</td>
<td>Yes#</td>
</tr>
<tr>
<td>Loopback host name (localhost)</td>
<td>Yes#</td>
</tr>
<tr>
<td>Cluster virtual IP address</td>
<td>No</td>
</tr>
<tr>
<td>Cluster virtual machine name</td>
<td>No</td>
</tr>
</tbody>
</table>

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 10-14 Support status of HORCM_MON parameter description format

<table>
<thead>
<tr>
<th>Version</th>
<th>Item</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>ip_address</td>
</tr>
<tr>
<td>6.1 or later</td>
<td>Yes</td>
</tr>
<tr>
<td>5.9 to 6.0</td>
<td>Yes</td>
</tr>
<tr>
<td>Version</td>
<td>Item</td>
</tr>
<tr>
<td>----------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>ip_address</td>
</tr>
<tr>
<td>5.8</td>
<td>Supports IP address, host name, and NONE.</td>
</tr>
<tr>
<td>Earlier than 5.7</td>
<td>Supports IP address and host name.</td>
</tr>
</tbody>
</table>

Legend:
Yes: Supports all description formats.

Related topics
- [Editing the configuration definition file on page 10-30](#)
- [Description conventions for the configuration definition file on page 10-32](#)
- [HORCM_INST parameter description format on page 10-42](#)
- [HORCM_INSTP parameter description format on page 10-44](#)
- [Notes on using the configuration definition file on page 10-47](#)

**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**
  ```plaintext
  \\
  IPCMD-IP-address-of-the-virtual-command-device-port-number[[-unit-ID-of-the-storage-system]
  ```

  **PhysicalDrive format**
  ```plaintext
  \\
  PhysicalDrive-disc-number-defined-by-Windows
  ```
  For the Device Manager agent 4.3 or earlier, this item is case sensitive.

  **GUID format**
  ```plaintext
  \\
  Volume{GUID}
  ```

  **CMD format**
  ```plaintext
  \\
  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 10-15 Support status of HORCM_CMD parameter description format**

<table>
<thead>
<tr>
<th>Version</th>
<th>Item</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>dev_name</td>
</tr>
<tr>
<td>7.4.1 or later</td>
<td>Windows Yes</td>
</tr>
<tr>
<td></td>
<td>UNIX Yes</td>
</tr>
<tr>
<td>7.1 to 7.4.0</td>
<td>Windows Yes</td>
</tr>
<tr>
<td></td>
<td>UNIX Only supports specification using a special file or specification using IPCMD format.</td>
</tr>
<tr>
<td>05-10 to 7.0</td>
<td>Windows Supports description formats other than IPCMD format.</td>
</tr>
<tr>
<td></td>
<td>UNIX Only supports specification using a special file.</td>
</tr>
<tr>
<td>05-00</td>
<td>Windows Supports description formats other than IPCMD and CMD format.</td>
</tr>
<tr>
<td></td>
<td>UNIX Only supports specification using a special file.</td>
</tr>
<tr>
<td>Earlier than 04-30</td>
<td>Windows Supports description formats other than IPCMD, CMD and GUID formats.</td>
</tr>
<tr>
<td></td>
<td>UNIX Only supports specification using a special file.</td>
</tr>
</tbody>
</table>

Legend:
Yes: Supports all description formats.

Related topics
- Editing the configuration definition file on page 10-30
- Description conventions for the configuration definition file on page 10-32
- Notes on using the configuration definition file on page 10-47

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 10-16 Support status of HORCM_VCMD parameter description format

<table>
<thead>
<tr>
<th>Version</th>
<th>Item</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Serial#</td>
</tr>
<tr>
<td>8.0.1 or later</td>
<td>Yes #1</td>
</tr>
<tr>
<td>8.0</td>
<td>Yes #2</td>
</tr>
<tr>
<td>Earlier than 7.6.1</td>
<td>No</td>
</tr>
</tbody>
</table>

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 topics:
- Editing the configuration definition file on page 10-30
- Description conventions for the configuration definition file on page 10-32
- Notes on using the configuration definition file on page 10-47

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 10-17 Support status of HORCM_DEV parameter description format

<table>
<thead>
<tr>
<th>Version</th>
<th>dev_group</th>
<th>dev_name</th>
<th>port#</th>
<th>targetID</th>
<th>LU#</th>
<th>MU#</th>
</tr>
</thead>
<tbody>
<tr>
<td>04-00 or later</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Earlier than 03-50</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Supports specification using mirror descriptors, omissions (blank), and numeric values.</td>
</tr>
</tbody>
</table>

Using the Device Manager agent
Hitachi Command Suite Administrator Guide
10-39
Legend:
Yes: Supports all description formats.

Related topics
- Editing the configuration definition file on page 10-30
- Description conventions for the configuration definition file on page 10-32
- Notes on using the configuration definition file on page 10-47

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 10-18 Support status of HORCM_LDEV parameter description format

<table>
<thead>
<tr>
<th>Version</th>
<th>dev_group</th>
<th>dev_name</th>
<th>Serial#</th>
<th>CU:LDEV(LDEV#)</th>
<th>MU#</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.2 or later</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Version</td>
<td>Item</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---------------</td>
<td>----------------------------------------------------------------------</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>dev_group</td>
<td>dev_name</td>
<td>Serial#</td>
<td>CU:LDEV(LDEV#)</td>
<td>MU#</td>
</tr>
<tr>
<td>6.1 to 05-60</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Supports description formats other than the serial-number:journal-ID format.</td>
<td>Yes</td>
</tr>
<tr>
<td>Earlier than 05-50</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

Legend:
Yes: Supports all description formats.
No: Does not support any description formats.

Related topics
- Editing the configuration definition file on page 10-30
- Description conventions for the configuration definition file on page 10-32
- Notes on using the configuration definition file on page 10-47

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), the host name, `NONE`, or `NONE6`. If you specify `NONE` or `NONE6`, the local host is assumed. If you use Replication Manager to add a new group to the existing configuration definition file, this item will always be specified using 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 10-19 Values that can be specified for the ip_address of HORCM_INST parameter**

<table>
<thead>
<tr>
<th>Value</th>
<th>Device Manager agent version</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>05-80 or later</td>
</tr>
<tr>
<td>IP address</td>
<td>Yes</td>
</tr>
<tr>
<td>Host name</td>
<td>Yes</td>
</tr>
<tr>
<td>Loopback IP addresses (127.0.0.1 to 127.255.255.254)</td>
<td>Yes#</td>
</tr>
<tr>
<td>Loopback host name (localhost)</td>
<td>Yes#</td>
</tr>
<tr>
<td>Cluster virtual IP address</td>
<td>No</td>
</tr>
<tr>
<td>Cluster virtual machine name</td>
<td>No</td>
</tr>
</tbody>
</table>

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 10-20 Support status of HORCM_INST parameter description format**

<table>
<thead>
<tr>
<th>Version</th>
<th>Item</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>dev_group</td>
</tr>
<tr>
<td>7.0 or later</td>
<td>Yes</td>
</tr>
<tr>
<td>6.1 to 6.4</td>
<td>Yes</td>
</tr>
<tr>
<td>Earlier than 6.0</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Legend:
Yes: Supports all description formats.
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, the host name, `NONE`, or `NONE6`. If you specify `NONE` or `NONE6`, the local host is assumed. If you use Replication Manager to add a new group to the existing configuration definition file, this item will always be specified using 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>
<thead>
<tr>
<th>Value</th>
<th>Device Manager agent version</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address</td>
<td>Yes</td>
</tr>
<tr>
<td>Host name</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Table 10-21 Values that can be specified for the ip_address of HORCM_INSTP parameter**

Use the HORCM_INSTP parameter to specify the machine information and path group ID of the remote host.
<table>
<thead>
<tr>
<th>Value</th>
<th>Device Manager agent version</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>7.6.0 or later</td>
</tr>
<tr>
<td>Loopback IP addresses (127.0.0.1 to 127.255.255.254)</td>
<td>Yes#</td>
</tr>
<tr>
<td>Loopback host name (localhost)</td>
<td>Yes#</td>
</tr>
<tr>
<td>Cluster virtual IP address</td>
<td>No</td>
</tr>
<tr>
<td>Cluster virtual machine name</td>
<td>No</td>
</tr>
</tbody>
</table>

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 10-22 Support status of HORCM_INSTP parameter description format**

<table>
<thead>
<tr>
<th>Version</th>
<th>Item</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>All parameters</td>
</tr>
<tr>
<td>7.6.0 or later</td>
<td>Yes</td>
</tr>
<tr>
<td>6.2 to 7.5.0</td>
<td>Yes#</td>
</tr>
<tr>
<td>Earlier than 6.1</td>
<td>No</td>
</tr>
</tbody>
</table>

Legend:
Yes: Supports all description formats.
Sometimes: The `HORCM_INSTP` parameter is ignored during copy pair creation or manipulation. During copy pair deletion, if the `HORCM_INSTP` parameter is used.
definition includes a group that has the same name as the copy pair group to be deleted, that group is deleted from the definition.
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 topics
- Editing the configuration definition file on page 10-30
- Description conventions for the configuration definition file on page 10-32
- HORCM_MON parameter description format on page 10-33
- HORCM_DEV parameter description format on page 10-37
- HORCM_LDEV parameter description format on page 10-40
- Notes on using the configuration definition file on page 10-47

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.

Operations to complete in advance
Log in as a user with Administrator permissions (for Windows) or as a root user (for UNIX).

To change the storage location of the configuration definition file:
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.
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 topics
- Starting and stopping the Device Manager agent service, and checking the operating status of the service (hbsasrv command) on page 10-15
- server.agent.rm.horcmSource on page D-21
- To stop an HORCM instance: See the CCI manual.
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 horcmXX.conf is backed up as horcmXX.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 topics

- Editing the configuration definition file on page 10-30
- server.agent.rm.optimization.userHorcmFile on page D-17
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 xxvi.

- 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 topics:**

- [Unlocking accounts on page 3-6](#)

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.

**Related topics:**

- How to change the area of the desktop heap: 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 topics:

- Changing Device Manager server properties on page A-4
- dbm.startingCheck.retryCount on page A-17
- dbm.startingCheck.retryPeriod on page A-17

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 topics:

- [Starting the Hitachi Command Suite services on page 8-4](#)
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 forcестop
   In Linux:
   \installation-directory-for-Hitachi-Command-Suite/TieredStorageManager/bin/htsmserver forcестop

   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 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:

a. 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.

b. 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.

c. 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 topics:

- Starting the Hitachi Command Suite services on page 8-4
- Stopping the Hitachi Command Suite services on page 8-5

**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 topics:**
- Restoring databases on page 9-6

## 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 topics:**
- Settings required for a host to manage 100 or more LUs on page 10-10
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 topics:

- Deleting the Device Manager agent's registry entries and files (hbsa_util command) on page 10-19

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 topics:

- Deleting the Device Manager agent's registry entries and files (hbsa_util command) on page 10-19

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
<title>400 Bad request</title>
<meta http-equiv="Content-Type" content="text/html; charset=ISO-8859-1">
<h1>400 Bad request</h1>
<p><strong>ServiceConnection#0: java.lang.OutOfMemoryError</strong></p>
</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 topics:

- Changing the memory heap size on page 1-9
- Settings required for a host to manage 100 or more LUs on page 10-10
- Setting the Device Manager server's information, HiScan command's execution period, and CCI's information (hdvmagt_setting command) on page 10-20
- Reporting host information to the Device Manager server manually (HiScan command) on page 10-22

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 topics:**

- [Reporting host information to the Device Manager server manually (HiScan command) on page 10-22](#)
- [Acquiring device information (hldutil command) on page 10-24](#)

**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\Harddisknn\DRn` 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 HBase 64 Storage Mgmt Common Service and 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.

Related topics

- 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 11-1 Values specified for the type option when collecting maintenance information**

<table>
<thead>
<tr>
<th>Product</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Manager</td>
<td>DeviceManager</td>
</tr>
<tr>
<td>Tiered Storage Manager</td>
<td>TieredStorageManager</td>
</tr>
<tr>
<td>Replication Manager</td>
<td>ReplicationManager</td>
</tr>
<tr>
<td>Other products</td>
<td>Refer to the manual for each product.</td>
</tr>
</tbody>
</table>

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.
To collect Tiered Storage Manager CLI log files:

1. 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 11-2 Properties set in the HtsmgetTI.properties file

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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:**
   
   `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\hdcd_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\hcResult

In Linux:
  directory-specified-for-the-o-option/hcResult

### 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\hc_target_getras.bat
  ```

