

Hitachi Ops Center Analyzer

Installation and Configuration Guide

This manual provides information for installing and configuring Hitachi Ops Center Analyzer and Ops Center Analyzer viewpoint.

© 2019, 2020 Hitachi, Ltd. All rights reserved.

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

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

Some of the features described in the Materials might not be currently available. Refer to the most recent product announcement for information about feature and product availability, or contact Hitachi Vantara LLC at <https://support.hitachivantara.com/en-us/contact-us.html>.

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

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

1. Acquiring the relevant consents as may be required under local privacy laws or otherwise from authorized employees and other individuals; and
2. Verifying that your data continues to be held, retrieved, deleted, or otherwise processed in accordance with relevant laws.

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

Hitachi and Lumada are trademarks or registered trademarks of Hitachi, Ltd., in the United States and other countries.

AIX, AS/400e, DB2, Domino, DS6000, DS8000, Enterprise Storage Server, eServer, FICON, FlashCopy, GDPS, HyperSwap, IBM, Lotus, MVS, OS/390, PowerHA, PowerPC, RS/6000, S/390, System z9, System z10, Tivoli, z/OS, z9, z10, z13, z14, z/VM, and z/VSE are registered trademarks or trademarks of International Business Machines Corporation.

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

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

Copyright and license information for third-party and open source software used in Hitachi Vantara products can be found at <https://www.hitachivantara.com/en-us/company/legal.html>.

Contents

Preface.....	15
Intended audience.....	15
Product version.....	15
Release notes.....	15
Referenced documents.....	15
Document conventions.....	16
Conventions for storage capacity values.....	17
Accessing product documentation.....	18
Getting help.....	18
Comments.....	19
Chapter 1: Overview.....	20
Ops Center Analyzer overview.....	20
Ops Center Analyzer system configuration.....	20
Authentication method in Ops Center Analyzer.....	23
Default installation directory.....	23
Chapter 2: System requirements.....	25
System requirements for using the installer.....	25
Analyzer server requirements (Linux).....	25
Analyzer server requirements (Windows).....	27
Analyzer detail view server requirements.....	28
Analyzer probe server requirements.....	30
Analyzer Windows probe requirements.....	33
Port requirements.....	34
Supported ciphers.....	38
Supported ciphers for Analyzer probe.....	38
Supported ciphers for Analyzer Windows probe.....	39
Supported browsers.....	40
Monitoring target requirements.....	41
Monitoring target storage systems.....	41
Monitoring target hypervisors.....	45
Monitoring target hosts.....	46
Monitoring target FC switches.....	47
Hardware requirements based on system scale.....	48

Chapter 3: Installation by using the virtual appliances.....	51
Workflow for installing and using a virtual appliance.....	51
Installing Ops Center Analyzer and Analyzer detail view servers (VMware vSphere Client).....	52
Running the setup tool (opsvmsetup).....	53
Default settings for the virtual machine and guest operating system.....	54
Installing Analyzer probe server (VMware vSphere Client).....	55
Initial setup of the guest OS or VMs.....	57
Chapter 4: Installation by using the installer.....	59
Workflow for installing using an installer.....	59
Installing or updating the RPM packages (Linux OS).....	60
Increasing the maximum number of open files (Linux OS).....	62
Installing Ops Center Analyzer and Analyzer detail view servers (Linux OS)...	63
Installing Analyzer server (Windows OS).....	69
Installing Analyzer probe server (Linux OS).....	70
Linux environment changed by the installer.....	74
Chapter 5: Initial setup after installation.....	80
Initial setup of Analyzer detail view server.....	80
Initial setup of Analyzer probe server.....	81
Initial setup of Analyzer server.....	84
Workflow for initial setup.....	84
Verifying access to the Analyzer server.....	85
Registering Ops Center Analyzer in Ops Center Common Services.....	85
Registering the license for Analyzer server.....	85
Changing the system account password.....	86
Assigning Analyzer permissions to Ops Center user groups.....	86
Setting up a connection with Analyzer detail view server.....	87
Configuring the mail server.....	87
Changing Ops Center Analyzer passwords.....	88
Changing the megha and meghadata passwords.....	88
Changing the real-time database password.....	89
Initial setup for connecting with Ops Center Automator.....	90
Configuring settings to connect to Ops Center Automator when it is not linked with Device Manager.....	90
Verifying that the Ops Center Automator host name can be resolved....	90
Changing Common component settings.....	91
Checking user account permissions.....	92
Configuring settings to connect to Ops Center Automator when it is linked with Device Manager.....	93
Verifying that the Ops Center Automator host name can be resolved....	93

Changing Common component settings.....	94
Creating user accounts.....	95
Checking user account permissions.....	95
Creating a definition file to connect with Ops Center Automator.....	96
Format of definition files used to connect with Ops Center Automator...	97
Resetting Common component settings.....	101
Configuring initial settings for limiting the I/O activity of Hitachi storage resources.....	103
Configuration overview for I/O controls using Ops Center Automator.....	103
Registering storage systems in the Ops Center API Configuration Manager.....	104
Setting up Ops Center Automator to run the I/O control configuration function.....	105
Configuring I/O control settings with user-defined scripts.....	109
Prerequisites for setting I/O controls (using a script).....	109
Creating the script files.....	110
Editing built-in command templates.....	113
Creating an I/O control task.....	114
Running the script files.....	115
Checking the status of the script execution.....	115
Initial setup for enabling Granular Data Collection.....	116
Configuring SSH to use Granular Data Collection.....	116
Creating keys on the Analyzer server.....	116
Configuring the public key authentication.....	117
Verifying SSH connections.....	118
Registering storage systems to be monitored by Granular Data Collection.....	119
Configuring initial settings for enabling the audit log of the Analyzer server...	122
Enabling audit logging.....	124
Settings in the auditlog.conf file.....	125
Sample audit.log.conf file.....	127
Format of data output to the audit log.....	128
Adding a secondary Analyzer detail view server	130
Configuring the downloader on the Analyzer detail view server.....	131

Chapter 6: Configuring the RAID Agent to monitor Hitachi Enterprise Storage Systems..... 134

Determining the appropriate agent for collecting data.....	134
Workflow for adding the Hitachi Enterprise Storage probe.....	136
Setting up RAID Agent.....	136
Selecting the data collection method.....	137
Workflow for setting up the Hitachi Enterprise Storage probe (when using RAID Agent).....	141

Passing the settings information of Tuning Manager - Agent for RAID to RAID Agent.....	142
Configuring RAID Agent for data collection using command devices and SVP.....	143
Configuring Analyzer probe server.....	143
Configuring storage systems.....	144
Connecting the RAID Agent host and the storage system.....	145
Configuring access to the command device from RAID Agent.....	146
Selecting the communication protocol.....	147
Creating an instance environment.....	147
Configuring RAID Agent for data collection using command device and REST API.....	152
Configuring Analyzer probe server.....	152
Configuring storage systems.....	152
Connecting the RAID Agent host and the storage system.....	153
Configuring access to the command device from RAID Agent.....	153
Selecting the communication protocol.....	154
Creating an instance environment.....	155
Importing a certificate to the truststore for RAID Agent.....	159
Configuring RAID Agent for data collection using SVP and REST API.....	160
Configuring Analyzer probe server.....	160
Configuring storage systems.....	161
Connecting the RAID Agent host and the storage system.....	162
Selecting the communication protocol.....	162
Creating an instance environment.....	163
Importing a certificate to the truststore for RAID Agent.....	167
Configuring RAID Agent for data collection using REST API.....	168
Configuring Analyzer probe server.....	168
Configuring storage systems.....	169
Connecting the RAID Agent host and the storage system.....	169
Selecting the communication protocol.....	169
Creating an instance environment.....	169
Importing a certificate to the truststore for RAID Agent.....	172
Setting up Tuning Manager - Agent for RAID.....	174
Requirements for adding the Hitachi Enterprise Storage probe (when using Tuning Manager - Agent for RAID).....	174
Changing the data collected by Tuning Manager - Agent for RAID.....	176
Settings for communication from Analyzer probe server to Tuning Manager - Agent for RAID.....	177
Notes on using Tuning Manager - Agent for RAID.....	177
Values used for estimating disk space when using Tuning Manager - Agent for RAID.....	178

Migrating Hitachi Tuning Manager historical data.....	179
Setting up a Tuning Manager connection	180
Starting the data migration.....	181
Accessing Tuning Manager historical data.....	181
Changing the default migration connection settings.....	182
Notes and restrictions.....	183
Switching from Tuning Manager - Agent for RAID to RAID Agent.....	183
Chapter 7: Adding probes to the Analyzer probe.....	185
Adding Hitachi Enterprise Storage probe.....	185
Collecting additional configuration metrics.....	187
Collecting additional configuration metrics with Hitachi Configuration Manager.....	187
Collecting additional configuration metrics with Hitachi Device Manager..	188
Switching from Hitachi Device Manager to Hitachi Configuration Manager	189
Adding Hitachi Adaptable Modular Storage (AMS) probe.....	189
Adding Hitachi NAS probe.....	190
Adding VMware probe.....	192
Viewing the host CSV file import status.....	193
Adding Brocade FC Switch (BNA) probe.....	194
Adding Brocade FC Switch (CLI) probe.....	195
Adding Cisco FC Switch (DCNM) probe.....	198
Adding Cisco FC Switch (CLI) probe.....	199
Encrypting the CSV file.....	201
Adding Linux probe.....	201
Installing the perl module.....	203
Adding third-party storage probes (add-on package).....	204
Initial setup after adding a probe.....	204
Chapter 8: Installing Analyzer Windows probe.....	206
Installing the Analyzer Windows probe.....	206
Data collection methods.....	206
Configuring Analyzer Windows probe.....	210
Configuring the data collection method.....	210
Configuring the FTP or HTTPS server.....	212
Starting the Analyzer Windows probe service.....	213
Downloading the Analyzer Windows probe diagnostic data.....	213
Analyzer Windows probe configuration backup.....	213
Initial setup after adding a probe.....	214
Uninstalling the Analyzer Windows probe.....	214

Chapter 9: Upgrade your Ops Center Analyzer environment..... 216

Upgrade workflow.....	216
Installing or updating the RPM packages (Linux OS).....	217
Upgrading the Ops Center Analyzer and the Analyzer detail view servers on a Linux host.....	220
Upgrading the Analyzer server on a Windows host.....	222
Upgrading the Analyzer probe server.....	222
Upgrading Analyzer Windows probe.....	224
Checking the settings after an upgrade.....	224
Reconfiguring the connection with Ops Center Automator after an upgrade..	225

Chapter 10: Configure external user authentication..... 230

External user authentication overview.....	230
Configuring multiple external authentication servers.....	231
Configuring LDAP authentication for Analyzer server.....	233
Workflow for configuring LDAP authentication.....	233
Configuring the LDAP directory server.....	234
Creating user accounts on an LDAP directory server.....	234
Checking the LDAP directory server settings.....	235
Creating an LDAP search user account.....	237
Connecting to the LDAP directory server.....	238
LDAP configuration properties.....	241
Settings for connecting directly to an LDAP directory server.....	242
Settings for using DNS to connect to an LDAP directory server.....	248
Settings for connecting directly to an LDAP directory server and an authorization server.....	250
Settings for using DNS to connect to an LDAP directory server and an authorization server.....	256
Examples of specifying settings in the exauth.properties file to use an LDAP directory server for authentication.....	260
Configuring RADIUS authentication for Analyzer server.....	264
Workflow for configuring RADIUS authentication.....	264
Configuring the RADIUS server.....	264
Creating user accounts on the RADIUS server.....	265
Configuring LDAP directory server as external authorization server....	265
Connecting to the RADIUS server.....	265
RADIUS configuration properties.....	269
Settings for connecting directly to a RADIUS server.....	270
Settings for connecting directly to a RADIUS server and an authorization server.....	273
Settings for using DNS to connect to a RADIUS server and an authorization server.....	278

Examples of specifying settings in the exauth.properties file to use a RADIUS server for authentication.....	283
Configuring Kerberos authentication for Analyzer server.....	284
Workflow for configuring Kerberos authentication.....	285
Configuring the Kerberos server.....	285
Creating user accounts on the Kerberos server.....	285
Configuring LDAP directory server as external authorization server....	286
Connecting to the Kerberos server.....	286
Kerberos configuration properties.....	289
Settings for connecting directly to a Kerberos server.....	290
Settings for using DNS to connect to a Kerberos server.....	293
Settings for connecting directly to a Kerberos server and an authorization server.....	295
Settings for using DNS to connect to a Kerberos server and an authorization server.....	299
Examples of specifying settings in the exauth.properties file to use a Kerberos server for authentication.....	302
Configuring external user authentication on the Analyzer probe server and the Analyzer detail view server.....	304
Configuring the SSL port.....	305
Verifying the Active Directory domain name.....	306
Matching non-default Active Directory server settings.....	306
Managing Active Directory groups.....	307

Chapter 11: Configure secure communications..... 309

About security settings.....	309
Workflow for configuring secure communications.....	311
Configuring an SSL certificate (Analyzer server).....	316
Creating a private key and a certificate signing request for Analyzer server.....	316
Submitting a certificate signing request (CSR) for Analyzer server	316
Enabling SSL communication for Analyzer server.....	317
Checking the expiration date of the certificate for Analyzer server.....	320
Deleting a certificate from the Analyzer server truststore	321
Configuring an SSL certificate (Analyzer detail view server).....	322
Creating a private key and a certificate signing request.....	322
Applying server certificates.....	324
Exporting a self-signed certificate for the Analyzer detail view server.....	326
Checking the expiration dates of certificates for Analyzer detail view server.....	326
Changing the SSL port number of the Analyzer detail view server.....	327
Deleting an SSL certificate from the Keystore.....	328

Importing Analyzer detail view server certificates to the Analyzer server truststore.....	330
Configuring an SSL certificate (Analyzer probe server).....	331
Creating a private key and a certificate signing request	331
Applying server certificates.....	333
Exporting a self-signed certificate for the Analyzer probe server.....	334
Checking the expiration dates of certificates for Analyzer probe server....	335
Changing the SSL port number of the Analyzer probe server.....	335
Enabling strict host name checking between the Analyzer probe server and Analyzer detail view server.....	337
Enabling strict host name checking between the Analyzer probe server and Hitachi Enterprise Storage.....	338
Deleting an SSL certificate from the Keystore.....	339
Configuring an SSL certificate (HTTP Proxy).....	340
Creating a private key and a certificate signing request.....	341
Applying server certificates.....	342
Configuring an SSL certificate (Ops Center Automator).....	344
Importing Ops Center Automator certificates to the Analyzer server truststore.....	344
Configuring an SSL certificate (LDAP directory server).....	346
Importing LDAP directory server certificates to the Analyzer server truststore.....	346
Requirements for an LDAP directory server certificate.....	348
Configuring an SSL certificate (Common Services).....	348
Importing Common Services certificates to the Analyzer server truststore	349
Configuring an SSL certificate (RAID Agent).....	350
Creating a private key and a certificate signing request for RAID Agent server.....	350
Submitting a certificate signing request (CSR) for RAID Agent.....	351
Enabling SSL communication for RAID Agent.....	352
Checking the expiration date of the RAID Agent certificate.....	354
Importing RAID Agent certificates to the Analyzer server truststore.....	355
Importing RAID Agent certificates to the Analyzer probe server truststore	356

Chapter 12: Changing Ops Center Analyzer system settings..... 358

Starting and stopping the Ops Center Analyzer services.....	358
Starting the Analyzer server services.....	358
Stopping the Analyzer server services.....	359
Starting the Analyzer detail view server or Analyzer probe server services.....	360
Stopping the Analyzer detail view server or Analyzer probe server services.....	360
Starting the RAID Agent services.....	361

Stopping the RAID Agent services.....	363
Changing the system information of Analyzer server.....	364
Changing the Analyzer server host name.....	364
Changing the Analyzer server IP address.....	365
Changing the port number used between Analyzer server and the web browser (Linux).....	366
Changing the SSL port number between the Analyzer server and a web browser (Linux).....	368
Changing the port number used between Analyzer server and the web browser (Windows).....	370
Changing the SSL port number between the Analyzer server and a web browser (Windows).....	371
Changing the port number used between Analyzer server and Common component.....	373
Changing the port number between Analyzer server and the SMTP server.....	374
Changing the time settings of the Analyzer server.....	374
Change the format of syslog output.....	375
Moving an Analyzer server installation to another host.....	375
Changing the primary server information.....	376
Setting the domain to permit cross-domain access.....	377
Changing the system information of Analyzer probe server.....	378
Changing the Analyzer probe server host name when the Hitachi Enterprise Storage probe is added.....	378
Changing the Analyzer probe server host name.....	381
Changing the Analyzer probe server IP address when the Hitachi Enterprise Storage probe is added.....	383
Changing the Analyzer probe server IP address.....	385
Changing the port number used by the RAID Agent.....	386
Changing the port number of the RAID Agent REST Web Service.....	388
Restricting access to servers that access RAID Agent.....	390
Changing the data collection intervals of performance metrics for the Analyzer detail view server.....	392
Changing data collection intervals for RAID Agent.....	392
Deleting an instance environment for RAID Agent.....	394
Collecting optional metrics for Brocade Network Advisor probe.....	395
Changing the configuration information collection time.....	396
Creating the collection time definition file.....	398
Enabling the definitions in the collection time definition file.....	399
Managing the Analyzer detail view server and the Analyzer probe server.....	400
Accessing the Analyzer detail view.....	400
Viewing Analyzer probe server status.....	400
Starting and stopping probes.....	401

Editing probes.....	402
Deleting probes.....	402
Viewing and updating the Analyzer detail view license.....	402
Viewing and updating the Analyzer probe license.....	403
Downloading the Analyzer probe server diagnostic data.....	403
Updating the downloader on the Analyzer detail view server.....	404
Analyzer detail view audit logs.....	406
Increasing the maximum number of open files (Linux OS).....	408
Grouping data centers using custom attributes.....	410
Adding the Data Center and Location attributes.....	411
Adding the Organization and Cost Center attributes.....	411
Changing the IP address of the Analyzer detail view server.....	412
Updating the connection details of the Analyzer detail view server on the Analyzer probe server.....	412
Reconfiguring the connection with Analyzer detail view server.....	413
Restarting the HTTP proxy service	413
Enabling system account locking.....	414
Chapter 13: Backing up and restoring Ops Center Analyzer.....	415
Overview of Ops Center Analyzer backup and restore.....	415
Backing up Ops Center Analyzer.....	416
Backing up the Analyzer server.....	417
Backing up the Analyzer detail view server.....	417
Backing up the Analyzer probe server.....	418
Backing up the RAID Agent.....	419
Restoring Ops Center Analyzer.....	420
Restoring the Analyzer server.....	421
Restoring the Analyzer detail view server.....	422
Restoring the Analyzer probe server.....	424
Restoring the RAID Agent.....	425
Chapter 14: Removing Ops Center Analyzer components.....	427
Removing Ops Center Analyzer and Analyzer detail view servers from a Linux host.....	427
Removing Ops Center Analyzer server from a Windows host.....	428
Removing Analyzer probe server.....	428
Chapter 15: Troubleshooting.....	429
Connection to the Analyzer server web client unsuccessful.....	429
Logging on to Analyzer server unsuccessful.....	430
Starting Analyzer server does not work.....	430
Analyzer server cannot connect to Analyzer detail view server.....	430

Analyzer probe server cannot connect to Analyzer detail view server using HTTPS.....	431
Cannot add a probe using an HTTPS connection in Analyzer probe.....	431
Cannot start the Analyzer Windows probe service from the Windows Services panel.....	432
Collecting maintenance information.....	432
Collecting the log file for the Analyzer server.....	432
Collecting the log file for the Analyzer detail view server and the Analyzer probe server.....	433
Collecting the log file for the RAID Agent.....	433
Disabling statistics collection for System Diagnostics.....	434
Enabling statistics collection for System Diagnostics.....	434
Restarting a probe stuck in the Stopping state.....	435

Chapter 16: Installing Ops Center Analyzer viewpoint.....438

Overview of Analyzer viewpoint.....	438
Analyzer viewpoint system configuration.....	438
Prerequisites.....	439
System requirements.....	439
Virtual environment requirements.....	439
Supported browsers.....	439
Resource requirements for the virtual machine.....	440
Monitoring target requirements.....	440
Installing Analyzer viewpoint using a virtual appliance.....	440
Deploying the OVF.....	441
Using VM customization specification to configure the network.....	441
Upgrading Analyzer viewpoint	442
Upgrading the JDK to be used by Analyzer viewpoint.....	443
Registering the Analyzer viewpoint license.....	444
Accessing Analyzer viewpoint.....	445
Setting up the monitoring environment.....	445
Specifying settings so that the host name of Ops Center Common Services can be resolved.....	446
Advanced Configuration.....	446
Configuring the network.....	446
Changing the maximum amount of memory used by the data collection process.....	448
Making Analyzer viewpoint accessible by using the host name.....	448
Configuring Analyzer viewpoint host name.....	449
Registering Analyzer viewpoint in Ops Center Common Services running on a different host.....	450
Changing the Analyzer viewpoint port number.....	451
Changing the HTTPS server certificate of Analyzer viewpoint.....	452

Using Analyzer viewpoint.....	452
Creating user accounts.....	452
Assigning user roles.....	453
Starting the data collection process.....	454
Collecting log files.....	454
Backing up and restoring Analyzer viewpoint.....	454
Appendix A: Ops Center Analyzer CLI commands.....	455
List of Commands.....	455
Command usage guidelines.....	457
Usable characters for command arguments.....	457
backupsystem.....	458
collection_config.....	460
encryptpassword.....	466
hcnds64checkauth.....	468
Escaping special characters.....	471
hcnds64fwcancel.....	472
hcnds64getlogs.....	472
hcnds64intg.....	478
hcnds64ldapuser.....	480
hcnds64prmset.....	483
hcnds64radiussecret.....	485
hcnds64srv.....	487
hcnds64ssltool.....	491
hcnds64unlockaccount.....	495
htmssltool.....	497
reloadtemplate.....	500
restoresystem.....	502
setupcommonservice.....	506
Appendix B: Analyzer server services.....	510
Appendix C: User-specified properties file (config_user.properties).....	511
Appendix D: Analyzer server audit events that are output to the audit log.....	517

Preface

This manual provides information for installing and configuring Hitachi Ops Center Analyzer and Ops Center Analyzer viewpoint.

Intended audience

This document is intended for system administrators and service administrators.

The concepts, procedures, and information described in this document require the following skills:

- Knowledge of VMware vSphere operations, and the understanding related to setting up these products
- Basic knowledge of Linux
- Familiarity with RAID storage systems and their basic functions

Product version

This document revision applies to Hitachi Ops Center Analyzer 10.1.1 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. Release notes are available on Hitachi Vantara Support Connect: <https://knowledge.hitachivantara.com/Documents>.

Referenced documents

The following documents are referenced or contain more information about the features described in this manual.

- *Hitachi Ops Center Installation and Configuration Guide*, MK-99OPS001
- *Hitachi Ops Center Analyzer User Guide*, MK-99ANA002
- *Hitachi Ops Center Analyzer REST API Reference Guide*, MK-99ANA003
- *Hitachi Ops Center Analyzer Detail View REST API Reference Guide*, MK-99ANA004

- *Hitachi Ops Center Analyzer Detail View Metrics Reference Guide*, MK-99ANA005
- *Hitachi Ops Center Automator Installation and Configuration Guide*, MK-99AUT000
- *Hitachi Ops Center Automator User Guide*, MK-99AUT001
- *Hitachi Ops Center API Configuration Manager REST API Reference Guide*, MK-99CFM000
- *Hitachi Ops Center API Configuration Manager System Requirements*, MK-99CFM002
- *Hitachi Command Suite Tuning Manager Agent Administration Guide*, MK-92HC013
- *Hitachi Command Suite Tuning Manager Installation Guide*, MK-96HC141
- *Hitachi Command Suite System Requirements*, MK-92HC209

Hitachi Vantara Support Connect, <https://knowledge.hitachivantara.com/Documents>





Document conventions

This document uses the following typographic conventions:

Convention	Description
Bold	<ul style="list-style-type: none"> ▪ Indicates text in a window, including window titles, menus, menu options, buttons, fields, and labels. Example: Click OK. ▪ Indicates emphasized words in list items.
<i>Italic</i>	<ul style="list-style-type: none"> ▪ Indicates a document title or emphasized words in text. ▪ Indicates a variable, which is a placeholder for actual text provided by the user or for output by the system. Example: <code>pairedisplay -g group</code> <p>(For exceptions to this convention for variables, see the entry for angle brackets.)</p>
Monospace	Indicates text that is displayed on screen or entered by the user. Example: <code>pairedisplay -g oradb</code>
< > angle brackets	<p>Indicates variables in the following scenarios:</p> <ul style="list-style-type: none"> ▪ Variables are not clearly separated from the surrounding text or from other variables. Example: <code>Status-<report-name><file-version>.csv</code> ▪ Variables in headings.
[] square brackets	Indicates optional values. Example: [a b] indicates that you can choose a, b, or nothing.

Convention	Description
{ } braces	Indicates required or expected values. Example: { a b } indicates that you must choose either a or b.
vertical bar	Indicates that you have a choice between two or more options or arguments. Examples: [a b] indicates that you can choose a, b, or nothing. { a b } indicates that you must choose either a or b.

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

Icon	Label	Description
	Note	Calls attention to important or additional information.
	Tip	Provides helpful information, guidelines, or suggestions for performing tasks more effectively.
	Caution	Warns the user of adverse conditions and/or consequences (for example, disruptive operations, data loss, or a system crash).
	WARNING	Warns the user of a hazardous situation which, if not avoided, could result in death or serious injury.

Conventions for storage capacity values

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

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

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

Logical capacity unit	Value
1 block	512 bytes
1 cylinder	Mainframe: 870 KB Open-systems: <ul style="list-style-type: none"> ▪ OPEN-V: 960 KB ▪ Others: 720 KB
1 KB	1,024 (2^{10}) bytes
1 MB	1,024 KB or $1,024^2$ bytes
1 GB	1,024 MB or $1,024^3$ bytes
1 TB	1,024 GB or $1,024^4$ bytes
1 PB	1,024 TB or $1,024^5$ bytes
1 EB	1,024 PB or $1,024^6$ bytes

Accessing product documentation

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

Getting help

[Hitachi Vantara Support Connect](https://support.hitachivantara.com/en-us/contact-us.html) is the destination for technical support of products and solutions sold by Hitachi Vantara. To contact technical support, log on to Hitachi Vantara Support Connect for contact information: <https://support.hitachivantara.com/en-us/contact-us.html>.

[Hitachi Vantara Community](https://community.hitachivantara.com) is a global online community for Hitachi Vantara customers, partners, independent software vendors, employees, and prospects. It is the destination to get answers, discover insights, and make connections. **Join the conversation today!** Go to community.hitachivantara.com, register, and complete your profile.

Comments

Please send us your comments on this document to doc.comments@hitachivantara.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 Vantara LLC.

Thank you!

Chapter 1: Overview

Install Hitachi Ops Center Analyzer components using the OVA or installer. Perform initial setup after the installation is successful.

Ops Center Analyzer overview

Ops Center Analyzer provides a comprehensive application service-level and storage performance management solution that enables you to quickly identify and isolate performance problems, determine the root cause, and provide solutions. It enables proactive monitoring from the application level through network and storage resources for end-to-end visibility of your monitored environment. It also increases performance and storage availability by identifying problems before they can affect applications.

Ops Center Analyzer collects and correlates data from these sources:

- Storage systems
- Fibre channel switches
- Hypervisors
- Hosts

Components of Ops Center Analyzer

To use Ops Center Analyzer, you install and configure the following components:

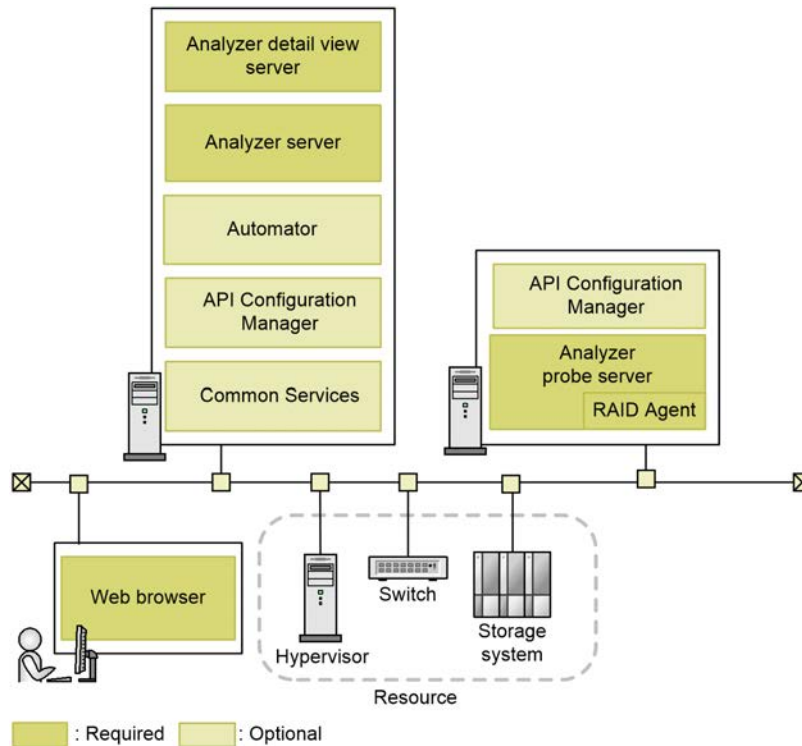
- **Analyzer server:** The primary component that communicates with the Analyzer detail view server. It correlates the configuration and performance data obtained by Analyzer detail view server to generate reports and enable data analytics for performance monitoring and problem resolution in your monitored infrastructure resources.
- **Analyzer detail view server:** This server processes performance and configuration data received from probes that connect to monitoring targets and provides the data to the Analyzer server for reporting and analysis.
- **Analyzer probe server:** This server manages the probes connected to the monitoring target.

Ops Center Analyzer system configuration

You can install the Ops Center Analyzer components either by deploying a virtual appliance or by using an installer. There are three types of virtual appliances: the Ops Center OVA, the Analyzer OVA, and the Analyzer probe OVA. The **Ops Center OVA** installs

multiple Ops Center components, including Ops Center Analyzer components, at the same time, and the **Analyzer OVA** installs only the Analyzer server and the Analyzer detail view server. You can deploy a virtual appliance for new installations only.

The following figure shows an example of a system configuration where Ops Center Analyzer components are installed by using the Ops Center OVA. Note that the required configuration is the same whether you use the Ops Center OVA or the Analyzer OVA.



The Analyzer server and Analyzer detail view server are installed on the same host. The Analyzer probe server must be installed on a different host than where the Analyzer detail view server is installed. When you install Analyzer probe server, RAID Agent is also installed.



Note: You can install the Analyzer server and the Analyzer detail view server on different hosts.

Use Ops Center API Configuration Manager in an environment installed by using the Analyzer probe OVA.

Note the following when configuring the system:

- Ops Center Analyzer cannot be used in a cluster environment.
- Ops Center Analyzer only supports IPv4 communications.
If an IPv6 environment is included as a communication destination for Ops Center Analyzer, configure the system so that Ops Center Analyzer can establish communications in IPv4.
- For each component of Ops Center Analyzer, if you change the OS time to an earlier time, the component no longer works properly. Configure settings to minimize the impact on applications. For example, if time is synchronized by using an NTP server, use slew mode.
- The Analyzer detail view server must be connected to one Analyzer server only.
- The Analyzer probe server cannot be installed on a host where the following products are installed:
 - Tuning Manager
 - Agent components for Tuning Manager
- If Tuning Manager is used in the existing environment, you can configure Tuning Manager - Agent for RAID with Ops Center Analyzer, instead of using RAID Agent.



Caution: Do not uninstall the Tuning Manager server if Tuning Manager - Agent for RAID is being used. The Tuning Manager server is necessary to maintain Tuning Manager - Agent for RAID.

- You can connect the Analyzer probe server to a RAID Agent installed on a different host. You can also connect the Analyzer probe server to RAID Agents installed on multiple hosts.

If you are not using the Analyzer probe server or RAID Agent, you must stop the relevant services.

- If you are using the RAID Agent installed on a host other than the Analyzer probe server host, stop the Analyzer probe server services on that host. For details, see [Stopping the Analyzer detail view server or Analyzer probe server services \(on page 360\)](#).
- If you are not using the RAID Agent installed on the Analyzer probe server host, stop the RAID Agent services on that host. For details, see [Stopping the RAID Agent services \(on page 363\)](#).

If you followed the procedure [Starting the RAID Agent services \(on page 361\)](#) to specify the setting that starts the RAID Agent services automatically when the OS starts, clear that setting.

- For some storage systems, you can select the data collection method. For details, see [Selecting the data collection method \(on page 137\)](#).
- Install Ops Center Automator if the following conditions apply:
 - If you run the Ops Center Automator service from the resource selected on Ops Center Analyzer

- If you use the Ops Center Analyzer Storage I/O controls feature to limit the I/O activity of volumes of the storage system by connecting with Ops Center Automator
- If you want to limit the I/O activity of volumes by using the Ops Center Analyzer Storage I/O controls feature, install the Ops Center API Configuration Manager on a host of your choice.
- If you are already using Ops Center Automator or the Ops Center API Configuration Manager, you can configure the product or products that you are currently using with Ops Center Analyzer.
- Make sure the difference between the time on the host running Analyzer and the times on the hosts running other Ops Center products is no more than 1 minute. We recommend configuring an NTP server.

Authentication method in Ops Center Analyzer

The following authentication methods are supported:

- Local user authentication:
This method uses the local built-in user authentication that uses the Common component.
- Common Services authentication:
This method centrally manages user information when using other Ops Center products. You can also use external user authentication (LDAP authentication or Kerberos authentication) through Ops Center Common Services. For details, see the *Hitachi Ops Center Installation and Configuration Guide*.
- External user authentication:
This method centrally manages user information when linking with other systems. For details, see [Configure external user authentication \(on page 230\)](#).

Default installation directory

The default installation directory for each component is as shown in the following table.

Component name	Default installation directory
Analyzer server	In Windows C:\Program Files\HITACHI In Linux /opt/hitachi
Analyzer detail view server	/data

Component name	Default installation directory
Analyzer probe server	/home
Ops Center API Configuration Manager	/opt/hitachi/ConfManager ³
Common component ¹	<p>In Windows</p> <p><i>Analyzer-server-installation-destination-folder\Base64²</i></p> <p>In Linux</p> <p><i>Analyzer-server-installation-destination-directory/Base64²</i></p>
<p>Notes:</p> <ol style="list-style-type: none"> 1. The Common component includes functions that are used by some Ops Center products and some Hitachi Command Suite products, and is installed as part of the Analyzer server. 2. If another product is being used and a Common component has already been installed, the new Common component will be installed in the same directory. 3. If this component was upgraded from a version earlier than 10.0.0, the previous installation path is inherited. 	

Chapter 2: System requirements

The system requirements for Hitachi Ops Center Analyzer server, Ops Center Analyzer detail view server, and Analyzer probe server are explained.

For details about system requirements for using the Ops Center consolidated virtual appliance, see the *Hitachi Ops Center consolidated virtual appliance System Requirements*.

System requirements for using the installer

This section provides the system requirements for using the installer, for additional information about the stand-alone OVA installations for the Analyzer server, Analyzer detail view server, and Analyzer probe, see *Chapter 3*.

Analyzer server requirements (Linux)

The requirements for Linux operating systems, network configuration, RPM packages, kernel parameters, and hardware are as follows:

Supported operating systems

- Red Hat Enterprise Linux 6.5-6.9, 7.0-7.7 (x64)
- Oracle Linux 6.7-6.9, 7.0-7.7 (Unbreakable Enterprise Kernel) (x64)
- Oracle Linux 7.4-7.7 (Red Hat Compatible Kernel release 4) (x64)



Note: You cannot send dashboard reports to users running Red Hat Enterprise Linux 6.x or Oracle Linux 6.x.

Network configuration

The Analyzer server supports IPv4 only.

Prerequisite RPM packages

Install the following RPM packages before installing the Analyzer server. You can check which RPM packages are missing by running the precheck tool (`analytics_precheck.sh`) provided by Ops Center Analyzer.

RPM packages	Details
<ul style="list-style-type: none"> ▪ tcsh ▪ net-tools ▪ bc 	<p>If dashboard reports are to be sent to users, you must install the following packages and package group.</p> <ul style="list-style-type: none"> ▪ package <ul style="list-style-type: none"> • gtk3-3.22.10 or later • libXScrnSaver • nss-3.22 or later ▪ package group <ul style="list-style-type: none"> • fonts

Kernel parameters

Before installing the Analyzer server on Linux, you must set the following kernel parameter values:

File*	Parameter	Value to be set
/etc/sysctl.conf	Fourth parameter (SEMMNI) of kernel.sem	The larger of 1024 and the following value: 24 + <i>current-system-value</i>
/etc/security/limits.conf	soft nofile hard nofile	The larger of 8514 and the following value: 4418 + <i>current-system-value</i>
*: The file path differs according to the environment. In addition, kernel parameters can also be set for files that are not listed here.		

Hardware requirements

Prerequisites		Value
Processor		Depends on the system scale ¹ .
Memory		Depends on the system scale ¹ .
Disk space	Installation directory ²	Depends on the system scale ¹ .
	/tmp ²	2 GB
	/var ²	1 GB

Prerequisites		Value
	<code>/var/ installation- directory-path²</code>	4 GB
Notes: <ol style="list-style-type: none"> 1. Refer to Hardware requirements based on system scale (on page 48) for more information. 2. Make sure that these directories are not created on Network File System (NFS) partition. 		

Analyzer server requirements (Windows)

The requirements for Windows operating systems, network configuration, and hardware are as follows:

Supported operating systems

OS name	Edition	SP	Architecture
Windows Server 2012 ¹	<ul style="list-style-type: none"> Standard Datacenter 	No SP	x64
Windows Server 2012 R2 ¹	<ul style="list-style-type: none"> Standard Datacenter 	No SP	x64
Notes: <ol style="list-style-type: none"> 1. Server core and Minimal Server Interface are not supported. 			

Network configuration

The Analyzer server supports IPv4 only.

Hardware requirements

Prerequisites	Minimum	Recommended
Processor	Dual-Core processor	Quad-Core processor
Memory	8 GB	16 GB minimum
Disk space	50 GB	100 GB minimum

Analyzer detail view server requirements

The requirements for operating systems, network configuration, java version, RPM packages, kernel parameters, and hardware are as follows:

Supported operating systems

- Red Hat Enterprise Linux 6.1, 6.5-6.9, 7.0-7.7 (x64)
- Oracle Linux 6.7-6.9, 7.0-7.7 (Unbreakable Enterprise Kernel) (x64)
- Oracle Linux 7.4-7.7 (Red Hat Compatible Kernel release 4) (x64)

Network configuration

The Analyzer detail view server supports IPv4 only.

Java version

JDK 1.8 update 91 or later (x64). For OpenJDK, the JDK must be equivalent to java-1.8.0-openjdk-devel.



Note: Before installing the Analyzer detail view server, you must set the paths for the `java` and `keytool` commands.

Prerequisite RPM packages

Install the following RPM packages before installing the Analyzer detail view server. You can check which RPM packages are missing by running the precheck tool (`analytics_precheck.sh`) provided by Ops Center Analyzer.

RPM packages	Details
<ul style="list-style-type: none"> ▪ perl ▪ expect ▪ openssl-devel (1.0.1e-fips 11 Feb 2013 or later) ▪ parted ▪ nss-3.21.0 or later ▪ gcc ▪ unzip ▪ perl-CPAN ▪ expat-devel ▪ sysstat ▪ zip ▪ bc 	<ul style="list-style-type: none"> ▪ If nc (or nmap-ncat), lsof, and telnet are not installed or the path for jstack of the JDK is not set, some maintenance information cannot be obtained. If a problem occurs, you might be asked to obtain maintenance information. For this reason, we recommend that you make all of them available. ▪ If you are using one of the following OSs, the package perl-XML-Simple is required: <ul style="list-style-type: none"> • Red Hat Enterprise Linux 7.0 or later • Oracle Linux 7.0 or later

RPM packages	Details
<ul style="list-style-type: none"> ▪ net-tools ▪ sudo ▪ crontabs ▪ nc or nmap-ncat (recommended) ▪ lsof (recommended) ▪ telnet (recommended) ▪ fontconfig 2.13.0-4.3 or later ▪ xorg-x11-font-utils 7.5-21 or later ▪ xorg-x11-fonts-Type1 ▪ dejavu-sans-fonts ▪ perl-IO-Socket-SSL ▪ perl-XML-Simple ▪ initscripts 	

Kernel parameters

Before installing the Analyzer detail view server on Linux, you must set the following kernel parameter values:

File*	Parameter	Value to be set
/etc/sysctl.conf	fs.file-max	327675 or greater
/etc/security/limits.conf	megha soft nofile megha hard nofile	262140 or greater
*: The file path differs according to the environment. In addition, kernel parameters can also be set for files that are not listed here.		

Hardware requirements

Prerequisites	Value
Processor	Depends on the system scale ¹ .
Memory	Depends on the system scale ¹ .

Prerequisites		Value
Disk space	Installation directory ^{2,3}	Depends on the system scale ¹ .
	/ (root) ³	5 GB
	/tmp ³	100 MB
	/usr/local ³	1 GB
	/home ³	100 MB
Notes: <ol style="list-style-type: none"> 1. The memory and disk capacity requirements vary depending on the managed resources. For example, if the managed storage systems contain a large number of volumes, the database will consume significant disk space. If you decrease the interval at which you obtain performance information from the managed resources, the volumes occupy more disk space in the database. Refer to Hardware requirements based on system scale (on page 48) for more information. 2. When you run the <code>analytics_install.sh</code> command, do not install the Analyzer detail view server on the same disk where the operating system is installed. You must install the Analyzer detail view server on a physical disk. 3. Make sure that these directories are not created on Network File System (NFS) partition. 		

Analyzer probe server requirements

The requirements for operating systems, network configuration, java version, RPM packages, kernel parameters, and hardware are as follows:

Supported operating systems

- Red Hat Enterprise Linux 6.1, 6.5-6.9, 7.0-7.7 (x64)
- Oracle Linux 6.7-6.9, 7.0-7.7 (Unbreakable Enterprise Kernel) (x64)
- Oracle Linux 7.4-7.7 (Red Hat Compatible Kernel release 4) (x64)

Network configuration

The Analyzer probe server supports IPv4 only.

Java version

JDK 1.8 update 91 or later (x64). For OpenJDK, the JDK must be equivalent to java-1.8.0-openjdk-devel.



Note: Before installing the Analyzer probe server, you must set the paths for the `java` and `keytool` commands.

Prerequisite RPM packages

Install the following RPM packages before installing the Analyzer probe server. You can check which RPM packages are missing by running the precheck tool (`dcaprobe_precheck.sh`) provided by Ops Center Analyzer.

RPM packages	Details
<ul style="list-style-type: none"> ▪ perl ▪ perl-CPAN ▪ gcc ▪ expect ▪ openssl-devel (1.0.1e-fips 11 Feb 2013 or later) ▪ unzip ▪ glibc.i686 ▪ glibc.x86_64 ▪ libstdc++.i686 ▪ libstdc++.x86_64 ▪ net-tools ▪ tcsh ▪ libyaml ▪ libgcc.x86_64 ▪ nss-softoken-freebl.x86_64 ▪ iproute.x86_64 ▪ ncurses ▪ openssh-clients ▪ nss-3.21.0 or later ▪ expat-devel ▪ xinetd ▪ sysstat ▪ zip ▪ bc ▪ sudo ▪ crontabs ▪ make 	<ul style="list-style-type: none"> ▪ If nc (or nmap-ncat), lsof, and telnet are not installed or the path for jstack of the JDK is not set, some maintenance information cannot be obtained. If a problem occurs, you might be asked to obtain maintenance information. For this reason, we recommend that you make all of them available. ▪ If you are using one of the following OSs, the packages perl-Digest-MD5 and perl-XML-Simple are required: <ul style="list-style-type: none"> • Red Hat Enterprise Linux 7.0 or later • Oracle Linux 7.0 or later

RPM packages	Details
<ul style="list-style-type: none"> ▪ nc or nmap-ncat (recommended) ▪ lsof (recommended) ▪ telnet (recommended) ▪ perl-IO-Socket-SSL ▪ perl-Digest-MD5 ▪ perl-XML-Simple ▪ initscripts 	

Kernel parameters

Before installing the Analyzer probe server on Linux, you must set the following kernel parameter values:

File*	Parameter	Value to be set
/etc/sysctl.conf	fs.file-max	327675 or greater
/etc/security/limits.conf	megha soft nofile megha hard nofile	262140 or greater
*: The file path differs according to the environment. In addition, kernel parameters can also be set for files that are not listed here.		

Hardware requirements

Prerequisites		Value for Analyzer probe server	Value for RAID Agent
Processor		Depends on the system scale*.	
Memory		Depends on the system scale*.	
Disk space	Installation directory	Depends on the system scale*.	
	/ (root)	5 GB	--
	/tmp	100 MB	350 MB
	/usr/local	1 GB	--
	/opt/jplpc	--	1 GB

Prerequisites		Value for Analyzer probe server	Value for RAID Agent
	/home	100MB	--
<p>*: The memory and disk capacity requirements vary depending on the managed resources. For example, if the managed storage systems contain a large number of volumes, the database will consume significant disk space. If you decrease the interval at which you obtain performance information from the managed resources, the volumes occupy more disk space in the database. Refer to Hardware requirements based on system scale (on page 48) for more information.</p>			

Analyzer Windows probe requirements

The requirements for operating systems, network configuration, locale, software, and hardware are as follows:

Supported operating systems

OS name	Edition	SP	Architecture
Windows Server 2012 ¹	<ul style="list-style-type: none"> Standard Datacenter 	No SP	x64
Windows Server 2012 R2 ¹	<ul style="list-style-type: none"> Standard Datacenter 	No SP	x64
Windows Server 2016 ²	<ul style="list-style-type: none"> Standard Datacenter 	No SP	x64
<p>Notes:</p> <ol style="list-style-type: none"> 1. Server core and Minimal Server Interface are not supported. 2. Server core and Nano Server are not supported. 			

Network configuration

The Windows probe supports IPv4 only.

Locale

The Analyzer Windows probe must be installed on a windows machine with one of the following English locales:

- Australia
- Belize
- Canada

- Caribbean
- India
- Ireland
- Jamaica
- Malaysia
- New Zealand
- Philippines
- Singapore
- South Africa
- Trinidad and Tobago
- United Kingdom
- United States
- Zimbabwe

The Display language and Input Method language on a Windows machine must be set to English.

Software requirements

Software name	Version	Protocol
Microsoft .NET Framework	3.5 Service Pack1 or later	HTTP
	4.5 or later	<ul style="list-style-type: none"> ▪ HTTP ▪ HTTPS

Hardware requirements

Prerequisites	Minimum
Memory	8 GB
Disk space (system drive)	50 GB



Note: You must install one Analyzer Windows probe for every 100 machines.

Port requirements

Before you install the Analyzer server, Analyzer detail view server or Analyzer probe server, review the desktop, port, and firewall requirements.

**Note:**

The installer enables support for `iptables` by default. If `firewalld` is used, then manually open the ports that are required for the product.

Default port number for Analyzer server

Source IP address	Target IP address	Default port	Protocol
User Desktop	Analyzer server	22015 ¹	HTTP
		22016 ¹	HTTPS
Analyzer server	RAID Agent Server or Tuning Manager - Agent for RAID Server	24221 ²	HTTP
		24222 ²	HTTPS
		22 ²	SSH
	Ops Center Common Services	443	TCP
<ol style="list-style-type: none"> 1. By default, HTTP and HTTPS can be used to access the Analyzer server. 2. For API requests that access RAID Agent, make sure that the server can communicate with RAID Agent. 			

Default port number for Analyzer detail view server

Source IP address	Target IP address	Default port	Protocol
User Desktop, Analyzer server	Analyzer detail view server	8443	TCP
Analyzer probe server	Analyzer detail view server	9092	TCP
Analyzer probe server	Analyzer detail view server / FTP Server	22 ¹	SFTP
		7443 ¹	HTTPS
		21 ¹	FTP
		990 ¹	FTPS
Analyzer probe server	Analyzer detail view server	8443 ²	HTTPS
User Desktop	Analyzer detail view server	8080	TCP

Source IP address	Target IP address	Default port	Protocol
Notes: <ol style="list-style-type: none"> 1. This port is required for the data transfer protocol. Close this port if it is not required. 2. This port is required if you want to migrate Tuning Manager data. For details, refer to Migrating Hitachi Tuning Manager historical data (on page 179). 			

Default port number for Analyzer probe server

Source IP address	Target IP address	Default port	Protocol
User Desktop	Analyzer probe server	8443	TCP
		22 ¹	TCP
		8080	TCP
Analyzer probe server	Tuning Manager server	22015 ²	HTTP
		22016 ²	HTTPS

Notes:

1. This port is required to connect to the Analyzer probe server through the SSH client. Close this port if it is not required.
2. This port is required if you want to migrate Tuning Manager data. For details, refer to [Migrating Hitachi Tuning Manager historical data \(on page 179\)](#).

Probe port and firewall requirements

Probe name	Collection method	Source IP address	Target IP address	Default port	Protocol
Storage systems					
Hitachi AMS	SNM2API	Analyzer probe server	AMS Controller	2000	TCP
Hitachi Enterprise Storage	RAID Agent or Tuning Manager - Agent for RAID	Analyzer probe server	RAID Agent Server or Tuning Manager - Agent for RAID Server	24221	HTTP
				24222	HTTPS

Probe name	Collection method	Source IP address	Target IP address	Default port	Protocol
		RAID Agent Server or Tuning Manager - Agent for RAID Server	Storage systems that are managed through SVP	1099 ³ , 11099 ⁴ , 51099, and 51100	TCP
	RAID Agent ¹	RAID Agent Server	GUM(CTL)	80	HTTP
				443	HTTPS
	Hitachi Device Manager API	Analyzer probe server	Hitachi Device Manager Server	2001	HTTP
				2443	HTTPS
	Hitachi Ops Center API Configuration Manager API	Analyzer probe server	Hitachi Ops Center API Configuration Manager Server	23450	HTTP
				23451	HTTPS
	Hitachi NAS	RUSC	Analyzer probe server	HNAS SMU	22
REST API		8444			HTTPS
Hypervisors					
VMware	VMware vCenter API	Analyzer probe server	VMware vCenter Server/ VMware ESXi Host	443	TCP
Windows (Hyper-V)	WMI	Windows probe	Windows Host/Hyper-V	135	TCP
	Perfmon			445	
	SCOM		SCOM server	5723, 5724, and 51905	
	SCCM		SCCM server	1433	
FC Switches					
Brocade FC Switch (BNA)	BNA (REST API)	Analyzer probe server	BNA server	80	HTTP
				443	HTTPS

Probe name	Collection method	Source IP address	Target IP address	Default port	Protocol
Brocade FC Switch (CLI)	Brocade Switch CLI	Analyzer probe server	Brocade FC Switch	22	SSH
Cisco DCNM ²	DCNM (Web Services)	Analyzer probe server	DCNM Server	80	HTTP
				443	HTTPS
Cisco SAN Switch	Cisco Switch CLI	Analyzer probe server	Cisco FC Switch	22	SSH
Hosts					
Linux	ssh	Analyzer probe server	Linux host	22	SSH
	xinetd	Linux host	Analyzer probe server	1111	TCP
Notes: <ol style="list-style-type: none"> 1. This port is required if the REST API is used. 2. Cisco DCNM 10.0 does not support HTTP. 3. This port is used to monitor storage systems other than VSP 5000 series. 4. This port is used to monitor VSP 5000 series storage systems. 					

Supported ciphers

The Analyzer detail view server and Analyzer probe server support various different ciphers when transferring data using HTTPS or SFTP connections.

Supported ciphers for Analyzer probe

The following ciphers are supported while transferring data using SFTP and HTTPS connections from the Analyzer probe server to the Analyzer detail view server or Intermediate FTP server:



Note: The first matching algorithm on the Analyzer detail view server or Intermediate FTP server is used for the SSL handshake.

Kex algorithm: diffie-hellman-group-exchange-sha256, diffie-hellman-group-exchange-sha1, diffie-hellman-group14-sha1, diffie-hellman-group1-sha1

Host key algorithm: ssh-rsa, ssh-dss

Encryption algorithm: aes256-cbc, aes192-cbc, aes128-cbc, aes256-ctr, aes192-ctr, aes128-ctr, twofish256-cbc, twofish192-cbc, twofish-cbc, twofish256-ctr, twofish192-ctr, serpent256-cbc, serpent192-cbc, serpent128-cbc, serpent256-ctr, serpent192-ctr, serpent128-ctr, 3des-cbc, 3des-ctr, cast128-cbc, cast128-ctr, arcfour256, arcfour128, arcfour, idea-cbc, idea-ctr, blowfish-ctr, none

MAC algorithm: hmac-sha2-512-96, hmac-sha2-512, hmac-sha2-256-96, hmac-sha2-256, hmac-sha1-96, hmac-sha1, hmac-md5-96, hmac-md5, none

Compression algorithm: zlib, none

Supported ciphers for Analyzer Windows probe

The following ciphers are supported while transferring data using an HTTPS connection from the Analyzer Windows probe to the Analyzer detail view server or Intermediate FTP server:



Note: The first matching algorithm on the Analyzer detail view server or Intermediate FTP server is used for the SSL handshake.

Kex algorithm: diffie-hellman-group-exchange-sha256, diffie-hellman-group-exchange-sha1, diffie-hellman-group14-sha1, diffie-hellman-group1-sha1

Host key algorithm: ssh-rsa, ssh-dss

Encryption algorithm: aes256-cbc, aes192-cbc, aes128-cbc, aes256-ctr, aes192-ctr, aes128-ctr, twofish256-cbc, twofish192-cbc, twofish-cbc, twofish256-ctr, twofish192-ctr, serpent256-cbc, serpent192-cbc, serpent128-cbc, serpent256-ctr, serpent192-ctr, serpent128-ctr, 3des-cbc, 3des-ctr, cast128-cbc, cast128-ctr, arcfour256, arcfour128, arcfour, idea-cbc, idea-ctr, blowfish-ctr, none

MAC algorithm: hmac-sha2-512-96, hmac-sha2-512, hmac-sha2-256-96, hmac-sha2-256, hmac-sha1-96, hmac-sha1, hmac-md5-96, hmac-md5, none

Compression algorithm: zlib, none

The following ciphers are supported while transferring data using an SFTP connection from the Analyzer Windows probe to the Analyzer detail view server or Intermediate FTP server:

Kex algorithm: AES-256-CBC, AES-192-CBC, AES-128-CBC, DES-EDE3-CBC encryption

MAC algorithm: hmac-sha2-512-etm@openssh.com, hmac-sha2-256-etm@openssh.com

Host key algorithm: ecdsa-sha2-nistp521, ecdsa-sha2-nistp384, ecdsa-sha2-nistp256, ssh-rsa, ssh-dss

Encryption algorithm: aes256-cbc, aes256-ctr, aes192-cbc, aes192-ctr, aes128-cbc, aes128-ctr, 3des-cbc, 3des-ctr

Supported browsers

The following browsers are supported:

Web browser/other	Version
Firefox	ESR 68
Internet Explorer	11*
Chrome Browser for enterprise	Latest version of stable channel
Flash Player	21.0 or later (to use Report Builder with the Analyzer detail view server)
*: Browser subwindows may open behind the main (parent) window.	

Monitoring target requirements

You can monitor the following storage system series, hypervisors, hosts, and FC switches.

Monitoring target storage systems

You can monitor the following storage system series:

Storage system series		Storage system	Microcode/ HNAS model	Analyzer probe name
VSP		Hitachi Virtual Storage Platform	70-06-33 or later	Hitachi Enterprise Storage probe ¹
VSP E series		Hitachi Virtual Storage Platform E990 (VSP E990)	93-01-01 or later	
VSP F series	VSP Fx00 models	Hitachi Virtual Storage Platform F600 (VSP F600)	83-02-01 or later	Note: This probe collects data from the storage systems when using the RAID Agent or Tuning Manager - Agent for RAID.
		Hitachi Virtual Storage Platform F800 (VSP F800)		
		Hitachi Virtual Storage Platform F350 (VSP F350)	88-01-03 or later ²	
		Hitachi Virtual Storage Platform F370 (VSP F370)		
		Hitachi Virtual Storage Platform F700 (VSP F700)		
		Hitachi Virtual Storage Platform F900 (VSP F900)		

Storage system series		Storage system	Microcode/ HNAS model	Analyzer probe name
	VSP F1500	Hitachi Virtual Storage Platform F1500	80-05 or later	
VSP G series	VSP Gx00 models	Hitachi Virtual Storage Platform G200 (VSP G200)	83-02-01 or later	
		Hitachi Virtual Storage Platform G400 (VSP G400)		
		Hitachi Virtual Storage Platform G600 (VSP G600)		
		Hitachi Virtual Storage Platform G800 (VSP G800)		
		Hitachi Virtual Storage Platform G350 (VSP G350)	88-01-03 or later ²	
		Hitachi Virtual Storage Platform G370 (VSP G370)		
		Hitachi Virtual Storage Platform G700 (VSP G700)		
		Hitachi Virtual Storage Platform G900 (VSP G900)		
	VSP G1000	Hitachi Virtual Storage Platform G1000	80-03-31 or later	
	VSP G1500	Hitachi Virtual Storage Platform G1500	80-05 or later	
VSP N series See "Notes on notation of the VSP N series" below.		Hitachi Virtual Storage Platform N400 (VSP N400)	83-06-01 or later	
		Hitachi Virtual Storage Platform N600 (VSP N600)		
		Hitachi Virtual Storage Platform N800 (VSP N800)		
VSP 5000 series		Hitachi Virtual Storage Platform 5100	90-02 or later	
		Hitachi Virtual Storage Platform 5500		
		Hitachi Virtual Storage Platform 5100H		

Storage system series	Storage system	Microcode/ HNAS model	Analyzer probe name
	Hitachi Virtual Storage Platform 5500H		
HUS VM	Hitachi Unified Storage VM	73-03-40 or later	
HUS100	Hitachi Unified Storage 110 (HUS110)	09-10 or later	Hitachi Adaptor Modular Storage (AMS) probe
	Hitachi Unified Storage 130 (HUS130)		
	Hitachi Unified Storage 150 (HUS150)		
Hitachi NAS	HNAS	<ul style="list-style-type: none"> ▪ 3080 ▪ 3090 ▪ 4040 ▪ 4060 ▪ 4080 ▪ 4100 ▪ VSP G400 (Unified) ▪ VSP G600 (Unified) ▪ VSP G800 (Unified) ▪ VSP F400 ▪ VSP F600 ▪ VSP F800 ▪ VSP N400 ▪ VSP N600 ▪ VSP N800 	HNAS probe Note: To view NAS configuration and performance reports, go to the Analyzer detail view server.

Storage system series	Storage system	Microcode/ HNAS model	Analyzer probe name
Notes: <ol style="list-style-type: none"> 1. If performance data is collected using a command device, make sure that the RAID Manager LIB is installed on the same server as the Hitachi Enterprise Storage probe. 2. The methods for collecting performance data differ depending on the microcode version. <ul style="list-style-type: none"> ▪ When using the command device and the SVP, one of the following microcode versions is required: 88-01-03 to 88-01-04 and 88-02-01. ▪ When using the command device and the REST API, microcode version 88-02-01 or later is required. ▪ When using the SVP and the REST API, microcode version 88-02-01 is required. ▪ When using only the REST API, microcode version 88-02-01 or later is required. 			

**Note:**

- The following storage systems might be referred to as VSP family:
 - VSP
 - VSP E series
 - VSP F series
 - VSP G series
 - VSP 5000 series
- VSP family and HUS VM support Granular Data Collection.
- To manage additional Hitachi storage system information (such as storage capacity and hosts), use Device Manager 8.4.1 or later.
- Ops Center Analyzer supports the use of Server Priority Manager (which controls I/O) for the following storage systems: VSP E series, VSP F series, VSP G series and VSP 5000 series. For VSP G200, G400, G600, G800 and VSP F400, F600, F800 storage systems with microcode 83-03-0x or earlier, you might get an error if you specify or refer to Server Priority Manager information using the Storage I/O controls feature.
- For I/O control settings using Server Priority Manager, use Automation Director 8.5.0 or later (except 8.5.1).

Notes on notation of the VSP N series

Because the VSP N series is equivalent to the VSP F series or VSP G series, Ops Center Analyzer uses the VSP F series or VSP G series storage model names to indicate the VSP N series. (The model descriptions are equivalent as well.)

The following table lists the correspondence.

Storage system model in the VSP N series	Notation in Ops Center Analyzer
VSP N400	VSP F400 or VSP G400
VSP N600	VSP F600 or VSP G600
VSP N800	VSP F800 or VSP G800

Monitoring target hypervisors

You can monitor the following hypervisors:

Product name		Version	Analyzer probe name
VMware	vCenter server	<ul style="list-style-type: none">▪ 5.5▪ 6.0▪ 6.5▪ 6.5u2▪ 6.6▪ 6.7	VMware probe
	VMware ESXi	<ul style="list-style-type: none">▪ 5.5▪ 6.0▪ 6.5▪ 6.5u2▪ 6.6▪ 6.7	
Hyper-V	Windows Server 2012 Hyper-V*	--	Windows probe
	Windows Server 2012 R2 Hyper-V*		
	Windows Server 2016 Hyper-V		

*: Server core is not supported.

Monitoring target hosts

You can monitor the following hosts:

OS name		Version/Edition	Analyzer probe name
Windows	Windows Server 2012 ¹	<ul style="list-style-type: none"> Standard Datacenter 	Windows probe
	Windows Server 2012 R2 ¹	<ul style="list-style-type: none"> Standard Datacenter 	
	Windows Server 2016 ²	<ul style="list-style-type: none"> Standard Datacenter 	
Linux	Red Hat Enterprise Linux	<ul style="list-style-type: none"> 6.1 6.5 6.9 7.1 7.2 7.3 7.4 7.5 7.6 7.7 	Linux probe
	SUSE Linux Enterprise Server	<ul style="list-style-type: none"> 11 12 	
	Oracle Linux	<ul style="list-style-type: none"> 6.8 7.0 7.3 7.4 7.5 	

OS name		Version/Edition	Analyzer probe name
		<ul style="list-style-type: none">▪ 7.6▪ 7.7	
	CentOS	<ul style="list-style-type: none">▪ 6.6▪ 7.1▪ 7.2	
Notes: <ul style="list-style-type: none">1. Server core is not supported.2. Nano Server is not supported.			

Monitoring target FC switches

You can monitor the following FC switches:

Switch name	Software	Version/Model	Analyzer probe name
Brocade	Brocade Network Advisor Professional Plus	12.3.1	Brocade FC Switch (BNA) probe
	Brocade Network Advisor Enterprise	12.3	
	Brocade Network Advisor Professional Plus or Brocade Network Advisor Enterprise	<ul style="list-style-type: none"> 12.3.3 12.4.1 12.4.2 12.4.4 14.0.1 14.2.1 14.3.0 14.4.2 	
	Brocade Fabric OS	<ul style="list-style-type: none"> 6.1.2b1 6.2.2d 6.3.2e8 7.0.2e 7.2.1a 	Brocade FC Switch (CLI) probe

Switch name	Software	Version/Model	Analyzer probe name
		<ul style="list-style-type: none"> 7.4.1b 8.2.0 8.2.0a 8.2.0b 8.2.1c 	
Cisco	Cisco Data Center Network Manager	<ul style="list-style-type: none"> 5.0 6.2 6.3 7.1 10.0 10.2 10.3 10.4(2) 	Cisco FC Switch (DCNM) probe
	Cisco SAN Switch (CLI)	<ul style="list-style-type: none"> MDS 9124 MDS 9145 MDS 9148 MDS 9148S MDS 9513 	Cisco FC Switch (CLI) probe

Hardware requirements based on system scale

This section provides guidelines for determining the size of your environment based on the number of monitoring targets. Based on the sizing and scalability recommendations, you can identify the hardware requirements and scale your Ops Center Analyzer environment to meet workload demands.

System scale	Maximum number of resources				
	Hypervisor		Storage		FC Switch
	VM	ESX	Volume	Storage	
Small scale	40	5	5000	1	1

System scale	Maximum number of resources				
	Hypervisor		Storage		FC Switch
	VM	ESX	Volume	Storage	
Medium scale	1,000	15	35,000	5	5
Large scale	6,000	120	70,000	10	40
	6,000	120	200,000	40	40

The hardware requirements for Ops Center Analyzer components vary depending on the size of your environment.

Hardware requirements for Analyzer server

System scale	CPU (cores)*	Memory (GB)	Disk (GB)
Small scale	4	8	100
Medium scale	4	8	100
Large scale	8	16	100
	16	32	100
*: Based on an Intel(R) Xeon(R) Processor E5-2670 v2 @ 2.50 GHz.			

Hardware requirements for Analyzer detail view server

System scale	CPU (cores)*	Memory (GB)	Disk (GB)		
			Data retention period		
			14 days	32 days	365 days
Small scale	4	8	150	150	800
Medium scale	4	8	150	300	3,000
Large scale	9	24	300	500	5,000
	24	64	700	2,000	12,000
*: Based on an Intel Xeon Processor E5-2670 v2 @ 2.50 GHz.					

Hardware requirements for Analyzer probe server

System scale	CPU (cores) ¹	Memory (GB)	Disk (GB)
Small scale	4	10	100
Medium scale	10	32	500
Large scale ²	12	64	1,000 ³
Notes: <ol style="list-style-type: none"> 1. Based on an Intel Xeon Processor E5-2670 v2 @ 2.50 GHz. 2. If you are monitoring a system similar to, or larger than Large scale, consider installing multiple Analyzer probe servers. 3. The types of disks used are SAN disks. 			

Chapter 3: Installation by using the virtual appliances

Install Ops Center Analyzer components using a virtual appliance by preparing your environment, installing all components, and performing initial setup.

To install the Analyzer server, the Analyzer detail view server, and the Analyzer probe server using the stand-alone OVA installers, first verify the system requirements and then deploy the software.

You can also install the Analyzer server and Analyzer detail view server using the consolidated Ops Center virtual appliance. For details, see the *Hitachi Ops Center Installation and Configuration Guide*.

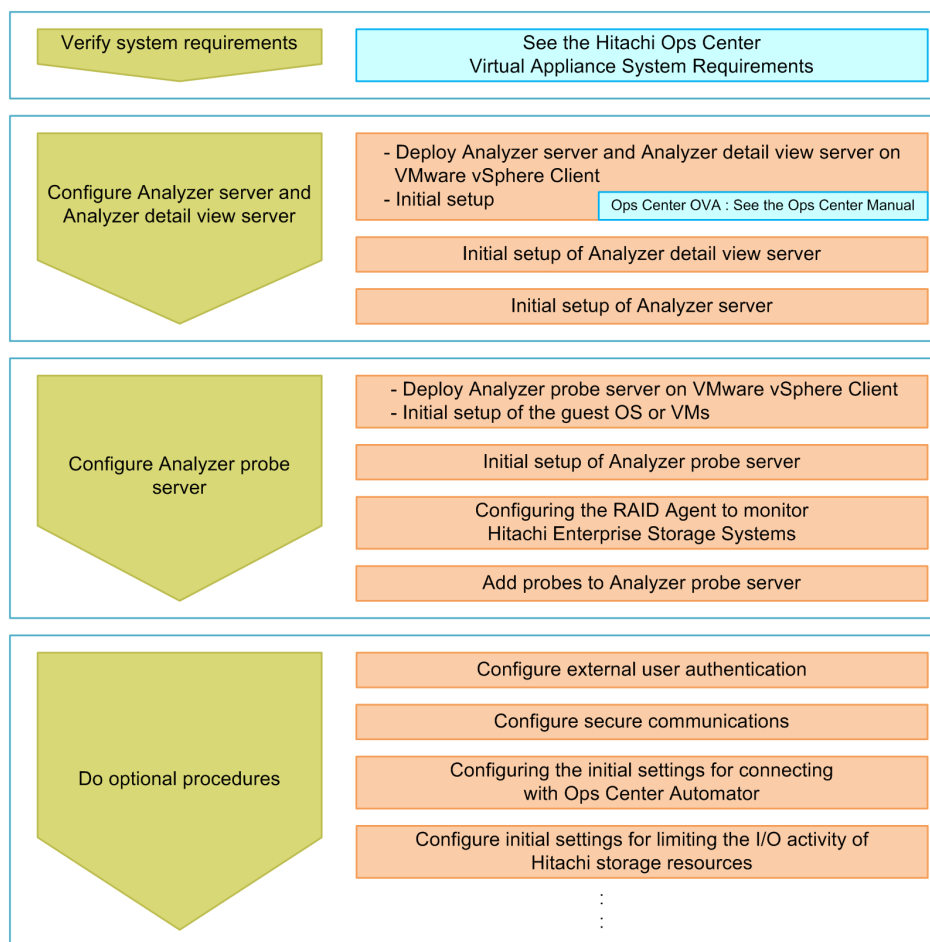
https://knowledge.hitachivantara.com/Documents/Management_Software/Ops_Center

Workflow for installing and using a virtual appliance

The following figure shows the workflow for creating an Ops Center Analyzer system by using a virtual appliance.

If you use the Ops Center consolidated OVA, Ops Center Analyzer is automatically registered in Common Services on the same host. However, in the following cases, you must manually register Ops Center Analyzer in Common Services after the installation.

- When you use Common Services on a different host
- When you use Common Services in the environment configured with Analyzer OVA



Installing Ops Center Analyzer and Analyzer detail view servers (VMware vSphere Client)

By deploying the OVA file (Analyzer OVA), you can create a virtual machine on which the Analyzer server and the Analyzer detail view server are installed.

Before you begin

- Review the requirements for the Analyzer server and the Analyzer detail view server (hardware and software).
- Check the hardware requirements for the virtual machine. For details, see [Default settings for the virtual machine and guest operating system \(on page 54\)](#).

Procedure

1. From a VMware vSphere client, log in to the VMware ESXi server.
2. Deploy the Analyzer OVA (`AnalyzerVM_version.ova`) by selecting **File > Deploy OVF Template**, and then following the prompts.
3. To avoid IP address conflicts when the virtual machine starts, you must change the settings so that the machine does not connect to the network.

You can skip this step if you are sure that the IP addresses will not conflict.

When deployment is complete, the following are set by default for the virtual machine:

- IP address: 172.30.197.92
- Network mask: 255.255.0.0
- Default gateway: 172.30.0.1
 - a. Right-click the new virtual machine, and select **Edit Settings**.
 - b. In the **Hardware** tab, select **Network adapter 1**, and then clear the **Connect at power on** check box.
- 4. Start the virtual machine.
- 5. If you changed the settings in step 3 so that the virtual machine does not connect to the network when it starts, perform the following steps:
 - a. Right-click the virtual machine, and select **Edit Settings**.
 - b. In the **Hardware** tab, select **Network adapter 1**, and then check the **Connect at power on** check box.

Running the setup tool (opsvmsetup)

After you complete the OVA deployment, run the setup tool (opsvmsetup) to complete the initial setup.

You can use the setup tool to set the following:

Network settings

- Host name
- IP address
- Default gateway
- Network mask
- DNS server (up to two servers)

Time settings

- Time zone
- NTP server

During initial setup, firewall settings for the service port are configured in addition to the network and time settings for the guest OS, and SSL settings.

**Note:**

- You can run the setup tool only once. Afterwards, you must use the operating system commands to change the settings.
- The setup tool only supports IPv4 addresses.
- Specify the time zone in the *area/location* format. If you do not know the proper values, use the following command to check the time zone values before running the setup tool:

```
timedatectl list-timezones
```

Procedure

1. From the VMware vSphere client, log in to the guest operating system using the following user ID and temporary password:

User ID: `root`

Password: `manager`

After logging in, you must change the root password.

2. Run the setup tool: `opsvmsetup`.
3. Specify the values as prompted.
When you are finished, a list of the settings is displayed.
4. Check the settings, enter `y`, and then apply the settings.
The guest operating system restarts automatically.
5. If you changed the settings so that the virtual machine is not connected to the network when deployed, enable the network adapter:
 - a. Log in to the guest operating system, and then stop the virtual machine by using the `shutdown` command.
 - b. From the VMware vSphere client, click **Power On the virtual machine**.

Default settings for the virtual machine and guest operating system

When you deploy the OVA file (Analyzer OVA), the necessary settings for the Analyzer server and the Analyzer detail view server are specified for the virtual machine and guest OS.

Confirm whether the virtualization server has sufficient resources to create the virtual machine.

Item	Settings
CPU	16 cores
Memory	32 GB
Disk size	800 GB

The following table lists the defaults for the guest operating system. To change the settings for the Analyzer server and the Analyzer detail view server after deployment, change the operating system settings as needed.

Item	Settings
Operating system version	Oracle Linux For details about the latest operating system version, see the <i>Hitachi Ops Center Virtual Appliance System Requirements</i> .
Installed libraries	Prerequisite libraries required for the Analyzer server and the Analyzer detail view server included in the Analyzer OVA.
Kernel parameters	Values required for the Analyzer server and the Analyzer detail view server included in the Analyzer OVA.
Registering firewall exceptions	In addition to the ports that are registered as exceptions by the operating system, the ports that must be registered as exceptions for each of the products.

Installing Analyzer probe server (VMware vSphere Client)

By deploying the OVA file for an Analyzer probe server, you can create a virtual machine on which the Analyzer probe server is installed.

Before you begin

- Review the Analyzer probe server requirements (hardware and software).
- Make sure that the ports you specify are available for communication. The default port is 8443. The default port for SSH is 22.
- If you use the Analyzer probe server in a DNS environment, exclude the domain name when specifying the host name because the Analyzer probe server does not support FQDN.

- Specify a static IP address for Analyzer probe server because the RAID Agent cannot run on hosts that use DHCP to assign IP addresses.
- When you run RAID Agent in a virtual environment:
 - Before setting up the RAID Agent, you must specify `C` for the `LANG` environment variable on the Analyzer probe server host.

At startup, RAID Agent is subject to the system `LANG` environment variable. If the `LC_ALL` environment variable differs from the `LANG` environment variable, either unset `LC_ALL` or change its value to match the `LANG` value. Use the following example as a reference when setting the `LANG` value for RAID Agent. The last line is an example of coding that unsets the `LC_ALL` value.

Example settings:

```
## Set Environment-variables
PATH=/sbin:/bin:/usr/bin:/opt/jplpc/bin
SHLIB_PATH=/opt/hitachi/common/lib
LD_LIBRARY_PATH=/opt/hitachi/common/lib
LIBPATH=/opt/hitachi/common/lib
HCCLIBCNF=/opt/jpl/hcclibcnf
LANG=C
export PATH SHLIB_PATH LD_LIBRARY_PATH LIBPATH HCCLIBCNF LANG
unset LC_ALL
```

- If you want to monitor VSP family or HUS VM, you must enable access from a guest OS to the command device. For details, see the documentation for your virtual system.

Use VMware vSphere Client file to add a device to the guest OS. By doing so, if you designate a command device as the device to be added, the command device can be accessed from the guest OS.

When configuring settings to add a device, make sure that the following requirements are met:

- Device type: Hard disk
- Disk selection: Raw device mapping
- Compatibility mode: Physical
- Virtual disks (including VMware VVols) are not used for the command device.



Note: If you do not want to collect performance information for the monitored storage systems using a command device, you do not need to configure these settings.

- When you use a virtualization system to replicate an OS environment in which the RAID Agent is running, do not apply the replicated environment to any other host. Startup of the RAID Agent might fail in the replicated environment.

Procedure

1. From a VMware vSphere client, log on to the VMware ESXi server.

2. Deploy the OVA file for Analyzer probe server from the installation media for virtual appliances.

From the VMware vSphere client, select **File > Deploy OVF Template**, and then follow the on-screen instructions.



Tip: We recommend selecting **Thick Provision Lazy Zeroed** in the window for selecting the disk provisioning method.

3. Change the settings so that the virtual machine does not connect to the network when started.

When deployment is complete, the following network settings will be set by default for the virtual machine. This operation is not required if you are sure that the IP addresses will not conflict.

- **IP address:** 10.197.74.209
- **Net mask:** 255.255.255.0
- **Default gateway:** 10.197.74.1
 - a. Right-click the virtual machine that you want to edit, and then select **Edit Settings**.
 - b. In the **Hardware** tab, select **Network adapter 1**, and then clear the **Connect at power on** check box.

4. Start the virtual machine.

When you log on for the first time, use the following user ID and password:

User ID: `root`

Password: `manager`

After you log on, you must change the root password.

5. Confirm that the network setting is correct.

Next steps

Run the setup tool on the guest OS, and then specify the initial settings for the guest OS.

Initial setup of the guest OS or VMs

After deploying the virtual appliance, run the setup tool (`hvaconfig`) to specify the initial settings for the guest OS.

Procedure

1. From the VMware vSphere Client, log on to the guest OS.
2. Run the **`hvaconfig`** command that is stored in `/opt/HIAA/vmtool`.



Note: You can run the setup tool only once. To change the settings after running the setup tool, use the operating system commands.

3. In the setup tool, you can specify the following settings.

■ **Network settings:**

- Host name: The Analyzer probe server does not support FQDNs. Omit the domain name when specifying the host name.
- DHCP: RAID Agent does not support the use of DHCP. If you are using RAID Agent, specify `n`.
- IP address: The setup tool specifies an IPv4 address.
- Default gateway
- Network mask
- DNS server (2 servers maximum)

■ **Time settings:**

- Time zone
 - Specify the time zone in the *area/location* format. If you do not know the specifiable values, use the following command in advance to check the time zone values that can be set:

```
timedatectl list-timezones
```

- The times and time zones of the following servers must be synchronized:
 - Analyzer server
 - Analyzer detail view server
- NTP server

■ **Security setting:**

- Server certificate

4. Check the contents of the list that displays your specified settings, and then apply the settings.

After the settings are applied, the guest OS restarts automatically.

5. If the virtual machine is not connected to the network when deployed, perform the following steps to enable the network adapter:

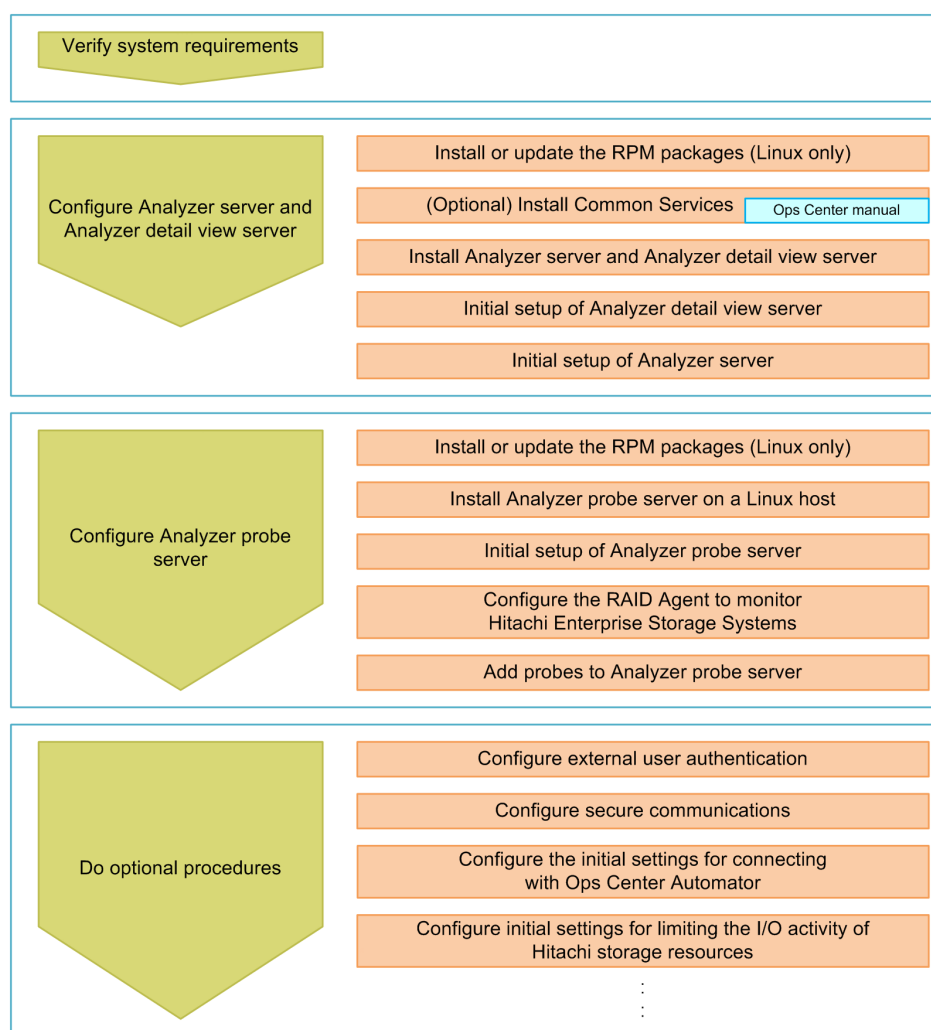
- a. Log on to the guest OS.
- b. Stop the virtual machine by running the **shutdown** command.
- c. Right-click the virtual machine that you want to stop, and then select **Edit Settings**.
- d. In the **Hardware** tab, select **Network adapter 1**, and then select the **Connect at power on** check box.
- e. Run the **Power On the virtual machine**.