  In UNIX:
  ```
  installation-directory-for-Host-Data-Collector/Base/bin/hc_target_getras.sh
  ```

- **Log in as a user with Administrator permissions (for Windows) or as a root user (for UNIX)**

#### Command format

In Windows:
```
hc_target_getras.bat -o folder-name [-f]
```

In UNIX:
```
hc_target_getras.sh -o directory-name [-f]
```
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.

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 HBase 64 Storage Mgmt Common Service (Windows)

To acquire a thread dump of HBase 64 Storage Mgmt Common Service, create a file called dump, and then restart HBase 64 Storage Mgmt Common Service.
To acquire a thread dump of HBase 64 Storage Mgmt Common Service:

1. In `installation-folder-for-Hitachi-Command-Suite\Base64\uCPSB\CC\web\containers\HiCommand64`, create a file called `dump`.
2. Access the Windows Services window.
3. Stop the HBase 64 Storage Mgmt Common Service.
4. From the Services window, start the HBase 64 Storage Mgmt Common Service.

The `javacorexxx.xxxx.txt` file is output when using JDK bundled with Hitachi Command Suite, or the `HiCommand64.log` file is output when using Oracle JDK, to the following folder:

`installation-folder-for-Hitachi-Command-Suite\Base64\uCPSB\CC\web\containers\HiCommand64`

If you are using the Oracle JDK, the `HiCommand64.log` file is overwritten each time it is output. We recommend saving the file by using a different name after the file is output.

---

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.

To acquire a thread dump of HCS Device Manager Web Service:

1. In `installation-folder-for-Hitachi-Command-Suite\Base64\uCPSB\CC\web\containers\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.

The `javacorexxx.xxxx.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\web\containers\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 HBase 64 Storage Mgmt Common Service (Linux)

To acquire a thread dump of HBase 64 Storage Mgmt Common Service, execute the `kill` command, and then restart the Hitachi Command Suite product services.

To acquire a thread dump of HBase 64 Storage Mgmt Common Service:

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/web/containers/
   HiCommand64/logs/cjstdout.log file.
   Multiple process IDs are written to the cjstdout.log file. Specify the last
   process ID written to the file.
   ```

2. Restart the Hitachi Command Suite product services.

The `javacorexxx.xxx.txt` file is output when using JDK bundled with Hitachi Command Suite, or the `HiCommand64.log` file is output when using Oracle JDK, to the following directory:

```
installation-directory-for-Hitachi-Command-Suite/Base64/
uCPSB/CC/web/containers/HiCommand64
```

If you are using the Oracle JDK, the `HiCommand64.log` file is overwritten each time it is output. We recommend saving the file by using a different name after the file is output.

Related topics

- [Starting the Hitachi Command Suite services on page 8-4](#)
- [Stopping the Hitachi Command Suite services on page 8-5](#)

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.

To acquire a thread dump of HCS Device Manager Web Service:

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/web/containers/
   DeviceManagerWebService/logs/cjstdout.log file.
   Multiple process IDs are written to the cjstdout.log file. Specify the last
   process ID written to the file.
   ```
2. Restart the Hitachi Command Suite product services.

The javacorexxx.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/web/containers/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 topics

- Starting the Hitachi Command Suite services on page 8-4
- Stopping the Hitachi Command Suite services on page 8-5
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 Universal Replicator performance analysis (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 A-1 Property files of a Device Manager server

<table>
<thead>
<tr>
<th>Property file</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>server.properties file</td>
<td>This property file contains the Device Manager server configuration information.</td>
</tr>
<tr>
<td></td>
<td><strong>Warning:</strong> 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.</td>
</tr>
<tr>
<td>database.properties file</td>
<td>This property file is related to the Device Manager database.</td>
</tr>
<tr>
<td></td>
<td><strong>Warning:</strong> 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.</td>
</tr>
<tr>
<td>logger.properties file</td>
<td>This property file is related to the Device Manager log output.</td>
</tr>
<tr>
<td>dispatcher.properties file</td>
<td>This property file is related to Device Manager threads.</td>
</tr>
<tr>
<td>mime.properties file</td>
<td>This property file is related to MIME (Multipurpose Internet Mail Extensions) types for Device Manager.</td>
</tr>
<tr>
<td>client.properties file</td>
<td>This property file is related to the Device Manager GUI.</td>
</tr>
<tr>
<td>• server.properties file</td>
<td>This property file is related to Device Manager security.</td>
</tr>
<tr>
<td>• cimxmlscpa.properties file</td>
<td></td>
</tr>
<tr>
<td>customizedsnmptrap.properties file</td>
<td>This property file is related to the log output of the SNMP traps received by Device Manager.</td>
</tr>
<tr>
<td>launchapp.properties file</td>
<td>This property file is related to the applications that can be launched from Device Manager.</td>
</tr>
<tr>
<td>host.properties file</td>
<td>This property file is related to communicating with hosts.</td>
</tr>
<tr>
<td>hostdatacollectors.properties file</td>
<td>This property file is related to the connection to Host Data Collector.</td>
</tr>
<tr>
<td>migration.properties file</td>
<td>This property file is related to migrations.</td>
</tr>
<tr>
<td>tuningmanager.properties file</td>
<td>This property file is related to the connection to Tuning Manager.</td>
</tr>
</tbody>
</table>
### Property file Description

<table>
<thead>
<tr>
<th>Property file</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>replication.properties</td>
<td>This property file is related to Universal Replicator performance analysis.</td>
</tr>
<tr>
<td>rpmlib.properties</td>
<td>This property file is related to the connection to Replication Manager.</td>
</tr>
<tr>
<td>jserver.properties</td>
<td>This property file is related to the CIM/WBEM functions.</td>
</tr>
<tr>
<td>cimxmlcpa.properties</td>
<td></td>
</tr>
<tr>
<td>cimxmlscpa.properties</td>
<td></td>
</tr>
</tbody>
</table>

#### 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.

#### Operations to complete in advance

Log in as a user with Administrator permissions (for Windows) or as a root user (for Linux).

#### To change the Device Manager server properties:

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 topics

- [Starting the Hitachi Command Suite services on page 8-4](#)
- [Stopping the Hitachi Command Suite services on page 8-5](#)

### 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.
- If user accounts are authenticated in Hitachi Command Suite when logging in to CCI or the SVP and the value of this property has been changed, reconfigure user account authentication in the Edit Storage Systems window in the Device Manager GUI.

### 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
The HiCommandCLI.serverurl property of the HiCommandCLI.properties file in the Device Manager CLI (for non-SSL communication with the Device Manager server)

Related topics

- Changing pop-up blocker settings on page 4-67
- Enabling SSL/TLS for the Device Manager CLI computer on page 4-68
- Changing the communication protocol between the Replication Manager server and the Device Manager server on page 4-75
- Setting the Device Manager server’s information, HiScan command’s execution period, and CCI’s information (hdvmagt_setting command) on page 10-20
- Changing Tiered Storage Manager server properties on page B-2
- hdvm.port on page B-9
- Changing the port number in the file server management software: See the file server manuals.

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 addition, if user accounts are authenticated in Hitachi Command Suite when logging in to CCI or the SVP and the value of this property has been changed, reconfigure user account authentication in the Edit Storage Systems window in the Device Manager GUI.
Related topics

- Changing pop-up blocker settings on page 4-67
- Enabling SSL/TLS for the Device Manager CLI computer on page 4-68
- Changing the communication protocol between the Replication Manager server and the Device Manager server on page 4-75

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 topics

- `client.rmi.port` on page A-29
- `hdvm.rmi.port` on page B-9

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: 1310720

**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.
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. If you edit the configuration definition file in Replication Manager, the host name is always used.

Related topics
- Notes on managing copy pairs on page 1-60

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.
If you want to execute CIM, you must set this property to \textit{true}.

\textbf{Default: true}

\textbf{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 \textit{true}, the method is executed asynchronously. If you set this property to \textit{false}, the method is executed synchronously. If the CIM client does not support the job control subprofile, specify \textit{false}.

If you specify any values other than \textit{true} or \textit{false}, or if this property does not exist, the method is executed asynchronously.

\textbf{Default: true}

\textbf{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.

\textbf{Default: 3}

\textbf{Related topics}

- \texttt{server.cim.http.port on page A-10}
- \texttt{server.cim.https.port on page A-11}

\textbf{server.cim.http.port}

Specify the port for non-SSL transmission for the CIM function.

\textbf{Default: 5988}

\textbf{Caution:} If you change the value of this property, also change the \texttt{HTTPPort} property of the Device Manager server to the same value.
**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 topics**

- [server.cim.support.protocol on page A-10](#)
- [HTTPPort on page A-52](#)

**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, or Hitachi USP, 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`, storage system information in the database is not automatically refreshed.

Default: `true`

---

**Related topics**

- [server.dispatcher.snm2.configchange.pollingPeriod on page A-21](#)
- [server.dispatcher.configchange.pollingPeriod on page A-22](#)
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 storage system alerts, events, and health check results to users by email.

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 topics

• server.mail.smtp.host on page A-13

server.mail.enabled.fileserver

Specify whether to send Hitachi NAS Platform 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 Hitachi NAS Platform, 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 topics

• server.mail.smtp.host on page A-13
**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 topics**

- [server.mail.enabled.storagesystem on page A-12](#)

**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 topics

• server.mail.from on page A-13

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**

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, Virtual Storage Platform, Universal Storage Platform V/VM, Hitachi USP 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, 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, 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:
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\`

Device Manager server properties

Hitachi Command Suite Administrator Guide
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 topics**

- `logger.MaxFileSize` on page A-18

**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 \texttt{HDvMtrace\textsubscript{n}.log}, \texttt{HDvM GuiTrace\textsubscript{n}.log}, and \texttt{HDvM GuiMessage\textsubscript{n}.log}, where \texttt{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 \texttt{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 \texttt{HDvMtrace\textsubscript{n}.log}, \texttt{HDvM GuiTrace\textsubscript{n}.log}, and \texttt{HDvM GuiMessage\textsubscript{n}.log} (the \texttt{n} in the file name indicates the backup generation number of the file).

When a log file reaches the size specified in the \texttt{logger.hicommandbase.MaxFileSize} property, a new log file is created with a counter added to the file name, for example \texttt{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 topics**

- [logger.hicommandbase.MaxFileSize on page A-20](#)
**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 HDvMtrace\(n\).log, HDvMGuiTracen.log, and HDvMGuiMessage\(n\).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)
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 topics
• server.configchange.enabled on page A-11

server.dispatcher.daemon.configUpdate.detection.interval

Specify the interval (in minutes) at which the Device Manager server checks whether the configuration of VSP G1000, 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, 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, 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
  - 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.
  - 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, 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 topics
• server.dispatcher.daemon.autoSynchro.doRefresh on page A-23
• server.dispatcher.daemon.autoSynchro.type on page A-24
• server.dispatcher.daemon.configUpdate.detection.variable.enabled on page A-25

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, 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, 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, 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, Virtual Storage Platform, Universal Storage Platform V/VM, or HUS VM is not updated in the database.

Related topics
- server.dispatcher.daemon.autoSynchro.type on page A-24

**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 topics
- server.dispatcher.daemon.autoSynchro.doRefresh on page A-23
- server.dispatcher.daemon.autoSynchro.dayOfWeek on page A-24
- server.dispatcher.daemon.autoSynchro.startTime on page A-25
- server.dispatcher.daemon.autoSynchro.interval on page A-25

**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.
Related topics

• server.dispatcher.daemon.autoSynchro.type on page A-24

server.dispatcher.daemon.autoSynchro.startTime

Specify the time at which storage system information is automatically refreshed (updated) in the database starts in the format \texttt{hh:mm}.

Specify a value from 00 to 23 for \texttt{hh}, and 00 to 59 for \texttt{mm}. This property is enabled only if the \texttt{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 topics

• server.dispatcher.daemon.autoSynchro.type on page A-24

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 \texttt{server.dispatcher.daemon.autoSynchro.type} property is set to H.

Default: 24 (hours)

Related topics

• server.dispatcher.daemon.autoSynchro.type on page A-24

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, Virtual Storage Platform or HUS VM has been changed.

If \texttt{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 \texttt{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 topics**

- server.dispatcher.daemon.configUpdate.detection.interval on page A-22

**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 topics**
- server.dispatcher.daemon.autoSynchro.performance.startTime on page A-27
- htnm.infoAcquirePeriod on page A-43

**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 topics**
- server.dispatcher.daemon.autoSynchro.performance.doRefresh on page A-26

**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 topics**

- [htnm.infoAcquirePeriod on page A-43](#)

**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 topics**

- [server.rmi.port on page A-8](#)

**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 topics

- Registering IP addresses in the environment definition file user_httpsd.conf of Common Component: Controlling management client access to the management server on page 4-122

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 topics
- Registering IP addresses in the environment definition file user_httpsd.conf of Common Component: Controlling management client access to the management server on page 4-122

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.

The keystore file shipped with a Device Manager server is an empty placeholder file that does not contain the required keypair and associated server certificate needed to run the Device Manager server in secure mode. If you attempt to start the server in secure mode with an empty keystore file, the server will log a fatal error and terminate abnormally. A keypair and associated self-signed or trusted certificate must first be installed into the keystore before encrypted communications can be started.

Default: keystore

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

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 by using commas (,) to separate them.

- 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
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) by using commas (,) to separate them.