Chapter 4: Installation by using the installer

Install Ops Center Analyzer components using the installer.

Workflow for installing using an installer

The following figure shows the workflow for creating an Ops Center Analyzer system by using the installer.



Installing or updating the RPM packages (Linux OS)

Before installing or upgrading the Analyzer server, Analyzer detail view server, or Analyzer probe server, check whether all of the RPM packages required for each component are installed. If some packages are missing, you must install them as an additional step. You can obtain the RPM packages from the Linux OS media or the distribution website, such as for Red Hat Enterprise Linux.

- For details about the RPM packages required for each component, see [Analyzer server requirements \(Linux\) \(on page 25\)](#), [Analyzer detail view server requirements \(on page 28\)](#), or [Analyzer probe server requirements \(on page 30\)](#).
- The package `nss-3.21.0` may not be included in the Linux OS media of certain versions. Obtain this package from the Linux OS media for version 6.8 or later, or from the distribution website.
- If the `libstdc++` package is already installed in the environment in which the Analyzer probe server will run, you might not be able to install `libstdc++.i686` and an error message such as the following might be output:

```
Protected multilib versions: libstdc++-xx.xx.xx-xx.xx.el6.i686 !=
libstdc++-yy.yy.yy-yy.yy.el6.x86_64
```

This error occurs because the version of the `x86_64` package (the 64-bit library) differs from that of the `i686` package (the 32-bit compatibility library). If this happens, update `x86_64` (the 64-bit library), and then retry the installation of `libstdc++`.

```
yum update libstdc++.x86_64
```

Installing or updating the packages by using the Linux OS media

The following describes how to install or update the RPM packages by using the Linux OS media. Change the information that you must specify in the procedure according to the environment you are using.

1. Mount the Linux OS media and obtain the RPM packages:

```
mkdir /media/OSImage
mount /dev/cdrom /media/OSImage
```

2. Configure the yum repository:

```
touch /etc/yum.repos.d/OSImage.repo
echo [dvd]>>/etc/yum.repos.d/OSImage.repo
echo name=dvd>>/etc/yum.repos.d/OSImage.repo
echo baseurl=file:///media/OSImage/>>/etc/yum.repos.d/OSImage.repo
echo gpgcheck=0>>/etc/yum.repos.d/OSImage.repo
echo enabled=1>>/etc/yum.repos.d/OSImage.repo
```

3. Run the **yum** command to install or update the packages and package group:

- **For packages:**

```
yum install package-to-be-installed
```

Example:

```
yum install java-1.8.0-openjdk-devel sysstat zip
```

- **For the package group:**

```
yum group install package-group-to-be-installed
```

4. Unmount the Linux OS media:

```
umount /media/OSImage/  
rm /etc/yum.repos.d/OSImage.repo
```

Installing or updating the packages using the distribution website

The following describes how to install or update the RPM packages by using the distribution website. Change the information that you must specify in the procedure according to the environment you are using.

1. Specify the repository to which the **yum** command is to connect.

For Red Hat Enterprise Linux, register the system by using Red Hat Subscription Management. For details, see <https://access.redhat.com/articles/11258>.

For Oracle Linux, the initial settings are set by default (the file `repo` is already located in the directory `/etc/yum.repos.d`). For details, see <http://yum.oracle.com/getting-started.html>.

2. If you are using a proxy, specify the proxy for the **yum** command.

- a. Add the following information to the `/etc/yum.conf` file:

```
proxy=http://host-name:port-number  
proxy_username=user-name  
proxy_password=password
```

- b. Clear the cache for the **yum** command.

```
yum clean all
```

3. Run the **yum** command to install or update the packages and package group.

- **For packages:**

```
yum install package-to-be-installed
```

Example:

```
yum install java-1.8.0-openjdk-devel sysstat zip
```

- **For the package group:**

```
yum group install package-group-to-be-installed
```

Increasing the maximum number of open files (Linux OS)

Before installing the Analyzer detail view server or Analyzer probe server on a Linux host, the minimum value of the system-wide and user-level limits on the number of open files must be set to 65535 or greater.

The recommended values are:

System-wide: 327675

User-level: 262140

Procedure

1. Log on as follows:
 - a. If you are installing the Analyzer detail view server or Analyzer probe server for the first time, log on to the Linux machine as **root**.
 - b. If you are performing this task post-installation or while upgrading, log on to the Analyzer detail view server or Analyzer probe server through an SSH client (like **putty**) as a root user.
2. Run the following command to check the system-wide kernel limit:



Note: The recommended kernel limit is 327675.

```
sysctl -a | grep fs.file-max
```

If the value is 65535 or greater, skip to step 3. Otherwise, do the following:

- a. Navigate to the `/etc` directory and create the `sysctl.d` directory if it does not exist:

```
mkdir sysctl.d
```

- b. Navigate to the `/etc/sysctl.d` directory and create the `sysctl.conf` file if it does not exist.

- c. Ensure that the `fs.file-max` property is present in the `sysctl.conf` file and the value is set to 65535 or greater.
- d. Run the following command to apply the revised configuration:

```
sysctl -p /etc/sysctl.d/sysctl.conf
```

3. Run the following command to check the user-level limit:



Note: The recommended user-level limit is 262140.

```
ulimit -a | grep -i open
```

If the value is less than 65535, then do the following:

- a. Navigate to the `/etc/security/limits.d` directory and create the following file, if it does not exist:
 - Create `90-nproc.conf` file, if you are using Red Hat Enterprise Linux and Oracle Linux version earlier than 7.0.
 - Create `20-nproc.conf` file, if you are using Red Hat Enterprise Linux and Oracle Linux version 7.0 or later.
- b. Ensure that the following two properties are present in the `90-nproc.conf` or `20-nproc.conf` file and set their values as follows:

```
* soft nofile 65535
* hard nofile 65535
```

4. If you changed the system-wide kernel or user-level limits on the Analyzer detail view machine, you must restart the machine.

Installing Ops Center Analyzer and Analyzer detail view servers (Linux OS)

To install the Analyzer server and Analyzer detail view server on a Linux host, run the installer and follow the prompts. You can install the Analyzer server and the Analyzer detail view server at the same time by using the installer (`analytics_install.sh`), or you can choose to install only one of the components.

The installer starts and stops the `crond` service. Therefore, do not run any operations that use the `crond` service when the installer is running.

Before you begin

Before you begin installation of Analyzer server on a Linux host, review the following prerequisites:

- Review the Analyzer server requirements (hardware and software).
- Verify that you can resolve the IP address from the host name of the Analyzer server.
Check the `hosts` file or the domain name system (DNS) server configuration of the host on which the Analyzer server is installed.
- Make sure that the ports you specify are available for communication. The default ports are 22015 (non-SSL) and 22016 (SSL).
- Verify that you have root permission to run the installer and the precheck tool.
- Make sure that the console and clock properties are set to the same time zone.
- Ensure the times and time zones of the following servers are synchronized:
 - Analyzer server
 - Analyzer detail view server
- During installation, when prompted to specify the installation directory for the Analyzer server, observe the following rules:
 - Specify a directory name of less than 94 bytes.
 - Use the following characters:
`A-Z a-z 0-9 / underscore ()` (space character not allowed)
 - Do not use a path separator (/) at the end of a path.
- Make sure that the `/tmp` directory was mounted without the `noexec` option.

Before you begin installation of Analyzer detail view server on a Linux host, review the following prerequisites:

- Review the Analyzer detail view server requirements (hardware and software).
- Prepare an external drive or LVM logical volume for installing the Analyzer detail view server. For details about disk space requirements, see the Analyzer detail view server requirements.
- Make sure that the ports you specify are available for communication. The default port is 8443.
- Verify that you have root permission to run the installer and the precheck tool.
- Verify that group and other users have read and execute permissions (755) for the installation path directories.
- Make sure that the console and clock properties are set to the same time zone.
- Ensure the times and time zones of the following servers are synchronized:
 - Analyzer server
 - Analyzer detail view server
- Do not change the time zone after installing Analyzer detail view server.

- Specify a directory name of less than 94 bytes for the installation destination directory.
- Check the kernel and system limits on the number of open files and processes. Refer to [Increasing the maximum number of open files \(Linux OS\) \(on page 62\)](#) for more information.

Procedure

1. Stop any security monitoring software, antivirus software, and process monitoring software.
2. Mount the Hitachi Ops Center installation media and copy the directories and files in the `ANALYTICS` directory on the installation media to a directory on the Linux host.



Note:

- The following characters can be used in the path of the directory to which the installer is copied: A-Z a-z 0-9 - . _
- Space characters cannot be used.

In the following example, if the `/root/ANALYTICS` directory already exists, create a new directory, and then perform the subsequent steps in the new directory.

```
mkdir /media/OpsImage
mount /dev/cdrom /media/OpsImage
cp -rT /media/OpsImage/Analyzer/ANALYTICS /root/ANALYTICS
```

3. Move to the `/root/ANALYTICS` directory.

```
cd /root/ANALYTICS
```

4. Run the precheck tool as a root user to check whether the Analyzer server and Analyzer detail view server can be installed.

```
sh ./analytics_precheck.sh
```



Note: When you run the precheck tool, it checks the static information of the system environment.

If `OK` is displayed in `[Check results]`, you can start the installation. If `NG` is displayed, make sure the system requirements have been met.

Output example when the Ops Center Analyzer version is 10.0.0:

```
=====
Analytics Precheck                               ver. 10.0.0-00
=====

[ Check results ]
Ops Center Analyzer detail view server [10.0.0-00]      [OK]
Ops Center Analyzer server [10.0.0-00]                  [OK]
```

```
[ Details ]
Check premise OS version.                                [OK]
      :
      :
```

If the `-v` option is specified, information such as the host name and the OS name is also displayed.

5. Run the following command as root to start the installation:

```
sh ./analytics_install.sh NEW
```

A message is displayed, confirming that you want to install the Analyzer detail view server and Analyzer server.

6. Enter `y`, and then specify the components that you want to install.



Tip: The prompt displays the default value. To use the default value, simply press the **Enter** key.

```
Do you want to install the Ops Center Analyzer detail view server?
(y/n) [n]: y
```

```
Do you want to install the Ops Center Analyzer server? (y/n) [n]: y
```

```
[Confirmation]
```

```
-----
Installation Product
```

```
(1) Ops Center Analyzer detail view server
```

```
(2) Ops Center Analyzer server
-----
```

```
Do you want to install the server listed above? (y/n) [n]: y
```

7. You are prompted for a drive and directory to install the Analyzer detail view server. The following describes how to specify a device as the installation destination:

- **To specify a physical device:** The device file name (Example: `sdb`)
- **To specify a logical device that uses the device-mapper functionality (devices in a configuration such as LVM, multipath, or RAID):** The device name of the terminal (whose TYPE is `lvm` or `mpath` or `raid`) as displayed in the tree in <System device information> (Example: `DCAvg-DCAlv00`)

```
[INFO] Analytics installer started
```

```
=====
Installation of the Ops Center Analyzer detail view server
=====
```

```
[INFO] Installation of the Ops Center Analyzer detail view server
started.
```

```
[Partition parameter]
-----
<System device information>
NAME          MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
sdb            8:16   0  100G  0 disk
sr0           11:0    1 1024M  0 rom
fd0            2:0    1    4K  0 disk
sda            8:0    0   80G  0 disk
|-sda2         8:2    0   79G  0 part
| |-ol-swap 252:1    0    2G  0 lvm  [SWAP]
| |-ol-home 252:2    0   27G  0 lvm  /home
| `--ol-root 252:0    0   50G  0 lvm  /
`--sda1        8:1    0    1G  0 part /boot

Specify the device name in which to store application data. [sdb]:
Product required: 153600MB
Free: 102400MB
The size of the specified device is less than the recommended size.
Do you want to continue the installation? (y/n) [n]: y

Specify the directory in which to store application data.
File permissions for all files in the top-level directory and below
will be changed to 'megha:megha'. [/data]:
```

8. When prompted, enter *y* to configure the firewall settings. Specify the IP addresses of the Analyzer probe servers. You can also accept the default value 0.0.0.0 and configure the IP addresses later:

```
[Firewall parameter ]
-----
Do you want to configure the firewall to accept connections from the
Ops Center Analyzer probe servers? (y/n) [y]: y

Specify the IP addresses of the Ops Center Analyzer probe servers,
so that these IP addresses will be added in the configuration of
iptables,
and the connection from these servers can be accepted. (port 22/tcp)
You can also use 0.0.0.0 and change it later.
[0.0.0.0]:
```

9. Specify the information to use for secure communication of the Analyzer detail view server.

To apply the default settings, press the **Enter** key in each prompt window.

```
[Keytool parameter ]
-----
[INFO] This setting is for SSL configuration.
What is the name of your organizational unit? [Unknown]:
organizational-unit
What is the name of your organization? [Unknown]: organization
```

```
What is the name of your City or Locality? [Unknown]: city-or-locality
What is the name of your State or Province? [Unknown]: state-or-
province
What is the two-letter country code for this unit? [Unknown]: two-
letter-country-code-for-unit
```

10. Verify the settings that you specified:

```
[Confirmation]
-----
Installation directory      : /data
Device name                 : /dev/sdb
Filesystem                  : xfs
Mount point                 : /data
Port number                 : 8443
Firewall accept rule to be added :
  Protocol Source IP       Destination IP   Destination PORT
  -----
  ALL      0.0.0.0          0.0.0.0        ALL <RELATED,ESTABLISHED>
  TCP      0.0.0.0          0.0.0.0        22
  TCP      0.0.0.0          0.0.0.0        8443
Required CPAN libraries     : Module::Build YAML Log::Log4perl
LWP::Protocol::https
Distinguished Name for keytool : CN=host-name, OU=organizational-
unit, O=organization, L=city-or-locality, ST=state-or-province, C=two-
letter-country-code-for-unit
-----
```

11. Check the CAUTION message.

```

** CAUTION **

* This installation will delete all the partitions on the disk.
(/dev/sdb)

* This installation will change iptables settings. (Listing above)

* Installation of the required CPAN libraries may take more than 4
minutes.
```

12. Unless the CAUTION message includes a problem that requires your attention, enter y.

```
Do you want to continue the installation? (y/n) [n]: y
```

Analyzer detail view server is installed, and then the following message is displayed.

```
[INFO] Installation of the Ops Center Analyzer detail view server
finished successfully.
```

13. You are prompted for a directory in which to install Analyzer server.

```
=====
Installation of the Ops Center Analyzer server
=====
[INFO] Installation of the Ops Center Analyzer server started.
Specify the directory to store application data. [/opt/hitachi]:
```

14. When prompted, enter `y` to configure the firewall settings.

```
[Firewall parameter ]
-----
Do you want to configure the firewall to accept connections to the Ops
Center Analyzer server? (y/n) [y]: y

The Ops Center Analyzer server sets 22015 and 22016 port as the
default port.
This port can be changed after installation.
If you change the port number, you must change the firewall setting.
```

15. If there are no problems with the specified settings, enter `y`.

```
Do you want to continue the installation? (y/n) [n]: y
```

Analyzer server is installed, and then the following message is displayed.

```
[INFO] Analytics installer finished.
```

Installing Analyzer server (Windows OS)

Start the wizard to install Analyzer server.

Before you begin

Review the following prerequisites:

- Review the Analyzer server requirements (hardware and software).
- The times and time zones of the following servers must be synchronized:
 - Analyzer server
 - Analyzer detail view server

Procedure

1. Log on to the host where you plan to install the Analyzer server as the Administrator user.
2. Stop any security monitoring software, antivirus software, and process monitoring software.

3. Run `ANALYTICS.msi` on the installation media to start installer. An installation wizard appears.
4. Go through the on-screen prompts and specify the required information to complete the installation.



Note: You cannot install Analyzer server on removable media, network drives, and UNC paths. In addition, you cannot use reserved words for the OS (such as CON, AUX, PRN, or NUL) as a file name or a directory name.

Installing Analyzer probe server (Linux OS)

To install the Analyzer probe server on a Linux host, run the installer (`dcaprobe_install.sh`) and follow the prompts.

The installer starts and stops the `crond` service. Therefore, do not run any operations that use the `crond` service when the installer is running.

Before you begin

Review the following prerequisites:

- Review the Analyzer probe server requirements (hardware and software).
- Install the Analyzer detail view server first. The Analyzer detail view server IP address is required for setting up the Analyzer probe server.
- Make sure that the ports you specify are available for communication. The default port is 8443. (The default port for SSH is 22.)
- Verify that you have root permission to run the installer and the precheck tool.
- Group and other users must have read and execute permissions (755) for the installation path directories.

- Check the kernel and system limits on the number of open files and processes. Refer to [Increasing the maximum number of open files \(Linux OS\) \(on page 62\)](#) for more information.
- When you install the Analyzer probe server, the RAID Agent is installed automatically. Review the RAID Agent requirements before you begin installation.
 - The installation directory is fixed (`/opt/jp1pc`) and cannot be changed. Make sure that the directory is empty. Do not include any symbolic links in the installation path.
 - Make sure that the following directories were mounted without the `noexec` option:
 - `/tmp`
 - `/var`
 - When you install the RAID Agent, a temporary work directory `jp1pc_AGT` is created in the `/opt` or `/opt/jp1pc` directory. (This directory is automatically deleted after the installation is successful.)

If an error occurs during installation, verify the directory exists and delete it manually.

- The IP address must be able to be resolved from the host name of the host on which RAID Agent is installed. Check the `hosts` file or the domain name system (DNS) server configuration of the host on which RAID Agent is installed.
- The RAID Agent cannot run on hosts that use DHCP to assign IP addresses. Therefore, you must specify a fixed IP address for Analyzer probe server.
- The Analyzer probe server can be used in a DNS environment but does not support FQDN. Therefore, you must exclude the domain name when you specify the host name.
- Before setting up the RAID Agent, you must specify `C` for the `LANG` environment variable on the Analyzer probe server host.

At startup, RAID Agent is subject to the system `LANG` environment variable. If the `LC_ALL` environment variable differs from the `LANG` environment variable, either unset `LC_ALL` or change its value to match the `LANG` value. Use the following example as a reference when setting the `LANG` value for RAID Agent. The last line is an example of coding that unsets the `LC_ALL` value.

Example settings:

```
## Set Environment-variables
PATH=/sbin:/bin:/usr/bin:/opt/jp1pc/bin
SHLIB_PATH=/opt/hitachi/common/lib
LD_LIBRARY_PATH=/opt/hitachi/common/lib
LIBPATH=/opt/hitachi/common/lib
HCCLIBCNF=/opt/jp1/hcclibcnf
LANG=C
export PATH SHLIB_PATH LD_LIBRARY_PATH LIBPATH HCCLIBCNF LANG
unset LC_ALL
```

Procedure

1. Stop any security monitoring software, antivirus software, and process monitoring software.
2. Mount the Hitachi Ops Center installation media and copy the directories and files in the `DCAPROBE` directory on the installation media to a directory on the Linux host.



Note:

- The following characters can be used in the path of the directory to which the installer is copied: A-Z a-z 0-9 - . _
- Space characters cannot be used.

In the following example, if the `/root/DCAPROBE` directory already exists, create a new directory, and then perform the subsequent steps in the new directory.

```
mkdir /media/OpsImage
mount /dev/cdrom /media/OpsImage
cp -rT /media/OpsImage/DCAPROBE /root/DCAPROBE
```

3. Move to the `/root/DCAPROBE` directory.

```
cd /root/DCAPROBE
```

4. Run the precheck tool as a root user to check whether the Analyzer probe server can be installed:

```
sh ./dcaprobe_precheck.sh
```



Note: When you run the precheck tool, it checks the static information of the system environment.

If `OK` is displayed in `[Check results]`, you can start the installation. If `NG` is displayed, make sure the system requirements have been met.

Output example when the Ops Center Analyzer version is 10.0.0:

```
=====
Ops Center Analyzer probe Precheck          ver. 10.0.0-00
=====

[ Check results ]
Ops Center Analyzer probe server [10.0.0-00]          [OK]

[ Details ]
Check resolved hostname. [host-name (IP-address)]    [OK]
Check premise OS version.                             [OK]
:
:
```

If the `-v` option is specified, information such as the OS name is also displayed.

5. Run the following command as root to start the installation:

```
sh ./dcaprobe_install.sh NEW
```

6. Specify a directory to install the Analyzer probe server:



Tip: The prompt displays the default value. To use the default value, press the **Enter** key only.

Specify the path of the directory in which to store application data.
[/home]:

7. Specify **y** to configure the firewall settings:

Do you want to configure the firewall to accept connections from the
Ops Center Analyzer probe servers? (y/n) [y]: y

8. Specify the information to use for secure communication of Analyzer probe server.
To apply the default settings, press the **Enter** key in each prompt window.

```
[Keytool parameter ]
-----
[INFO] This setting is for SSL configuration.
What is the name of your organizational unit? [Unknown]:
organizational-unit
What is the name of your organization? [Unknown]: organization
What is the name of your City or Locality? [Unknown]: city-or-locality
What is the name of your State or Province? [Unknown]: state-or-
province
What is the two-letter country code for this unit? [Unknown]: two-
letter-country-code-for-unit
```

9. Verify the settings that you specified:

The number of CPAN libraries to be installed varies depending on the environment.

```
[Confirmation]
-----
Data directory (for the RAID Agent)           : /home/RAIDAgent
Data directory (for the Ops Center Analyzer probe server): /home
Port number (for the Ops Center Analyzer probe server): 8443,24221
Firewall accept rule to be added              :
  Protocol Source IP      Destination IP  Destination PORT
  -----
  ALL      0.0.0.0         0.0.0.0         ALL <RELATED,ESTABLISHED>
  TCP      0.0.0.0         0.0.0.0         24221
  TCP      0.0.0.0         0.0.0.0         8443
  TCP      10.197.195.109  10.197.195.109  ALL
  TCP      127.0.0.1       127.0.0.1       ALL
Required CPAN libraries                       : Module::Build YAML
IO::Pty Date::Calc Net::OpenSSH DateTime DateTime::Format::Strptime
```

```
Date::Gregorian Log::Log4perl Log::Dispatch::FileRotate Sys::RunAlone
LWP::Protocol::https
Distinguished Name for keytool           : CN=host-name,
OU=organizational-unit, O=organization, L=city-or-locality, ST=state-
or-province, C=two-letter-country-code-for-unit
-----
```

10. Check the CAUTION message.

```

** CAUTION **

* This installation will change iptables settings. (Listing above)

* Installation of the required CPAN libraries may take more than 12
minutes.
```

11. Unless the CAUTION message includes a problem that requires your attention, enter y.

```
Do you want to continue the installation? (y/n) [n]: y
```



Note: Installation of the CPAN library Net::OpenSSH package might display the following prompt:

```
root@localhost's password:
```

You should ignore this prompt and the installation process will resume in approximately ten seconds.

When the process is complete, the following message is displayed:

```
[INFO] Installation of the Ops Center Analyzer probe servers finished
successfully.
```

Linux environment changed by the installer

When you run the Ops Center Analyzer installer, the installer internal processing changes the environment setting of the host when you install the Analyzer detail view server or the Analyzer probe server.



Note: The installer does not make any changes when you install the Analyzer server.

Analyzer detail view server

When you install the Analyzer detail view server by using the installer, the installer makes the following changes to the host environment settings.

Change	Details
Addition of users	<p>The following users are added:</p> <ul style="list-style-type: none">▪ megha▪ meghadata <p>You must change the default passwords. Refer to Changing the megha and meghadata passwords (on page 88) for more information.</p>
Addition of groups	<p>The following group is added: megha.</p>
Changes to the cron settings	<p>A setting that periodically starts the service and monitors resource usage for the Analyzer detail view server is added.</p>
Changes to the ssh settings	<p>The file <code>/etc/ssh/sshd_config</code> is edited, and settings are specified to allow the user meghadata to access the Analyzer detail view server by using password authentication.</p>

Change	Details
Kernel parameter settings	<p>The following kernel parameters are set:</p> <ul style="list-style-type: none"> Maximum number of file descriptors for the entire system If the maximum number of file descriptors for the entire system specified in the OS is less than 327675, 327675 is specified in the following definition files: <ul style="list-style-type: none"> For Red Hat Enterprise Linux 7.0 or later, or for Oracle Linux 7.0 or later: <code>/usr/lib/sysctl.d/60-hiaa.conf</code> For any other Linux OS: <code>/etc/sysctl.d/60-hiaa.conf</code> Maximum number of file descriptors for the user megha If the maximum number of file descriptors for the user megha specified in the OS is less than 262140, 262140 is specified in the following definition files: <code>/etc/security/limits.conf</code> Maximum number of processes for the user megha If the maximum number of processes specified in the OS for the user megha is less than 2048, 2048 is specified in the following definition file: <ul style="list-style-type: none"> For Red Hat Enterprise Linux 7.0 or later, or for Oracle Linux 7.0 or later: <code>/etc/security/limits.d/20-nproc.conf</code> For any other Linux OS: <code>/etc/security/limits.d/90-nproc.conf</code>

Change	Details
	These maximum values can be specified in multiple definition files. If these maximum values are specified in any file that has a higher priority than the files listed here, you must change those settings manually.
Automatic startup settings for the Analyzer detail view server service	A setting that automatically starts the service when the OS is started is added to <code>/etc/rc.local</code> .
Installation of the Perl module	<p>The Analyzer detail view server uses the Perl module registered in CPAN (Comprehensive Perl Archive Network). If the Perl module is not installed as follows in the default path on the host where Analyzer detail view server is installed, the module is installed as part of the installation of Analyzer detail view server.</p> <ul style="list-style-type: none"> Module::Build YAML XML::Simple Log::Log4perl LWP::UserAgent LWP::Protocol::https <p>Required prerequisite perl modules are also installed.</p>

Analyzer probe server

When you install the Analyzer probe server by using the installer, the installer makes the following changes to the host environment settings.

Change	Details
Addition of users	<p>The following user is added:</p> <ul style="list-style-type: none"> megha <p>You must change the default password. Refer to Changing the megha and meghadata passwords (on page 88) for more information.</p>
Addition of groups	The following group is added: megha.

Change	Details
Changes to the cron settings	A setting that periodically starts the service and monitors resource usage for the Analyzer probe server is added.
Kernel parameter settings	<p>The following kernel parameters are set:</p> <ul style="list-style-type: none"> Maximum number of file descriptors for the entire system If the maximum number of file descriptors for the entire system specified in the OS is less than 327675, 327675 is specified in the following definition files: <ul style="list-style-type: none"> For Red Hat Enterprise Linux 7.0 or later, or for Oracle Linux 7.0 or later: <code>/usr/lib/sysctl.d/60-hiaa.conf</code> For any other Linux OS: <code>/etc/sysctl.d/60-hiaa.conf</code> Maximum number of file descriptors for the user megha If the maximum number of file descriptors for the user megha specified in the OS is less than 262140, 262140 is specified in the following definition files: <code>/etc/security/limits.conf</code> Maximum number of processes for the user megha If the maximum number of processes specified in the OS for the user megha is less than 2048, 2048 is specified in the following definition file: <ul style="list-style-type: none"> For Red Hat Enterprise Linux 7.0 or later, or for Oracle Linux 7.0 or later: <code>/etc/security/limits.d/20-nproc.conf</code> For any other Linux OS: <code>/etc/security/limits.d/90-nproc.conf</code>

Change	Details
	These maximum values can be specified in multiple definition files. If these maximum values are specified in any file that has a higher priority than the files listed here, you must change those settings manually.
Automatic startup settings for the Analyzer probe server service	A setting that automatically starts the service when the OS is started is added to <code>/etc/rc.local</code> .
Installation of the Perl module	<p>The Analyzer probe server uses the Perl module registered in CPAN (Comprehensive Perl Archive Network). If the Perl module is not installed as follows in the default path on the host where Analyzer probe server is installed, the module is installed as part of the installation of Analyzer probe server.</p> <ul style="list-style-type: none"> ▪ Module::Build ▪ YAML ▪ IO::Pty ▪ Date::Calc ▪ Net::OpenSSH ▪ DateTime ▪ DateTime::Format::Strptime ▪ Date::Gregorian ▪ Log::Log4perl ▪ Log::Dispatch::FileRotate ▪ Sys::RunAlone ▪ HTTP::Request ▪ LWP::UserAgent ▪ LWP::Protocol::https ▪ Time::HiRes ▪ XML::Simple <p>Required prerequisite perl modules are also installed.</p>

Chapter 5: Initial setup after installation

After installing the Ops Center Analyzer components, continue with the setup of Ops Center Analyzer detail view, the Analyzer probe server, Analyzer server, the environment for Storage I/O controls feature, and Granular Data Collection.

Initial setup of Analyzer detail view server

Open the URL of the Analyzer detail view server and follow the prompts.

Before you begin

- Check the IP address of the Analyzer detail view server.
- Obtain the Analyzer detail view license from your Hitachi Vantara representative.

Procedure

1. Enter the Analyzer detail view server URL in your browser:
`https://ip-address:port-number`
The default port for HTTPS access is 8443.
2. Read and accept the license agreement, and then click **Next**.
3. In the **Upload License** window, click **Choose File** to browse to the license file and click **Open**.
4. Click **Submit** to register the license.
5. In the **Set Details For Existing admin User** window, enter the password, select the locale, and then click **Submit**. (The user name for the built-in administrator account is `admin`.)



Note: The current version of Ops Center Analyzer detail view supports only the English locale.

6. In the Analyzer detail view server login window, enter the administrator user credentials and click **Login**.
7. In the **Select Time zone** window, select the appropriate time zone and click **Next**. The Analyzer detail view server home page is displayed.



Note: Reports display data using the time zone of the Analyzer detail view server (not that of the storage systems). For example, if the Analyzer detail view server UI time zone is configured to IST, reports will use IST time regardless of where individual storage systems are located.

8. (Optional) Configure an alert notification email or Syslog to monitor the downloader and import delay, license expiration, and system memory usage. Configure SNMP for performance-based alerts. For information, see "Monitoring Analyzer detail view server alerts" in the *Analyzer detail view server Online Help*. For instructions on setting up the mail server, see "Configuring the SMTP server" in the online help.
9. (Optional) Create an Analyzer server account that belongs to the Administrator group on the Analyzer detail view server.

For information about how to add accounts, see the *Analyzer detail view server Online Help*. If you use the built-in administrator account to access the Analyzer server, this step is unnecessary.



Note: Several accounts are created automatically in Analyzer detail view server when you configure Analyzer server for connecting with the Analyzer server. Do not change or delete the information of the following user accounts:

- HIAA_Server_Admin
- HIAA_REST_Admin
- HIAA_REST_Normal
- HIAA_GUI_Report

Initial setup of Analyzer probe server

Open the URL of the Analyzer probe server and follow the prompts.

Before you begin

- Check the IP address of the Analyzer detail view server.
- Check the IP address of the Analyzer probe server.
- Obtain the Analyzer detail view license from your Hitachi Vantara representative.

Procedure

1. Open your browser and enter the Analyzer probe server URL.
`https://Analyzer-probe-server-IP-address:8443`
2. When you first launch the Analyzer probe server UI, you see the license agreement details. Read it and then click **Next**.
3. In the **Upload License** window, click **Choose File** to browse to a license file and click **Open**.
4. Click **Submit** to add the license.
5. In the **Create Administrator Account** window, provide the following and then click **Submit**:
 - User name and password
 - First name, last name, and email address of the user

- **Locale:** Only the U.S. English locale is currently supported
- **Group:** Select `Admin` to create an administrator account



Note: To complete the Analyzer probe server configuration you must create a Local user with an administrator account. After creating the Local user you can add the desired Active Directory users.

6. In the **Analyzer probe login** window, enter the administrator user credentials and click **Login**.
7. The **Basic Information** window displays the Customer Name (which cannot be changed). Provide the following contact information and click **Next**:
 - Administrator Contact Name and email
 - Technical Contact Name and email
8. In the **Select Time zone** window, make a selection and then click **Next**.
9. In the **Primary Analyzer detail view Server Information** window, specify the following details:



Note:

- If you are connecting the Analyzer detail view server to the Analyzer probe server using the host name and a proxy server, you must add the IP address and host name of the Analyzer detail view server to the `/etc/hosts` file on the Analyzer probe server.
- If you edit the existing connection details, make sure that you update these details on the Analyzer detail view server by updating the downloader. For more information, refer to [Updating the downloader on the Analyzer detail view server \(on page 404\)](#)

- **Protocol:** **FTP**, **FTPS**, **SFTP**, or **HTTPS**.

The Analyzer detail view server supports SFTP and HTTPS protocols. If you are using an FTP or FTPS protocol, then make sure that the FTP or FTPS server is configured and you provide the FTP or FTPS server IP address in the **Host** field. The intermediate FTP or FTPS server must not be the same as the Analyzer detail view server.

If you are using SFTP and HTTPS protocols, refer to [Supported ciphers for Analyzer probe \(on page 38\)](#).

- **Host:** Analyzer detail view server or intermediate FTP server IP address.

If you are using intermediate FTP server as a primary server, then you must [configure the downloader \(on page 131\)](#) on the Analyzer detail view server to download the data from this FTP server.

- **Port:** Based on the selected protocol.

- **User:** User name for the host. For an Analyzer detail view server the user name is: `meghadata`



Note: If you are using an intermediate FTP server, the FTP user must have the required permission to create a new directory in the current working directory on the FTP server, after connecting to the FTP server.

- **Password:** Password for the host. For an Analyzer detail view server the default password is: `meghadata123`



Note: To improve security for the FTP account, you must change the `meghadata` default password. Refer to [Changing the megha and meghadata passwords \(on page 88\)](#) for more information.

- **Advanced Settings:**

- **Proxy:** Select to configure a proxy server.
- **Real-time Server:** By default the **Real time server** field uses the value that you entered in the **Host** field.

If you are using intermediate FTP server, then make sure you type in the Analyzer detail view server IP address that is processing the data of the primary server, also make sure that you are not connecting the Analyzer probe server to Analyzer detail view server using proxy.



Note: Port number 9092 must be open on the Analyzer detail view server. The Analyzer probe server must be able to connect to the Analyzer detail view server using port number 9092 to send the real-time data.

10. Click **Next.**

In addition to sending probe data to a single (local) Analyzer detail view server, you can configure a secondary, cloud-based Analyzer detail view server. The purpose is to host a copy of the probe data where it can be accessed outside of your internal network. You can add this secondary server from the Analyzer probe server UI.



Note: The secondary Analyzer detail view server does not support real-time collection.

- 11.** In the **Data Collection duration** window, verify the license expiry date in your license, and then click **Next**.
- 12.** From the list of probes, select the probe type and configure it to collect data from the monitoring target. You must add at least one probe to complete the installation. To add additional probes, go to the Analyzer probe server web UI home page and click **Add Probe**.

The following are available:

- Hitachi Adaptable Modular Storage (AMS) probe
- Hitachi Enterprise Storage probe

- Hitachi NAS probe
- VMware probe
- Brocade FC Switch (BNA) probe
- Brocade FC Switch (CLI) probe
- Cisco FC Switch (DCNM) probe
- Cisco FC Switch (CLI) probe
- Linux probe

Initial setup of Analyzer server

After installing Analyzer server and the Analyzer detail view server, set up the Analyzer server, register the license, change the system account password, connect to the Analyzer detail view server, and then configure the mail server.

To use Common Services, you must also register Analyzer in Common Services and assign Analyzer permissions to Ops Center user groups. If you deployed the Ops Center OVA, Analyzer is already registered in Common Services. If you change the host name, IP address, or port number of the server where Common Services is installed, you must register Analyzer again.



Note:

Products installed in the Ops Center OVA are registered in Ops Center Common Services with their host names. Specify the settings so that the host names of individual Ops Center products can be resolved from client machines.

Workflow for initial setup

After installing the Analyzer server and the Analyzer detail view server, complete the following tasks on the Analyzer server:

Procedure

1. Make sure that you can access the Analyzer server from your web browser.
2. (Optional) If you want to use Common Services, run the **setupcommonservice** command to register Analyzer in Common Services.
3. Register the license.
4. Change the system account password.
5. (Optional) If you want to use Common Services, assign Analyzer permissions to the Ops Center user group.
6. Set up a connection to the Analyzer detail view server.
7. Configure the mail server.

Verifying access to the Analyzer server

Use your web browser to make sure that you can access the Analyzer server.

Before you begin

Check the IP address or host name of the host where the Analyzer server is installed.

Procedure

1. Open a web browser that is supported by Ops Center Analyzer.
2. If you are using a pop-up blocker, add the Analyzer server product URL to the list of exceptions in your browser.
3. Enter the URL for the Analyzer server in your web browser:
`http://host-name-or-IP-address-of-the-Analyzer-server:22015/Analytics/login.htm`

Result

The login window is displayed, indicating that you can access the Analyzer server.

Registering Ops Center Analyzer in Ops Center Common Services

If you want to use Common Services installed on a different host, or if you want to use Common Services in the environment configured with Analyzer OVA, you must register Analyzer with Common Services as described here. If you deployed the Ops Center consolidated OVA, Analyzer is already registered in Common Services.

Procedure

1. Run the **setupcommonservice** command with the `auto` option specified to register Analyzer in Common Services.
 For details, see [setupcommonservice \(on page 506\)](#).

Registering the license for Analyzer server

Register the license for Analyzer server, and then use the built-in account to log on to Analyzer server.

If you are using Common Services, you can use the Ops Center Portal to register the license. For details, see the *Ops Center Help*.

Before you begin

Obtain the Analyzer server license from your Hitachi Vantara representative.

Procedure

1. In the login window, click the **Licenses information** link.

- a. Use either of the following methods:
 - Enter the license key
 - Specify the license file
 - b. Click **Save**.
The license is added in the list.
2. To log on to the Analyzer server, use these credentials:
 - **User ID:** system
 - **Password:** manager



Note: The account "zzz_HIAA_Reportuser_xxx" is created automatically in Analyzer server.

Result

The login is complete, and the Analyzer server **Dashboard** displays.

Changing the system account password

Change the default password for the system account. The system account is a built-in account that has the user management permission and permissions for all Analyzer server operations.

Procedure

1. In the **Administration** tab, select **User Management > Users and Permissions**.
2. From the displayed dialog box, display **Users**, and then select **System**.
3. Click **Change Password**.

Assigning Analyzer permissions to Ops Center user groups

When you use the Common Services single sign-on to perform operations in Analyzer, you must assign Analyzer operating permissions to Ops Center user groups.

Before you begin

Make sure that Analyzer is registered in Common Services.

Procedure

1. Log in to the Ops Center Portal as a user with the Security Admin role or System Admin role, and then launch Analyzer.
2. In the Analyzer **Administration** tab, select **User Group Management > User Groups And Permissions**.
3. Select the check box for the user group to which you want to assign permissions, and then click **Edit Permission Mapping**.



Note: You can select multiple user groups.

4. In the Edit User Groups window, select the check boxes for the permissions you want to assign.
5. Click **OK**.

Setting up a connection with Analyzer detail view server

Set up a connection so that the data collected by the Analyzer detail view server can be analyzed by the Analyzer server.

Before you begin

Check the IP address of the Analyzer detail view server.

Procedure

1. In the **Administration** tab, select **System Settings > Analyzer detail view Server**.
2. Click **Edit Settings**, and specify the Analyzer detail view server information.



Note: Specify the built-in administrator account. If you want to use a different account, specify the account created during the initial setup of the Analyzer detail view server. If you change the password of the specified user on the Analyzer detail view server, you must also change the same password in **Password** of the **Edit Settings** dialog box.

3. Click **Check Connection** to confirm that the server is connected properly.
If you cannot access the Analyzer detail view server, verify the following:
 - The certificate is correctly specified on the Analyzer server.
 - The certificate is not expired.
4. Click **OK**.

Configuring the mail server

Configure the mail server and the email address of the sender to send emails in the following cases:

- To notify the administrator of problems that occur in monitored resources and information related to Analyzer server operations.
- To periodically send dashboard reports to users.

Before you begin

Make sure you have the Admin permission of Ops Center Analyzer.

Procedure

1. In the **Administration** tab, select **Notification Settings > Email Server**.
2. Click **Edit Settings** to specify information about the mail server.
3. To verify that the mail server is configured correctly, click **Send Test Mail**.
4. Confirm that the test email arrives, and then click **Save Settings**.

Changing Ops Center Analyzer passwords

You must change the Ops Center Analyzer passwords.

Changing the megha and meghadata passwords

You should change the megha and meghadata user passwords to enhance the security. The megha user exists on both the Analyzer detail view server and the Analyzer probe server. The Analyzer probe server does not have a meghadata account.



Note: You can also use the following steps if the current password of the megha and meghadata user is expired.

Procedure

1. Log on to the Analyzer detail view server or Analyzer probe server through an SSH client (like **putty**) as a root user.



Note: If you do not want to stop the **crond** service, you can stop the specific processes of the Analyzer detail view server and Analyzer probe server by using the **crontab -e** command as described in [Stopping the Analyzer detail view server or Analyzer probe server services \(on page 360\)](#) and [Starting the Analyzer detail view server or Analyzer probe server services \(on page 360\)](#)

2. Stop the crond service using the command:

```
service crond stop
```

3. Stop the megha service using the command:

```
/usr/local/megha/bin/megha-jetty.sh stop
```

4. Verify the stopped status of the megha service:

```
/usr/local/megha/bin/megha-jetty.sh status
```

5. Run the change password script:

```
/usr/local/megha/bin/changePassword.sh --user
```

6. Choose the account you want to change.
7. Type the user password and confirm it.
8. Start the megha service using the command:

```
/usr/local/megha/bin/megha-jetty.sh start
```


9. Start the crond service using the command:

```
service crond start
```

Next steps

If the Analyzer probe server is uploading the data directly to an Analyzer detail view server for which you have changed the meghadata user password, you must also update the meghadata user password on the Analyzer probe server. To change the password, log on to the Analyzer probe server and then go to the Home > Reconfigure > Analyzer detail view Server tab.

Changing the real-time database password

A real-time mechanism transfers data to the Analyzer detail view server as soon as the data is received by the Analyzer probe server. This real-time data is stored in the database for 30 minutes. You must change the real-time database password to improve security.



Note:

The Analyzer detail view server and the Analyzer probe server share the same username and password for the real-time database. When changing the password you must change it on both servers.

Procedure

1. Log on to the Analyzer detail view server or Analyzer probe server through an SSH client (like **putty**) as a root user.



Note: If you do not want to stop the **crond** service, you can stop the specific processes of the Analyzer detail view server and Analyzer probe server by using the **crontab -e** command as described in [Stopping the Analyzer detail view server or Analyzer probe server services \(on page 360\)](#) and [Starting the Analyzer detail view server or Analyzer probe server services \(on page 360\)](#)

2. Stop the crond service using the command:

```
service crond stop
```

3. Stop all the running services using the command:

```
/usr/local/megha/bin/stop-all-services.sh
```

4. Change the real-time database password using the command:

```
/usr/local/megha/bin/changePassword.sh --realTimeDB
```

5. Start the megha service using the command:

```
/usr/local/megha/bin/megha-jetty.sh start
```

6. Start the crond service using the command:

```
service crond start
```

Initial setup for connecting with Ops Center Automator

You can resolve performance issues by running the Ops Center Automator service templates. The procedure for performing initial configuration varies depending on whether Ops Center Automator is linked with Device Manager.

If you do not want to link Ops Center Automator with Device Manager, we recommend installing Ops Center Automator on the same host as the Analyzer server. For details about how to install Ops Center Automator, see the *Hitachi Ops Center Automator Installation and Configuration Guide*.

Configuring settings to connect to Ops Center Automator when it is not linked with Device Manager

To configure settings to connect to Ops Center Automator when it is not linked with Device Manager:

Prerequisites

Ops Center Automator is installed.

Procedure

- Verify that the Ops Center Automator host name can be resolved.
- Change the Common component settings (if Ops Center Automator and the Analyzer server are installed on separate hosts).
- Check the permissions of the user account.
- (Optional) Create Ops Center Automator service-integration definition files.

Verifying that the Ops Center Automator host name can be resolved

Verify that the Ops Center Automator host name can be resolved by the Analyzer server host.

Procedure

1. Log on to the host on which Ops Center Automator is installed as a user with Administrator permission (Windows) or root permission (Linux).

2. Display the Ops Center Automator URL by running the **hcnds64chgurl** command, and check the host name.

In Windows

```
Automator-installation-destination-folder\Base64\bin\hcnds64chgurl /list
```

In Linux

```
Automator-installation-destination-directory/Base64/bin/hcnds64chgurl -list
```

3. On the Analyzer server host, verify that you can resolve Ops Center Automator host name reported by **hcnds64chgurl** command.

If the name resolution fails, enable name resolution for the Ops Center Automator host name by using a method such as adding an entry to the `hosts` file.

Changing Common component settings

If Ops Center Automator and the Analyzer server are installed on different hosts, you must change the settings of the Common component so that the user accounts used by each product can be centrally managed on the Analyzer server. If you use Common Services, user information is centrally managed in Common Services. However, if you do not perform this procedure, you will not be able to connect to Ops Center Automator.



Note: If Ops Center Automator and the Analyzer server are installed on the same host, skip this procedure.

The host that manages the user accounts is called the primary server. The host on which the user accounts are managed by the primary server is called the secondary server.

Perform the following steps to set the Analyzer server as the primary server and Ops Center Automator as the secondary server.

Procedure

1. Log on to the host on which Ops Center Automator is installed as a user with Administrator permission (Windows) or root permission (Linux).
2. Run the **hcnds64prmset** command to change the settings of the Common component.

For the `host`, `port`, and `sslport` options, specify information about the Analyzer server to use as the primary server. The default port number for non-SSL communication is 22015. The default port number for SSL communication is 22016.

In Windows

```
Automator-installation-destination-folder\Base64\bin\hcnds64prmset /host host-name-or-IP-address {/port port-number-for-non-SSL-communication | /sslport port-number-for-SSL-communication}
```

In Linux

```
Automator-installation-destination-directory/Base64/bin/hcmds64prmset -
host host-name-or-IP-address {-port port-number-for-non-SSL-
communication | -sslport port-number-for-SSL-communication}
```

3. Stop and restart the services:
 - a. Run the **hcmds64srv** command with the `stop` option.
 - b. Run the **hcmds64srv** command with the `start` option.

Result

User account information on Ops Center Automator can now be managed in the Analyzer server.

Checking user account permissions

Check whether the required permissions have been assigned to the user account used to connect to Ops Center Automator. Check the settings in both the Analyzer server and Ops Center Automator.

Procedure

1. Log on to the Analyzer server by using the system account or as a user who has user management permissions.
2. Check the settings of the user account for Ops Center Analyzer:
 - a. In the **Administration** tab, select **User Management > Users and Permissions**.
 - b. In the **Users and Permissions** window, select **Users**. From the user list, click the user account to use to connect to Ops Center Automator.
 - c. In the **Granted Permission** field, make sure that the IAA Admin or Modify permission is set. If the permission is not set, click **Change Permission** to set it.
3. Log on to Ops Center Automator by using the system account.
4. Assign the user account to use to connect Ops Center Automator to an Ops Center Automator user group:
 - a. In the **Administration** tab, select **Resources and Permissions > User Groups**.
 - b. Select a user group that has permission to execute services in Ops Center Automator. On the **Users** tab, click **Assign** to assign the user account to the user group.
5. Assign the user group to an Ops Center Automator service group:
 - a. Select **Resources and Permissions > Service Groups**.
 - b. Select the service group of the Ops Center Automator, and then select the **Permissions** tab.
 - c. Confirm that the user group is assigned to the service group.

Next steps

Check the connection between Ops Center Analyzer and Ops Center Automator.

Configuring settings to connect to Ops Center Automator when it is linked with Device Manager

To configure Ops Center Automator connection settings when linked with Device Manager:

- Verify that the Ops Center Automator host name can be resolved.
- Change the Common component settings (if Device Manager and the Analyzer server are installed on separate hosts).
- Create a user account.
- Check the permissions of the user account.
- (Optional) Create Ops Center Automator service-integration definition files.

Verifying that the Ops Center Automator host name can be resolved

Verify that the Ops Center Automator host name can be resolved by the Analyzer server host.

Procedure

1. Log on to the host on which Ops Center Automator is installed as a user with Administrator permission (Windows) or root permission (Linux).
2. Display the Ops Center Automator URL by running the **hcnds64chgurl** command, and check the host name.

In Windows

```
Automator-installation-destination-folder\Base64\bin\hcnds64chgurl /list
```

In Linux

```
Automator-installation-destination-directory/Base64/bin/hcnds64chgurl -list
```

3. On the Analyzer server host, verify that you can resolve Ops Center Automator host name reported by **hcnds64chgurl** command.
If the name resolution fails, enable name resolution for the Ops Center Automator host name by using a method such as adding an entry to the `hosts` file.

Changing Common component settings

If Device Manager and the Analyzer server are installed on different hosts, you must change the settings of the Common component so that the user accounts used by each product can be centrally managed in Device Manager. If you use Common Services, user information is centrally managed in Common Services. However, if you do not perform this procedure, you will not be able to connect to Ops Center Automator.



Note: If Device Manager and the Analyzer server are installed on the same host, skip this procedure.

The host that manages the user accounts is called the primary server. The host on which the user accounts are managed by the primary server is called the secondary server.

Perform the following steps to set Device Manager as the primary server and the Analyzer server as the secondary server.

Procedure

1. Log on to the host on which the Analyzer server is installed as a user with Administrator permission (Windows) or root permission (Linux).
2. Run the **hcnds64prmset** command to change the settings of the Common component.

For the `host`, `port`, and `sslport` options, specify information about the Device Manager instance to use as the primary server. The default port number for non-SSL communication is 22015, and the default port number for SSL communication is 22016.

In Windows

```
Common-component-installation-destination-folder\bin\hcnds64prmset /
host host-name-or-IP-address {/port port-number-for-non-SSL-
communication | /sslport port-number-for-SSL-communication}
```

In Linux

```
Common-component-installation-destination-directory/bin/hcnds64prmset -
host host-name-or-IP-address {-port port-number-for-non-SSL-
communication | -sslport port-number-for-SSL-communication}
```

3. Stop and restart the services:
 - a. Run the **hcnds64srv** command with the `stop` option.
 - b. Run the **hcnds64srv** command with the `start` option.

Result

User account information on the Analyzer server can now be managed in Device Manager.

Creating user accounts

If you set the Analyzer server as a secondary server using the `hcnds64prmset` command, Ops Center Analyzer users (other than the system account and users with the User Management permission) that were created previously will no longer be able to log on to the Analyzer server. In this case, you must use the Ops Center Analyzer web client to create new user accounts that have Ops Center Analyzer permissions.



Note: This procedure only applies to local user authentication. If Common Services is used, this procedure is not necessary.

Procedure

1. Log on to the Analyzer server by using the system account.
2. In the **Administration** tab, select **User Management > Users and Permissions**.
3. In the **Users and Permissions** window, select **Users**, and then click **Add User**.
4. Specify all required items, and then click **OK**.
5. From the list of users, click the link for the user account that you created in the previous step, and then click **Change Permission**.
6. Select the check box for Admin or Modify permission for IAA, and then click **OK**.

Checking user account permissions

Check whether the user account used to connect to Ops Center Automator has the required permissions. Check the settings in Ops Center Automator.

Procedure

1. Log on to Ops Center Automator as a user who belongs to the Admin group of Ops Center Automator.
2. Assign the user account to use to connect to Ops Center Automator, to an Ops Center Automator user group:
 - a. In the **Administration** tab, select **Resources and Permissions > User Groups**.
 - b. Select a user group that has permission to execute services in Ops Center Automator. On the **Users** tab, click **Assign** to assign the user account to the user group.
3. Assign the user group to the service group of the Ops Center Automator:
 - a. Select **Resources and Permissions > Service Groups**.
 - b. Select the service group of the Ops Center Automator, and then select the **Permissions** tab.
 - c. Confirm that the user group is assigned to the service group.

Next steps

Check the connection between Ops Center Analyzer and Ops Center Automator.

Creating a definition file to connect with Ops Center Automator

If you create a definition file to connect with Ops Center Automator, the Ops Center Automator service defined in that file is displayed in the **Execute Action** window. This allows you to select the service. Information about the selected resources (such as resource names, IP addresses, and virtual host names) is inherited as parameters when the **Submit Service Request** window of Ops Center Automator is opened. In addition, by specifying resource information as filtering conditions, you can display the Ops Center Automator services that meet the conditions in the **Execute Action** window.

The sample definition files to connect with Ops Center Automator are stored in the following location:

In Windows

```
Analyzer-server-installation-destination-folder\Analytics\conf
\template\automation_sample
```

In Linux

```
Analyzer-server-installation-destination-directory/Analytics/conf/
template/automation_sample
```

Sample files usually must be revised to match your environment; however, the following sample file for the built-in service of Ops Center Automator can be used without change: `AllocateLikeVolumeswithConfigurationManager_016200`.

- **Allocate Like Volumes with Configuration Manager:** In the definition file to connect with Ops Center Automator, filtering conditions are specified so that this service is displayed in the **Execute Action** window only when a volume of the storage system is selected.

Note, however, that if you change the service group to which this service template is assigned from `Default Service Group` to a different service group in Ops Center Automator, you must also change the contents of the sample file.

For details, see [Format of definition files used to connect with Ops Center Automator \(on page 97\)](#).

Procedure

1. Create a definition file corresponding to the service to be executed in Ops Center Automator.

In the definition file, you can define the property key to use for the Ops Center Automator service. If you specify information (variables) about the resource owned by Ops Center Analyzer, you can apply the information about the specified resource in the service execution window of Ops Center Automator launched from Ops Center Analyzer.

2. Store the created definition file in the following location:

In Windows

Analyzer-server-installation-destination-folder\Analytics\conf\template\automation

In Linux

Analyzer-server-installation-destination-directory/Analytics/conf/template/automation

3. Restart the Analyzer server or execute the **reloadtemplate** command for changes to take effect.

Format of definition files used to connect with Ops Center Automator

The following items are set in the definition file used to connect with Ops Center Automator:

Format

specified-key-name=specified-value

File

- You can specify any file name and file extension.
- Save the file in UTF-8 format.
- The maximum number of files that can be set in Ops Center Analyzer (including the number of email template definition files and command definition files) is 1,000. Files load in alphabetical order by file name, and any files after the 1,000th file are not loaded.

Folder

In Windows

Analyzer-server-installation-destination-folder\Analytics\conf\template\automation

In Linux

Analyzer-server-installation-destination-directory/Analytics/conf/template/automation

Update frequency

Indicates when the Analyzer server is started or the **reloadtemplate** command is run.

Content to specify

Specify each key name and value on a single line. The following rules apply when you specify settings in a definition file to connect with Ops Center Automator:

- A line starting with # is treated as a comment line.
- Blank lines are ignored.
- The entered values are case-sensitive.

- If you specify an invalid value, the default value is used.
- If you specify the same key more than once in the same file, the last key is used.
- To display \, specify \\..
- To display %, specify %%..
- If you specify the filter condition `SE.template.filter.xxxxxxx.string` more than once, settings display when all of the conditions are met.

Setting descriptions

Key name	Setting description	Specifiable values	Default value	Optional or required
<code>SE.automation.template.serviceGroupName.string</code>	Specify the service group name used in Ops Center Automator.	The same service group name as the one used in Ops Center Automator	N/A	Required
<code>SE.automation.template.serviceName.string</code>	Specify the service name used in Ops Center Automator.	The same service name as the one used in Ops Center Automator	N/A	Required
<code>SE.template.filter.resourceName.string</code>	Specify conditions to narrow down the resource names that appear in the Execute Actions list. ¹	Values of no more than 255 bytes that do not include control characters	Null character	Optional If this key is omitted, the default value is used.
<code>SE.template.filter.resourceType.string</code>	Specify conditions to narrow down the types of resources that display in the Execute Actions list. ¹	Values of no more than 32 bytes that do not include control characters	Null character	Optional If this key is omitted, the default value is used.

Key name	Setting description	Specifiable values	Default value	Optional or required
<code>SE.template.filter.vmHostname.string</code>	Specify conditions to narrow down the virtual machine names that display in the Execute Actions list. ¹	Values of no more than 64 bytes that do not include control characters	Null character	Optional If this key is omitted, the default value is used.
<code>SE.template.filter.ipaddress.string</code>	Specify conditions for the IP addresses that display in the action list during resource selection. ¹	Values of no more than 255 bytes that do not include control characters	Null character	Optional If this key is omitted, the default value is used.
<code>SE.template.filter.upperResourceName.string</code>	Specify conditions to narrow down the names of higher-level resources during resource selection. ¹	Values of no more than 512 bytes that do not include control characters	Null character	Optional If this key is omitted, the default value is used.
<code>SE.template.filter.upperResourceType.string</code>	Specify conditions to narrow down the higher-level resource types during resource selection. ¹	Values of no more than 32 bytes that do not include control characters	Null character	Optional If this key is omitted, the default value is used.

Key name	Setting description	Specifiable values	Default value	Optional or required
SE.template.filter.MultipleResources.boolean	To execute actions for multiple selected resources, specify whether to display the services in the Execute Actions list.	true or false	false	Optional If this key is omitted, the default value is used.
SE.automation.template.service.parameter.Ops Center Automator-service-property-key	Specify the property key ² used for the Ops Center Automator service.	Values of no more than 1,024 bytes that do not include control characters	Null character	Optional If this key is omitted, the default value is used.
Notes: <ol style="list-style-type: none"> Settings display only when the Execute Action window is called from a resource that matches the specified conditions. You cannot specify a property key whose data type is password or composite. To check the property key, use the flow window of the service template. 				

By using variables, you can set information about a selected resource as the value of a setting.

The following table lists the variables you can use.

Variable name	Variable description	Remarks
%ANALYTICS_RESOURCENAME%	Name of the selected resource	N/A
%ANALYTICS_UPPERRESOURCENAME%	Name of the higher-level resource of the selected resource	N/A
%ANALYTICS_IPADDRESS%	IP address	N/A

Variable name	Variable description	Remarks
%ANALYTICS_VIRTUALMACHINENAME%	Name of the virtual host	Displays only when the resource is a virtual machine
%ANALYTICS_RESOURCETYPE%	Resource type	N/A
%ANALYTICS_UPPERRESOURCE%	Type of higher-level resource	N/A

If no value is set for the selected resource, a null character displays.

To display information about virtual hosts and IP addresses, VMware Tools must be installed on virtual hosts.

Definition example

The following is a definition example of displaying the service for stopping virtual machines defined in Ops Center Automator, in the Execute Action window of the virtual machine selected:

```
SE.automation.template.serviceGroupName.string=Services for VM
SE.automation.template.serviceName.string=Stop Virtual Machine
SE.template.filter.MultipleResources.boolean=true
SE.template.filter.resourceType.string=VM
SE.automation.template.service.parameter.vmware.foreachVmName=
%ANALYTICS_IPADDRESS%
```

Resetting Common component settings

If you no longer integrate Ops Center Analyzer with Ops Center Automator, or if you want to remove Ops Center Analyzer, remove the authentication information about the secondary server from the primary server, and reset the settings of the Common component.

Procedure

1. Log on to the host of the primary server as a user with Administrator permission (Windows) or root permission (Linux).
2. Run the `hcmds64intg` command to remove the authentication information about the secondary server from the primary server.

The following is an example of running the command if the Analyzer server is a primary server:

In Windows

```
Common-component-installation-destination-folder\bin\hcnds64intg /
delete /type component-name /user user-ID /pass password
```

In Linux

```
Common-component-installation-destination-directory/bin/hcnds64intg -
delete -type component-name -user user-ID -pass password
```

For the `type` option, specify either of the following as the component name for the secondary server where the authentication information is to be deleted:

- **For Ops Center Automator:** Automation
- **For the Analyzer server:** Analytics

For the `user` and `pass` options, specify a user ID and password of the primary server that has the User Management permission.

3. Stop and restart the services:
 - a. Run the **hcnds64srv** command with the `stop` option to stop the services.
 - b. Run the **hcnds64srv** command with the `start` option to start the services.
4. Log on to the host of the secondary server as a user with Administrator permission (for Windows) or root permission (for Linux).
5. Run the **hcnds64prmset** command to change the settings of the Common component.

The following is an example of running the command if Ops Center Automator is a secondary server:

In Windows

```
Automator-installation-destination-folder\Base64\bin\hcnds64prmset /
setprimary
```

In Linux

```
Automator-installation-destination-directory/Base64/bin/hcnds64prmset -
setprimary
```

Result

The relationship between the primary server and the secondary server is released, and user accounts are managed at each host.

User accounts that were registered before connecting to the primary server can be used again in the secondary server.



Note: If Device Manager was used as the primary server, after the Common component settings are removed, the user accounts created on the Analyzer server remain in Device Manager. If these user accounts are no longer necessary, delete them in the user management window of Device Manager.

Configuring initial settings for limiting the I/O activity of Hitachi storage resources

The I/O control configuration feature of Ops Center Analyzer enables storage administrators to prioritize I/O activity. You can set the upper limit of IOPS processed by volumes during critical workload periods and optimize the performance of resources in a shared infrastructure.

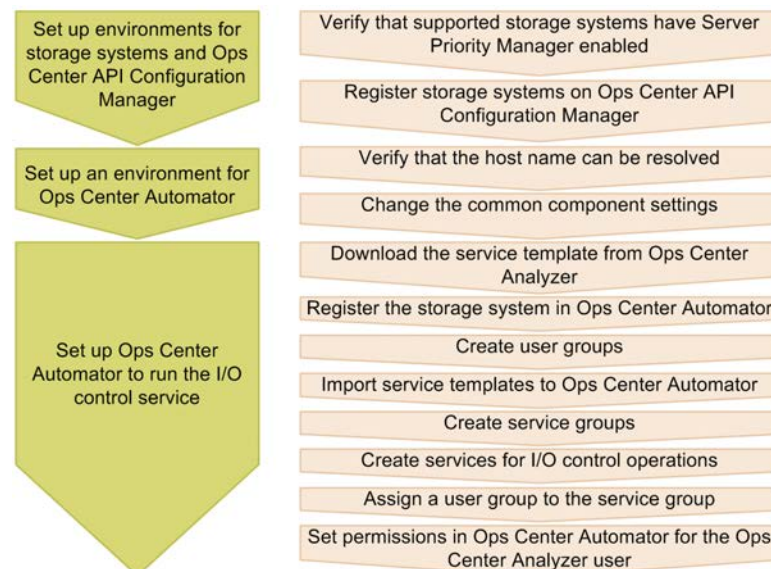
The I/O control feature requires the Server Priority Manager function provided by Hitachi storage systems. To configure Analyzer to work with the Server Priority Manager, use one of the following methods:

- Set up an environment in advance by using the Ops Center API Configuration Manager and Ops Center Automator.
- Create a script file in advance instead of using Ops Center Automator.

Configuration overview for I/O controls using Ops Center Automator

The following figure shows the workflow for configuring I/O controls for the target storage resource by connecting with the Ops Center API Configuration Manager and Ops Center Automator.

I/O Control Configuration Workflow



Before you begin

- Ops Center API Configuration Manager and Ops Center Automator must be installed.
- The target storage systems must have the Server Priority Manager function enabled.
- You must have a user account with storage administrator permissions for the target storage systems.

The procedure for configuring the Ops Center Automator environment is the same as the procedure described in the explanation about configuring the initial settings for connecting with Ops Center Automator.

For details about using Ops Center API Configuration Manager and Ops Center Automator, see the following manuals:

- *Hitachi Ops Center Automator Installation and Configuration Guide*
- *Hitachi Ops Center Automator User Guide*
- *Hitachi Ops Center API Configuration Manager REST API Reference Guide*
- *Hitachi Ops Center Analyzer User Guide*

For details about how to enable the functionalities of Server Priority Manager, see the manuals of the storage systems that you are using.



Note: The Ops Center API Configuration Manager cannot operate the Server Priority Manager function if that function is already being operated by another program (such as Storage Navigator) in the storage system. To use the I/O control configuration function of Ops Center Analyzer, delete all of the settings for Server Priority Manager from the other program (such as Storage Navigator), and then perform operations.

Registering storage systems in the Ops Center API Configuration Manager

Before initiating the services for I/O control tasks between Ops Center Analyzer and Ops Center Automator, you must register the target storage systems in the Ops Center API Configuration Manager.

You can register storage system information by running a script. Script files are provided with the Analyzer probe server.

Procedure

1. Specify Ops Center API Configuration Manager information in the following file:

```
Analyzer-server-installation-destination-directory/Analytics/  
sample/config.sh
```

2. Create a JSON-format text file (with the extension ".json") that contains information about the storage system to register in Ops Center API Configuration Manager.

For the format of the JSON file, see the following sample files:

- For VSP G200, G400, G600, G800, VSP G1000, G1500, VSP F400, F600, F800, VSP F1500, or VSP 5000 series:

```
Analyzer-server-installation-destination-directory/Analytics/
sample/registerSvpStorage.json
```

- For VSP E series, VSP G350, G370, G700, G900, VSP F350, F370, F700, F900:

```
Analyzer-server-installation-destination-directory/Analytics/
sample/registerGumStorage.json
```

For details about the items to specify in the JSON file, see the descriptions about registration of storage systems in the *Hitachi Ops Center API Configuration Manager REST API Reference Guide*.

3. Specify the created JSON file as an argument, and then run the script.

```
./operate_storage.sh register userID password path-of-the-created-json-
file
```

For `userID`, specify an account that belongs to the Administrator user group.

4. From the script execution result, note the value of `storageDeviceID`. You need this value in the next task. Alternatively, you can check the result by running the following script:

```
./operate_storage.sh list
```



Note: If a VSP G1000 storage system is registered in the Ops Center API Configuration Manager, and SSL is enabled between the Ops Center API Configuration Manager and the storage system, the storage system cannot be registered on another instance of the Ops Center API Configuration Manager. For details about SSL communication settings, see the *Hitachi Ops Center API Configuration Manager REST API Reference Guide*.

Setting up Ops Center Automator to run the I/O control configuration function

Download the service template for I/O control configuration from the Ops Center Analyzer GUI, and then register the target storage system and set services on the Ops Center Automator GUI.

Procedure

1. In Ops Center Analyzer, download the service templates.
 - a. On the **Administration** tab, select **System Settings > Automator Server**.
 - b. Click the link to download the service template.
The name of the service template is `AnalyticsServiceTemplate.zip`.
2. Register the storage system in Ops Center Automator.

- a. On the **Administration** tab, select **Connection Settings > Web Service Connections**.
- b. Click **Add**, and then specify the following information about the storage systems with Server Priority Manager:
 - Category: Specify "ConfigurationManager"
 - Name: Device number of the storage system
 - IPAddress/HostName: IP address or host name of the host on which the Ops Center API Configuration Manager is installed
 - Protocol: **http** or **https**
 - Port: Port number used by the Ops Center API Configuration Manager
 - User ID and password: User account with permission to access the logical devices and ports (specified when the storage system was registered to the Ops Center API Configuration Manager)
 - Assigned Infrastructure Groups: Infrastructure group to which the target storage system is registered

If you are not using the infrastructure group functionality, specify "IG_Default Service Group".



Note:

- If any name other than "ConfigurationManager" is specified for the category, you must edit the file `config_user.properties`.
- If any name other than "ConfigurationManager" is specified, an error message is displayed when you connect with the Ops Center API Configuration Manager by clicking the **Test** button. Despite this error message, the I/O control configuration function operates normally when the correct value is registered to each field.
- When registering storage system information in Ops Center Automator, use a user account that is used for the I/O control configuration function. If you attempt to register storage system information by using a user account that is being used in another application (such as RAID Agent), I/O control configuration tasks will fail.

3. Create an Ops Center Automator user group to use in Ops Center Analyzer.
 - a. On the **Administration** tab, select **Resources and Permissions > User Groups**.
 - b. Click **Create**, and then specify a name for the user group.



Note: If any name other than "AnalyticsGroup" is specified for the user group name, you must edit the configuration file.

4. Import the service templates in Ops Center Automator.
 - a. Decompress the file `AnalyticsServiceTemplate.zip` to a location of your choice.
 - b. On the **Service Templates** tab, click **Import**.

c. Click **Browse**, and then specify one of the following zip files:

- If you are using Automation Director version 8.5.0:
ServiceTemplate_03.00.02.zip
- If you are using any version other than the above:
ServiceTemplate_03.20.00.zip

These zip files contain two service templates:

- `com.hitachi.software.dna.analytics_DeleteIoControlSettings_version.st` - disables I/O control configuration tasks
- `com.hitachi.software.dna.analytics_ModifyIoControlSettings_version.st` - enables or modifies I/O control configuration tasks

d. Click **OK**.



Tip: If you do not see the service template for I/O control configuration, sort service template files by **Registered**, and the latest imported templates will appear with the **New** tag.



Note: If you import the file `ServiceTemplate_03.00.02.zip`, "OUTDATED" might be displayed in the imported service template, indicating that the version has expired. If "OUTDATED" is displayed, do not update the service template. If you update the file, the service template will become unusable.

5. Create a service group.

- a. On the **Administration** tab, select **Resources and Permissions > Service Groups**.
- b. Click **Create**, and then specify a name for the service group.



Note:

If any name other than "Analytics Service Group" is specified for the service group name, you must edit the configuration file.

6. Use the service templates to create the services for Server Priority Manager:

- a. On the **Administration** tab, select **Resources and Permissions > Service Groups**.
- b. Select the service group you created.
- c. On the **Services** tab, click **Create**.
- d. Select the service templates, and then click **Create Service**.
- e. Verify or specify the following information:
 - Name of the service for updating Server Priority Manager settings: Modify IO Control Settings for Volume
 - Name of the service for deleting Server Priority Manager settings: Delete IO Control Settings for Volume
 - Status: Release



Note: Do not modify the I/O control configuration. These fields are autopopulated by the information entered on the Ops Center Analyzer user interface when you submit an I/O control configuration task.

- f. Click **Save and Close** to close the window.
7. Assign the user group to the service group.
 - a. On the **Permissions** tab, click **Assign**.
 - b. Select the user group, and then click **Add**.
 - c. Select the **Submit** role, and then click **OK**.
8. Assign the user account that runs the I/O control configuration function to the user group created in step 3.
 - a. On the **Permissions** tab, select a user group that has the Submit role.
 - b. Click **Assign**, and then select the user account that runs the I/O control configuration function.



Note:

For the user account, the Admin or Modify permission of Ops Center Analyzer needs to be set.

- c. Click **Add**, and then click **OK**.
9. Assign an infrastructure group to the service group.
 - a. On the **Resources** tab, click **Assign**.
 - b. From **Available Infrastructure Groups**, select an infrastructure group, and then click **Add**.
If you are not using the infrastructure group functionality, specify "IG_Default Service Group".
 - c. Confirm that the selected infrastructure group has been moved to **Assigned Infrastructure Groups**, and then click **OK**.
10. If you use a name other than the recommended name for the service group name, category name, or service name, edit the `config_user.properties` file.

Specify the values set in the Ops Center Automator.

The location of the `config_user.properties` file is as follows:

For Windows

`Analyzer-server-installation-destination-folder\Analytics\conf`

For Linux

`Analyzer-server-installation-destination-directory/Analytics/conf`

Specify the following keys and values:

- `automation.parameter.serviceGroupName`: Service group name specified in Ops Center Automator
- `automation.parameter.productName`: Category name specified in Ops Center Automator

- `automation.parameter.serviceName.ioControl.modify`: Service name set in Ops Center Automator as the name of the service for updating Server Priority Manager settings
 - `automation.parameter.serviceName.ioControl.delete`: Service name set in Ops Center Automator as the name of the service for deleting Server Priority Manager settings
11. If you have edited the `config_user.properties` file, restart the Analyzer server services.

Result

The environment setup for controlling storage resources is now complete.

Next steps

Check the connection between Ops Center Analyzer and Ops Center Automator.

Configuring I/O control settings with user-defined scripts

This example describes how to use Ops Center Analyzer and Ops Center API Configuration Manager to configure the I/O control settings for the target storage resources with user-defined scripts.

Procedure

1. Create the script files. One for create or modify operation and another for delete operation.
2. Specify the script file name in the built-in template file.
3. Submit an I/O control task from the Ops Center Analyzer **Operations** tab or from the **Analyze Bottleneck > Analyze Shared Resources** window.
4. Script execution is initiated by Ops Center Analyzer after you submit the I/O control task.
5. Check the status of the script execution on the Ops Center Analyzer **Events** tab.

Prerequisites for setting I/O controls (using a script)

The prerequisites for setting I/O controls by using the script file to execute the Ops Center API Configuration Manager are as follows:

- You must have the Ops Center Analyzer User Interface login credentials with StorageOps permissions to configure the I/O control settings.
- Make sure the Ops Center API Configuration Manager is installed on a host. For installation instructions, see the *Hitachi Ops Center API Configuration Manager REST API Reference Guide*.
- Make sure the target storage systems are registered on the Ops Center API Configuration Manager.

- Make sure the Server Priority Manager function is enabled for the target storage systems.
- You must have a user account with storage administrator permissions for the target storage systems.

Creating the script files

Analyzer server can run user-defined script files for creating, updating and deleting storage I/O control settings.

Procedure

1. Create the script files. You must create one script file for create or update operation and another for delete operation. You can specify any file name.
2. Save the script file anywhere on the Analyzer server.

Example: create or update request

You can set the upper limit of I/O activity for the volumes in a shared infrastructure. You can also update the existing I/O settings. While creating the scripts, you must determine the logical workflow for the successful completion of a task, a sequence of tasks for creating or updating I/O control settings for the target storage resources.

The script depends on the following parameters:

- The *.json file, which includes the I/O control parameters that you input from the UI. The *.json file is autocreated by the system after you submit the I/O control task using the Ops Center Analyzer UI.
 - Storage device ID
 - LDEV ID
 - Host WWN
- The user-environment configuration details includes the following:
 - storage-account-user-name
 - storage-account-password
 - API-Configuration-Manager-host-name
 - API-Configuration-Manager-protocol
 - API-Configuration-Manager-access-port

For example, when you run the script, it reads the *.json file to obtain the storage device ID based on which it determines the user-environment configuration details.

The sequence of tasks for creating or updating the I/O control settings is as follows:

1. Obtain the storage device ID and the user-environment configuration details.
2. Access the Ops Center API Configuration Manager to obtain a list of storage resources enabled for I/O control settings.

An example of the **curl** command that is used to communicate with the storage system to check the current I/O control settings is as follows:

```
curl --user storage-account-user-name:storage-account-password -H
"Accept: application/json" -H "Contenttype:application/json" -X
GET "API-Configuration-Manager-protocol://API-Configuration-Manager-
host-name(or IP address):API-Configuration-Manager-accessport/
ConfigurationManager/v1/objects/storages/storageDeviceID/io-control-
ldev-wwns-iscsis/"
```

The request returns a list of volumes enabled for I/O control settings.

3. Determine whether the request is to create or update by comparing the input I/O control settings and the existing settings.
 - **For a creation request:** Identify the volumes without I/O control settings.
 - **For an update request:** Identify the volumes for which I/O control settings are already configured.
4. Access the Ops Center API Configuration Manager to run the create request for the volumes without I/O control settings.

An example of the **curl** command used to create the I/O control settings for the target storage resources is as follows:

```
json={"ldevId":ldevId,"hostWwn": "wwn","upperLimitForIops
":upperLimit}
curl --user storage-account-user-name:storage-account-password -H
"Accept:application/json" -H "Contenttype:application/json" -X POST -d
$json "API-Configuration-Manager-protocol://API-Configuration-Manager-
host-name(or IP address):API-Configuration-Manager-access-port/
ConfigurationManager/v1/objects/storages/storageDeviceID/io-control-
ldev-wwns-iscsis/"
```

5. Access the Ops Center API Configuration Manager to run the update request for the volumes already configured with I/O control settings.

An example of the **curl** command used to update the I/O control settings:

```
json={"upperLimitForIops":upperLimit}
curl --user storage-account-user-name:storage-account-password -H
"Accept:application/json" -H "Contenttype:application/json" -X PUT -d
$json "API-Configuration-Manager-protocol://API-Configuration-Manager-
host-name(or IP address):API-Configuration-Manager-access-port/
ConfigurationManager/v1/objects/storages/storageDeviceID/io-control-
ldev-wwns-iscsis/ldevId,hostWwn"
```



Note: The sample **curl** commands require you to provide the user credentials to access the resources in the protected zone. Apply security measures to protect the sensitive information.

Example: delete request

You can delete the I/O control settings when the requirements change and you no longer want to limit the I/O control activity. While creating the scripts, you must determine the logical workflow for the successful completion of a task, a logical sequence of tasks to delete the I/O control settings for the target storage resources.

The script depends on the following parameters:

- The *.json file, which includes the I/O control parameters that you input from the UI. The *.json file is autocreated by the system after you submit the I/O control task using the Ops Center Analyzer UI.
 - Storage device ID
 - LDEV ID
 - Host WWN
- The user-environment configuration details includes the following:
 - storage-account-user-name
 - storage-account-password
 - API-Configuration-Manager-host-name
 - API-Configuration-Manager-protocol
 - API-Configuration-Manager-access-port

For example, when you run the script, it reads the *.json file to get the storage device ID that determines the user-environment configuration details.

The logical order of tasks to be executed by the script for deleting the I/O control settings is as follows:

1. Obtain the storage device ID and the user-environment configuration details.
2. Access the Ops Center API Configuration Manager to obtain a list of storage resources enabled for I/O control settings.

An example of the **curl** command that is used to communicate with the storage system to check the current I/O control settings is as follows:

```
curl --user storage-account-user-name:storage-account-password -H
"Accept: application/json" -H "Contenttype:application/json" -X
GET "API-Configuration-Manager-protocol://API-Configuration-Manager-
host-name(or IP address):API-Configuration-Manager-accessport/
ConfigurationManager/v1/objects/storages/storageDeviceID/io-control-
ldev-wwns-iscsis/"
```

The request returns a list of volumes enabled for I/O control settings.

3. Determine whether the target volumes exist and whether they are enabled for I/O control settings by initiating a comparison between the input I/O control settings and the existing settings.
4. Access the Ops Center API Configuration Manager to delete the I/O control settings for the target volumes.

An example of the **curl** command used to delete the I/O control settings is as follows:

```
curl --user storage-account-user-name:storage-account-password -H
"Accept:application/json" -H "Contenttype:application/json" -X DELETE
"API-Configuration-Manager-protocol://API-Configuration-Manager-host-
name(or IP address):API-Configuration-Manager-access-port/
ConfigurationManager/v1/objects/storages/storageDeviceID/io-control-
ldev-wwns-iscsis/ldevId,hostWwn"
```



Note: The sample **curl** commands require you to provide the user credentials of the storage system to access the storage resources. Apply security measures to protect the sensitive information.

Editing built-in command templates

The built-in command template files contain details about the script files for configuring I/O control settings. You must edit the built-in command templates to specify the script file path.

Procedure

1. Edit the built-in command templates to specify the script file path.

The templates are stored in the following location:

Windows:

```
Analyzer-server-installation-destination-folder\Analytics\conf\template
\command\Built-in
```

Linux:

```
Analyzer-server-installation-destination-directory/Analytics/conf/
template/command/Built-in
```

2. For creating or updating the I/O control settings, edit the `BuiltinTemplateIoControlModify.txt` file.

An example of the `BuiltinTemplateIoControlModify.txt`:

```
SE.template.name.string = Script to modify I/O control settings
SE.cmd.template.timeOut.num = 18000000
SE.cmd.template.cmdName.string = File-path-of-the-scriptfile
```

3. For deleting the I/O control settings, edit the `BuiltinTemplateIoControlDelete.txt` file.

An example of the `BuiltinTemplateIoControlDelete.txt`:

```
SE.template.name.string = Script to delete I/O control settings
SE.cmd.template.timeOut.num = 18000000
SE.cmd.template.cmdName.string = File-path-of-the-scriptfile
```

The prerequisites for the keys included in the built-in command definition file are as follows:

- `SE.cmd.template.timeOut.num` is the timeout period that specifies the system response after the command is executed. The default value is 18,000,000 milliseconds. You can specify a value from 1 millisecond to 2,147,483,647 milliseconds.
 - `SE.cmd.template.cmdName.string` specifies the command name. Specify the absolute path to the command. You can specify a value from 0 to 255 bytes that do not include control characters. To specify \, type \\\.
4. Restart the Analyzer server or execute the **reloadtemplate** command for changes to take effect.

Creating an I/O control task

You must submit an I/O control task using the Ops Center Analyzer UI.