The cipher suites used by default are as follows:

- 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 topics**
- [server.dispatcher.daemon.receiveTrap on page A-21](#)

**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:

```plaintext
customizedsnmptrap.customizelist = \
enterprise-ID-1:generic-trap-number-1:specific-trap-number-1:severity-1:content-to-be-output-1, \
\...\enterprise-ID-n:generic-trap-number-n:specific-trap-number-n:severity-n:content-to-be-output-n
```

**Table A-2 Items specified in the customizedsnmptrap.customizelist property**

<table>
<thead>
<tr>
<th>Item</th>
<th>Format</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>enterprise-ID</code></td>
<td>Specify by using dots (for example, .1.3.6.1.4.116.3.11.1.2)</td>
<td>Required</td>
</tr>
<tr>
<td><code>generic-trap-number</code></td>
<td>Numeric value, from 0 to 6</td>
<td>Required</td>
</tr>
<tr>
<td><code>specific-trap-number</code></td>
<td>Numeric value</td>
<td>Required</td>
</tr>
<tr>
<td><code>severity</code></td>
<td>Specify the severity of each trap by using one of the character strings below. You cannot use character strings other than the following:</td>
<td>This item is optional. If you omit this item, <code>null</code> is assumed. The severity indicators in the message IDs are output as follows:</td>
</tr>
<tr>
<td></td>
<td>Information</td>
<td>-I for Information</td>
</tr>
<tr>
<td></td>
<td>Warning</td>
<td>-W for Warning</td>
</tr>
<tr>
<td></td>
<td>Error</td>
<td>-E for Error, Critical, and Alert</td>
</tr>
<tr>
<td></td>
<td>Critical</td>
<td>No log data is output for <code>Null</code></td>
</tr>
<tr>
<td></td>
<td>Alert</td>
<td>Special: <code>$a$e$g$s</code> is output.</td>
</tr>
<tr>
<td></td>
<td>Null</td>
<td>Optional. If you omit this item, the <code>$a$e$g$s$</code> content is output.</td>
</tr>
</tbody>
</table>

---

**A-34**

Device Manager server properties

Hitachi Command Suite Administrator Guide
<table>
<thead>
<tr>
<th>Item</th>
<th>Format</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>below. You cannot use character strings other than the following:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• $a</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• $e</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• $g</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• $s</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• $n (where n indicates an integer, which is 1 or larger)</td>
<td></td>
</tr>
</tbody>
</table>

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 $nth 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 = \n\.1.2.3:6:1:Information:$a$e$g$s$1$2, \n\.1.3.6.1.4.1.2854:6:1:Warning:$e$a$s$3$2$1$g, \n\.1.3.6.1.4.1.116.3.11.4.1.1:6:1:Error:$a$s, \n\.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 topics**

- [customizedsnmptrap.customizedSNMPTrapEnable on page A-33](#)

**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:

```
```

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
Related topics

- Checking and modifying the communication port number set by Storage Navigator Modular 2: See the documentation for Storage Navigator Modular 2.

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 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:

\[
\text{IP-address-or-host-name:}[\text{port-number}], \text{IP-address-or-host-name:}\
\text{[port-number]}, ...\
\]

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 topics**

- [hdc.rmiserver on page A-39](#)
- [hdc.classloader on page A-40](#)
- [hdc.usessl on page A-41](#)
- [hdc.common.rmi.registryPort on page C-3](#)
- [hdc.common.rmi.ssl.registryPort on page C-5](#)
- [hdc.service.rmi.registryIPAddress on page C-6](#)

---

**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 topics
- hdc.rmiregistry on page A-39
- hdc.classloader on page A-40
- hdc.usessl on page A-41
- hdc.common.rmi.serverPort on page C-4
- hdc.common.rmi.ssl.serverPort on page C-5
- hdc.service.rmi.registryIPAddress on page C-6

**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 topics**
- `hdc.rmiregistry` on page A-39
- `hdc.rmiserver` on page A-39
- `hdc.usessl` on page A-41
- `hdc.common.http.serverPort` on page C-4
- `hdc.common.https.serverPort` on page C-6
- `hdc.service.rmi.registryIPAddress` on page C-6

**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:
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 \(value\text{-specified-in-htnm.servers-property} - 1\).

- 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 topics**

- htnm.server.\_n.protocol on page A-45

**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.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 Universal Replicator performance analysis (replication.properties file)**

The `replication.properties` file contains properties related to Universal Replicator performance analysis.

- 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 *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 topics
• server.dispatcher.daemon.replication.config.updateInterval on page A-47
• server.dispatcher.daemon.replication.config.offset on page A-47
• server.dispatcher.daemon.replication.config.minute on page A-48

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 topics
• server.dispatcher.daemon.replication.config.doUpdate on page A-46

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 topics**

- `server.dispatcher.daemon.replication.config.doUpdate` on page A-46
- `server.dispatcher.daemon.replication.config.updateInterval` on page A-47

**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 topics**

- `server.dispatcher.daemon.replication.config.doUpdate` on page A-46

**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 topics**

- server.dispatcher.daemon.replication.performance.tnm.updateInterval on page A-49

**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.

Default: 25200

**Related topics**

- For details about the `base.rmi.port` property in the Replication Manager server's `base.properties` file, see the *Replication Manager Configuration Guide*.

**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 topics**
- `server.cim.http.port` on page A-10

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 topics**
- `server.cim.https.port` on page A-11
- `Ciphers` on page A-33
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>
<thead>
<tr>
<th>Property file</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>server.properties file</td>
<td>This property file is related to the Tiered Storage Manager server operations.</td>
</tr>
<tr>
<td>database.properties file</td>
<td>This property file is related to the Tiered Storage Manager database.</td>
</tr>
<tr>
<td>devicemanager.properties file</td>
<td>This property file is related to access from Tiered Storage Manager to the Device Manager server.</td>
</tr>
<tr>
<td>logger.properties file</td>
<td>This property file is related to Tiered Storage Manager log output.</td>
</tr>
<tr>
<td>server.properties file</td>
<td>This property file is related to Tiered Storage Manager security.</td>
</tr>
</tbody>
</table>

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.

Operations to complete in advance

Log in as a user with Administrator permissions (for Windows) or as a root user (for Linux).

To change Tiered Storage Manager server properties:

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.
Tip: 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
```

Related topics

- [Starting the Hitachi Command Suite services on page 8-4](#)
- [Stopping the Hitachi Command Suite services on page 8-5](#)

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 `htsmsserver.location` property in the `htsmcli.properties` file of the Tiered Storage Manager CLI.

**Related topics**

- [Enabling SSL/TLS for the Tiered Storage Manager CLI computer on page 4-70](#)
- [server.rmi.secure on page B-15](#)

**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 `htsmsserver.location` property in the `htsmcli.properties` file of the Tiered Storage Manager CLI.

**Related topics**

- [Enabling SSL/TLS for the Tiered Storage Manager CLI computer on page 4-70](#)
- [server.rmi.secure on page B-15](#)
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: `htsmsserver`

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 topics

- [server.mail.from on page B-5](#)
**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 topics**

- server.http.port on page A-6

**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 topics**

- [server.rmi.port](#) on page A-8

## 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 B-1 Relationship between the threshold value of the output levels and the output messages](image)

### logger.messagelogLevel

Specify an output level for the log data that is output to the `HTSMServerMessage.log` file and the `HTSMGuiMessage.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 B-2 Output level of message log data**

<table>
<thead>
<tr>
<th>Type of message</th>
<th>Output level</th>
<th>Message descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Error</td>
<td>0</td>
<td>An error occurred that affects the operation of the management server or Java servlet.</td>
</tr>
<tr>
<td></td>
<td>10</td>
<td>An execution error occurred due to a reason such as an operational mistake.</td>
</tr>
<tr>
<td>Warning</td>
<td>20</td>
<td>An error occurred, but execution can continue with limitations.</td>
</tr>
<tr>
<td>Information</td>
<td>0</td>
<td>Information has been produced about the actions of the management server and the GUI.</td>
</tr>
<tr>
<td></td>
<td>20</td>
<td>Information has been produced about the processing for an operation.</td>
</tr>
</tbody>
</table>

*logger.traceLogLevel*

Specify an output level for the log data that is output to the `HTSMServerTrace.log` file and the `HTSMGuiTrace.log` file.

This property applies to the Tiered Storage Manager server trace log (`HTSMServerTrace.log`) and the GUI trace log (`HTSMGuiTrace.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 B-3 Output level of trace log data**

<table>
<thead>
<tr>
<th>Type of message</th>
<th>Output level</th>
<th>Message descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Error</td>
<td>0</td>
<td>An error occurred that affects the operation of the management server or Java servlet.</td>
</tr>
<tr>
<td></td>
<td>10</td>
<td>An execution error occurred due to a reason such as an operational mistake.</td>
</tr>
<tr>
<td>Warning</td>
<td>20</td>
<td>An error occurred, but execution can continue with limitations.</td>
</tr>
<tr>
<td>Information</td>
<td>0</td>
<td>Information has been produced about the actions of the management server and management client.</td>
</tr>
<tr>
<td>Type of message</td>
<td>Output level</td>
<td>Message descriptions</td>
</tr>
<tr>
<td>-----------------</td>
<td>--------------</td>
<td>----------------------</td>
</tr>
<tr>
<td></td>
<td>10</td>
<td>Information has been produced about exchanges with other programs or machines.</td>
</tr>
<tr>
<td></td>
<td>20</td>
<td>Information has been produced about the starting/ stopping of a major method, or the creation/deletion of a major object.</td>
</tr>
<tr>
<td></td>
<td>30</td>
<td>Detailed information has been produced.</td>
</tr>
</tbody>
</table>

**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 topics**

- [logger.serverMessageMaxFileSize on page B-14](#)

**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 topics**
- [logger.serverTraceMaxFileSize on page B-14](#)

**logger/guiMessageFileCount**

Specify the maximum number of backups of the `HTSMGuiMessagesn.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 topics**
- [logger/guiMessageMaxFileSize on page B-14](#)

**logger/guiTraceFileCount**

Specify the maximum number of backups of the `HTSMGuiTracen.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 topics**

- [logger.guiTraceMaxFileSize on page B-14](#)

**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 `HTSMServerTrace.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: 5,242,880 (5 MB)

**logger guiMessageMaxFileSize**

Specify the maximum size of the `HTSMGuiMessage.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 guiTraceMaxFileSize**

Specify the maximum size of the `HTSMGuiTrace.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: 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 topics

- [server.rmi.security.enabledCipherSuites on page B-15](#)

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 by using commas (,) to separate them.

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 topics**
- [server.rmi.secure on page B-15](#)
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>
<thead>
<tr>
<th>Property file</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>hdcbase.properties file</td>
<td>This property file is related to Host Data Collector operation.</td>
</tr>
<tr>
<td>logger.properties file</td>
<td>This property file is related to log output by Host Data Collector.</td>
</tr>
<tr>
<td>javaconfig.properties file</td>
<td>This property file is related to a Java environment for Host Data Collector.</td>
</tr>
<tr>
<td>hdcbase.properties file</td>
<td>This property file is related to Host Data Collector security.</td>
</tr>
</tbody>
</table>

Changing Host Data Collector properties

Use a text editor to edit the property files of Host Data Collector.

Operations to complete in advance

Log in as a user with Administrator permissions (for Windows) or as a root user (for Linux).

To change the Host Data Collector properties:

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 topics

- Starting the Host Data Collector service on page 8-9
- Stopping the Host Data Collector service on page 8-9

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 topics**

- [hdc.adapter.adapterProcessNum on page C-3](#)

**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 topics

- [Registering an exception for the Host Data Collector service (for non-SSL communication)](page 2-30)
- `hdc.rmiserver` on page A-39
- `hdc.ssl.secure` on page C-7

**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.rmiregistry` property of the Device Manager server (when non-SSL communication is used by Host Data Collector and the Device Manager server).

Related topics

- [Registering an exception for the Host Data Collector service (for non-SSL communication)](page 2-30)
- `hdc.rmiserver` on page A-39
- `hdc.ssl.secure` on page C-7

**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 topics

• [Registering an exception for the Host Data Collector service (for non-SSL communication)] on page 2-30

• `hdc.classloader` on page A-40

• `hdc.ssl.secure` on page C-7

**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 topics

• [Registering an exception for the Host Data Collector service (for SSL communication)] on page 2-31

• `hdc.rmiregistry` on page A-39

• `hdc.ssl.secure` on page C-7

**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 topics**

- [Registering an exception for the Host Data Collector service (for SSL communication)](#) on page 2-31
- hdc.rmiserver on page A-39
- hdc.ssl.secure on page C-7

**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 topics**

- [Registering an exception for the Host Data Collector service (for SSL communication)](#) on page 2-31
- hdc.classloader on page A-40
- hdc.ssl.secure on page C-7

**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
If you do not specify an IP address, the IP address acquired by Host Data Collector will be used.

**Related topics:**
- hdc.rmiregistry on page A-39
- hdc.rmiserver on page A-39
- hdc.classloader on page A-40

**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 C-2 Correspondences between the hdc.ssl.secure property values and the port numbers to be opened**

<table>
<thead>
<tr>
<th><strong>hdc.ssl.secure property value</strong></th>
<th><strong>Port numbers to be opened (Default)</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>1 RMI registry</td>
<td>22098/tcp</td>
</tr>
<tr>
<td>RMI server 22099/tcp</td>
<td></td>
</tr>
<tr>
<td><strong>hdc.ssl.secure</strong> property value</td>
<td><strong>Port numbers to be opened (Default)</strong></td>
</tr>
<tr>
<td>----------------------------------</td>
<td>----------------------------------------</td>
</tr>
<tr>
<td>Class loader</td>
<td>22100/tcp</td>
</tr>
<tr>
<td>2</td>
<td>RMI registry</td>
</tr>
<tr>
<td></td>
<td>22098/tcp, 22104/tcp</td>
</tr>
<tr>
<td></td>
<td>RMI server</td>
</tr>
<tr>
<td></td>
<td>22099/tcp, 22105/tcp</td>
</tr>
<tr>
<td></td>
<td>Class loader</td>
</tr>
<tr>
<td></td>
<td>22100/tcp, 22106/tcp</td>
</tr>
<tr>
<td>3</td>
<td>RMI registry</td>
</tr>
<tr>
<td></td>
<td>22098/tcp, 22104/tcp</td>
</tr>
<tr>
<td></td>
<td>RMI server</td>
</tr>
<tr>
<td></td>
<td>22105/tcp</td>
</tr>
<tr>
<td></td>
<td>Class loader</td>
</tr>
<tr>
<td></td>
<td>22106/tcp</td>
</tr>
</tbody>
</table>

#

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 topics**

- [hdc.common.rmi.registryPort on page C-3](#)
- [hdc.common.rmi.serverPort on page C-4](#)
- [hdc.common.http.serverPort on page C-4](#)
- [hdc.common.rmi.ssl.registryPort on page C-5](#)
- [hdc.common.rmi.ssl.serverPort on page C-5](#)
- [hdc.common.https.serverPort on page C-6](#)

**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>
<thead>
<tr>
<th>Message type</th>
<th>Output level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ERROR</td>
<td>0</td>
<td>error</td>
</tr>
<tr>
<td>WARNING</td>
<td>10</td>
<td>warning</td>
</tr>
<tr>
<td>INFO</td>
<td>30</td>
<td>information</td>
</tr>
<tr>
<td>-</td>
<td>40</td>
<td>debug</td>
</tr>
</tbody>
</table>

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 topics
• logger.trace.maxFileSize on page C-9

**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 topics
• logger.iotrace.maxFileSize on page C-10

**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 by using commas (,) to separate them.

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
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 D-1 Device Manager agent property files**

<table>
<thead>
<tr>
<th>Property file</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>agent.properties file</td>
<td>This property file is related to the connection between the Device Manager agent and the Replication Manager server.</td>
</tr>
<tr>
<td>hldutil.properties file</td>
<td>This property file is related to the Device Manager agent operations performed when executing the hldutil command.</td>
</tr>
<tr>
<td>logger.properties file</td>
<td>This property file is related to the Device Manager agent log output.</td>
</tr>
<tr>
<td>programproductinfo.properties file</td>
<td>This property file is related to the program information of the Device Manager agent.</td>
</tr>
<tr>
<td>server.properties file</td>
<td>This property file is related to Device Manager agent operations.</td>
</tr>
<tr>
<td>rgcmddev.properties file</td>
<td>This property file is related to the command devices that Device Manager agent connects to.</td>
</tr>
</tbody>
</table>

**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.

**Operations to complete in advance**

Log in as a user with Administrator permissions (for Windows) or as a root user (for UNIX).

**To change Device Manager agent properties:**

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 topics

- Starting and stopping the Device Manager agent service, and checking the operating status of the service (hbsasrv command) on page 10-15

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 topics**

- [agent.rm.horcmRange on page D-5](#)
- [server.agent.rm.temporaryInstance on page D-18](#)
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 topics
- agent.rm.horcmRange on page D-5
- server.agent.rm.temporaryPort on page D-18

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:

\[ 2 \times (2 + \text{number-of-storage-systems-that-comprise-the-virtual-storage-machine}) \]

Default: 100
**Related topics**
- [agent.rm.horcmInstance on page D-4](#)
- [agent.rm.horcmService on page D-5](#)

**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:

\[
\text{amount-of-information-output-to-log-file (MB/week)} = 0.75 \times \text{number-of-copy-pairs} + 4
\]

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 topics**
- [agent.logger.MaxFileSize on page D-6](#)

**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:

\[
\text{amount-of-information-output-to-log-file (MB/week)} = 0.75 \times \text{number-of-copy-pairs} + 4
\]

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 topics**

- `agent.logger.MaxBackupIndex` on page D-6

**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. This property cannot be specified in an OS other than HP-UX 11i v3.

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:

\[
\text{amount-of-information-output-to-log-file (MB/week)} = 0.8 \times \text{number-of-copy-pairs} + 25
\]

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 topics**

- logger.MaxFileSize on page D-9

**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 \times 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 topics
- `logger.MaxBackupIndex` on page D-9

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.

Default: `localhost`

**server.http.socket.agentAddress**

Specify the IP address at which the Device Manager agent transmits notifications to the Device Manager server.
In order to limit the IP addresses notified to the Device Manager server from the Device Manager agent, specify the IP address to be notified.

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#

#: 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 via API will be used.)

**Related topics**
- [server.http.socket.bindAddress on page D-12](#)

**server.http.socket.bindAddress**

In situations in which the Device Manager agent runs on a platform on which two or more network interface cards (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 topics**
- [server.http.socket.agentAddress on page D-11](#)

**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 topics**
- For details on the required memory size for Device Manager: [Settings required for a host to manage 100 or more LUs on page 10-10](#)
- For details on the required memory size for Replication Manager: [Managing copy pairs on page 10-7](#)

### 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 922372036854775807.

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 an enterprise-class storage system is acquired by using the CIM/WBEM function
    If the host OS is Red Hat Enterprise Linux 7 or later, or Oracle Linux 7 or later, use the 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: 32768

**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:

```
```

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 topics**
- [server.http.port on page A-6](#)
- [server.https.port on page A-7](#)

### 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 for each host when the system uses the local management method. To use the local management method, you need to install the Device Manager agent and CCI on each host.
- When the local management method is used, if you specify LUs as a copy pair that has different hosts, make sure that each LU is recognized by each host.

**enable**
- When the system uses the central management method, specify this value to manage all copy pairs with a single host (pair management server). To use the central management method, you must install the Device Manager agent and CCI only in the pair management server, and the Device Manager agent only in other hosts.
When the central management method is used, if the pair management server recognizes the command device in each storage system, the server can use all LUs, including LUs that are not recognized by the hosts of each storage system, to create copy pairs.

Default: disable

**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, Virtual Storage Platform, Universal Storage Platform V/VM, Hitachi USP, 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
- If you create a global-active device copy pair on VSP G1000

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: \texttt{HORCM\_DEV} format or \texttt{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 \texttt{HORCM\_DEV} or \texttt{HORCM\_LDEV} format in the configuration definition file.

**Table D-2 Conditions on which the Device Manager agent decides which format should be used in the configuration definition file**

<table>
<thead>
<tr>
<th>Which format is used in the existing configuration definition file</th>
<th>Pair operation</th>
<th>Format to be used in the configuration definition file</th>
</tr>
</thead>
<tbody>
<tr>
<td>No format is used.</td>
<td>Creating a pair for a new copy group.</td>
<td>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 \texttt{HORCM_DEV}</td>
</tr>
<tr>
<td>\texttt{HORCM_DEV} format is used.</td>
<td>Adding a pair to an existing copy group.</td>
<td>\texttt{HORCM_DEV} format, regardless of the format specified in the property</td>
</tr>
<tr>
<td></td>
<td>Creating a pair for a new copy group.</td>
<td>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 \texttt{HORCM_DEV}</td>
</tr>
<tr>
<td>\texttt{HORCM_LDEV} format is used.</td>
<td>Adding a pair to an existing copy group.</td>
<td>\texttt{HORCM_LDEV} format, regardless of the format specified in the property</td>
</tr>
<tr>
<td></td>
<td>Creating a pair for a new copy group.</td>
<td>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 \texttt{HORCM_LDEV}</td>
</tr>
<tr>
<td>Both \texttt{HORCM_DEV} format and \texttt{HORCM_LDEV} format are used.</td>
<td>Adding a pair to an existing copy group that uses \texttt{HORCM_DEV} format.</td>
<td>\texttt{HORCM_DEV} format, regardless of the format specified in the property</td>
</tr>
<tr>
<td></td>
<td>Adding a pair to an existing copy group that uses \texttt{HORCM_LDEV} format.</td>
<td>\texttt{HORCM_LDEV} format, regardless of the format specified in the property</td>
</tr>
<tr>
<td>Which format is used in the existing configuration definition file</td>
<td>Pair operation</td>
<td>Format to be used in the configuration definition file</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
</tbody>
</table>
| 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` | |
| 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`

**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 topics**

- [Changing the storage location of the configuration definition file on page 10-46](#)

**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`

**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.
Properties for command devices connected to Device Manager agent (rgcmddev.properties file)

If the storage system is VSP G1000, Virtual Storage Platform, or HUS VM, and resources in the storage system are partitioned, in the rgcmddev.properties file, specify a resource pool of the default virtual storage machine or a command device whose resource group ID is 0.

- 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`

Devine the command device in the following format. If you define multiple command devices, 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
- **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 or Virtual Storage Platform, specify a 5-digit number. For 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 resource pool of the default virtual storage machine or a command device whose resource group ID is 0.
Acronyms and abbreviations

The following acronyms and abbreviations might be used in this guide.

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

TCP
Transmission Control Protocol

TLS
Transport Layer Security

UDP
User Datagram Protocol

URL
Uniform Resource Locator

Acronyms-8
V

V-VOL
  Virtual VOLume

W

WAN
  Wide Area Network

WBEM
  Web - Based Enterprise Management

WWN
  Worldwide name

X

XML
  eXtensible Markup Language
Symbols

- .truststore 4-32

A

- account 3-14
- account.lock.num 3-5
- acquiring maintenance information on management server 11-14
- adding SVP to trusted zone 5-28
- agent.logger.loglevel D-6
- agent.logger.MaxBackupIndex D-6
- agent.logger.MaxFileSize D-6
- agent.properties file D-3
- agent.rm.everytimeShutdown D-3
- agent.rm.horcmInstance D-4
- agent.rm.horcmRange D-5
- agent.rm.horcmService D-5
- agent.rm.shutdownWait D-4
- agent.rm.TimeOut D-3
- agent.util.hpux.displayDsf D-7
- alerts 6-3
- SNMP traps 6-5
- analyzing performance
- Universal Replicator 5-20
- analyzing Universal Replicator performance
  settings for Device Manager 5-23
  settings for Replication Manager 5-24
  settings for Tuning Manager 5-24
  system configuration 5-20
- applying

B

- backing up
  database 9-2
- BaseDN 3-17
- Blocking HTTP communications 4-95
- bridge
  network settings 2-32
- built-in user 5-26

C

- C/T Delta
  analyzing 5-20
- central management method 1-35
- certificate
  checking 4-75
  checking for Host Data Collector 4-77
  importing into Common Component 4-71
  importing into Device Manager server truststore 4-52
  importing into Host Data Collector 4-76
- certificate signing request
  creating for Common Component 4-33
  creating for Device Manager server 4-45
creating for Host Data Collector 4-56
certificates, acquiring 4-86
checking connections
  external authentication server 3-47
  external authorization server 3-47
CIM/WBEM 7-2
  enabling 7-5
  user account settings 7-4
cimxmlcpa.properties A-51
cimxmlscpa.properties A-29, A-51
Ciphers A-33
Client certificate
  exporting for CIM client 4-121
  exporting for event indications 4-116
  importing for object operations 4-113
  importing into CIM client 4-121
client.properties A-28
client.rmi.port A-29
com.wbemsolutions.jservr.bindto A-51
Common Component
  log output 6-2
  ports 2-2
communication protocol
  changing between Replication Manager server and Device Manager server 4-75
Compute Systems Manager 1-34
condition
  message (warning banner) 4-2
conditions
  account 3-14
  LDAP search user account 3-42
config.xml file 5-19
configforclient.xml file 5-19
configuration definition file
  changing storage location 10-46
  description conventions 10-32
  editing 10-30
  notes 10-47
  prerequisite environment 10-29
  supported parameter 10-31
configuring
  networks 1-6
connecting
  notes and requirements for Storage Navigator Modular 2 5-2
copy pair
  prerequisite version of Device Manager agent 1-58
  storage system requirements 1-53
system configuration 1-35
copy pairs
  central management method 1-35
  local management method 1-35
  managing (Device Manager agent) 10-7
  system requirements 1-34
  virtual command device server method 1-35
creating a report 5-34
customizedsnmptrap.customizedSNMPTrapEnable A-33
customizedsnmptrap.customizelist A-34
customizedsnmptrap.properties A-33

D
database
  backing up 9-2
  exporting 9-19, 9-20
  importing 9-22, 9-25
  migrating 9-16
  restoring 9-6
database.properties file A-16, B-8
dbm.startingCheck.retryCount A-17
dbm.startingCheck.retryPeriod A-17
dbm.traceSQL A-17, B-8
Device Manager
  IPv6 environments 2-33
Device Manager - Storage Navigator
  backing up settings 5-31
  downloading settings 5-32
  setting time periods 5-29
Device Manager agent 1-4
  acquiring maintenance information [host] 11-19
  environment settings 10-3
  firewall 10-6
  ports 2-7
  prerequisite version 1-58
  property files D-2
  reinstalling after host OS upgrade 10-2
  resident process 10-15
Device Manager agent service
  checking operating status 10-15
  starting 10-15
  stopping 10-15
Device Manager CLI 1-3