Before you begin

- Make sure you have specified the name of script files that you want to run in the built-in command template files.
- You must be logged into the Ops Center Analyzer UI with StorageOps permissions.

Procedure

1. To launch the **Set IO Control** window, perform any of the following:
 - From the **Operations** tab, search for the related volumes. Select the volumes, and then click **Set IO Control**.
 - From the **Analyze Bottleneck** window, click the **Analyze Shared Resources** tab. In the **Analyze Shared Resources** window, select the target volumes, and click **Set IO Control**.
2. In the **Set IO Control** window, configure the I/O control settings:
 - a. In **Upper Limit Setting**, select **ON** for creating or updating I/O control settings. Select **OFF** for deleting the I/O control settings.
 - b. In **Collective Settings**, select the metric and enter the limit in **Upper Limit for each volume**.
 - c. Enter a task name and description, and then click **Next**.
A default task name based on the date and time is automatically assigned: `yyyymmdd_hhmm_IOControlSettings`.
3. Review the information, and then click **Submit**.

Running the script files

Ops Center Analyzer lets you configure the I/O control settings by executing the user-defined scripts.

Procedure

1. After you submit the I/O control task, the system automatically creates a *.json file with the input I/O control parameters.

Sample file format of the *.json file:

```
{
  "storageDeviceId": "836000123456",
  "IOControlParameter":
  [ {
    "ldevId": 101,
    "hostWwn": "000000102ccec9",
    "upperLimitForIops": 50 },
    {
    "ldevId": 102,
    "hostWwn": "000000102ccec0",
    "upperLimitForIops": 400
  } ]
}
```

2. The system then inputs the following parameters to the script files:
 - Ops Center Analyzer user name
You can use this information to track the users running the script files.
 - File path of the *.json file
3. The scripts read the *.json file and interface with the Ops Center API Configuration Manager to configure the I/O control settings.

Checking the status of the script execution

You can verify whether the scripts were successfully executed. The script execution task is logged in as an information event on the **Events** tab.

Procedure

1. From the Ops Center Analyzer home page, click the **Events** tab.
2. Click **All Events** or **System Events** tab to track the status of the script execution. The name of the script file is displayed as the command action name.



Note: You can only track the status of the script execution on the **Events** tab. The status and execution results of the I/O control task based on the user definition script cannot be viewed under **History**.

Initial setup for enabling Granular Data Collection

If you enable Granular Data Collection from Ops Center Analyzer, the RAID Agent commands are run remotely, and performance data (in units of seconds) for the monitored storage systems is output in CSV format. You can use this data for further analysis.

Before enabling Granular Data Collection, make sure the following conditions are satisfied:

- The Analyzer server is running a Linux OS.
- RAID Agent or Tuning Manager - Agent for RAID is running on a Linux OS that is supported by the Analyzer server.
- Performance information for the monitored storage systems is being collected using a command device.
- For details on the types of storage systems for which Granular Data Collection can be used, see [Monitoring target requirements \(on page 41\)](#).

To enable Granular Data Collection:

- Configure SSH on both the Analyzer server and the RAID Agent (or Tuning Manager - Agent for RAID) host.
- Register the storage systems to be monitored by using Granular Data Collection on the Analyzer server.

Configuring SSH to use Granular Data Collection

You must enable SSH to use Granular Data Collection to remotely execute commands on the RAID Agent host from the Ops Center Analyzer server.

You must also configure the SSH settings if you want to use Tuning Manager - Agent for RAID to collect data from the monitored storage systems.

To enable SSH, specify the following settings:

1. Create keys on the Analyzer server.
2. Register the public key for the RAID Agent host and configure authentication using public key cryptography.
3. Verify the connection.

Creating keys on the Analyzer server

Create the public and private keys used for SSH on the Analyzer server. You can use both the RSA and DSA cryptography key types.

Before you begin

You must have the root permission.

Procedure

1. Run the **ssh-keygen** command as follows:

- For RSA keys:

```
ssh-keygen -t rsa
```

- For DSA keys:

```
ssh-keygen -t dsa
```

2. Specify the full pathname of the file where the private key will be stored.

The default location is `~/.ssh/id_rsa`.

3. Press **Enter** twice.

When you are prompted to enter the password for the private key, press **Enter**.
When you are prompted again, press **Enter** again.

An example of running the **ssh-keygen -t rsa** command:

```
[root@HOST]$ ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/home/ssh-user/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/ssh-user/.ssh/id_rsa.
Your public key has been saved in /home/ssh-user/.ssh/id_rsa.pub.
The key fingerprint is:
ax:xx:xx:xx:xx:bx:xx:xc:xx:xx:xx:xd:xd:xa:ed:xx root@HOST
```

4. Run the **chmod** command to specify 600 as the attribute of the private key file.

```
[root@HOST]$ chmod 600 id_rsa
```

Be sure to protect private keys.

Result

The private key and public key for authentication are created.

Next steps

Configure the public key authentication.

Configuring the public key authentication

Configure the public key authentication using public key cryptography.

Before you begin

You must have the root permission.

Procedure

1. Navigate to the `.ssh` directory. Specify 700 as the attribute of the directory.



Note: If there is no `.ssh` directory, create one.

2. Add the contents of the Analyzer server public key file to the authentication key file of the RAID Agent host.
3. Run the `chmod` command to specify 600 as the attribute of the authentication key file.

The following is an example of running the command. In this example, the host name of the Analyzer server where keys are created is "HIAAHost", and the host name of the RAID Agent host is "AgentHost".

```
[root@AgentHost]$ cd .ssh

[root@AgentHost .ssh]$ ssh root@HIAAHost 'cat /root/.ssh/id_rsa.pub'
>> authorized_keys
root@HIAAHost's password: Enter a password here.
[root@AgentHost .ssh]$ chmod 600 authorized_keys
```

4. Set the authentication key file as the value of `AuthorizedKeysFile` in `/etc/ssh/sshd_config`.



Note: By default, `~/.ssh/authorized_keys` or `.ssh/authorized_keys` is set as the value of `AuthorizedKeysFile`. If you have changed the path of the authentication key file, revise the value of `AuthorizedKeysFile`.

5. Specify `yes` for the value of `PubkeyAuthentication` in `/etc/ssh/sshd_config`.
6. Specify `yes` for the value of `PermitRootLogin` in `/etc/ssh/sshd_config`.
7. Restart the `sshd`.



Note: For details about the items to specify in `sshd_config` and how to specify settings, see the documentation for the SSH server that you plan to use.

Result

The public key is registered to the RAID Agent host, and the authentication is configured.

Next steps

Verify the SSH connection.

Verifying SSH connections

Verify whether an SSH connection can be established between the Analyzer server and the RAID Agent host.

Before you begin

You must have the root permission.

Procedure

1. Use the created private key to run the **ssh** command for the RAID Agent host from the Analyzer server.

If a connection is successfully established without any prompt for an identity, SSH configuration is complete. If an error occurs or you are prompted to enter a password and a passphrase, check whether the settings are configured as described.

Registering storage systems to be monitored by Granular Data Collection

Use a definition file to register the storage systems when performance information (in seconds) is collected by using the Granular Data Collection feature in Ops Center Analyzer. As with RAID Agent, you also must use a definition file to register target storage systems if you use Tuning Manager - Agent for RAID to collect information from the monitored storage systems.

Definition file

`storage_agent_map.txt`

Location

`Analyzer-server-installation-destination-directory/Analytics/bin/
command/granular`

Definition items

Specify the following items by using commas to separate them.

Setting item	Description	Required/Optional
Model name of the storage system	Model name of the storage system	Required
Serial number of the storage system	Serial number of the storage system	Required
IP address of the RAID Agent host	IP address of the RAID Agent host	Required
Port number of the RAID Agent host	Port number of the RAID Agent host If you fail to provide this information, 24221 is used as the default port number.	Optional

Setting item	Description	Required/Optional
Instance name for collecting performance information (in seconds)	<p>The name of instance that you want collect performance information (in seconds)</p> <p>If you fail to provide this information, RAID Agent searches for the target instance by comparing the model name and serial number specified in the definition file to the information that RAID Agent holds.</p>	Optional
Use of a proxy server	<p>Whether to use a proxy server for communication between the Analyzer server and the RAID Agent host.</p> <p>If a proxy server is available, specify one of the following values:</p> <ul style="list-style-type: none"> ▪ <code>noproxy</code>: Specify this if the server and the host communicate directly with each other without using a proxy server. ▪ <code>proxy</code>: Specify this if you use a proxy server. <p>If a proxy server is not available, omit this item.</p>	Optional
URL of the proxy server	<p>The URL of the proxy server.</p> <p>If you use a proxy server, you must specify a value for this item.</p>	Optional
Authentication information for the proxy server	<p>Authentication information for the proxy server.</p> <p>If you use a proxy server that requires user authentication, specify the authentication information in the following format:</p>	Optional

Setting item	Description	Required/Optional
	<i>user-name:password</i>	

Definition example

In the definition file example below, the following three storage systems are registered to be monitored once per second.

- VSP F1500
- VSP G1000
- HUS VM

Storage system	VSP F1500	VSP G1000	HUS VM
Model name of the storage system	VSP F1500	VSP G1000	HUS VM
Serial number of the storage system	123456	7890	10000
IP address of the RAID Agent host	10.196.1.2	10.196.1.3	10.196.1.4
Port number of the RAID Agent host	Not set	24221	Not set
Instance name for collecting performance information (in seconds)	Not set	INSTANCE1	INSTANCE2
Use of a proxy server	Not set	Not set	Not set
URL of the proxy server	Not set	Not set	Not set
Authentication information for the proxy server	Not set	Not set	Not set

Definition file example

```
VSP F1500,123456,10.196.1.2
VSP G1000,7890,10.196.1.3,24221,INSTANCE1
HUS VM,10000,10.196.1.4,,INSTANCE2
```

Configuring initial settings for enabling the audit log of the Analyzer server

The audit log provides a record of all user operations on the Analyzer server. The audit log tracks events from several categories such as external services, authentication, configuration access, start and stop services. By examining the audit log, you can check the system usage status or audit for unauthorized access.

The audit log data is output to the event log file (in Windows) or to the `syslog` file (in Linux).

The following table lists and describes the categories of audit log data that can be generated from products that use the Common component. Different products generate different types of audit log data.

Categories	Description
StartStop	Events indicating starting or stopping of hardware or software: <ul style="list-style-type: none">Starting or shutting down an OSStarting or stopping a hardware component (including micro components)Starting or stopping software on a storage system or SVP, and products that use the Common component
Failure	Events indicating hardware or software failures: <ul style="list-style-type: none">Hardware failuresSoftware failures (memory error, etc.)
LinkStatus	Events indicating link status among devices: <ul style="list-style-type: none">Whether a link is up or down
ExternalService	Events indicating the results of communication with external services: <ul style="list-style-type: none">Communication with an external server, such as NTP or DNSCommunication with a management server (SNMP)

Categories	Description
Authentication	<p>Events indicating that a device, administrator, or end user succeeded or failed in connection or authentication:</p> <ul style="list-style-type: none"> ▪ Fibre Channel login ▪ Device authentication (Fibre Channel - Security Protocol authentication, iSCSI login authentication, SSL server/client authentication) ▪ Administrator or end user authentication
AccessControl	<p>Events indicating that a device, administrator, or end user succeeded or failed in gaining access to resources:</p> <ul style="list-style-type: none"> ▪ Access control for devices ▪ Access control for the administrator or end users
ContentAccess	<p>Events indicating that attempts to access important data succeeded or failed:</p> <ul style="list-style-type: none"> ▪ Access to important files on NAS or to contents when HTTP is supported ▪ Access to audit log files
ConfigurationAccess	<p>Events indicating that the administrator succeeded or failed in performing an allowed operation:</p> <ul style="list-style-type: none"> ▪ Reference or update of the configuration information ▪ Update of account settings including addition or deletion of accounts ▪ Security configuration ▪ Reference or update of audit log settings
Maintenance	<p>Events indicating that a performed maintenance operation succeeded or failed:</p> <ul style="list-style-type: none"> ▪ Addition or deletion of hardware components ▪ Addition or deletion of software components

Categories	Description
AnomalyEvent	<p>Events indicating that an anomaly, such as a threshold being exceeded, occurred:</p> <ul style="list-style-type: none"> ▪ A network traffic threshold was exceeded ▪ A CPU load threshold was exceeded ▪ Pre-notification that a limit is being reached or a wraparound occurred for audit log data temporarily saved internally
	<p>Events indicating that abnormal communication occurred:</p> <ul style="list-style-type: none"> ▪ SYN flood attacks to a regularly used port, or protocol violations ▪ Access to an unused port (port scanning, etc.)

Enabling audit logging

To enable the audit log of the Analyzer server and change the audit events to be output to the audit log, first configure the environment configuration file (`auditlog.conf`) for the Common component. Then you must restart the Analyzer server.



Note:

- If the Analyzer server is installed by using a virtual appliance, the audit log is enabled by default.
If the Analyzer server is installed by using the installer, the audit log is disabled by default. Enable the settings as required.
- A large volume of audit log data might be output. Change the log file size and back up or archive the generated log files accordingly.

Procedure

1. Log on to the Analyzer server as a user with Administrator permission (Windows) or root permission (Linux).
2. Open the `auditlog.conf` file, which is located in one of the following locations:

In Windows

`Common-component-installation-destination-folder\conf\sec\auditlog.conf`

In Linux

`Common-component-installation-destination-directory/conf/sec/auditlog.conf`



Note: The `auditlog.conf` file is an environment configuration file for the Common component. Therefore, if another product that uses the Common component is installed on the same host as the Analyzer server, the audit log settings will be shared among both products.

3. To enable audit logging, specify the audit event categories for the `Log.Event.Category` property in the `auditlog.conf` file.
4. To disable audit logging, delete all audit even categories specified for the `Log.Event.Category` property in the `auditlog.conf` file.
5. Restart the Analyzer server services.

Settings in the auditlog.conf file

You can specify the audit event categories and severity to be output in the `auditlog.conf` file.

The following shows the items you can set in the `auditlog.conf` file.

Log.Facility (Linux only)

Specify a numeric value for the facility (the log type) required to output audit log data to the `syslog` file in Linux. (Default value: 1)

`Log.Facility` is ignored in Windows, even if it is specified. Also, if an invalid value or a non-numeric character is specified, the default value is used.

The following table shows the correspondence between the specifiable values for `Log.Facility` and the facility defined in the `syslog.conf` file.

Specifiable value for <code>Log.Facility</code>	Facility defined in the <code>syslog.conf</code> file
1	user
2	mail*
3	daemon
4	auth*
6	lpr*
16	local0
17	local1
18	local2
19	local3
20	local4

Specifiable value for Log.Facility	Facility defined in the syslog.conf file
21	local5
22	local6
23	local7
*: Although you can specify this value, we do not recommend that you specify it.	

To filter audit logs output to the `syslog` file, you can combine the facility specified for `Log.Facility` and the severity specified for each audit event.

The following table shows the correspondence between the severity of audit events and the severity defined in the `syslog.conf` file.

Severity of audit events	Severity defined in the syslog.conf file
0	emerg
1	alert
2	crit
3	err
4	warning
5	notice
6	info
7	debug

Log.Event.Category

Specify the audit event categories to be output. (Default value: none)

When specifying multiple categories, use commas (,) to separate them. In this case, do not insert spaces between categories and commas. If

`Log.Event.Category` is not specified, audit log data is not output.

`Log.Event.Category` is not case-sensitive. If an invalid category name is specified, the specified file name is ignored.

Valid categories: `StartStop`, `Failure`, `LinkStatus`, `ExternalService`, `Authentication`, `AccessControl`, `ContentAccess`, `ConfigurationAccess`, `Maintenance`, or `AnomalyEvent`

Log.Level (Effective in Windows only)

Specify the severity level of audit events to be output. (Default value: 6)

Events with the specified severity level or lower will be output to the event log file.

For details about the severity of each audit event, see the list of audit events output to the audit log.

`Log.Level` has an effect in Windows only. `Log.Level` is ignored in Linux, even if it is specified. Also, if an invalid value or a non-numeric character is specified, the default value is used.

The following table shows the correspondence between the specifiable value for `Log.Level` and the levels displayed in the event log.

Specifiable value for <code>Log.Level</code>	Levels displayed in the event log
0	Error
1	
2	
3	
4	Warning
5	Information
6	
7	

Sample audit.log.conf file

The following shows an example of the `auditlog.conf` file:

```
# Specify an integer for Facility. (specifiable range: 1-23)
Log.Facility 1

# Specify the event category.
# You can specify any of the following:
# StartStop, Failure, LinkStatus, ExternalService,
# Authentication, AccessControl, ContentAccess,
# ConfigurationAccess, Maintenance, or AnomalyEvent.
Log.Event.Category StartStop,Failure,LinkStatus,ExternalService,
Authentication,AccessControl,ContentAccess,ConfigurationAccess,Maintenance,
AnomalyEvent

# Specify an integer for Severity. (specifiable range: 0-7)
Log.Level 6
```

In the example above, all types of audit events are output.

For Windows, `Log.Level 6` outputs audit log data corresponding to the Error, Warning, and Information levels. For Linux, `Log.Facility 1` outputs the audit log data to the `syslog` file that is defined as the `user` facility in the `syslog.conf` file.

Format of data output to the audit log

The audit log data is output to the event log file (in Windows) or to the `syslog` file (in Linux).

The following shows the format of data output to the audit log:

In Windows

```
program-name [process-ID]: message-part
```

In Linux

```
syslog-header-message message-part
```

The format of the `syslog-header-message` differs depending on the OS environment settings. If necessary, change the settings.

For example, if you use `rsyslog` and specify the following in `/etc/rsyslog.conf`, messages are output in a format corresponding to RFC5424:

```
$ActionFileDefaultTemplate RSYSLOG_SyslogProtocol23Format
```

The format and contents of `message-part` are described below. In `message-part`, a maximum of 953 single-byte characters can be displayed in a `syslog` file.

```
uniform-identifier, unified-specification-revision-number, serial-number,
message-ID, date-and-time, detected-entity, detected-location, audit-event-type,
audit-event-result, audit-event-result-subject-identification-information,
hardware-identification-information, location-information, location-
identification-information, redundancy-identification-information, agent-
information, request-source-host, request-source-port-number, request-
destination-host, request-destination-port-number, batch-operation-
identifier, log-data-type-information, application-identification-
information, reserved-area, message-text
```

Item*	Description
<code>uniform-identifier</code>	Fixed to CELFSS.
<code>unified-specification-revision-number</code>	Fixed to 1.1.
<code>serial-number</code>	Serial number of audit log messages.

Item*	Description
<i>message-ID</i>	Message ID.
<i>date-and-time</i>	The date and time when the message was output. This item is output in the format of <i>yyyy-mm-ddThh:mm:ss.stime-zone</i> .
<i>detected-entity</i>	Component or process name.
<i>detected-location</i>	Host name.
<i>audit-event-type</i>	Event type.
<i>audit-event-result</i>	Event result.
<i>audit-event-result-subject-identification-information</i>	Account ID, process ID, or IP address corresponding to the event.
<i>hardware-identification-information</i>	Hardware model or serial number.
<i>location-information</i>	Identification information for the hardware component.
<i>location-identification-information</i>	Location identification information.
<i>FQDN</i>	Fully qualified domain name.
<i>redundancy-identification-information</i>	Redundancy identification information.
<i>agent-information</i>	Agent information.
<i>request-source-host</i>	Host name of the request sender.
<i>request-source-port-number</i>	Port number of the request sender.
<i>request-destination-host</i>	Host name of the request destination.
<i>request-destination-port-number</i>	Port number of the request destination.
<i>batch-operation-identifier</i>	Serial number of operations through the program.
<i>log-data-type-information</i>	Fixed to BasicLog or DetailLog.
<i>application-identification-information</i>	Program identification information.
<i>reserved-area</i>	Not output. This is a reserved space.

Item*	Description
<i>message-text</i>	The contents vary according to the audit events. Characters that cannot be displayed are output as asterisks (*).
*: Some items are not output for some audit events.	

The following is an example of the message portion of an audit log login event:

```
CELFSS,1.1,0,KAPM01124-I,2017-05-15T14:08:23.1+09:00,HBase-SSO,management-
host,Authentication,Success,uid=system,,,,,,,,,BasicLog,,, "The login was
successful. (session ID = session ID) "
```

Adding a secondary Analyzer detail view server

In addition to sending Analyzer probe server data to a single (local) Analyzer detail view server, you can configure a secondary, cloud-based Analyzer detail view server. The purpose is to host a copy of the probe data where it can be accessed outside of your internal network.



Note: The secondary Analyzer detail view server does not support real-time data; the data might be received at different times from the Analyzer probe server.

The secondary Analyzer detail view server hosts an independent, non-synchronous copy of the probe data and does not constitute a failover configuration. Furthermore, the secondary Analyzer detail view server does not include primary Analyzer detail view server configuration data, including:

- Alert definitions
- Custom reports
- Custom trees
- User logins and profiles

You can use the Analyzer detail view server backup and restore feature to save or copy these settings.

Procedure

1. On the Analyzer probe home page, click **Reconfigure**.
2. Go to **Analyzer detail view Server** tab and click **Add Analyzer detail view Server**.
3. In the **Secondary** Analyzer detail view **Server** window, specify the following details:



Note: If you are connecting the Analyzer detail view server to the Analyzer probe server using the host name and a proxy server, you must add the IP address and host name of the Analyzer detail view server to the `/etc/hosts` file on the Analyzer probe server.

- **Protocol:** **FTP**, **FTPS**, **SFTP**, or **HTTPS**.

The Analyzer detail view server supports SFTP and HTTPS protocols. If you are using an FTP or FTPS protocol, then make sure that the FTP or FTPS server is configured and you provide the FTP or FTPS server IP address in the **Host** field.

- **Host:** Analyzer detail view server or intermediate FTP server IP address.

If you are using an intermediate FTP server as a secondary server, then make sure that you [configure the downloader \(on page 131\)](#) on the Analyzer detail view server to download the data from this FTP server.

- **Port:** Based on the selected protocol.

- **User:** User name for the host. For an Analyzer detail view server the user name is: `meghadata`



Note: If you are using an intermediate FTP server, the FTP user must have the required permission to create a new directory in the current working directory on the FTP server, after connecting to the FTP server.

- **Password:** Password for the host. For an Analyzer detail view server the default password is: `meghadata123`



Note: To improve security for the FTP account, you must change the `meghadata` user default password. Refer to [Changing the megha and meghadata passwords \(on page 88\)](#) for more information.

- **Advanced Settings:**

- **Proxy:** Select to configure a proxy server.

4. Click **Save**.

Configuring the downloader on the Analyzer detail view server

When the Analyzer probe server sends the data to an intermediate FTP server instead of an Analyzer detail view server, then the Analyzer detail view server needs to know details of the FTP server to download the data.

Before you begin



Note: If you do not want to stop the **crond** service, you can stop the specific processes of the Analyzer detail view server and Analyzer probe server by using the **crontab -e** command as described in [Stopping the Analyzer detail view server or Analyzer probe server services \(on page 360\)](#) and [Starting the Analyzer detail view server or Analyzer probe server services \(on page 360\)](#)

Procedure

1. Log on to the Analyzer detail view server through an SSH client (like **putty**) as a root user.
2. Stop the crond service using the command:

```
service crond stop
```

3. Stop the megha service using the command:

```
/usr/local/megha/bin/megha-jetty.sh stop
```

4. Verify the stopped status of the megha service:

```
/usr/local/megha/bin/megha-jetty.sh status
```

5. Run the create or update FTP configuration script:

- If you want to download the data of all the Analyzer probe server appliances, run the following command:

```
sh /usr/local/megha/bin/createOrUpdateFTPConfiguration.sh --create -
--ftpServer FTP-server-host-name-or-IP-address --ftpMethod FTP-method-
(FTP/FTPS/SFTP) --ftpPort FTP-port --ftpUsername FTP-username --
ftpPassword
```

For example:

```
sh /usr/local/megha/bin/createOrUpdateFTPConfiguration.sh --create -
--ftpServer 192.168.1.2 --ftpMethod SFTP --ftpPort 22 --ftpUsername
abc --ftpPassword
```

- If you want to download the data of the specific Analyzer probe server appliances, run the following command:

```
sh /usr/local/megha/bin/createOrUpdateFTPConfiguration.sh --create -
--ftpServer FTP-server-host-name-or-IP-address --ftpMethod FTP-method-
(FTP/FTPS/SFTP) --ftpPort FTP-port --ftpUsername FTP-server-username
--ftpPassword --applianceidOption ApplianceIds --applianceidList
Appliance-ID-list-separated-by-comma
```

For example:

```
sh /usr/local/megha/bin/createOrUpdateFTPConfiguration.sh --create -
--ftpServer 192.168.1.2 --ftpMethod SFTP --ftpPort 22 --ftpUsername
abc --ftpPassword --applianceidOption ApplianceIds --applianceidList
1c5fbdd9-8ed3-43fe-8973-e9cba6d103c6,39cfcb01-11b2-46b4-8fce-
b4d84ea5acda
```

- 6. Type the FTP user password and confirm it.**
- 7. Start the megha service using the command:**

```
/usr/local/megha/bin/megha-jetty.sh start
```

- 8. Start the crond service using the command:**

```
service crond start
```

Chapter 6: Configuring the RAID Agent to monitor Hitachi Enterprise Storage Systems

Before adding the Hitachi Enterprise Storage probe, you choose and configure the RAID Agent based on your monitoring environment and data collection requirements to monitor VSP family or HUS VM.

Determining the appropriate agent for collecting data

The agent to be used depends on your environment. Both agents collect information from storage systems.

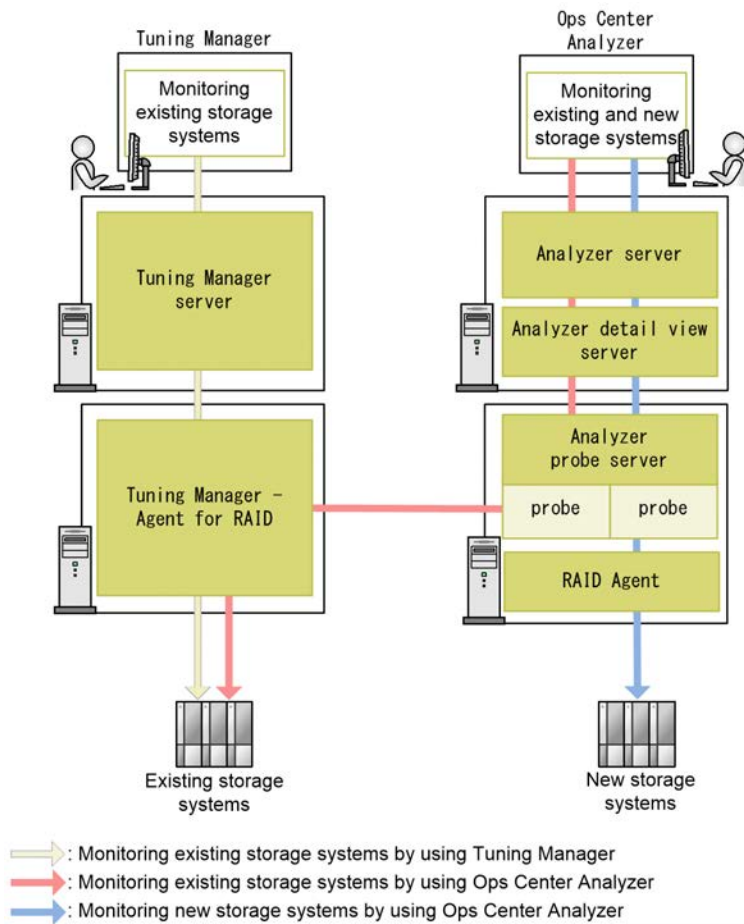
- **RAID Agent:** This agent is installed with Ops Center Analyzer.
- **Tuning Manager - Agent for RAID:** This agent is used in environments where Tuning Manager had previously been used to monitor storage system performance.

The following table shows the correspondence between the environment you are using and the agent to be used by the Hitachi Enterprise Storage probe:

Monitoring environment		Use this Agent	Go to this section
New installation of Ops Center Analyzer		RAID Agent installed with Ops Center Analyzer	Setting up RAID Agent (on page 136)
Migration from Tuning Manager to Ops Center Analyzer		RAID Agent installed with Ops Center Analyzer	Setting up RAID Agent (on page 136)
Migration from Tuning Manager to Ops Center Analyzer; both currently in use	Storage systems previously monitored by Tuning Manager will now be monitored by Ops Center Analyzer.	Tuning Manager - Agent for RAID	Setting up Tuning Manager - Agent for RAID (on page 174)
	Newly installed storage systems to be monitored by Ops Center Analyzer.	RAID Agent installed with Ops Center Analyzer	Setting up RAID Agent (on page 136)

Monitoring environment	Use this Agent	Go to this section
Previous Tuning Manager and Ops Center Analyzer environment now only Ops Center Analyzer	RAID Agent installed with Ops Center Analyzer	Switching from Tuning Manager - Agent for RAID to RAID Agent (on page 183)

The following figure shows the flow of monitoring Ops Center Analyzer when Tuning Manager is used in combination with Ops Center Analyzer:



RAID Agent and Tuning Manager - Agent for RAID cannot connect to the same storage system. Select one of the following:

- To monitor storage systems that are newly installed, connect the storage systems to RAID Agent and monitor the storage systems in Ops Center Analyzer.
- To monitor existing storage systems that were monitored by Tuning Manager using Ops Center Analyzer, use Tuning Manager - Agent for RAID.

Do not uninstall the Tuning Manager server if Tuning Manager - Agent for RAID is being used. The Tuning Manager server is necessary to maintain Tuning Manager - Agent for RAID.

Workflow for adding the Hitachi Enterprise Storage probe

To monitor VSP family or HUS VM by using Ops Center Analyzer, you must use the following procedure to add the Hitachi Enterprise Storage probe to Analyzer probe server.

Procedure

1. Verify the collection methods supported by the monitored storage systems, and determine the collection method to be used by the agent.

For details, see [Selecting the data collection method \(on page 137\)](#).

2. Add the Hitachi Enterprise Storage probe to use to collect information from the monitored storage systems to the Analyzer probe server.

- When collecting information by using RAID Agent bundled with Ops Center Analyzer

Set up RAID Agent and add the Hitachi Enterprise Storage probe to the Analyzer probe server. For details, see [Setting up RAID Agent \(on page 136\)](#).

- When collecting information by using Tuning Manager - Agent for RAID

Set up Tuning Manager - Agent for RAID and add the Hitachi Enterprise Storage probe to the Analyzer probe server. For details, see [Setting up Tuning Manager - Agent for RAID \(on page 174\)](#).

- When you want to change the agent used by the Hitachi Enterprise Storage probe that has already been added.

For details, see [Switching from Tuning Manager - Agent for RAID to RAID Agent \(on page 183\)](#).

Setting up RAID Agent

The Hitachi Enterprise Storage probe collects data from the monitored VSP family or HUS VM using RAID Agent, which is bundled with Ops Center Analyzer.

The workflow for adding the Hitachi Enterprise Storage probe depends on the data collection method. You select the data collection method by specifying the `Access Type` when you create a RAID Agent instance environment, which designates the method used by the RAID Agent to collect data from the storage system.

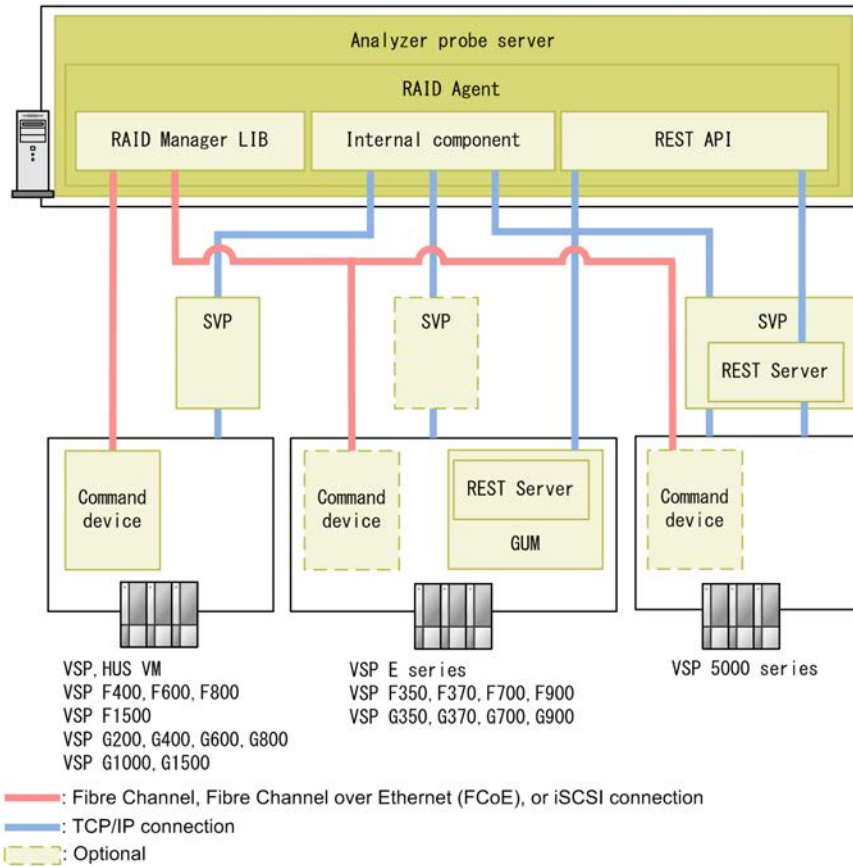
RAID Agent supports the following values for `Access Type`:

- `Access Type: 1`
Data collection using command device and SVP
- `Access Type: 2`
Data collection using command device and REST API
- `Access Type: 3`
Data collection using SVP and REST API
- `Access Type: 4`
Data collection using REST API

Selecting the data collection method

The method for collecting data differs depending on the combination of the storage system configuration and the agent. Specify the collection method in `Access Type` when you create an instance environment. You can specify only one `Access Type` for each storage system.

Consider the above when determining the collection method. The procedure for setting up the Hitachi Enterprise Storage probe varies depending on the value specified in `Access Type`.

Performance data collection methods (for RAID Agent)**Data collection methods**

The data collection method varies depending on the storage system.

To determine which method is supported by your storage systems, use the following table:

Storage systems to be monitored	Data collection method			Access Type to select
	Command devices	SVP	REST API of the storage system	
HUS VM	Used	Used	-	1
VSP				
VSP F400				
VSP F600				
VSP F800				
VSP F1500				
VSP G200				

Storage systems to be monitored	Data collection method			Access Type to select
	Command devices	SVP	REST API of the storage system	
VSP G400 VSP G600 VSP G800 VSP G1000 VSP G1500				
VSP E series	Used	Used	-	1
VSP 5000 series	Used	-	Used	2
VSP F350*	-	Used	Used	3
VSP F370*	-	-	Used	4
VSP F700*				
VSP F900*				
VSP G350*				
VSP G370*				
VSP G700*				
VSP G900*				
<p>*: For details on the microcode version required to collect performance data using the REST API, see Monitoring target storage systems (on page 41).</p> <p>Legend:</p> <p>-: Not used</p>				

Performance data that can be collected

Depending on the data collection method, you can collect different types of performance data.

If RAID Agent bundled with Ops Center Analyzer will be used to monitor VSP E series, VSP 5000 series, VSP F350, F370, F700, F900, VSP G350, G370, G700, or G900, select the `Access Type` based on the information in the following table:

Do you use a network that uses Fibre Channel (use a command device)?	Do you use the SVP?	Do you want to track the following details?	Access Type to select
Yes	Yes	<ul style="list-style-type: none"> Storage system performance and configuration Virtual IDs for parity groups Pool names Tier information Saving capacity and ratio information Current Capacity in License window 	1
Yes	No	<ul style="list-style-type: none"> Storage system performance and configuration Pool names Tier information Saving capacity and ratio information 	2
No	Yes	<ul style="list-style-type: none"> Storage system performance and configuration Virtual IDs for parity groups Current Capacity in License window 	3
No	No	<ul style="list-style-type: none"> Storage system performance and configuration 	4

The number of types of performance data to collect varies depending on the *Access Type*, as follows:

Access Type is 1 > *Access Type* is 2 > *Access Type* is 3 > *Access Type* is 4

This means that, if Fibre Channel is used for the network, more detailed information can be viewed about the storage system. In addition, if the selected *Access Type* is 1, the storage system can be monitored at the same level as the following storage systems:

HUS VM, VSP, VSP F400, F600, F800, F1500, VSP G200, G400, G600, G800, G1000, G1500

For details about performance data, see the *Hitachi Ops Center Analyzer REST API Reference Guide* and the *Hitachi Ops Center Analyzer Detail View Metrics Reference Guide*.

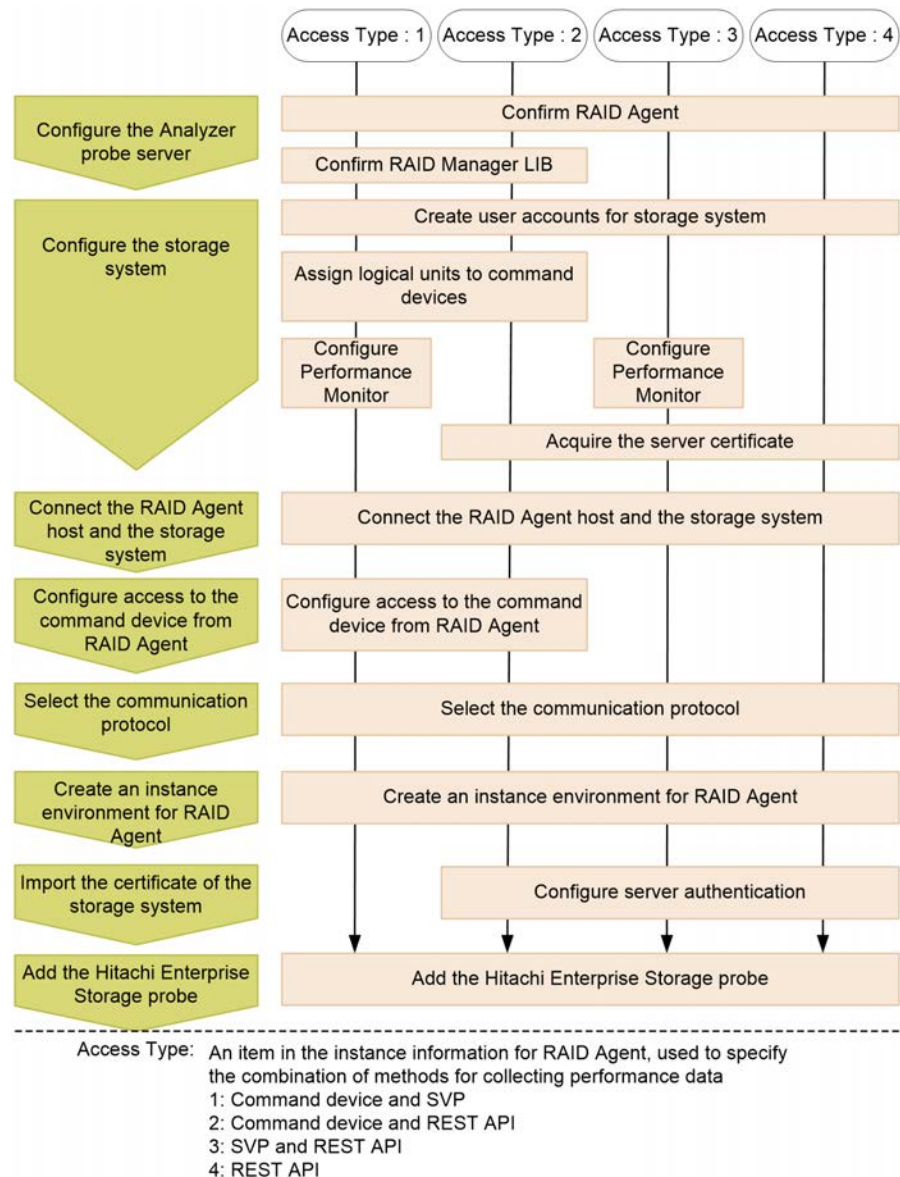
Workflow for setting up the Hitachi Enterprise Storage probe (when using RAID Agent)

To monitor VSP family or HUS VM by using RAID Agent, use the following workflow to add the Hitachi Enterprise Storage probe.



Caution: Before changing the agent used to monitor a storage system from Tuning Manager - Agent for RAID to RAID Agent, make sure that the instance of Tuning Manager - Agent for RAID is not running.

The operations differ depending on the combination of methods for collecting performance data (Access Type).



Next steps

When Access Type is 1: [Configuring RAID Agent for data collection using command devices and SVP \(on page 143\)](#)

When Access Type is 2: [Configuring RAID Agent for data collection using command device and REST API \(on page 152\)](#)

When Access Type is 3: [Configuring RAID Agent for data collection using SVP and REST API \(on page 160\)](#)

When Access Type is 4: [Configuring RAID Agent for data collection using REST API \(on page 168\)](#)

Passing the settings information of Tuning Manager - Agent for RAID to RAID Agent

If you want to migrate from Tuning Manager to Ops Center Analyzer and want to continue monitoring the same storage systems, perform the following procedure so that RAID Agent inherits the instance information and information about data collection intervals from Tuning Manager - Agent for RAID.

If you are currently using both Tuning Manager and Ops Center Analyzer, and want to switch to using only Ops Center Analyzer, you must switch from Tuning Manager - Agent for RAID to the RAID Agent bundled with Ops Center Analyzer. For details on this procedure, see [Switching from Tuning Manager - Agent for RAID to RAID Agent \(on page 183\)](#).

Procedure

1. Check the settings of Tuning Manager - Agent for RAID.
 - a. Display a list of instance names by running the `jpcinslist` command on the host on which Tuning Manager - Agent for RAID is installed:

```
jpcinslist agtd
```

- b. Check the instance information by running the `jpctdchkinst` command on the host on which Tuning Manager - Agent for RAID is installed:

```
jpctdchkinst -inst instance-name
```

- c. If the collection intervals for Tuning Manager - Agent for RAID have been changed, check the collection intervals.
For details about how to check the collection intervals for Tuning Manager - Agent for RAID, see the *Hitachi Command Suite Tuning Manager Agent Administration Guide*.

2. Depending on the information you want to inherit, change the settings of RAID Agent as follows:

- To inherit instance information:

When creating an instance environment for RAID Agent, specify settings as follows, based on the instance information of Tuning Manager - Agent for RAID that you checked.

- The item `Access Type` corresponds to the item `Method for collecting` for Tuning Manager - Agent for RAID.

To set the value that was set for Tuning Manager - Agent for RAID, specify 1.

- Make sure that the value of `Serial No` is the same as the value set for Tuning Manager - Agent for RAID.
- (Optional) If you want RAID Agent to inherit other settings, specify the same values for those settings as were set for Tuning Manager - Agent for RAID.

- To inherit data collection intervals:

Perform this task after you finish configuring RAID Agent.

- Change the collection intervals for RAID Agent by referring to [Changing data collection intervals for RAID Agent \(on page 392\)](#).
- If you are adding a Hitachi Enterprise Storage probe, specify the same collection intervals for the probe as were set for RAID Agent.

Configuring RAID Agent for data collection using command devices and SVP

Use this method to collect all available information about storage system capacity and performance metrics. To use this data collection method, you must specify 1 for `Access Type` when you create the RAID Agent instance environment.

Configuring Analyzer probe server

Confirm RAID Agent

Confirm that the RAID Agent and the Analyzer probe server are installed on the same host. RAID Agent is installed when the Analyzer probe server is installed.

Confirm RAID Manager LIB

If you used the installer to install Analyzer probe server, confirm that RAID Manager Library is installed on the RAID Agent host. In an environment that was created by deploying the OVA file for Analyzer probe server, the RAID Manager Library is already installed.

Configuring storage systems

Create user accounts for a storage system

On the storage system, verify that a user account for use by RAID Agent was created. The user account must meet the following conditions:

- SVP

The account must belong to a user group that has been assigned one of the following roles:

- Storage administrator (viewing)
- Storage administrator (initial setup)
- Storage administrator (system resource management)
- Storage administrator (provisioning)
- Storage administrator (performance management)
- Storage administrator (local backup management)
- Storage administrator (remote backup management)

- Performance Monitor

The user account must belong to a user group that has been assigned the Storage administrator (performance management) role.

For details about how to create a user account for a storage system, see the appropriate documentation for your storage system.

Set up a command device

Verify that a command device exists in the storage system. For details about command devices, see the appropriate documentation for the storage system you are using.

The following restrictions apply to command devices used by RAID Agent:

- If a virtual ID is set on a command device, that command device cannot be monitored by RAID Agent.
- Command devices must be defined as RAW devices. RAW devices must comply with the following rules:
 - Command devices for the ZFS file system cannot be used.
 - Do not create file systems in the logical devices specified as the command devices.
 - Do not mount file systems to the logical devices specified as the command devices.
- If any of the following conditions are met, RAID Agent cannot obtain performance data:
 - A remote command device is used.
 - A virtual command device is used.
 - VMware Fault Tolerance (VMware vSphere Fault Tolerance) is used.

Configure Performance Monitor

Make sure that the following settings have been configured for the instance of Performance Monitor for the storage system. For details on how to configure these settings and the values that can be specified for each setting, see the applicable Performance Monitor documentation for your storage system.

Setting	Description
Monitor switch	Enable the monitoring switch setting
Monitoring-target CUs	Set the logical devices (on a CU basis) from which you want to collect performance data. This setting is not required if you use HUS VM.
Monitoring-target WWNs	Set the performance data collection-target WWNs.
Sampling interval	Set the interval to short range.

Connecting the RAID Agent host and the storage system

Verify that the RAID Agent host and the storage system are connected by the following methods:

- TCP/IP connection for the SVP
- Fibre Channel, Fibre Channel over Ethernet (FCoE), or iSCSI connection for the command device

Some functions cannot be run while performance data is being collected using the SVP. If you execute these functions while performance data is being collected using the SVP of RAID Agent, either the data collection or the execution of one or more functions will fail. Before using a function for which the problem occurs, run the **htmsrv stop** command (/opt/jp1pc/htnm/bin/htmsrv stop -all) to temporarily stop the RAID Agent instance.

The following are examples of tasks that cannot be performed while performance data is being collected using the SVP:

- Data migration in Device Manager
- Displaying the following Storage Navigator windows:
 - Server Priority Manager window
 - Volume Migration window
 - **Usage Monitor** window of True Copy (for HUS VM and VSP)
 - **Usage Monitor** window of Universal Replicator (for HUS VM and VSP)
- Using the export tools described in the Performance Monitor manuals

Configuring access to the command device from RAID Agent

If performance data is to be collected using a command device, make sure that the command device of the monitored storage system can be accessed from the host on which RAID Agent is installed.

Procedure

1. Set an LU path to a logical device designated as the command device.

Set the LU path to the host in which RAID Agent is installed on the logical device designated as the command device. If the installation destination of RAID Agent is a guest OS of VMware ESXi, set the LU path to the host OS.

Access to the command device of RAID Agent might temporarily occupy resources, such as the processor, of the storage system on the LU path. Therefore, when setting an LU path, make sure that the processor to use is not being used by business applications that generate steady I/O traffic.

2. Ensure that the command device can be accessed from a guest OS.

This procedure is necessary if RAID Agent is installed on a guest OS of VMware ESXi. For details, see the VMware ESXi documentation.

Use VMware vSphere Client to add a device to the guest OS. By doing so, if you designate a command device as the device to be added, the command device can be accessed from the guest OS.

When configuring settings to add a device, make sure that the following requirements are met:

- Device type: Hard disk
- Disk selection: Raw device mapping
- Compatibility mode: Physical

Virtual disks (including VMware VVols) cannot be used for the command device.

3. Make sure that the command device can be accessed from the host on which RAID Agent is installed.

Run the `jpctdlistraid` command on the host on which RAID Agent is installed, and confirm that the information you set on the command device is output:

```
/opt/jplpc/tools/jpctdlistraid
```



Tip: In a Linux host environment, rescanning a disk device might change a device file name of the form `/dev/sd`. To prevent this, use the WWID based form of the device file name (`/dev/disk/by-id/scsi-hexadecimal-wwid`). To specify the WWID based file name:

- a. Use the `jpctdlistraid` command to display the `/dev/sd` form of the device file name:

```
/opt/jplpc/tools/jpctdlistraid
```

- b. Use the `ls` command to search for the symbolic links managed in the `/dev/disk/by-id` directory for the WWID device file name mapped to the corresponding `/dev/sd` file name.

For example:

```
ls -la /dev/disk/by-id/* | grep sdc
```

- c. Use the output as the Command Device File Name.

Selecting the communication protocol

To monitor storage systems for which the communication protocol can be selected, set TLS 1.2 as the communication protocol.

Creating an instance environment

To collect data from the Hitachi Enterprise Storage probe, you must create a RAID Agent instance environment on the host on which Analyzer probe server is installed.

Procedure

1. On the Analyzer probe server, run the `jpccinssetup` command with the service key and instance name specified. Instance names must be no longer than 32 bytes, and only half-width alphanumeric characters (A-Z, a-z, 0-9) are allowed.

For example, to create an instance environment for the instance named 35053 for RAID Agent, run the following command:

```
/opt/jplpc/tools/jpccinssetup agtd -inst 35053
```

2. Set up the instance information for the storage system you will monitor.

To use the default value (or no value), press **Enter**.

The following table lists the instance information to specify.

Item	Description
Storage model	<p>Specify the storage type.</p> <ul style="list-style-type: none"> 11: VSP 12: VSP G1000, G1500, VSP F1500 13: VSP 5000 series 21: HUS VM 22: VSP G200, G400, G600, G800, VSP F400, F600, F800 23: VSP E990, VSP G350, G370, G700, G900, VSP F350, F370, F700, F900
Serial No	Specify the serial number of the storage system.
Access Type	<p>Specify 1.</p> <p>If a value other than 13 and 23 is specified for <code>Storage model</code>, 1 is automatically specified.</p>
Command Device File Name	<p>Specify the device file name of the storage system specified for <code>Serial No</code>, from among the command devices in the list output by using the <code>/opt/jplpc/tools/jpctdlstraid</code> command. RAID Agent uses this command device to collect information about the storage system.</p> <p>The <code>/dev/sd*</code> form of the device file name might be changed by rescanning the disk device. The best practice is to use the WWID based form of the device file name. See Configuring access to the command device from RAID Agent (on page 146) for details about assigning a WWID based device file name.</p>
Unassigned Open Volume Monitoring ¹	<p>Specify Y to monitor a logical device or a parity group for which an open system emulation type has been set and that has not been mapped to a port.</p> <ul style="list-style-type: none"> If no value is entered, the default value Y is set. If you enter a value other than Y, y, N, or n, the system prompts you to enter a value again.

Item	Description
Mainframe Volume Monitoring ¹	<p>Specify <code>Y</code> to monitor a logical device for which the emulation type used for a mainframe is set.</p> <ul style="list-style-type: none"> For HUS VM, mainframe emulation is not supported. Mainframe volumes are excluded from monitoring when an HUS VM is monitored. If no value is entered, the default value <code>Y</code> is set. If you enter a value other than <code>Y</code>, <code>y</code>, <code>N</code>, or <code>n</code>, the system prompts you to enter a value again. <p>Ops Center Analyzer does not obtain information about mainframe devices. For this reason, you cannot identify the mainframe host with which a logical device is associated.</p>
SVP IP Address or Host Name	Specify the IP address or host name of the SVP that manages the storage system that was specified for <code>Serial No.</code>
Storage User ID for SVP	Specify the user ID of the user account that was created to access the target storage system using the SVP.
Storage Password for SVP	Specify the password of the user account that was created to access the target storage system using the SVP.
SVP Port No	<p>Specify the port number if <code>Storage model</code> is set to 22 or 23. You can specify a value from 0 to 65535. The default value is 1099.</p> <p>This value is the same as the initial value for the <code>RMIIFRegist</code> port number of the storage system. To change the port number of the storage system, see the storage system manual that explains how to change or initialize the port number for use with the SVP.</p>

Item	Description
SVP HTTPS Port No	<p>If 22 or 23 is specified for <code>Storage model</code>, specify the port number that is used for connection using the HTTPS protocol, from a host on which RAID Agent is installed, to the SVP. You can specify a value from 0 to 65535. The default value is 443.</p> <p>This value is the same as the initial value for the <code>MAPPWebServerHttps</code> port number of the storage system. To change the port number of the storage system, see the storage system manual that explains how to change or initialize the port number for use with the SVP.</p>
Java VM Heap Memory setting Method	<p>Specify the method to use for setting the required memory size for the Java VM. The default value is 1.</p> <p>However, in a large-scale environment that exceeds an assumed value², if you specify 1 for this item, processing might end abnormally because of insufficient memory. For this reason, for a large-scale environment, specify 2.</p> <ul style="list-style-type: none"> ▪ To specify a method that automatically calculates the required memory size based on the maximum number of volumes: 1 ▪ To specify a method where the user specifies the memory size: 2
Maximum number of Volumes	<p>If you specified 1 for <code>Java VM Heap Memory setting Method</code>, specify the maximum number of volumes to be created on the target storage system. The required memory size for the Java VM will be automatically specified based on this setting.</p> <p>You can specify a value in the range from 1000 to 99999. The default value is 4000.</p>
Java VM Heap Memory for SVP	<p>If you specified 2 for <code>Java VM Heap Memory setting Method</code>, specify the required memory size for the Java VM. The default value is 1.</p> <ul style="list-style-type: none"> ▪ 1: 0.5 GB ▪ 2: 1.0 GB

Item	Description
	<ul style="list-style-type: none"> 3: 2.0 GB 4: 4.0 GB 5: 8.0 GB
<p>Notes:</p> <p>1. Depending on the microcode version of the storage system, you might not be able to use the Mainframe Volume Monitoring or Unassigned Open Volume Monitoring function even though you enabled the setting (and verified that it is enabled).</p> <p>2. The following values are assumed for the environment when the required memory size is calculated based on the maximum number of volumes and the data is collected by using the SVP:</p> <ul style="list-style-type: none"> Number of LU paths: 0 Sampling interval (in minutes): 1 	

- When configuring multiple instances, repeat steps 1 and 2 for each instance.
- Make sure that RAID Manager LIB is installed.
- Before you start operation in an instance environment, run the `jpctdchkinst` command to verify the instance settings.

The command references the set instance information. (This command checks whether the settings allow information to be collected from the storage system monitored by RAID Agent.)

```
/opt/jplpc/tools/jpctdchkinst -inst instance-name
```



Note: If you upgraded from Infrastructure Analytics Advisor 4.2.1-00 or earlier and have not changed the settings in the instance information, VSP G350, G370, G700, G900, VSP F350, F370, F700, or F900 storage systems are reported as, VSP G200 G400 G600 G800 F400 F600 F800 by the `jpctdchkinst` command.

- (Optional) Configure the collection-time definition file (`conf_refresh_times.ini`).
Set the time for collecting configuration information as described in [Changing the configuration information collection time \(on page 396\)](#). This setting helps ensure the proper collection of performance data when the storage system contains a large amount of configuration data.
- Run the following command to start the RAID Agent instance services:

```
/opt/jplpc/htm/bin/htmsrv start -all
```



Note: You must wait for approximately one hour to add the Hitachi Enterprise Storage probe after adding an instance on the RAID agent.

Next steps

[Adding Hitachi Enterprise Storage probe \(on page 185\)](#)

Configuring RAID Agent for data collection using command device and REST API

Use this method to collect all available information about storage system capacity performance metrics through both Fibre Channel and IP connections without using an SVP. To use this data collection method, you must specify 2 for `Access Type` when you create the RAID Agent instance environment.

Configuring Analyzer probe server

Confirm RAID Agent

Confirm that the RAID Agent and the Analyzer probe server are installed on the same host. RAID Agent is installed when the Analyzer probe server is installed.

Confirm RAID Manager LIB

If you used the installer to install Analyzer probe server, confirm that RAID Manager Library is installed on the RAID Agent host. In an environment that was created by deploying the OVA file for Analyzer probe server, the RAID Manager Library is already installed.

Configuring storage systems

Create user accounts for a storage system

On the storage system, verify that a user account for use by RAID Agent was created. The user account must meet the following conditions:

- REST API

The user account must belong to a user group for which All Resource Groups Assigned is enabled. If the user group is assigned to one of the following roles, All Resource Groups Assigned is enabled.

- Security Administrator (View Only)
- Security Administrator (View & Modify)
- Audit Log Administrator (View Only)
- Audit Log Administrator (View & Modify)
- Support Personnel (Vendor Only)

For details about how to create a user account for a storage system, see the appropriate documentation for your storage system.

Set up a command device

Verify that a command device exists in the storage system. For details about command devices, see the appropriate documentation for the storage system you are using.

The following restrictions apply to command devices used by RAID Agent:

- If a virtual ID is set on a command device, that command device cannot be monitored by RAID Agent.
- Command devices must be defined as RAW devices. RAW devices must comply with the following rules:
 - Command devices for the ZFS file system cannot be used.
 - Do not create file systems in the logical devices specified as the command devices.
 - Do not mount file systems to the logical devices specified as the command devices.
- If any of the following conditions are met, RAID Agent cannot obtain performance data:
 - A remote command device is used.
 - A virtual command device is used.
 - VMware Fault Tolerance (VMware vSphere Fault Tolerance) is used.

Acquire a server certificate

Acquire the server certificate of the storage system. This server certificate is required for server authentication, as well as for encryption by using HTTPS communication between RAID Agent and the storage system. If you are not using server authentication, you do not need to acquire a server certificate.

Connecting the RAID Agent host and the storage system

Verify that the RAID Agent host and the storage system are connected by the following methods:

- TCP/IP connection for the GUM (CTL)
- Fibre Channel, Fibre Channel over Ethernet (FCoE), or iSCSI connection for the command device

Configuring access to the command device from RAID Agent

If performance data is to be collected using a command device, make sure that the command device of the monitored storage system can be accessed from the host on which RAID Agent is installed.

Procedure

1. Set an LU path to a logical device designated as the command device.

Set the LU path to the host in which RAID Agent is installed on the logical device designated as the command device. If the installation destination of RAID Agent is a guest OS of VMware ESXi, set the LU path to the host OS.

Access to the command device of RAID Agent might temporarily occupy resources, such as the processor, of the storage system on the LU path. Therefore, when setting an LU path, make sure that the processor to use is not being used by business applications that generate steady I/O traffic.

2. Ensure that the command device can be accessed from a guest OS.

This procedure is necessary if RAID Agent is installed on a guest OS of VMware ESXi. For details, see the VMware ESXi documentation.

Use VMware vSphere Client to add a device to the guest OS. By doing so, if you designate a command device as the device to be added, the command device can be accessed from the guest OS.

When configuring settings to add a device, make sure that the following requirements are met:

- Device type: Hard disk
- Disk selection: Raw device mapping
- Compatibility mode: Physical

Virtual disks (including VMware VVols) cannot be used for the command device.

3. Make sure that the command device can be accessed from the host on which RAID Agent is installed.

Run the `jpctdlistraid` command on the host on which RAID Agent is installed, and confirm that the information you set on the command device is output:

```
/opt/jplpc/tools/jpctdlistraid
```



Tip: In a Linux host environment, rescanning a disk device might change a device file name of the form `/dev/sd`. To prevent this, use the WWID based form of the device file name (`/dev/disk/by-id/scsi-hexadecimal-WWID`). To specify the WWID based file name:

- a. Use the `jpctdlistraid` command to display the `/dev/sd` form of the device file name:

```
/opt/jplpc/tools/jpctdlistraid
```

- b. Use the `ls` command to search for the symbolic links managed in the `/dev/disk/by-id` directory for the WWID device file name mapped to the corresponding `/dev/sd` file name.

For example:

```
ls -la /dev/disk/by-id/* | grep sdc
```

- c. Use the output as the Command Device File Name.

Selecting the communication protocol

To monitor storage systems for which the communication protocol can be selected, set TLS 1.2 as the communication protocol.

Creating an instance environment

To collect data from the Hitachi Enterprise Storage probe, you must create a RAID Agent instance environment on the host on which Analyzer probe server is installed.

Procedure

1. On the Analyzer probe server, run the **jpcinssetup** command with the service key and instance name specified. Instance names must be no longer than 32 bytes, and only half-width alphanumeric characters (A-Z, a-z, 0-9) are allowed.

For example, to create an instance environment for the instance named 35053 for RAID Agent, run the following command:

```
/opt/jplpc/tools/jpcinssetup agtd -inst 35053
```

2. Set up the instance information for the storage system you will monitor.

To use the default value (or no value), press **Enter**.

The following table lists the instance information to specify.

Item	Description
Storage model	Specify the storage type. <ul style="list-style-type: none"> 13: VSP 5000 series 23: VSP E990, VSP G350, G370, G700, G900, VSP F350, F370, F700, F900
Serial No	Specify the serial number of the storage system.
Access Type	Specify 2.
Command Device File Name	Specify the device file name of the storage system specified for Serial No , from among the command devices in the list output by using the <code>/opt/jplpc/tools/jpctdlistraid</code> command. RAID Agent uses this command device to collect information about the storage system. The <code>/dev/sd*</code> form of the device file name might be changed by rescanning the disk device. The best practice is to use the WWID based form of the device file name. See Configuring access to the command device from RAID Agent (on page 146) for details about assigning a WWID based device file name.

Item	Description
Unassigned Open Volume Monitoring ¹	<p>Specify <code>Y</code> to monitor a logical device or a parity group for which an open system emulation type has been set and that has not been mapped to a port.</p> <ul style="list-style-type: none"> ▪ If no value is entered, the default value <code>Y</code> is set. ▪ If you enter a value other than <code>Y</code>, <code>y</code>, <code>N</code>, or <code>n</code>, the system prompts you to enter a value again.
Mainframe Volume Monitoring ¹	<p>Specify <code>Y</code> to monitor a logical device for which the emulation type used for a mainframe is set.</p> <ul style="list-style-type: none"> ▪ For HUS VM, mainframe emulation is not supported. Mainframe volumes are excluded from monitoring when an HUS VM is monitored. ▪ If no value is entered, the default value <code>Y</code> is set. ▪ If you enter a value other than <code>Y</code>, <code>y</code>, <code>N</code>, or <code>n</code>, the system prompts you to enter a value again. <p>Ops Center Analyzer does not obtain information about mainframe devices. For this reason, you cannot identify the mainframe host with which a logical device is associated.</p>
SVP IP Address or Host Name	If <code>13</code> is specified for <code>Storage model</code> , specify the IP address or host name of the SVP that manages the storage system that was specified for <code>Serial No.</code>
GUM(CTL) IP Address or Host Name (Primary)	<p>If <code>23</code> is specified for <code>Storage model</code>, specify the IP address or the host name (for which name resolution is possible) of the GUM (CTL) of the storage system that was specified for <code>Serial No.</code> The default value is blank.</p> <p>Connections with the connection destination set for GUM(CTL) IP Address or Host Name (Primary) will be prioritized.</p>

Item	Description
GUM(CTL) IP Address or Host Name (Secondary)	Note that you do not need to specify both GUM(CTL) IP Address or Host Name (Primary) and GUM(CTL) IP Address or Host Name (Secondary).
Storage User ID for REST-API	Specify the user ID of the user account that was created for accessing the target storage system using the REST API.
Storage Password for REST-API	Specify the password of the user account that was created for accessing the target storage system using the REST API.
REST-API Protocol	Specify the protocol to use for accessing the target storage system using the REST API. The default value is 1. <ul style="list-style-type: none"> To use HTTP: 1 To use HTTPS: 2
Java VM Heap Memory setting Method	Specify the method to use for setting the required memory size for the Java VM. The default value is 1. However, in a large-scale environment that exceeds an assumed value ² , if you specify 1 for this item, processing might end abnormally because of insufficient memory. For this reason, for a large-scale environment, specify 2. <ul style="list-style-type: none"> To specify a method that automatically calculates the required memory size based on the maximum number of volumes: 1 To specify a method where the user specifies the memory size: 2
Maximum number of Volumes	If you specified 1 for Java VM Heap Memory setting Method, specify the maximum number of volumes to be created on the target storage system. The required memory size for the Java VM will be automatically specified based on this setting. You can specify a value in the range from 1000 to 99999. The default value is 4000.
Java VM Heap Memory for REST-API	If you specified 2 for Java VM Heap Memory setting Method, specify the required

Item	Description
	<p>memory size for the Java VM. The default value is 1.</p> <ul style="list-style-type: none"> ▪ 1: 128 MB ▪ 2: 256 MB ▪ 3: 512 MB ▪ 4: 1.0 GB ▪ 5: 2.0 GB ▪ 6: 4.0 GB ▪ 7: 8.0 GB
<p>Notes:</p> <p>1. Depending on the microcode version of the storage system, you might not be able to use the <code>Mainframe Volume Monitoring</code> or <code>Unassigned Open Volume Monitoring</code> function even though you enabled the setting (and verified that it is enabled).</p> <p>2. The following values are assumed for the environment when the required memory size is calculated based on the maximum number of volumes and the data is collected by using the REST API:</p> <ul style="list-style-type: none"> ▪ Number of LU paths per LDEV: 4 ▪ Number of SPM settings per LDEV: 4 ▪ Number of host groups assigned to each LDEV: 1 ▪ Number of WWNs assigned to the hosts of each LDEV: 2 	

3. When configuring multiple instances, repeat steps 1 and 2 for each instance.
4. Make sure that RAID Manager LIB is installed.
5. Before you start operation in an instance environment, run the `jpctdchkinst` command to verify the instance settings.

The command references the set instance information. (This command checks whether the settings allow information to be collected from the storage system monitored by RAID Agent.)

```
/opt/jplpc/tools/jpctdchkinst -inst instance-name
```

6. (Optional) Configure the collection-time definition file (`conf_refresh_times.ini`).
Set the time for collecting configuration information as described in [Changing the configuration information collection time \(on page 396\)](#). This setting helps ensure the proper collection of performance data when the storage system contains a large amount of configuration data.

7. Run the following command to start the RAID Agent instance services:

```
/opt/jplpc/htnm/bin/htmsrv start -all
```



Note: You must wait for approximately one hour to add the Hitachi Enterprise Storage probe after adding an instance on the RAID agent.

Importing a certificate to the truststore for RAID Agent

To enable verification of a storage system's server certificate in RAID Agent, import the storage system's certificate to the truststore for RAID Agent, and then edit the `ipdc.properties` file.

Before you begin

- You must have the root permission.
- You must prepare the storage system's certificate.

If you use a certificate issued by a certificate authority, the certificates of all the certificate authorities, from the certificate authority that issued the storage system's server certificate to the root certificate authority, must be connected in a chain of trust.

- If the storage system's certificate already exists in the truststore, delete the existing certificate before importing new certificate. To delete the existing certificate, execute the following command:

```
rm /opt/jplpc/agtd/agent/instance-name/jssecacerts
```

Procedure

1. Execute the following command to import the storage system's certificate to the truststore:

```
/opt/jplpc/htnm/HBasePSB/jdk/bin/keytool -import -alias alias-name -file certificate-file-name -keystore truststore-file-name -storepass access-password-for-truststore
```

- For *alias-name*, specify a name that makes it possible to determine which storage system the server certificate belongs to.
- For *certificate-file-name*, specify the absolute path of the location in which the certificate is stored.
- For *truststore-file-name*, specify the following absolute path:

```
/opt/jplpc/agtd/agent/instance-name/jssecacerts
```
- For *access-password-for-truststore*, specify a password of your choice.

2. Enable verification of the server certificate by changing the following properties in the file `/opt/jplpc/agt/agent/instance-name/ipdc.properties`. If there is a hash mark (#) at the beginning of a property line, delete that hash mark.

- `ssl.check.cert=true`
- `ssl.check.cert.self.truststore=true`
- `ssl.check.cert.hostname=true`

**Note:**

- To check the name of the host of the SSL certificate, specify a host name that can be resolved for GUM(CTL) IP Address or Host Name in the RAID Agent instance information. If you cannot specify a host name that can be resolved, specify `false` because the host name cannot be verified.
- If the web server certificate is not a wildcard certificate, specify `false`, because the host name cannot be verified.

3. Execute the command `jpctdchkinst` and confirm the instance settings:

```
/opt/jplpc/tools/jpctdchkinst -inst instance-name
```

4. Execute the following commands to restart the services of the RAID Agent instance:

```
/opt/jplpc/htm/bin/htmsrv stop -all
```

```
/opt/jplpc/htm/bin/htmsrv start -all
```

Next steps

[Adding Hitachi Enterprise Storage probe \(on page 185\)](#)

Configuring RAID Agent for data collection using SVP and REST API

Use this method to collect all available information about storage system capacity and performance metrics through an IP network connection. To use this data collection method, you must specify 3 for `Access Type` when you create the RAID Agent instance environment.

Configuring Analyzer probe server

Confirm RAID Agent

Confirm that the RAID Agent and the Analyzer probe server are installed on the same host. RAID Agent is installed when the Analyzer probe server is installed.

Configuring storage systems

Create user accounts for a storage system

On the storage system, verify that a user account for use by RAID Agent was created. The user account must meet the following conditions:

- SVP

The account must belong to a user group that has been assigned one of the following roles:

- Storage administrator (viewing)
- Storage administrator (initial setup)
- Storage administrator (system resource management)
- Storage administrator (provisioning)
- Storage administrator (performance management)
- Storage administrator (local backup management)
- Storage administrator (remote backup management)

- REST API

The user account must belong to a user group for which All Resource Groups Assigned is enabled. If the user group is assigned to one of the following roles, All Resource Groups Assigned is enabled.

- Security Administrator (View Only)
- Security Administrator (View & Modify)
- Audit Log Administrator (View Only)
- Audit Log Administrator (View & Modify)
- Support Personnel (Vendor Only)

- Performance Monitor

The user account must belong to a user group that has been assigned the Storage administrator (performance management) role.

For details about how to create a user account for a storage system, see the appropriate documentation for your storage system.

Configure Performance Monitor

Make sure that the following settings have been configured for the instance of Performance Monitor for the storage system. For details on how to configure these settings and the values that can be specified for each setting, see the applicable Performance Monitor documentation for your storage system.

Setting	Description
Monitor switch	Enable the monitoring switch setting

Setting	Description
Monitoring-target CUs	Set the logical devices (on a CU basis) from which you want to collect performance data. This setting is not required if you use HUS VM.
Monitoring-target WWNs	Set the performance data collection-target WWNs.
Sampling interval	Set the interval to short range.

Acquire a server certificate

Acquire the server certificate of the storage system. This server certificate is required for server authentication, as well as for encryption by using HTTPS communication between RAID Agent and the storage system. If you are not using server authentication, you do not need to acquire a server certificate.

Connecting the RAID Agent host and the storage system

Verify that the RAID Agent host and the storage system are connected by the following methods:

- TCP/IP connection for the SVP
- TCP/IP connection for the GUM (CTL)

Some functions cannot be run while performance data is being collected using the SVP. If you execute these functions while performance data is being collected using the SVP of RAID Agent, either the data collection or the execution of one or more functions will fail. Before using a function for which the problem occurs, run the **htmsrv stop** command (`/opt/jplpc/htnm/bin/htmsrv stop -all`) to temporarily stop the RAID Agent instance.

The following are examples of tasks that cannot be performed while performance data is being collected using the SVP:

- Data migration in Device Manager
- Displaying the following Storage Navigator windows:
 - Server Priority Manager window
 - Volume Migration window
 - **Usage Monitor** window of True Copy (for HUS VM and VSP)
 - **Usage Monitor** window of Universal Replicator (for HUS VM and VSP)
- Using the export tools described in the Performance Monitor manuals

Selecting the communication protocol

To monitor storage systems for which the communication protocol can be selected, set TLS 1.2 as the communication protocol.

Creating an instance environment

To collect data from the Hitachi Enterprise Storage probe, you must create a RAID Agent instance environment on the host on which Analyzer probe server is installed.

Procedure

1. On the Analyzer probe server, run the **jpcinssetup** command with the service key and instance name specified. Instance names must be no longer than 32 bytes, and only half-width alphanumeric characters (A-Z, a-z, 0-9) are allowed.

For example, to create an instance environment for the instance named 35053 for RAID Agent, run the following command:

```
/opt/jplpc/tools/jpcinssetup agtd -inst 35053
```

2. Set up the instance information for the storage system you will monitor.

To use the default value (or no value), press **Enter**.

The following table lists the instance information to specify.

Item	Description
Storage model	Specify the storage type. <ul style="list-style-type: none"> 13: VSP 5000 series 23: VSP E990, VSP G350, G370, G700, G900, VSP F350, F370, F700, F900
Serial No	Specify the serial number of the storage system.
Access Type	Specify 3.
SVP IP Address or Host Name	Specify the IP address or host name of the SVP that manages the storage system that was specified for <code>Serial No</code> .
Storage User ID for SVP	Specify the user ID of the user account that was created to access the target storage system using the SVP.
Storage Password for SVP	Specify the password of the user account that was created to access the target storage system using the SVP.
SVP Port No	Specify the port number if <code>Storage model</code> is set to 22 or 23. You can specify a value from 0 to 65535. The default value is 1099.

Item	Description
	This value is the same as the initial value for the <code>RMIIFRegist</code> port number of the storage system. To change the port number of the storage system, see the storage system manual that explains how to change or initialize the port number for use with the SVP.
SVP HTTPS Port No	<p>If 22 or 23 is specified for <code>Storage model</code>, specify the port number that is used for connection using the HTTPS protocol, from a host on which RAID Agent is installed, to the SVP. You can specify a value from 0 to 65535. The default value is 443.</p> <p>This value is the same as the initial value for the <code>MAPPWebServerHttps</code> port number of the storage system. To change the port number of the storage system, see the storage system manual that explains how to change or initialize the port number for use with the SVP.</p>
GUM(CTL) IP Address or Host Name (Primary)	<p>If 23 is specified for <code>Storage model</code>, specify the IP address or the host name (for which name resolution is possible) of the GUM (CTL) of the storage system that was specified for <code>Serial No.</code> The default value is blank. Connections with the connection destination set for <code>GUM(CTL) IP Address or Host Name (Primary)</code> will be prioritized.</p> <p>Note that you do not need to specify both <code>GUM(CTL) IP Address or Host Name (Primary)</code> and <code>GUM(CTL) IP Address or Host Name (Secondary)</code>.</p>
GUM(CTL) IP Address or Host Name (Secondary)	
Storage User ID for REST-API	Specify the user ID of the user account that was created for accessing the target storage system using the REST API.
Storage Password for REST-API	Specify the password of the user account that was created for accessing the target storage system using the REST API.

Item	Description
REST-API Protocol	<p>Specify the protocol to use for accessing the target storage system using the REST API. The default value is 1.</p> <ul style="list-style-type: none"> ▪ To use HTTP: 1 ▪ To use HTTPS: 2
Java VM Heap Memory setting Method	<p>Specify the method to use for setting the required memory size for the Java VM. The default value is 1.</p> <p>However, in a large-scale environment that exceeds an assumed value*, if you specify 1 for this item, processing might end abnormally because of insufficient memory. For this reason, for a large-scale environment, specify 2.</p> <ul style="list-style-type: none"> ▪ To specify a method that automatically calculates the required memory size based on the maximum number of volumes: 1 ▪ To specify a method where the user specifies the memory size: 2
Maximum number of Volumes	<p>If you specified 1 for Java VM Heap Memory setting Method, specify the maximum number of volumes to be created on the target storage system. The required memory size for the Java VM will be automatically specified based on this setting.</p> <p>You can specify a value in the range from 1000 to 99999. The default value is 4000.</p>
Java VM Heap Memory for SVP	<p>If you specified 2 for Java VM Heap Memory setting Method, specify the required memory size for the Java VM. The default value is 1.</p> <ul style="list-style-type: none"> ▪ 1: 0.5 GB ▪ 2: 1.0 GB ▪ 3: 2.0 GB ▪ 4: 4.0 GB ▪ 5: 8.0 GB
Java VM Heap Memory for REST-API	<p>If you specified 2 for Java VM Heap Memory setting Method, specify the required</p>

Item	Description
	<p>memory size for the Java VM. The default value is 1.</p> <ul style="list-style-type: none"> ▪ 1: 128 MB ▪ 2: 256 MB ▪ 3: 512 MB ▪ 4: 1.0 GB ▪ 5: 2.0 GB ▪ 6: 4.0 GB ▪ 7: 8.0 GB
<p>*: The following values are assumed for the environment when the required memory size is calculated based on the maximum number of volumes.</p> <ul style="list-style-type: none"> ▪ If data is collected by using the REST API: <ul style="list-style-type: none"> ▪ Number of LU paths per LDEV: 4 ▪ Number of SPM settings per LDEV: 4 ▪ Number of host groups assigned to each LDEV: 1 ▪ Number of WWNs assigned to the hosts of each LDEV: 2 ▪ If data is collected by using the SVP: <ul style="list-style-type: none"> ▪ Number of LU paths: 0 ▪ Sampling interval (in minutes): 1 	

3. When configuring multiple instances, repeat steps 1 and 2 for each instance.
4. Before you start operation in an instance environment, run the `jpctdchkinst` command to verify the instance settings.

The command references the set instance information. (This command checks whether the settings allow information to be collected from the storage system monitored by RAID Agent.)

```
/opt/jplpc/tools/jpctdchkinst -inst instance-name
```

5. (Optional) Configure the collection-time definition file (`conf_refresh_times.ini`).
Set the time for collecting configuration information as described in [Changing the configuration information collection time \(on page 396\)](#). This setting helps ensure the proper collection of performance data when the storage system contains a large amount of configuration data.
6. Run the following command to start the RAID Agent instance services:

```
/opt/jplpc/htnm/bin/htmsrv start -all
```



Note: You must wait for approximately one hour to add the Hitachi Enterprise Storage probe after adding an instance on the RAID agent.

Importing a certificate to the truststore for RAID Agent

To enable verification of a storage system's server certificate in RAID Agent, import the storage system's certificate to the truststore for RAID Agent, and then edit the `ipdc.properties` file.

Before you begin

- You must have the root permission.
- You must prepare the storage system's certificate.
If you use a certificate issued by a certificate authority, the certificates of all the certificate authorities, from the certificate authority that issued the storage system's server certificate to the root certificate authority, must be connected in a chain of trust.
- If the storage system's certificate already exists in the truststore, delete the existing certificate before importing new certificate. To delete the existing certificate, execute the following command:

```
rm /opt/jplpc/agtd/agent/instance-name/jssecacerts
```

Procedure

1. Execute the following command to import the storage system's certificate to the truststore:

```
/opt/jplpc/htnm/HBasePSB/jdk/bin/keytool -import -alias alias-name -  
file certificate-file-name -keystore truststore-file-name -storepass  
access-password-for-truststore
```

- For *alias-name*, specify a name that makes it possible to determine which storage system the server certificate belongs to.
- For *certificate-file-name*, specify the absolute path of the location in which the certificate is stored.
- For *truststore-file-name*, specify the following absolute path:
`/opt/jplpc/agtd/agent/instance-name/jssecacerts`
- For *access-password-for-truststore*, specify a password of your choice.

2. Enable verification of the server certificate by changing the following properties in the file `/opt/jplpc/agt/agent/instance-name/ipdc.properties`. If there is a hash mark (#) at the beginning of a property line, delete that hash mark.

- `ssl.check.cert=true`
- `ssl.check.cert.self.truststore=true`
- `ssl.check.cert.hostname=true`

**Note:**

- To check the name of the host of the SSL certificate, specify a host name that can be resolved for GUM(CTL) IP Address or Host Name in the RAID Agent instance information. If you cannot specify a host name that can be resolved, specify `false` because the host name cannot be verified.
- If the web server certificate is not a wildcard certificate, specify `false`, because the host name cannot be verified.

3. Execute the command `jpctdchkinst` and confirm the instance settings:

```
/opt/jplpc/tools/jpctdchkinst -inst instance-name
```

4. Execute the following commands to restart the services of the RAID Agent instance:

```
/opt/jplpc/htm/bin/htmsrv stop -all
```

```
/opt/jplpc/htm/bin/htmsrv start -all
```

Next steps

[Adding Hitachi Enterprise Storage probe \(on page 185\)](#)

Configuring RAID Agent for data collection using REST API

Use this method to collect basic information about storage system capacity and performance metrics through an IP connection. To use this data collection method, you must specify 4 for `Access Type` when you create the RAID Agent instance environment.

Configuring Analyzer probe server

Confirm RAID Agent

Confirm that the RAID Agent and the Analyzer probe server are installed on the same host. RAID Agent is installed when the Analyzer probe server is installed.

Configuring storage systems

Create user accounts for a storage system

On the storage system, verify that a user account for use by RAID Agent was created. The user account must meet the following conditions:

- REST API

The user account must belong to a user group for which All Resource Groups Assigned is enabled. If the user group is assigned to one of the following roles, All Resource Groups Assigned is enabled.

- Security Administrator (View Only)
- Security Administrator (View & Modify)
- Audit Log Administrator (View Only)
- Audit Log Administrator (View & Modify)
- Support Personnel (Vendor Only)

For details about how to create a user account for a storage system, see the appropriate documentation for your storage system.