  changing password-encoding level 4-124
  enabling SSL/TLS 4-68
Device Manager server 1-4

Index-2
enabling TLS/SSL  4-44
ports  2-3
property files  A-3
devicemanager.properties file  B-9
dispatcher.properties  A-20
downloading
Device Manager server truststore file  4-65
Tiered Storage Manager server truststore file  4-69
downloading trace files, FD Dump Tool  5-49
dvmcacerts  4-31
Dynamic Link Manager  1-34

E
e-mail notifications
setting up  6-24
Element Manager
deleting settings for using  5-5
settings  5-3
e-mail alerts
customizing templates  6-9
receiving  6-6
registering recipients  6-7
setting up SMTP server  6-7
enabling
TLS/SSL for Device Manager server  4-44
two-way authentication for event indications 4-116
two-way authentication for object operations 4-112
enabling SSL/TLS
Device Manager CLI computer  4-68
Tiered Storage Manager CLI computer  4-70
encryption types
Kerberos authentication  3-50
environment settings
Device Manager agent  10-3
event notification
customizing template  6-14
setting properties  6-14
specifying SMTP user authentication information 6-19
using  6-13
exauth.properties file
Kerberos server  3-34
LDAP directory server  3-19
RADIUS server  3-26
exception registration
Host Data Collector service  2-30, 2-31
exporting
client certificate for a CIM client  4-121
certificate for event indications  4-116
databases  9-19, 9-20
Device Manager server self-signed certificate  4-66
server certificate for a CIM client  4-121
server certificate for object operations  4-111
external authentication server  3-7
checking connections  3-47
registering  3-17
external authorization server  3-7
checking connections  3-47
registering  3-17

F
FD Dump Tool
downloading trace files  5-49
file servers  1-12
firewall
Device Manager agent  10-6
Host Data Collector  2-30
registering exceptions  2-15
registering exceptions in Linux  2-15
registering exceptions in Windows  2-15
settings  2-15
flat model  3-16

G
Global Link Manager  1-34
global-active device  1-65
GUI  1-3

H
hbsa_modinfo command  10-17
hbsa_util command  10-19
hbsasrv command  10-15
hc-mds64 banner
command  4-3, 4-4
hc-mds64 getlogs command  11-14
hc-mds64 unlockaccount command  3-6
hdc.adapter.adapterProcessNum  C-3
hdc.adapter.esx.timeout  C-7
server certificate into CIM client  4-121
server certificate into Device Manager agent 4-79
server certificate into Device Manager server keystore  4-47
server certificate into Web browser  4-66
indtruststore  4-33
IPv6
global address  2-34
global-unique local address  2-34
link-local address  2-34
linking with storage systems that support IPv6  2-35
migrating Device Manager server  2-34
site-local address  2-34

J
Java
   changing (Device Manager agent)  10-4
   changing (Host Data Collector)  1-11
javacfg.properties file  C-10
javapath_setup command  10-4
javapathlocation  C-11
JDK
   changing  1-10
jserver.properties  A-51
jssecacerts  4-30

K
Kerberos authentication
   encryption types  3-50
Kerberos server
   exauth.properties file  3-34
key pair
   changing password of Device Manager server  4-50
   creating for CIM client  4-120
   creating for Device Manager server  4-41
   creating for Host Data Collector  4-56
   deleting from Device Manager server keystore  4-50
   viewing in normal mode (Device Manager server)  4-48
   viewing in verbose mode (Device Manager server)  4-49
keystore
   changing password of Device Manager server  4-51
Importing a Host Data Collector server certificate  4-59
keystore file
   creating for event indications  4-113
   creating for object operations  4-109

L
launchapp.elementmanager.role.mode  A-37
launchapp.elementmanager.usehostname  A-37
launchapp.properties  A-35
launchapp.sn2.rmi.port  A-36
launchapp.sn2.url  A-36
launching
   Hitachi Storage Services Manager  5-25
LDAP directory server
   condition for server certificate  4-74
   exauth.properties file  3-19
LDAP search user
   registering  3-43
LDAP search user account  3-41
   checking  3-45
   conditions  3-42
   deleting  3-45
ldapcacerts  4-31
Linux
   registering firewall exceptions  2-15
local management method  1-35
locking
   System account  3-5
   unlocking accounts  3-6
   user accounts  3-4
logger.guiMessageFileCount  B-13
logger.guiMessageMaxFileSize  B-14
logger.guiTraceFileCount  B-13
logger.guiTraceMaxFileSize  B-14
logger.hicommandbase.loglevel  A-19
logger.hicommandbase.MaxBackupIndex  A-19
logger.hicommandbase.MaxFileSize  A-20
logger.hicommandbase.sysloglevel  A-19
logger.iotrace.maxFileSize  C-10
logger.iotrace.numOfFile  C-10
logger.loglevel  A-18, D-8
logger.MaxBackupIndex  A-18, D-9
logger.MaxFileSize  A-18, D-9
logger.messagelogLevel  B-10
logger.properties  A-17, C-9
logger.properties file  B-10, D-8
logger.serverMessageFileCount  B-12
logger.serverMessageMaxFileSize  B-14
logger.serverTraceFileCount  B-12
logger.serverTraceMaxFileSize  B-14
logger.syslogLevel  B-12
logger.trace.level  C-9
logger.trace.maxFileSize  C-9
logger.trace.numOfFile  C-9
logger.traceLogLevel  B-11
logging in  5-27
logs
  setup  6-1

mail-alert-detection.txt file  6-10
mainframe hosts  1-12
mainframe volumes  1-28
maintenance information
  acquiring on management server  11-14
  Host Data Collector  11-17
  host managed by Device Manager agent  11-19
  host managed by Host Data Collector  11-18
Management client  1-3
Management server  1-3
management server
  changing host name  2-36
  changing IP address  2-38
managing
  host  1-12
memory heap size
  changing  1-9
migrating
  databases  9-16
  Device Manager to IPv6 environment  2-34
migration.dataErase.defaultValue  A-42
migration.multiExecution  A-43
migration.plan.candidateCapacityGroupDisplayMaxCount  A-42
migration.plan.candidateVolumeCountLimit  A-42
migration.properties  A-41
migration.volumeDelete.defaultValue  A-43
mime.properties  A-28
MOF file
  editing for event indications  4-114
  editing for object operations  4-110

N
namespace  7-4
network
  bridge  2-32
NIC
  network settings multiple NICs  2-32
normal host  1-12
  prerequisites (Device Manager agent)  1-16
  prerequisites (Host Data Collector)  1-14

O
open hosts  1-12
OutOfRange error  11-10

P
Pair management server  1-4
pair management server  1-35
parameter
  configuration definition file  10-31
password
  truststore for Device Manager agent  4-81
  truststore for Host Data Collector  4-78
password.check.userId  3-3
password.min.length  3-2
password.min.lowercase  3-3
password.min.numeric  3-3
password.min.symbol  3-3
password.min.uppercase  3-2
performance information
  settings for acquiring  7-9, 7-14
  storage system (CIM/WBEM functions)  7-7
  storage systems  5-6
  system configuration  7-7
pop-up blocker
  changing settings  4-67
ports
  changing  2-10
  changing (CIM/WBEM)  7-6
registering exceptions  2-15
used by Common Component  2-2
used by Device Manager agent  2-7
used by Device Manager server  2-3
used by Host Data Collector  2-5
used by storage systems  2-7
used by Tiered Storage Manager server  2-5
prerequisite environment
  using configuration definition file 10-29
prerequisites
  normal host (Device Manager agent) 1-16
  normal host (Host Data Collector) 1-14
  virtual machine (Device Manager agent) 1-20
  virtual machine (Host Data Collector) 1-17
  virtualization server 1-26
programproductinfo.properties file D-10
properties
  changing (Host Data Collector) C-2
  Device Manager server, changing A-4
properties (Device Manager agent)
  changing D-2
properties (Tiered Storage Manager server)
  changing B-2
property files
  agent.properties D-3
  cimxmlscp.properties A-29
  client.properties A-28
  customizedsnmptrap.properties A-33
  database.properties A-16, B-8
  Device Manager agent D-2
  Device Manager server A-3
  devicemanager.properties B-9
  dispatcher.properties A-20
  hdcbase.properties C-2
  hldutil.properties D-7
  Host Data Collector C-2
  hostdatacollectors A-38
  javaconfig.properties C-10
  launchapp.properties A-35
  logger.properties A-17, B-10, C-9, D-8
  migration.properties A-41
  mime.properties A-28
  programproductinfo.properties D-10
  server.properties A-5, B-3, B-15
  syntax rules A-4, B-3
  Tiered Storage Manager server B-2
  tuningmanager.properties A-43

R
RADIUS server
  exauth.properties file 3-26
  raidinf add report 5-37
  raidinf command 5-35
  raidinf delete report 5-38, 5-39
  raidinf get reportinfo 5-40
receiving
  email alerts 6-6
registering
  recipients of email alerts 6-7
remote connection
  Tuning Manager (in a non-cluster environment) 5-15
  Tuning Manager (in cluster environment) 5-15
Replication Manager 1-34
Replication Manager server 1-4
replication.properties file A-46
Report Configuration Tool Command Reference 5-34
requirements
  connecting to Storage Navigator Modular 2 5-2
resident process 8-2
  Device Manager agent 10-15
  Host Data Collector 8-8
restoring
  database 9-6