Acquire a server certificate

Acquire the server certificate of the storage system. This server certificate is required for server authentication, as well as for encryption by using HTTPS communication between RAID Agent and the storage system. If you are not using server authentication, you do not need to acquire a server certificate.

Connecting the RAID Agent host and the storage system

Verify that the RAID Agent host and the storage system are connected by the following method:

- TCP/IP connection for the GUM (CTL)

Selecting the communication protocol

To monitor storage systems for which the communication protocol can be selected, set TLS 1.2 as the communication protocol.

Creating an instance environment

To collect data from the Hitachi Enterprise Storage probe, you must create a RAID Agent instance environment on the host on which Analyzer probe server is installed.

Procedure

1. On the Analyzer probe server, run the **jpcinssetup** command with the service key and instance name specified. Instance names must be no longer than 32 bytes, and only half-width alphanumeric characters (A-Z, a-z, 0-9) are allowed.

For example, to create an instance environment for the instance named 35053 for RAID Agent, run the following command:

```
/opt/jplpc/tools/jpcinssetup agtd -inst 35053
```

2. Set up the instance information for the storage system you will monitor.

To use the default value (or no value), press **Enter**.

The following table lists the instance information to specify.

Item	Description
Storage model	Specify the storage type. <ul style="list-style-type: none"> 13: VSP 5000 series 23: VSP E990, VSP G350, G370, G700, G900, VSP F350, F370, F700, F900
Serial No	Specify the serial number of the storage system.
Access Type	Specify 4.
SVP IP Address or Host Name	If 13 is specified for <code>Storage model</code> , specify the IP address or host name of the SVP that manages the storage system that was specified for <code>Serial No</code> .
GUM(CTL) IP Address or Host Name (Primary)	If 23 is specified for <code>Storage model</code> , specify the IP address or the host name (for which name resolution is possible) of the GUM (CTL) of the storage system that was specified for <code>Serial No</code> . The default value is blank. Connections with the connection destination set for <code>GUM(CTL) IP Address or Host Name (Primary)</code> will be prioritized. Note that you do not need to specify both <code>GUM(CTL) IP Address or Host Name (Primary)</code> and <code>GUM(CTL) IP Address or Host Name (Secondary)</code> .
GUM(CTL) IP Address or Host Name (Secondary)	
Storage User ID for REST-API	Specify the user ID of the user account that was created for accessing the target storage system using the REST API.
Storage Password for REST-API	Specify the password of the user account that was created for accessing the target storage system using the REST API.

Item	Description
REST-API Protocol	<p>Specify the protocol to use for accessing the target storage system using the REST API. The default value is 1.</p> <ul style="list-style-type: none"> ▪ To use HTTP: 1 ▪ To use HTTPS: 2
Java VM Heap Memory setting Method	<p>Specify the method to use for setting the required memory size for the Java VM. The default value is 1.</p> <p>However, in a large-scale environment that exceeds an assumed value*, if you specify 1 for this item, processing might end abnormally because of insufficient memory. For this reason, for a large-scale environment, specify 2.</p> <ul style="list-style-type: none"> ▪ To specify a method that automatically calculates the required memory size based on the maximum number of volumes: 1 ▪ To specify a method where the user specifies the memory size: 2
Maximum number of Volumes	<p>If you specified 1 for Java VM Heap Memory setting Method, specify the maximum number of volumes to be created on the target storage system. The required memory size for the Java VM will be automatically specified based on this setting.</p> <p>You can specify a value in the range from 1000 to 99999. The default value is 4000.</p>
Java VM Heap Memory for REST-API	<p>If you specified 2 for Java VM Heap Memory setting Method, specify the required memory size for the Java VM. The default value is 1.</p> <ul style="list-style-type: none"> ▪ 1: 128 MB ▪ 2: 256 MB ▪ 3: 512 MB ▪ 4: 1.0 GB ▪ 5: 2.0 GB ▪ 6: 4.0 GB ▪ 7: 8.0 GB

Item	Description
	<p>*: The following values are assumed for the environment when the required memory size is calculated based on the maximum number of volumes and the data is collected by using the REST API:</p> <ul style="list-style-type: none"> ▪ Number of LU paths per LDEV: 4 ▪ Number of SPM settings per LDEV: 4 ▪ Number of host groups assigned to each LDEV: 1 ▪ Number of WWNs assigned to the hosts of each LDEV: 2

3. When configuring multiple instances, repeat steps 1 and 2 for each instance.
4. Before you start operation in an instance environment, run the `jpctdchkinst` command to verify the instance settings.

The command references the set instance information. (This command checks whether the settings allow information to be collected from the storage system monitored by RAID Agent.)

```
/opt/jplpc/tools/jpctdchkinst -inst instance-name
```

5. (Optional) Configure the collection-time definition file (`conf_refresh_times.ini`).
Set the time for collecting configuration information as described in [Changing the configuration information collection time \(on page 396\)](#). This setting helps ensure the proper collection of performance data when the storage system contains a large amount of configuration data.
6. Run the following command to start the RAID Agent instance services:

```
/opt/jplpc/htm/bin/htmsrv start -all
```



Note: You must wait for approximately one hour to add the Hitachi Enterprise Storage probe after adding an instance on the RAID agent.

Importing a certificate to the truststore for RAID Agent

To enable verification of a storage system's server certificate in RAID Agent, import the storage system's certificate to the truststore for RAID Agent, and then edit the `ipdc.properties` file.

Before you begin

- You must have the root permission.
- You must prepare the storage system's certificate.

If you use a certificate issued by a certificate authority, the certificates of all the certificate authorities, from the certificate authority that issued the storage system's server certificate to the root certificate authority, must be connected in a chain of trust.

- If the storage system's certificate already exists in the truststore, delete the existing certificate before importing new certificate. To delete the existing certificate, execute the following command:

```
rm /opt/jplpc/agtd/agent/instance-name/jssecacerts
```

Procedure

1. Execute the following command to import the storage system's certificate to the truststore:

```
/opt/jplpc/htnm/HBasePSB/jdk/bin/keytool -import -alias alias-name -  
file certificate-file-name -keystore truststore-file-name -storepass  
access-password-for-truststore
```

- For *alias-name*, specify a name that makes it possible to determine which storage system the server certificate belongs to.
- For *certificate-file-name*, specify the absolute path of the location in which the certificate is stored.
- For *truststore-file-name*, specify the following absolute path:

```
/opt/jplpc/agtd/agent/instance-name/jssecacerts
```
- For *access-password-for-truststore*, specify a password of your choice.

2. Enable verification of the server certificate by changing the following properties in the file `/opt/jplpc/agt/agent/instance-name/ipdc.properties`. If there is a hash mark (#) at the beginning of a property line, delete that hash mark.

- `ssl.check.cert=true`
- `ssl.check.cert.self.truststore=true`
- `ssl.check.cert.hostname=true`

**Note:**

- To check the name of the host of the SSL certificate, specify a host name that can be resolved for GUM(CTL) IP Address or Host Name in the RAID Agent instance information. If you cannot specify a host name that can be resolved, specify `false` because the host name cannot be verified.
- If the web server certificate is not a wildcard certificate, specify `false`, because the host name cannot be verified.

3. Execute the command `jpctdchkinst` and confirm the instance settings:

```
/opt/jplpc/tools/jpctdchkinst -inst instance-name
```

4. Execute the following commands to restart the services of the RAID Agent instance:

```
/opt/jplpc/htm/bin/htmsrv stop -all
```

```
/opt/jplpc/htm/bin/htmsrv start -all
```

Next steps

[Adding Hitachi Enterprise Storage probe \(on page 185\)](#)

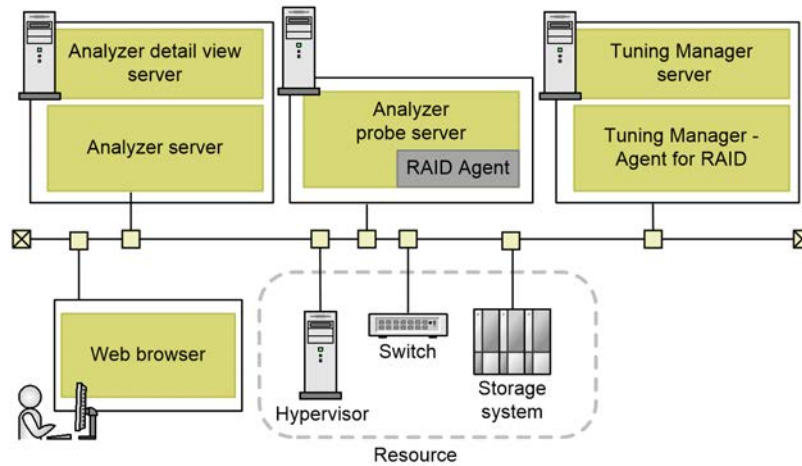
Setting up Tuning Manager - Agent for RAID

If you are running Tuning Manager in your environment, then you can configure the Tuning Manager - Agent for RAID to collect performance data from the monitored VSP family or HUS VM.

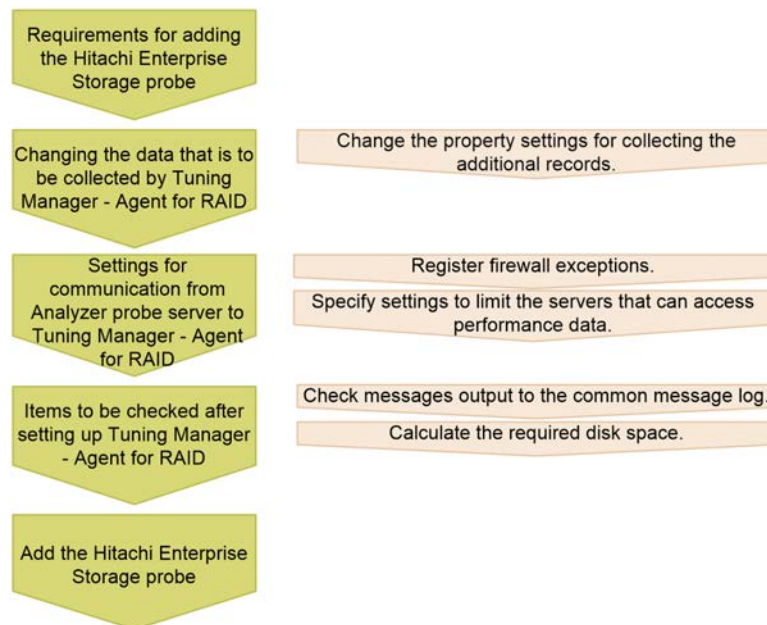
Requirements for adding the Hitachi Enterprise Storage probe (when using Tuning Manager - Agent for RAID)

To use Tuning Manager - Agent for RAID to monitor VSP family or HUS VM, you must perform the following operations before adding the Hitachi Enterprise Storage probe.

Example system configuration for Ops Center Analyzer (when using Tuning Manager - Agent for RAID)



Operation workflow for adding Hitachi Enterprise Storage probe (when using Tuning Manager - Agent for RAID)



Prerequisites

To use Tuning Manager - Agent for RAID, make sure that all of the following conditions are met:

- The Tuning Manager server is set up to connect to Tuning Manager - Agent for RAID.
- Version of Tuning Manager - Agent for RAID: 8.5.3 or later.
- Performance database for Tuning Manager - Agent for RAID: Hybrid Store. If you are using a Store database, switch to Hybrid Store.

- Value specified for Method for collecting (the connection method to use when collecting performance data) in the Tuning Manager - Agent for RAID instance information: Verify that 3 (Collect from both command devices and SVP) is selected.

For Ops Center Analyzer, the only value of Method for collecting that is supported is 3. If 3 is not selected, update the instance environment.

- Disk capacity of Tuning Manager - Agent for RAID: There is sufficient space for the additional records that will be collected for Ops Center Analyzer analysis.

Changing the data collected by Tuning Manager - Agent for RAID

To enable Tuning Manager - Agent for RAID to collect the following additional records for use in Ops Center Analyzer, you must modify the existing data collection settings (Log property settings) in Tuning Manager - Agent for RAID:

- PD_HGC
- PD_HHGC
- PD_LDCC
- PD_LDD
- PD_LHGC
- PD_LWPC
- PD_MPBC
- PD_PWPC
- PD_RGD

Procedure

1. Log on to the Tuning Manager software as a user with administrator permissions.
2. Start Performance Reporter.
3. In the main window of Performance Reporter, in the Navigation frame, select the **Services** tab.

This tab is displayed only for users with administrator permissions.

4. In the main window of Performance Reporter, in the Navigation frame, select **System > Machines > *folder-representing-Tuning-Manager-Agent-for-RAID-installation-host* > Agent Collector Service**.
5. In the main window of Performance Reporter, in the method pane, select **Properties**, and then **Detail Records**.
A list of records is displayed.
6. Select the record for which you must change the settings, and then change the **Log** property value to **Yes**.



Note:

To use Tuning Manager - Agent for RAID after upgrading it from a version earlier than 8.5.2 to version 8.5.2 or a later version, change the Collection Interval value for the PD_RGD record to 3600.

Settings for communication from Analyzer probe server to Tuning Manager - Agent for RAID

To use the data collected by Tuning Manager - Agent for RAID in Ops Center Analyzer, you must specify the necessary settings for communication with Analyzer probe server.

Procedure

1. On the host on which Tuning Manager - Agent for RAID is installed, register the port to use for communication with Analyzer probe server as a firewall exception.
The default port number is 24221.
2. (Optional) To limit the servers that can access the performance data of Tuning Manager - Agent for RAID, add Analyzer probe server to the `htnm_httpsd.conf` file managed by Tuning Manager - Agent for RAID.
 - a. Stop the Tuning Manager Agent REST API component services.
 - b. To the last line of the `htnm_httpsd.conf` file, register information about the Analyzer probe server that can connect to the agents on which use of the API is enabled.
 - c. Start the Tuning Manager Agent REST API component services.



Note: To use the API functions that access RAID Agent, you must also register information about Analyzer server in the `htnm_httpsd.conf` file.

Notes on using Tuning Manager - Agent for RAID

Keep in mind the following if you want to use Tuning Manager - Agent for RAID with Ops Center Analyzer:

- Collecting additional records for Ops Center Analyzer might affect the performance of Tuning Manager - Agent for RAID. Check whether the message KAVE00213-W, which indicates that the PI record type could not be generated, is output to the common message log at a specific time every hour.
- When you change the host name or port number used for Tuning Manager - Agent for RAID, update the settings information for the Hitachi Enterprise Storage probe by using Analyzer probe server.
- If the data retention period of Tuning Manager - Agent for RAID is shorter than the record collection interval, there will be a period of time during which no data exists, and Ops Center Analyzer might determine that the monitoring targets were deleted. To properly retain data, you must change the data retention period of Tuning Manager - Agent for RAID as follows. For details about how to change the data retention period, see the *Hitachi Command Suite Tuning Manager Agent Administration Guide*.
 - **If the maximum record collection interval is less than 48 hours:** 48 hours or more
 - **If the maximum record collection interval is 48 hours or more:** Maximum record collection interval + at least one hour

Values used for estimating disk space when using Tuning Manager - Agent for RAID

The following information is necessary for calculating the disk space required to use Tuning Manager - Agent for RAID with Ops Center Analyzer.

Calculate the disk space required by Tuning Manager - Agent for RAID and verify that there is adequate disk space available. The calculation is performed based on information about records already collected by Tuning Manager - Agent for RAID, and information about records that will be additionally collected for Ops Center Analyzer by Tuning Manager - Agent for RAID.

The record information described here relates to records to be additionally collected by Tuning Manager - Agent for RAID. For details about other records, see *Hitachi Command Suite System Requirements*.

Methods for estimating number of instances

Record ID	Method for estimating number of instances
PD_HGC	Number of host groups that exist in the storage system
PD_HHGC	Total number of hosts that belong to the host groups that exist in the storage system
PD_LDCC	Number of copied logical devices
PD_LDD	Number of logical devices
PD_LHGC	Total number of LUNs that belong to the host groups that exist in the storage system
PD_LWPC	Sum of the number of settings related to LDEVs and the WWNs of host bus adapters*, and the number of settings related to LDEVs and iSCSI names*
PD_MPBC	Number of MP blades
PD_PWPC	Total number of settings related to ports and the WWNs of host bus adapters*
PD_RGD	Number of parity groups
*: To specify this setting, use Server Priority Manager, provided by Hitachi storage systems.	

Size of each record

Record ID	Fixed part 1 (bytes)	Variable part 1 (bytes)	Fixed part 2 (bytes)	Variable part 2 (bytes)
PD_HGC	80	563	--	--
PD_HHGC	68	580	--	--
PD_LDCC	72	281	--	--
PD_LDD	76	265	--	--
PD_LHGC	68	272	--	--
PD_LWPC	64	617	--	--
PD_MPBC	52	113	--	--
PD_RGD	80	295	--	--
PD_PWPC	80	361	--	--

Retention period for the records (default value)

Record ID	Retention period (unit: hours)
PD_HGC	168
PD_HHGC	168
PD_LDCC	168
PD_LDD	168
PD_LHGC	168
PD_LWPC	168
PD_MPBC	168
PD_RGD	168
PD_PWPC	168

Migrating Hitachi Tuning Manager historical data

The Tuning Manager data migration feature copies storage systems historical data from the Tuning Manager to Analyzer detail view database. You can obtain the migrated data,

which is preserved in the Analyzer detail view database, by using the Analyzer detail view REST API.

The Tuning Manager data migration feature supports deployments in which Tuning Manager and Tuning Manager - Agent for RAID are on the same or on different machines.



Note: The Tuning Manager, Tuning Manager - Agent for RAID, and Analyzer probe server must belong to the same subnet.

Tuning Manager data migration workflow:

1. The Analyzer probe server connects to Tuning Manager to identify the RAID Agent associated with it.
2. The Analyzer probe server connects to the RAID Agent to collect the historical data.
3. The Analyzer probe server transfers the collected data to the Analyzer detail view database.
4. The user connects to the Analyzer detail view database using the REST API to obtain the migrated data.

Setting up a Tuning Manager connection

Set up a connection so that you can migrate the historical data stored in Tuning Manager to the Analyzer probe server.

Before you begin

Verify the following:

- Tuning Manager server version is 8.5.3-00 or later.
- Tuning Manager - Agent for RAID version is 8.5.3-04 or later.
- Tuning Manager accessible host settings to allow a connection between Tuning Manager and the Analyzer probe server (using the HTTP protocol on port 22015 or the HTTPS protocol on port 22016).
- Tuning Manager server, Tuning Manager - Agent for RAID, and Analyzer probe server all belong to the same subnet.
- All storage systems about which you want to migrate data are registered in Tuning Manager.
- Tuning Manager server services are running.
- Tuning Manager - Agent for RAID REST service is running.
- Tuning Manager server can recognize the Tuning Manager - Agent for RAID instance.
- Tuning Manager server has an unexpired license.
- The performance database for Tuning Manager - Agent for RAID is Hybrid Store.
- Tuning Manager server and Tuning Manager - Agent for RAID can restrict API clients that connect to them. If this is configured, the Analyzer probe server must be registered to allow the connection.

Procedure

1. Log on to the Analyzer probe as the `admin` user.
2. In the application bar, click **Manage**.
3. In the **Administration** section, click **Migrate Hitachi Tuning Manager Data**.
4. In the **Add Hitachi Tuning Manager** window, provide the following details:
 - **Connection Method:** HTTP or HTTPS
 - **IP Address:** IP address of Tuning Manager
 - **Port Number:** Port number based on the selected connection method. The default ports are:
 - **HTTP:** 22015
 - **HTTPS:** 22016
 - **Username and Password:** Username and password for Tuning Manager.
5. Click **Add**. After you have successfully set up the connection, the RAID Agents and storage systems associated with Tuning Manager are listed in the **Migrate Hitachi Tuning Manager Data** window.

Starting the data migration

Data migration is performed on a per-system basis. After you complete the data migration for storage systems, you cannot run it again.



Note: By default, the Analyzer probe server uses HTTPS protocol on port 8443 to communicate with the Analyzer detail view server. If you specify a different port, ensure it is available for communication.

Procedure

1. In the **Migrate Hitachi Tuning Manager Data** window, select the storage systems from which to migrate data. (You can migrate data simultaneously for four storage systems per Tuning Manager - Agent for RAID instance.)
2. In the **Duration** column, select the duration in years for which you want to migrate the data.
When you select the duration, the **Remarks** column shows the exact duration for which the data is available for migration. Make sure that you select the correct duration. You cannot migrate data with different durations for the same storage system.
3. Click **Start**, and then click **OK** to begin the data migration.
The **Remarks** column is updated with the status as the migration proceeds.

Accessing Tuning Manager historical data

You can use REST API to query the Ops Center Analyzer detail view database for the Tuning Manager historical data.

Sample query:

- **Configuration data:** You can query the migrated configuration data as you would query any other probe data using the following request line:

```
POST baseUrl?action=retrieveResourceData&dataset=defaultDs
```

- **Performance Data:** You can query the migrated performance data using the following request line:

```
POST baseUrl?action=query&dataset=defaultDs&processSync=true
```

- You must specify the following parameters in the request body:
 - `db=cdb1`: Restricts the query to the migrated performance data.
 - `inputInterval=supported-values`: Collection intervals of the migrated data. The supported values are: `h` (hour), `d` (day), `w` (week), `m` (month), and `y` (year).

For more information, refer to *Hitachi Ops Center Analyzer detail view REST API Reference Guide*.

Changing the default migration connection settings

The Analyzer probe server uses HTTP: 24221 as a default connection setting. To change this default connection setting, do the following:

Procedure

1. In the **Migrate Hitachi Tuning Manager Data** window, in the **RAID Agent** column, click the RAID Agent IP address.
The **RAID Agent Connection Details** window opens.
2. Select the connection method and provide the corresponding port number. This setting applies to all storage systems associated with the selected RAID Agent.
3. Click **Ok**.

Notes and restrictions

The following restrictions apply to the Tuning Manager data migration feature.

- Historical performance data is migrated for the following frequencies:
 - Hourly
 - Daily
 - Weekly
 - Monthly
 - Yearly
- Historical configuration data is migrated for a frequency of one day only.
- Migration supports Hitachi Enterprise Storage probe resources and records only (except for RAID Agent instance name). For a specific list, refer to *Hitachi Ops Center Analyzer detail view Metrics Reference Guide*.
- Migration does not support migrating Tuning Manager alarms and alerts.
- Migration does not support migrating Hitachi Device Manager data.

Switching from Tuning Manager - Agent for RAID to RAID Agent

You can change the agent used by the Hitachi Enterprise Storage probe from Tuning Manager - Agent for RAID to RAID Agent bundled with Ops Center Analyzer.



Note: RAID Agent will not automatically inherit the settings of Tuning Manager - Agent for RAID. Configure the settings manually by performing the following steps.

Procedure

1. Check the settings of Tuning Manager - Agent for RAID.
 - a. Display a list of instance names by running the `jpcinslist` command on the host on which Tuning Manager - Agent for RAID is installed:

```
jpcinslist agtd
```

- b. Check the instance information by running the `jpctdchkinst` command on the host on which Tuning Manager - Agent for RAID is installed:

```
jpctdchkinst -inst instance-name
```

- c. If the collection intervals for Tuning Manager - Agent for RAID have been changed, check the collection intervals.
For details about how to check the collection intervals for Tuning Manager - Agent for RAID, see the *Hitachi Command Suite Tuning Manager Agent Administration Guide*.

2. Stop the Hitachi Enterprise Storage probe.
For details, see [Starting and stopping probes \(on page 401\)](#).
3. Stop the instance of Tuning Manager - Agent for RAID by running the `htmsrv` command on the host on which Tuning Manager - Agent for RAID is installed:

```
htmsrv stop -key agtd -inst instance-name
```

4. Set up RAID Agent.
 - a. Determine `Access Type`. (For details, see [Selecting the data collection method \(on page 137\)](#).)
 - b. Set up RAID Agent. (For details, see [Workflow for setting up the Hitachi Enterprise Storage probe \(when using RAID Agent\) \(on page 141\)](#) and the sections that follow.)
Specify the instance information of the storage system to be monitored as follows:
 - The item `Access Type` in the instance information for RAID Agent corresponds to the item `Method for collecting` in the instance information for Tuning Manager - Agent for RAID.
Example: The value 1 (Command-Device and SVP) for `Access Type` has the same meaning as the value 3 (both) for `Method for collecting`.
 - Make sure that the value of `Serial No` is the same as the value set for Tuning Manager - Agent for RAID.
 - (Optional) If you want RAID Agent to inherit other settings, specify the same values for those settings as were set for Tuning Manager - Agent for RAID.
5. If the collection intervals for Tuning Manager - Agent for RAID have been changed, change the collection intervals for RAID Agent to match those for Tuning Manager - Agent for RAID.
For details, see [Changing data collection intervals for RAID Agent \(on page 392\)](#).
6. Change the agent used by the Hitachi Enterprise Storage probe from Tuning Manager - Agent for RAID to RAID Agent.
For details, see [Editing probes \(on page 402\)](#).
Change the following probe settings:
 - Connection Type: Select `HTTP`.
 - RAID Agent IP address: Specify the IP address of the RAID Agent host.
 - RAID Agent Hostname: Specify the name of the RAID Agent host.
 - RAID Agent Port: Specify the port number of the RAID Agent host.
 - Storage System Instance: Specify the name of the instance of RAID Agent that you created in a previous step.
7. Start the Hitachi Enterprise Storage probe.
For details, see [Starting and stopping probes \(on page 401\)](#).

Chapter 7: Adding probes to the Analyzer probe

Start collecting information about your system resources by adding probes to the Analyzer probe server.

Adding Hitachi Enterprise Storage probe

The Hitachi Enterprise Storage probe collects data about the following Hitachi Enterprise storage systems: HUS VM, VSP, VSP F series, VSP G series, VSP 5000 series, and VSP E990. This procedure presumes you are using the RAID Agent bundled with Analyzer server. The procedure is the same for using Tuning Manager - Agent for RAID.

The Hitachi Enterprise Storage probe collects all performance data and specific configuration data from the RAID Agent using the REST API.

Additional configuration data not collected from the RAID Agent is available from Hitachi Configuration Manager (preferred) or Hitachi Device Manager. (You are prompted with this option when adding the Hitachi Enterprise Storage probe.)



Note: When you add the Hitachi Enterprise Storage probe, the following message might be displayed:

Some required opcodes are turned off by default on RAID Agent. Ensure that these are enabled to collect the related metrics. Before proceeding further, refer to product user documentation.

Ignore this message as this setting is automatically enabled on RAID Agent in Ops Center Analyzer.

Procedure

1. On the Analyzer probe home page, click **Add Probe**.
2. In the **Add Probe** window, from the **Probes** list, select **Hitachi Enterprise Storage**.
3. In the **Provide RAID Agent Details** section, provide the following details, and then click **Next**:
 - **Probe Name:** The probe name must be unique and contain a minimum 4 to maximum 100 alphanumeric characters, and no special characters other than hyphen and underscore.
 - **Connection Type:** Choose **HTTP** or **HTTPS**.
 - **RAID Agent IP Address:** IP address of the machine on which the RAID Agent is installed.

- **RAID Agent Host name:** Host name of the machine on which the RAID Agent is installed. The host name must match the machine host name (case-sensitive). Specify the host name that is returned when you run the `uname -n` command on the RAID Agent server. Do not use `localhost`.
- **RAID Agent Port:** Port number used by the RAID Agent on the RAID Agent host. The default port number is:

`24221-HTTP`
- **Storage System Serial number:** Serial number of the storage system configured on the RAID Agent.
- **Storage System Instance:** Storage instance name (alias) used to add the storage system to the RAID Agent.
- **Enable real time data collection:** Select this check box to collect real-time data that can be used for alerts, reports, and the REST API.



Note: Enabling the real-time data collection increases the load on the Analyzer detail view server.

4. In the **Configure RAID Agent Collection Interval** window, specify the collection intervals as follows and then click **Next**:

- **Collection interval for PLC (Pool Configuration):** 60
- **Collection interval for VVC (V-VOL status of Dynamic Provisioning):** 60
- **Collection interval for LDSX (LDEV Summary Extra):** 300 (only if the `Access Type` is 2 or 4)



Note:

- The data collection interval for each record must match the data collection interval set in RAID Agent or in Tuning Manager - Agent for RAID.
- The data collection interval for each record must also match the data collection interval set on the storage system. If these intervals do not match, the performance charts might not display properly (the graphs might not be continuous).
- If you are using RAID Agent, use the `collection_config` command to verify the setting for the data collection interval, and specify a value that is the same as the displayed data collection interval.
- For the data collection interval of records that are not displayed by using the `collection_config` command, use the default setting (without change).

5. Select the **Collect additional configuration metrics** check box, and select the option to use for collecting the additional configuration metrics:



Note: If you do not want to collect additional configuration data, click **Next** and skip the rest of this procedure.

- Select **Hitachi Configuration Manager** to collect configuration metrics from Hitachi Configuration Manager. For details and prerequisites, see [Collecting additional configuration metrics with Hitachi Configuration Manager \(on page 187\)](#).
 - Select **Hitachi Device Manager** to collect configuration data from Hitachi Device Manager. For details and prerequisites, see [Collecting additional configuration metrics with Hitachi Device Manager \(on page 188\)](#).
6. In the **Validation** window, click **Next**, and then click **OK**.
 7. In the **Status** window, in **Action**, click **Start** to start collecting data.



Note: If you change the storage system configuration after you add a Hitachi Enterprise Storage probe, the old information displays until the status is updated.

Collecting additional configuration metrics

The Hitachi Enterprise Storage probe provides an option to collect additional configuration metrics not available from the RAID Agent. These additional metrics can be collected using the Hitachi Configuration Manager (preferred) or Hitachi Device Manager. This is optional; you can skip it if you do not want to collect these metrics. Refer to *Hitachi Ops Center Analyzer Detail View Metrics Reference Guide* for the list of additional configuration metrics.

Collecting additional configuration metrics with Hitachi Configuration Manager

The Hitachi Configuration Manager collects additional configuration metrics from the following storage systems: HUS VM, VSP, VSP F series, VSP G series, VSP 5000 series.

Before you begin

Verify the following:

- User credentials used to connect to the storage systems have one of the following roles:
 - Security Administrator (view only) or greater
 - Storage Administrator (view only) with access to all Resource Groups
- The Hitachi Configuration Manager server is configured for fcConnectionMode (in-band). (Using in-band communication mode, the Hitachi Configuration Manager server communicates with the storage system through the command device.) If you are using another communication mode, then change the mode to in-band before configuring the Hitachi Configuration Manager server in the Hitachi Enterprise Storage probe. (Multiple communication mode with lanConnectionMode is not supported.)

- `User Authentication` is enabled on the command device.
- The Hitachi Configuration Manager server must be connected with SVP to collect data from the following storage systems: VSP F350, VSP F370, VSP F700, VSP F900, VSP G350, VSP G370, VSP G700, VSP G900.

Procedure

1. Select the **Collect additional configuration metrics** check box, and then select the **Hitachi Configuration Manager** option.
2. In the **Hitachi Configuration Manager Details** section, provide the following details and click **Next**:
 - **Connection Type:** Choose **HTTP** or **HTTPS**.
 - **Host:** IP Address or Host name of the Hitachi Configuration Manager server.
 - **Port:** Port number of the Hitachi Configuration Manager server. The default port numbers are:
`23450-HTTP`
`23451-HTTPS`
 - **Username/Password:** User name and password of the storage system specified in the **Provide RAID Agent Details** section.
3. In the **Validation** window, click **Next**, and then click **OK**.
4. In the **Status** window, in **Action**, click **Start** to start collecting data.

Notes:

- The Hitachi Configuration Manager server supports only 30 storage system instances.
- It is recommended that the Hitachi Configuration Manager server that is configured in the Analyzer probe is not used by any other external application because it might affect the Hitachi Enterprise Storage probe data collection.

Collecting additional configuration metrics with Hitachi Device Manager

The Hitachi Device Manager collects additional configuration metrics related to the Hitachi storage systems.

Before you begin

- Configure Hitachi Device Manager with all required storage devices.
- Ensure that Hitachi Device Manager:
 - is capable of querying the storage capacity and host information.
 - has read-only privileges (at minimum).
 - is a member of the ViewGroup user group.
 - is version 7.5 or later.

Procedure

1. Select the **Collect additional configuration metrics** check box, and then select the **Hitachi Device Manager** option.
2. In the **Hitachi Device Manager Details** section, provide the following details and click **Next**:
 - **Connection Type:** Choose **HTTP** or **HTTPS**.
 - **Host:** IP address or host name of the Hitachi Device Manager server.
 - **Port:** Port number of the Hitachi Device Manager server. The default port numbers are:
2001-HTTP
2443-HTTPS
 - **Username/Password:** User name and password for Hitachi Device Manager. (This user must be added in the ViewGroup user group of Hitachi Device Manager.)
3. In the **Validation** window, click **Next**, and then click **OK**.
4. In the **Status** window, in **Action**, click **Start** to start collecting data.

Switching from Hitachi Device Manager to Hitachi Configuration Manager

You can change the option to collect additional configuration metrics used by the Hitachi Enterprise Storage probe from Hitachi Device Manager to Hitachi Configuration Manager and vice versa.


Procedure

1. Log on to the Analyzer probe.
2. In the **Action** column, stop the probe if it is running, and then click **Edit**.
3. In the **Edit Hitachi Enterprise Storage Probe** window, select the collection option.
 - Select **Hitachi Configuration Manager** to collect configuration metrics from Hitachi Configuration Manager. For details and prerequisites, refer [Collecting additional configuration metrics with Hitachi Configuration Manager option \(on page 187\)](#).
 - Select **Hitachi Device Manager** to collect configuration data from Hitachi Device Manager. For details and prerequisites, refer [Collecting additional configuration metrics with Hitachi Device Manager option. \(on page 188\)](#)

Adding Hitachi Adaptable Modular Storage (AMS) probe

The AMS probe collects data from AMS and HUS storage systems.


Procedure

1. On the Analyzer probe home page, click **Add Probe**.
 2. In the **Add Probe** window, from the **Probes** list, select **Hitachi AMS**.
 3. In the **Add Hitachi AMS Probe** section, provide the following details, then click **Next**:
 - **Hitachi AMS Probe Name**: Name of the HUS100 storage system for which the probe is added. (This must not be the same as the storage name that is defined in your environment.) After you add the probe, it is identified with this name in the Analyzer probe.
 - **Controller 0 IP address** and **Controller 1 IP address**: IP addresses of Controller 0 and Controller 1.
 - **User name** and **Password**: User name and password of the user with read-only permissions.
-  **Note:**
If user authentication for the HUS100 storage system is disabled, then you must type a dummy user name and password because these two fields are mandatory for adding the AMS probe.
4. In the **Validation** window, click **Next**, and then click **OK**.
 5. In the **Status** window, in **Action**, click **Start** to start collecting data.

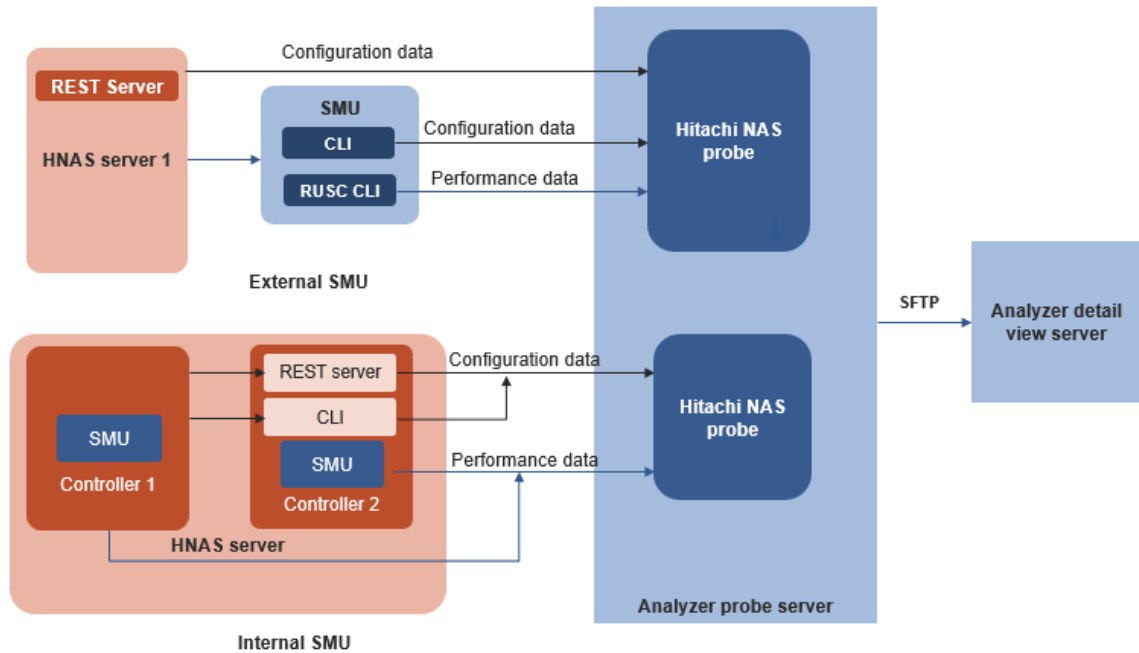
Adding Hitachi NAS probe

Hitachi NAS probe collects configuration and performance data for the Hitachi NAS platform. There are two types of Hitachi NAS configurations: External SMU and Internal SMU. The Hitachi NAS probe collects configuration data using REST API, and performance data using RUSC CLI.

Hitachi NAS probe supports the Hitachi NAS server configured as a cluster, single node cluster, and a standalone (non-clustered) server.

 **Note:** The Analyzer probe supports the REST API v4 and v7 of the target Hitachi NAS storage system. If you are using the REST API v7, then make sure that following criteria are met: VSP G/F/Nx00 with NAS OS 13.5 or higher and HNAS 4000 series with NAS OS 13.5 or higher.

The following diagram illustrates the data collection flow.



Configuration metrics that are not collected using REST API and are required for reporting in the UI are collected using CLI.

Before you begin

External SMU

- To collect the performance data, make sure that the user has SMU CLI access.
- To collect the configuration data, a login with a role of supervisor is required to execute REST API calls.

A valid Enterprise Virtual Server (EVS) IP address with admin services type (called an Admin EVS IP address) is required to execute REST API calls. The Hitachi NAS probe obtains this information based on the SMU details that you provide when adding the Hitachi NAS probe.


Internal SMU

- A user with a role of supervisor is required to collect the performance and configuration data.
- To collect the configuration data, make sure that the REST API server is installed on one of the controllers.
- The controller and the REST API server must use the same login with a role of supervisor.


Procedure

- On the Analyzer probe home page, click **Add Probe**.
- In the **Add Probe** window, from the **Probes** list, select **Hitachi NAS**.

3. On the **Add Hitachi NAS Probe** window, in the **Provide SMU details** section, provide the following details, then click **Next**:
 - **IP address:** The IP address of the Hitachi NAS System Management Unit (SMU).
 - **User name and Password:** User credentials of the SMU user.
4. In the **Validation** window, click **Next**.
5. Based on the SMU IP address, the **Provide REST API server details** or **Provide controller details** window opens.
 - **External SMU:** The **Provide REST API server details** window lists all the Hitachi NAS servers managed by the SMU. Select the **Hitachi NAS server** and **Admin EVS IP address**, and enter the REST API server details. Click **Next**.

 **Note:** You can select multiple Hitachi NAS servers; each is added as an individual probe in the Analyzer probe. (The probe is added as an SMU-Hitachi NAS server combination.)

- **Internal SMU:** The **Provide controller details** window lists all the controllers managed by the SMU. Type the username and password of the controller that you want to add. (The default port is 8444 and cannot be changed.)

 **Note:** You can select multiple controllers, and a single probe is added for multiple controllers. (The probe is added as an SMU-Controller combination.) If you provide the details of one controller, then the configuration data is collected from all controllers managed by the SMU. However, to collect the performance data you must provide the details of each controller from which you want to collect the performance data.
6. In the **Validation** window, click **Next**, then click **OK**.
7. In the **Status** window, in **Action**, click **Start** to start collecting data.

Adding VMware probe

VMware probe collects data from the VMware vCenter server and standalone VMware ESXi host.

Procedure

1. From the Analyzer probe server home page, click **Add Probe**.
2. In the **Add Probe** window, from the **Probes** drop-down list, select **VMware**.

3. In the **Add VMware Probe** section, provide the following details, then click **Next**:
 - **vCenter Server**: Host name or IP address of the VMware vCenter Server Appliance or VMware ESXi host IP address.
 - **User name**: Any user with access to VMware vCenter Server (read-only privileges are sufficient). Ensure that the user has access to all the ESXi hosts (within the VMware vCenter Server) that you want to monitor.
 - **Password**: Password associated with the user name.
4. In the **Validation** window, click **Next**.



Note: If you have entered the standalone VMware ESXi host details, skip to step 6.

5. In the **Choose Hosts for Data Collection** window, select the hosts that you want to monitor.



Note: When a new host is added to the VMware vCenter server, the probe begins collecting data automatically. To override this setting, clear **Include hosts that are added in the future**.

You can also add the hosts using the **Import CSV** option, which allows you to add a large number of hosts with a flexibility of adding only those hosts that you want to monitor. For example, if you have 100 hosts in a vCenter server and out of these you want to monitor 60, you can specify these hosts in the CSV file and import it to the probe.

- a. Select the **Select hosts for data collection using csv file import** option.
 - b. Ensure the CSV file is in a specific format. Download a sample file by clicking the **Export** option.
 - c. Edit the CSV file details offline based on your requirements. In the CSV file, you can add only those hosts that you want to monitor or type **No** for each host that you do not want to monitor.
 - d. Import the CSV file by clicking the **Import** option. The imported hosts are listed in the **Select hosts for data collection** section.
 - e. Track the status of the hosts in the **Uploaded Host CSV Record Status** window. To view the status, click the **Details** option. Refer to [Viewing the host CSV file import status \(on page 193\)](#) for more information.
6. Click **Next**, and then click **OK**.
 7. In the **Status** window, in **Action**, click **Start** to start collecting data.


Viewing the host CSV file import status

The details link shows the following status of the imported CSV file.

The following figure shows an example status of an imported CSV file and the resources monitored:

STATE	NO. OF RECORDS	ACTION
Valid	106	View
Monitored	104	View
Not monitored	2	View
Invalid	4	View
Bad	3	View
Unknown	1	View

- **Valid:** Total number of valid records (Monitored and Not monitored)
 - **Monitored:** The list of records from which the data is collected.
 - **Not monitored:** The list of records that are marked as `No` in the CSV file.
- **Invalid:** Total number of invalid records that cannot be added.

 **Note:** You can edit the invalid records and re-import the CSV file. To view the details of the invalid records, click View.


 - **Bad Record:** The list of records with incorrect values, which cannot be read by Analyzer probe server.
 - **Unknown state:** The list of records with incorrect monitored status in the CSV file. The monitored status in the CSV file must be either `Yes` or `No`.

Adding Brocade FC Switch (BNA) probe

Brocade FC Switch (BNA) probe collects configuration and performance data about the brocade switches from Brocade Network Advisor using REST API. Brocade Network Advisor manages the entire Brocade IP address and SAN portfolio for unified network visibility and control.

Before you begin

- The user must have Area of Responsibility as All Fabrics and at least one role: SAN Discovery setup or Performance with read-only permissions.
- Brocade Network Advisor Professional plus or Brocade Network Advisor Enterprise must be installed.

 **Note:** Do not use both the Brocade FC Switch (BNA) probe and Brocade FC Switch (CLI) probe to collect data for the same switch.

Procedure

1. From the Analyzer probe server home page, click **Add Probe**.
2. In the **Add Probe** window, from the **Probes** drop-down list, select **Brocade FC Switch (BNA)**.

3. In the **Add Brocade FC Switch (BNA) Probe** window, type the following details, and then click **Next**:
 - **BNA IP address**: IP address of Brocade Network Advisor
 - **BNA Port**: Port number of the Brocade Network Advisor
 - **Protocol**: Select **HTTP** or **HTTPS**

The default ports are:

80 (HTTP)

443 (HTTPS)

 - **Username and Password**: User name and password of the Brocade Network Advisor
4. In the **Validation** window, click **Next**.
5. In the **Choose switches for data collection** window, select the switches that you want to monitor.



Note: When a new switch is added to Brocade Network Advisor, the probe begins collecting data automatically. To override this setting, clear **Include Switches that are added in the future**.

You can also add the switches using the **Import CSV** option, which allows you to add a large number of switches with a flexibility of adding only those switches that you want to monitor. For example, if you have 100 switches and out of these you want to monitor 60, you can specify these switches in the CSV file and import it to the probe.

- a. Select the **Select switches for data collection using csv file import** option.
 - b. Ensure that the CSV file is in a specific format. Download a sample file by clicking the **Export** option.
 - c. Edit the CSV file details offline based on your requirements. In the CSV file, you can add only those switches that you want to monitor or type **No** for each switch that you do not want to monitor.
 - d. Import the CSV file by clicking the **Import** option. The imported switches are listed in the **Select switches for data collection** section.
 - e. Track the status of the switches in the **Uploaded Switch CSV Record Status** window. To view the status click the **Details** option. Refer to [Viewing the host CSV file import status \(on page 193\)](#) for more information.
6. Click **Next**, and then click **OK**.
 7. In the **Status** window, in **Action**, click **Start** to begin collecting data.

Adding Brocade FC Switch (CLI) probe

Brocade FC Switch (CLI) probe collects the performance and configuration data using the CLI commands from the individual Brocade FC Switch. The probe logs on to the switch using SSH and runs CLI commands to collect the data.

This probe is an alternative to the Brocade Network Advisor probe that requires the installation of Brocade Network Advisor Professional plus or Brocade Network Advisor Enterprise.



Note: Do not use both the Brocade FC Switch (BNA) probe and Brocade FC Switch (CLI) probe to collect data for the same switch.

Procedure

1. On the Analyzer probe home page, click **Add Probe**.
2. In the **Add Probe** window, from the **Probes** menu, select **Brocade FC Switch (CLI)**.

3. In the **Add Switch Details** section select any of the following options to add the target switches:

- **Add Device:** You can add the range of switch IP addresses with the same credentials under one data center. The switches are shown under this data center in the Analyzer detail view Resources tree.

- **Data Center:** Name of the data center; you can enter any name.



Note: The switch is displayed under this data center in the Analyzer detail view Resources tree.

- **Start IP Address and End IP Address:** You can enter one IP address or a range of IP addresses for the switch.



Note: If you have entered a range for addresses, the username and password must be the same for all switches.

- **User Name:** User name with read-only access.

- **Password:** Password of the user.

- **SSH Port:** The port number (default: 22).

- **Upload CSV:** You can add the range of switch IP addresses with different credentials, and group the switches based on the data center. While adding multiple data centers, make sure that each has a unique name. The switches are shown under the respective data center in the Analyzer detail view Resources tree.

- Select **Upload CSV** to upload the switch details in a CSV file, and then click **Import CSV**.

The CSV file must be in a specific format. You can download a sample file by clicking **Download Sample CSV File**.

- **Upload Encrypted CSV:** The upload encrypted CSV works similar to the upload CSV option. However, it is useful when you want to provide the switch details, including login credentials, that need to be kept confidential.

- Select **Upload Encrypted CSV** to upload details of encrypted random key and encrypted CSV file, and then click **Import CSV**.

The Encrypted CSV file must be in a specific format. You can download the sample file by clicking **Download Sample CSV File**. Refer to [Encrypting the CSV file \(on page 201\)](#) for more information.

- **Encrypted Random Key:** Select an encrypted random key.

- **Upload Encrypted CSV:** Upload an encrypted CSV.

Scroll down to view the list of switches. You can also add more switches or delete a switch before adding the probe.

4. To add more Brocade FC Switch IP addresses, click **Add More**.

5. Click **Next**.

The system scans the switch IP addresses and adds the valid switches to the system.

6. In the **Switch Validation** window, click **Next**, and then **OK**.
Each valid switch IP address is added as an individual probe.
7. In the **Status** window, in **Action**, click **Start** to start collecting data.

Adding Cisco FC Switch (DCNM) probe

The Cisco FC Switch (DCNM) probe collects data from the Cisco Data Center Network Manager using Web Services APIs.



Note: Do not use both the Cisco FC Switch (DCNM) and Cisco FC Switch (CLI) probe to collect data for the same switch.

Procedure

1. From the Analyzer probe server home page, click **Add Probe**.
2. In the **Add Probe** window, from the **Probes** drop-down list, select **Cisco FC Switch (DCNM)**.
3. In the **Add Cisco FC Switch (DCNM) Probe** window, type the following details and click **Next**:
 - **Cisco FC Switch (DCNM) IP Address:** IP address of DCNM.
 - **DCNM Web service Port:** The port number to access web service on the DCNM server.



Note: In some environments, the port number is optional.

- **Protocol** : Select **HTTP** or **HTTPS**.
The default ports are:
80 - HTTP
443 - HTTPS
 - **Username** and **password** of DCNM. The user must have access to the DCNM web client.
4. In the **Validation** window, click **Next**.
 5. In the **Choose switches for data collection** window, select the switch that you want to monitor.



Note: When a new switch is added to the Cisco Data Center Network Manager, the probe begins collecting data automatically. To override this setting, clear **Include Switches that are added in the future**.

You can also add the switches using the **Import CSV** option, which allows you to add a large number of switches with a flexibility of adding only those switches that you want to monitor. For example, if you have 100 switches and out of these you want to monitor 60, you can specify these switches in the CSV file and import it to the probe.

- a. Select the **Select switches for data collection using csv file import** option.
 - b. Ensure that the CSV file is in a specific format. Download a sample file by clicking the **Export** option.
 - c. Edit the CSV file details offline based on your requirements. In the CSV file, you can add only those switches that you want to monitor or type `No` for each switch that you do not want to monitor.
 - d. Import the CSV file by clicking the **Import** option. The imported switches are listed in the **Select switches for data collection** section.
 - e. Track the status of the switches in the **Uploaded Switch CSV Record Status** window. To view the status click the **Details** option. Refer to [Viewing the host CSV file import status \(on page 193\)](#) for more information.
6. Click **Next**, and then click **OK**.
 7. In the **Status** window, under **Action**, click **Start** to start collecting data.

Adding Cisco FC Switch (CLI) probe

Cisco FC Switch (CLI) probe collects the performance and configuration data using the CLI commands from Cisco SAN switches.



Note: Do not use both the Cisco FC Switch (DCNM) and Cisco FC Switch (CLI) probe to collect data for the same switch.

Procedure

1. On the Analyzer probe home page, click **Add Probe**.
2. In the **Add Probe** window, from the **Probes** menu, select **Cisco FC Switch (CLI)**.

3. In the **Add Switch Details** section, select any of the following options to add the target switches:

- Select **Add Device**, type the following details, and then click **Add Switch**:

- **Data Center**: Name of the data center; you can enter any name.



Note: The switch is displayed under this data center in the Analyzer detail view Resources tree.

- **Start IP Address** and **End IP Address**: Range of the IP address from which to start collecting data. This scans all the switch IP addresses in that range.



Note: If you have entered a range for addresses, the username and password must be the same for all switches.

- **User Name**: User name with the network-operator role (at minimum)
- **Password**: Password of the user
- **SSH Port**: The port number (default: 22)

- **Upload CSV**: You can add the range of switch IP addresses with different credentials and group the switches based on the data center. While adding multiple data centers, make sure that each has a unique name. The switches are shown under the respective data center in the Analyzer detail view Resources tree.

- Select **Upload CSV** to upload the switch details in a CSV file, and then click **Import CSV**.

The CSV file must be in a specific format. You can download a sample file by clicking **Download Sample CSV File**.

- **Upload Encrypted CSV**: The upload encrypted CSV works similar to the upload CSV option. However, it is useful when you want to provide the switch details, including login credentials, that must be kept confidential.

- Select **Upload Encrypted CSV** to upload details in an encrypted CSV file, and then click **Import CSV**.

The Encrypted CSV file must be in a specific format. You can download the sample file by clicking **Download Sample CSV File**. Refer to [Encrypting the CSV file \(on page 201\)](#) for more information.

- **Encrypted Random Key**: Select an encrypted random key.
- **Upload Encrypted CSV**: Upload an encrypted CSV.

Scroll down to view the list of switches. You can also add more switches or delete a switch before adding the probe.

4. To add more Cisco SAN switch IP addresses, click **Add More**.

5. Click **Next**.

The system scans the switch IP addresses and adds the valid switches to the system.

6. In the **Switch Validation** window, click **Next**, and then **OK**.

Each valid switch IP address is added as an individual probe.

7. In the **Status** window, in **Action**, click **Start** to start collecting data.

Encrypting the CSV file

Before uploading the CSV file you must encrypt it using the public key.

1. Contact customer support for the public key.
2. Log on to the Analyzer probe server through an SSH client (like **putty**) as a root user.
3. Create the temporary folder in the /data folder and save the public key.
4. Generate the random key using the following command:

```
openssl rand -base64 32 > randomkey.bin
```

5. Encrypt the random key by using the public key, using the following command:

```
openssl rsautl -encrypt -inkey public-key.pem -pubin -in randomkey.bin  
-out randomkey.bin.enc
```

6. Encrypt the CSV file by using the random key (not encrypted):

```
openssl enc -aes-256-cbc -salt -in <name of the CVS file that you want  
to encrypt> -out <outputfilename.CSV> -pass file:./randomkey.bin
```

For example, `openssl enc -aes-256-cbc -salt -in BrocadeSANSwitchProbeSample.csv -out BrocadeSANSwitchProbeEncrypted.csv -pass file:./randomkey.bin`

7. Download the encrypted random file and encrypted CSV file to your local machine.
8. Provide the encrypted random file and CSV file when adding the probe.

Adding Linux probe

The Linux probe collects performance and configuration data from individual machines running the Linux operating system.

Before you begin

- The following packages must be installed on the virtual machine (or host) to be monitored:
 - sysstat
 - perl
 - zip
- The following perl modules must be executable on the virtual machine or host to be monitored:

```
File::Path, Getopt::Std, HTTP::Request::Common, IO::Select, IO::Handle,
LWP::UserAgent, Time::HiRes
```



Note: When you install the perl modules, be sure to install them at the common location (accessible to all users). Refer to [Installing the perl module \(on page 203\)](#) for more information.

- The `openssh-clients` must be installed on the target machine or host.
- Create an installation directory with read, write, and execute permissions on all target machines for the data collection scripts. (Installation directory names are restricted to alphanumeric, hyphen, and underscore characters only.)
- A user with read, write, and execute permissions for `crontab` must be present on each target machine.
- Data for the following resources must be collected as the root user: Host Volume Group, Host Logical Volume, and Host Physical Volume.
- The `xinetd` service must be running on the Analyzer probe server.



Note: The Linux probe does not collect multipath information.

Procedure

1. On the Analyzer probe home page, click **Add Probe**.
2. In the **Add Probe** window, from the **Probes** list, select **Linux**.
3. In the **Add Host Details** section, type the following details, and then click **Next**:
 - **HOST IP ADDRESS:** The IP address of the target Linux host or machine.
 - **USERNAME:** A user on the target Linux host or machine.
 - **PASSWORD:** User password
 - **INSTALLATION DIRECTORY:** Location for the data collection scripts on the target Linux host or machine.
4. To add multiple targets, click **Add More** or click **Next** to continue.
The **Host Validation** section opens. The system validates the host IP address.

5. Click **Next**.
The **Script Deployment** section opens. The data collection scripts are deployed on the target host or machine.
6. Click **Next**, and then click **OK**.
7. In the **Status** window, in **Action**, click **Start** to start collecting data.
When adding multiple targets, the **Status** window shows multiple probes. You must start each probe individually.

Installing the perl module

The perl module must be installed on the virtual machine (or host) to be monitored by the Linux probe. Make sure that you install the perl module at the common location that is accessible to all users.

Procedure

1. Verify if the perl module is installed; you have two options for verification (using the **perl** command or **find**):

```
perl -e "use Date::module name"
```

For example: `perl -e "use Date::Gregorian"`

If the perl module is not installed, the following output is shown:

```
Can't locate Date/Gregorian.pm in @INC (@INC contains: /usr/local/lib64/perl5 /usr/local/share/perl5 /usr/lib64/perl5/vendor_perl /usr/share/perl5/vendor_perl /usr/lib64/perl5 /usr/share/perl5 .) at -e line 1.
```

Or

```
find `perl -e 'print "@INC"'` -name '*.pm' -print |grep -i module name
```

For example: `find `perl -e 'print "@INC"'` -name '*.pm' -print | grep -i Gregorian`

If the perl module is not installed, then the output is blank.

2. Install the perl module, using the following command:

```
cpan -i module name
```

For example, `cpan -i Date::Gregorian`



Note: You might be prompted for additional instructions. Follow the instructions to complete the installation.

3. Verify if the installation is successful. You can do this by using the **perl** or **find** commands).

Using the find command:

```
find `perl -e 'print "@INC"'` -name '*.pm' -print | grep -i
module_name
```

For example: `find `perl -e 'print "@INC"'` -name '*.pm' -print | grep -i Gregorian`

If the installation is successful, the output will be similar to the following:

```
/usr/local/share/perl5/Date/Gregorian/Business.pm
/usr/local/share/perl5/Date/Gregorian/Exact.pm
/usr/local/share/perl5/Date/Gregorian.pm
./cpan/build/Date-Gregorian-0.12-PmPHQp/lib/Date/Gregorian/Business.pm
./cpan/build/Date-Gregorian-0.12-PmPHQp/lib/Date/Gregorian/Exact.pm
./cpan/build/Date-Gregorian-0.12-PmPHQp/lib/Date/Gregorian.pm
./cpan/build/Date-Gregorian-0.12-PmPHQp/blib/lib/Date/Gregorian/
Business.pm
./cpan/build/Date-Gregorian-0.12-PmPHQp/blib/lib/Date/Gregorian/
Exact.pm
./cpan/build/Date-Gregorian-0.12-PmPHQp/blib/lib/Date/Gregorian.pm
```

Using the perl command:

```
perl -e "use Date::module_name"
```

For example: `perl -e "use Date::Gregorian"`

If the installation is successful, the output is blank.

Adding third-party storage probes (add-on package)

In addition to the Hitachi storage probes, you can also collect data about third-party storage systems by installing the third-party add-on package. This package is a separate download that requires an additional license.

For details on how to obtain, install, and use the third-party add-on package, see *Installing the third-party storage probe add-on package* in the Analyzer section of the Ops Center documentation:

https://knowledge.hitachivantara.com/Documents/Management_Software/Ops_Center

Initial setup after adding a probe

After adding a probe, check if the Analyzer detail view server is collecting data.

Procedure

1. Open a web browser, and then enter the following URL in the address bar to log on to the Analyzer detail view server :
`https://IP-address-of-Analyzer-detail-view-server:8443/`
2. In the logon window, enter the user name and password used to set up the Analyzer detail view server.
3. Click the **Server Status** icon.
4. Verify that the added probe appears in **Last Configuration Import Time** and **Last Performance Import Time** of **Data Import Status**, and that data is collected.



Note: After a probe is added, it might take some time before the probe appears in the Analyzer detail view server UI.

5. Open a web browser, and then enter the following URL in the address bar to log in to the Analyzer server:
`http://IP-address-of-the-Analyzer-server:22015/Analytics/login.htm`
6. Enter the following information to log on:
 - **User ID:** system
 - **Password:** manager (This is the default password that should be changed during installation.)
7. In the **Administration** tab, select **Resource Management**.
8. Verify that the resources monitored by the probe appear and are ready to be analyzed by the Analyzer server.



Note: After a probe is added, it might take some time before the registered resources appear in the the Analyzer server UI.

Chapter 8: Installing Analyzer Windows probe

Analyzer Windows probe collects performance and configuration data from the Windows host and Hyper-V machines. You can install this probe using Analyzer Windows probe installer.

Installing the Analyzer Windows probe

Install the Analyzer Windows probe by using the installer.

Procedure

1. Run the Analyzer Windows probe installer.
2. To continue installation, click **Next**.
3. In the **Log on Information** window, type the Domain Administrator or Local user name and password for the Windows machine in the format specified in the window, and click **Next**.



Note: The user must have the Administrator privileges and Logon as a Service permission.

4. In the **Choose Destination Location** window, browse to select the installation folder, and click **Next**.
5. In the **Ready to Install the Program** window, click **Install** to complete the installation.
6. Click **Finish**.



Note: If you deselect the **Launch Ops Center Analyzer Windows Probe** check box, double-click the **Ops Center Analyzer Windows Probe** icon on the desktop. If you do not see the icon on the desktop, then open a command prompt and enter the following to refresh the icon in the database:

```
ie4uinit.exe -ClearIconCache
```

7. In the **License** tab, browse to the license file and click **Submit** to register the license.

Data collection methods

You can use one of the following methods to collect data using the Analyzer Windows probe:



Note: Ops Center Analyzer only supports Method 3 (data collection using Perfmon API and WMI query).

Method 1: Data collection from System Center Operation Manager (SCOM) and System Center Configuration Manager (SCCM).

- Performance data is collected from SCOM
- Configuration data is collected from SCCM

Prerequisites

SCOM

- Target Windows machines must be configured in the SCOM server.
- A user with Advanced Operator or Administrator role with the permission to log on remotely to the SCOM server.
- Remote registry service must be running on the machine that is configured in the SCOM server.
- Import Management Pack in the SCOM server to configure the performance rules. You must copy the Management Pack from *Analyzer-Windows-probe-installation-directory\bin\SCOM Management Pack* and import it in SCOM server.

- Add the following DLLs in the *Analyzer Windows probe installer\bin* folder:

`Microsoft.EnterpriseManagement.Core.dll`

`Microsoft.EnterpriseManagement.OperationsManager.dll`

`Microsoft.EnterpriseManagement.Runtime.dll`

The above DLLs are located in the SDK Binaries folder on Windows machines:

Sample SCOM 2016 installation directory path: *SCOM Installation Directory*
`\Microsoft System Center 2016\Operations Manager\Server\SDK Binaries`

SCCM

- Target Windows machines must be configured in the SCCM server.
- Hardware Inventory Client Agent of SCCM must be running on the target machines. This agent collects required configuration data and stores it in the SCCM database.
- A user from the db_datareader group in the SQL Server who can access the SCCM database.

Method 2: Data collection from the System Center Operation Manager (SCOM) and WMI query

- Performance data is collected from the SCOM.
- Configuration data is collected from the individual machine using WMI query.

Prerequisites

SCOM

- Target Windows machines must be configured in the SCOM server.
- A user with Advanced Operator or Administrator role with the permission to log on remotely to the SCOM server.
- Remote registry service must be running on the machine that is configured in SCOM server.
- Import Management Pack in the SCOM server to configure the performance rules. You must copy the Management Pack from *Analyzer-Windows-probe-installation-directory\bin\SCOM Management Pack* and import it in SCOM server.

- Add the following DLLs in the *Analyzer Windows probe installer\bin* folder:

`Microsoft.EnterpriseManagement.Core.dll`

`Microsoft.EnterpriseManagement.OperationsManager.dll`

`Microsoft.EnterpriseManagement.Runtime.dll`

The above DLLs are located in the SDK Binaries folder on Windows machines:

Sample SCOM 2016 installation directory path: *SCOM Installation Directory*
`\Microsoft System Center 2016\Operations Manager\Server\SDK`
 Binaries

WMI Query

- You must be a user who has been assigned the Domain Administrator role and who has permission to access WMI namespaces (ROOT\WMI, ROOT, and ROOT\CIMV2) on the target host.

The **Execute Methods** and **Remote Enable** permissions are required for the namespaces.

- The authentication information (user name and password) on the Analyzer Windows probe server and the monitoring target server must match.
- Firewall exceptions must be added for the WMI on the target machine. To add the exceptions run the following commands on the target machine:
 - `netsh advfirewall firewall set rule group="remote administration" new enable=yes`
 - `netsh advfirewall firewall set rule group="File and Printer Sharing" new enable=yes`
- For workgroup computers, change the settings for the Remote User Account Control (UAC) `LocalAccountTokenFilterPolicy` registry entry.

Method 3: Data collection using Perfmon API and WMI query

- Performance and configuration data is collected from individual machines using the Perfmon API and WMI query.

Prerequisites

- The probe machine and the target machines must be part of either the same workgroup or the same domain.
- Firewall exceptions must be added for the WMI and Perfmon on the target machine. To add the firewall exceptions, run the following commands on the target machine:

- `netsh firewall set service RemoteAdmin`
- `netsh firewall set service type=fileandprint mode=enable profile=all scope=all`

- To connect to Windows machines remotely, the following must exist:
 - The remote registry service must be running on the target machine.
 - On the target machine the Local Service must have read permissions for the following registry key:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control
\SecurePipeServers\winreg
```

- Users who are to use this method must be added to **Log on as a service** of the **Local Group Policy Editor** on the target machine and the machine on which the Analyzer Windows probe is installed. To add these users, perform the following procedure:

Execute the **Local Group Policy Editor** (`gpedit.msc`), select Computer Configuration > Windows Settings > Security Settings > Local Policies > User Rights Assignment, and then add the users who are to use this method to the Log on as a service policy.

- The authentication information (user name and password) on the Analyzer Windows probe server and the monitoring target server must match.
- Distributed COM must be enabled in **Component Services** on the target machine and the machine on which the Analyzer Windows probe is installed. To enable distributed COM, perform the following procedure:

Execute **Component Services** (`dcomcnfg.exe`), and then select Component Services > Computers. When My Computer is displayed, right-click My Computer, and then select Properties. After that, select the Default Properties tab, and then select Enable Distributed COM on this computer.

- **For domain computers:** A user with the Domain Administrator role or local administrator group of the target machine and the machine on which the Analyzer Windows probe is installed.
- **For workgroup computer:** The following settings are required if you are not using the built-in administrator for connections:
 - You must be a user who has been assigned the Domain Administrator role and who has permission to access WMI namespaces (ROOT\WMI, ROOT, and ROOT\cimv2) on the target host.

Execute Methods and **Remote Enable** permissions are required for the namespaces.

 - Change the settings for the Remote User Account Control (UAC) `LocalAccountTokenFilterPolicy` registry entry. For more information, see <http://support2.microsoft.com/kb/942817/en-us>.
 - Computer Browser service must be running on the target machine.

Configuring Analyzer Windows probe

After installing the Analyzer Windows probe, you must configure a collection method, set up an FTP or HTTPS server, and start the service for that probe.

Configuring the data collection method

You must register the Analyzer Windows probe and select the data collection method for that Analyzer Windows probe.

Procedure

1. On the Analyzer Windows probe console, click the **Collection** tab, and configure the collection method settings based on your requirements:

Method 1: Data collection from SCOM and SCCM

- a. In the **Performance** section, select **Use SCOM** and type the following details:
 - **SCOM Server:** SCOM server IP address
 - **User Name (Advanced Operator):** SCOM server user name
 - **Password:** SCOM server password
- b. In the **Configuration** section, select **Use SCCM** and type the following details:
 - **SCCM Database Server:** SCCM Server IP address or the name
 - **Database Name:** SCCM database name

- **SQL Server User Name:** SCCM database user name
- **SQL Server Password:** SCCM database password



Note: If you select the **Trusted Connection** check-box, then the **SQL Server User Name** and **SQL Server Password** fields are disabled.

Method 2: Data collection from SCOM and WMI

- a. In the **Performance** section, select **Use SCOM** and type the following details:
 - **SCOM Server:** SCOM server IP address
 - **User Name (Advanced Operator):** SCOM server user name
 - **Password:** SCOM server password
- b. In the **Configuration** section, select **Use WMI** and type the following details:
 - **User Name (Administrator):** Domain administrator user name
 - **Password:** Domain administrator user name password

Method 3: Data collection through WMI and PerfMon

- a. In the **Performance** section, select **Use Perfmon**.
This enables the **Use WMI** option automatically.
- b. Type the following details for **Use Perfmon** and **Use WMI** options:
 - i. **User name (Administrator):**
 - In Workgroup environment: `Machine Name\User`
Computer Name: Machine name on which the Analyzer Windows probe is installed.
User: A user with an Administrator role.
 - In the Active Directory environment: `Domain Name\User`
Domain Name: Name of the domain.
User: A user with the Domain Administration role.
 - ii. **Password**
- c. In the **Performance** section, select the **Collect Process Data** box if you want to collect process data.

2. On the **Collection** tab, in the right-most side section:
 - Click **Discover Hosts** to discover the hosts available in the current domain. You can then select the target host that you want to monitor.
 - Click **Add Hosts** and type the host names manually. The **Add Hosts** window opens. Enter a comma-separated list of Windows machines (host names or IP addresses).
3. Click **Validate & Save** to establish the connection, and click **OK**.

Configuring the FTP or HTTPS server

You must configure the FTP server for the Analyzer Windows probe to send data.

Procedure

1. On the Analyzer Windows probe console, click the **Upload Settings** tab.
2. On the **Upload Settings** tab, select the protocol **FTP** or **HTTPS**.
3. Type the following details:
 - **FTP Server:** The Analyzer detail view server IP address where you want to upload the data. For the supported ciphers refer to [Supported ciphers for Analyzer Windows probe \(on page 38\)](#).
 - **Port:** Port number. The default port for FTP is 21.
 - **User:** meghadata
 - **Password:** The default password is meghadata123
4. To use a proxy server, select the **Use Proxy** check box and type the following details:
 - **Proxy Server:** Name or IP address of the proxy server.
 - **Proxy Type:** Proxy type of the proxy server `HTTP` or `SOCKS5`.
 - **Port:** Proxy FTP port.
 - **Login and Password:** User name and Password of the proxy server.
5. Click **Validate & Save**.
6. Start the Analyzer Windows probe service.



Note: To improve security for the FTP account, you must change the meghadata user default password. Refer to [Changing the megha and meghadata passwords \(on page 88\)](#) for more information.



Note: The Analyzer Windows probe must be installed on a Windows machine with the System Locale as English.

Starting the Analyzer Windows probe service

Start the probe service from the Status tab in the Analyzer Windows probe console.

Procedure

1. On the Analyzer Windows probe console, click the **Status** tab.
The **Status** tab list the details of the upload information and service information.
2. Verify the upload and service information, and click **Start**.



Note: When you change the time zone of the Windows machine on which the Analyzer Windows probe is installed, restart the Analyzer Windows probe console to update the Analyzer Windows probe with this new time zone.

Downloading the Analyzer Windows probe diagnostic data

The Analyzer Windows probe collects various log files that are useful for troubleshooting. The Diagnostic Data feature provides the facility to download these files in an archive file. If you cannot resolve the problem, send the generated data file with the error messages to customer support for analysis.

Before you begin

- To download diagnostic data, you must have the Administrator privileges.
- Make sure that minimum 1 GB free disk space is available on the C drive.

Procedure

1. On the Analyzer Windows probe console, click the **Diagnostic Data** tab.
2. Click **Download**.
The diagnostic data generation process begins.
3. In the **Save As** window, choose any location to save the file and then click **Save**.
Sample diagnostic data file name: Analyzer-Windows-probe_diag_20190611192343.zip

Analyzer Windows probe configuration backup

The Analyzer Windows probe configuration is automatically backed up at midnight to the following location on the FTP server:

*Probe-appliance-ID/probeConfigBackup/
WindowsProbeConfigurationBackup_Probeversion.zip.enc*

The time of the last backup is displayed in the **Status** tab. For example:

Last Backup Upload Time: 15 Nov 2017 00:30:50

The backup data can be used to migrate the Analyzer Windows probe to another machine if it is corrupted or inaccessible. However, the backup can only be restored by contacting customer support.

Initial setup after adding a probe

After adding a probe, check if the Analyzer detail view server is collecting data.

Procedure

1. Open a web browser, and then enter the following URL in the address bar to log on to the Analyzer detail view server :
`https://IP-address-of-Analyzer-detail-view-server:8443/`
2. In the logon window, enter the user name and password used to set up the Analyzer detail view server.
3. Click the **Server Status** icon.
4. Verify that the added probe appears in **Last Configuration Import Time** and **Last Performance Import Time** of **Data Import Status**, and that data is collected.



Note: After a probe is added, it might take some time before the probe appears in the Analyzer detail view server UI.

5. Open a web browser, and then enter the following URL in the address bar to log in to the Analyzer server:
`http://IP-address-of-the-Analyzer-server:22015/Analytics/login.htm`
6. Enter the following information to log on:
 - **User ID:** system
 - **Password:** manager (This is the default password that should be changed during installation.)
7. In the **Administration** tab, select **Resource Management**.
8. Verify that the resources monitored by the probe appear and are ready to be analyzed by the Analyzer server.



Note: After a probe is added, it might take some time before the registered resources appear in the the Analyzer server UI.

Uninstalling the Analyzer Windows probe

To remove the Analyzer Windows probe, use the uninstall function of Windows.

Procedure

1. Go to the **Control Panel** of the Windows machine.
2. In **Programs**, click **Uninstall a program**.
3. Select the Analyzer Windows probe to uninstall.

To uninstall the Analyzer Windows probe, you must have the Domain Administrator or Local user with Administrator privileges.

4. Click **Uninstall/Change**.
5. Confirm the uninstall by clicking **Yes**.
6. When the completion status message is shown, confirm it by selecting **OK**.
The following files of the Analyzer Windows probe are not deleted after uninstalling the probe. (You can remove them manually.)
 - C:\Temp\HDCA\ProbeDataStatus.properties
 - C:\Temp\WindowProbeInstallerOutput.txt
 - C:\Temp\Collected configuration and performance files which are not uploaded

Chapter 9: Upgrade your Ops Center Analyzer environment

You can upgrade Ops Center Analyzer components.

Upgrade workflow

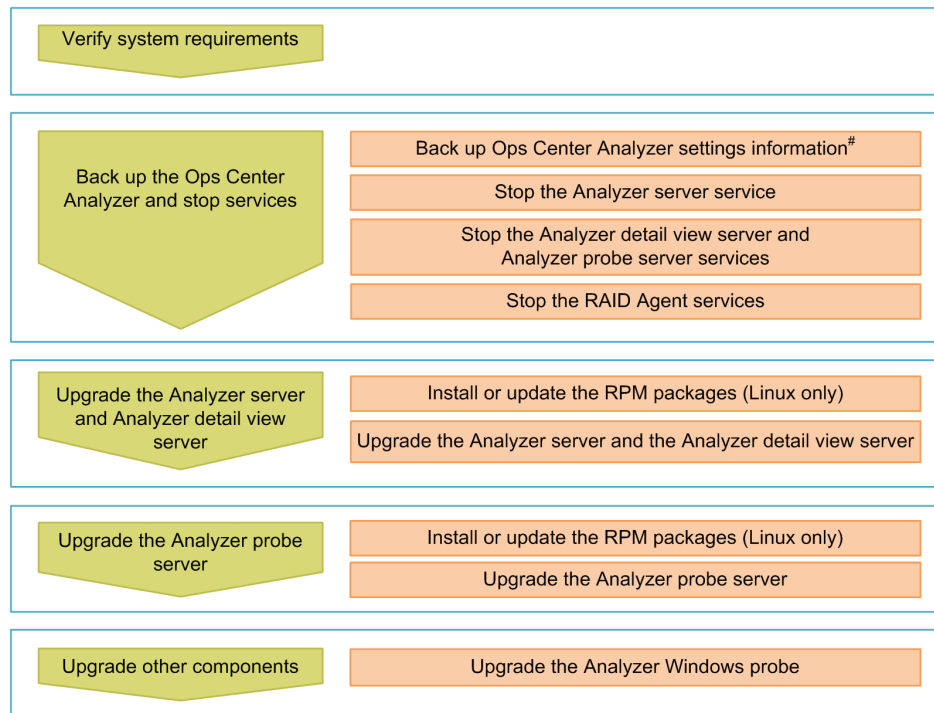
Run the installer to upgrade the following components:

- Analyzer server
- Analyzer detail view server
- Analyzer probe server (including the RAID Agent on the same host)
- Windows probe



Note: If you are using Tuning Manager - Agent for RAID, check whether it is supported by the upgraded version of Ops Center Analyzer. If it is not supported, you must upgrade Tuning Manager - Agent for RAID. For the upgrade procedure, see the *Hitachi Command Suite Tuning Manager Installation Guide*.

The following figure shows the sequence of tasks for upgrading Ops Center Analyzer. Even if you used a virtual appliance to complete the initial installation, you must use the installers when upgrading. Note that you must also follow this sequence of tasks if you are upgrading to Ops Center Analyzer from Infrastructure Analytics Advisor.



[#]: This is a precautionary task in case the upgrade fails.

Installing or updating the RPM packages (Linux OS)

Before installing or upgrading the Analyzer server, Analyzer detail view server, or Analyzer probe server, check whether all of the RPM packages required for each component are installed. If some packages are missing, you must install them as an

additional step. You can obtain the RPM packages from the Linux OS media or the distribution website, such as for Red Hat Enterprise Linux.

- For details about the RPM packages required for each component, see [Analyzer server requirements \(Linux\) \(on page 25\)](#), [Analyzer detail view server requirements \(on page 28\)](#), or [Analyzer probe server requirements \(on page 30\)](#).
- The package `nss-3.21.0` may not be included in the Linux OS media of certain versions. Obtain this package from the Linux OS media for version 6.8 or later, or from the distribution website.
- If the `libstdc++` package is already installed in the environment in which the Analyzer probe server will run, you might not be able to install `libstdc++.i686` and an error message such as the following might be output:

```
Protected multilib versions: libstdc++-xx.xx.xx-xx.xx.el6.i686 !=
libstdc++-yy.yy.yy-yy.yy.el6.x86_64
```

This error occurs because the version of the `x86_64` package (the 64-bit library) differs from that of the `i686` package (the 32-bit compatibility library). If this happens, update `x86_64` (the 64-bit library), and then retry the installation of `libstdc++.i686`:

```
yum update libstdc++.x86_64
```

Installing or updating the packages by using the Linux OS media

The following describes how to install or update the RPM packages by using the Linux OS media. Change the information that you must specify in the procedure according to the environment you are using.

1. Mount the Linux OS media and obtain the RPM packages:

```
mkdir /media/OSImage
mount /dev/cdrom /media/OSImage
```

2. Configure the yum repository:

```
touch /etc/yum.repos.d/OSImage.repo
echo [dvd]>>/etc/yum.repos.d/OSImage.repo
echo name=dvd>>/etc/yum.repos.d/OSImage.repo
echo baseurl=file:///media/OSImage/>>/etc/yum.repos.d/OSImage.repo
echo gpgcheck=0>>/etc/yum.repos.d/OSImage.repo
echo enabled=1>>/etc/yum.repos.d/OSImage.repo
```

3. Run the **yum** command to install or update the packages and package group:

- **For packages:**

```
yum install package-to-be-installed
```

Example:

```
yum install java-1.8.0-openjdk-devel sysstat zip
```

- **For the package group:**

```
yum group install package-group-to-be-installed
```

4. Unmount the Linux OS media:

```
umount /media/OSImage/  
rm /etc/yum.repos.d/OSImage.repo
```

Installing or updating the packages using the distribution website

The following describes how to install or update the RPM packages by using the distribution website. Change the information that you must specify in the procedure according to the environment you are using.

1. Specify the repository to which the **yum** command is to connect.

For Red Hat Enterprise Linux, register the system by using Red Hat Subscription Management. For details, see <https://access.redhat.com/articles/11258>.

For Oracle Linux, the initial settings are set by default (the file `repo` is already located in the directory `/etc/yum.repos.d`). For details, see <http://yum.oracle.com/getting-started.html>.

2. If you are using a proxy, specify the proxy for the **yum** command.

- a. Add the following information to the `/etc/yum.conf` file:

```
proxy=http://host-name:port-number  
proxy_username=user-name  
proxy_password=password
```

- b. Clear the cache for the **yum** command.

```
yum clean all
```

3. Run the **yum** command to install or update the packages and package group.

- **For packages:**

```
yum install package-to-be-installed
```

Example:

```
yum install java-1.8.0-openjdk-devel sysstat zip
```

- **For the package group:**

```
yum group install package-group-to-be-installed
```

Upgrading the Ops Center Analyzer and the Analyzer detail view servers on a Linux host

You can upgrade both the Analyzer server and the Analyzer detail view server by using the installer (`analytics_install.sh`). If you are only upgrading one of the components, also refer to this section.

The installer starts and stops the `crond` service. Therefore, do not run any operations that use the `crond` service when the installer is running.

Before you begin

To upgrade the Analyzer detail view server, a license must be registered.

Upgrading from version 3.0.0 or a later version

1. Log on to the host where the components to upgrade are installed.
2. Stop any security monitoring software, antivirus software, and process monitoring software.
3. Mount the Hitachi Ops Center installation media and copy the directories and files in the `ANALYTICS` directory from the installation media to a directory on the Linux host.



Note:

- The following characters can be used in the path of the directory to which the installer is copied: `A-Z a-z 0-9 - . _`
- Space characters cannot be used.

In the following example, if the `/root/ANALYTICS` directory already exists, create a new directory, and then perform the subsequent steps in the new directory.

```
mkdir /media/OpsImage  
mount /dev/cdrom /media/OpsImage
```

```
mkdir /root/ANALYTICS
cp -rT /media/OpsImage/Analyzer/ANALYTICS /root/ANALYTICS
```

4. Move to the `/root/ANALYTICS` directory.

```
cd /root/ANALYTICS
```

5. Run the precheck tool as a root user to check whether Analyzer server and Analyzer detail view server can be installed:

```
sh ./analytics_precheck.sh
```



Note: When you run the precheck tool, it checks the static information of the system environment.

If OK is displayed in [Check results], you can start the installation. If NG is displayed, make sure the system requirements have been met.

Output example when the Ops Center Analyzer version is 10.0.0:

```
=====
Analytics Precheck                                ver. 10.0.0-00
=====

[ Check results ]
Ops Center Analyzer detail view server [10.0.0-00]      [OK]
Ops Center Analyzer server [10.0.0-00]                  [OK]

[ Details ]
Check premise OS version.                               [OK]
      :
      :
```

If the `-v` option is specified, information such as the installed version of Analyzer server and Analyzer detail view server, the host name, and the OS name is also displayed.

6. Run the following command as root to start the upgrade:

```
sh ./analytics_install.sh VUP
```

A message is displayed, confirming that you want to upgrade the Analyzer detail view server and Analyzer server.

7. Enter `y`, and then specify the components that you want to upgrade.

```
Do you want to install the Ops Center Analyzer detail view server?
(y/n) [n]: y

Do you want to install the Ops Center Analyzer server? (y/n) [n]: y
```

```
[Confirmation]
-----
Installation Product
(1) Ops Center Analyzer detail view server
(2) Ops Center Analyzer server
-----
Do you want to install the server listed above? (y/n) [n]: y
```

Upgrading the Analyzer server on a Windows host

Upgrade the Analyzer server on a Windows host by using the installation media.

Procedure

1. Log on to the host where the Analyzer server is installed as the Administrator user.
2. Stop any security monitoring software, antivirus software, and process monitoring software.
3. Run `ANALYTICS.msi` on the installation media to start Analyzer server installer. Follow the on-screen prompts and specify the required information.
You can specify, as an option, whether to back up the data before performing the upgrade (best practice).

This option is `yes` by default.

Upgrading the Analyzer probe server

If you upgrade the Analyzer probe server, the RAID Agent on the same host is automatically upgraded.

The installer (`dcaprobe_install.sh`) starts and stops the `crond` service. Therefore, do not run any operations that use the `crond` service when the installer is running.

Before you begin

- To upgrade the Analytics probe server from a version earlier than 4.0.0, you must first upgrade the Analyzer probe server to version 4.0.0.
- A license for the Analyzer probe server must be registered.

Upgrading from version 3.0.0 or a later version

1. Log on to the host where the component to upgrade is installed.
2. Stop any security monitoring software, antivirus software, and process monitoring software.
3. Mount the Hitachi Ops Center installation media and copy the directories and files in the `DCAPROBE` directory from the installation media to a directory on the Linux host.

**Note:**

- The following characters can be used in the path of the directory to which the installer is copied: A-Z a-z 0-9 - . _
- Space characters cannot be used.

In the following example, if the `/root/DCAPROBE` directory already exists, create a new directory, and then perform the subsequent steps in the new directory.

```
mkdir /media/OpsImage
mount /dev/cdrom /media/OpsImage
mkdir /root/DCAPROBE
cp -rT /media/OpsImage/DCAPROBE /root/DCAPROBE
```

4. Move to the `/root/DCAPROBE` directory.

```
cd /root/DCAPROBE
```

5. Run the precheck tool as a root user to check whether Analyzer probe server can be installed:

```
sh ./dcaprobe_precheck.sh
```



Note: When you run the precheck tool, it checks the static information of the system environment.

If OK is displayed in [Check results], you can start the installation. If NG is displayed, make sure the system requirements have been met.

Output example when the Ops Center Analyzer version is 10.0.0:

```
=====
Ops Center Analyzer probe Precheck          ver. 10.0.0-00
=====

[ Check results ]
Ops Center Analyzer probe server [10.0.0-00]          [OK]

[ Details ]
Check resolved hostname. [host-name (IP-address)]     [OK]
Check premise OS version.                             [OK]
:
:
```

If the `-v` option is specified, information such as the installed version of Analyzer probe server and the OS name is also displayed.

6. Run the following command as root to start the upgrade:

```
sh ./dcaprobe_install.sh VUP
```

Upgrading Analyzer Windows probe

You can upgrade the Analyzer Windows probe by using the Analyzer Windows probe installer.

Before you begin

- The user must have the Administrator privileges and Logon as a Service permission.
- The Analyzer Windows probe must be installed on a Windows machine with one of the following English System Locale:

English (Australia), English (Belize), English (Canada), English (Caribbean), English (India), English (Ireland), English (Jamaica), English (Malaysia), English (New Zealand), English (Philippines), English (Singapore), English (South Africa), English (Trinidad and Tobago), English (United Kingdom), English (United States), English (Zimbabwe).
- The Display language and Input Method language on a Windows machine must be set to English.
- If you are using data collection Method 1 and Method 2, then verify that the following DLLs are present in the *Analyzer Windows probe installer\bin* folder:

`Microsoft.EnterpriseManagement.Core.dll`

`Microsoft.EnterpriseManagement.OperationsManager.dll`

`Microsoft.EnterpriseManagement.Runtime.dll`

If the above DLLs are not available, then you can copy it from the following folder on Windows machine and save it in the *Analyzer Windows probe installer\bin* folder:

Sample installation directory path: *SCOM Installation Directory\Microsoft System Center 2016\Operations Manager\Server\SDK Binaries*

Procedure

1. Download the Analyzer Windows probe installer to your machine.
2. Double-click on the Analyzer Windows probe installer, and then follow the instructions.

The Analyzer Windows probe is installed at the following default location:

`C:\Program Files\HDCA\HDCA Windows Probe`

If you are upgrading the Analyzer Windows probe earlier than version 9.2.0-00 installed on a Windows 64-bit machine, the upgrade process takes the backup of the current Analyzer Windows probe configuration file. The installer moves the backed-up file to a new location after the upgrade: `C:\Program Files\HDCA\HDCA Windows Probe`

Checking the settings after an upgrade

After a successful upgrade, certain custom settings may require resetting so that all items are displayed correctly in the Ops Center Analyzer web user interface.

Check the following:

- **Content display:** If any tables are missing content or display content incorrectly, select File > Clear Settings, and then click OK to clear the settings saved in the browser.

This procedure also clears the following information:

- Table configuration information (column settings, column widths, column sorting status, filtering status)
- History of search keywords
- **Connection settings with Ops Center Automator:** If you upgrade the components from version 3.1.0-01 or earlier, the connection settings with Ops Center Automator are disabled. If you are using the I/O control configuration function using Ops Center Automator, perform the procedure for [Reconfiguring the connection with Ops Center Automator after an upgrade \(on page 225\)](#).
- **Data collection method:** If you upgrade the components from a version earlier than 4.1.0, you can choose the data collection method by specifying the `Access Type` in the instance information for all RAID Agent instances. `Access Type` corresponds to `Method for collecting` in versions earlier than 4.1.0. We recommend revising the settings because, in addition to `Access Type`, other items in the instance information are also changed.

If you change the value of `Access Type`, make sure that the value of the collection interval for RAID Agent and the value of the collection interval for the Hitachi Enterprise Storage probe are the same. If these values do not match, change one or both of the values so that the specified collection intervals are the same.

If you want to use Common Services with Analyzer after an upgrade, check the following:

- **Security communication settings:** To use Common Services, the SSL settings are required. If you did not enable SSL communication during the use of Infrastructure Analytics Advisor, see [Configuring an SSL certificate \(Analyzer server\) \(on page 316\)](#) and [Configuring an SSL certificate \(Common Services\) \(on page 348\)](#). If you enabled SSL communication during the use of Infrastructure Analytics Advisor, see [Configuring an SSL certificate \(Common Services\) \(on page 348\)](#).
- **Initial settings for using Common Services:** When you use Common Services for the first time, perform the procedures in [Registering Ops Center Analyzer in Ops Center Common Services \(on page 85\)](#) and [Assigning Analyzer permissions to Ops Center user groups \(on page 86\)](#).

Reconfiguring the connection with Ops Center Automator after an upgrade

If you upgrade the components from version 3.1.0-01 or earlier, and want to continue to use the I/O control settings functionality that uses Ops Center Automator, you must reconfigure the connection with Ops Center Automator.

Before you begin

- This procedure is necessary if all of the following conditions exist:
 - The I/O control configuration function that uses Ops Center Automator was used before upgrading the components.
 - The components were upgraded from version 3.1.0-01 or earlier.

Procedure

1. Revise the Common component settings.
For more information, see [Initial setup for connecting with Ops Center Automator \(on page 90\)](#).
2. In Ops Center Analyzer, download the service templates.
 - a. On the **Administration** tab, select **System Settings > Automator Server**.
 - b. Click the link to download the service template.
The name of the service template is `AnalyticsServiceTemplate.zip`.
3. Register the storage system in Ops Center Automator.
 - a. On the **Administration** tab, select **Connection Settings > Web Service Connections**.
 - b. Click **Add**, and then specify the following information about the storage systems with Server Priority Manager:
 - Category: Specify "ConfigurationManager".
 - Name: Device number of the storage system
 - IPAddress/HostName: IP address or host name of the host on which the Ops Center API Configuration Manager is installed
 - Protocol: **http** or **https**
 - Port: Port number used by the Ops Center API Configuration Manager
 - User ID and password: User account with permission to access the logical devices and ports that you want to operate (user ID that was specified when the storage system was registered to the Ops Center API Configuration Manager)
 - Assigned Infrastructure Groups: Infrastructure group to which the target storage system is registered

If you are not using the infrastructure group functionality, specify "IG_Default Service Group".

**Note:**

- If a name other than "ConfigurationManager" was specified for the category before the upgrade, we recommend that you continue to use the same name.

If any name other than "ConfigurationManager" is specified for the category, you must edit the file `config_user.properties`.
- If any name other than "ConfigurationManager" is specified, an error message is displayed when you connect with the Ops Center API Configuration Manager by clicking the **Test** button. Despite this error message, the I/O control settings functionality operates normally when the correct value is registered to each field.

4. Import the service templates in Ops Center Automator.
 - a. Unzip the file `AnalyticsServiceTemplate.zip` to a location of your choice.
 - b. On the **Service Templates** tab, click **Import**.
 - c. Click **Browse**, and then specify one of the following zip files:
 - If you are using Automation Director version 8.5.2 or a later version:
`ServiceTemplate_03.20.00.zip`
 - If you are using Automation Director version 8.5.0:
`ServiceTemplate_03.00.02.zip`

These zip files contain two service templates:

- `com.hitachi.software.dna.analytics_DeleteIoControlSettings_version.st` - This template disables an I/O control task.
- `com.hitachi.software.dna.analytics_ModifyIoControlSettings_version.st` - This template enables or modifies an I/O control task.

- d. Click **OK**.



Tip: If you do not see the I/O control settings service templates, sort service template files by using **Registered**, and the latest imported templates will appear with the **New** tag.



Note: If you import the file `ServiceTemplate_03.00.02.zip`, "OUTDATED" might be displayed in the imported service template, indicating that the version has expired. If "OUTDATED" is displayed, do not update the service template. If you update the file, the service template will become unusable.

5. Use the service templates to create the services for Server Priority Manager:
 - a. On the **Administration** tab, select **Resources and Permissions** > **Service Groups**.
 - b. Select the service group that was used for the I/O control settings functionality.
 - c. On the **Services** tab, click **Create**.
 - d. Select the service templates, and then click **Create Service**.

- e. Verify or specify the following information using the best practice names to create the service:
 - Name of the service for updating Server Priority Manager settings: Modify IO Control Settings for Volume
 - Name of the service for deleting Server Priority Manager settings: Delete IO Control Settings for Volume
 - Status: Release



Note: Do not modify the I/O control settings. These fields are autopopulated by the information entered on the Ops Center Analyzer user interface when you submit an I/O control task.

- f. Click **Save and Close** to close the window.
6. Assign an infrastructure group to the service group to which you registered the services.
 - a. On the **Resources** tab, click **Assign**.
 - b. From **Available Infrastructure Groups**, select an infrastructure group, and then click **Add**.

If you are not using the infrastructure group functionality, specify "IG_Default Service Group".
 - c. Confirm that the selected infrastructure group has been moved to **Assigned Infrastructure Groups**, and then click **OK**.

7. Edit the `config_user.properties` file.

This step is not required if you use the recommended name for the service group name, category name, or service name. If you use a name other than the recommended name, specify, in the `config_user.properties` file, the name set in Ops Center Automator.

The location of the `config_user.properties` file is as follows:

For Windows

`Analyzer-server-installation-destination-folder\Analytics\conf`

For Linux

`Analyzer-server-installation-destination-directory/Analytics/conf`

Specify the following keys and values:

- `automation.parameter.serviceGroupName`: Service group name specified in Ops Center Automator
- `automation.parameter.productName`: Category name specified in Ops Center Automator
- `automation.parameter.serviceName.ioControl.modify`: Service name set in Ops Center Automator as the name of the service for updating Server Priority Manager settings
- `automation.parameter.serviceName.ioControl.delete`: Service name set in Ops Center Automator as the name of the service for deleting Server Priority Manager settings

8. If you have edited the `config_user.properties` file, restart the Analyzer server services.

Result

The setup procedure for controlling storage resources is now complete.

Next steps

Check the connection between Ops Center Analyzer and Ops Center Automator.

Chapter 10: Configure external user authentication

You can set user authentication on an external authentication server.

If you use Ops Center Common Services for user authentication, you can use external user authentication (LDAP authentication or Kerberos authentication). For details, see the *Hitachi Ops Center Installation and Configuration Guide*.

External user authentication overview

Analyzer server supports external authentication using LDAP, RADIUS, and Kerberos servers.

External authentication servers can be used to authenticate the users who log on to the Ops Center Analyzer. The built-in administrator accounts cannot be authenticated by external authentication servers. The user credentials are managed by the external authentication servers.

Analyzer server users can be assigned privileges using an external authorization server such as LDAP directory server (Active Directory). The user privileges can be managed using Active Directory groups (authorization groups) registered on the external authorization server.

To perform user authentication for Ops Center Analyzer by using an external authentication server, you must configure settings for external user authentication on both the Analyzer server and the Analyzer probe server.



Note:

Configuring the settings for external user authentication for the Analyzer detail view server is optional.

You must configure the settings for external user authentication only if you want to log on to the Analyzer detail view server by using Active Directory user accounts.

When the Analyzer detail view UI is launched from the Ops Center Analyzer UI, you do not need to configure settings for external user authentication on the Analyzer detail view server because internal user accounts are used.

Analyzer probe server and Analyzer detail view server support connection to LDAP directory servers (Active Directory) for use as external authentication servers.

**Note:**

In Analyzer server, 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

Configuring multiple external authentication servers

The Analyzer server supports external user authentication using multiple external authentication servers in a redundant configuration or in a multi-domain configuration.

In a redundant configuration each external authentication server manages the same user information. If a failure occurs on one external authentication server, user authentication can be performed by using another external authentication server.

A multi-domain configuration is used to manage different user information for each external authentication server. If a user logs on with a user ID that includes a domain name, the user will be authenticated by an external authentication server in the domain whose name is included in the user ID. When a Kerberos server is used as an external authentication server, you can create a configuration similar to a multi-domain configuration by managing different user information for each realm.

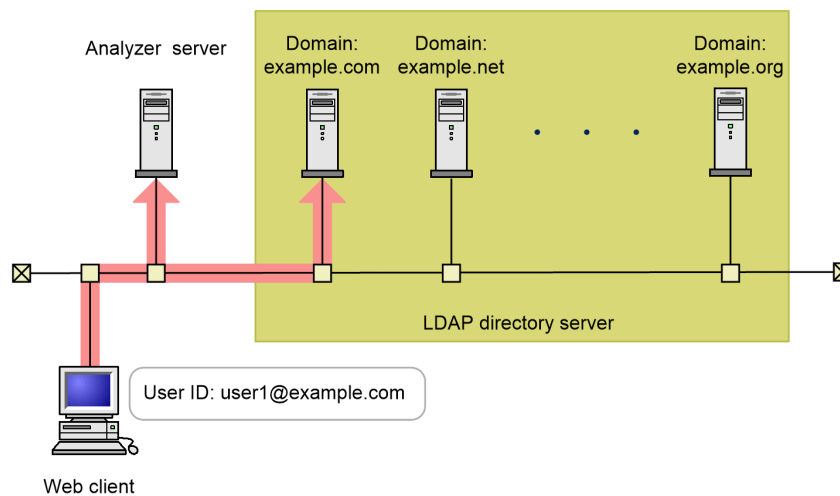
The following table shows external authentication servers for which redundant configurations and multi-domain configurations are supported.

External authentication server	Redundant configuration	Multi-domain configuration
LDAP directory server	Y ¹	Y ¹
RADIUS server	Y	N
Kerberos server	Y	Y ²
Legend: Y: Supported N: Not supported Notes:		


External authentication server	Redundant configuration	Multi-domain configuration
<ol style="list-style-type: none"> 1. You can use either a redundant configuration or a multi-domain configuration. If the global catalog for Active Directory is set, you can use both a redundant configuration and a multi-domain configuration. 2. By managing different user information for each realm, you can create a configuration that is similar to a multi-domain configuration. 		

When an LDAP directory server is used for user authentication in a multi-domain configuration, the user authentication process varies depending on whether you log on by entering a user ID that includes a domain name.

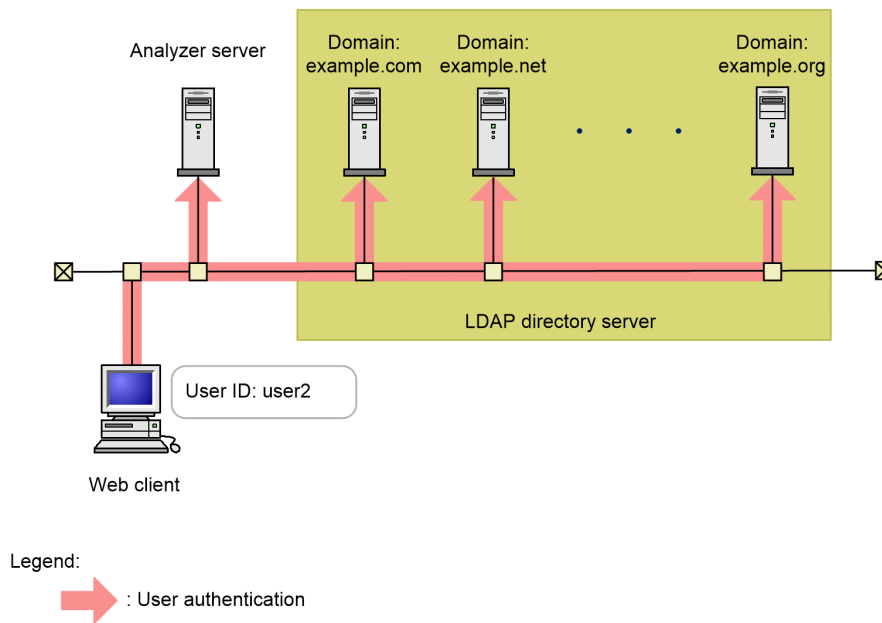
If you log on with a user ID that includes a domain name, as in the following figure, user authentication will be performed by using the LDAP directory server of the specified domain.



Legend:

 : User authentication

If you log on with a user ID that does not include a domain name, user authentication is performed sequentially on all LDAP directory servers until the user is authorized, as shown in the figure below. In an environment that includes a large number of LDAP directory servers, user authentication will take a long time. For this reason, we recommend that you log on with a user ID that includes a domain name.



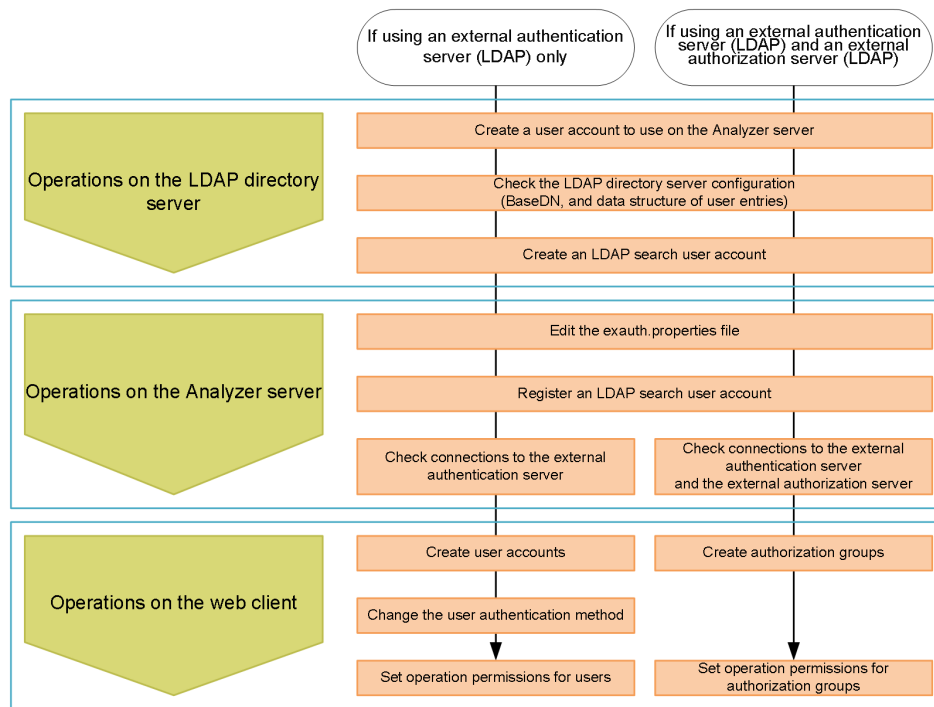
Configuring LDAP authentication for Analyzer server

To use LDAP authentication for the Analyzer server, you must configure the following settings.

Workflow for configuring LDAP authentication

The workflow for connecting to the LDAP directory server varies depending on whether only an external authentication server is used or both an external authentication server and an external authorization server are used.

The following figure shows the workflow for connecting to the LDAP directory server.



Note: To use StartTLS to communicate between the LDAP directory server and the Analyzer server, you must set up an environment specifically for this purpose to ensure secure communications.

Configuring the LDAP directory server

On the LDAP directory server, create a user account for the Analyzer server. Next, check the configuration details of the LDAP directory server, and then create an LDAP search user account.

Creating user accounts on an LDAP directory server

On an LDAP directory server, you must create user accounts (user IDs and passwords) to use on the Analyzer server.

For details about how to create user accounts on an LDAP directory server, see the documentation of the LDAP directory server.

User IDs and passwords must satisfy the following conditions:

- They are within 256 bytes.
- They use no characters other than the following:

A to Z

a to z

0 to 9

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

In Analyzer server, user IDs are not case-sensitive. The combination of character types for passwords must follow the settings in the external authentication server.

Checking the LDAP directory server settings

To use the LDAP directory server as an external authentication server or external authorization server, you must check the LDAP directory server settings in advance.

Check the following two settings:

- BaseDN

A BaseDN is the entry point from where a server starts searching for users during authentication or authorization. The BaseDN must be an entry from which the Analyzer server can search for all users that it needs to authenticate or authorize.

- Data structure of user entries (only when the LDAP directory server is used as an external authentication server)

There are two types of data structures for user entries on the LDAP directory server: the hierarchical structure model and the flat model.

You will need information about these settings when you edit the `exauth.properties` file on the Analyzer server. Note that, depending on data structure of the user entries, you must perform different tasks on the Analyzer server.

For details about how to check the information about the settings, see the documentation for the LDAP directory server that you are using.

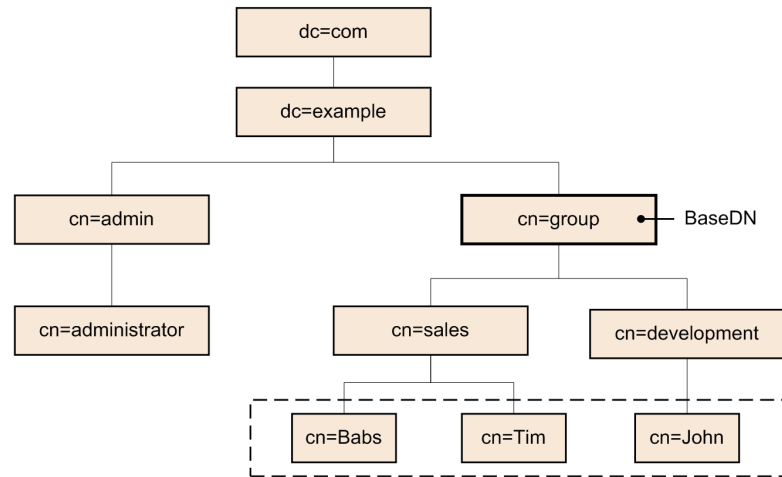
The following describes BaseDN in the hierarchical structure model and in the flat model.

- In the hierarchical structure model:

The hierarchical structure model is a data structure in which the hierarchy below BaseDN branches out, and user entries are registered under each of these hierarchies.

If the hierarchical structure model is used, the entries in the hierarchy below BaseDN are searched for an entry that has the same logon ID and user attribute value.

The following figure shows an example of the hierarchical structure model.



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

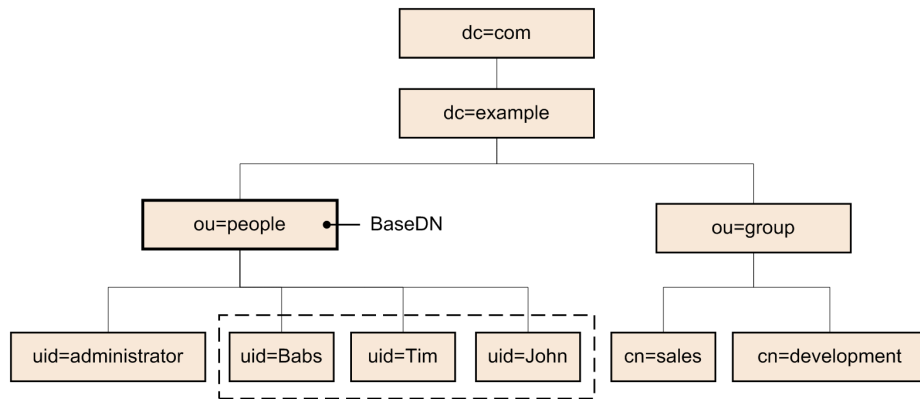
The user entries enclosed by the dotted line can be authenticated. In this example, BaseDN is `cn=group,dc=example,dc=com`, because the target user entries extend across two departments (`cn=sales` and `cn=development`).

- In the flat model:

The flat model is a data structure where there are no branches in the hierarchy below BaseDN, and where user entries are registered in the hierarchy directly 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 logon ID and BaseDN. If such a value is found, the user is authenticated.

The following figure shows an example of the flat model.



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

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`.

However, even if the flat model is being used, if either of the following conditions is satisfied, you must specify the settings by following the explanation for the hierarchical structure model:

- A user attribute value other than the RDN attribute value (such as a Windows logon ID) is used as the user ID of the Analyzer server.
- The RDN attribute value of a user entry includes a character that cannot be used in a user ID for the Analyzer server.

Creating an 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.

You must create an LDAP search user account for the following use cases:

- 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

When registering an authorization group in Analyzer server by using the web client, 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 Analyzer server, you must register a user account used to search for LDAP user information on the Analyzer server.

Assign the LDAP search user account, the necessary permissions so that the account can access all entries under the BaseDN to be referenced on the Analyzer server, and all attributes specified for those entries.

For details about how to create user accounts on an LDAP directory server, see the documentation of the LDAP directory server.

Connecting to the LDAP directory server

To connect to the LDAP directory server, you must perform the following operations on the Analyzer server.

Before you begin

- You must have Administrator permission (Windows) or root permission (Linux) .
- You must create two LDAP user accounts on LDAP directory server:
 - An LDAP user account for accessing the Analyzer server
 - An LDAP search user account for querying the LDAP directory server

If no external authorization servers are used, and if a flat model data structure is used, you do not need to create an LDAP search user account.
- Check the following information. This information is necessary for editing the file `exauth.properties`.
 - Method for connecting to the LDAP directory server

The properties to be specified depend on whether information about the LDAP directory server is to be directly specified, or whether information about the connection-destination LDAP directory server is to be obtained from the DNS server.
 - Data structures of the LDAP directory servers

Settings for properties depend on whether the hierarchical structure model or the flat model is used.
 - Machine information about the LDAP directory server (Host name or IP address, Port number)
 - BaseDN
 - Domain name for external authorization servers managed by the LDAP directory server (when connecting to an external authorization server)
 - Domain name for multi-domain configurations managed by the LDAP directory server (for a multi-domain configuration)

Procedure

1. Edit the `exauth.properties` file.
 - a. Make a copy of the `exauth.properties` file template, which is stored in the following location, and place the copy in another folder or directory.

In Windows

```
Common-component-installation-destination-folder\sample\conf\exauth.properties
```

In Linux

```
Common-component-installation-destination-directory/sample/conf/exauth.properties
```
 - b. In the copy of the `exauth.properties` file, specify the required information.

- c. Save the `exauth.properties` file in the following location:

In Windows

`Common-component-installation-destination-folder\conf`

In Linux

`Common-component-installation-destination-directory/conf`

- d. If the values of the property `auth.ocsp.enable` or the property `auth.ocsp.responderURL` have been changed, restart the Analyzer server service.

2. Register, to the Analyzer server, an LDAP search user account that was created on the LDAP directory server.

Skip this step if no external authorization servers are used and if the data structure of the LDAP directory servers is a flat model.

- a. Run the **hcnds64ldapuser** command to register the LDAP search user account.

In Windows

```
Common-component-installation-destination-folder\bin
\hcnds64ldapuser /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

```
Common-component-installation-destination-directory/bin/
hcnds64ldapuser -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
```

- b. To view a list of LDAP directory servers for which LDAP search user accounts are registered, run the following command.

In Windows

```
Common-component-installation-destination-folder\bin
\hcnds64ldapuser /list
```

In Linux

```
Common-component-installation-destination-directory/bin/
hcnds64ldapuser -list
```



Tip:

To delete the LDAP search user account from the Analyzer server, run the **hcnds64ldapuser** command with the `delete` option.

3. Run the **hcnds64checkauth** command to confirm whether connections to the external authentication server and the external authorization server can be established properly.

In Windows

```
Common-component-installation-destination-folder\bin\hcnds64checkauth
[/user user-ID] [/pass password] [/summary]
```

In Linux

```
Common-component-installation-destination-directory/bin/
hcnds64checkauth [-user user-ID] [-pass password] [-summary]
```

4. On the web client, specify the following settings.
 - When an LDAP directory server is configured for external user authentication:
 - Create an user account.
Make sure that the user ID is the same as the user ID that was created on the external authentication server.
 - Change the user authentication method.
 - Specify the operation permissions for the user.
 - When an LDAP directory server is configured for external user authentication and authorization:
 - Register an authorization group.
 - Specify the operation permissions for the authorization group.

For details about how to perform these operations on the web client, see the *Hitachi Ops Center Analyzer User Guide*.



Note:

If you are using both an external authentication server and an external authorization server, and the user ID created on the external authentication server is registered on the Analyzer server, the user account is authenticated internally by the Analyzer server.

If the current configuration uses only an external authentication server and you want to use both an external authentication server and an external authorization server, you must remove the user ID that was created with the same name on the Analyzer server.

LDAP configuration properties

In the `exauth.properties` file, set the type of the external authentication server to use the server identification name, and the machine information about the external authentication server.

Items to be configured in the `exauth.properties` file differ depending on the LDAP directory server environment. Use the following table to check the configuration items corresponding to your LDAP directory server environment.

External authorization server used	Server connection method	Reference
No	Directly specify information about the LDAP directory server.	Settings for connecting directly to an LDAP directory server (on page 242)
	Obtain LDAP directory server information from the DNS server.	Settings for using DNS to connect to an LDAP directory server (on page 248)
Yes	Directly specify information about the LDAP directory server.	Settings for connecting directly to an LDAP directory server and an authorization server (on page 250)
	Obtain LDAP directory server information from the DNS server.	Settings for using DNS to connect to an LDAP directory server and an authorization server (on page 256)



Note:

- Be sure to distinguish between uppercase and lowercase letters for property settings.
- To use StartTLS for communication between the Analyzer server and the LDAP directory server, you must directly specify information about the LDAP directory server in the `exauth.properties` file.
- If you use a DNS server to look up the LDAP directory server to connect to, it might take longer for users to log on.
- If the LDAP directory server to which you want to connect is in a multi-domain configuration, you will not be able to look up the LDAP directory server by using the DNS server.

Settings for connecting directly to an LDAP directory server

To use an LDAP directory server as an external authorization server by directly specifying the LDAP directory information in the `exauth.properties` file, specify the settings in the `exauth.properties` file as shown in the following table.

Property names	Details
<code>auth.server.type</code>	Specify an external authentication server type. Specify <code>ldap</code> . Default value: <code>internal</code> (do not connect to an external authentication server)
<code>auth.server.name</code>	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 are applied to. <code>ServerName</code> has been set as the initial value. You must specify at least one name. To specify multiple server identification names, delimit the server identification names by using commas (,). Do not register the same server identification name more than once. Specifiable values: No more than 64 bytes of the following characters: A to Z a to z 0 to 9 ! # () + - . = @ [] ^ _ { } ~ Default value: none
<code>auth.ldap.multi_domain</code>	When specifying multiple server identification names for LDAP directory servers, specify the configuration to use for each server. Specify <code>true</code> to use a multi-domain configuration. Specify <code>false</code> to use a redundant configuration. Default value: <code>false</code>
<code>auth.ldap.default_domain</code>	Specify settings for the Active Directory global catalog. Specify the domain name of the default server configuration to use for authentication when no domain name is specified in the logon ID. If you specify multiple servers in <code>auth.server.name</code> , a multi-domain configuration will be used, and a redundant configuration will not be used. Default value: none
<code>auth.group.mapping</code>	Specify whether to also connect to an external authorization server (LDAP directory server). Specify <code>false</code> (do not connect). Default value: <code>false</code> (do not connect)

Property names	Details
<code>auth.ocsp.enable</code>	<p>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.</p> <p>If you want to verify the validity of certificates, specify <code>true</code>. To not verify the validity of certificates, specify <code>false</code>.</p> <p>Default value: <code>false</code></p>
<code>auth.ocsp.responderURL</code>	<p>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.</p> <p>Default value: none</p>
<code>auth.ldap.auth.server.name-property-value.protocol</code>	<p>Specify the protocol for connecting to the LDAP directory server. This attribute is required.</p> <p>When communicating in plain text format, specify <code>ldap</code>. When using StartTLS communication, specify <code>tls</code>.</p> <p>Before specifying <code>tls</code>, you must specify the security settings of Common component. In addition, make sure that one of the following encryption methods can be used on the LDAP directory server.</p> <ul style="list-style-type: none"> ▪ <code>TLS_RSA_WITH_AES_256_GCM_SHA384</code> ▪ <code>TLS_RSA_WITH_AES_256_CBC_SHA256</code> ▪ <code>TLS_RSA_WITH_AES_256_CBC_SHA</code> ▪ <code>TLS_RSA_WITH_AES_128_CBC_SHA256</code> ▪ <code>TLS_RSA_WITH_AES_128_CBC_SHA</code> <p>Specifiable values: <code>ldap</code> or <code>tls</code></p> <p>Default value: none</p>
<code>auth.ldap.auth.server.name-property-value.host</code>	<p>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 (<code>[]</code>). This attribute is required.</p>

Property names	Details
	<p>To use a redundant configuration when the global catalog is enabled (<code>auth.ldap.default_domain</code> is specified), specify multiple host names or IP addresses, delimited by commas.</p> <p>When using StartTLS as the protocol for connecting to the LDAP directory server, in the <code>host</code> attribute specify the same host name as the value of CN in the LDAP directory server certificate. You cannot use an IP address.</p> <p>Default value: none</p>
<code>auth.ldap.auth.server.name-property-value.port</code>	<p>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. To use a redundant configuration when the global catalog is enabled (<code>auth.ldap.default_domain</code> is specified), specify multiple port numbers, delimited by commas. Make sure that the number of ports is the same as the number of host names or IP addresses specified in <code>host</code>.</p> <p>Specifiable values: 1 to 65535</p> <p>Default value: 389 (when the global catalog is disabled), 3268 (when the global catalog is enabled)</p>
<code>auth.ldap.auth.server.name-property-value.timeout</code>	<p>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.</p> <p>Specifiable values: 0 to 120 (seconds)</p> <p>Default value: 15</p>

Property names	Details
<code>auth.ldap.auth.server.name-property-value.attr</code>	<p>Specify the attribute (Attribute Type) to use as the user ID during authentication.</p> <ul style="list-style-type: none"> For the hierarchical structure model <p>Specify the name of the attribute containing the unique value to use for identifying the user. The value stored in this attribute will be used as the user ID for Analyzer server. The specified attribute must not include characters that cannot be used in a user ID of the Analyzer server.</p> <p>For example, if you are using Active Directory and you want to use the Windows logon ID for the user ID of an Analyzer server, specify the attribute name <code>sAMAccountName</code> in which the Windows logon ID has been defined.</p> For the flat model <p>Specify the RDN attribute name of the user entry.</p> <p>For example, if the user's DN is <code>uid=John,ou=People,dc=example,dc=com</code>, specify the <code>uid</code> that is the attribute name of the <code>uid=John</code>.</p> <p><code>sAMAccountName</code> has been set as the initial value. This attribute is required.</p> <p>Default value: none</p>
<code>auth.ldap.auth.server.name-property-value.basedn</code>	<p>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.</p> <ul style="list-style-type: none"> For the hierarchical structure model <p>Specify the DN of the hierarchy that includes all of the user entries to be searched.</p> For the flat model <p>Specify the DN of the hierarchy just above the user entries to be searched.</p>

Property names	Details
	<p>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 must use a backslash (\) to escape each character.</p> <p>Spaces # + ; , < = > \</p> <p>Default value: none</p>
<code>auth.ldap.auth.server.name-property-value.retry.interval</code>	<p>Specify the retry interval (in seconds) for when an attempt to connect to the LDAP directory server fails.</p> <p>Specifiable values: 1 to 60 (seconds)</p> <p>Default value: 1</p>
<code>auth.ldap.auth.server.name-property-value.retry.times</code>	<p>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.</p> <p>Specifiable values: 0 to 50</p> <p>Default value: 20</p>
<code>auth.ldap.auth.server.name-property-value.domain</code>	<p>Specify the name of a domain for multi-domain configurations managed by the LDAP directory server, or the domain name for the global catalog.</p> <p>If you log on by using a user ID that includes the domain name specified in this attribute, the LDAP directory server that belongs to the specified domain will be used as the authentication server.</p> <p>When specifying a domain name for the server identification name of each LDAP directory server, do not specify the same domain name more than once. This value is not case sensitive.</p> <p>If the global catalog is enabled, be sure to specify the domain name that is specified in <code>auth.ldap.default_domain</code> as the default server configuration to use for authentication.</p> <p>This attribute is required when a multi-domain configuration is used.</p> <p>Default value: none</p>
<code>auth.ldap.auth.server.name-property-value.dns_lookup</code>	<p>Specify whether to use the DNS server to look up the information about the LDAP directory server. Specify <code>false</code> (do not look up the information).</p> <p>Default value: <code>false</code> (do not look up the information)</p>

Settings for using DNS to connect to an LDAP directory server

To use an LDAP directory server as an external authorization server by obtaining the LDAP directory information from the DNS server, specify the settings in the `exauth.properties` file as shown in the following table.

Property names	Details
<code>auth.server.type</code>	Specify an external authentication server type. Specify <code>ldap</code> . Default value: <code>internal</code> (do not connect to an external authentication server)
<code>auth.server.name</code>	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 are applied to. <code>ServerName</code> has been set as the initial value. This attribute is required. Specifiable values: No more than 64 bytes of the following characters: A to Z a to z 0 to 9 ! # () + - . = @ [] ^ _ { } ~ Default value: none
<code>auth.group.mapping</code>	Specify whether to also connect to an external authorization server (LDAP directory server). Specify <code>false</code> (do not connect). Default value: <code>false</code> (do not connect)
<code>auth.ldap.auth.server.name-property-value.protocol</code>	Specify the protocol for connecting to the LDAP directory server. This attribute is required. Specifiable values: <code>ldap</code> Default value: none
<code>auth.ldap.auth.server.name-property-value.timeout</code>	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

Property names	Details
<code>auth.ldap.auth.server.name-property-value.attr</code>	<p>Specify the attribute (Attribute Type) to use as the user ID during authentication.</p> <ul style="list-style-type: none"> For the hierarchical structure model <p>Specify the name of the attribute containing the unique value to use for identifying the user. The value stored in this attribute will be used as the user ID for Analyzer server. The specified attribute must not include characters that cannot be used in a user ID of the Analyzer server.</p> <p>For example, if you are using Active Directory and you want to use the Windows logon ID for the user ID of an Analyzer server, specify the attribute name <code>sAMAccountName</code> in which the Windows logon ID has been defined.</p> For the flat model <p>Specify the RDN attribute name of the user entry.</p> <p>For example, if the user's DN is <code>uid=John,ou=People,dc=example,dc=com</code>, specify the <code>uid</code> that is the attribute name of the <code>uid=John</code>.</p> <p><code>sAMAccountName</code> has been set as the initial value. This attribute is required.</p> <p>Default value: none</p>
<code>auth.ldap.auth.server.name-property-value.basedn</code>	<p>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.</p> <ul style="list-style-type: none"> For the hierarchical structure model <p>Specify the DN of the hierarchy that includes all of the user entries to be searched.</p> For the flat model <p>Specify the DN of the hierarchy just above the user entries to be searched.</p>

Property names	Details
	<p>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 must use a backslash (\) to escape each character.</p> <p>Spaces # + ; , < = > \</p> <p>Default value: none</p>
<code>auth.ldap.auth.server.name-property-value.retry.interval</code>	<p>Specify the retry interval (in seconds) for when an attempt to connect to the LDAP directory server fails.</p> <p>Specifiable values: 1 to 60 (seconds)</p> <p>Default value: 1</p>
<code>auth.ldap.auth.server.name-property-value.retry.times</code>	<p>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.</p> <p>Specifiable values: 0 to 50</p> <p>Default value: 20</p>
<code>auth.ldap.auth.server.name-property-value.domain.name</code>	<p>Specify the name of a domain managed by the LDAP directory server. This attribute is required.</p> <p>Default value: none</p>
<code>auth.ldap.auth.server.name-property-value.dns_lookup</code>	<p>Specify whether to use the DNS server to look up the information about the LDAP directory server. Specify <code>true</code> (look up the information).</p> <p>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.</p> <ul style="list-style-type: none"> <code>auth.ldap.auth.server.name-property-value.host</code> <code>auth.ldap.auth.server.name-property-value.port</code> <p>Default value: <code>false</code> (do not look up the information)</p>

Settings for connecting directly to an LDAP directory server and an authorization server

To use an LDAP directory server as both an external authentication server and an external authorization server by directly specifying the LDAP directory information in the `exauth.properties` file, specify the settings in the `exauth.properties` file as shown in the following table.

Property names	Details
<code>auth.server.type</code>	Specify an external authentication server type. Specify <code>ldap</code> . Default value: <code>internal</code> (do not connect to an external authentication server)
<code>auth.server.name</code>	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 are applied to. <code>ServerName</code> has been set as the initial value. You must specify at least one name. To specify multiple server identification names, delimit the server identification names by using commas (,). Do not register the same server identification name more than once. Specifiable values: No more than 64 bytes of the following characters: A to Z a to z 0 to 9 ! # () + - . = @ [] ^ _ { } ~ Default value: none
<code>auth.ldap.multi_domain</code>	When specifying multiple server identification names for LDAP directory servers, specify the configuration to use for each server. Specify <code>true</code> to use a multi-domain configuration. Specify <code>false</code> to use a redundant configuration. Default value: <code>false</code>
<code>auth.ldap.default_domain</code>	Specify settings for the Active Directory global catalog. Specify the domain name of the default server configuration to use for authentication when no domain name is specified in the logon ID. If you specify multiple servers in <code>auth.server.name</code> , a multi-domain configuration will be used, and a redundant configuration will not be used. Default value: none
<code>auth.group.mapping</code>	Specify whether to also connect to an external authorization server (LDAP directory server). Specify <code>true</code> (connect). Default value: <code>false</code> (do not connect)

Property names	Details
<code>auth.ocsp.enable</code>	<p>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.</p> <p>If you want to verify the validity of certificates, specify <code>true</code>. To not verify the validity of certificates, specify <code>false</code>.</p> <p>Default value: <code>false</code></p>
<code>auth.ocsp.responderURL</code>	<p>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.</p> <p>Default value: none</p>
<code>auth.ldap.auth.server.name-property-value.protocol</code>	<p>Specify the protocol for connecting to the LDAP directory server. This attribute is required.</p> <p>When communicating in plain text format, specify <code>ldap</code>. When using StartTLS communication, specify <code>tls</code>.</p> <p>Before specifying <code>tls</code>, you must specify the security settings of Common component. In addition, make sure that one of the following encryption methods can be used on the LDAP directory server.</p> <ul style="list-style-type: none"> ▪ <code>TLS_RSA_WITH_AES_256_GCM_SHA384</code> ▪ <code>TLS_RSA_WITH_AES_256_CBC_SHA256</code> ▪ <code>TLS_RSA_WITH_AES_256_CBC_SHA</code> ▪ <code>TLS_RSA_WITH_AES_128_CBC_SHA256</code> ▪ <code>TLS_RSA_WITH_AES_128_CBC_SHA</code> <p>Specifiable values: <code>ldap</code> or <code>tls</code></p> <p>Default value: none</p>
<code>auth.ldap.auth.server.name-property-value.host</code>	<p>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 (<code>[]</code>). This attribute is required.</p>

Property names	Details
	<p>To use a redundant configuration when the global catalog is enabled (<code>auth.ldap.default_domain</code> is specified), specify multiple host names or IP addresses, delimited by commas.</p> <p>When using StartTLS as the protocol for connecting to the LDAP directory server, in the <code>host</code> attribute specify the same host name as the value of CN in the LDAP directory server certificate. You cannot use an IP address.</p> <p>Default value: none</p>
<code>auth.ldap.auth.server.name-property-value.port</code>	<p>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. To use a redundant configuration when the global catalog is enabled (<code>auth.ldap.default_domain</code> is specified), specify multiple port numbers, delimited by commas. Make sure that the number of ports is the same as the number of host names or IP addresses specified in <code>host</code>.</p> <p>Specifiable values: 1 to 65535</p> <p>Default value: 389 (when the global catalog is disabled), 3268 (when the global catalog is enabled)</p>
<code>auth.ldap.auth.server.name-property-value.timeout</code>	<p>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.</p> <p>Specifiable values: 0 to 120 (seconds)</p> <p>Default value: 15</p>

Property names	Details
<code>auth.ldap.auth.server.name-property-value.attr</code>	<p>Specify the attribute (Attribute Type) to use as the user ID during authentication.</p> <ul style="list-style-type: none"> For the hierarchical structure model <p>Specify the name of the attribute containing the unique value to use for identifying the user. The value stored in this attribute will be used as the user ID for Analyzer server. The specified attribute must not include characters that cannot be used in a user ID of the Analyzer server.</p> <p>For example, if you are using Active Directory and you want to use the Windows logon ID for the user ID of an Analyzer server, specify the attribute name <code>sAMAccountName</code> in which the Windows logon ID has been defined.</p> For the flat model <p>Specify the RDN attribute name of the user entry.</p> <p>For example, if the user's DN is <code>uid=John,ou=People,dc=example,dc=com</code>, specify the <code>uid</code> that is the attribute name of the <code>uid=John</code>.</p> <p><code>sAMAccountName</code> has been set as the initial value. This attribute is required.</p> <p>Default value: none</p>
<code>auth.ldap.auth.server.name-property-value.basedn</code>	<p>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.</p> <ul style="list-style-type: none"> For the hierarchical structure model <p>Specify the DN of the hierarchy that includes all of the user entries to be searched.</p> For the flat model <p>Specify the DN of the hierarchy just above the user entries to be searched.</p>

Property names	Details
	<p>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 must use a backslash (\) to escape each character.</p> <p>Spaces # + ; , < = > \</p> <p>Default value: none</p>
<code>auth.ldap.auth.server.name-property-value.retry.interval</code>	<p>Specify the retry interval (in seconds) for when an attempt to connect to the LDAP directory server fails.</p> <p>Specifiable values: 1 to 60 (seconds)</p> <p>Default value: 1</p>
<code>auth.ldap.auth.server.name-property-value.retry.times</code>	<p>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.</p> <p>Specifiable values: 0 to 50</p> <p>Default value: 20</p>
<code>auth.ldap.auth.server.name-property-value.domain.name</code>	<p>Specify the name of a domain managed by the LDAP directory server. This attribute is required.</p> <p>Default value: none</p>
<code>auth.ldap.auth.server.name-property-value.domain</code>	<p>Specify the name of a domain for multi-domain configurations managed by the LDAP directory server, or the domain name for the global catalog.</p> <p>If you log on by using a user ID that includes the domain name specified in this attribute, the LDAP directory server that belongs to the specified domain will be used as the authentication server.</p> <p>When specifying a domain name for the server identification name of each LDAP directory server, do not specify the same domain name more than once. This value is not case sensitive.</p> <p>If the global catalog is enabled, be sure to specify the domain name that is specified in <code>auth.ldap.default_domain</code> as the default server configuration to use for authentication.</p> <p>This attribute is required when a multi-domain configuration is used.</p> <p>Default value: none</p>

Property names	Details
<code>auth.ldap.auth.server.name-property-value.dns_lookup</code>	Specify whether to use the DNS server to look up the information about the LDAP directory server. Specify <i>false</i> (do not look up the information). Default value: <i>false</i> (do not look up the information)

Settings for using DNS to connect to an LDAP directory server and an authorization server

To use an LDAP directory server as both an external authentication server and an external authorization server by obtaining the LDAP directory information from the DNS server, specify the settings in the `exauth.properties` file as shown in the following table.

Property names	Details
<code>auth.server.type</code>	Specify an external authentication server type. Specify <i>ldap</i> . Default value: <i>internal</i> (do not connect to an external authentication server)
<code>auth.server.name</code>	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 are applied to. <i>ServerName</i> has been set as the initial value. This attribute is required. Specifiable values: No more than 64 bytes of the following characters: A to Z a to z 0 to 9 ! # () + - . = @ [] ^ _ { } ~ Default value: none
<code>auth.group.mapping</code>	Specify whether to also connect to an external authorization server (LDAP directory server). Specify <i>true</i> (connect). Default value: <i>false</i> (do not connect)
<code>auth.ldap.auth.server.name-property-value.protocol</code>	Specify the protocol for connecting to the LDAP directory server. This attribute is required. Specifiable values: <i>ldap</i>

Property names	Details
	Default value: none
<code>auth.ldap.auth.server.name-property-value.timeout</code>	<p>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.</p> <p>Specifiable values: 0 to 120 (seconds)</p> <p>Default value: 15</p>
<code>auth.ldap.auth.server.name-property-value.attr</code>	<p>Specify the attribute (Attribute Type) to use as the user ID during authentication.</p> <ul style="list-style-type: none"> For the hierarchical structure model <p>Specify the name of the attribute containing the unique value to use for identifying the user. The value stored in this attribute will be used as the user ID for Analyzer server. The specified attribute must not include characters that cannot be used in a user ID of the Analyzer server.</p> <p>For example, if you are using Active Directory and you want to use the Windows logon ID for the user ID of an Analyzer server, specify the attribute name <code>sAMAccountName</code> in which the Windows logon ID has been defined.</p> For the flat model <p>Specify the RDN attribute name of the user entry.</p> <p>For example, if the user's DN is <code>uid=John,ou=People,dc=example,dc=com</code>, specify the <code>uid</code> that is the attribute name of the <code>uid=John</code>.</p> <p><code>sAMAccountName</code> has been set as the initial value. This attribute is required.</p> <p>Default value: none</p>

Property names	Details
<code>auth.ldap.auth.server.name-property-value.basedn</code>	<p>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.</p> <ul style="list-style-type: none"> 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. <p>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 must use a backslash (\) to escape each character.</p> <p>Spaces # + ; , < = > \</p> <p>Default value: none</p>
<code>auth.ldap.auth.server.name-property-value.retry.interval</code>	<p>Specify the retry interval (in seconds) for when an attempt to connect to the LDAP directory server fails.</p> <p>Specifiable values: 1 to 60 (seconds)</p> <p>Default value: 1</p>
<code>auth.ldap.auth.server.name-property-value.retry.times</code>	<p>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.</p> <p>Specifiable values: 0 to 50</p> <p>Default value: 20</p>
<code>auth.ldap.auth.server.name-property-value.domain.name</code>	<p>Specify the name of a domain managed by the LDAP directory server. This attribute is required.</p> <p>Default value: none</p>
<code>auth.ldap.auth.server.name-property-value.dns_lookup</code>	<p>Specify whether to use the DNS server to look up the information about the LDAP directory server. Specify <code>true</code> (look up the information).</p>

Property names	Details
	<p>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.</p> <ul style="list-style-type: none">▪ <code>auth.ldap.auth.server.name-property-value.host</code>▪ <code>auth.ldap.auth.server.name-property-value.port</code> <p>Default value: <code>false</code> (do not look up the information)</p>

Examples of specifying settings in the exauth.properties file to use an LDAP directory server for 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 connecting 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 connecting 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 connecting 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 connecting to an authorization server):

```
auth.server.type=ldap
auth.server.name=ServerName
auth.group.mapping=true
auth.ldap.ServerName.protocol=ldap
auth.ldap.ServerName.timeout=15
auth.ldap.ServerName.attr=sAMAccountName
auth.ldap.ServerName.basedn=dc=Example,dc=com
auth.ldap.ServerName.retry.interval=1
auth.ldap.ServerName.retry.times=20
auth.ldap.ServerName.domain.name=EXAMPLE.COM
auth.ldap.ServerName.dns_lookup=true
```

- When using a redundant configuration:

```
auth.server.type=ldap
auth.server.name=ServerName1,ServerName2
auth.ldap.multi_domain=false
auth.group.mapping=false
auth.ldap.ServerName1.protocol=ldap
auth.ldap.ServerName1.host=ldap1.example.com
auth.ldap.ServerName1.port=389
auth.ldap.ServerName1.timeout=15
auth.ldap.ServerName1.attr=sAMAccountName
auth.ldap.ServerName1.basedn=dc=Example,dc=com
auth.ldap.ServerName1.retry.interval=1
auth.ldap.ServerName1.retry.times=20
auth.ldap.ServerName2.protocol=ldap
auth.ldap.ServerName2.host=ldap2.example.com
auth.ldap.ServerName2.port=389
auth.ldap.ServerName2.timeout=15
auth.ldap.ServerName2.attr=sAMAccountName
auth.ldap.ServerName2.basedn=dc=Example,dc=net
auth.ldap.ServerName2.retry.interval=1
auth.ldap.ServerName2.retry.times=20
```

- When using a multi-domain configuration:

```
auth.server.type=ldap
auth.server.name=ServerName1,ServerName2
auth.ldap.multi_domain=true
auth.group.mapping=false
auth.ldap.ServerName1.protocol=ldap
auth.ldap.ServerName1.host=ldap1.example.com
auth.ldap.ServerName1.port=389
auth.ldap.ServerName1.timeout=15
auth.ldap.ServerName1.attr=sAMAccountName
auth.ldap.ServerName1.basedn=dc=Example,dc=com
auth.ldap.ServerName1.retry.interval=1
auth.ldap.ServerName1.retry.times=20
auth.ldap.ServerName1.domain=example.com
auth.ldap.ServerName2.protocol=ldap
auth.ldap.ServerName2.host=ldap2.example.com
auth.ldap.ServerName2.port=389
auth.ldap.ServerName2.timeout=15
auth.ldap.ServerName2.attr=sAMAccountName
auth.ldap.ServerName2.basedn=dc=Example,dc=net
auth.ldap.ServerName2.retry.interval=1
auth.ldap.ServerName2.retry.times=20
auth.ldap.ServerName2.domain=example.net
```

- When the global catalog is enabled:

```
auth.server.type=ldap
auth.server.name=ServerName1,ServerName2
auth.ldap.default_domain=example.com
auth.ldap.ServerName1.protocol=ldap
auth.ldap.ServerName1.host=ldap.example1.com,ldap.example2.com
auth.ldap.ServerName1.port=3268,3268
auth.ldap.ServerName1.timeout=15
auth.ldap.ServerName1.attr=sAMAccountName
auth.ldap.ServerName1.basedn=dc=Example,dc=com
auth.ldap.ServerName1.retry.interval=1
auth.ldap.ServerName1.retry.times=20
auth.ldap.ServerName1.domain=example.com
auth.ldap.ServerName2.protocol=ldap
auth.ldap.ServerName2.host=ldap.example1.com,ldap.example2.com
auth.ldap.ServerName2.port=3268,3268
auth.ldap.ServerName2.timeout=15
auth.ldap.ServerName2.attr=sAMAccountName
auth.ldap.ServerName2.basedn=dc=Example,dc=net
auth.ldap.ServerName2.retry.interval=1
auth.ldap.ServerName2.retry.times=20
auth.ldap.ServerName2.domain=example.net
```

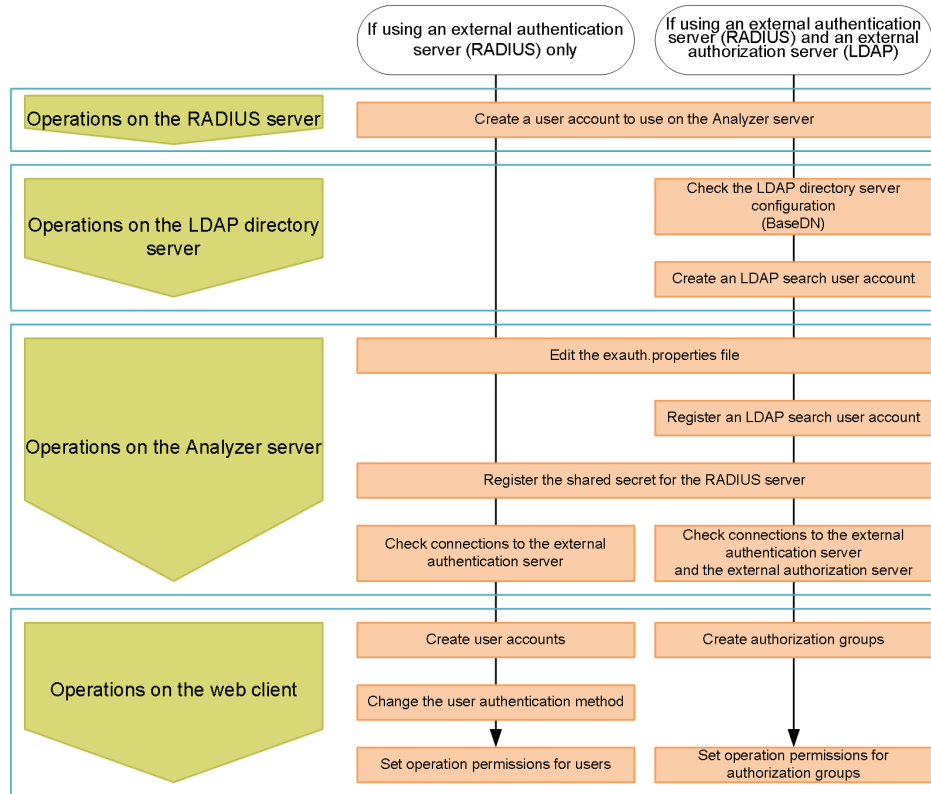
Configuring RADIUS authentication for Analyzer server

To use RADIUS authentication for the Analyzer server, you must configure the following settings.

Workflow for configuring RADIUS authentication

The workflow for connecting to the RADIUS server varies depending on whether only an external authentication server is used or both an external authentication server and an external authorization server (LDAP directory server) are used.

The following figure shows the workflow for connecting to the RADIUS server.



Note: To use StartTLS to communicate between the LDAP directory server and the Analyzer server, you must set up an environment specifically for this purpose to ensure secure communications.

Configuring the RADIUS server

On the RADIUS server, create a user account for the Analyzer server. To use an external authorization server (LDAP directory server), check the configuration details of the LDAP directory server, and then create an LDAP search user account.

Creating user accounts on the RADIUS server

On the RADIUS server, you must create user accounts (user IDs and passwords) to use on the Analyzer server.

For details about how to create user accounts on the RADIUS server, see the documentation of the RADIUS server.

User IDs and passwords must satisfy the following conditions:

- They are within 256 bytes.
- They use no characters other than the following:

A to Z

a to z

0 to 9

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

In Analyzer server, user IDs are not case-sensitive. The combination of character types for passwords must follow the settings in the external authentication server.

Configuring LDAP directory server as external authorization server

To use the LDAP directory server as an external authorization server, you must configure the LDAP directory server.

For details about how to configure the LDAP directory server, see the following descriptions:

- [Checking the LDAP directory server settings \(on page 235\)](#)

Check the BaseDN for the LDAP directory server. You will need the BaseDN information when you edit the `exauth.properties` file of the Analyzer server.

- [Creating an LDAP search user account \(on page 237\)](#)

On the LDAP directory server, create an LDAP search user account. This user account is necessary when the Analyzer server connects to the LDAP directory server to acquire user information and other information.

Connecting to the RADIUS server

To connect to the RADIUS server, you must perform the following operations on the Analyzer server.

Before you begin

- You must have Administrator permission (Windows) or root permission (Linux).
- On the RADIUS server, create a user account to use on the Analyzer server.
- Check the following information. This information is necessary for editing the file `exauth.properties`.
 - Machine information about the RADIUS server (Host name or IP address, Port number)
 - Authentication protocol for the RADIUS server
 - Host name or IP address of the Analyzer server

If you also want to connect to an external authorization server (an LDAP directory server), check the following requirements.

- Create a user account on the LDAP directory server for searching for user information.
- Check the following information. This information is necessary for editing the file `exauth.properties`.
 - Method for connecting to the LDAP directory server

The properties to be specified depend on whether information about the LDAP directory server is to be directly specified, or whether information about the connection-destination LDAP directory server is to be obtained from the DNS server.

 - Machine information about the LDAP directory server (Host name or IP address, Port number)
 - BaseDN
 - Domain name for external authorization servers managed by the LDAP directory server

Procedure

1. Edit the `exauth.properties` file.
 - a. Make a copy of the `exauth.properties` file template, which is stored in the following location, and place the copy in another folder or directory.

In Windows

Common-component-installation-destination-folder\sample\conf\exauth.properties

In Linux

Common-component-installation-destination-directory/sample/conf/exauth.properties

- b. In the copy of the `exauth.properties` file, specify the required information.

- c. Save the `exauth.properties` file in the following location:

In Windows

Common-component-installation-destination-folder\conf

In Linux

Common-component-installation-destination-directory/conf

- d. If the values of the property `auth.ocsp.enable` or the property `auth.ocsp.responderURL` have been changed, restart the Analyzer server service.

2. If a connection also needs to be established with an external authorization server (an LDAP directory server), register on the Analyzer server a user account to use for retrieving user information.

- a. Run the **hcnds64ldapuser** command to register the LDAP search user account.

In Windows

```
Common-component-installation-destination-folder\bin
\hcnds64ldapuser /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

```
Common-component-installation-destination-directory/bin/
hcnds64ldapuser -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
```

- b. To view a list of LDAP directory servers for which LDAP search user accounts are registered, run the following command.

In Windows

```
Common-component-installation-destination-folder\bin
\hcnds64ldapuser /list
```

In Linux

```
Common-component-installation-destination-directory/bin/
hcnds64ldapuser -list
```



Tip:

To delete the LDAP search user account from the Analyzer server, run the **hcnds64ldapuser** command with the `delete` option.

3. Register to the Analyzer server a shared secret for communicating with the RADIUS server.

- a. Use the **hcnds64radiussecret** command to register the shared secret of the RADIUS server.

In Windows

```
Common-component-installation-destination-folder\bin
\hcnds64radiussecret [/set shared-secret] /name RADIUS-server-
identification-name
```

In Linux

```
Common-component-installation-destination-directory/bin/
hcnds64radiussecret [-set shared-secret] -name RADIUS-server-
identification-name
```

- b. You can use one of the following commands to list RADIUS servers for which shared secrets are registered:

In Windows

```
Common-component-installation-destination-folder\bin
\hcnds64radiussecret /list
```

In Linux

```
Common-component-installation-destination-directory/bin/
hcnds64radiussecret -list
```



Tip:

To delete shared secrets that have been registered to the Analyzer server, execute the **hcnds64radiussecret** command with the `delete` option specified.

4. Run the **hcnds64checkauth** command to confirm whether connections to the external authentication server and the external authorization server can be established properly.

In Windows

```
Common-component-installation-destination-folder\bin\hcnds64checkauth
[/user user-ID] [/pass password] [/summary]
```

In Linux

```
Common-component-installation-destination-directory/bin/
hcnds64checkauth [-user user-ID] [-pass password] [-summary]
```

5. On the web client, specify the following settings.
 - When a RADIUS server is configured for external user authentication:
 - Create an user account.
Make sure that the user ID is the same as the user ID that was created on the external authentication server.
 - Change the user authentication method.
 - Specify the operation permissions for the user.
 - When a RADIUS server is configured for external user authentication and an LDAP directory server is configured for authorization:
 - Register an authorization group.
 - Specify the operation permissions for the authorization group.

For details about how to perform these operations on the web client, see the *Hitachi Ops Center Analyzer User Guide*.



Note:

If you are using both an external authentication server and an external authorization server, and the user ID created on the external authentication server is registered on the Analyzer server, the user account is authenticated internally by the Analyzer server.

If the current configuration uses only an external authentication server and you want to use both an external authentication server and an external authorization server, you must remove the user ID that was created with the same name on the Analyzer server.

RADIUS configuration properties

In the `exauth.properties` file, set the type of the external authentication server to use, the server identification name, and the machine information about the external authentication server.

Items to be configured in the `exauth.properties` file differ depending on the RADIUS server environment. Use the following table to check the configuration items corresponding to your RADIUS server environment.

External authorization server used	Server connection method	Reference
No	Directly specify information about the RADIUS server.	Settings for connecting directly to a RADIUS server (on page 270)

External authorization server used	Server connection method	Reference
Yes	Directly specify information about the external authorization server (the LDAP directory server).	Settings for connecting directly to a RADIUS server and an authorization server (on page 273)
	Obtain external authorization server (LDAP directory server) information from the DNS server.	Settings for using DNS to connect to a RADIUS server and an authorization server (on page 278)

**Note:**

- Be sure to distinguish between uppercase and lowercase letters for property settings.
- To use StartTLS for communication between the Analyzer server and the LDAP directory server, you must directly specify information about the LDAP directory server in the `exauth.properties` file.
- If you use a DNS server to look up the LDAP directory server to connect to, it might take longer for users to log on.

Settings for connecting directly to a RADIUS server

To use a RADIUS server as an external authentication server, specify the settings in the `exauth.properties` file as shown in the following table.

Property names	Details
<code>auth.server.type</code>	Specify an external authentication server type. Specify <code>radius</code> . Default value: <code>internal</code> (do not connect to an external authentication server)
<code>auth.server.name</code>	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 are applied to. <code>ServerName</code> has been set as the initial value. You must specify at least one name. When configuring a redundant configuration, separate the server identification name of each server with a comma (,). Do not register the same server identification name more than once.

Property names	Details
	<p>Specifiable values: No more than 64 bytes of the following characters:</p> <p>A to Z</p> <p>a to z</p> <p>0 to 9</p> <p>! # () + - . = @ [] ^ _ { } ~</p> <p>Default value: none</p>
<code>auth.group.mapping</code>	<p>Specify whether to also connect to an external authorization server (LDAP directory server). Specify <code>false</code> (do not connect).</p> <p>Default value: <code>false</code> (do not connect)</p>
<code>auth.radius.auth.server.name-property-value.protocol</code>	<p>Specify the protocol for RADIUS server authentication. This attribute is required.</p> <p>Specifiable values: PAP or CHAP</p> <p>Default value: none</p>
<code>auth.radius.auth.server.name-property-value.host</code>	<p>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. To specify an IPv6 address, enclose it in square brackets ([]). This attribute is required.</p> <p>To connect to an external authorization server (LDAP directory server) that is running on the same computer and to use StartTLS as the protocol for connecting to the LDAP directory server, in the <code>host</code> attribute, specify the same host name as the value of CN in the LDAP directory server certificate. You cannot use an IP address.</p> <p>Default value: none</p>
<code>auth.radius.auth.server.name-property-value.port</code>	<p>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.</p> <p>Specifiable values: 1 to 65535</p> <p>Default value: 1812</p>
<code>auth.radius.auth.server.name-property-value.timeout</code>	<p>Specify the amount of time to wait before timing out when connecting to the RADIUS server.</p> <p>Specifiable values: 1 to 65535 (seconds)</p> <p>Default value: 1</p>

Property names	Details
<code>auth.radius.auth.server.name-property-value.retry.times</code>	<p>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.</p> <p>Specifiable values: 0 to 50</p> <p>Default value: 3</p>
<code>auth.radius.auth.server.name-property-value.attr.NAS-IP-Address</code>	<p>Specify the IPv4 address of the Analyzer server. The RADIUS server uses this attribute value to identify the Analyzer server.</p> <p>If the format of the address is invalid, this property is disabled.</p> <p>You must specify exactly one of the following: <code>attr.NAS-IP-Address</code>, <code>attr.NAS-IPv6-Address</code>, or <code>attr.NAS-Identifier</code>.</p> <p>Default value: none</p>
<code>auth.radius.auth.server.name-property-value.attr.NAS-IPv6-Address</code>	<p>Specify the IPv6 address of the Analyzer server. The RADIUS server uses this attribute value to identify the Analyzer server. Enclose the IPv6 address in square brackets ([]).</p> <p>If the format of the address is invalid, this property is disabled.</p> <p>You must specify exactly one of the following: <code>attr.NAS-IP-Address</code>, <code>attr.NAS-IPv6-Address</code>, or <code>attr.NAS-Identifier</code>.</p> <p>Default value: none</p>
<code>auth.radius.auth.server.name-property-value.attr.NAS-Identifier</code>	<p>Specify the host name of the Analyzer server. The RADIUS server uses this attribute value to identify the Analyzer server. The host name of the Analyzer server has been set as the initial value.</p> <p>You must specify exactly one of the following: <code>attr.NAS-IP-Address</code>, <code>attr.NAS-IPv6-Address</code>, or <code>attr.NAS-Identifier</code>.</p> <p>Specifiable values: Specify no more than 253 bytes of the following characters:</p> <p>A to Z</p> <p>a to z</p> <p>0 to 9</p> <p>! " # \$ % & ' () * + , - . / : ; < = > ? @ [\] ^ _ ` { } ~</p>

Property names	Details
	Default value: none

Settings for connecting directly to a RADIUS server and an authorization server

To use a RADIUS server as an external authentication server and to use an LDAP directory server as an external authorization server by directly specifying the LDAP directory information in the `exauth.properties` file, specify the settings in the `exauth.properties` file as shown in the following table.

Property names	Details
<code>auth.server.type</code>	Specify an external authentication server type. Specify <code>radius</code> . Default value: <code>internal</code> (do not connect to an external authentication server)
<code>auth.server.name</code>	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 are applied to. <code>ServerName</code> has been set as the initial value. You must specify at least one name. When configuring a redundant configuration, separate the server identification name of each server with a comma (,). Do not register the same server identification name more than once. Specifiable values: No more than 64 bytes of the following characters: A to Z a to z 0 to 9 ! # () + - . = @ [] ^ _ { } ~ Default value: none
<code>auth.group.mapping</code>	Specify whether to also connect to an external authorization server (LDAP directory server). Specify <code>true</code> (connect). Default value: <code>false</code> (do not connect)
<code>auth.ocsp.enable</code>	Specify whether or not to verify the validity of an LDAP directory server's electronic signature certificate by using an OCSP responder when the LDAP directory server and StartTLS are used for communication.

Property names	Details
	<p>If you want to verify the validity of certificates, specify <code>true</code>. To not verify the validity of certificates, specify <code>false</code>.</p> <p>Default value: <code>false</code></p>
<code>auth.ocsp.responderURL</code>	<p>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.</p> <p>Default value: none</p>
<code>auth.radius.auth.server.name-property-value.protocol</code>	<p>Specify the protocol for RADIUS server authentication. This attribute is required.</p> <p>Specifiable values: <code>PAP</code> or <code>CHAP</code></p> <p>Default value: none</p>
<code>auth.radius.auth.server.name-property-value.host</code>	<p>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. To specify an IPv6 address, enclose it in square brackets (<code>[]</code>). This attribute is required.</p> <p>To connect to an external authorization server (LDAP directory server) that is running on the same computer and to use StartTLS as the protocol for connecting to the LDAP directory server, in the <code>host</code> attribute, specify the same host name as the value of CN in the LDAP directory server certificate. You cannot use an IP address.</p> <p>Default value: none</p>
<code>auth.radius.auth.server.name-property-value.port</code>	<p>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.</p> <p>Specifiable values: 1 to 65535</p> <p>Default value: 1812</p>
<code>auth.radius.auth.server.name-property-value.timeout</code>	<p>Specify the amount of time to wait before timing out when connecting to the RADIUS server.</p> <p>Specifiable values: 1 to 65535 (seconds)</p> <p>Default value: 1</p>
<code>auth.radius.auth.server.name-</code>	<p>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.</p>

Property names	Details
<code>property-value.retry.times</code>	<p>Specifiable values: 0 to 50</p> <p>Default value: 3</p>
<code>auth.radius.auth.server.name-property-value.attr.NAS-IP-Address</code>	<p>Specify the IPv4 address of the Analyzer server. The RADIUS server uses this attribute value to identify the Analyzer server.</p> <p>If the format of the address is invalid, this property is disabled.</p> <p>You must specify exactly one of the following: <code>attr.NAS-IP-Address</code>, <code>attr.NAS-IPv6-Address</code>, or <code>attr.NAS-Identifier</code>.</p> <p>Default value: none</p>
<code>auth.radius.auth.server.name-property-value.attr.NAS-IPv6-Address</code>	<p>Specify the IPv6 address of the Analyzer server. The RADIUS server uses this attribute value to identify the Analyzer server. Enclose the IPv6 address in square brackets ([]).</p> <p>If the format of the address is invalid, this property is disabled.</p> <p>You must specify exactly one of the following: <code>attr.NAS-IP-Address</code>, <code>attr.NAS-IPv6-Address</code>, or <code>attr.NAS-Identifier</code>.</p> <p>Default value: none</p>
<code>auth.radius.auth.server.name-property-value.attr.NAS-Identifier</code>	<p>Specify the host name of the Analyzer server. The RADIUS server uses this attribute value to identify the Analyzer server. The host name of the Analyzer server has been set as the initial value.</p> <p>You must specify exactly one of the following: <code>attr.NAS-IP-Address</code>, <code>attr.NAS-IPv6-Address</code>, or <code>attr.NAS-Identifier</code>.</p> <p>Specifiable values: Specify no more than 253 bytes of the following characters:</p> <p>A to Z</p> <p>a to z</p> <p>0 to 9</p> <p>! " # \$ % & ' () * + , - . / : ; < = > ? @</p> <p>[\] ^ _ ` { } ~</p> <p>Default value: none</p>

Property names	Details
<code>auth.radius.auth.server.name-property-value.domain.name</code>	<p>Specify the name of a domain managed by the LDAP directory server (external authorization server). This attribute is required.</p> <p>Default value: none</p>
<code>auth.radius.auth.server.name-property-value.dns_lookup</code>	<p>Specify whether to use the DNS server to look up the information about the LDAP directory server (external authorization server). Specify <code>false</code> (do not look up the information).</p> <p>Default value: <code>false</code> (do not look up the information)</p>
<code>auth.group.domain-name.protocol</code>	<p>Specify the protocol for connecting to the LDAP directory server (external authorization server).</p> <p>When communicating in plain text format, specify <code>ldap</code>. When using StartTLS communication, specify <code>tls</code>.</p> <p>Before specifying <code>tls</code>, you must specify the security settings of Common component. In addition, make sure that one of the following encryption methods can be used on the LDAP directory server.</p> <ul style="list-style-type: none"> ▪ <code>TLS_RSA_WITH_AES_256_GCM_SHA384</code> ▪ <code>TLS_RSA_WITH_AES_256_CBC_SHA256</code> ▪ <code>TLS_RSA_WITH_AES_256_CBC_SHA</code> ▪ <code>TLS_RSA_WITH_AES_128_CBC_SHA256</code> ▪ <code>TLS_RSA_WITH_AES_128_CBC_SHA</code> <p>Specifiable values: <code>ldap</code> or <code>tls</code></p> <p>Default value: <code>ldap</code></p>
<code>auth.group.domain-name.host</code>	<p>If the external authentication server and the external authorization server (LDAP directory 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 ([]).</p> <p>If you omit this attribute, the external authentication server and the external authorization server are assumed to be running on the same computer.</p>

Property names	Details
	<p>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 <code>host</code> attribute specify the same host name as the value of CN in the LDAP directory server certificate. You cannot use an IP address.</p> <p>Default value: none</p>
<code>auth.group.domain-name.port</code>	<p>Specify the port number of the LDAP directory server (external authorization server). Make sure beforehand that the port you specify is set as the listen port number on the LDAP directory server.</p> <p>Specifiable values: 1 to 65535</p> <p>Default value: 389</p>
<code>auth.group.domain-name.basedn</code>	<p>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 (external authorization 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.</p> <p>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.</p> <p>Spaces # + ; , < = > \</p> <p>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.</p> <p>If you omit this attribute, the value specified in the <code>defaultNamingContext</code> property of Active Directory is assumed as the BaseDN.</p> <p>Default value: none</p>
<code>auth.group.domain-name.timeout</code>	<p>Specify the amount of time to wait before timing out when connecting to the LDAP directory server (external authorization server). If you specify 0, the system waits until a communication error occurs without timing out.</p> <p>Specifiable values: 0 to 120 (seconds)</p> <p>Default value: 15</p>

Property names	Details
<code>auth.group.domain-name.retry.interval</code>	Specify the retry interval (in seconds) for when an attempt to connect to the LDAP directory server (external authorization server) fails. Specifiable values: 1 to 60 (seconds) Default value: 1
<code>auth.group.domain-name.retry.times</code>	Specify the number of retries to attempt when an attempt to connect to the LDAP directory server (external authorization server) fails. If you specify 0, no retries are attempted. Specifiable values: 0 to 50 Default value: 20
Note: For <i>domain-name</i> , specify the value specified for <code>auth.radius.auth.server.name-property-value.domain.name</code> .	

Settings for using DNS to connect to a RADIUS server and an authorization server

To use a RADIUS server as an external authentication server and to use an LDAP directory server as an external authorization server by obtaining the LDAP directory information from the DNS server, specify the settings in the `exauth.properties` file as shown in the following table.

Property names	Details
<code>auth.server.type</code>	Specify an external authentication server type. Specify <code>radius</code> . Default value: <code>internal</code> (do not connect to an external authentication server)
<code>auth.server.name</code>	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 are applied to. <code>ServerName</code> has been set as the initial value. You must specify at least one name. When configuring a redundant configuration, separate the server identification name of each server with a comma (,). Do not register the same server identification name more than once. Specifiable values: No more than 64 bytes of the following characters:

Property names	Details
	<p>A to Z</p> <p>a to z</p> <p>0 to 9</p> <p>! # () + - . = @ [] ^ _ { } ~</p> <p>Default value: none</p>
<code>auth.group.mapping</code>	<p>Specify whether to also connect to an external authorization server (LDAP directory server). Specify <code>true</code> (connect).</p> <p>Default value: <code>false</code> (do not connect)</p>
<code>auth.radius.auth.server.name-property-value.protocol</code>	<p>Specify the protocol for RADIUS server authentication. This attribute is required.</p> <p>Specifiable values: PAP or CHAP</p> <p>Default value: none</p>
<code>auth.radius.auth.server.name-property-value.host</code>	<p>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. To specify an IPv6 address, enclose it in square brackets ([]). This attribute is required.</p> <p>To connect to an external authorization server (LDAP directory server) that is running on the same computer and to use StartTLS as the protocol for connecting to the LDAP directory server, in the <code>host</code> attribute, specify the same host name as the value of CN in the LDAP directory server certificate. You cannot use an IP address.</p> <p>Default value: none</p>
<code>auth.radius.auth.server.name-property-value.port</code>	<p>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.</p> <p>Specifiable values: 1 to 65535</p> <p>Default value: 1812</p>
<code>auth.radius.auth.server.name-property-value.timeout</code>	<p>Specify the amount of time to wait before timing out when connecting to the RADIUS server.</p> <p>Specifiable values: 1 to 65535 (seconds)</p> <p>Default value: 1</p>
<code>auth.radius.auth.server.name-</code>	<p>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.</p>

Property names	Details
<code>property-value.retry.times</code>	<p>Specifiable values: 0 to 50</p> <p>Default value: 3</p>
<code>auth.radius.auth.server.name-property-value.attr.NAS-IP-Address</code>	<p>Specify the IPv4 address of the Analyzer server. The RADIUS server uses this attribute value to identify the Analyzer server.</p> <p>If the format of the address is invalid, this property is disabled.</p> <p>You must specify exactly one of the following: <code>attr.NAS-IP-Address</code>, <code>attr.NAS-IPv6-Address</code>, or <code>attr.NAS-Identifier</code>.</p> <p>Default value: none</p>
<code>auth.radius.auth.server.name-property-value.attr.NAS-IPv6-Address</code>	<p>Specify the IPv6 address of the Analyzer server. The RADIUS server uses this attribute value to identify the Analyzer server. Enclose the IPv6 address in square brackets ([]).</p> <p>If the format of the address is invalid, this property is disabled.</p> <p>You must specify exactly one of the following: <code>attr.NAS-IP-Address</code>, <code>attr.NAS-IPv6-Address</code>, or <code>attr.NAS-Identifier</code>.</p> <p>Default value: none</p>
<code>auth.radius.auth.server.name-property-value.attr.NAS-Identifier</code>	<p>Specify the host name of the Analyzer server. The RADIUS server uses this attribute value to identify the Analyzer server. The host name of the Analyzer server has been set as the initial value.</p> <p>You must specify exactly one of the following: <code>attr.NAS-IP-Address</code>, <code>attr.NAS-IPv6-Address</code>, or <code>attr.NAS-Identifier</code>.</p> <p>Specifiable values: Specify no more than 253 bytes of the following characters:</p> <p>A to Z</p> <p>a to z</p> <p>0 to 9</p> <p>! " # \$ % & ' () * + , - . / : ; < = > ? @</p> <p>[\] ^ _ ` { } ~</p> <p>Default value: none</p>

Property names	Details
<code>auth.radius.auth.server.name-property-value.domain.name</code>	<p>Specify the name of a domain managed by the LDAP directory server (external authorization server). This attribute is required.</p> <p>Default value: none</p>
<code>auth.radius.auth.server.name-property-value.dns_lookup</code>	<p>Specify whether to use the DNS server to look up the information about the LDAP directory server (external authorization server). Specify <code>true</code> (look up the information).</p> <p>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.</p> <ul style="list-style-type: none"> <code>auth.group.domain-name.host</code> <code>auth.group.domain-name.port</code> <p>Default value: <code>false</code> (do not look up the information)</p>
<code>auth.group.domain-name.protocol</code>	<p>Specify the protocol for connecting to the LDAP directory server (external authorization server).</p> <p>Specifiable values: <code>ldap</code></p> <p>Default value: <code>ldap</code></p>
<code>auth.group.domain-name.basedn</code>	<p>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 (external authorization 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.</p> <p>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.</p> <p>Spaces # + ; , < = > \</p> <p>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.</p> <p>If you omit this attribute, the value specified in the <code>defaultNamingContext</code> property of Active Directory is assumed as the BaseDN.</p> <p>Default value: none</p>

Property names	Details
<code>auth.group.domain-name.timeout</code>	<p>Specify the amount of time to wait before timing out when connecting to the LDAP directory server (external authorization server). If you specify 0, the system waits until a communication error occurs without timing out.</p> <p>Specifiable values: 0 to 120 (seconds)</p> <p>Default value: 15</p>
<code>auth.group.domain-name.retry.interval</code>	<p>Specify the retry interval (in seconds) for when an attempt to connect to the LDAP directory server (external authorization server) fails.</p> <p>Specifiable values: 1 to 60 (seconds)</p> <p>Default value: 1</p>
<code>auth.group.domain-name.retry.times</code>	<p>Specify the number of retries to attempt when an attempt to connect to the LDAP directory server (external authorization server) fails. If you specify 0, no retries are attempted.</p> <p>Specifiable values: 0 to 50</p> <p>Default value: 20</p>
<p>Note:</p> <p>For <i>domain-name</i>, specify the value specified for <code>auth.radius.auth.server.name-property-value.domain.name</code>.</p>	

Examples of specifying settings in the `exauth.properties` file to use a RADIUS server for authentication

Examples of how to set the `exauth.properties` file when using a RADIUS server to perform authentication are provided below.

- When connecting to only an external authentication server:

```
auth.server.type=radius
auth.server.name=ServerName
auth.group.mapping=false
auth.radius.ServerName.protocol=PAP
auth.radius.ServerName.host=radius.example.com
auth.radius.ServerName.port=1812
auth.radius.ServerName.timeout=1
auth.radius.ServerName.retry.times=3
auth.radius.ServerName.attr.NAS-Identifier=host_A
```

- When directly specifying information about an external authorization server:

```
auth.server.type=radius
auth.server.name=ServerName
auth.group.mapping=true
auth.ocsp.enable=false
auth.ocsp.responderURL=
auth.radius.ServerName.protocol=PAP
auth.radius.ServerName.host=radius.example.com
auth.radius.ServerName.port=1812
auth.radius.ServerName.timeout=1
auth.radius.ServerName.retry.times=3
auth.radius.ServerName.attr.NAS-Identifier=host_A
auth.radius.ServerName.domain.name=EXAMPLE.COM
auth.radius.ServerName.dns_lookup=false
auth.group.EXAMPLE.COM.protocol=ldap
auth.group.EXAMPLE.COM.host=ldap.example.com
auth.group.EXAMPLE.COM.port=389
auth.group.EXAMPLE.COM.basedn=dc=Example,dc=com
auth.group.EXAMPLE.COM.timeout=15
auth.group.EXAMPLE.COM.retry.interval=1
auth.group.EXAMPLE.COM.retry.times=20
```

- When using the DNS server to look up an external authorization server:

```
auth.server.type=radius
auth.server.name=ServerName
auth.group.mapping=true
auth.radius.ServerName.protocol=PAP
auth.radius.ServerName.host=radius.example.com
auth.radius.ServerName.port=1812
auth.radius.ServerName.timeout=1
auth.radius.ServerName.retry.times=3
auth.radius.ServerName.attr.NAS-Identifier=host_A
auth.radius.ServerName.domain.name=EXAMPLE.COM
auth.radius.ServerName.dns_lookup=true
auth.group.EXAMPLE.COM.protocol=ldap
auth.group.EXAMPLE.COM.basedn=dc=Example,dc=com
auth.group.EXAMPLE.COM.timeout=15
auth.group.EXAMPLE.COM.retry.interval=1
auth.group.EXAMPLE.COM.retry.times=20
```

- When using a redundant configuration:

```
auth.server.type=radius
auth.server.name=ServerName1,ServerName2
auth.group.mapping=false
auth.radius.ServerName1.protocol=PAP
auth.radius.ServerName1.host=radius1.example.com
auth.radius.ServerName1.port=1812
auth.radius.ServerName1.timeout=1
auth.radius.ServerName1.retry.times=3
auth.radius.ServerName1.attr.NAS-IP-Address=127.0.0.1
auth.radius.ServerName2.protocol=PAP
auth.radius.ServerName2.host=radius2.example.com
auth.radius.ServerName2.port=1812
auth.radius.ServerName2.timeout=1
auth.radius.ServerName2.retry.times=3
auth.radius.ServerName2.attr.NAS-IP-Address=127.0.0.1
```

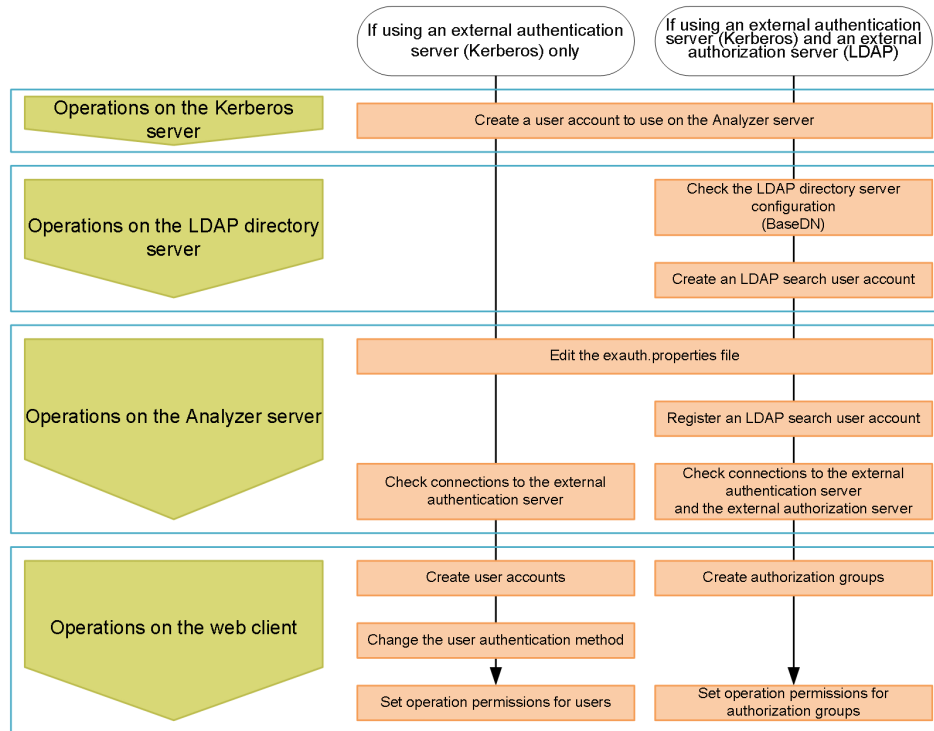
Configuring Kerberos authentication for Analyzer server

To use Kerberos authentication for the Analyzer server, you must configure the following settings.

Workflow for configuring Kerberos authentication

The workflow for connecting to the Kerberos server varies depending on whether only an external authentication server is used or both an external authentication server and an external authorization server (LDAP directory server) are used.

The following figure shows the workflow for connecting to the Kerberos server.



Note: To use StartTLS to communicate between the LDAP directory server and the Analyzer server, you must set up an environment specifically for this purpose to ensure secure communications.

Configuring the Kerberos server

On the Kerberos server, create a user account for the Analyzer server. To use an external authorization server (LDAP directory server), check the configuration details of the LDAP directory server, and then create an LDAP search user account.

Creating user accounts on the Kerberos server

On the Kerberos server, you must create user accounts (user IDs and passwords) to use on the Analyzer server.

For details about how to create user accounts on the Kerberos server, see the documentation of the Kerberos server.

User IDs and passwords must satisfy the following conditions:

- They are within 256 bytes.
- They use no characters other than the following:

A to Z

a to z

0 to 9

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

In Analyzer server, user IDs are not case-sensitive. The combination of character types for passwords must follow the settings in the external authentication server.

Configuring LDAP directory server as external authorization server

To use the LDAP directory server as an external authorization server, you must configure the LDAP directory server.

For details about how to configure the LDAP directory server, see the following descriptions:

- [Checking the LDAP directory server settings \(on page 235\)](#)

Check the BaseDN for the LDAP directory server. You will need the BaseDN information when you edit the `exauth.properties` file of the Analyzer server.

- [Creating an LDAP search user account \(on page 237\)](#)

On the LDAP directory server, create an LDAP search user account. This user account is necessary when the Analyzer server connects to the LDAP directory server to acquire user information and other information.

Connecting to the Kerberos server

To connect to the Kerberos server, you must perform the following operations on the Analyzer server.

Before you begin

- You must have Administrator permission (Windows) or root permission (Linux).
- On the Kerberos server, create a user account to use on the Analyzer server.
- Check the following information. This information is necessary for editing the file `exauth.properties`.
 - Method for connecting to the Kerberos server

The properties to be specified depend on whether information about the Kerberos server is to be directly specified, or whether information about the connection-destination Kerberos server is to be obtained from the DNS server.
 - Machine information about the Kerberos server (Host name or IP address, Port number)
 - Realm name

If you also want to connect to an external authorization server (an LDAP directory server), check the following requirements.

- Create a user account on the LDAP directory server for searching for user information.
- Check the following information. This information is necessary for editing the file `exauth.properties`.
 - Method for connecting to the LDAP directory server

The properties to be specified depend on whether information about the LDAP directory server is to be directly specified, or whether information about the connection-destination LDAP directory server is to be obtained from the DNS server.
 - Machine information about the LDAP directory server (Host name or IP address, Port number)
 - BaseDN
 - Domain name for external authorization servers managed by the LDAP directory server

Procedure

1. Edit the `exauth.properties` file.
 - a. Make a copy of the `exauth.properties` file template, which is stored in the following location, and place the copy in another folder or directory.

In Windows

`Common-component-installation-destination-folder\sample\conf\exauth.properties`

In Linux

`Common-component-installation-destination-directory/sample/conf/exauth.properties`
 - b. In the copy of the `exauth.properties` file, specify the required information.

- c. Save the `exauth.properties` file in the following location:

In Windows

`Common-component-installation-destination-folder\conf`

In Linux

`Common-component-installation-destination-directory/conf`

- d. If the values of the property `auth.ocsp.enable` or the property `auth.ocsp.responderURL` have been changed, restart the Analyzer server service.

2. If a connection also needs to be established with an external authorization server (an LDAP directory server), register on the Analyzer server a user account to use for retrieving user information.

- a. Run the **hcnds64ldapuser** command to register the LDAP search user account.

In Windows

```
Common-component-installation-destination-folder\bin
\hcnds64ldapuser /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

```
Common-component-installation-destination-directory/bin/
hcnds64ldapuser -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
```

- b. To view a list of LDAP directory servers for which LDAP search user accounts are registered, run the following command.

In Windows

```
Common-component-installation-destination-folder\bin
\hcnds64ldapuser /list
```

In Linux

```
Common-component-installation-destination-directory/bin/
hcnds64ldapuser -list
```



Tip:

To delete the LDAP search user account from the Analyzer server, run the **hcnds64ldapuser** command with the `delete` option.

3. Run the **hcnds64checkauth** command to confirm whether connections to the external authentication server and the external authorization server can be established properly.

In Windows

```
Common-component-installation-destination-folder\bin\hcnds64checkauth
[/user user-ID] [/pass password] [/summary]
```

In Linux

```
Common-component-installation-destination-directory/bin/
hcnds64checkauth [-user user-ID] [-pass password] [-summary]
```

4. On the web client, specify the following settings.
 - When a Kerberos server is configured for external user authentication:
 - Create an user account.
Make sure that the user ID is the same as the user ID that was created on the external authentication server.
 - Change the user authentication method.
 - Specify the operation permissions for the user.
 - When a Kerberos server is configured for external user authentication and an LDAP directory server is configured for authorization:
 - Register an authorization group.
 - Specify the operation permissions for the authorization group.

For details about how to perform these operations on the web client, see the *Hitachi Ops Center Analyzer User Guide*.



Note:

If you are using both an external authentication server and an external authorization server, and the user ID created on the external authentication server is registered on the Analyzer server, the user account is authenticated internally by the Analyzer server.

If the current configuration uses only an external authentication server and you want to use both an external authentication server and an external authorization server, you must remove the user ID that was created with the same name on the Analyzer server.

Kerberos configuration properties

In the `exauth.properties` file, set the type of the external authentication server to use, the server identification name, and the machine information about the external authentication server.

Items to be configured in the `exauth.properties` file differ depending on the Kerberos server environment. Use the following table to check the configuration items corresponding to your Kerberos server environment.

External authorization server used	Server connection method	Reference
No	Directly specify information about the Kerberos server.	Settings for connecting directly to a Kerberos server (on page 290)
	Obtain Kerberos server information from the DNS server.	Settings for using DNS to connect to a Kerberos server (on page 293)
Yes	Directly specify information about the Kerberos server.	Settings for connecting directly to a Kerberos server and an authorization server (on page 295)
	Obtain Kerberos server information from the DNS server.	Settings for using DNS to connect to a Kerberos server and an authorization server (on page 299)



Note:

- Be sure to distinguish between uppercase and lowercase letters for property settings.
- To use StartTLS for communication between the Analyzer server and the LDAP directory server, you must directly specify information about the LDAP directory server in the `exauth.properties` file.
- If you use a DNS server to look up the LDAP directory server to connect to, it might take longer for users to log on.

Settings for connecting directly to a Kerberos server

To use a Kerberos server as an external authorization server by directly specifying the Kerberos server information in the `exauth.properties` file, specify the settings in the `exauth.properties` file as shown in the following table.

Property names	Details
<code>auth.server.type</code>	<p>Specify an external authentication server type. Specify <code>kerberos</code>.</p> <p>Default value: <code>internal</code> (do not connect to an external authentication server)</p>
<code>auth.group.mapping</code>	<p>Specify whether to also connect to an external authorization server (LDAP directory server). Specify <code>false</code> (do not connect).</p> <p>Default value: <code>false</code> (do not connect)</p>
<code>auth.kerberos.default_realm</code>	<p>Specify the default realm name. If you specify a user ID but not a realm name in the logon window of the GUI, the user is authenticated as a user who belongs to the realm specified for this attribute. This attribute is required.</p> <p>Default value: <code>none</code></p>
<code>auth.kerberos.dns_lookup_kdc</code>	<p>Specify whether to use the DNS server to look up the information about the Kerberos server. Specify <code>false</code> (do not look up the information).</p> <p>Default value: <code>false</code> (do not look up the information)</p>
<code>auth.kerberos.default_tkt_enctypes</code>	<p>Specify the encryption type used for Kerberos authentication. This property is enabled only if the Analyzer server OS is Windows.</p> <p>You can use the following encryption types:</p> <ul style="list-style-type: none"> ▪ <code>aes256-cts</code> ▪ <code>aes128-cts</code> ▪ <code>rc4-hmac</code> ▪ <code>des3-cbc-sha1</code> ▪ <code>des-cbc-md5</code> ▪ <code>des-cbc-crc</code> <p>If you want to specify multiple encryption types, use a comma to separate the encryption types.</p> <p>Among the specified encryption types, an encryption type that is supported by both the Analyzer server OS and a Kerberos server will be used.</p>

Property names	Details
<code>auth.kerberos.clockskew</code>	<p>Specify the acceptable range of difference between the Analyzer server time and Kerberos server time. If the difference exceeds this value, an authentication error occurs.</p> <p>Specifiable values: 0 to 300 (seconds)</p> <p>Default value: 300</p>
<code>auth.kerberos.timeout</code>	<p>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.</p> <p>Specifiable values: 0 to 120 (seconds)</p> <p>Default value: 3</p>
<code>auth.kerberos.realm_name</code>	<p>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.</p> <p>Default value: none</p>
<code>auth.kerberos.auth.kerberos.realm_name-property-value.realm</code>	<p>Specify the name of the realm set in the Kerberos server. This attribute is required.</p> <p>Default value: none</p>
<code>auth.kerberos.auth.kerberos.realm_name-property-value.kdc</code>	<p>Specify the information about the Kerberos server in the following format:</p> <p><i>host-name-or-IP-address[:port-number]</i></p> <p>This attribute is required.</p> <p><i>host-name-or-IP-address</i></p> <p>If you specify the host name, make sure beforehand that the name can be resolved to an IP address.</p> <p>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).</p> <p>When using StartTLS as the protocol for connecting to the external authorization server (LDAP directory server), specify the same host name as the value of CN in the external authorization server certificate. You cannot use an IP address.</p>

Property names	Details
	<p><i>port-number</i></p> <p>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.</p> <p>When configuring the Kerberos server in redundant configuration, separate the servers with commas (,) as follows:</p> <p><i>host-name-or-IP-address[:port-number], host-name-or-IP-address[:port-number], ...</i></p>

Settings for using DNS to connect to a Kerberos server

To use a Kerberos server as an external authorization server by obtaining the Kerberos server information from the DNS server, specify the settings in the `exauth.properties` file as shown in the following table.

Property names	Details
<code>auth.server.type</code>	<p>Specify an external authentication server type. Specify <code>kerberos</code>.</p> <p>Default value: <code>internal</code> (do not connect to an external authentication server)</p>
<code>auth.group.mapping</code>	<p>Specify whether to also connect to an external authorization server (LDAP directory server). Specify <code>false</code> (do not connect).</p> <p>Default value: <code>false</code> (do not connect)</p>
<code>auth.kerberos.default_realm</code>	<p>Specify the default realm name. If you specify a user ID but not a realm name in the logon window of the GUI, the user is authenticated as a user who belongs to the realm specified for this attribute. This attribute is required.</p> <p>Default value: <code>none</code></p>
<code>auth.kerberos.dns_lookup_kdc</code>	<p>Specify whether to use the DNS server to look up the information about the Kerberos server. Specify <code>true</code> (look up the information). This attribute is required.</p>

Property names	Details
	<p>However, if all the following attributes values are already set, the Kerberos server will not be looked up by using the DNS server.</p> <ul style="list-style-type: none"> ▪ <code>auth.kerberos.realm_name</code> ▪ <code>auth.kerberos.auth.kerberos.realm_name-property-value.realm</code> ▪ <code>auth.kerberos.auth.kerberos.realm_name-property-value.kdc</code> <p>Default value: <code>false</code> (do not look up the information)</p>
<code>auth.kerberos.default_tkt_enctypes</code>	<p>Specify the encryption type used for Kerberos authentication. This property is enabled only if the Analyzer server OS is Windows.</p> <p>You can use the following encryption types:</p> <ul style="list-style-type: none"> ▪ <code>aes256-cts</code> ▪ <code>aes128-cts</code> ▪ <code>rc4-hmac</code> ▪ <code>des3-cbc-sha1</code> ▪ <code>des-cbc-md5</code> ▪ <code>des-cbc-crc</code> <p>If you want to specify multiple encryption types, use a comma to separate the encryption types.</p> <p>Among the specified encryption types, an encryption type that is supported by both the Analyzer server OS and a Kerberos server will be used.</p>
<code>auth.kerberos.clockskew</code>	<p>Specify the acceptable range of difference between the Analyzer server time and Kerberos server time. If the difference exceeds this value, an authentication error occurs.</p> <p>Specifiable values: 0 to 300 (seconds)</p> <p>Default value: 300</p>
<code>auth.kerberos.timeout</code>	<p>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.</p>

Property names	Details
	Specifiable values: 0 to 120 (seconds) Default value: 3

Settings for connecting directly to a Kerberos server and an authorization server

To use an LDAP directory server as an external authorization server and to use a Kerberos server as an external authentication server by directly specifying the Kerberos server information in the `exauth.properties` file, specify the settings in the `exauth.properties` file as shown in the following table.

Property names	Details
<code>auth.server.type</code>	Specify an external authentication server type. Specify <code>kerberos</code> . Default value: <code>internal</code> (do not connect to an external authentication server)
<code>auth.group.mapping</code>	Specify whether to also connect to an external authorization server (LDAP directory server). Specify <code>true</code> (connect). Default value: <code>false</code> (do not connect)
<code>auth.ocsp.enable</code>	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 <code>true</code> . To not verify the validity of certificates, specify <code>false</code> . Default value: <code>false</code>
<code>auth.ocsp.responderURL</code>	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
<code>auth.kerberos.default_realm</code>	Specify the default realm name. If you specify a user ID but not a realm name in the logon 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

Property names	Details
<code>auth.kerberos.dns_lookup_kdc</code>	<p>Specify whether to use the DNS server to look up the information about the Kerberos server. Specify <code>false</code> (do not look up the information).</p> <p>Default value: <code>false</code> (do not look up the information)</p>
<code>auth.kerberos.default_tkt_enctypes</code>	<p>Specify the encryption type used for Kerberos authentication.</p> <p>This property is enabled only if the Analyzer server OS is Windows.</p> <p>You can use the following encryption types:</p> <ul style="list-style-type: none"> ▪ <code>aes256-cts</code> ▪ <code>aes128-cts</code> ▪ <code>rc4-hmac</code> ▪ <code>des3-cbc-sha1</code> ▪ <code>des-cbc-md5</code> ▪ <code>des-cbc-crc</code> <p>If you want to specify multiple encryption types, use a comma to separate the encryption types.</p> <p>Among the specified encryption types, an encryption type that is supported by both the Analyzer server OS and a Kerberos server will be used.</p>
<code>auth.kerberos.clockskew</code>	<p>Specify the acceptable range of difference between the Analyzer server time and Kerberos server time. If the difference exceeds this value, an authentication error occurs.</p> <p>Specifiable values: 0 to 300 (seconds)</p> <p>Default value: 300</p>
<code>auth.kerberos.timeout</code>	<p>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.</p> <p>Specifiable values: 0 to 120 (seconds)</p> <p>Default value: 3</p>

Property names	Details
<code>auth.kerberos.realm_name</code>	<p>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.</p> <p>Default value: none</p>
<code>auth.kerberos.auth.kerberos.realm_name-property-value.realm</code>	<p>Specify the name of the realm set in the Kerberos server. This attribute is required.</p> <p>Default value: none</p>
<code>auth.kerberos.auth.kerberos.realm_name-property-value.kdc</code>	<p>Specify the information about the Kerberos server in the following format:</p> <p><i>host-name-or-IP-address[:port-number]</i></p> <p>This attribute is required.</p> <p><i>host-name-or-IP-address</i></p> <p>If you specify the host name, make sure beforehand that the name can be resolved to an IP address.</p> <p>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).</p> <p>When using StartTLS as the protocol for connecting to the external authorization server (LDAP directory server), specify the same host name as the value of CN in the external authorization server certificate. You cannot use an IP address.</p> <p><i>port-number</i></p> <p>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.</p> <p>When configuring the Kerberos server in redundant configuration, separate the servers with commas (,) as follows:</p> <p><i>host-name-or-IP-address[:port-number], host-name-or-IP-address[:port-number], ...</i></p>

Property names	Details
<code>auth.group.realm-name.protocol</code>	<p>Specify the protocol for connecting to the LDAP directory server (external authorization server).</p> <p>When communicating in plain text format, specify <code>ldap</code>. When using StartTLS communication, specify <code>tls</code>.</p> <p>Before specifying <code>tls</code>, you must specify the security settings of Common component. In addition, make sure that one of the following encryption methods can be used on the LDAP directory server.</p> <ul style="list-style-type: none"> ▪ <code>TLS_RSA_WITH_AES_256_GCM_SHA384</code> ▪ <code>TLS_RSA_WITH_AES_256_CBC_SHA256</code> ▪ <code>TLS_RSA_WITH_AES_256_CBC_SHA</code> ▪ <code>TLS_RSA_WITH_AES_128_CBC_SHA256</code> ▪ <code>TLS_RSA_WITH_AES_128_CBC_SHA</code> <p>Specifiable values: <code>ldap</code> or <code>tls</code></p> <p>Default value: <code>ldap</code></p>
<code>auth.group.realm-name.port</code>	<p>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.</p> <p>Specifiable values: 1 to 65535</p> <p>Default value: 389</p>
<code>auth.group.realm-name.basedn</code>	<p>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 (external authorization 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.</p> <p>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.</p> <p>Spaces # + ; , < = > \</p> <p>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.</p>

Property names	Details
	<p>If you omit this attribute, the value specified in the <code>defaultNamingContext</code> property of Active Directory is assumed as the BaseDN.</p> <p>Default value: none</p>
<code>auth.group.realm-name.timeout</code>	<p>Specify the amount of time to wait before timing out when connecting to the LDAP directory server (external authorization server). If you specify 0, the system waits until a communication error occurs without timing out.</p> <p>Specifiable values: 0 to 120 (seconds)</p> <p>Default value: 15</p>
<code>auth.group.realm-name.retry.interval</code>	<p>Specify the retry interval (in seconds) for when an attempt to connect to the LDAP directory server (external authorization server) fails.</p> <p>Specifiable values: 1 to 60 (seconds)</p> <p>Default value: 1</p>
<code>auth.group.realm-name.retry.times</code>	<p>Specify the number of retries to attempt when an attempt to connect to the LDAP directory server (external authorization server) fails. If you specify 0, no retries are attempted.</p> <p>Specifiable values: 0 to 50</p> <p>Default value: 20</p>
<p>Note:</p> <p>For <code>realm-name</code>, specify the value specified for <code>auth.kerberos.auth.kerberos.realm_name-property-value.realm</code>.</p>	

Settings for using DNS to connect to a Kerberos server and an authorization server

To use an LDAP directory server as an external authorization server and to use a Kerberos server as an external authentication server by obtaining the Kerberos server information from the DNS server, specify the settings in the `exauth.properties` file as shown in the following table.

Property names	Details
<code>auth.server.type</code>	<p>Specify an external authentication server type. Specify <code>kerberos</code>.</p> <p>Default value: <code>internal</code> (do not connect to an external authentication server)</p>

Property names	Details
<code>auth.group.mapping</code>	Specify whether to also connect to an external authorization server (LDAP directory server). Specify <code>true</code> (connect). Default value: <code>false</code> (do not connect)
<code>auth.kerberos.default_realm</code>	Specify the default realm name. If you specify a user ID but not a realm name in the logon 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
<code>auth.kerberos.dns_lookup_kdc</code>	Specify whether to use the DNS server to look up the information about the Kerberos server. Specify <code>true</code> (look up the information). 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. <ul style="list-style-type: none"> <code>auth.kerberos.realm_name</code> <code>auth.kerberos.auth.kerberos.realm_name-property-value.realm</code> <code>auth.kerberos.auth.kerberos.realm_name-property-value.kdc</code> Default value: <code>false</code> (do not look up the information)
<code>auth.kerberos.default_tkt_enctypes</code>	Specify the encryption type used for Kerberos authentication. This property is enabled only if the Analyzer server OS is Windows. You can use the following encryption types: <ul style="list-style-type: none"> <code>aes256-cts</code> <code>aes128-cts</code> <code>rc4-hmac</code> <code>des3-cbc-sha1</code> <code>des-cbc-md5</code> <code>des-cbc-crc</code> If you want to specify multiple encryption types, use a comma to separate the encryption types.

Property names	Details
	Among the specified encryption types, an encryption type that is supported by both the Analyzer server OS and a Kerberos server will be used.
auth.kerberos.clockskew	Specify the acceptable range of difference between the Analyzer 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
auth.kerberos.time out	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

Examples of specifying settings in the exauth.properties file to use a Kerberos server for 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 connecting to an external authorization server):

```
auth.server.type=kerberos
auth.group.mapping=false
auth.kerberos.default_realm=EXAMPLE.COM
auth.kerberos.dns_lookup_kdc=false
auth.kerberos.clockskew=300
auth.kerberos.timeout=3
auth.kerberos.realm_name=RealmName
auth.kerberos.RealmName.realm=EXAMPLE.COM
auth.kerberos.RealmName.kdc=kerberos.example.com:88
```

- When using the DNS server to look up a Kerberos server (when not connecting to an external authorization server):

```
auth.server.type=kerberos
auth.group.mapping=false
auth.kerberos.default_realm=EXAMPLE.COM
auth.kerberos.dns_lookup_kdc=true
auth.kerberos.clockskew=300
auth.kerberos.timeout=3
```

- When directly specifying information about a Kerberos server (when also connecting to an external authorization server):

```
auth.server.type=kerberos
auth.group.mapping=true
auth.ocsp.enable=false
auth.ocsp.responderURL=
auth.kerberos.default_realm=EXAMPLE.COM
auth.kerberos.dns_lookup_kdc=false
auth.kerberos.clockskew=300
auth.kerberos.timeout=3
auth.kerberos.realm_name=RealmName
auth.kerberos.RealmName.realm=EXAMPLE.COM
auth.kerberos.RealmName.kdc=kerberos.example.com:88
auth.group.EXAMPLE.COM.protocol=ldap
auth.group.EXAMPLE.COM.port=389
auth.group.EXAMPLE.COM.basedn=dc=Example,dc=com
auth.group.EXAMPLE.COM.timeout=15
auth.group.EXAMPLE.COM.retry.interval=1
auth.group.EXAMPLE.COM.retry.times=20
```

- When using the DNS server to look up a Kerberos server (when also connecting to an external authorization server):

```
auth.server.type=kerberos
auth.group.mapping=true
auth.kerberos.default_realm=EXAMPLE.COM
auth.kerberos.dns_lookup_kdc=true
auth.kerberos.clockskew=300
auth.kerberos.timeout=3
```

- When using a redundant configuration:

```
auth.server.type=kerberos
auth.group.mapping=false
auth.kerberos.default_realm=EXAMPLE.COM
auth.kerberos.dns_lookup_kdc=false
auth.kerberos.clockskew=300
auth.kerberos.timeout=3
auth.kerberos.realm_name=S1
auth.kerberos.S1.realm=EXAMPLE.COM
auth.kerberos.S1.kdc=kerberos.example.com:88,kerberos.example.net:88
```

- When specifying multiple realm identifiers:

```
auth.server.type=kerberos
auth.group.mapping=false
auth.kerberos.default_realm=EXAMPLE.COM
auth.kerberos.dns_lookup_kdc=false
auth.kerberos.clockskew=300
auth.kerberos.timeout=3
auth.kerberos.realm_name=S1,S2
auth.kerberos.S1.realm=EXAMPLE.COM
auth.kerberos.S1.kdc=kerberos1.example.com:88,kerberos1.example.net:88
auth.kerberos.S2.realm=EXAMPLE.NET
auth.kerberos.S2.kdc=kerberos2.example.com:88,kerberos2.example.net:88
```

Configuring external user authentication on the Analyzer probe server and the Analyzer detail view server

To authenticate users by using an external authentication server (Active Directory), you will need to configure settings on the Analyzer probe server and the Analyzer detail view server.

The procedure for configuring settings on the Analyzer probe server and on the Analyzer detail view server is the same.



Note:

Configuring the settings for external user authentication for the Analyzer detail view server is optional.

You must configure the settings for external user authentication only if you want to log on to the Analyzer detail view server by using Active Directory user accounts.

When the Analyzer detail view UI is launched from the Ops Center Analyzer UI, you do not need to configure settings for external user authentication on the Analyzer detail view server because internal user accounts are used.

Configuring the SSL port

The SSL port is enabled and the non-SSL port is disabled while connecting to the Active Directory server.

Procedure

1. From the Analyzer detail view server or Analyzer probe server, verify the domain name of the Active Directory using the command:

```
nslookup domain-name
```

2. If you cannot resolve the domain name, then add an entry of the following form in the `/etc/hosts` file:

```
Active-Directory-server-IP-address domain-name
```

3. Import one of the following certificates into the Analyzer detail view server or Analyzer probe server keystore:



Note: The password for the keystore is `changeit`.

- Active Directory Server certificate (CER format).
 - Microsoft Public Key Infrastructure (MSPKI) chain Certificate (CER format), one file that contains all the keys.
4. Upload the CER file at the following location `/tmp` on the Analyzer detail view server or Analyzer probe server using an FTP client (like WinSCP).
 5. Log on to the Analyzer detail view server or Analyzer probe server through an SSH client (like **putty**) as a root user.
 6. Run the command to import the certificate:

```
keytool -importcert -keystore /etc/pki/java/cacerts -trustcacerts -alias "alias-name" -file full-path-of-the-certificate-file
```

For example:

```
keytool -importcert -keystore /etc/pki/java/cacerts -trustcacerts -alias "detailviewAD" -file /data/cer1/LAB_chain.cer
```



Note: If you do not want to stop the **crond** service, you can stop the specific processes of the Analyzer detail view server and Analyzer probe server by using the **crontab -e** command as described in [Stopping the Analyzer detail view server or Analyzer probe server services \(on page 360\)](#) and [Starting the Analyzer detail view server or Analyzer probe server services \(on page 360\)](#)

7. Stop the **crond** service using the command:

```
service crond stop
```

8. Stop the jetty service using the command:

```
/usr/local/megha/bin/megha-jetty.sh stop
```

9. Confirm the stop status of the jetty service using the command:

```
/usr/local/megha/bin/megha-jetty.sh status
```

10. Start the jetty service using the command:

```
/usr/local/megha/bin/megha-jetty start
```

11. Start the crond service using the command:

```
service crond start
```

12. Access the Analyzer detail view or Analyzer probe UI as an administrator user, and then add the Active Directory users.

Verifying the Active Directory domain name

Before you can add an Active Directory user, the Active Directory domain name must be resolved by the Analyzer detail view server or Analyzer probe server.

Procedure

1. Log on to the Analyzer detail view server or Analyzer probe server through an SSH client (like **putty**) as a root user.
2. Verify the domain name of the Active Directory using the following command:

```
nslookup domain-name
```

3. If you cannot resolve the domain name, then add an entry of the following form in the `/etc/hosts` file:

```
Active-Directory-server-IP-address domain-name
```

Matching non-default Active Directory server settings

If you are using a non-default setting to connect to the Active Directory server, you must follow this procedure to change the settings on the Analyzer detail view server and Analyzer probe server

The default non-SSL port is 389 and the SSL port is 636.

Procedure

1. Log on to the Analyzer detail view server or Analyzer probe server through an SSH client (like **putty**) as a root user.

2. List the details of the properties using the command:

```
cat /usr/local/megha/conf/sys/ad.properties
```

The default values are:

- ad.ssl.port=636
- ad.non.ssl.port=389
- ad.auth.type=simple
- ad.connect.timeout=5000
- ad.connect.retry.interval=1000
- ad.connect.retry.times=2

3. Note any property value that needs to be changed. For example, ad.ssl.port=123.

4. Enter the command:

```
cd /usr/local/megha/conf
```

5. Create a new custom directory as follows:

```
mkdir custom
```

6. Create a file custom.properties in the new folder you just created (/usr/local/megha/conf/custom).

7. In the custom.properties file, add the property you noted earlier. For example: ad.ssl.port=123.

8. Change the owner of the new files and folders:

```
chown -R megha:megha /usr/local/megha/conf/custom
```

9. Stop the megha service:

```
/usr/local/megha/bin/megha-jetty.sh stop
```

10. Confirm the megha service has stopped:

```
/usr/local/megha/bin/megha-jetty.sh status
```

11. Restart the megha service:

```
/usr/local/megha/bin/megha-jetty.sh start
```

Managing Active Directory groups

You can add Active Directory groups to the Analyzer detail view or Analyzer probe. (To log on to the server Ops Center Analyzer detail view as an Active Directory user, the Active Directory user must be a member of the Active Directory groups.)

Procedure

1. Log on to the Ops Center Analyzer detail view and make the appropriate selection:
 - **Analyzer detail view:** In the application bar, click the **Manage** menu.
 - **Analyzer probe:** Click the **Manage** menu.
2. In the **Administration** section, click the **Manage Active Directory Groups** link.
3. In the **Manage Active Directory Groups** window, click **Add Active Directory Group**.
4. Type the Active Directory group name.
5. Type the user name (with the fully qualified domain name) and the password.
All users from the specified Active Directory group are registered on the Analyzer detail view or Analyzer probe as Normal users and can access the UI with the Active Directory logon credentials.
6. Click **Submit**.

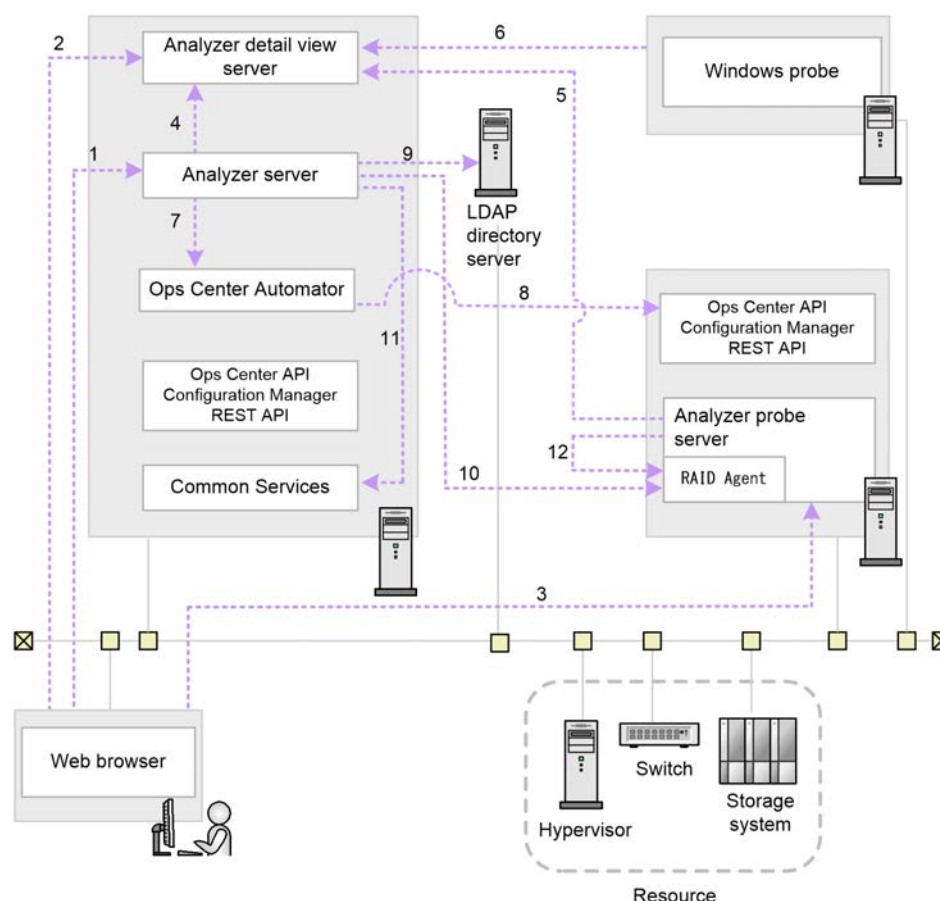
Chapter 11: Configure secure communications

You can configure secure communications between each of the servers and clients.

About security settings

In Ops Center Analyzer, you can use SSL and SSH to ensure secure network communications. In SSL and SSH communications, communication routes are encrypted to prevent information leakage and detect any data manipulation during transfer. You can further enhance security using authentication.

The following shows the security communication routes for Ops Center Analyzer.



The following shows the security communication routes that can be used in Ops Center Analyzer and the supported protocols for each route that is used. Note that the number in the table corresponds with the number in the figure.

Route	Server (program)	Client	Protocol
1	Analyzer server	Web client	HTTP HTTPS
2	Analyzer detail view server	Web client	HTTPS
3	Analyzer probe server	Web client	HTTPS
4	Analyzer detail view server	Analyzer server	HTTPS*
5	Analyzer detail view server	Analyzer probe server	FTP FTPS HTTPS SFTP
6	Analyzer detail view server	Windows host	FTP HTTPS
7	Ops Center Automator	Analyzer server	HTTP HTTPS
8	Ops Center API Configuration Manager	Ops Center Automator	HTTP HTTPS
9	LDAP directory server	Analyzer server	HTTP HTTPS
10	RAID Agent	Analyzer server	HTTP HTTPS SSH
11	Ops Center Common Services	Analyzer server	HTTPS
12	RAID Agent	Analyzer probe server	HTTP HTTPS
*: Under the initial settings, server certificates are not verified.			

If you use a certificate issued by a trusted certificate authority, use the information in this module to enhance security.

**Note:**

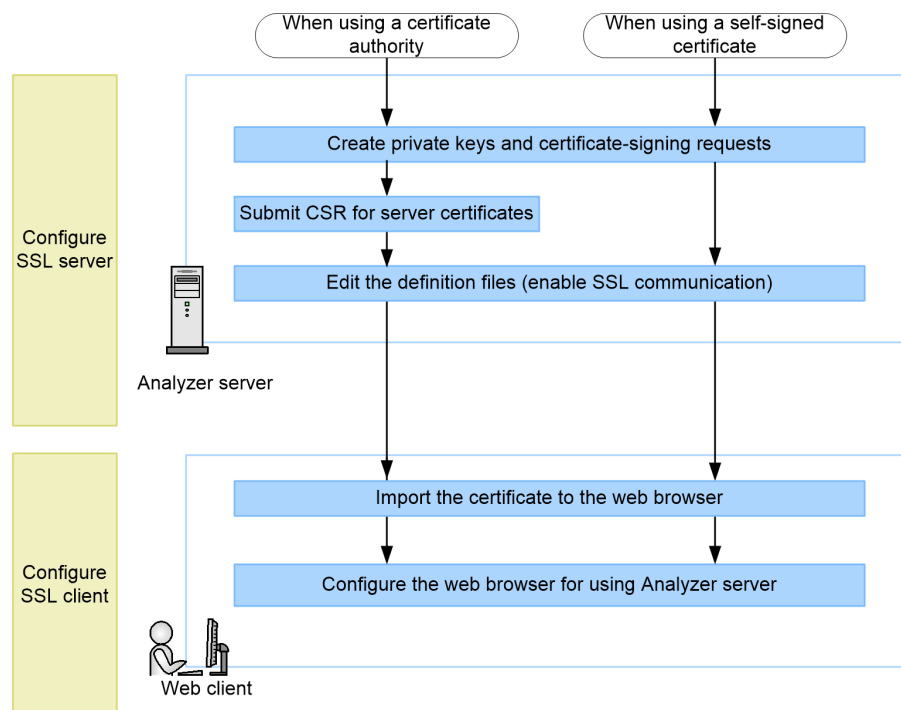
To use Ops Center Analyzer with security settings enabled, the server certificate must be valid. If the server certificate has expired, you cannot connect to Ops Center Analyzer using a secure connection.

- For communication route 1, HTTP (port: 22015) and HTTPS (port: 22016) are available by default. During initial setup after installation, HTTPS communication can be performed by using the default self-signed certificate. The default self-signed certificate is created by running the `hcmds64ssltool` command with no arguments specified. If you want to use a new self-signed certificate or a certificate issued by a certificate authority, perform the procedure in this topic.
- For security settings for communication route 8, see the *Hitachi Ops Center API Configuration Manager REST API Reference Guide*.
- For security settings for communication route 10, see the [Initial setup for enabling Granular Data Collection \(on page 116\)](#).

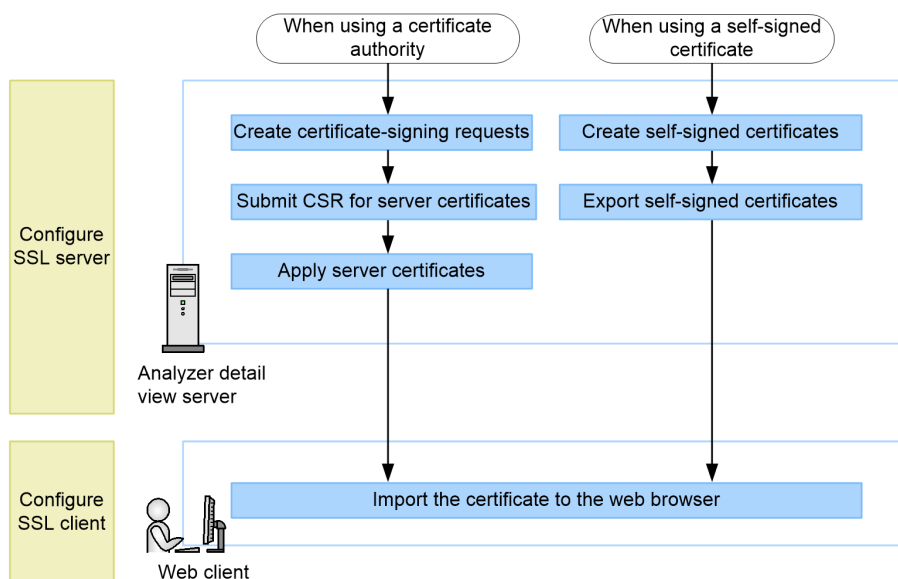
Workflow for configuring secure communications

The following figure describes the workflow for configuring secure communication in the Ops Center Analyzer environment.

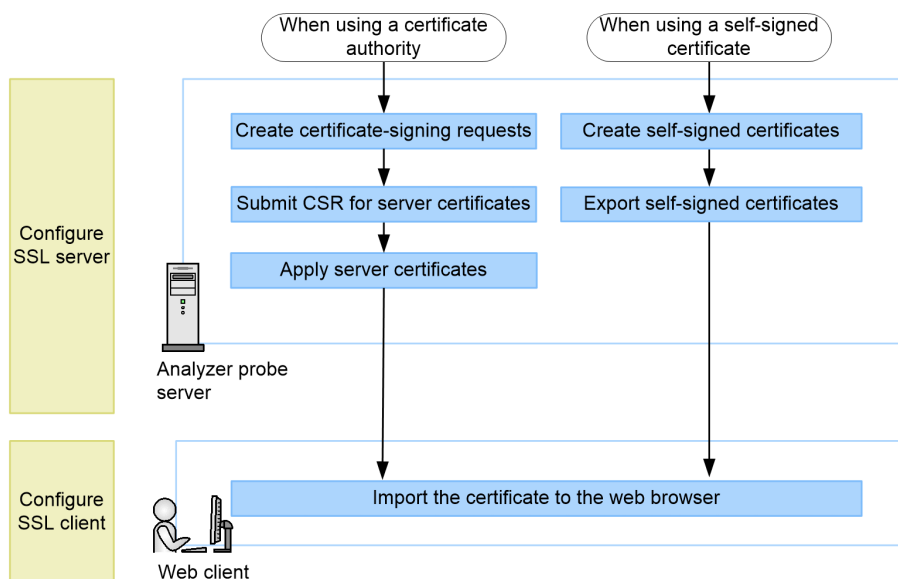
Configuration workflow for secure communication between the Analyzer server and the web client



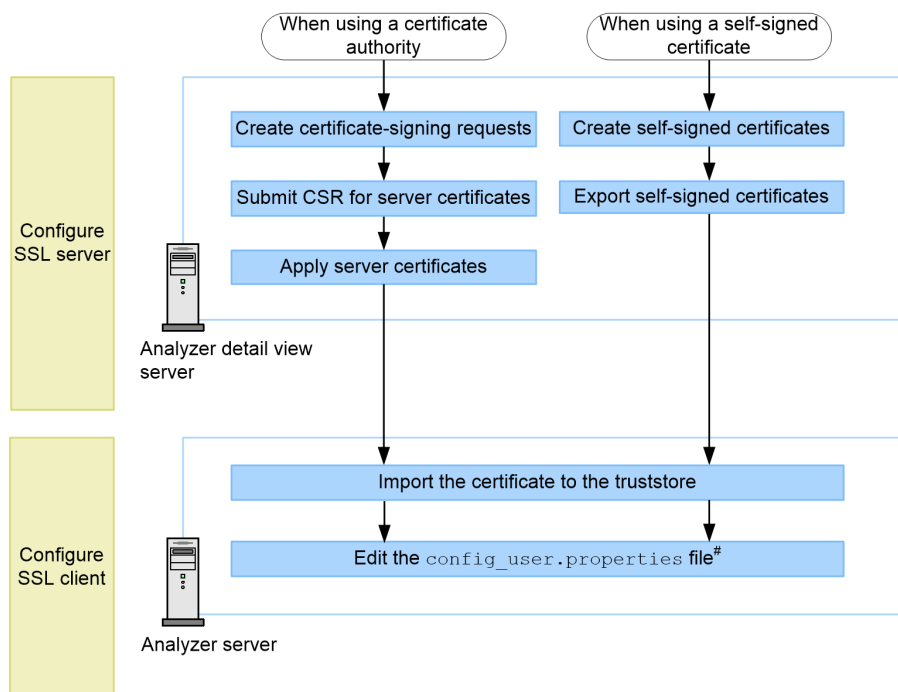
Configuration workflow for secure communication between the Analyzer detail view server and the web client



Configuration workflow for secure communication between the Analyzer probe server and the web client

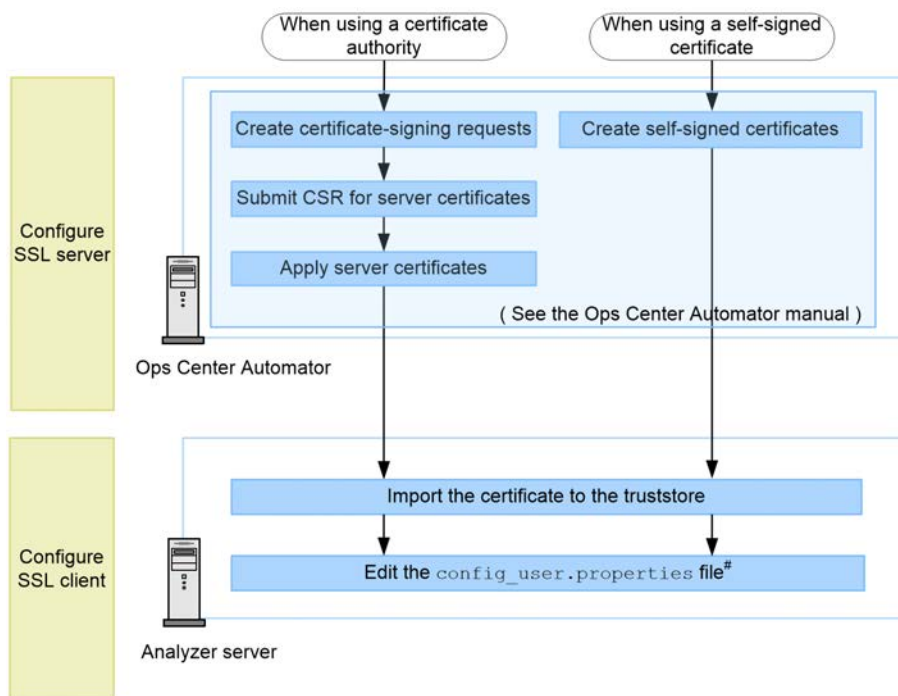


Configuration workflow for secure communication between the Analyzer detail view server and the Analyzer server



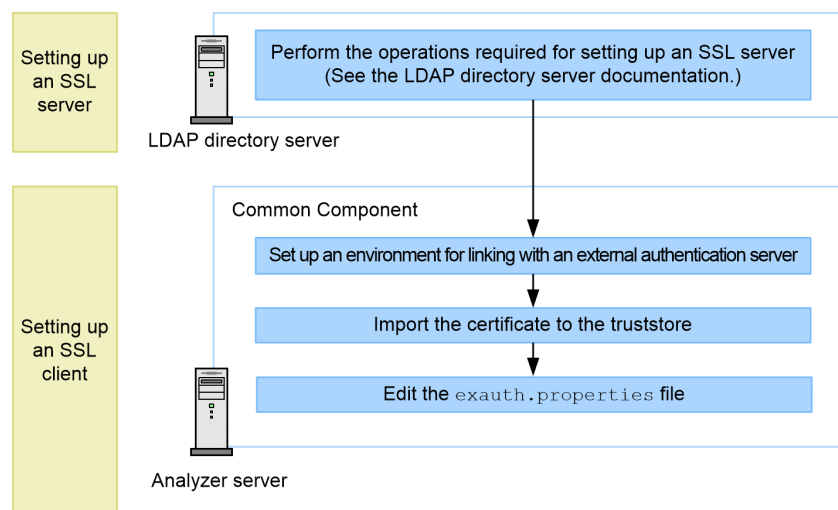
[#]: This procedure is required for enabling verification of the server certificate.
This is disabled by default.

Configuration workflow for secure communication between the Ops Center Automator and Analyzer server

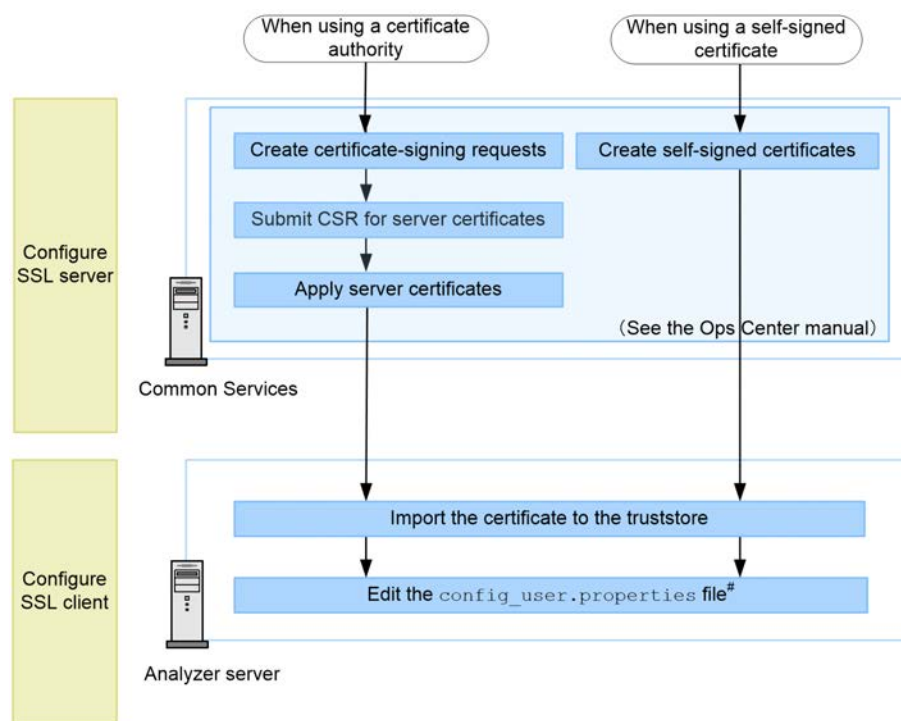


[#]: This procedure is required for enabling verification of the server certificate.
This is disabled by default.

Configuration workflow for secure communication between the LDAP directory server and Analyzer server

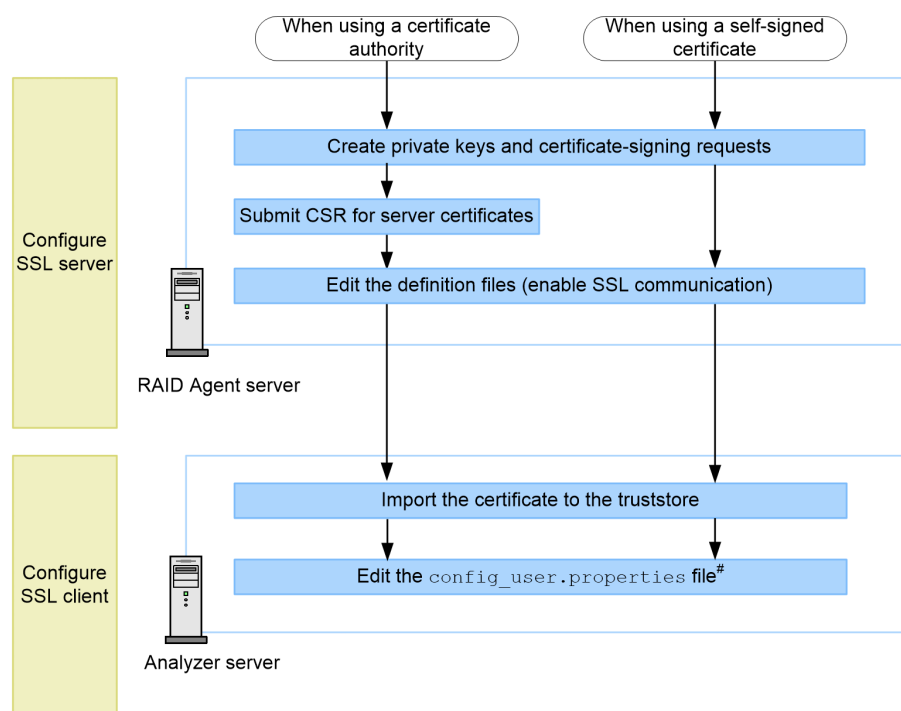


Configuration workflow for secure communication between the Analyzer server and Common Services



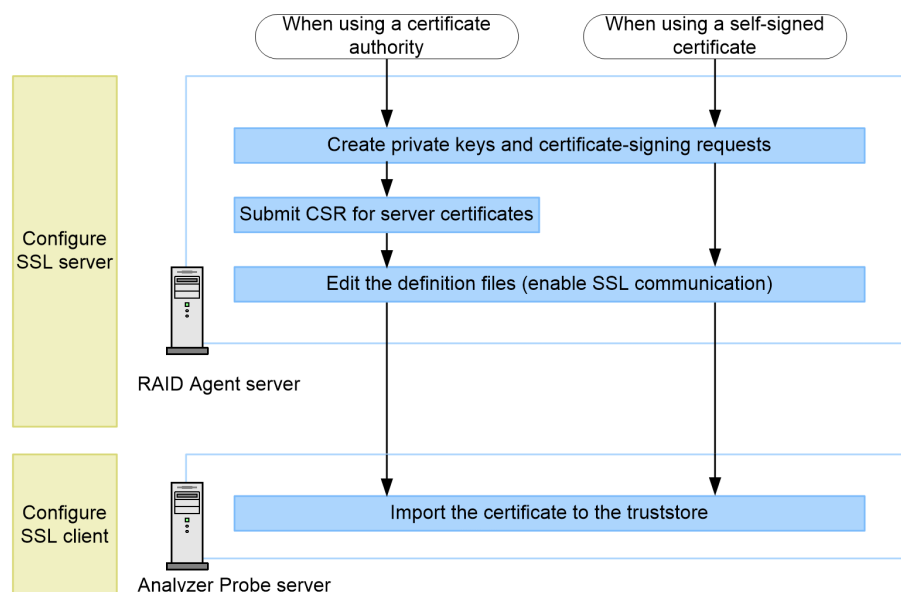
[#]: This procedure is required for enabling verification of the server certificate. This is disabled by default.

Configuration workflow for secure communication between the RAID Agent server and Analyzer server



[#]: This procedure is required for enabling verification of the server certificate.
This is disabled by default.

Configuration workflow for secure communication between the RAID Agent server and Analyzer probe server



Configuring an SSL certificate (Analyzer server)

Configure the Analyzer server as an SSL server by creating a private key and a certificate signing request, applying for a server certificate, and configuring secure communication.



Note: For an upgrade installation, the SSL settings from before the upgrade are inherited.

Creating a private key and a certificate signing request for Analyzer server

Use the `hcnds64ssltool` command to create a private key and a certificate signing request (CSR) for Analyzer server.

Before you begin

- You must have Administrator permission (Windows) or root permission (Linux) .
- Check with the certificate authority regarding the requirements for the certificate signing request.
- Make sure that the signature algorithm of the server certificate is supported by the version of the web browser.
- When re-creating a private key, certificate signing request, or self-signed certificate, send the output to a new location. (If a file of the same name exists in the output location, the file cannot be re-created.)

Procedure

1. Run the `hcnds64ssltool` command to create private keys, certificate signing requests, and self-signed certificates that support RSA cryptography and elliptic curve cryptography (ECC).

The certificate signing request is created in PEM format.



Note:

By default, the self-signed certificate and private key that were created by running the `hcnds64ssltool` command with no arguments specified are applied. Use a self-signed certificate only to test encrypted communications.

Submitting a certificate signing request (CSR) for Analyzer server

In general, applications for server certificates are submitted online. Create a certificate signing request (CSR) for Analyzer server, and send it to the certificate authority to obtain a digital signature.

Before you begin

Create a certificate signing request for Analyzer server.

You must have a server certificate that was issued in X.509 PEM format by the certificate authority. For details on how to apply, see the website of the certificate authority you use. In addition, make sure the certificate authority supports the signature algorithm.

Procedure

1. Send the created certificate signing request to the certificate authority.
2. Save the server certificate that was issued by the certificate authority in Analyzer server.



Note:

Use the `hcmds64checkcerts` command to verify the expiration date of the certificate.

Enabling SSL communication for Analyzer server

To enable SSL communication, edit the `user_httpsd.conf` file and the `command_user.properties` file.

Before you begin

- Create a private key for the Analyzer server.
- Prepare the Analyzer server certificate file from the certificate authority.

We recommend that you copy the file to the following location:

In Windows

Common-component-installation-destination-folder\uCPSB\httpsd\conf\ssl\server

In Linux

Common-component-installation-destination-directory/uCPSB/httpsd/conf/ssl/server

- Verify the host name specified for `Common Name` in the certificate signing request.

Procedure

1. Stop the Analyzer server services.
2. Edit the `user_httpsd.conf` file.

In Windows

Common-component-installation-destination-folder\uCPSB\httpsd\conf\user_httpsd.conf

In Linux

Common-component-installation-destination-directory/uCPSB/httpsd/conf/user_httpsd.conf

The following is an example of how to edit the `user_httpsd.conf` file.

```

ServerName Analyzer-server-host-name
#Listen [::]:22015
Listen 22015
#Listen 127.0.0.1:22015
SSLDisable
#Listen [::]:22016
Listen 22016
<VirtualHost *:22016>
    ServerName Analyzer-server-host-name
    SSLEnable
    SSLProtocol TLSv12
    SSLRequiredCiphers ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-
GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-
SHA256:AES256-GCM-SHA384:AES128-GCM-SHA256
    SSLRequireSSL
    SSLCertificateKeyFile "Common-component-installation-destination-
directory/uCPSB/httpsd/conf/ssl/server/httpsdkey.pem"
    SSLCertificateFile "Common-component-installation-destination-
directory/uCPSB/httpsd/conf/ssl/server/httpsd.pem"
    SSLECCCertificateKeyFile "Common-component-installation-destination-
directory/uCPSB/httpsd/conf/ssl/server/ecc-httpsdkey.pem"
    SSLECCCertificateFile "Common-component-installation-destination-
directory/uCPSB/httpsd/conf/ssl/server/ecc-httpsd.pem"
    # SSLCACertificateFile "Common-component-installation-destination-
directory/uCPSB/httpsd/conf/ssl/cacert/anycert.pem"
    # Header set Strict-Transport-Security max-age=31536000
</VirtualHost>
HWSLogSSLVerbose On

```

Uncomment the lines from `#Listen 22016` to `#HWSLogSSLVerbose On`, by removing the hash mark (#).

**Note:**

- Keep the lines `#Listen [::]:22015` and `#Listen [::]:22016` commented out, because Ops Center Analyzer does not support IPv6.
 - Even if you enable SSL communication, do not remove or comment out the line `Listen 22015`.
 - To interrupt non-SSL communication, add a hash mark (#) to the beginning of the line `Listen 22015` to comment it out, then uncomment the line `#Listen 127.0.0.1:22015`.
- For the `ServerName` directive in the first line and the `ServerName` directive inside the `<VirtualHost>` tags, enter the Analyzer server host name that you specified for `Common Name` in the certificate signing request. (Host names are case sensitive.)
 - For RSA cryptography, specify the absolute paths of the secret key and the server certificate of Analyzer server for the following directives.
 - `SSLCertificateKeyFile`
 - `SSLCertificateFile`

For elliptic curve cryptography, specify the absolute paths of the secret key and the server certificate of Analyzer server for the following directives.

 - `SSLECCCertificateKeyFile`
 - `SSLECCCertificateFile`
 - If the server certificate for Analyzer server originated from an intermediate certificate authority, remove the hash mark (#) from the beginning of the line of the `SSLCACertificateFile` directive, and then specify the absolute path of all server certificates issued by the intermediate certificate authorities. You can include multiple certificates in a single file by using a text editor to chain those certificates.
 - Do not remove the hash mark (#) from the beginning of the following line:


```
# Header set Strict-Transport-Security max-age=31536000
```

**Note:**

If Analyzer server was upgraded, `user_httpsd.conf` might not include the required directives. In such cases, copy the lines relevant to those directives from the sample file stored in the following location.

In Windows

```
Common-component-installation-destination-folder\sample
\httpsd\conf\user_httpsd.conf
```

In Linux

```
Common-component-installation-destination-directory/
sample/httpsd/conf/user_httpsd.conf
```

Note the following:

- Do not edit the `httpsd.conf`, `hssso_httpsd.conf`, or `user_hssso_httpsd.conf` files.
 - Do not specify the same directive twice.
 - Do not enter a line break in the middle of a directive.
 - When specifying paths in the directives listed below, do not specify symbolic links or junction points.
 - When specifying certificates and private key files in the directives listed below, specify PEM-format files.
3. Edit the `command_user.properties` file.

In Windows

```
Analyzer-server-installation-folder\Analytics\conf
\command_user.properties
```

In Linux

```
Analyzer-server-installation-directory/Analytics/conf/
command_user.properties
```

Change the value of the `command.ssl` property from `false` to `true`.

```
command.ssl = true
```

4. Start the Analyzer server services.
5. If Ops Center Automator is connected with the Analyzer server and the Analyzer server is set as the primary server, perform the following procedure on the host on which Ops Center Automator is installed to apply the changed port number.



Note: You must also set up SSL communication on Ops Center Automator. For details, see the section describing how to set up SSL in the *Hitachi Ops Center Automator Installation and Configuration Guide*.

- a. Run the `hcnds64prmset` command with `sslport` option to change the Common component settings.
- b. Restart Ops Center Automator.

Checking the expiration date of the certificate for Analyzer server

Use the `hcnds64checkcerts` command to check the expiration date of the Analyzer server certificate and the certificate issued by a certificate authority.

Before you begin

- The paths to the following certificates must be specified in the `user_httpsd.conf` file:
 - Server certificate for Analyzer server

When the certificate for both the RSA cryptography and the elliptic curve cryptography is used, the path of both certificates must be specified.
 - All certificates issued by intermediate certificate authorities
- You must have Administrator permission (Windows) or root permission (Linux).

Procedure

1. Run the following command:

In Windows

```
Common-component-installation-destination-folder\bin\hcmds64checkcerts { [/days number-of-days] [/log] | /all }
```

In Linux

```
Common-component-installation-destination-directory/bin/hcmds64checkcerts { [-days number-of-days] [-log] | -all }
```

The options are:

- `days`

Specify the period (in days). The range of days is 30 to 3,652 (10 years). This options displays expired certificates and those due to expire during the specified period. (When you omit this option, the command displays certificates due to expire in 30 days.)
- `log`

Specify this option if you want to regularly check the expiration dates of certificates as an operating system task. When certificates are displayed, a warning message is output to the event log or to `syslog`.
- `all`

Specify the expiration date to display for all certificates listed in the `user_httpsd.conf` file.

Deleting a certificate from the Analyzer server truststore

You can delete a certificate that was imported into Analyzer server.

Before you begin

You must have Administrator permissions (Windows) or root permissions (Linux).

Procedure

1. Run the following command to delete the certificate that was imported to Analyzer server.

In Windows

```
Common-component-installation-destination-folder\bin\hcmds64keytool -
delete -alias alias-name -keystore truststore-file-name -storepass
truststore-password
```

In Linux

```
Common-component-installation-destination-directory/uCPSB/jdk/bin/
keytool -delete -alias alias-name -keystore truststore-file-name -
storepass truststore-password
```

**Note:**

- For the *alias-name*, specify the alias name that was specified when the server certificate was imported to the truststore.
- For the *truststore-file-name*, specify the absolute path to the location where the truststore file is stored.

The truststore file is stored in the following location:

In Windows

```
Common-component-installation-destination-folder\uCPSB
\jdk\jre\lib\security\jssecacerts
```

In Linux

```
Common-component-installation-destination-directory/
uCPSB/jdk/jre/lib/security/jssecacerts
```

Configuring an SSL certificate (Analyzer detail view server)

Configure an SSL certificate to initiate a secure session with browsers by creating a private key, creating a certificate signing request (CSR), and applying the server certificate.

Creating a private key and a certificate signing request

Create a certificate signing request (CSR) for Analyzer detail view server, and send it to the certificate authority to obtain the certificate file.

Procedure

1. Log on to the Analyzer detail view server through an SSH client (like **putty**) as a root user.

2. Stop the crond service using the command:

```
service crond stop
```



Note: If you do not want to stop the **crond** service, you can stop the specific processes of the Analyzer detail view server and Analyzer probe server by using the **crontab -e** command as described in [Stopping the Analyzer detail view server or Analyzer probe server services \(on page 360\)](#) and [Starting the Analyzer detail view server or Analyzer probe server services \(on page 360\)](#)

3. Stop all the running services using the command:

```
/usr/local/megha/bin/stop-all-services.sh
```

4. Verify that the megha and crond services are stopped by entering these commands:

```
/usr/local/megha/bin/megha-jetty.sh status
```

```
service crond status
```

5. Make a backup copy of the keystore files at the following location:

```
cd /usr/local/megha/jetty/etc
cp -p keystore keystore.bak
cp -p jetty-ssl.xml jetty-ssl.xml.bak
cp -p userKeystoreConfig.xml userKeystoreConfig.xml.bak
```



Note: Use these backup copies if any error occurs during the configuration process.

6. Remove an existing keystore file present at the following location `/usr/local/megha/jetty/etc/keystore` using the command:

```
rm /usr/local/megha/jetty/etc/keystore
```

7. Create a new keystore and enter the certificate information:

```
keytool -genkey -keyalg RSA -alias jetty -keystore
/usr/local/megha/jetty/etc/keystore
```



Note: The default keystore password for the Analyzer detail view server is `megha.jeos`. If you are using a password other than the default, you must change the following fields in the `/usr/local/megha/jetty/etc/userKeystoreConfig.xml` file:

```
KeyStorePassword
KeyManagerPassword
TrustStorePassword
```

8. Change the ownership to megha in the keystore file:

```
chown megha:megha /usr/local/megha/jetty/etc/keystore
```

9. Change the access permission of the keystore file:

```
chmod 640 /usr/local/megha/jetty/etc/keystore
```

10. Create a certificate signing request (CSR) for the jetty alias:

```
keytool -certreq -alias jetty -file /tmp/certreq.txt -keystore /usr/local/megha/jetty/etc/keystore
```



Note: You must use the keystore password of the Analyzer detail view server .

11. Take a backup of jetty keystore after creating the CSR:

```
cp /usr/local/megha/jetty/etc/keystore /usr/local/megha/jetty/etc/keystoreCSR
```

12. Copy the certificate request file and submit it to the certificate authority to create the certificate file:

```
cat /tmp/certreq.txt
```

13. Start the megha service using the command:

```
/usr/local/megha/bin/megha-jetty.sh start
```

14. Start the crond service using the command:

```
service crond start
```

Applying server certificates

The certificate authority creates the following three certificate files:

- Root
- Intermediate
- Host

Procedure

1. Stop the crond service using the command:

```
service crond stop
```



Note: If you do not want to stop the **crond** service, you can stop the specific processes of the Analyzer detail view server and Analyzer probe server by using the **crontab -e** command as described in [Stopping the Analyzer detail view server or Analyzer probe server services \(on page 360\)](#) and [Starting the Analyzer detail view server or Analyzer probe server services \(on page 360\)](#)

2. Stop all the running services using the command:

```
/usr/local/megha/bin/stop-all-services.sh
```

3. Verify that the megha and crond services are stopped by entering these commands:

```
/usr/local/megha/bin/megha-jetty.sh status
```

```
service crond status
```

4. Upload the certificate files to the Analyzer detail view server. For example, upload them to `/usr/local/megha/jetty/etc`.

- a. Import the Root certificate: You must use the keystore password of the Analyzer detail view server.

```
keytool -import -alias ROOT_CA_NAME -keystore /usr/local/megha/jetty/etc/keystore -trustcacerts -file Path_to_Root_Cert
```

For example, `keytool -import -alias RootCA -keystore /usr/local/megha/jetty/etc/keystore -trustcacerts -file /usr/local/megha/jetty/etc/root.cer`

- b. Import the intermediate certificate: You must use the keystore password of the Analyzer detail view server.

```
keytool -import -alias Intermediate_CA_NAME -keystore /usr/local/megha/jetty/etc/keystore -trustcacerts -file Path_to_Intermediate_CA_Cert
```

For example, `keytool -import -alias IntermediateCA -keystore /usr/local/megha/jetty/etc/keystore -trustcacerts -file /usr/local/megha/jetty/etc/imd.cer`

- c. Import the Host certificate: You must use the keystore password of the Analyzer detail view server.

```
keytool -import -alias jetty -keystore /usr/local/megha/jetty/etc/keystore -trustcacerts -file Path_to_host_Cert
```

For example, `keytool -import -alias jetty -keystore /usr/local/megha/jetty/etc/keystore -trustcacerts -file /usr/local/megha/jetty/etc/host.cer`

5. Start the megha service using the command:

```
/usr/local/megha/bin/megha-jetty.sh start
```

6. Start the crond service using the command:

```
service crond start
```

Exporting a self-signed certificate for the Analyzer detail view server

Use the keytool command to export self-signed certificates.

Procedure

1. Run the following command to export the certificate for the Analyzer detail view server:

```
keytool -export -keystore /usr/local/megha/jetty/etc/keystore -alias  
alias-name -file certificate-file-name
```



Note:

- For the *alias-name*, specify `jetty` to export the default self-signed certificate.
- For *certificate-file-name*, specify the absolute path to the export destination of the self-signed certificate.

For example: `keytool -export -keystore /usr/local/megha/jetty/etc/keystore -alias jetty -file /root/test/Certificate`

Checking the expiration dates of certificates for Analyzer detail view server

Check the expiration dates of the server certificates and Certificate Authority certificates for Analyzer detail view server.

Procedure

1. Run the following command to check the expiration date:

```
keytool -list -v -keystore /usr/local/megha/jetty/etc/keystore
```



Note: You must use the keystore password of the Analyzer detail view server.

Sample output:

```
Valid from: Thu Nov 27 04:43:53 EST 2014 until: Tue Nov 26  
04:43:53 EST 2024
```

Changing the SSL port number of the Analyzer detail view server

To change the port number for SSL communication, you must change the port numbers specified in the definition files, and then open the new port in the firewall settings.

Procedure

1. Log on to the Analyzer detail view server through an SSH client (like putty) as the root user.
2. Stop the crond service using the command:

```
service crond stop
```



Note: If you do not want to stop the **crond** service, you can stop the specific processes of the Analyzer detail view server and Analyzer probe server by using the **crontab -e** command as described in [Stopping the Analyzer detail view server or Analyzer probe server services \(on page 360\)](#) and [Starting the Analyzer detail view server or Analyzer probe server services \(on page 360\)](#)

3. Stop all the running services using the command:

```
/usr/local/megha/bin/stop-all-services.sh
```

4. Verify that the megha and crond services are stopped by entering these commands:

```
/usr/local/megha/bin/megha-jetty.sh status
```

```
service crond status
```

5. Take the backup of `start.ini` and `jetty-ssl.xml` file:
 - `cp /usr/local/megha/jetty/start.ini /usr/local/megha/jetty/org_start.ini.backup`
 - `cp /usr/local/megha/jetty/jetty-ssl.xml /usr/local/megha/jetty/org_jetty-ssl.xml.backup`

6. Change the port number in the following files:

- /usr/local/megha/jetty/start.ini

Change the following:

```
jetty.httpConfig.securePort=required https port

jetty.http.port=required http port

https.port=required https port
```

For example:

```
jetty.httpConfig.securePort=9443

jetty.http.port=8080

https.port=9443
```

- /usr/local/megha/jetty/etc/jetty-ssl.xml

Change the following:

```
<Set name="port"><Property name="jetty.ssl.port"
deprecated="ssl.port" default="REQUIRED PORT" /></Set>
```

For example:

```
<Set name="port"><Property name="jetty.ssl.port"
deprecated="ssl.port" default="9443" /></Set>
```

7. Start the crond service using the command:

```
service crond start
```

8. Start the megha service using the command:

```
/usr/local/megha/bin/megha-jetty.sh start
```

9. After changing the port number, make sure you change the firewall settings accordingly.

Deleting an SSL certificate from the Keystore

You can delete a previously imported or expired SSL certificate from the keystore.

Procedure

1. Log on to the Analyzer detail view server or Analyzer probe server through an SSH client (like **putty**) as a root user.

2. Stop the crond service using the command:

```
service crond stop
```



Note: If you do not want to stop the **crond** service, you can stop the specific processes of the Analyzer detail view server and Analyzer probe server by using the **crontab -e** command as described in [Stopping the Analyzer detail view server or Analyzer probe server services \(on page 360\)](#) and [Starting the Analyzer detail view server or Analyzer probe server services \(on page 360\)](#)

3. Stop all the running services using the command:

```
/usr/local/megha/bin/stop-all-services.sh
```

4. Verify that the megha and crond services are stopped by entering these commands:

```
/usr/local/megha/bin/megha-jetty.sh status
```

```
service crond status
```

5. Go to the `/usr/local/megha/jetty/etc` directory and run the following command to get the list of all SSL certificates from keystore file:

```
keytool -list -v -keystore Keystore_File_Name
```

6. Check the expired status of the certificates and note the alias name of expired certificates that you want to delete.
7. Run the following command to delete the certificate from the keystore.

```
keytool -delete -alias Alias_Name -keystore Keystore_File_Name
```



Note: You must use the keystore password of Analyzer detail view server or Analyzer probe server.

8. Run the following command to verify if the certificate is deleted from keystore file.

```
keytool -list -v -keystore Keystore_File_Name
```

9. Start the megha service using the command:

```
/usr/local/megha/bin/megha-jetty.sh start
```

10. Start the crond service using the command:

```
service crond start
```

Importing Analyzer detail view server certificates to the Analyzer server truststore

To enable the Analyzer server to verify Analyzer detail view server certificates, import the certificates to the Analyzer server truststore and edit the `config_user.properties` file.