rgcmddev.properties file D-23
rpmlib.properties file A-50
rpmlib.rpm.port A-50

S
secret key
  creating for Common Component 4-33
security
  configuring networks (common security risks) 1-6
self-signed certificate
  checking for CIM server 4-118
  creating for CIM client 4-120
  creating for Common Component 4-33
  creating for Device Manager server 4-41
  exporting 4-66
  for object operations 4-119
sending
  SNMP traps to log files 6-11
server certificate
  applying to certificate authority for Common Component 4-36
  applying to certificate authority for Device Manager 4-46
  applying to certificate authority for Host Data Collector 4-58
checking for Device Manager agent 4-81
conditions for LDAP directory 4-74
deleting from Device Manager server truststore 4-54
deleting from truststore for Device Manager agent 4-82
exporting for CIM client 4-121
exporting for object operations 4-111
importing for event indications 4-117
importing into CIM client 4-121
importing into Device Manager agent 4-79
importing into Device Manager server keystore 4-47
importing into keystore for Host Data Collector 4-59
importing into Web browser 4-66
server.agent.differentialrefresh.manual.enabled A-15
server.agent.differentialrefresh.periodical.enabled A-16
server.agent.evtwait.timeout D-22
server.agent.JRE.location D-13
server.agent.maxMemorySize D-12
server.agent.port D-11
server.agent.rm.centralizePairConfiguration D-15
server.agent.rm.culdevForm D-16
server.agent.rm.exclusion.instance D-16
server.agent.rm.horcm.poll D-17
server.agent.rm.horcmSource D-21
server.agent.rm.ignorePairStatus D-20
server.agent.rm.location D-16
server.agent.rm.moduleTimeOut D-21
server.agent.rm.optimization.userHorcmFile D-17
server.agent.rm.pairDefinitionForm D-18
server.agent.rm.temporaryInstance D-18
server.agent.rm.temporaryPort D-18
server.agent.rm.userAuthentication D-20
server.agent.shutDownTime D-13
server.base.home A-8
server.base.initialsynchrony A-9, B-5
server.checkOutVolumeRange B-7
server.cim.agent A-9
server.cim.http.port A-10
server.cim.httpss.port A-11
server.cim.support A-9
server.cim.support.job A-10
server.cim.support.protocol A-10
server.configchange.enabled A-11
server.dispatcher.configchange.pollingPeriod A-22
server.dispatcher.daemon.autoSynchro.dayOfWeek A-24
server.dispatcher.daemon.autoSynchro.doRefresh A-23
server.dispatcher.daemon.autoSynchro.interval A-25
server.dispatcher.daemon.autoSynchro.logicalGroup.doRefresh A-27
server.dispatcher.daemon.autoSynchro.performce.doRefresh A-26
server.dispatcher.daemon.autoSynchro.performce.startTime A-27
server.dispatcher.daemon.autoSynchro.startTime A-25
server.dispatcher.daemon.autoSynchro.type A-24
server.dispatcher.daemon.configUpdate.detection.interval A-22
server.dispatcher.daemon.configUpdate.detection.variable.enabled A-25
server.dispatcher.daemon.logicalGroupMappingUpdate.startTime A-28
server.dispatcher.daemon.pollingPeriod A-21
server.dispatcher.daemon.receiveTrap A-21
server.dispatcher.daemon.replication.config.doUpdate A-46
server.dispatcher.daemon.replication.config.minute A-48
server.dispatcher.daemon.replication.config.offset A-47
server.dispatcher.daemon.replication.config.updateInterval A-47
server.dispatcher.daemon.replication.performance.rpm.updateInterval A-48
server.dispatcher.daemon.replication.performance.tnm.minute A-50
server.dispatcher.daemon.replication.performance.tnm.offset A-49
server.dispatcher.daemon.replication.performance.tnm.updateInterval A-49
server.dispatcher.message.timeout A-20
server.dispatcher.message.timeout.in.processing A-20
server.dispatcher.snmp2.configchange.pollingPeriod A-21
server.dispatcher.traps.purgePeriod A-21
server.eventMonitoringIntervalInMinute B-6
server.eventNotification.mail.to A-14, B-6
server.horcmconfigfile.hostname A-9
server.http.entity.maxLength A-8, D-14
server.http.host A-5, D-11
server.http.localPort D-11
server.http.port A-6, D-11
server.http.security.clientIP A-30, D-14
server.http.security.clientIPv6 A-30
server.http.security.unprotected A-31
server.http.server.timeOut D-22
server.http.socket.agentAddress D-11
server.http.socket.bindAddress D-12
server.httpss.enabledCipherSuites A-32
server.https.port A-7
server.https.security.keystore A-31
server.https.security.truststore A-32
server.logicalGroupMapping.updateInterval A-16
server.logicalview.initialsynchro A-12
server.mail.alert.status A-14
server.mail.alert.type.storagesystem A-14
server.mail.enabled.filesystem A-12
server.mail.enabled.storagesystem A-12
server.mail.errorsTo A-14, B-5
server.mail.from A-13, B-5
server.mail.smtp.auth A-13, B-6
server.mail.smtp.host A-13, B-5
server.mail.smtp.port A-13, B-6
server.migration.dataErase.defaultValue B-7
server.migration.maxRetryCount B-8
server.migration.multiExecution B-6
server.migrationPlan.candidateCapacityGroupDisplayMaxCount B-7
server.migrationPlan.candidateVolumeCountLimit B-7
server.properties A-29
server.properties file
  Device Manager agent D-10
  Device Manager server A-5, A-29
  Tiered Storage Manager server B-3, B-15
server.rmi.port A-8, B-4
server.rmi.security.enabledCipherSuites B-15
server.rmi.security.port B-4
server.server.authorization D-14
server.server.serverIPAddress D-14
server.server.serverPort D-15
server.server.ssl.hdvm D-22
server.smisclient.indication.port A-15
server.subsystem.ssid.availableValues A-15
server.util.processTimeOut D-22
service
  changing user (Device Manager agent) 10-17
service processor 1-6
setting up
  SMTP server for email alerts 6-7
settings
  IPv6 2-33
  properties for event notification 6-14
shared secret
  checking 3-47
  deleting 3-46
  registering 3-46
signed certificates 4-86
SLP service
  releasing 7-17
  starting and stopping 7-16
SMTP server
  setting up for email alerts 6-7
SNMP traps
  alerts 6-5
  sending to log files 6-11
specifying
  SMTP user authentication information for event notification 6-19
SSL-encrypted communications
  blocking HTTP communications 4-95
  creating a private keypair 4-85
  creating a public keypair 4-85
  updating the certificate 4-87
storage location
  configuration definition file, changing 10-46
Storage Navigator Modular 2
  linking 5-2
storage system 1-4
  acquiring performance information (by using CIM/WBEM functions) 7-7
  changing 4-83
  requirements for managing copy pairs 1-53
storage systems
  collecting performance information 5-6
  ports 2-7
SVP 1-6
SVP, adding to trusted sites 5-28
System account
  automatically lock 3-5
system configuration 1-3
  central management method 1-40
  for acquiring performance information 7-7
  local management method 1-36
  managing copy pairs 1-35
  SVP configuration 1-48, 1-50
virtual command device server configuration 1-44
system requirements
  managing copy pairs 1-34

T
TIC command 11-19
Tiered Storage Manager CLI 1-3
  changing password-encoding level 4-124
  enabling SSL/TLS 4-70
  generating log file 11-16
  log file 11-16
Tiered Storage Manager server 1-4
  ports 2-5
  property files B-2
truststore
  changing password for Device Manager agent 4-81
  changing password for Host Data Collector 4-78
  deleting server certificate for Device Manager agent 4-82
  viewing in normal mode (Device Manager server) 4-53
  viewing in verbose mode (Device Manager server) 4-53
truststore file
  downloading (Device Manager server) 4-65
  downloading (Tiered Storage Manager server) 4-69
truststores 4-30
Tuning Manager 1-34
  remote connection (in a non-cluster environment) 5-15
  remote connection (in cluster environment) 5-15
tuningmanager.properties file A-43
two-way authentication
  disabling 4-119
  enabling for event indications 4-116
  enabling for object operations 4-112

U
Universal Replicator
  analyzing performance 5-20
user accounts
  account locking 3-3
  account locking policies 3-4
password policies 3-2
setting account locking policies 3-4
setting password policies 3-2
unlocking accounts 3-6
user authentication
  email alerts 6-8
  event notification 6-19
user_httpsd.conf file 4-36
  using
    event notification 6-13

V
veritas.volume.manager.version D-10
virtual command device server 1-35
virtual machine 1-12
  prerequisites (Device Manager agent) 1-20
  prerequisites (Host Data Collector) 1-17
  tasks for changing configuration 1-25
virtualization server 1-12
  changing 4-79
  prerequisites 1-26

W
warning banner 4-2
  creating and registering a message 4-2
  deleting message 4-4
  message display condition 4-2
Web browser
  accepting certificates 4-90
Windows
  registering firewall exceptions 2-15
Hitachi Data Systems

Corporate Headquarters
2845 Lafayette Street
Santa Clara, California 95050-2639
U.S.A.
www.hds.com

Regional Contact Information

Americas
+1 408 970 1000
info@hds.com

Europe, Middle East, and Africa
+44 (0)1753 618000
info.emea@hds.com

Asia Pacific
+852 3189 7900
hds.marketing.apac@hds.com

Hitachi Data Systems

MK-90HC175-16