Before you begin

You must have administrator permissions (for Windows) or root permissions (for Linux).

Procedure

1. Stop the Analyzer server services.
2. Run the following command to import the certificates for the Analyzer detail view server to the truststore file:

In Windows

```
Common-component-installation-destination-folder\bin\hcmds64keytool -import -alias alias-name -file certificate-file-name -keystore truststore-file-name -storepass truststore-password -storetype JKS
```

In Linux

```
Common-component-installation-destination-directory/uCPSB/jdk/bin/keytool -import -alias alias-name -file certificate-file-name -keystore truststore-file-name -storepass truststore-password -storetype JKS
```



Note:

- For the *alias-name*, specify a name to identify which host server has the certificate.
- For the *certificate-file-name*, specify the absolute path.
- The truststore file is stored in the following location:

In Windows

```
Common-component-installation-destination-folder\uCPSB\jdk\jre\lib\security\jssecacerts
```

In Linux

```
Common-component-installation-destination-directory/uCPSB/jdk/jre/lib/security/jssecacerts
```

- The password to access the default truststore is `changeit`.
- You must specify `JKS` for the keystore type of the truststore.

3. To enable the verification of server certificates, change the following properties in the `config_user.properties` file:
 - Location:

In Windows

```
Analyzer-server-installation-destination-folder\Analytics\conf
```

In Linux

```
Analyzer-server-installation-destination-directory/Analytics/conf
```
 - Key: `cert.verify.enabled`
 - Value: `true`
4. Start the Analyzer server services.

Configuring an SSL certificate (Analyzer probe server)

Configure an SSL certificate to initiate a secure session with browsers by creating a private key, creating a certificate signing request (CSR), and applying the server certificate.

Creating a private key and a certificate signing request

Create a certificate signing request (CSR) for Analyzer probe server, and send it to the certificate authority to obtain the certificate file.

Procedure

1. Log on to the Analyzer probe server through an SSH client (like **putty**) as a root user.
2. Stop the `crond` service using the command:

```
service crond stop
```



Note: If you do not want to stop the `crond` service, you can stop the specific processes of the Analyzer detail view server and Analyzer probe server by using the `crontab -e` command as described in [Stopping the Analyzer detail view server or Analyzer probe server services \(on page 360\)](#) and [Starting the Analyzer detail view server or Analyzer probe server services \(on page 360\)](#)

3. Stop all the running services using the command:

```
/usr/local/megha/bin/stop-all-services.sh
```

4. Verify that the megha and crond services are stopped by entering these commands:

```
/usr/local/megha/bin/megha-jetty.sh status
```

```
service crond status
```

5. Make a backup copy of the keystore files at the following location:

```
cd /usr/local/megha/jetty/etc
cp -p keystore keystore.bak
cp -p jetty-ssl.xml jetty-ssl.xml.bak
cp -p userKeystoreConfig.xml userKeystoreConfig.xml.bak
```



Note: Use these backup copies if any error occurs during the configuration process.

6. Remove an existing keystore file present at the following location `/usr/local/megha/jetty/etc/keystore` using the command:

```
rm /usr/local/megha/jetty/etc/keystore
```

7. Create a new keystore and enter the certificate information:

```
keytool -genkey -keyalg RSA -alias jetty -keystore /usr/local/megha/jetty/etc/keystore
```



Note: The default keystore password for the Analyzer probe server is `megha.jeos`. If you are using a password other than the default, you must change the following fields in the `/usr/local/megha/jetty/etc/userKeystoreConfig.xml` file:

```
KeyStorePassword
KeyManagerPassword
TrustStorePassword
```

8. Change the ownership to megha in the keystore file:

```
chown megha:megha /usr/local/megha/jetty/etc/keystore
```

9. Change the access permission of the keystore file:

```
chmod 640 /usr/local/megha/jetty/etc/keystore
```

10. Create a certificate signing request (CSR) for the jetty alias:

```
keytool -certreq -alias jetty -file /tmp/certreq.txt -keystore /usr/local/megha/jetty/etc/keystore
```



Note: You must use the keystore password of the Analyzer probe server.

11. Take a backup of jetty keystore after creating the CSR:

```
cp /usr/local/megha/jetty/etc/keystore /usr/local/megha/jetty/etc/keystoreCSR
```

12. Copy the certificate request file and submit it to the certificate authority to create the certificate file:

```
cat /tmp/certreq.txt
```

13. Start the megha service using the command:

```
/usr/local/megha/bin/megha-jetty.sh start
```

14. Start the crond service using the command:

```
service crond start
```

Applying server certificates

The certificate authority creates the following three certificate files:

- Root
- Intermediate
- Host

Procedure

1. Stop the crond service using the command:

```
service crond stop
```



Note: If you do not want to stop the **crond** service, you can stop the specific processes of the Analyzer detail view server and Analyzer probe server by using the **crontab -e** command as described in [Stopping the Analyzer detail view server or Analyzer probe server services \(on page 360\)](#) and [Starting the Analyzer detail view server or Analyzer probe server services \(on page 360\)](#)

2. Stop all the running services using the command:

```
/usr/local/megha/bin/stop-all-services.sh
```

3. Verify that the megha and crond services are stopped by entering these commands:

```
/usr/local/megha/bin/megha-jetty.sh status
```

```
service crond status
```

4. Upload certificate files to the Analyzer probe server. For example, upload them to `/usr/local/megha/jetty/etc`.

- a. Import the Root certificate: You must use the keystore password of the Analyzer probe server.

```
keytool -import -alias ROOT_CA_NAME -keystore /usr/local/megha/jetty/etc/keystore -trustcacerts -file Path_to_Root_Cert
```

For example, `keytool -import -alias RootCA -keystore /usr/local/megha/jetty/etc/keystore -trustcacerts -file /usr/local/megha/jetty/etc/root.cer`

- b. Import the intermediate certificate: You must use the keystore password of the Analyzer probe server.

```
keytool -import -alias Intermediate_CA_NAME -keystore /usr/local/megha/jetty/etc/keystore -trustcacerts -file Path_to_Intermediate_CA_Cert
```

For example, `keytool -import -alias IntermediateCA -keystore /usr/local/megha/jetty/etc/keystore -trustcacerts -file /usr/local/megha/jetty/etc/imd.cer`

- c. Import the Host certificate: You must use the keystore password of the Analyzer probe server.

```
keytool -import -alias jetty -keystore /usr/local/megha/jetty/etc/keystore -trustcacerts -file Path_to_host_Cert
```

For example, `keytool -import -alias jetty -keystore /usr/local/megha/jetty/etc/keystore -trustcacerts -file /usr/local/megha/jetty/etc/host.cer`

5. Start the megha service using the command:

```
/usr/local/megha/bin/megha-jetty.sh start
```

6. Start the crond service using the command:

```
service crond start
```

Exporting a self-signed certificate for the Analyzer probe server

Use the keytool command to export self-signed certificates.

Procedure

1. Run the following command to export the certificate for the Analyzer probe server:

```
keytool -export -keystore /usr/local/megha/jetty/etc/keystore -alias alias-name -file certificate-file-name
```

**Note:**

- For the *alias-name*, specify `jetty` to export the default self-signed certificate.
- For *certificate-file-name*, specify the absolute path to the export destination of the self-signed certificate.

Checking the expiration dates of certificates for Analyzer probe server

Check the expiration dates of the server certificates and Certificate Authority certificates for Analyzer probe server.

Procedure

1. Run the following command to check the expiration date:

```
keytool -list -v -keystore /usr/local/megha/jetty/etc/keystore
```



Note: You must use the keystore password of the Analyzer probe server.

Sample output: Valid from: Thu Nov 27 04:43:53 EST 2014 until: Tue Nov 26 04:43:53 EST 2024

Changing the SSL port number of the Analyzer probe server

To change the port number for SSL Communication, change the port numbers specified in the definition files, and then open the new port in the firewall settings.

Procedure

1. Log on to the Analyzer probe server through an SSH client (like **putty**) as a root user.
2. Stop the crond service using the command:

```
service crond stop
```



Note: If you do not want to stop the **crond** service, you can stop the specific processes of the Analyzer detail view server and Analyzer probe server by using the **crontab -e** command as described in [Stopping the Analyzer detail view server or Analyzer probe server services \(on page 360\)](#) and [Starting the Analyzer detail view server or Analyzer probe server services \(on page 360\)](#)

3. Stop all the running services using the command:

```
/usr/local/megha/bin/stop-all-services.sh
```

4. Verify that the megha and crond services are stopped by entering these commands:

```
/usr/local/megha/bin/megha-jetty.sh status
```

```
service crond status
```

5. Make a backup of the start.ini and jetty-ssl.xml files:

- `cp /usr/local/megha/jetty/start.ini/usr/local/megha/jetty/org_start.ini.backup`
- `cp /usr/local/megha/jetty/jetty-ssl.xml/usr/local/megha/jetty/org_jetty-ssl.xml.backup`

6. Change the port number in the following files:

- `/usr/local/megha/jetty/start.ini` file.

Change the following:

```
jetty.httpConfig.securePort=<required https port>

jetty.http.port=<required http port>

https.port=<required https port>
```

For example:

```
jetty.httpConfig.securePort=9443

jetty.http.port=8080

https.port=9443
```

- `/usr/local/megha/jetty/etc/jetty-ssl.xml`

Change the following:

```
<Set name="port"><Property name="jetty.ssl.port"
deprecated="ssl.port" default="REQUIRED PORT" /></Set>
```

7. Start the crond service using the command:

```
service crond start
```

8. Start the megha service using the command:

```
/usr/local/megha/bin/megha-jetty.sh start
```

9. After changing the required port number, make sure you open the new port number in the firewall settings.

Enabling strict host name checking between the Analyzer probe server and Analyzer detail view server

When you are connecting the Analyzer probe server to the Analyzer detail view server over HTTPS, you can enable strict host name checking by editing the `custom.properties` file.

After enabling this option, the Analyzer probe server verifies whether the connection destination (IP address or host name) is the same as the `subject alternate name` or `common name` of the SSL certificate that is installed on the Analyzer detail view server. For details on setting up this connection, refer to [Initial setup of Analyzer probe server \(on page 81\)](#).

Before you begin

Verify the following:

- A valid SSL certificate is installed on the Analyzer detail view server in the keystore file (`/usr/local/httpProxy/jetty/etc/`).
- If you are connecting to the Analyzer detail view server using the IP address:
 - The IP address is listed in `subject alternate name` of the SSL certificate on the Analyzer detail view server.
 - If the `subject alternate name` is not provided in the SSL certificate, the IP address must exist in `common name`.
- If you are connecting to the Analyzer detail view server using the host name:
 - The host name exists in `subject alternate name` of the SSL certificate on the Analyzer detail view server.
 - If the `subject alternate name` is not provided in the SSL certificate, the host name must exist in `common name`.
- If the Analyzer probe server cannot resolve the host name, add the valid Analyzer detail view server IP address and host name in the `/etc/hosts` file.



Note: If you install the new SSL certificate or make any changes to the default SSL certificate, then you must restart the HTTP proxy service. Refer to [Restarting the HTTP proxy service \(on page 413\)](#).

Procedure

1. Log on to the Analyzer probe server through an SSH client (like **putty**) as a root user.
2. Stop the `crond` service using the command:

```
service crond stop
```



Note: If you do not want to stop the **crond** service, you can stop the specific processes of the Analyzer detail view server and Analyzer probe server by using the **crontab -e** command as described in [Stopping the Analyzer detail view server or Analyzer probe server services \(on page 360\)](#) and [Starting the Analyzer detail view server or Analyzer probe server services \(on page 360\)](#)

3. Stop all the running services using the command:

```
/usr/local/megha/bin/stop-all-services.sh
```

4. Verify that the following services are stopped by entering these commands:

- Megha

```
/usr/local/megha/bin/megha-jetty.sh status
```

- Crond

```
service crond status
```

5. Go to the `/usr/local/megha/conf/custom.properties` file, add the following property, and save the file:

```
https.strict.hostname.check=true
```

6. Start the megha service using the command:

```
/usr/local/megha/bin/megha-jetty.sh start
```

7. Start the crond service using the command:

```
service crond start
```

Enabling strict host name checking between the Analyzer probe server and Hitachi Enterprise Storage

When you are connecting the Analyzer probe server to Hitachi Enterprise Storage over HTTPS, you can enable strict host name checking by editing the `custom.properties` file.

After enabling this option, the Analyzer probe server verifies if the target host name (used while adding the Hitachi Enterprise Storage probe) is the same as the host name present in the target SSL certificate, and allows the probe addition only after the verification is successful.

Procedure

1. Log on to the Analyzer probe server through an SSH client (like **putty**) as a root user.

2. Stop the crond service using the command:

```
service crond stop
```



Note: If you do not want to stop the **crond** service, you can stop the specific processes of the Analyzer detail view server and Analyzer probe server by using the **crontab -e** command as described in [Stopping the Analyzer detail view server or Analyzer probe server services \(on page 360\)](#) and [Starting the Analyzer detail view server or Analyzer probe server services \(on page 360\)](#)

3. Stop all the running services using the command:

```
/usr/local/megha/bin/stop-all-services.sh
```

4. Verify that the megha and crond services are stopped by entering these commands:

```
/usr/local/megha/bin/megha-jetty.sh status
```

```
service crond status
```

5. Go to the `/usr/local/megha/conf/custom.properties` file, add the following property, and save the file:

```
https.strict.hostname.check.for.target=true
```

6. Start the megha service using the command:

```
/usr/local/megha/bin/megha-jetty.sh start
```

7. Start the crond service using the command:

```
service crond start
```

Deleting an SSL certificate from the Keystore

You can delete a previously imported or expired SSL certificate from the keystore.

Procedure

1. Log on to the Analyzer detail view server or Analyzer probe server through an SSH client (like **putty**) as a root user.
2. Stop the crond service using the command:

```
service crond stop
```



Note: If you do not want to stop the **crond** service, you can stop the specific processes of the Analyzer detail view server and Analyzer probe server by using the **crontab -e** command as described in [Stopping the Analyzer detail view server or Analyzer probe server services \(on page 360\)](#) and [Starting the Analyzer detail view server or Analyzer probe server services \(on page 360\)](#)

3. Stop all the running services using the command:

```
/usr/local/megha/bin/stop-all-services.sh
```

4. Verify that the megha and crond services are stopped by entering these commands:

```
/usr/local/megha/bin/megha-jetty.sh status
```

```
service crond status
```

5. Go to the `/usr/local/megha/jetty/etc` directory and run the following command to get the list of all SSL certificates from keystore file:

```
keytool -list -v -keystore Keystore_File_Name
```

6. Check the expired status of the certificates and note the alias name of expired certificates that you want to delete.
7. Run the following command to delete the certificate from the keystore.

```
keytool -delete -alias Alias_Name -keystore Keystore_File_Name
```



Note: You must use the keystore password of Analyzer detail view server or Analyzer probe server.

8. Run the following command to verify if the certificate is deleted from keystore file.

```
keytool -list -v -keystore Keystore_File_Name
```

9. Start the megha service using the command:

```
/usr/local/megha/bin/megha-jetty.sh start
```

10. Start the crond service using the command:

```
service crond start
```

Configuring an SSL certificate (HTTP Proxy)

Configure an SSL certificate to initiate a secure connection while transferring the data from Analyzer probe server to Analyzer detail view server by creating a private key, creating a certificate signing request (CSR), and applying the server certificate.

Creating a private key and a certificate signing request

Create a certificate signing request (CSR) for Analyzer detail view server and send it to the certificate authority to obtain the certificate file.

Procedure

1. Log on to the Analyzer detail view server through an SSH client (like **putty**) as a root user.
2. Stop the crond service using the command:

```
service crond stop
```



Note: If you do not want to stop the **crond** service, you can stop the specific processes of the Analyzer detail view server and Analyzer probe server by using the **crontab -e** command as described in [Stopping the Analyzer detail view server or Analyzer probe server services \(on page 360\)](#) and [Starting the Analyzer detail view server or Analyzer probe server services \(on page 360\)](#)

3. Stop all the running services using the command:

```
/usr/local/httpProxy/bin/stop-all-services.sh
```

4. Verify that the httpProxy and crond services are stopped by entering these commands:

```
/usr/local/httpProxy/bin/megha-jetty.sh status
```

```
service crond status
```

5. Make a backup copy of the keystore files:

```
cd /usr/local/httpProxy/jetty/etc
cp -p keystore keystore.bak
cp -p jetty-ssl.xml jetty-ssl.xml.bak
cp -p userKeystoreConfig.xml userKeystoreConfig.xml.bak
```



Note: You can use these backup copies if any error occurs during the configuration process.

6. Remove an existing keystore file using the command:

```
rm /usr/local/httpProxy/jetty/etc/keystore
```

7. Create a new keystore and enter the certificate information:

```
keytool -genkey -keyalg RSA -alias jetty -keystore
/usr/local/httpProxy/jetty/etc/keystore
```



Note: The default keystore password for the Analyzer detail view server is `megha.jeos`. If you are using a password other than the default, you must change the following fields in the `/usr/local/httpProxy/jetty/etc/userKeystoreConfig.xml` file:

```
KeyStorePassword
KeyManagerPassword
TrustStorePassword
```

8. Change the ownership to `megha` in the keystore file:

```
chown megha:megha /usr/local/httpProxy/jetty/etc/keystore
```

9. Change the access permission of the keystore file:

```
chmod 640 /usr/local/httpProxy/jetty/etc/keystore
```

10. Create a certificate signing request (CSR) for the `jetty` alias:

```
keytool -certreq -alias jetty -file /tmp/certreq.txt -keystore /usr/local/httpProxy/jetty/etc/keystore
```



Note: You must use the keystore password of the Analyzer detail view server.

11. Create a backup copy of the `jetty` keystore after creating the CSR:

```
cp /usr/local/httpProxy/jetty/etc/keystore /usr/local/httpProxy/jetty/etc/keystoreCSR
```

12. Copy the certificate request file and submit it to the certificate authority:

```
cat /tmp/certreq.txt
```

13. Start the `httpProxy` service using the command:

```
/usr/local/httpProxy/bin/megha-jetty.sh start
```

14. Start the `crond` service using command:

```
service crond start
```

Applying server certificates

The certificate authority creates the following three certificate files:

- Root
- Intermediate
- Host

Procedure

1. Stop the crond service using the command:

```
service crond stop
```



Note: If you do not want to stop the **crond** service, you can stop the specific processes of the Analyzer detail view server and Analyzer probe server by using the **crontab -e** command as described in [Stopping the Analyzer detail view server or Analyzer probe server services \(on page 360\)](#) and [Starting the Analyzer detail view server or Analyzer probe server services \(on page 360\)](#)

2. Stop all the running services using the command:

```
/usr/local/httpProxy/bin/stop-all-services.sh
```

3. Verify that the httpProxy and crond services are stopped by entering these commands:

```
/usr/local/httpProxy/bin/megha-jetty.sh status
```

```
service crond status
```

4. Verify that the following services are stopped by entering these commands:

- **httpProxy**

```
/usr/local/httpProxy/bin/megha-jetty.sh status
```

- **Crond**

```
service crond status
```

5. Upload the certificate files to the Analyzer detail view server. For example, upload them to `/usr/local/httpProxy/jetty/etc`.

- a. Import the Root certificate: You must use the keystore password of the Analyzer detail view server.

```
keytool -import -alias ROOT_CA_NAME -keystore /usr/local/httpProxy/jetty/etc/keystore -trustcacerts -file Path_to_Root_Cert
```

For example, `keytool -import -alias RootCA -keystore /usr/local/httpProxy/jetty/etc/keystore -trustcacerts -file /usr/local/httpProxy/jetty/etc/root.cer`

- b. Import the intermediate certificate: You must use the keystore password of the Analyzer detail view server.

```
keytool -import -alias Intermediate_CA_NAME -keystore /usr/local/httpProxy/jetty/etc/keystore -trustcacerts -file Path_to_Intermediate_CA_Cert
```

```
For example, keytool -import -alias IntermediateCA -
keystore /usr/local/httpProxy/jetty/etc/keystore -
trustcacerts -file /usr/local/httpProxy/jetty/etc/imd.cer
```

- c. Import the Host certificate: You must use the keystore password of the Analyzer detail view server.

```
keytool -import -alias jetty -keystore /usr/local/httpProxy/
jetty/etc/keystore -trustcacerts -file Path_to_host_Cert
```

```
For example, keytool -import -alias jetty -keystore /usr/local/
httpProxy/jetty/etc/keystore -trustcacerts -file /usr/local/
httpProxy/jetty/etc/host.cer
```

6. Start the httpProxy service using the command:

```
/usr/local/httpProxy/bin/megha-jetty.sh start
```

7. Start the crond service using command:

```
service crond start
```

Configuring an SSL certificate (Ops Center Automator)

To use Analyzer server to specify settings for SSL communication with Ops Center Automator, you must first enable SSL on Ops Center Automator. For details, see the section describing how to set up SSL in the *Hitachi Ops Center Automator Installation and Configuration Guide*.

Importing Ops Center Automator certificates to the Analyzer server truststore

To enable the Analyzer server to verify Ops Center Automator certificates, import the certificates to the Analyzer server truststore.

Before you begin

- Prepare the Ops Center Automator certificates. For details, see the section describing how to set up SSL in the *Hitachi Ops Center Automator Installation and Configuration Guide*.
- You must have administrator permissions (for Windows) or root permissions (for Linux).

Procedure

1. Stop the Analyzer server services.
2. Run the following command to import the Ops Center Automator certificates to the truststore:

In Windows

```
Common-component-installation-destination-folder\bin\hcmds64keytool -
import -alias alias-name -file certificate-file-name -keystore
truststore-file-name -storepass truststore-password -storetype JKS
```

In Linux

```
Common-component-installation-destination-directory/uCPSB/jdk/bin/
keytool -import -alias alias-name -file certificate-file-name -
keystore truststore-file-name -storepass truststore-password -
storetype JKS
```



Note:

- For the *alias-name*, specify the name of the host on which the certificate you want to use is located.
- For the *certificate-file-name*, specify the absolute path to the location where the certificate is stored.
- The truststore file is stored in the following location:

In Windows

```
Common-component-installation-destination-folder\uCPSB
\jdk\jre\lib\security\jssecacerts
```

In Linux

```
Common-component-installation-destination-directory/
uCPSB/jdk/jre/lib/security/jssecacerts
```

- The default password to access the truststore is `changeit`.
- You must specify `JKS` for the keystore type of the truststore.

3. To enable the verification of server certificates, change the following properties in the `config_user.properties` file.

- Location:

In Windows

```
Analyzer-server-installation-destination-folder\Analytics\conf
```

In Linux

```
Analyzer-server-installation-destination-directory/Analytics/
conf
```

- Key: `cert.verify.enabled`
- Value: `true`

4. Start the Analyzer server services.

Configuring an SSL certificate (LDAP directory server)

To set up SSL communication with the LDAP directory server in Ops Center Analyzer, you must configure the SSL server on the LDAP directory server and then specify settings in the Analyzer server. For details about SSL configuration on the LDAP directory server, see the manuals about the LDAP directory server.

Importing LDAP directory server certificates to the Analyzer server truststore

To enable the Analyzer server to verify LDAP directory server certificates, import the certificates from the LDAP directory server to the Analyzer server.



Note: 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 truststore.

Before you begin

- The environment settings for connecting with an external authentication server must be completed. For details, see [Configuring LDAP authentication for Analyzer server \(on page 233\)](#).

- Prepare an LDAP directory server certificate.

The certificates issued by all the authorities from the authority that issued an LDAP directory server certificate to the root certificate authority must form a certificate chain. The certificate must satisfy the product requirements for Analyzer server.

- You must have administrator permissions (for Windows) or root permissions (for Linux).

Procedure

1. Stop the Analyzer server services.
2. Run the following command to import certificates for the LDAP directory server to the truststore:

In Windows

```
Common-component-installation-destination-folder\bin\hcmds64keytool -
import -alias alias-name -file certificate-file-name -keystore
truststore-file-name -storepass truststore-password -storetype JKS
```

In Linux

```
Common-component-installation-destination-directory/uCPSB/jdk/bin/
keytool -import -alias alias-name -file certificate-file-name -
```

```
keystore truststore-file-name -storepass truststore-password -  
storetype JKS
```

- For the *alias-name*, specify the name of the host on which the certificate you want to use is located.
- For the *certificate-file-name*, specify the absolute path to the location where the certificate is stored.
- For the *truststore-file-name*, specify the absolute path to the location where the truststore file is stored. If the specified file does not exist, the file is 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`.

The truststore file is stored in the following location:

- `ldapcacerts`

In Windows

`Common-component-installation-destination-folder\conf\sec
\ldapcacerts`

In Linux

`Common-component-installation-destination-directory/
conf/sec/ldapcacerts`

- `jssecacerts`

In Windows

`Common-component-installation-destination-folder\uCPSB\jdk
\jre\lib\security\jssecacerts`

In Linux

`Common-component-installation-destination-directory/
uCPSB/jdk/jre/lib/security/jssecacerts`

- Specify a password for the *truststore-password*.
- You must specify `JKS` for the keystore type of the truststore.

**Note:**

Note the following when you use the `hcmds64keytool` or `keytool` command to specify a unique name in the truststore, the truststore file name, and the password:

- Do not use the following symbols in the file name:
: , ; * ? " < > | -
- Specify the file name as a character string of no more than 255 bytes.
- Do not include double quotation marks (") in the unique name in the truststore or the password.

3. Start the Analyzer server services.
4. Edit the `exauth.properties` file so that Analyzer server can communicate with LDAP directory server by using StartTLS.

Requirements for an LDAP directory server certificate

To use StartTLS to communicate between the Analyzer server and an LDAP directory server, check that the obtained LDAP directory server certificate satisfies the following requirements:

- 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 connects 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 connects with an external authorization server
`auth.kerberos.auth.kerberos.realm_name-property-value.kdc`

Configuring an SSL certificate (Common Services)

To use Analyzer server to specify settings for SSL communication with Ops Center Common Services, you must first enable SSL for Ops Center Common Services. For

details, see the description of SSL communication settings in the *Hitachi Ops Center Installation and Configuration Guide*.

Importing Common Services certificates to the Analyzer server truststore

To enable the Analyzer server to verify Common Services certificates, import the certificates to the Analyzer server truststore.

Before you begin

- Prepare the Common Services certificates. For details, see the description of SSL communication settings in the *Hitachi Ops Center Installation and Configuration Guide*.
- You must have administrator permissions (for Windows) or root permissions (for Linux).

Procedure

1. Stop the Analyzer server services.
2. Run the following command to import the Common Services certificates to the truststore:

In Windows

```
Common-component-installation-destination-folder\bin\hcmds64keytool -  
import -alias alias-name -file certificate-file-name -keystore  
truststore-file-name -storepass truststore-password -storetype JKS
```

In Linux

```
Common-component-installation-destination-directory/uCPSB/jdk/bin/  
keytool -import -alias alias-name -file certificate-file-name -  
keystore truststore-file-name -storepass truststore-password -  
storetype JKS
```

**Note:**

- For the *alias-name*, specify the name of the host on which the certificate you want to use is located.
- For the *certificate-file-name*, specify the absolute path to the location where the certificate is stored.
- The truststore file is stored in the following location:

In Windows

```
Common-component-installation-destination-folder\uCPSB
\jdk\jre\lib\security\jssecacerts
```

In Linux

```
Common-component-installation-destination-directory/
uCPSB/jdk/jre/lib/security/jssecacerts
```

- The default password to access the truststore is `changeit`.
- You must specify `JKS` for the keystore type of the truststore.

3. To enable the verification of server certificates, change the following properties in the `config_user.properties` file.

- Location:

In Windows

```
Analyzer-server-installation-destination-folder\Analytics\conf
```

In Linux

```
Analyzer-server-installation-destination-directory/Analytics/
conf
```

- Key: `cert.verify.enabled`
- Value: `true`

4. Start the Analyzer server services.

Configuring an SSL certificate (RAID Agent)

To initiate a secure session with a host that uses the RAID Agent services, you must create a private key and a certificate signing request (CSR), apply the server certificate, and configure secure communications.

Creating a private key and a certificate signing request for RAID Agent server

Use the `htmsstool` command to create a private key and a certificate signing request (CSR) for RAID Agent.

Before you begin

- You must have the root permission.
- The certificate signing request is created in PEM format. Check with the certificate authority regarding the requirements for the certificate signing request.
- When re-creating a private key, certificate signing request, or self-signed certificate, send the output to a new location. (If a file of the same name exists in the output location, the file cannot be re-created.)

Procedure

1. Log on to the Analyzer probe server through an SSH client (like **putty**).
2. Run the following command to create private keys, certificate signing requests, and self-signed certificates:

```
/opt/jplpc/htnm/bin/htmssltool -key private-key-file-name -csr CSR-  
file-name -cert self-signed-certificate-file-name -certtext name-of-  
the-content-file-of-the-self-signed-certificate
```

Example:

```
/opt/jplpc/htnm/bin/htmssltool -key /root/htnmkey.key -csr /root/  
htnmkey.csr -cert /root/htnmkey.cert -certtext /root/htnmkey.cert.txt
```

Example of response input:

```
Enter Server Name [default=MyHostname]:example.com  
Enter Organizational Unit:Analyzer  
Enter Organization Name [default=MyHostname]:HITACHI  
Enter your City or Locality:Santa Clara  
Enter your State or Province:California  
Enter your two-character country-code:US  
Is CN=example.com,OU=Analyzer,O=HITACHI,L=Santa Clara,ST=California,  
C=US  
correct? (y/n) [default=n]:y
```

**Tip:**

Use a self-signed certificate only to test encrypted communications.

Submitting a certificate signing request (CSR) for RAID Agent

In general, applications for server certificates are submitted online. Create a certificate signing request (CSR) for RAID Agent, and send it to the certificate authority to obtain a digital signature.

Before you begin

Create a certificate signing request for RAID Agent.

You must have a server certificate that was issued in X.509 PEM format by the certificate authority. For details on how to apply, see the website of the certificate authority you use. In addition, make sure the certificate authority supports the signature algorithm.

Procedure

1. Send the created certificate signing request to the certificate authority.
2. Save the server certificate that was issued by the certificate authority in Analyzer probe server.



Note:

For details on how to check the expiration date of the certificate, see [Checking the expiration date of the RAID Agent certificate \(on page 354\)](#).

Enabling SSL communication for RAID Agent

To enable SSL communication that uses the RAID Agent services, edit the `htnm_httpsd.conf` file.

Before you begin

- Prepare the private key file and the server certificate (which was sent from the certificate authority) for RAID Agent.

We recommend that you copy the file to the following location:

- Private key file for RAID Agent
`/opt/jplpc/htnm/HBasePSB/httpsd/conf/ssl/server`
 - Server certificate for RAID Agent (if you are using a certificate from a certificate authority)
`/opt/jplpc/htnm/HBasePSB/httpsd/conf/ssl/cacert`
 - Server certificate for RAID Agent (if you are using a self-signed certificate*)
`/opt/jplpc/htnm/HBasePSB/httpsd/conf/ssl/server`
- *: You can use a self-signed certificate for purposes such as to test encrypted communications.

- Verify the host name specified for `Common Name` in the certificate signing request.

Procedure

1. Run the following command to stop the RAID Agent services.

```
/opt/jplpc/htnm/bin/htmsrv stop -all
```

2. Edit the `/opt/jplpc/htnm/Rest/config/htnm_httpsd.conf` file.
The following is an example of how to edit the `htnm_httpsd.conf` file.

Add a hash mark (#) to the beginning of the lines `Listen 24221` and `SSLDisable` to comment out these lines.

```

ServerName RAID-Agent-server-host-name
#Listen 24221
#Listen [::]:24221
#SSLDisable
Listen 24222
#Listen [::]:24222
SSLEnable
SSLProtocol TLSv12
SSLRequiredCiphers ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-
GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256
SSLRequireSSL
SSLCertificateFile /opt/jplpc/htnm/HBasePSB/httpsd/conf/ssl/server/
httpsd.pem
SSLCertificateKeyFile /opt/jplpc/htnm/HBasePSB/httpsd/conf/ssl/server/
httpsdkey.pem
SSLECCCertificateFile /opt/jplpc/htnm/HBasePSB/httpsd/conf/ssl/
server/ecc-httpsd.pem
SSLECCCertificateKeyFile /opt/jplpc/htnm/HBasePSB/httpsd/conf/ssl/
server/ecc-httpsdkey.pem
#SSLCACertificateFile /opt/jplpc/htnm/HBasePSB/httpsd/conf/ssl/cacert/
anycert.pem
HWSLogSSLVerbose On

```

Uncomment the lines from `#Listen 24222` to `#HWSLogSSLVerbose On`, by removing the hash mark (#).



Note: Keep the lines `#Listen [::]:24221` and `#Listen [::]:24222` commented out, because Ops Center Analyzer does not support IPv6.

- For the `ServerName` directive in the first line, enter the host name that you specified for `Common Name` in the certificate signing request. (Host names are case sensitive.)
- For RSA cryptography, specify the absolute paths of the secret key and the server certificate of RAID Agent for the following directives.
 - `SSLCertificateKeyFile`
 - `SSLCertificateFile`

For elliptic curve cryptography, specify the absolute paths of the secret key and the server certificate of RAID Agent for the following directives.

- `SSLECCCertificateKeyFile`
- `SSLECCCertificateFile`
- If the server certificate for RAID Agent originated from an intermediate certificate authority, remove the hash mark (#) from the beginning of the line of the `SSLCACertificateFile` directive, and then specify the absolute path of all server certificates issued by the intermediate certificate authorities. You can include multiple certificates in a single file by using a text editor to chain those certificates.

Note the following:

- Do not edit the `httpsd.conf`, `hssso_httpsd.conf`, or `user_hssso_httpsd.conf` files.
 - Do not specify the same directive twice.
 - Do not enter a line break in the middle of a directive.
 - When specifying paths in the directives listed below, do not specify symbolic links or junction points.
 - When specifying certificates and private key files in the directives listed below, specify PEM-format files.
3. Run the following command to start the RAID Agent services.

```
/opt/jplpc/htnm/bin/htmsrv start -all
```

Checking the expiration date of the RAID Agent certificate

To check the expiration date of the RAID Agent server certificate or a certificate issued by a certificate authority, use the **keytool** command.

Procedure

1. Check the expiration date using the command:

```
keytool -printcert -v -file certificate-file-name
```

For *certificate-file-name*, specify the location of the certificate file as an absolute path.

Example:

```
keytool -printcert -v -file /opt/jplpc/htnm/HBasePSB/httpsd/conf/ssl/cacert/htnmcert.crt
```

Importing RAID Agent certificates to the Analyzer server truststore

To enable the Analyzer server to verify RAID Agent certificates, import the certificates to the Analyzer server truststore and edit the `config_user.properties` file.

Before you begin

You must have administrator permissions (for Windows) or root permissions (for Linux).

Procedure

1. Stop the Analyzer server services.
2. Run the following command to import the certificates for RAID Agent to the truststore file:

In Windows

```
Common-component-installation-destination-folder\bin\hcmds64keytool -import -alias alias-name -file certificate-file-name -keystore truststore-file-name -storepass truststore-password -storetype JKS
```

In Linux

```
Common-component-installation-destination-directory/uCPSB/jdk/bin/keytool -import -alias alias-name -file certificate-file-name -keystore truststore-file-name -storepass truststore-password -storetype JKS
```

**Note:**

- For the *alias-name*, specify a name that identifies whether the certificate is the certificate for RAID Agent.
- For the *certificate-file-name*, specify the absolute path.
- The truststore file is stored in the following location:

In Windows

```
Common-component-installation-destination-folder\uCPSB
\jdk\jre\lib\security\jssecacerts
```

In Linux

```
Common-component-installation-destination-directory/
uCPSB/jdk/jre/lib/security/jssecacerts
```

- The password to access the default truststore is `changeit`.
- You must specify `JKS` for the keystore type of the truststore.

3. To enable the verification of server certificates, change the following properties in the `config_user.properties` file:

- Location:

In Windows

```
Analyzer-server-installation-destination-folder\Analytics\conf
```

In Linux

```
Analyzer-server-installation-destination-directory/Analytics/
conf
```

- Key: `cert.verify.enabled`
- Value: `true`

4. Start the Analyzer server services.

Importing RAID Agent certificates to the Analyzer probe server truststore

To enable the Analyzer probe server to verify RAID Agent certificates, import the certificates to the Analyzer probe server truststore.

Before you begin

You must have root permissions.

Procedure

1. Log on to the Analyzer probe server through an SSH client (like `putty`).
2. Use the following command to stop the `crond` service:

```
service crond stop
```



Note: If you do not want to stop the **crond** service, you can stop the specific processes of the Analyzer detail view server and Analyzer probe server by using the **crontab -e** command as described in [Stopping the Analyzer detail view server or Analyzer probe server services \(on page 360\)](#) and [Starting the Analyzer detail view server or Analyzer probe server services \(on page 360\)](#)

3. Use the following command to stop the megha service:

```
/usr/local/megha/bin/megha-jetty.sh stop
```

4. Run the following commands to verify that the services have been stopped:

- **Megha**

```
/usr/local/megha/bin/megha-jetty.sh status
```

- **Crond**

```
service crond status
```

5. Import the certificate for RAID Agent: You must use the keystore password of the Analyzer probe server.

```
keytool -import -alias alias-name -keystore /usr/local/megha/jetty/etc/keystore -trustcacerts -file certificate-file-name
```

Example:

```
keytool -import -alias RAIDAgent -keystore /usr/local/megha/jetty/etc/keystore -trustcacerts -file htnmcert.crt
```



Note:

- For *alias-name*, specify a name by which the certificate can be identified as the certificate for RAID Agent.
- For the *certificate-file-name*, specify the absolute path.

6. Use the following command to start the megha service:

```
/usr/local/megha/bin/megha-jetty.sh start
```

7. Use the following command to start the crond service:

```
service crond start
```

Chapter 12: Changing Ops Center Analyzer system settings

You can start and stop Ops Center Analyzer services, change, and enable system account locking.

Starting and stopping the Ops Center Analyzer services

Start and stop the Ops Center Analyzer services with the **hcnds64srv** command.

Starting the Analyzer server services

To start the Analyzer server services, run the **hcnds64srv** command.

Before you begin

You must have Administrator permission (Windows) or root permission (Linux).

Procedure

1. Run the following command:

For Windows:

```
Common-component-installation-destination-folder\bin\hcnds64srv /start
```

For Linux:

```
Common-component-installation-destination-directory/bin/hcnds64srv -  
start
```

**Note:**

- For Windows, do not use Service Control Manager to start the services.
- To stop or start only the Analyzer server services when the Common component services are running, specify `-server AnalyticsWebservice` in the command.
- When you restart the Analyzer server services, the status of monitored resources can be delayed for 5 minutes or longer. During this time, the status displays as **Unknown**.

Stopping the Analyzer server services

To stop the services, run the `hcnds64srv` command.

Before you begin

You must have Administrator permission (Windows) or root permission (Linux).

Procedure

1. Run the following command:

For Windows:

```
Common-component-installation-destination-folder\bin\hcnds64srv /stop /
server server-name
```

For Linux:

```
Common-component-installation-destination-directory/bin/hcnds64srv -
stop -server server-name
```

**Note:**

- For Windows, do not use Service Control Manager to stop the service. Doing so might cause the process to fail
- To stop or start only the Analyzer server services when the Common component service is running, specify `-server AnalyticsWebservice` in the command.
- When you restart the Analyzer server services, the status of monitored resources can be delayed for 5 minutes or longer. During this time, the status displays as **Unknown**.

Starting the Analyzer detail view server or Analyzer probe server services

Start the Analyzer detail view server or Analyzer probe server services by editing `crontab`.

Before you begin

Log on to the Analyzer detail view server or Analyzer probe server as the root user.

Procedure

1. Run the `crontab -e` command.
2. Delete the hash marks (#) from the beginning of each line as shown in this example:

```
* /5 * * * * F=/usr/local/megha/cron.5min; test -f $F && bash $F
13 0 * * * F=/usr/local/megha/cron.1hr; test -f $F && bash $F
11 * * * * F=/usr/local/megha/cron.24hr; test -f $F && bash $F
* /5 * * * * F=/usr/local/megha/bin/sysstat.sh; test -f $F && (bash $F
>> /usr/local/megha/logs/sys/`date +%Y%m%d`.log)
```

3. Start the megha service using the command:

```
/usr/local/megha/bin/megha-jetty.sh start
```

4. Confirm the megha service has started:

```
/usr/local/megha/bin/megha-jetty.sh status
```

Stopping the Analyzer detail view server or Analyzer probe server services

Stop the Analyzer detail view server or Analyzer probe server services by editing `crontab`.

Before you begin

Log on to the Analyzer detail view server or Analyzer probe server as the root user.

Procedure

1. Run the `crontab -e` command.
2. At the beginning of each line add a hash mark (#) to comment out a line as shown in this example:

```
# * /5 * * * * F=/usr/local/megha/cron.5min; test -f $F && bash $F
# 13 0 * * * F=/usr/local/megha/cron.1hr; test -f $F && bash $F
# 11 * * * * F=/usr/local/megha/cron.24hr; test -f $F && bash $F
```



```
* /5 * * * * F=/usr/local/megha/bin/sysstat.sh; test -f $F && (bash
$F >> /usr/local/megha/logs/sys/`date +%Y%m%d`.log)
```

3. Stop all services using the command:

```
/usr/local/megha/bin/stop-all-services.sh
```

4. Confirm the megha service has stopped:

```
/usr/local/megha/bin/megha-jetty.sh status
```

Starting the RAID Agent services

Start the RAID Agent services when creating or deleting an instance environment for RAID Agent.



Note:

This procedure is applicable for RAID Agent installed with Ops Center Analyzer. If you are using Tuning Manager - Agent for RAID, see the *Hitachi Command Suite Tuning Manager Agent Administration Guide*.

Before you begin

Log on as the root user to the host where RAID Agent is installed, or use the **su** command to assume root user privileges.

Procedure

To start services manually:

1. Run the following command:

```
/opt/jplpc/htnm/bin/htmsrv start -all
```

2. If you are starting the services after performing a restore operation, check `htmRestDbEngineMessage#.log` (# refers to the log file number) of the RAID Agent to make sure that the KATR13248-E message is not logged before KATR13244-I is output.

Note that it might take about one hour from when the RAID Agent service starts until the KATR13244-I message is output.

If the KATR13248-E message is logged, restoration of RAID Agent might have failed. Check whether the prerequisites for restoration are met. If there is a problem, restore the entire RAID Agent system again.

The `htmRestDbEngineMessage#.log` is located in `/opt/jplpc/htnm/logs`.

To start services automatically:

1. Run the following command:

```
cd /opt/jplpc
```

2. Set the service automatic start script file for the RAID Agent.

- Name of the .model file of the service automatic start script:
jpc_start.model
- Name of the service automatic start script file: jpc_start

3. Copy the .model file to the service automatic start script file to add execution permission.

```
cp -p jpc_start.model jpc_start
chmod 555 jpc_start
```

4. Register the RAID Agent services in the OS (in Red Hat Enterprise Linux 7 and Oracle Linux 7 only).

- a. Edit the service automatic start script (/etc/rc.d/init.d/jpl_pc).

Original file content:

```
#!/bin/sh
## Copyright (C) 2004, Hitachi, Ltd.
## Licensed Material of Hitachi, Ltd.
:
```

Revised file content:

```
#!/bin/sh
## Copyright (C) 2004, Hitachi, Ltd.
## Licensed Material of Hitachi, Ltd.
### BEGIN INIT INFO
# Provides: jpl_pc
# Required-Start: $local_fs $remote_fs $syslog $network
# Required-Stop: $local_fs $remote_fs $syslog $network
# Default-Start: 3 5
# Default-Stop: 0 6
# Description: Start RAID Agent services.
### END INIT INFO
:
```

- b. Execute the following command:

```
chkconfig jpl_pc on
```

Stopping the RAID Agent services

Do the following steps to stop the RAID Agent services.



Note:

This procedure is applicable for RAID Agent installed with Ops Center Analyzer. If you are using Tuning Manager - Agent for RAID, see the *Hitachi Command Suite Tuning Manager Agent Administration Guide*.

Before you begin

- Log on as the root user to the host where RAID Agent is installed, or use the `su` command to assume root user privileges.
- When you enable the automatic service stop feature in Red Hat Enterprise Linux 7, or Oracle Linux 7, you must also enable the automatic start feature.

Procedure

To stop services manually:

1. Run the following command:

```
/opt/jplpc/htnm/bin/htmsrv stop -all
```

To stop services automatically:

1. Run the following command:

```
cd /opt/jplpc
```

2. Set the service automatic stop script file for the RAID Agent.

- Name of the `.model` file of the service automatic stop script:
`jpc_stop.model`
- Name of the service automatic stop script file: `jpc_stop`

Copy the `.model` file of the service automatic stop script to the service automatic stop script file to add execution permission. Run the command as follows:

```
cp -p jpc_stop.model jpc_stop
chmod 555 jpc_stop
```

3. To apply the settings, execute the following command to start the RAID Agent services (in Red Hat Enterprise Linux 7 and Oracle Linux 7 only):

```
systemctl start jpl_pc
```

If you do not execute this command, automatic stop processing will fail for the first service that is run after the settings were specified.

Changing the system information of Analyzer server

For a host where Analyzer server is installed, you can change the host name, IP address, time settings, format of syslog output, and the port number used for connection with Analyzer server.

Changing the Analyzer server host name

After stopping Analyzer server services by running the **hcnds64srv** command, change the host name of the Analyzer server.

Before you begin

You must have Administrator permission (Windows) or root permission (Linux).

Procedure

1. Run the **hcnds64srv** command with the **stop** option to stop the Analyzer server services.
2. Change the host name on the OS of the Analyzer server.
3. Change the host name specified in **ServerName** in the **user_httpsd.conf** file.

In Windows

Common-component-installation-destination-folder\uCPSB\httpsd\conf\user_httpsd.conf

In Linux

Common-component-installation-destination-directory/uCPSB/httpsd/conf/user_httpsd.conf

4. If Ops Center Analyzer is registered to Common Services by using a host name, run the **setupcommonservice** command to update the host name.

```
setupcommonservice -appHostname new-host-name
```

5. Restart the OS of the host on which the Analyzer server is installed.
6. If you use Linux, verify that the IP address can be resolved from the host name of the Analyzer server.
7. If a RADIUS server is used to perform user authentication and the host name before the change is set for the **attr.NAS-Identifier** property in the **exauth.properties** file, change the host name to the new host name.

The **exauth.properties** file is stored in the following location:

In Windows:

Common-component-installation-destination-folder\conf\exauth.properties

In Linux:

Common-component-installation-destination-directory/conf/exauth.properties

8. If Ops Center Automator is connected with the Analyzer server and the Analyzer server is set as the primary server, perform the following procedure on the host on which Ops Center Automator is installed to apply the changed host name.
 - a. Run the **hcnds64prmset** command to change the Common component settings.
 - b. Restart Ops Center Automator.

Changing the Analyzer server IP address

After stopping Analyzer server services by running the **hcnds64srv** command, change the IP address of the Analyzer server.

Before you begin

You must have Administrator permission (Windows) or root permission (Linux).

Procedure

1. Run the **hcnds64srv** command with the **stop** option to stop Analyzer server services.
2. Change the IP address on the OS of the Analyzer server.
3. If Ops Center Analyzer is registered to Common Services by using an IP address, run the **setupcommonservice** command to update the IP address.

```
setupcommonservice -appHostname new-IP-address
```

4. Restart the OS of the host on which the Analyzer server is installed.
5. If you use Linux, verify that the IP address can be resolved from the host name of the Analyzer server.
6. If a RADIUS server is used to perform user authentication and the IP address before the change is set for the `attr.NAS-IP-Address` property in the `exauth.properties` file, change the IP address to the new IP address.

The `exauth.properties` file is stored in the following location:

In Windows:

```
Common-component-installation-destination-folder\conf  
exauth.properties
```

In Linux:

```
Common-component-installation-destination-directory/conf/  
exauth.properties
```

7. If Ops Center Automator is connected with the Analyzer server and the Analyzer server is set as the primary server, perform the following procedure on the host on which Ops Center Automator is installed to apply the changed IP address.
 - a. Run the **hcnds64prmset** command to change the Common component settings.
 - b. Restart Ops Center Automator.

Changing the port number used between Analyzer server and the web browser (Linux)

To change the port number used between Analyzer server and the web browser, change the port numbers specified in the definition files, then register the firewall exceptions. Note that, if SSL communication is used between the Analyzer server and the web browser, refer to the procedure for changing port numbers for SSL communication.

Before you begin

You must have the root permission.

Procedure

1. Run the **hcmd64srv** command with the **stop** option to stop Analyzer server services.
2. Change the port numbers in the following definition files:

- *Common-component-installation-destination-directory*/uCPSP/httpsd/conf/user_httpsd.conf

Change the following three lines. The default port number is 22015.

```
#Listen [::]:22015
Listen 22015
#Listen 127.0.0.1:22015
```

- *Analyzer-server-installation-destination-directory*/Analytics/conf/command_user.properties

Change the following line:

```
command.http.port = 22015
```

3. Register the firewall exceptions.

- In Linux (version 6)

Run the **iptables** command to register Linux firewall exceptions.

- a. Open the firewall settings file (*/etc/sysconfig/iptables*), for example by using a text editor.
- b. Insert the following line before the line "--reject-with icmp-host-prohibited":

```
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --
dport port-number -j ACCEPT
```

**Note:**

- Make sure that you enter the entire text in one line.
- For *port-number*, enter the number of the port to be opened.
- You must specify this setting for each port number.

- Overwrite the firewall settings file to save the settings.
- Restart the service.

Execute the following command on the console:

```
/etc/rc.d/init.d/iptables restart
```

- In Linux (version 7)

Use the **firewall-cmd** command to specify the port number used by Analyzer server for the port that has the zone applied.

- Specify the service name to be enabled for the port that has the zone applied.

The following shows an example of specifying the service name in the default zone, and enabling the settings even after the OS is restarted:

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



Note: For *service-name*, specify `http`.

- For the port that has the zone applied, specify a combination of the port number to use in Analyzer server (as the permitted port number for communication) and the protocol for that port number.

The following shows an example of specifying a combination of the port number and protocol in the default zone, and enabling the settings even after the OS is restarted:

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

**Note:**

- For *port-number*, specify the port number to use in Analyzer server.
- For *protocol*, specify `tcp` or `udp`.

- Run the **hcmds64srv** command with the `start` option to start the Analyzer server services.
- If Ops Center Automator is connected with the Analyzer server and the Analyzer server is set as the primary server, perform the following procedure on the host on which Ops Center Automator is installed to apply the changed port number.

- a. Run the **hcnds64prmsset** command to change the Common component settings.
- b. Restart Ops Center Automator.

Changing the SSL port number between the Analyzer server and a web browser (Linux)

To change the port number for SSL Communication, change the port numbers specified in the definition files, then register the firewall exceptions.

Before you begin

You must have the root permission.

Procedure

1. Run the **hcnds64srv** command with the **stop** option to stop Analyzer server services.
2. Change the port numbers in the following definition files:

- *Common-component-installation-destination-directory*/uCPSP/httpsd/conf/user_httpsd.conf

Change the following three lines. The default port number is 22016.

```
#Listen [::]:22016
Listen 22016
<VirtualHost *:22016>
```

- *Analyzer-server-installation-destination-directory*/Analytics/conf/command_user.properties

Change the following line:

```
command.https.port = 22016
```

3. Register the firewall exceptions.

- In Linux (version 6)

Run the **iptables** command to register Linux firewall exceptions.

- a. Open the firewall settings file (*/etc/sysconfig/iptables*), for example by using a text editor.
- b. Insert the following line before the line "**--reject-with icmp-host-prohibited**":

```
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --
dport port-number -j ACCEPT
```


**Note:**

- Make sure that you enter the entire text in one line.
- For *port-number*, enter the number of the port to be opened.
- You must specify this setting for each port number.

- Overwrite the firewall settings file to save the settings.
- Restart the service.

Execute the following command on the console:

```
/etc/rc.d/init.d/iptables restart
```

- In Linux (version 7)

Use the **firewall-cmd** command to specify the port number used by Analyzer server for the port that has the zone applied.

- Specify the service name to be enabled for the port that has the zone applied.

The following shows an example of specifying the service name in the default zone, and enabling the settings even after the OS is restarted:

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



Note: For *service-name*, specify `https`.

- For the port that has the zone applied, specify a combination of the port number to use in Analyzer server (as the permitted port number for communication) and the protocol for that port number.

The following shows an example of specifying a combination of the port number and protocol in the default zone, and enabling the settings even after the OS is restarted:

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

**Note:**

- For *port-number*, specify the port number to use in Analyzer server.
- For *protocol*, specify `tcp` or `udp`.

- If you are using Common Services, run the **setupcommonservice** command to update the port number.

```
setupcommonservice -appPort new-port-number
```

5. Run the **hcnds64srv** command with the `start` option to start the Analyzer server services.
6. If Ops Center Automator is connected with the Analyzer server and the Analyzer server is set as the primary server, perform the following procedure on the host on which Ops Center Automator is installed to apply the changed port number.
 - a. Run the **hcnds64prmset** command to change the Common component settings.
 - b. Restart Ops Center Automator.

Changing the port number used between Analyzer server and the web browser (Windows)

To change the port number used between Analyzer server and the web browser, change the port numbers specified in the definition files, then register the firewall exceptions. Note that, if SSL communication is used between the Analyzer server and the web browser, refer to the procedure for changing port numbers for SSL communication.

Before you begin

You must have the Administrator permission.

Procedure

1. Run the **hcnds64srv** command with the `stop` option to stop Analyzer server services.
2. Change the port numbers in the following definition files:
 - `Common-component-installation-destination-folder\uCPSB\httpsd\conf\user_httpsd.conf`

Change the following three lines. The default port number is 22015.

```
#Listen [::]:22015
Listen 22015
#Listen 127.0.0.1:22015
```

- `Analyzer-server-installation-destination-folder\Analytics\conf\command_user.properties`

Change the following line:

```
command.http.port = 22015
```

3. Change the shortcut to the program as follows:



Note: The default URL is:

```
http://localhost:22015/Analytics/
```

For Windows Server 2012

- a. From the desktop, display the **Start** window.
 - b. Right-click the **Start** window to display **All apps**.
 - c. Display the properties of **Analyzer Login** in the **Hitachi Ops Center Analyzer** folder.
 - d. In the **Web Document** tab, change the port number of the URL specified in **URL**.
4. Run the **hcnds64fwcancel** command to register Windows-based firewall exceptions.
5. Run the **hcnds64srv** command with the `start` option to start the Analyzer server services.
6. If Ops Center Automator is connected with the Analyzer server and the Analyzer server is set as the primary server, perform the following procedure on the host on which Ops Center Automator is installed to apply the changed port number.
 - a. Run the **hcnds64prmset** command to change the Common component settings.
 - b. Restart Ops Center Automator.

Changing the SSL port number between the Analyzer server and a web browser (Windows)

To change the port number for SSL Communication, change the port numbers specified in the definition files, then register the firewall exceptions.

Before you begin

You must have the Administrator permission.

Procedure

1. Run the **hcnds64srv** command with the `stop` option to stop Analyzer server services.

2. Change the port numbers in the following definition files:

- *Common-component-installation-destination-folder*\uCPSPB\httpsd\conf\user_httpsd.conf

Change the following three lines. The default port number is 22016.

```
#Listen [::]:22016
Listen 22016
<VirtualHost *:22016>
```

- *Analyzer-server-installation-destination-folder*\Analytics\conf\command_user.properties

Change the following line:

```
command.https.port = 22016
```

3. Change the shortcut to the program as follows:

For Windows Server 2012

- a. From the desktop, display the **Start** window.
 - b. Right-click the **Start** window to display **All apps**.
 - c. Display the properties of **Analyzer Login** in the **Hitachi Ops Center Analyzer** folder.
 - d. In the **Web Document** tab, change the port number of the URL specified in **URL**.
4. Run the **hcnds64fwcancel** command to register Windows-based firewall exceptions.
 5. If you are using Common Services, run the **setupcommonservice** command to update the port number.

```
setupcommonservice /appPort new-port-number
```

6. Run the **hcnds64srv** command with the **start** option to start the Analyzer server services.
7. If Ops Center Automator is connected with the Analyzer server and the Analyzer server is set as the primary server, perform the following procedure on the host on which Ops Center Automator is installed to apply the changed port number.
 - a. Run the **hcnds64prmset** command to change the Common component settings.
 - b. Restart Ops Center Automator.

Changing the port number used between Analyzer server and Common component

To change the port number used between the Analyzer server and Common component, edit the `worker.properties` file.

Before you begin

You must have Administrator permission (Windows) or root permission (Linux).

Procedure

1. Run the `hcmds64srv` command with the `stop` option to stop the Analyzer server services.
2. Edit the following definition files:

In Windows

- `Common-component-installation-destination-folder\uCPSB\CC\web\redirector\workers.properties`

Change the port number in the following line:

```
worker.AnalyticsWebService.port=27100
```

- `Common-component-installation-destination-folder\uCPSB\CC\web\containers\AnalyticsWebService\usrconf\usrconf.properties`

Change the port number in the following lines:

```
      :
webserver.connector.ajp13.port=27100
      :
webserver.shutdown.port=27101
      :
```

In Linux

- `Common-component-installation-destination-directory/uCPSB/CC/web/redirector/workers.properties`

Change the port number in the following line:

```
worker.AnalyticsWebService.port=27100
```

- `Common-component-installation-destination-directory/uCPSB/CC/web/containers/AnalyticsWebService/usrconf/usrconf.properties`

Change the port number in the following lines:

```
:
webserver.connector.ajp13.port=27100
:
webserver.shutdown.port=27101
:
```

3. Run the `hcmds64srv` command with the `start` option to start the Analyzer server services.

Changing the port number between Analyzer server and the SMTP server

You can change the port number used between Analyzer server and the SMTP server in the **Email Server Settings** window.

Before you begin

Make sure you have the Admin permission of Analyzer server.

Procedure

1. In the **Administration** tab, select **Notification Settings > Email Server**.
2. Click **Edit Settings** and enter the new port number in **Port Number**, and then click **Save Settings**.

Changing the time settings of the Analyzer server

Stop the Analyzer server services using the `hcmds64srv` command, and then change the time settings of the Analyzer server.

Before you begin

You must have Administrator permission (Windows) or root permission (Linux).

Procedure

1. Run the **hcnds64srv** command with the `stop` option to stop Analyzer server services.
2. Change the time setting of the Analyzer server.
If you change the server time to a time that is earlier than the current server time, wait until the new server time exceeds the previous server time (the server time before you changed the settings).
3. Run the **hcnds64srv** command with the `start` option to start the Analyzer server services.

Change the format of syslog output

When using Analyzer server, you can output records of user operations to syslog.

Syslogs are saved in the following format:

```
syslog-header-message message-part
```

The format of the *syslog-header-message* differs depending on the OS environment settings. If necessary, change the settings.

For example, if you use rsyslog and specify the following in `/etc/rsyslog.conf`, messages are output in a format corresponding to RFC5424:

```
$ActionFileDefaultTemplate RSYSLOG_SyslogProtocol23Format
```

Moving an Analyzer server installation to another host

To move Analyzer server to a host that has a different host name or IP address than that of the source host, first change the host name and IP address of the destination host to match those of the source host. After doing a restore operation, change the host name and IP address of the destination host back to their original values.

Before you begin

- Stop the Analyzer server services on the source server.
- Verify that the following items are the same on the source server and the destination server:
 - System locale
 - Environment for Hitachi Command Suite products (configuration and version number)
- Verify that Analyzer server is not installed on the destination server.



Note: Ops Center Analyzer does not support data migration for Ops Center Analyzer between Windows and Linux hosts.

Procedure

1. Back up Analyzer server on the source server.
2. Change the host name and IP address of the destination host to match those of the source host.
3. Install Analyzer server on the destination server.
The migration-destination directory of Analyzer server must be the same on both the destination host and the source host.
4. Restore Analyzer server on the destination server.
5. Restore the original host name and IP address of the destination host by following the procedure for changing host names and IP addresses.
6. Verify that the destination server is running and then start operation.

Result

Analyzer server is migrated to the destination host.

Changing the primary server information

When Ops Center Automator is connected, the host on which Device Manager is installed is set as the primary server, and the host on which the Analyzer server is installed is set as the secondary server, if the host name, IP address, or port number of the primary server is changed, you must change the information on the primary server that is configured on the secondary server.

Before you begin

You must have Administrator permission (Windows) or root permission (Linux).

Procedure

1. Run the **hcnds64prmset** command to change the settings of the Common component.

- When changing the host name or IP address:

In Windows

```
Common-component-installation-destination-folder\bin\hcnds64prmset /
host host-name-or-IP-address-of-Device-Manager
```

In Linux

```
Common-component-installation-destination-directory/bin/
hcnds64prmset -host host-name-or-IP-address-of-Device-Manager
```

- When changing the port number:

In Windows

```
Common-component-installation-destination-folder\bin\hcnds64prmset
{/port port-number-for-non-SSL-communication | /sslport port-number-
for-SSL-communication}
```

In Linux

```
Common-component-installation-destination-directory/bin/
hcnds64prmset {-port port-number-for-non-SSL-communication | -
sslport port-number-for-SSL-communication}
```

Specify either the `port` option or the `sslport` option according to the SSL communication setting of Device Manager.

2. Stop and restart the services:
 - a. Run the **hcnds64srv** command with the `stop` option to stop the Analyzer server services.
 - b. Run the **hcnds64srv** command with the `start` option to start the Analyzer server services.

Setting the domain to permit cross-domain access

Access to Ops Center Analyzer is only permitted from domains for which communication is explicitly permitted by using the Cross-Origin Resource Sharing (CORS) mechanism. You do not have to be aware of the settings to directly access Analyzer server using a web browser. However, if you must use cross-domain access, such as when configuring your own system or services by using the REST API for Ops Center Analyzer, you must use CORS to configure settings for the domain for which communication is to be permitted.

Procedure

1. Open the following CORS settings file:

In Windows

```
Analyzer-server-installation-destination-folder\Analytics\conf
\config_cors_origin.txt
```

In Linux

```
Analyzer-server-installation-destination-directory/Analytics/
conf/config_cors_origin.txt
```

2. Enter each domain for which access is to be permitted on a separate line, such as in the following format. To permit access for all domains, specify an asterisk (*).

```
http-or-https://host-name-or-IP-address:port-number
```

Example settings:

```
http://172.30.195.118:80
https://host2:8080
```

3. Restart the Analyzer server services.

Changing the system information of Analyzer probe server

You can change system information such as the host name of the Analyzer probe server, the IP address of the Analyzer probe server, the port number used by the RAID Agent, and the port number used by the RAID Agent REST Web Service.

Changing the Analyzer probe server host name when the Hitachi Enterprise Storage probe is added

Change the host name of the host where the Analyzer probe server is installed. Because RAID Agent is also installed on the host where the Analyzer probe server is installed, change the host name by performing the following procedure if the Hitachi Enterprise Storage probe is added.

**Note:**

This procedure is applicable for RAID Agent installed with Ops Center Analyzer. If you are using Tuning Manager - Agent for RAID, see *Hitachi Command Suite Tuning Manager Installation Guide* and *Hitachi Command Suite Tuning Manager Agent Administration Guide*.

If you are using Tuning Manager - Agent for RAID, be sure to re-specify the settings of the Hitachi Enterprise Storage probe and other settings, similar to when using the RAID Agent installed with Ops Center Analyzer.

Procedure

1. Perform the following steps to stop the Analyzer probe server services:

- a. Run the following command:

```
crontab -e
```

- b. At the beginning of each line in the ordinary execution schedule that was output for the Analyzer probe server, add a hash mark (#) to comment out each line:

```
# */5 * * * * F=/usr/local/megha/cron.5min; test -f $F && bash $F
# 13 0 * * * F=/usr/local/megha/cron.1hr; test -f $F && bash $F
# 11 * * * * F=/usr/local/megha/cron.24hr; test -f $F && bash $F
# */5 * * * * F=/usr/local/megha/bin/sysstat.sh; test -f $F &&
(bash $F >> /usr/local/megha/logs/sys/`date +%Y%m%d`.log)
```

- c. Run the following command to stop the services:

```
/usr/local/megha/bin/megha-jetty.sh stop
```

2. Run the following command to stop the RAID Agent services.

```
/opt/jplpc/htnm/bin/htmsrv stop -all
```

3. Change the monitoring host name of the RAID Agent. The monitoring host name refers to the unique host name that is used to identify internal RAID Agent services.

Execute the **jpccconf host hostname** command to change the monitoring host name.

The following example of the command changes the physical host name to **host02**:

```
/opt/jplpc/tools/jpccconf host hostname -newhost host02 -d /root/backup
-dbconvert convert
```

Do not execute any other commands during the execution of the **jpccconf host hostname** command.



Tip: If execution of the command fails, the RAID Agent configuration file is stored in the directory specified for the **-d** option of the **jpccconf host hostname** command. If execution of the command fails, collect all of the stored configuration files, and then contact the system administrator or Hitachi Vantara Support Contact.

4. Edit the **htnm_httpsd.conf** file to specify the new host name of the Analyzer probe server for the **ServerName** directive on the first line. Make sure that you will specify the same name (case sensitive) for the physical host.

The **htnm_httpsd.conf** file is stored in the following location:

```
/opt/jplpc/htnm/Rest/config/htnm_httpsd.conf
```

5. If the servers that can access RAID Agent are limited (the access source restriction function is configured), change the host name of the Analyzer probe server defined in the `htnm_httpsd.conf` file to the new host name.
6. Change the physical host name of the host on which Analyzer probe server is installed.
7. The IP address must be able to be resolved from the host name of the host on which Analyzer probe server is installed. After changing the physical host name, check the `hosts` file or the domain name system (DNS) server configuration of the host on which Analyzer probe server is installed.
8. Run the following command to start the RAID Agent services.



Note: If the service automatic startup script is configured, when you restart the OS after changing the host name, the services will start automatically.

```
/opt/jplpc/htnm/bin/htmsrv start -all
```

9. Perform the following steps to start the Analyzer probe server services:
 - a. Run the following command:

```
crontab -e
```

- b. Delete the hash marks (#) from the beginning of each line in the ordinary execution schedule that generates output for the Analyzer probe server:

```
*/5 * * * * F=/usr/local/megha/cron.5min; test -f $F && bash $F
13 0 * * * F=/usr/local/megha/cron.1hr; test -f $F && bash $F
11 * * * * F=/usr/local/megha/cron.24hr; test -f $F && bash $F
*/5 * * * * F=/usr/local/megha/bin/sysstat.sh; test -f $F && (bash
$F >> /usr/local/megha/logs/sys/`date +%Y%m%d`.log)
```

- c. Run the following command:



Note: If the service automatic startup script is configured, when you restart the OS after changing the host name, the services will start automatically.

```
/usr/local/megha/bin/megha-jetty.sh start
```

10. Change the settings of Hitachi Enterprise Storage probe as follows:
 - a. On the Analyzer probe server home page, stop the target probe and click **Edit**.
 - b. In the **Edit Hitachi Enterprise Storage Probe** section, enter the host name of the machine on which the RAID Agent is installed in the **RAID Agent Hostname** field. Then, click **Next**.
 - c. In the **Validating Hitachi Enterprise Storage Probe details** window, click **Next**, and then click **OK**.
 - d. In the **Status** window, in **ACTION**, click **Start** to start collecting data.

11. To use the API functions that access RAID Agent, manually refresh the Agent list from the API client.

For details about how to manually refresh the Agent list, see the *Hitachi Ops Center Analyzer REST API Reference Guide*.

12. Log on to Analyzer detail view server, and then verify that data is collected.
 - a. Log on to Analyzer detail view server.
 - b. Click the **Server Status** icon.
 - c. Verify that the probe appears in **Last Configuration Import Time** and **Last Performance Import Time** of **Data Import Status**, and that data is collected.



Note: It might take some time before the probe appears in the Analyzer detail view server GUI.

13. Log on to Analyzer server, and then verify that the resources are ready to be analyzed.
 - a. Log on to Analyzer server.
 - b. In the **Administration** tab, select **Resource Management**.
 - c. Verify that the resources collected by the probe appear and are ready to be analyzed by Analyzer server.



Note: It might take some time before the resources collected by the probe appear in the Analyzer server GUI.

Changing the Analyzer probe server host name

Change the host name by performing the following procedure if the Hitachi Enterprise Storage probe is not added.

Procedure

1. Perform the following steps to stop the Analyzer probe server services:
 - a. Run the following command:

```
crontab -e
```

- b. At the beginning of each line in the ordinary execution schedule that was output for the Analyzer probe server, add a hash mark (#) to comment out each line:

```
# */5 * * * * F=/usr/local/megha/cron.5min; test -f $F && bash $F
# 13 0 * * * F=/usr/local/megha/cron.1hr; test -f $F && bash $F
# 11 * * * * F=/usr/local/megha/cron.24hr; test -f $F && bash $F
# */5 * * * * F=/usr/local/megha/bin/sysstat.sh; test -f $F &&
(bash $F >> /usr/local/megha/logs/sys/`date +%Y%m%d`.log)
```

- c. Run the following command to stop the services:

```
/usr/local/megha/bin/megha-jetty.sh stop
```

2. Change the physical host name of the host on which Analyzer probe server is installed.
3. (Optional) Edit the `htnm_httpsd.conf` file to specify the new host name of the Analyzer probe server for the `ServerName` directive on the first line.
In preparation for adding the Hitachi Enterprise Storage probe in the future, we recommend performing this step. Make sure that you specify the same host name (case sensitive).

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

```
/opt/jplpc/htnm/Rest/config/htnm_httpsd.conf
```

4. Perform the following steps to start the Analyzer probe server services:
 - a. Run the following command:

```
crontab -e
```

- b. Delete the hash marks (#) from the beginning of each line in the ordinary execution schedule that generates output for the Analyzer probe server:

```
*/5 * * * * F=/usr/local/megha/cron.5min; test -f $F && bash $F
13 0 * * * F=/usr/local/megha/cron.1hr; test -f $F && bash $F
11 * * * * F=/usr/local/megha/cron.24hr; test -f $F && bash $F
*/5 * * * * F=/usr/local/megha/bin/sysstat.sh; test -f $F && (bash
$F >> /usr/local/megha/logs/sys/`date +%Y%m%d`.log)
```

- c. Run the following command:



Note: If the service automatic startup script is configured, when you restart the OS after changing the host name, the services will start automatically.

```
/usr/local/megha/bin/megha-jetty.sh start
```

5. Log on to Analyzer detail view server, and then verify that data is collected.
 - a. Log on to Analyzer detail view server.
 - b. Click the **Server Status** icon.
 - c. Verify that the probe appears in **Last Configuration Import Time** and **Last Performance Import Time** of **Data Import Status**, and that data is collected.



Note: It might take some time before the probe appears in the Analyzer detail view server GUI.

6. Log on to Analyzer server, and then verify that the resources are ready to be analyzed.
 - a. Log on to Analyzer server.
 - b. In the **Administration** tab, select **Resource Management**.
 - c. Verify that the resources collected by the probe appear and are ready to be analyzed by Analyzer server.



Note: It might take some time before the resources collected by the probe appear in the Analyzer server GUI.

Changing the Analyzer probe server IP address when the Hitachi Enterprise Storage probe is added

Change the IP address of the host where the Analyzer probe server is installed. Because RAID Agent is also installed on the host where the Analyzer probe server is installed, change the IP address by performing the following procedure if the Hitachi Enterprise Storage probe is added.



Note:

This procedure is applicable for RAID Agent installed with Ops Center Analyzer. If you are using Tuning Manager - Agent for RAID, see *Hitachi Command Suite Tuning Manager Agent Administration Guide*.

If you are using Tuning Manager - Agent for RAID, be sure to re-specify the settings of the Hitachi Enterprise Storage probe and other settings, similar to when using the RAID Agent installed with Ops Center Analyzer.

Procedure

1. Perform the following steps to stop the Analyzer probe server services:

- a. Run the following command:

```
crontab -e
```

- b. At the beginning of each line in the ordinary execution schedule that was output for the Analyzer probe server, add a hash mark (#) to comment out each line:

```
# */5 * * * * F=/usr/local/megha/cron.5min; test -f $F && bash $F
# 13 0 * * * F=/usr/local/megha/cron.1hr; test -f $F && bash $F
# 11 * * * * F=/usr/local/megha/cron.24hr; test -f $F && bash $F
# */5 * * * * F=/usr/local/megha/bin/sysstat.sh; test -f $F &&
(bash $F >> /usr/local/megha/logs/sys/`date +%Y%m%d`.log)
```

- c. Run the following command to stop the services:

```
/usr/local/megha/bin/megha-jetty.sh stop
```

2. Run the following command to stop the RAID Agent services.

```
/opt/jplpc/htnm/bin/htmsrv stop -all
```

3. Change the IP address of the host on which Analyzer probe server is installed.
4. Verify that the IP address can be resolved from the host name of the host on which Analyzer probe server is installed.
5. When Granular Data Collection is enabled, change the IP address of the RAID Agent host defined in the `storage_agent_map.txt` file to the new IP address.

6. If the servers that can access RAID Agent are limited (the access source restriction function is configured), change the IP address of the Analyzer probe server defined in the `htnm_httpsd.conf` file to the new IP address.
7. Run the following command to start the RAID Agent services.

```
/opt/jplpc/htnm/bin/htmsrv start -all
```

8. Perform the following steps to start the Analyzer probe server services:
 - a. Run the following command:

```
crontab -e
```

- b. Delete the hash marks (#) from the beginning of each line in the ordinary execution schedule that generates output for the Analyzer probe server:

```
*/5 * * * * F=/usr/local/megha/cron.5min; test -f $F && bash $F
13 0 * * * F=/usr/local/megha/cron.1hr; test -f $F && bash $F
11 * * * * F=/usr/local/megha/cron.24hr; test -f $F && bash $F
*/5 * * * * F=/usr/local/megha/bin/sysstat.sh; test -f $F && (bash
$F >> /usr/local/megha/logs/sys/`date +%Y%m%d`.log)
```

- c. Run the following command:

```
/usr/local/megha/bin/megha-jetty.sh start
```

9. Change the settings of Hitachi Enterprise Storage probe as follows:
 - a. On the Analyzer probe server home page, stop the target probe and click **Edit**.
 - b. In the **Edit Hitachi Enterprise Storage Probe** section, enter the IP address of the machine on which the RAID Agent is installed in the **RAID Agent IP address** field. Then, click **Next**.
 - c. In the **Validating Hitachi Enterprise Storage Probe details** window, click **Next**, and then click **OK**.
 - d. In the **Status** window, in **ACTION**, click **Start** to start collecting data.
10. Log on to Analyzer detail view server, and then verify that data is collected.
 - a. Log on to Analyzer detail view server.
 - b. Click the **Server Status** icon.
 - c. Verify that the probe appears in **Last Configuration Import Time** and **Last Performance Import Time** of **Data Import Status**, and that data is collected.



Note: It might take some time before the probe appears in the Analyzer detail view server GUI.

11. Log on to Analyzer server, and then verify that the resources are ready to be analyzed.
 - a. Log on to Analyzer server.
 - b. In the **Administration** tab, select **Resource Management**.
 - c. Verify that the resources collected by the probe appear and are ready to be analyzed by Analyzer server.



Note: It might take some time before the resources collected by the probe appear in the Analyzer server GUI.

Changing the Analyzer probe server IP address

Change the IP address by performing the following procedure if the Hitachi Enterprise Storage probe is not added.

Procedure

1. Perform the following steps to stop the Analyzer probe server services:

- a. Run the following command:

```
crontab -e
```

- b. At the beginning of each line in the ordinary execution schedule that was output for the Analyzer probe server, add a hash mark (#) to comment out each line:

```
# */5 * * * * F=/usr/local/megha/cron.5min; test -f $F && bash $F
# 13 0 * * * F=/usr/local/megha/cron.1hr; test -f $F && bash $F
# 11 * * * * F=/usr/local/megha/cron.24hr; test -f $F && bash $F
# */5 * * * * F=/usr/local/megha/bin/sysstat.sh; test -f $F &&
(bash $F >> /usr/local/megha/logs/sys/`date +%Y%m%d`.log)
```

- c. Run the following command to stop the services:

```
/usr/local/megha/bin/megha-jetty.sh stop
```

2. Change the IP address of the host on which Analyzer probe server is installed.

3. Perform the following steps to start the Analyzer probe server services:

- a. Run the following command:

```
crontab -e
```

- b. Delete the hash marks (#) from the beginning of each line in the ordinary execution schedule that generates output for the Analyzer probe server:

```
*/5 * * * * F=/usr/local/megha/cron.5min; test -f $F && bash $F
13 0 * * * F=/usr/local/megha/cron.1hr; test -f $F && bash $F
11 * * * * F=/usr/local/megha/cron.24hr; test -f $F && bash $F
*/5 * * * * F=/usr/local/megha/bin/sysstat.sh; test -f $F && (bash
$F >> /usr/local/megha/logs/sys/`date +%Y%m%d`.log)
```

- c. Run the following command:

```
/usr/local/megha/bin/megha-jetty.sh start
```

4. Log on to Analyzer detail view server, and then verify that data is collected.

- a. Log on to Analyzer detail view server.
- b. Click the **Server Status** icon.
- c. Verify that the probe appears in **Last Configuration Import Time** and **Last Performance Import Time** of **Data Import Status**, and that data is collected.



Note: It might take some time before the probe appears in the Analyzer detail view server GUI.

5. Log on to Analyzer server, and then verify that the resources are ready to be analyzed.
 - a. Log on to Analyzer server.
 - b. In the **Administration** tab, select **Resource Management**.
 - c. Verify that the resources collected by the probe appear and are ready to be analyzed by Analyzer server.



Note: It might take some time before the resources collected by the probe appear in the Analyzer server GUI.

Changing the port number used by the RAID Agent

To change the port number for each service used by the RAID Agent, use the **jpcnsconfig port** command.



Note:

This procedure is applicable for RAID Agent installed with Ops Center Analyzer. If you are using Tuning Manager - Agent for RAID, see *Hitachi Command Suite Tuning Manager Installation Guide*.

Procedure

1. Run the following command to stop the RAID Agent services.

```
/opt/jplpc/htnm/bin/htmsrv stop -all
```

2. Run the **jpcnsconfig port** command:

```
/opt/jplpc/tools/jpcnsconfig port define all
```

3. Configure a port number for each service. If the **jpcnsconfig port** command is run, the system displays the currently configured port number.
For example, the system displays the following if the port number 22285 is currently configured for the Name Server service:

```
Component[Name Server]
ServiceID[PN1001]
Port[22285] :
```

Tasks in this procedure might vary depending on how you set the port number. The following table shows port number settings and related tasks. Unless the port numbers conflict in the system, use the port numbers which display when you run the **jpcnsconfig port** command.

Setting	Task
When using the number displayed as a fixed port number as is	Press Enter .
When changing the displayed port number	Specify a port number from 1024 to 65535. You cannot specify the port number currently in use.
When not setting a fixed port number	Specify 0. Even if 0 is specified for the following services, the default value is set: <ul style="list-style-type: none"> ▪ Name Server service ▪ Status Server service

4. Run the **jpcnsconfig port** command again to make sure that the port number is configured correctly.

For example, to display port numbers for all services, run the command as follows:

```
/opt/jplpc/tools/jpcnsconfig port list all
```

If **<error>** is displayed in either the Services column or the Port column, it means that an invalid port number is configured. Reset the port number. If an error still results, the following causes are possible:

- The port number is not registered in the services file.
- The same port number is registered more than once in the services file.

**Note:**

- If the **jpcnsconfig port** command is canceled with the Ctrl +C key, the port number is not set correctly. Run the **jpcnsconfig port** command again and reset the port numbers.
- You do not need to change the port number for the Name Server service, because it will not be used.
- If you use the **jpcnsconfig port** command to display the Status Server port number or to set the Status Server port number to 22350, the following message is displayed:

- For the **jpcnsconfig port** command with the **list** option specified:

```
KAVE05919-E The port number is not registered correctly
in the services file.
```

- For the **jpcnsconfig port** command with the **define** option specified:

```
KAVE05918-W The specified port number is in use by
another.
```

In such cases, the following text is included in `/etc/services`:

```
CodeMeter 22350/tcp
```

This entry is the default, regardless of whether the CodeMeter is actually installed. Check whether the CodeMeter is being used. If it is not being used, comment out the text. If the CodeMeter is being used or the port number is registered for a different product, make sure that there are no conflicting port numbers on the server.

Changing the port number of the RAID Agent REST Web Service

When a port number of the RAID Agent REST Web Service is changed, you must apply the new port number to the Hitachi Enterprise Storage probe and the Analyzer server.

**Note:**

This procedure is applicable for RAID Agent installed with Ops Center Analyzer. If you are using Tuning Manager - Agent for RAID, see *Hitachi Command Suite Tuning Manager Agent Administration Guide*.

Procedure

1. Run the following command to stop the RAID Agent services.

```
/opt/jplpc/htnm/bin/htmsrv stop -all
```

2. Use the table that follows to change the port number.

Note that to change the port number, open the relevant file shown in the following table by using a text editor.

Default port number	Procedure for changing the port number
24221 (Access port for RAID Agent REST Web Service for non-SSL communication)	Change the port number specified in the Listen directive in the following file: <code>/opt/jplpc/htnm/Rest/config/htnm_httpsd.conf</code>
24222 (Access port for RAID Agent REST Web Service for SSL communication)	
24223 (AJP port for RAID Agent REST Application Service)	Change the values for the following properties. You must specify the same value for both properties. <ul style="list-style-type: none"> The <code>worker.worker1.port</code> property in the <code>/opt/jplpc/htnm/HBasePSB/CC/web/redirector/workers.properties</code> file The <code>webserver.connector.ajp13.port</code> property in the <code>/opt/jplpc/htnm/HBasePSB/CC/server/usrconf/ejb/AgentRESTService/usrconf.properties</code> file
24224 (Port number of RMI registry used by RAID Agent REST Application Service)	Change the value of the following property: The <code>ejbserver.rmi.naming.port</code> property in the <code>/opt/jplpc/htnm/HBasePSB/CC/server/usrconf/ejb/AgentRESTService/usrconf.properties</code> file
24225 (Port number server management commands used to communicate with RAID Agent REST Application Service)	Change the value for the following property: The <code>ejbserver.rmi.remote.listener.port</code> property in the <code>/opt/jplpc/htnm/HBasePSB/CC/server/usrconf/ejb/AgentRESTService/usrconf.properties</code> file

Default port number	Procedure for changing the port number
24226 (Port number of the RAID Agent REST Application Service simple Web server)	Change the value for the following property: The <code>ejbserver.http.port</code> property in the <code>/opt/jplpc/htnm/HBasePSB/CC/server/usrconf/ejb/AgentRESTService/usrconf.properties</code> file

3. Run the following command to start the RAID Agent services.

```
/opt/jplpc/htnm/bin/htmsrv start -all
```

4. When a port number of RAID Agent REST Web Service is changed, you must change the settings of Hitachi Enterprise Storage probe as follows:
 - a. On the Analyzer probe server home page, click **Stop** to stop the target probe, and then click **Edit**.
 - b. In the **Edit Hitachi Enterprise Storage Probe** section, enter the access port number of RAID Agent REST Web Service in the RAID Agent Port field. Then, click **Next**.
 - c. In the **Validating Hitachi Enterprise Storage Probe details** window, click **Next**, and then click **OK**.
 - d. In the **Status** window, in **ACTION**, click **Start** to start collecting data.
5. When a port number of RAID Agent REST Web Service is changed, you must perform one of the following operations in Analyzer server:
 - Manually refresh the RAID Agent list information for Analyzer server.
For details, see the section describing how to refresh the RAID Agent list manually in the *Hitachi Ops Center Analyzer REST API Reference Guide*.
 - Restart the Analyzer server services.
For details, see [Starting and stopping the Ops Center Analyzer services \(on page 358\)](#).

Restricting access to servers that access RAID Agent

To enhance security, you can enable only the trusted servers to access RAID Agent. Edit the `htnm_httpsd.conf` file to include only the names of the servers that can access RAID Agent data.

When the Analyzer server analyzes data, the Analyzer probe server accesses performance data in RAID Agent. In addition, when you use API functions that access RAID Agent, the Analyzer server accesses performance data in RAID Agent.

**Note:**

This procedure presumes you are using the RAID Agent bundled with Ops Center Analyzer. The procedure is the same for using Tuning Manager - Agent for RAID.

Procedure

1. Run the following command to stop the RAID Agent services.

```
/opt/jplpc/htnm/bin/htmsrv stop -all
```

2. Open the `htnm_httpsd.conf` file.

The `htnm_httpsd.conf` file is located in the following directory.

```
/opt/jplpc/htnm/Rest/config/htnm_httpsd.conf
```

3. Register information about the servers that are allowed to connect to the RAID Agent in the last line of the `htnm_httpsd.conf` file. Information about a server refers to the host name or IP address of each host on which Analyzer probe server or Analyzer server is installed.

The following shows the format for registering hosts in the `htnm_httpsd.conf` file.

```
<Location /TuningAgent>
order allow,deny
allow from host [ host...]
</Location>
```

Make sure that hosts are written in one of the following formats:

- The domain name (example: `hitachi.ABCDEFG.com`)
- Part of the domain name (example: `hitachi`)
- The complete IP address (example: `10.1.2.3 127.0.0.1`)
- Part of the IP address (example: `10.1` which, in this case, means `10.1.0.0/16`)
- *Network/Netmask* format (example: `10.1.0.0/255.255.0.0`)
- *Network/n* (CIDR notation: *n* is the number of bits representing the network address) (example: `10.1.0.0/16`)

**Note:**

- Multiple lines can be used to specify hosts for `allow from`.
- If you want to specify two or more hosts in a command line for `allow from`, delimit the hosts with a space.
- If you attempt to connect from a host on which RAID Agent is installed, you must also specify the local loop-back address (`127.0.0.1` or `localhost`).
- Make sure that you specify `order` according to the specified format. If extra spaces or tabs are inserted, the operation will fail.

Example of host registration:

```
<Location /TuningAgent>
order allow,deny
allow from 127.0.0.1 10.0.0.1
allow from 10.0.0.0/26
</Location>
```

4. Run the following command to start the RAID Agent services.

```
/opt/jplpc/htnm/bin/htmsrv start -all
```

Changing the data collection intervals of performance metrics for the Analyzer detail view server

To set alerts for performance metrics on the Analyzer detail view server, the record collection intervals of the Hitachi Enterprise Storage probe and those of RAID Agent must be the same as or shorter than the alert criteria. Furthermore, the record collection intervals of the Hitachi Enterprise Storage probe must be the same as those of RAID Agent.

Procedure

1. Check the values that can be set as alert criteria for the Analyzer detail view server. For details, see the *Analyzer detail view server Online Help*.
2. For performance metrics for which you want to set alerts, refer to the *Hitachi Ops Center Analyzer Detail View Metrics Reference Guide* and check the record names in RAID Agent.
3. Change the record collection intervals for the Hitachi Enterprise Storage probe.
4. Use the **collection_config** command to change the record collection intervals for RAID Agent. Refer to [Changing data collection intervals for RAID Agent \(on page 392\)](#).

Changing data collection intervals for RAID Agent

Use the **collection_config** command to change data collection intervals for RAID Agent. To change the intervals for collecting data from VSP family or HUS VM, specify the same value as the data collection intervals for both the RAID Agent and the Hitachi Enterprise Storage probe.

Note that you do not need to change the collection intervals of the Hitachi Enterprise Storage probe for records that are not displayed in the configuration window of the Hitachi Enterprise Storage probe.

**Note:**

- This procedure is applicable for RAID Agent installed with Ops Center Analyzer. If you are using Tuning Manager - Agent for RAID, see the *Hitachi Command Suite Tuning Manager Agent Administration Guide*.
- In Ops Center Analyzer 4.1.0 and later, the command for changing the data collection intervals of RAID Agent is **collection_config**, not **raid_agent_config**. The command **raid_agent_config** is no longer available.

Procedure

1. Log on to the Analyzer probe server through an SSH client (like **putty**).
2. Execute the following command to check the current settings of data collection intervals:

```
/opt/hitachi/Analytics/bin/collection_config showinterval -at
AccessType
```

Output example:

```
[root@localhost ~]# /opt/hitachi/Analytics/bin/collection_config
showinterval -at 1
#Record : Mode : Type : Current : Default : Modified
#----- : ---- : ----- : ----- : ----- : -----
PD      : R    : Collection Interval : 3600 : 3600 :
PI_LDS  : RW   : Collection Interval : 60   : 60   :
PI_LDS1 : R    : Sync Collection With : PI_LDS : PI_LDS :
PI_PTS  : RW   : Collection Interval : 60   : 300 : Y
PI_LDSX : N/A  : Not Collectable    : -    : -    :
:
```

You can change the data collection intervals for the records displayed with **RW** in the **Mode** column.

The current settings (unit: seconds) of data collection intervals are shown in the **Current** column.

3. Execute the following command to change data collection intervals:

```
/opt/hitachi/Analytics/bin/collection_config changeinterval -at
AccessType -r record-ID -i data-collection-interval (seconds) -stop
```

The data collection interval is changed for all instances whose **Access Type** is the same as the **Access Type** specified in the **-at** option.

You can specify only one record ID for the **-r** option.

Specify the **-stop** option to stop the RAID Agent service.

**Note:**

Values that can be specified for the `-i` option vary depending on the record.

For details, see the descriptions of the `collection_config` command.

Example:

```
[root@vm025254 bin]# ./collection_config changeinterval -at 1 -r
PD_PLC -i 60 -stop
KATR15100-I Make sure that the services are not running.
KATR15101-I The service is stopping. (service = Tuning Manager - Agent
REST Web Service).
KATR15101-I The service is stopping. (service = Tuning Manager - Agent
REST Application Service).
KATR15102-I The collection interval is being changed. (access type =
1, record = PD_PLC, before = 3600, after = 60).
KATR15117-W The instance whose settings are to be updated does not
exist. (access type = 1).
KATR15105-I The collection interval was changed successfully.
KATR15106-I After you finish changing the collection interval, start
the services.
```

4. Execute the following command to start RAID Agent services:

```
/opt/hitachi/Analytics/bin/collection_config service -start
```

Deleting an instance environment for RAID Agent

To delete multiple instance environments, repeat the following procedure for each instance environment.

Procedure

1. Log on to the Analyzer probe server through an SSH client (like **putty**).
2. Find the instance name of RAID Agent using this command:

```
/opt/jplpc/tools/jpcinslist agtd
```

For example, if the instance name is 35053, the command displays 35053.

3. Run the following command to stop any active RAID Agent services in the instance environment.

```
/opt/jplpc/htnm/bin/htmsrv stop -all
```

4. Delete the instance environment using this command:

```
/opt/jplpc/tools/jpcinsunsetup agtd -inst instance-name
```

The following example shows how to delete the instance environment 35053:

```
/opt/jplpc/tools/jpcinsunsetup agtd -inst 35053
```

5. Run the following command to start the RAID Agent services:

```
/opt/jplpc/htnm/bin/htmsrv start -all
```

Result

If the command is successful, the directories created during instance environment setup are deleted. If a service with the specified instance name is active, a message appears asking whether the service is to be stopped. If this message appears, stop the service of the applicable instance.

Collecting optional metrics for Brocade Network Advisor probe

The data collection of the following switch port metrics are disabled by default. To start collecting these metrics, you need to enable the data collection on the Analyzer probe server.

```
fabPortCrcErrors
fabPortSignalLosses
fabPortSyncLosses
fabPortLinkFailures
fabPortLinkResets
fabPortSequenceErrors
fabPortDroppedPackets
```



Note: Enabling the data collection for these metrics might cause a delay in the data collection of the Brocade Network Advisor probe.

Procedure

1. Log on to the Analyzer probe server through an SSH client (like **putty**) as a root user.
2. Stop the crond service using the command:

```
service crond stop
```

3. Stop the megha service using the command:

```
/usr/local/megha/bin/megha-jetty.sh stop
```

4. Verify the stopped status of the megha service:

```
/usr/local/megha/bin/megha-jetty.sh status
```

5. Go to the `/usr/local/megha/conf/probe` directory using the following command:

```
cd /usr/local/megha/conf/probe
```

6. Take a backup of `bfa_default.properties` file using the following command:

```
cp bfa_default.properties bkp_bfa_default.properties_org
```

7. Edit the `bfa_default.properties` file:

```
vi bfa_default.properties
```

8. At the end of the file, add the following:

```
collect.switch.error.data=true
```

9. Save the file and exit.

10. Start the megha service using the command:

```
/usr/local/megha/bin/megha-jetty.sh start
```

11. Start the crond service using the command:

```
service crond start
```

Changing the configuration information collection time

In RAID Agent, if a problem occurs where performance information is not collected at the specified time, you can prevent this problem by changing the timing of configuration information collection.

By default, if the collection of RAID Agent configuration information takes a minute or more, the performance information to collect concurrently might be skipped. However, by changing the timing of configuration information collection, you can ensure that the performance information collection is not be skipped even if the configuration information collection takes a minute or more.



Note:

- In RAID Agent, performance data is collected from storage systems as follows: configuration information is collected as RD records and performance information is collected as PI records.
- To determine whether performance information collection has been skipped, check whether the KAVE00213-W message is output to the log. Log information is stored in one of the followings: `/opt/jp1pc/log/jpclog01` or `/opt/jp1pc/log/jpclog02`.

You can change the timing of RAID Agent configuration information collection by using the collection time definition file (`conf_refresh_times.ini`) provided by RAID Agent.

When you change the configuration information collection timing, you should reexamine the capacity of the virtual memory for the Analyzer probe server.

The following table shows the required capacity of the virtual memory for each monitored storage system.

Storage system to be monitored	Required capacity of the virtual memory (MB)
VSP	1100
VSP G200, G400, G600, G800, VSP F400, F600, F800	450
VSP E series, VSP G350, G370, G700, G900, VSP G1000, G1500, VSP F350, F370, F700, F900, VSP F1500	1100
VSP 5000 series	1100
HUS VM	450
HUS100	180

You can collect the configuration information for the following records at the time defined in the collection time definition file. For PD records other than the following, configuration information is collected based on the Collection Interval value even if the collection time definition file is enabled:

- PD record
- PD_ELC record
- PD_LDC record
- PD_LSEC record
- PD_PTC record
- PD_RGC record
- PD_HGC record
- PD_HHGC record
- PD_LHGC record
- PD_PWPC record
- PD_LWPC record

By default, collection of configuration information, for which you can define collection times, starts on the hour every hour. The collected configuration information is stored in PD records that are generated at the same time (on the hour every hour).

When the definitions in the collection time definition file are enabled, the on-the-hour collection of configuration information stops, and configuration information is collected only at the times defined in the file. The collected configuration information is used for the PD records that are generated on the hour every hour and for the real-time report until the next time configuration information is collected.

You can use the `COLLECTION_TIME` field value of each record to check the time at which the configuration information stored in the PD record was collected.

Example:

Even if configuration information is defined so that it is collected twice a day at 00:00 and 12:00, the PD records in which that configuration information was stored are generated on the hour every hour. After configuration information is collected at 00:00, the information is used for each record generated hourly until the next time configuration information is collected at 12:00.



Caution:

The following notes apply to configuration information:

- Changes made to the timing of configuration information collection affects the generation results of PI records. The timing of "increases or decreases" in the number of instances for multi-instance records and in the number of logical devices that are aggregated using the `PI_LDA` record is synchronized with the timing of "increases or decreases" in the configuration information collection. Note that this does not apply to `PI_CLPS` records.
- The actual times that configuration information is collected might differ from the times defined in the collection time definition file.

Collection of configuration information can occur at the periodic collection times determined by the Collection Interval value. If a time defined in the collection time definition file does not exactly match any of the periodic collection times determined by the collection interval, the actual collection occurs at the nearest periodic collection time after the defined time.

For example, assume that the minimum Collection Interval value is set to 300 (five minutes) and 12:02 is defined as a configuration information collection time in the collection time definition file. In this case, configuration information is collected at 12:05, the same time that performance information is collected.

Creating the collection time definition file

Create the collection time definition file (`conf_refresh_times.ini`) after setting up the instance environment but before starting RAID Agent. You must create the file for each instance.

The directories in which the collection time definition file are saved are shown below.

`/opt/jplpc/agtd/agent/instance-name/`

When you create the collection time definition file, use a sample file (`conf_refresh_times.ini.sample`) contained in the same directory.

In the collection time definition file, specify the times at which you want to collect the configuration information of storage systems in `hh:mm` format.

Rules for specifying times in the collection time definition file

- Each `hh:mm` entry must consist only of single-byte characters.
- The `hh` part indicates the hour and the `mm` part indicates the minutes. Both must be specified as two digits.
- The time must be specified on a 24-hour basis (00:00 to 23:59).
- A time must be specified on a separate line.
- The collection time definition file can define a maximum of 48 collection times.
- The sixth and following characters on each line are ignored.
- The lines beginning with a hash mark (#) are treated as comment lines.

The following notes apply to the collection time definition file:

- Lines that violate any of the above rules have no effect.
- The definitions in the collection time definition file can be enabled even if the file does not contain any valid lines. If the collection time definition file does not contain any valid lines, configuration information is collected only once when RAID Agent starts. Configuration information is not collected after that time.
- The definitions in the collection time definition file are disabled if the file contains a line that is, including the terminating character, is 1024 or more bytes.

Coding example of a collection time definition file

```
#VSP G1000: 14053
02:30 #for Volume Migration 1
04:30 #for Volume Migration 2
```

Enabling the definitions in the collection time definition file

After you create the collection time definition file and save it in the specified directory, start RAID Agent.

Check the logs to determine whether the collection time definition file is enabled and whether it is functioning normally.

RAID Agent logs are stored in one of the followings: `/opt/jp1pc/log/jpclog01`
or `/opt/jp1pc/log/jpclog02`.

If the collection of performance information is skipped, the KAVE00213-W message is output to the log file. If the KAVE00213-W message is output, revise the settings in the collection time definition file.

The definitions in the collection time definition file are not enabled if you save the file in the specified directory while RAID Agent is being started or after RAID Agent has started. Also note that changes made to the collection time definition file while RAID Agent is starting are not applied.

Managing the Analyzer detail view server and the Analyzer probe server

You can manage individual probes as well as the servers.

Accessing the Analyzer detail view

You can access the Analyzer detail view UI from any supported browser.

For most Analyzer detail view operations, you can access the Analyzer detail view server from the Ops Center Analyzer Tools menu. Certain management tasks require logging into the Analyzer detail view server as the `admin` user instead of using the Tools menu (which logs into the server as a general user). The management tasks documented in this guide state when it is necessary to log in as the `admin` user.

Procedure

1. In your browser, enter the Analyzer detail view URL:
`https://server-IP-address:Port-Number`
 (The default port for https access is 8443.)
 The **Logon** window appears.
2. In the **Username** and **Password** fields, type your user name and password, and then click **Login**.

Viewing Analyzer probe server status

The **Status** window displays information about all configured probes and includes controls to manage them.

Log on to the Analyzer probe to display the **Status** window.

Column	Description
PROBE TYPE	Type of probe
NAME	Target from which data is being collected
STATUS	<p>The probe status is displayed in any one of the following four colors:</p> <p>Stopped (Grey): Probe is stopped.</p> <p>Running (Green): Probe is collecting data from targets.</p>

	<p>Error (Red): Probe has abruptly stopped collecting data.</p> <p>Processing delay (Yellow): Probe is running behind schedule.</p> <p>Stopping/Monitoring Stopped (Black): Probe has stopped monitoring targets or probe is stopping .</p>
ACTION	<p>Displayed when the probe is stopped or started. You can perform the following tasks using links in this column:</p> <p>Stop: Stops the probe</p> <p>Start: Starts data collection</p> <p>Edit: Let you edit the probe</p> <p>Delete: Deletes the probe</p>
CONFIGURATION DATA	Displays the LAST COLLECTED and NEXT COLLECTION times.
PERFORMANCE DATA	Displays the LAST COLLECTED and NEXT COLLECTION times.

Analyzer probe server configuration backup

The Analyzer probe server configuration is automatically backed up at midnight to the following location on the primary FTP server:

Probe-appliance-ID/probeConfigBackup/ProbeConfigurationBackup_Probe-version.zip.enc.

The backup can be used to migrate the Analyzer probe server to another VM if it is corrupted or otherwise inaccessible. The backup data can only be restored by contacting Customer Support.

The time of the last backup is displayed in the **Status** window of the Analyzer probe server. For example:

Last Appliance Configuration Backup Time: 15 Nov 2017 00:30:50

Starting and stopping probes

You can start or stop data collection from the target systems.

Procedure

1. Log on to the Analyzer probe server.
2. In the **Status** window, you can search for one or more probes by using the Search Criteria (type, name, status).

3. In the **Action** column, click **Start** or **Stop**.
You can select multiple probes, and then click **Start** or **Stop**. If you want to start or stop all configured probes across all the pages, click the check box in the table header row, click **Select All**, and then click **Start** or **Stop**.

Editing probes

You can edit the probe details, such as the IP address or password of the target system, or to select or deselect the targets for monitoring.



Note:

Settings may vary according to probe type.

Procedure

1. Log on to the Analyzer probe.
2. In the **Status** window, you can search for one or more probes by using the Search Criteria (type, name, status).
3. In the **Action** column, stop the probe if the probe is running, and then click **Edit**.
4. In the **Edit Probe Details** window, type the probe details.
5. Click **Next**, and save the changes.

Deleting probes

You can delete a probe when you want to stop monitoring the target system or when the target system is removed from the environment.

Procedure

1. Log on to the Analyzer probe.
2. In the **Status** window, you can search for one or more probes by using the Search Criteria (type, name, status).
3. In the **Action** column, stop the probe if it is already running, and then click **Delete**.
You can select the multiple probes and then click **Delete**. If you want to delete all configured probes across all the pages, click the check box in the table header row, click **Select All**, and then click **Delete**.
4. The confirmation message appears. Click **OK**.

Viewing and updating the Analyzer detail view license

You can view the current license information (including the licensed monitoring capacity), or add new licenses.

Procedure

1. Log on to the Analyzer detail view as the `admin` user.
2. In the application bar, click the **Manage** menu.

3. In the **Manage** window, in the **Status** section, click the **License Information** link. The **License Information** window displays all the configured licenses including identifier, key code, key limit, license usage, total license value, date range, and status. The identifier is used as a unique ID for Hitachi storage systems. The criteria for license can be capacity or count.
 - You can check the Usage and Value columns to verify that you have license nodes available.
 - In the case of license expiration or adding a new license, you can upload the license file using the **Select File** and **Submit** buttons.



Note: If you delete a probe or stop monitoring a target, the license count in the Usage column is decreased next time the configuration data is updated.

Viewing and updating the Analyzer probe license

You can view the current license information, or add new licenses.

Procedure

1. Log on to the Analyzer probe as the `admin` user.
2. In the application bar, click **Manage**.
3. In the **Manage** window, in the **Status** section, click the **License Information** link. The **License Information** window displays all the configured licenses, and status. In the case of adding a new license, you can upload the license file using the **Choose File** and **Submit** buttons.

Downloading the Analyzer probe server diagnostic data

The Analyzer probe server collects various log files that are useful for troubleshooting. The Download Diagnostic Data feature provides the facility to download these files in an archive file. If you cannot resolve the problem, send the generated data file with the error messages to the customer support for analysis.

Procedure

1. Log on to Analyzer probe.
2. On the home page, in the application menu area, click the **Manage**.
3. In the **Administration** section, click **Download Diagnostic Data**.
4. In the **Download Diagnostic Data** window, click **OK**.
The system initiates the diagnostic data generation process.
5. Click **Download**.
Sample diagnostic data file name: `diag_probe_20190807121514.gz`

Updating the downloader on the Analyzer detail view server

When Analyzer detail view server or intermediate FTP server connection details are changed, make sure that you update these connection details on the Analyzer detail view server to start downloading the data again.

Before you begin



Note: If you do not want to stop the **crond** service, you can stop the specific processes of the Analyzer detail view server and Analyzer probe server by using the **crontab -e** command as described in [Stopping the Analyzer detail view server or Analyzer probe server services \(on page 360\)](#) and [Starting the Analyzer detail view server or Analyzer probe server services \(on page 360\)](#)

Procedure

1. Log on to the Analyzer detail view server through an SSH client (like **putty**) as a root user.
2. Stop the crond service using the command:

```
service crond stop
```

3. Stop the megha service using the command:

```
/usr/local/megha/bin/megha-jetty.sh stop
```

4. Verify the stopped status of the megha service:

```
/usr/local/megha/bin/megha-jetty.sh status
```

5. Run the update FTP configuration script to update the FTP server details:
 - If you are downloading the data of all the Analyzer probe server appliances, run the following command:

```
sh /usr/local/megha/bin/createOrUpdateFTPConfiguration.sh --update -
-ftpServer FTP-server --ftpMethod FTP-method-(FTP/FTPS/SFTP) --
ftpPort FTP-port --ftpUsername FTP-username --ftpPassword
```

For example:

```
sh /usr/local/megha/bin/createOrUpdateFTPConfiguration.sh --update -
-ftpServer 192.168.1.2 --ftpMethod SFTP --ftpPort 22 --ftpUsername
abc --ftpPassword
```



Note:

- The `--ftpServer` and `--ftpUsername` parameters are mandatory. You cannot update the value of these two parameters.
- You can update the FTP server password, port, and FTP method. You can update all or one of these details. For example, if you want to update only the FTP method, enter only the `--ftpMethod` parameter and its value.
- If you want to change the password, enter only the `--ftpPassword` parameter. Do not enter any value for it. You can define the password in the next step.

- If you are downloading the data of the specific Analyzer probe server appliances, run the following command:

```
sh /usr/local/megha/bin/createOrUpdateFTPConfiguration.sh --update -
--ftpServer FTP-server --ftpMethod FTP-method-(FTP/FTPS/SFTP) --
ftpPort FTP-port --ftpUsername FTP-username --ftpPassword --
applianceidOption ApplianceIds --applianceidList Appliance-ID-list-
separated-by-comma
```

For example:

```
sh /usr/local/megha/bin/createOrUpdateFTPConfiguration.sh --update -
--ftpServer 192.168.1.2 --ftpMethod SFTP --ftpPort 22 --ftpUsername
abc --ftpPassword --applianceidOption ApplianceIds --applianceidList
1c5fbdd9-8ed3-43fe-8973-e9cba6d103c6,39cfcb01-11b2-46b4-8fce-
b4d84ea5acda
```



Note:

- The `--ftpServer` and `--ftpUsername` parameters are mandatory. You cannot update these values.
 - You can add new appliance IDs or you can remove the existing appliance IDs.
 - You can update the FTP server password, port, and FTP method. You can update all or one of these details. For example, if you want to update only the FTP method, enter only the `--ftpMethod` parameter and its value.
 - If you want to change the password, enter only the `--ftpPassword` parameter. Do not enter any value for it. You can define the password in the next step.
6. If you have provided the `ftpPassword` parameter, enter the FTP user password and confirm it.
 7. Start the megha service using the command:

```
/usr/local/megha/bin/megha-jetty.sh start
```

8. Start the crond service using the command:

```
service crond start
```

Analyzer detail view audit logs

The Analyzer detail view captures various types of logs in the `/usr/local/megha/logs` directory. These logs are important for troubleshooting issues related to user logins, alerts, email notifications, and so on. You can provide these log details to customer support for advanced troubleshooting.

Log file name	Description	Analyzer detail view server	Analyzer probe server
alertApi-AuditTrail.log	Alerts configured on the Analyzer detail view server.	✓	
app.log	Email groups	✓	✓
appApi-AuditTrail.log	Registration or deregistration of Analyzer detail view add-on applications.	✓	
appinit.log	Application component initialization, including verification and status of components.	✓	✓
dbApi-AuditTrail.log	Database API calls, such as resource and attribute definition APIs, data set and data subset APIs, and so on.	✓	

Log file name	Description	Analyzer detail view server	Analyzer probe server
transaction.log	<p>Contains the logs of the following activities:</p> <ul style="list-style-type: none"> Operating system upgrade Data export using Custom Reports Time zone settings Manage menu settings <p>Note: On the Analyzer probe server, the time zone details are not logged.</p>	✓	✓
upgrade.log	Analyzer detail view upgrade actions including time, status, and results.	✓	✓
user.log	User login, user creation or deletion, user validation, and so on.	✓	✓

Increasing the maximum number of open files (Linux OS)

Before installing the Analyzer detail view server or Analyzer probe server on a Linux host, the minimum value of the system-wide and user-level limits on the number of open files must be set to 65535 or greater.

The recommended values are:

System-wide: 327675

User-level: 262140

Procedure

1. Log on as follows:

- a. If you are installing the Analyzer detail view server or Analyzer probe server for the first time, log on to the Linux machine as **root**.
- b. If you are performing this task post-installation or while upgrading, log on to the Analyzer detail view server or Analyzer probe server through an SSH client (like **putty**) as a root user.

2. Run the following command to check the system-wide kernel limit:



Note: The recommended kernel limit is 327675.

```
sysctl -a | grep fs.file-max
```

If the value is 65535 or greater, skip to step 3. Otherwise, do the following:

- a. Navigate to the `/etc` directory and create the `sysctl.d` directory if it does not exist:

```
mkdir sysctl.d
```

- b. Navigate to the `/etc/sysctl.d` directory and create the `sysctl.conf` file if it does not exist.
- c. Ensure that the `fs.file-max` property is present in the `sysctl.conf` file and the value is set to 65535 or greater.
- d. Run the following command to apply the revised configuration:

```
sysctl -p /etc/sysctl.d/sysctl.conf
```

3. Run the following command to check the user-level limit:



Note: The recommended user-level limit is 262140.

```
ulimit -a | grep -i open
```

If the value is less than 65535, then do the following:

- a. Navigate to the `/etc/security/limits.d` directory and create the following file, if it does not exist:
 - Create `90-nproc.conf` file, if you are using Red Hat Enterprise Linux and Oracle Linux version earlier than 7.0.
 - Create `20-nproc.conf` file, if you are using Red Hat Enterprise Linux and Oracle Linux version 7.0 or later.
- b. Ensure that the following two properties are present in the `90-nproc.conf` or `20-nproc.conf` file and set their values as follows:

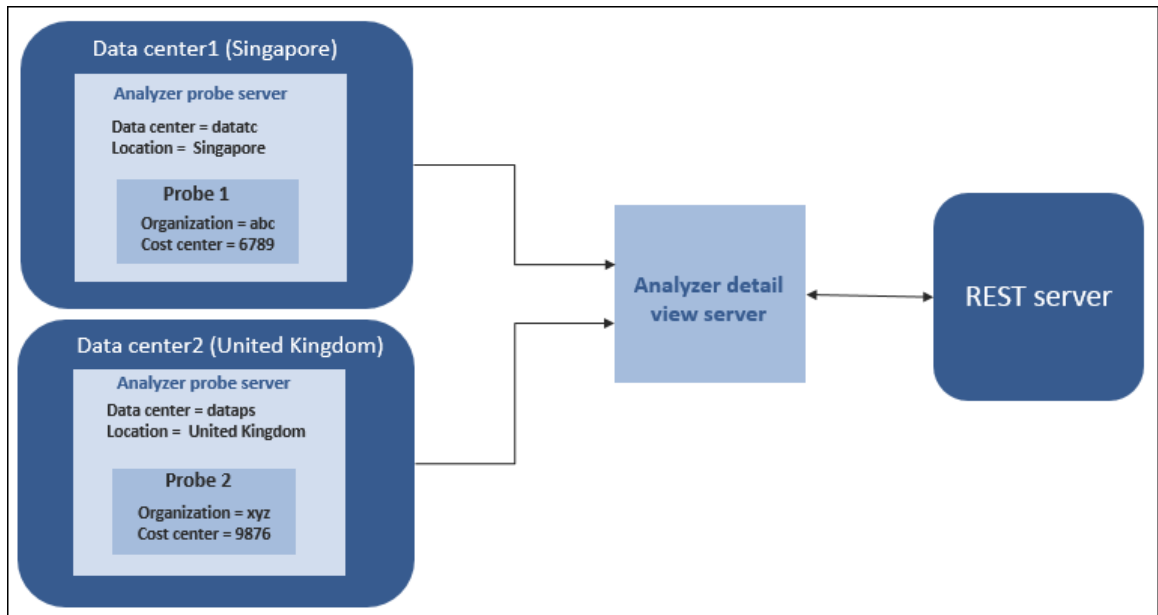
```
* soft nfile 65535
* hard nfile 65535
```

4. If you changed the system-wide kernel or user-level limits on the Analyzer detail view machine, you must restart the machine.

Grouping data centers using custom attributes

Custom attributes let you group data based on your organization infrastructure. The Analyzer probe server includes four attributes: the Data Center and Location attribute at the Analyzer probe server level, and the Organization and Cost Center attribute at each probe level. This enables you to extend the set of attributes to accommodate information based on your organization for custom reporting and grouping.

The following figure illustrates the flow of the custom attributes.



You can query the Analyzer detail view server database using the REST API based on the following attribute IDs:

- Data Center: __datacenter
- Location: __location
- Organization: __custattr01
- Cost Center: __custattr02

Sample query:

- ```
__probe[=__datacenter rx .] [=__location rx .][=__custattr01 rx .]
[=__custattr02 rx .]
```
- ```
h[=__datacenter rx .] [=__location rx .][=__custattr01 rx .]  
[=__custattr02 rx .]
```
- ```
vm[=__datacenter rx .] [=__location rx .][=__custattr01 rx .]
[=__custattr02 rx .]
```

## Adding the Data Center and Location attributes

### Procedure

1. Log on to the Analyzer probe.
2. On the home page, click **Reconfigure**.  
The Reconfigure Settings page opens.
3. Open the **Probe Server Attributes** tab and provide the `Data Center` and `Location` attributes.
4. Click **Save**.



**Note:** The new attributes are associated with all resources collected by the Analyzer probe.

## Adding the Organization and Cost Center attributes

### Procedure

1. Log on to the Analyzer probe server.
2. On the home page, in the application menu area, click the **Manage** link.
3. In the **Manage** window, click **Manage Custom Attributes**.
4. In the **Probe Attributes** section, select one or more probes for which you want to assign the attribute.  
You can use the filter option to display by Probe Name, Probe Type, or Attribute value.
5. In the **Update Probe Attributes** section, provide the details of the `Organization` and `Cost Center` attributes.
6. Click **Save**.



**Note:** The new attributes are associated with all resources collected by the probe.

## Changing the IP address of the Analyzer detail view server

After you change the IP address of the Analyzer detail view server, you must reconfigure the connections with the Analyzer probe server and the Analyzer server.

### Before you begin

You must have Administrator permission (Windows) or root permission (Linux).

### Procedure

1. Change the IP address of the Analyzer detail view server.
  - If the Analyzer detail view server and the Analyzer server are installed on the same host:  
Change the IP address. For details, see [Changing the Analyzer server IP address \(on page 365\)](#).
  - If the Analyzer detail view server and the Analyzer server are installed on different hosts:  
Change the IP address on the OS of the Analyzer detail view server.
2. Reconfigure the connection with the Analyzer probe server. For details, see [Updating the connection details of the Analyzer detail view server on the Analyzer probe server \(on page 412\)](#).
3. Reconfigure the connection with the Analyzer server. For details, see [Reconfiguring the connection with Analyzer detail view server \(on page 413\)](#).

## Updating the connection details of the Analyzer detail view server on the Analyzer probe server

When the Analyzer detail view server IP address is changed, make sure that you update the new IP address on the Analyzer probe UI. After you update the IP address, the Analyzer probe server can transfer the data to the Analyzer detail view server.

### Procedure

1. Log on to the Analyzer probe.
2. In the **Status** window, click **Reconfigure**.
3. In the **Reconfigure** window, click the **Analyzer detail view server** tab.
4. In the **Server Details** section, Click **Edit**.
5. In the **Edit Primary Analyzer detail view server Details** window, provide the host details of the Analyzer detail view server.
  - **Protocol:** FTP, FTPS, SFTP, or HTTPS.
  - **Host:** Analyzer detail view server IP address.
  - **Port:** Based on the selected protocol.

- **User:** User name for the host. For an Analyzer detail view server the user name is: meghadata
  - **Password:** Password for the host. For an Analyzer detail view server the default password is: meghadata123
6. In the **Advanced Settings** section, update the **Real-Time Server** IP address to match the Analyzer detail view server IP address.
  7. Click **Save**.

## Reconfiguring the connection with Analyzer detail view server

If you change the IP address or host name of the Analyzer detail view server, you must reconfigure the connections with the Analyzer server and the Analyzer detail view server.

### Procedure

1. In the **Administration** tab, select **System Settings > Analyzer detail view Server**.
2. Click **Edit Settings**, and specify the Analyzer detail view server information.



**Note:** Specify the built-in administrator account. If you want to use a different account, specify the account created during the initial setup of the Analyzer detail view server. If you change the password of the specified user on the Analyzer detail view server, you must also change the same password in **Password** of the **Edit Settings** dialog box.

3. Click **Check Connection** to confirm that the server is connected properly.  
If you cannot access the Analyzer detail view server, verify the following:
  - The certificate is correctly specified on the Analyzer server.
  - The certificate is not expired.
4. Click **OK**.

### Result

The Analyzer detail view server is connected.

## Restarting the HTTP proxy service

If you install the new SSL certificate or make any changes to the default SSL certificate, then you must restart the HTTP proxy service.

### Procedure

1. Log on to the Analyzer detail view server through an SSH client (like **putty**) as a root user.
2. Stop the HTTP proxy service by using the command:

```
sh /usr/local/httpProxy/bin/megha-jetty.sh stop
```

3. Confirm the HTTP proxy service has stopped by using the command:

```
sh /usr/local/httpProxy/bin/megha-jetty.sh status
```

4. Start the HTTP proxy service by using the command:

```
sh /usr/local/httpProxy/bin/megha-jetty.sh start
```

5. Confirm whether the HTTP proxy service has started by using the command:

```
sh /usr/local/httpProxy/bin/megha-jetty.sh status
```

## Enabling system account locking

When Analyzer server is initially installed, the locking of the system account is disabled. For security purposes, you may want to lock the system account.



### Note:

Locking or unlocking an account requires user management permissions. You cannot unlock your own account on a web client, but you can unlock your own account on the Analyzer server.

### Procedure

1. Stop the Analyzer server services.
2. Create a `user.conf` file in the following location:

#### In Windows

*Common-component-installation-destination-folder\conf\*

#### In Linux

*Common-component-installation-destination-directory/conf/*

3. Add the property `account.lock.system`, and set the value to `true` to enable system account locking, then save the file.  
If you do not want to lock the system account, specify `false`.
4. Start the Analyzer server services.

---

## Chapter 13: Backing up and restoring Ops Center Analyzer

You can back up and restore Ops Center Analyzer system information.

### Overview of Ops Center Analyzer backup and restore

You can back up the following four components of the Ops Center Analyzer system, so that they can be restored later if, for example, a failure occurs, causing your system to go down:

- Analyzer server
- Analyzer detail view server
- Analyzer probe server
- RAID Agent



**Note:** The backup and restore procedures described in this documentation apply to the RAID Agent that is bundled with Ops Center Analyzer. If you are using Tuning Manager - Agent for RAID, refer to the *Hitachi Command Suite Tuning Manager Agent Administration Guide*.

You can back up and restore the entire Ops Center Analyzer system by backing up and restoring all four of these components, or any of the components selectively. For example, if a failure occurs in Analyzer server, you can choose to restore only Analyzer server.

#### Use cases for backing up and restoring

- Periodic backup: Prepare for any failures by periodically backing up your data as part of your normal operations. Then, if a failure occurs, restore the backed up data to recover from the failure.
- Reinstall an OS or a component on the same host or migrate components to a different host. In this case, you can restore backed up data in the new environment so that the settings and accumulated data are migrated to the new environment.

Ops Center Analyzer does not support the migration of data between an Analyzer server installed on a Windows host and an Analyzer server installed on a Linux host.

Ops Center Analyzer does not support functions for periodic automatic backup. Create a backup schedule that fits your requirements and perform backup according to that schedule.

You can back up and restore components in a virtual or physical environment. The procedures for backup or restore are the same, regardless of whether they are performed in a virtual environment or in a physical environment.

## Backing up Ops Center Analyzer

You can back up the entire Ops Center Analyzer system by backing up its four components according to the following workflow. You can also select an individual component, and back up only that component.

The general backup workflow for Ops Center Analyzer components is as follows:

1. Stop each service in the following order:
  - a. Analyzer server  
[Stopping the Analyzer server services \(on page 359\)](#)
  - b. Analyzer detail view server  
[Stopping the Analyzer detail view server or Analyzer probe server services \(on page 360\)](#)
  - c. Analyzer probe server  
[Stopping the Analyzer detail view server or Analyzer probe server services \(on page 360\)](#)
  - d. RAID Agent  
[Stopping the RAID Agent services \(on page 363\)](#)
2. Back up data for each of the following components:
  - [Backing up the Analyzer server \(on page 417\)](#)
  - [Backing up the Analyzer detail view server \(on page 417\)](#)
  - [Backing up the Analyzer probe server \(on page 418\)](#)
  - [Backing up the RAID Agent \(on page 419\)](#)
3. Start each service in the following order:
  - a. RAID Agent  
[Starting the RAID Agent services \(on page 361\)](#)
  - b. Analyzer probe server  
[Starting the Analyzer detail view server or Analyzer probe server services \(on page 360\)](#)
  - c. Analyzer detail view server  
[Starting the Analyzer detail view server or Analyzer probe server services \(on page 360\)](#)
  - d. Analyzer server  
[Starting the Analyzer server services \(on page 358\)](#)



## Backing up the Analyzer server

You can back up the settings information of the Analyzer server.

### Before you begin

- You must have Administrator permission (Windows) or root permission (Linux).
- Stop all Analyzer server services.

### Procedure

1. Run the **backupsystem** command to back up the Analyzer server settings information.

## Backing up the Analyzer detail view server

You can back up the settings information and database of the Analyzer detail view server. Information such as user passwords and SSL settings is not backed up. You must reset this information after a restore.

### Before you begin

- Stop all Analyzer detail view server services.
- Make sure that the location where the backup files are to be stored has sufficient space.
- The properties that are required for this utility are backed up by default. The backup of the optional properties is controlled by the `/usr/local/megha/conf/backup.properties` file.

Note the following when editing the file `backup.properties`:

- Comment out lines corresponding to information that does not need to be backed up. To comment out a line, enter a hash mark (#) at the beginning of the line.
- The parameter `RAW_BACKUP_DATA` is used to back up raw data (data imported into the database). It is commented out by default. To back up raw data, delete the hash mark (#) at the beginning of the line containing this parameter.

### Procedure

1. Log on to the Analyzer detail view server through an SSH client (like **putty**) as a root user.
2. (Optional) Edit the file `backup.properties`. Delete hash marks (#) from lines that are commented out, as needed.

3. Run the following command to perform backup.

```
sh /usr/local/megha/bin/backupAndRestore.sh -o backup -z zip_file_path
```

- *zip\_file\_path*

Specify the name of the directory in which the backed-up data (a ZIP file) is to be saved.

Example:

```
sh /usr/local/megha/bin/backupAndRestore.sh -o backup -z /root/
hdca_backup
```

4. Manually reset the following settings:

- OS settings (*hosts* file, passwords of the megha user and meghadata user, and so on)
- SSL communication settings
- External user authentication settings (Connection with Active Directory)

## Backing up the Analyzer probe server

You can back up the settings information of the Analyzer probe server. Information such as user passwords and SSL settings is not backed up. You must reset this information after a restore.

### Before you begin

- Stop all Analyzer probe server services.
- Make sure that the location where the backup files are to be stored has sufficient space.
- The properties that are required for this utility are backed up by default. The backup of the optional properties is controlled by the `/usr/local/megha/conf/backup.properties` file.

Note the following when editing the file `backup.properties`:

- Comment out lines corresponding to information that does not need to be backed up. To comment out a line, enter a hash mark (#) at the beginning of the line.
- The parameter `RAW_BACKUP_DATA` is used to back up raw data (data normally transferred to Analyzer detail view server). It is commented out by default. To back up raw data, delete the hash mark (#) at the beginning of the line containing this parameter.
- If the Tuning Manager data migration is in process, then make sure that it is completed before taking the back up of the Analyzer probe server.

## Procedure

1. Log on to the Analyzer probe server through an SSH client (like **putty**) as a root user.
2. (Optional) Edit the file `backup.properties`. Delete hash marks (#) from lines that are commented out, as needed.
3. Run the following command to perform backup.

```
sh /usr/local/megha/bin/backupAndRestore.sh -o backup -z zip_file_path
```

- `zip_file_path`

Specify the name of the directory in which the backed-up data (a ZIP file) is to be saved.

Example:

```
sh /usr/local/megha/bin/backupAndRestore.sh -o backup -z /root/
probe_backup
```

4. Manually reset the following settings:
  - OS settings (`hosts` file, passwords of the megha user and megadata user, and so on)
  - SSL communication settings
  - External user authentication settings (Connection with Active Directory)

## Backing up the RAID Agent

You can back up the performance data and the configuration information files of the RAID Agent. If you are using Tuning Manager - Agent for RAID, you cannot use this procedure. Refer to the *Hitachi Command Suite Tuning Manager Agent Administration Guide*.

### Before you begin

- Stop all RAID Agent services.
- Make sure that the directory to which backed-up data is to be output has sufficient free space.

Use size of the following directory as an indication of the estimated amount of required free space:

*Analyzer-probe-server-installation-directory/RAIDAgent*

## Procedure

1. Run the following command to back up the performance data and the configuration information files.

```
/opt/jplpc/htnm/bin/htmshsbackup -dir output-directory
```

2. Manually copy the following definition information files and back them up in a directory of your choice.

You will need the following definition information files for investigation if an attempt to perform restore fails:

- /opt/jplpc/jpchosts
- /opt/jplpc/\*.ini
- /opt/jplpc/bin/action/\*.ini
- /opt/jplpc/bin/statsvr/\*.ini

## Restoring Ops Center Analyzer

You can restore the entire Ops Center Analyzer system by restoring its four components according to the following workflow. You can also select an individual component, and restore only that component.

The general restore workflow for Ops Center Analyzer components is as follows:

1. Stop the following services in this order:
  - a. Analyzer server  
[Stopping the Analyzer server services \(on page 359\)](#)
  - b. Analyzer detail view server  
[Stopping the Analyzer detail view server or Analyzer probe server services \(on page 360\)](#)
  - c. Analyzer probe server  
[Stopping the Analyzer detail view server or Analyzer probe server services \(on page 360\)](#)
  - d. RAID Agent  
[Stopping the RAID Agent services \(on page 363\)](#)
2. Restore data for each of the following components:
  - [Restoring the Analyzer server \(on page 421\)](#)
  - [Restoring the Analyzer detail view server \(on page 422\)](#)
  - [Restoring the Analyzer probe server \(on page 424\)](#)
  - [Restoring the RAID Agent \(on page 425\)](#)
3. Start the following services in this order:
  - a. RAID Agent  
[Starting the RAID Agent services \(on page 361\)](#)
  - b. Analyzer probe server  
[Starting the Analyzer detail view server or Analyzer probe server services \(on page 360\)](#)

## c. Analyzer detail view server

[Starting the Analyzer detail view server or Analyzer probe server services \(on page 360\)](#)

## d. Analyzer server

[Starting the Analyzer server services \(on page 358\)](#)

## Restoring the Analyzer server

You can restore the settings information of the Analyzer server. After a successful restore, specify the settings related to communication between the Analyzer server and the web client in the new environment.

### Before you begin

- You must have Administrator permission (Windows) or root permission (Linux).
- Stop all Analyzer server services on the restore destination host.
- Make sure that the following items are the same between the backup source host and the restore destination host:

- Analyzer server installation destination directory
- Version number of the installed instance of Analyzer server

You can check the version number of the Analyzer server in the **Version** window.

- Host name

If you are performing the restore as part of the procedure for migrating the system to a host with a different host name, the host names of the backup source host and restore destination host do not need to match.

- IP address
- System locale

### Procedure

1. Run the **restoresystem** command to restore the settings information of Analyzer server.
2. Edit the following definition files on the restore destination host to match any information that was changed on the backup source host.

If you performed a backup by specifying `Analytics` for the `type` option, the definition files are not stored in the backup data.

## In Windows

- Security definition file (`security.conf`)

Backup: `backup-folder\HBase\base\conf\sec`

Restore: `Common-component-installation-destination-folder\conf\sec`

- File for setting port numbers and host names (`user_httpsd.conf`)

Backup: `backup-folder\HBase\base\httpsd.conf`

Restore: `Common-component-installation-destination-folder\uCPSB\httpsd\conf`

## In Linux

- Security definition file (`security.conf`)

Backup: `backup-directory/HBase/base/conf/sec`

Restore: `Common-component-installation-destination-directory/conf/sec`

- File for setting port numbers and host names (`user_httpsd.conf`)

Backup: `backup-directory/HBase/base/httpsd.conf`

Restore: `Common-component-installation-destination-directory/uCPSB/httpsd/conf`

3. In the restore destination environment, if HTTPS connections are used between Analyzer server and the web client, enable HTTPS connections.
4. In the restore destination environment, if you changed the port number for communication between Analyzer server and the web client, reset the port number.
5. If you were using the function to connect with Ops Center Automator, reconfigure the primary server settings and the secondary server settings for the Common component.

## Restoring the Analyzer detail view server

You can restore the settings information and database of the Analyzer detail view server.

### Before you begin

- Stop all Analyzer detail view server services on the restore destination host.
- Make sure that the restore destination directory has sufficient free space.
- To restore the data, you must have a new setup with settings matching the original, including the following:
  - Version: The base version of the Analyzer detail view server must be same.
  - Deployment Model: The deployment model must be the same. To verify the deployment model, navigate to Manage > Status > License Information.
  - Machine: The machine time zone must be the same, and the machine locale must be English.

### Procedure

1. Log on to the Analyzer detail view server through an SSH client (like **putty**) as a root user.
2. Copy the backed-up data to any directory on the restore destination host.
3. Run the following command on the restore destination host to restore the data.

```
sh /usr/local/megha/bin/backupAndRestore.sh -o restore -z zip_file_path
```

- `zip_file_path`

Specify the path of the backed-up data (a ZIP file) to be restored.

Example:

```
sh /usr/local/megha/bin/backupAndRestore.sh -o restore -z /root/hdca_backup/backup-hdca-server-9.0.0-01_18041109_201806131342.zip
```

4. If necessary, reset the following information based on the notes you made during the backup procedure.
  - OS settings
    - The `hosts` file
 

Add connection destination hosts if the backup source host and the restore destination host are different, or if settings were reset when the host OS was reinstalled.
    - Passwords of the `megha` user and the `meghadata` user
    - Any other OS settings that were changed
  - SSL communication settings
  - External user authentication settings (Connection with Active Directory)
5. Verify the settings of the SMTP server, the Syslog server, and the SNMP Manager.

6. If the IP addresses or host names of the backup source host and restore destination host are different, reset the following settings on the host that will connect to the Analyzer detail view server.
  - Settings of the Analyzer detail view server to which the Analyzer probe server connects
  - Settings of the Analyzer detail view server to which Analyzer server connects
  - Settings of the Analyzer detail view server to which the Windows probe connects

## Restoring the Analyzer probe server

You can restore the settings information of the Analyzer probe server.

### Before you begin

- Stop all Analyzer probe server services on the restore destination host.
- Make sure that the restore destination directory has sufficient free space.
- To restore the data, you must have a new setup with settings matching the original, including the following:
  - Version: The base version of the Analyzer detail view server must be same.
  - Deployment Model: The deployment model must be the same. To verify the deployment model, navigate to Manage > Status > License Information.
  - Machine: The machine time zone must be the same, and the machine locale must be English.

### Procedure

1. Log on to the Analyzer probe server through an SSH client (like **putty**) as a root user.
2. Copy the backed-up data to any directory on the restore destination host.
3. Run the following command on the restore destination host to restore the data.

```
sh /usr/local/megha/bin/backupAndRestore.sh -o restore -z zip_file_path
```

- *zip\_file\_path*

Specify the path of the backed-up data (a ZIP file) to be restored.

Example:

```
sh /usr/local/megha/bin/backupAndRestore.sh -o restore -z /root/
probe_backup/backup-hdca-probe-9.0.0-01_18041109_201806150907.zip
```



4. If necessary, reset the following information based on the notes you made during the backup procedure.
  - OS settings
    - The `hosts` file
 

Add connection destination hosts if the backup source host and the restore destination host are different, or if settings were reset when the host OS was reinstalled.
    - Passwords of the `megha` user and the `meghadata` user
    - Any other OS settings that were changed
  - SSL communication settings
  - External user authentication settings (Connection with Active Directory)
5. If you were performing monitoring by using a Linux probe and the IP addresses of the backup source host and restore destination host are different, after performing restore, delete the Linux probe and then add it back to the Analyzer probe server.

## Restoring the RAID Agent

You can restore the performance data and configuration information files of the RAID Agent. If you are using Tuning Manager - Agent for RAID, you cannot use this procedure. Refer to the *Hitachi Command Suite Tuning Manager Agent Administration Guide*.

### Before you begin

- Stop all RAID Agent services on the restore destination host.
- Verify that the restore destination has free space equal to or greater than the size of the data to be restored.
- Verify that the following items are the same between the backup source host and the restore destination host:
  - OS
  - Version number of the RAID Agent
  - Instance name
- Verify that the setup of the instance on the restore destination host is complete.

When transferring backup data to another host, make sure of the following:

- Binary mode must be used to transfer backup data using FTP.
- When the backup data is transferred, the data sizes at the source and destinations must match.

## Procedure

1. Run the following command to restore the backed-up performance data and configuration information files:

```
/opt/jplpc/htnm/bin/htmhsrestore -dir storage-directory-of-the-backed-up-data
```

2. Run the **jpctdchkinst** command to check whether the instance is monitoring the targets correctly.
3. If the instance is not properly monitoring the targets, run the **jpctinssetup** command to change the settings, and then run the **jpctdchkinst** command again to check the monitoring status.
4. The following items cannot be restored by using the **htmhsrestore** command. Update the settings files as needed.

- a. If you changed the port numbers or SSL communication settings in the backup source environment, you must also change them in the restore destination environment by editing the following file.

```
/opt/jplpc/htnm/Rest/config/htnm_httpsd.conf
```

- b. If you changed the port numbers specified in the following files in the backup source environment, you must also change them in the restore destination environment.

- /opt/jplpc/htnm/HBasePSB/CC/web/redirector/workers.properties
- /opt/jplpc/htnm/HBasePSB/CC/server/usrconf/ejb/AgentRESTService/usrconf.properties

---

## Chapter 14: Removing Ops Center Analyzer components

Removing an Analyzer server, Analyzer detail view server, or Analyzer probe server is explained.

### Removing Ops Center Analyzer and Analyzer detail view servers from a Linux host

You can remove Analyzer server and Analyzer detail view server. You can choose to remove Analyzer server, Analyzer detail view server, or both.



**Note:** If a virtual machine is configured with the virtual appliance of the Infrastructure Analytics Advisor system (of a version that is 3.0.0-01 or later, and earlier than 4.0.0-00), do not remove the Infrastructure Analytics Advisor server. Because the Data Center Analytics server references some components of the Infrastructure Analytics Advisor server, if the Infrastructure Analytics Advisor server is removed, the Data Center Analytics server cannot start.

If the Infrastructure Analytics Advisor server is no longer used, check the [Port requirements \(on page 34\)](#) explanation and close any unnecessary port.

#### Procedure

1. Log on to the Analyzer server or Analyzer detail view server by using a user account with the root permission.
2. Stop any security monitoring software, antivirus software, and process monitoring software.
3. If you are using the functionality for connecting with Ops Center Automator in the Analyzer server, reset the settings of the Common component.  
If you are removing the Analyzer detail view server only, this step is not required.
4. Run the following commands:

```
cd /opt/hitachi/Analytics/installer
sh ./analytics_uninstall.sh SYS
```

5. Following the prompts, select the components you want to remove, and then complete the uninstallation process.

## Removing Ops Center Analyzer server from a Windows host

Remove the Analyzer server from a Windows host by setting the Startup type to Automatic or Manual and then removing it using the Windows control panel.

### Procedure

1. Log on to the Analyzer server by using a user account with the Administrator permission.
2. Stop any security monitoring software, antivirus software, and process monitoring software.
3. If you are using the functionality for connecting with Ops Center Automator, reset the settings of the Common component.
4. Stop the services of products that use Common component. To identify these services, see the *appendix*.
5. Set **Startup type** for the Analyzer server services to **Automatic** or **Manual**.  
In Windows environment, if the **Startup type** is set to **Disabled**, the removal process might fail because the services cannot be started.
6. To remove Analyzer server, go to **Control Panel > Programs > Programs and Features** and select **Hitachi Ops Center Analyzer**, and then click **Uninstall**.

### Next steps

The settings files remain in the installation folder. You must delete the settings files manually as necessary.

## Removing Analyzer probe server

Remove Analyzer probe server using the `dcaprobe_uninstall.sh` command.

### Procedure

1. Log on to the Analyzer probe server by using a user account with the root permission.
2. Stop any security monitoring software, antivirus software, and process monitoring software.
3. Run the following commands:

```
cd /opt/hitachi/Analytics/installer
sh ./dcaprobe_uninstall.sh SYS
```

## Chapter 15: Troubleshooting

You can troubleshoot common problems such as unsuccessful connections to the web client or between components.

### Connection to the Analyzer server web client unsuccessful

If you cannot connect to the Analyzer server web client check the operation status of Analyzer server and the port number setting.

#### Procedure

1. Run the `hcmds64srv` command with the `status` option to check the operation status of Analyzer server.

If the services "HAnalytics Engine Web Service" and "HBase 64 Storage Mgmt SSO Service" are running, and the service "HBase 64 Storage Mgmt Web Service" is not running, a port number might be redundant.

2. Check the event log.

If the following log is output, review the configuration of port numbers used by the Analyzer server:

| Item    | Contents                                                                                                                                                                                                                                                          |
|---------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Level   | Error                                                                                                                                                                                                                                                             |
| Source  | HitachiWebServer                                                                                                                                                                                                                                                  |
| Message | The service named HBase 64 Storage Mgmt Web Service reported the following error: >>> (OS 10048) Only one usage of each socket address (protocol/network address/port) is normally permitted. : make_sock: could not bind to address [::]:[redundant-port-number] |

3. From the web browser, confirm that communication with the Analyzer server is normal.
4. Confirm that the web browser is supported by Analyzer server.

## Logging on to Analyzer server unsuccessful

When you cannot log on to Analyzer server, check your user information:

### Procedure

1. Confirm that the user ID and password are correct.
2. Confirm that the user is registered in Analyzer server.
3. Ask a user with User Management permissions to confirm the following:
  - User has required permissions
  - User account is not locked

## Starting Analyzer server does not work

If Analyzer server cannot start, check that the resources of the Analyzer server are sufficient, and the hardware and OS are supported by Analyzer server.

### Procedure

1. Confirm that resources such as memory and disk space are sufficient on the Analyzer server.
2. Confirm that Analyzer server has been installed on the OS and hardware supported by Analyzer server.
3. Run the **hcmds64srv** command with the `status` option to check the operation status of Analyzer server.
4. If the Analyzer server services are not running, start the service.
5. See the log data and take appropriate actions from the error message.
6. If no error message is output to the log, or the problem is not solved, run the **hcmds64getlogs** command to collect the log file, and contact the administrator or Hitachi Vantara Support Contact.

## Analyzer server cannot connect to Analyzer detail view server

If Analyzer server cannot be connected to Analyzer detail view server, check the operating status of Analyzer detail view server and the status of the connection between Analyzer server and Analyzer detail view server.

### Procedure

1. Run the following command on the Analyzer detail view server to verify that the status of the service of the Analyzer detail view server is running:

```
/usr/local/megha/bin/megha-jetty.sh status
```

Output example:

```
Megha server is running
```

2. In the **Administration** tab of Analyzer server, select **System Settings > Analyzer detail view Server**.
3. Click **Edit Settings** to check information about the Analyzer detail view server.
4. Click **Check Connection** to check whether Analyzer server can be properly connected to the Analyzer detail view server.
5. Click **OK**.

## Analyzer probe server cannot connect to Analyzer detail view server using HTTPS

If Analyzer probe server cannot connect to Analyzer detail view server through an HTTPS connection, check the status of the HTTP proxy server on the host on which Analyzer detail view server is installed.

### Procedure

1. Run the following command to check the operation status of the HTTP proxy server:

```
/usr/local/httpProxy/bin/megha-jetty.sh status
```

2. If the HTTP proxy server is not running, run the following command to start it:

```
/usr/local/httpProxy/bin/megha-jetty.sh start
```

## Cannot add a probe using an HTTPS connection in Analyzer probe

If a problem occurs while adding any of the following probes using an HTTPS connection in Analyzer probe, do the following:

- Hitachi Enterprise Storage probe
- Brocade FC Switch (BNA) probe
- Cisco FC Switch (DCNM) probe

### Procedure

1. Check the SSL certificate details in the target environment and the Analyzer probe server. They must have an SSL certificate created by the same certificate authority.

2. If the certificate authority is different, you must create an SSL certificate using the same certificate authority and apply it on the Analyzer probe server by uploading the certificate files to `/usr/local/megha/jetty/etc`.

For information on applying certificates on the Analyzer probe server, refer to [Configuring an SSL certificate \(Analyzer detail view server\) \(on page 322\)](#).

## Cannot start the Analyzer Windows probe service from the Windows Services panel

After installing or upgrading the Analyzer Windows probe, if you are using the Windows **Services** panel to start the Analyzer Windows probe service and a problem occurs while starting the service, then do the following:

1. Check the Analyzer Windows probe logs in the `WindowsProbe.log` file to identify the reason for a problem. You can find the log file at the following location:  
`Analyzer Windows probe installer\bin\Logs`

If a reason is due to a system locale.

2. Verify the system locale. Follow the Microsoft procedure to verify the system locale  
If the system locale is other than the English.
3. Change the system locale to English. Follow the Microsoft procedure to change the system locale.

The following are the supported English System Locales: English (Australia), English (Belize), English (Canada), English (Caribbean), English (India), English (Ireland), English (Jamaica), English (Malaysia), English (New Zealand), English (Philippines), English (Singapore), English (South Africa), English (Trinidad and Tobago), English (United Kingdom), English (United States), English (Zimbabwe).

4. Start the Analyzer Windows probe service.

A similar problem can occur while starting the Analyzer Windows probe service from the Analyzer Windows probe console.

## Collecting maintenance information

If no messages are output when a problem occurs, or you are unable to correct the problem even after following the instructions in the message, collect maintenance information, and then contact customer support.

## Collecting the log file for the Analyzer server

Run the `hcnds64getlogs` command to collect the log file for the Analyzer server.



## Procedure

1. Log on to the host on which the Analyzer server is installed as a user with Administrator permission (Windows) or root permission (Linux).
2. Run the **hcnds64getlogs** command to collect the log file for the Analyzer server.

In Windows

```
Common-component-installation-destination-folder\bin\hcnds64getlogs /
dir output-folder-path
```

In Linux

```
Common-component-installation-destination-directory/bin/hcnds64getlogs
-dir output-directory-path
```

An archive file is output to the specified output destination.

For details about the **hcnds64getlogs** command, see the command reference in the Appendix.

## Collecting the log file for the Analyzer detail view server and the Analyzer probe server

You can download the log files for the Analyzer detail view server and the Analyzer probe server by using a web browser.

The procedure for downloading the log files for the Analyzer detail view server and for the Analyzer probe server is the same.

## Procedure

1. In the web browser, type the Analyzer detail view server or the Analyzer probe server URL:  

```
https://server-IP-address:Port-Number
```

The **Logon** window appears.
2. Log on to the desired server as the admin user and make the appropriate selection:
  - **Analyzer detail view server:** In the application bar, click the Manage icon (⚙️).
  - **Analyzer probe server:** Click the **Manage** link.
3. In the **Manage** window, click the **Download Diagnostic Data** link.
4. In the **Download Diagnostic Data** window, click the **Download** button.

## Collecting the log file for the RAID Agent

Run the **jpcras** command to collect the log file for the RAID Agent.

**Note:**

This procedure is applicable for RAID Agent installed with Ops Center Analyzer. If you are using Tuning Manager - Agent for RAID, see the *Hitachi Command Suite Tuning Manager Agent Administration Guide*.

**Procedure**

1. Log on to the host on which the Analyzer probe server is installed, as a user with the root permission.
2. Run the **jpcras** command to collect the log file for the RAID Agent.

```
/opt/jplpc/tools/jpcras output-directory-path all all
```

An archive file named `jpcrasYYMMDD.tar.Z` is output to the specified output destination.

## Disabling statistics collection for System Diagnostics

By default, System Diagnostics is enabled on the Analyzer detail view server and Analyzer probe server for collection of operating statistics. You can disable the statistics collection using this procedure.

**Procedure**

1. Log on to the Analyzer detail view server or Analyzer probe server through an SSH client (like putty) using the following credentials:

- User: megha
- Password: megha!234

2. Run the following commands:

- `/usr/local/megha/dbgUtils/bin/hdebug.sh`  
`setSystemDiagnosticsConfig -key sds.enabled --value false`
- `/usr/local/megha/dbgUtils/bin/manage-sds.sh stop`

The statistics collection is stopped. But you can still access System Diagnostics by launching it from the Analyzer detail view server UI to view historical data in reports.

## Enabling statistics collection for System Diagnostics

By default, System Diagnostics is enabled on the Analyzer detail view server and Analyzer probe server for collection of operating statistics. If you have disabled collection, you can enable it using this procedure.

**Procedure**

1. Log on to the Analyzer detail view server or Analyzer probe server through an SSH client (like **putty**) using the following credentials:
  - User: **megha**
  - Password: **megha!234**
2. Run the following commands:
  - `/usr/local/megha/dbgUtils/bin/hdebug.sh  
setSystemDiagnosticsConfig -key sds.enabled --value true`
  - `/usr/local/megha/dbgUtils/bin/manage-sds.sh start`

The operating statistics collection is started.

## Restarting a probe stuck in the Stopping state

If you are attempting to Start, Edit, or Delete a probe and it becomes stuck in the "Stopping" state on the Analyzer probe server, follow this procedure to restart the probe.

**Procedure**

1. Log on to the Analyzer probe server through an SSH client (like **putty**) as a root user.



**Note:** If you do not want to stop the **crond** service, you can stop the specific processes of the Analyzer detail view server and Analyzer probe server by using the **crontab -e** command as described in [Stopping the Analyzer detail view server or Analyzer probe server services \(on page 360\)](#) and [Starting the Analyzer detail view server or Analyzer probe server services \(on page 360\)](#)

2. Stop the **crond** service using the command:

```
service crond stop
```

3. Stop the **megha** service using the command:

```
/usr/local/megha/bin/megha-jetty.sh stop
```

4. Confirm the **megha** service has stopped:

```
/usr/local/megha/bin/megha-jetty.sh status
```

5. Go to the probe configuration directory:

```
cd /usr/local/megha/conf/probe
```

6. Make a backup copy of the of the probe properties file using following command syntax:

```
cp probe_type_default.properties probe_type_default.properties_bkp
```

For example:

```
cp vmware_default.properties vmware_default.properties_bkp
```

For a list of the other probe properties files, see the list at the end of this procedure.

7. Open the properties file with an editor such as **vi** as in this example:

```
vi vmware_default.properties
```

8. Change the property `start_type=auto` to `start_type=manual` and save the file.
9. Start the megha service using the command:

```
/usr/local/megha/bin/megha-jetty.sh start
```

10. Confirm the megha service has started:

```
/usr/local/megha/bin/megha-jetty.sh status
```

11. Start the crond service using the command:

```
service crond start
```

12. Log in to the Analyzer probe server UI.  
The affected probe should now be in the "Stopped" state. You can now Edit or Delete the probe and restart data collection.
13. After this process is complete, you should reverse the change made to the properties file (or else the probe will always remain in the "Stopped" state after a restart of the megha service or a reboot of the Analyzer probe server).  
To do this, change `start_type=manual` to `start_type=auto`.

### Probe types

The properties files for each probe type are as follows:

AMS - `ams_default.properties`

Brocade FC Switch (BNA) - `bfa_default.properties`

Brocade FC Switch (CLI) - `brocadesanswitch_default.properties`

Cisco FC Switch (DCNM) - `cfa_default.properties`

Cisco FC Switch (CLI) - `ciscosanswitch_default.properties`

Hitachi Enterprise Storage - `hitachienterprisestorage_default.properties`

Hitachi NAS - `hnas_default.properties`

Linux - `linux_default.properties`

VMware - vmware\_default.properties

---

## Chapter 16: Installing Ops Center Analyzer viewpoint

Install Ops Center Analyzer viewpoint by deploying an OVF and performing initial setup.

### Overview of Analyzer viewpoint

By using Analyzer viewpoint, you can easily display and check the comprehensive operational status of data centers around the world in a single window.

With Analyzer viewpoint, you can do the following:

- Check the overall status of multiple data centers.

By accessing Analyzer viewpoint from a web browser, you can collectively display and view information about supported resources in the data centers.

Even for a large-scale system consisting of multiple data centers, you can check the comprehensive status of all data centers.

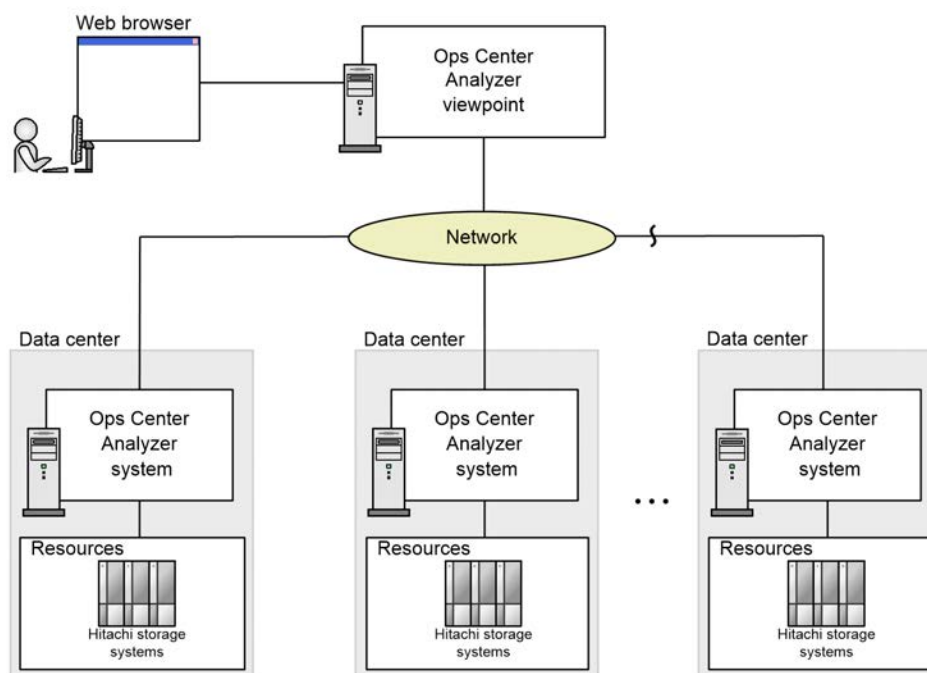
- Easily analyze problems related to resources.

By using the UI, you can display information about resources in a specific data center in a drill-down view and easily identify where a problem occurred.

In addition, because you can launch the Ops Center Analyzer UI from the Analyzer viewpoint UI, you can quickly perform the tasks needed to resolve the problem.

### Analyzer viewpoint system configuration

The following shows an example of an Analyzer viewpoint system configuration. Analyzer viewpoint periodically collects information about each resource from Ops Center Analyzer servers running at multiple data centers.



## Prerequisites

To use Analyzer viewpoint, your environment must meet the following requirements:

- Ops Center Analyzer is 10.0.1 or later.

## System requirements

The following provides the Analyzer viewpoint system requirements.

### Virtual environment requirements

Check the virtual environment requirements as shown in the following table.

| Product name |                | Version                                 |
|--------------|----------------|-----------------------------------------|
| VMware       | vCenter Server | 6.0, 6.5, or 6.7                        |
|              | ESXi           | Use the same version as vCenter Server. |

### Supported browsers

Check the browser requirements as shown in the following table.

| Web browser                   | Version                              |
|-------------------------------|--------------------------------------|
| Firefox                       | ESR 68                               |
| Chrome Browser for enterprise | Latest version of the stable channel |

## Resource requirements for the virtual machine

Check the virtual machine resource settings as shown in the following table.

| Item       | Minimum when the number of LDEVs is 40,000 or less | Minimum when the number of LDEVs is greater than 40,000 and less than 640,000 |
|------------|----------------------------------------------------|-------------------------------------------------------------------------------|
| Processor  | Octa-Core processor                                | Hexadeca-Core processor                                                       |
| Memory     | 64 GB                                              | 256 GB                                                                        |
| Disk space | 1 TB                                               | 8 TB                                                                          |
| Disk type  | SSD (1,000 IOPS)                                   | SSD (10,000 IOPS, 1GB/sec)                                                    |

## Monitoring target requirements

Analyzer viewpoint supports the following storage systems, which are monitored by Ops Center Analyzer, from which data is collected by using the RAID Agent.

- VSP
- VSP E series
- VSP F series
- VSP G series
- VSP 5000 series
- HUS VM

The following methods can be used to collect data about the supported storage systems:

- The command device and the SVP (`Access Type: 1`)
- The command device and the REST API (`Access Type: 2`)

If you use Tuning Manager - Agent for RAID to collect information, you need to change the settings so that the RAID Agent included in the Ops Center Analyzer is used.

## Installing Analyzer viewpoint using a virtual appliance



## Deploying the OVF

Deploy the Analyzer viewpoint OVF file by using the installation media.

Before you install Analyzer viewpoint, be aware of the following:

- The virtual machine you create in the following procedure is for use as the Analyzer viewpoint host only. Do not use this virtual machine for any other purpose.
- After installation, if you change the OS time to an earlier time, Analyzer viewpoint will no longer work properly.
- Make sure the difference between the time of the Analyzer viewpoint virtual machine and the times on the hosts running other Ops Center products is no more than 1 minute. We recommend configuring chrony to synchronize the time between each host and an NTP server. For details, see the step that describes how to set up the NTP server in [Configuring the network \(on page 446\)](#).

### Procedure

1. Log in to the vSphere Client.
2. Deploy the OVF file.

- For vCenter v6.7:

In the OVF template deployment wizard, select the following OVF template and files:

- Analyzer\_viewpoint\_version.ovf
- Analyzer\_viewpoint\_version-disk1.vmdk
- Analyzer\_viewpoint\_version-disk2.vmdk
- Analyzer\_viewpoint\_version-file1.nvram

- For vCenter v6.5 or v6.0:

- a. In the OVF template deployment wizard, select the following OVF template and files:

- Analyzer\_viewpoint\_version-65.ovf
- Analyzer\_viewpoint\_version-disk1.vmdk
- Analyzer\_viewpoint\_version-disk2.vmdk
- Analyzer\_viewpoint\_version-file1.nvram

- b. After the files are deployed, open the **Edit Settings** dialog box for the deployed virtual machine.

- c. Select the **VM Options** tab.

- d. In **Boot Options**, select **EFI** from the **Choose which firmware should be used to boot the virtual machine** drop-down list.

## Using VM customization specification to configure the network

We recommend that you configure the network with VM guest customization of the virtual machine. However, if you prefer not to use VM customization specification, you

can skip this procedure and configure the network manually by performing the procedure described in [Configuring the network \(on page 446\)](#).

### Procedure

1. Log in to the vSphere Client.
2. Create a VM customization specification.
  - a. Select **Menu > Policies and Profiles**. In the **VM Customization Specifications** window, click **New**.
  - b. Follow instructions in the **New VM Guest Customization Spec** window to enter information about the VM Customization Specification.



**Note:** On the **Computer name** screen, we strongly recommend that you specify a computer name without selecting the option to append a numeric value.

- c. Make sure that the VM customization specification you created appears in the list in the **VM Customization Specifications** window.
3. Apply the VM customization specification to the Analyzer viewpoint virtual machine to customize the guest OS.
  - a. Right-click the virtual machine, and then select **Guest OS > Customize Guest OS**.
  - b. In the **Customize Guest OS** window, select the VM customization specification that you created in the previous step, and then click **OK**.

## Upgrading Analyzer viewpoint

To upgrade Analyzer viewpoint, deploy the OVF file from the installation media and inherit the data from the old virtual machine. You must reinstall any Analyzer viewpoint plug-ins.

### Procedure

1. Log in to vSphere Client.
2. Right-click in the vSphere Client window, and then click **Deploy OVF Template** to create a new virtual machine.
3. In vSphere Client, right-click the old virtual machine, and then select **Power > Shutdown Guest OS**.
4. If you did not obtain a snapshot on the old virtual machine, skip this step. If you obtained a snapshot, create a clone of the old virtual machine so that the new virtual machine can take over the snapshot. For the following steps, assume that the clone is the old virtual machine.
5. Copy the virtual disk that was used by the old virtual machine to the newly deployed virtual machine.
  - a. In vSphere Client, open the **Storage** tree view.
  - b. From **datastore**, select the folder where the data from the old virtual machine is stored.

- c. Select the vmdk that was used by the old virtual machine and click **Copy to**.



**Note:** From the files named **Analyzer\_viewpoint\_xx.yy.zz\_N.vmdk**, select and copy the file for which the value of *N* is greatest.

- d. Select the folder where the new virtual machine is stored, and click **OK**.
6. Specify settings to add the existing hard disk to the new virtual machine.
  - a. In vSphere Client, open the **Hosts and Clusters** tree view.
  - b. Right-click the new virtual machine, and select **Edit settings**.
  - c. On the **Virtual Hardware** tab, click the **ADD NEW DEVICE** button, and then select **Existing Hard Disk**.
  - d. From **datastore**, select the folder where the new virtual machine is stored.
  - e. Select the vmdk that was used by the old virtual machine, and click the **OK** button.
  - f. Select **Hard disk 2**, and then click the **x** button and then **OK** to delete the disk.
7. To configure the network, refer to [Using VM customization specification to configure the network \(on page 441\)](#).
8. If you are using vCenter version 6.5 or 6.0, change the boot option to EFI:
  - a. Right-click the new virtual machine, and open the **Edit Settings** dialog box.
  - b. Go to the **VM Options** tab.
  - c. Under **Boot Options**, from the menu **Choose which firmware should be used to boot the virtual machine**, select EFI and click **OK**.
9. Right-click the new virtual machine, and select **Power > Power ON**.
10. Re-import the Analyzer viewpoint plug-ins.
  - a. Use an administrator account to log in to Analyzer viewpoint, and from the plug-in menu in the upper right part of the window, select **Plugin Config**.
  - b. Select the **Dashboards** tab, and click the **Re-import** button for each plug-in.

### Next steps

If you changed the port number for Analyzer viewpoint on the old virtual machine, the firewall settings are not inherited. Specify firewall settings so that the same port can be used on the new virtual machine.

## Upgrading the JDK to be used by Analyzer viewpoint

When Analyzer viewpoint is installed or upgraded, Amazon Corretto 11, which is included in Analyzer viewpoint, is simultaneously installed as a JDK. If the version of the JDK that is already installed is older than those supported by Analyzer viewpoint, upgrade the JDK.

**Before you begin**

- Check the release notes for the versions of Amazon Corretto 11 that are supported by Analyzer viewpoint.
- Before upgrading the JDK, obtain snapshots of the virtual machine that is being used for Analyzer viewpoint.

**Procedure**

1. Check the version of Amazon Corretto 11 that is installed on the virtual machine used for Analyzer viewpoint. If it is the latest version supported by Analyzer viewpoint, you do not need to perform the following steps:
2. From the Amazon Corretto site, download a version of the JDK that is supported by Analyzer viewpoint, and then install the JDK on the virtual machine used for Analyzer viewpoint.
3. Run the RPM command to upgrade Amazon Corretto 11.

## Registering the Analyzer viewpoint license

Register a license for Analyzer viewpoint by using the Ops Center Portal. You need to perform this procedure when you perform a new installation of Analyzer viewpoint or when you upgrade from version 10.0.0.

**Procedure**

1. Locate and record the Analyzer viewpoint UUID.
  - a. Log in to the Ops Center Portal.
  - b. Click the **Launcher** tab to open the **Launcher** window, and the Analyzer viewpoint instance that you want to use, and then click the license status link. The **License** window opens.
  - c. In the **License** window, find the UUID of your product and record it because you need it when requesting a license.
2. Contact your Hitachi Vantara representative to request a license. You must provide your UUID.
3. After receiving the license, register it as follows:
  - a. Log in to the Ops Center Portal.
  - b. Click the **Launcher** tab to open the **Launcher** window, and the Analyzer viewpoint instance that you want to use, and then click the license status link. The **License** window opens.
  - c. Register the license by using one of the following methods:
    - Enter the license key.
    - Specify the license file.
  - d. Click **submit**.  
The license is added to the list.

## Accessing Analyzer viewpoint



**Tip:** After you finish installation, you can log on to the Analyzer viewpoint virtual machine by using the following root user credentials:

- User ID: `root`
- Password: `hitachi`

You must change the password of the root user account after you log in for the first time.

You can access Analyzer viewpoint by using the following address:

```
https://IP-address-of-the-virtual-machine/
```

When you log on to the Analyzer viewpoint UI, the web browser displays a warning because the web server uses a self-signed certificate by default.

## Setting up the monitoring environment

### Before you begin

Register Analyzer viewpoint and Ops Center Analyzer instances in the same Ops Center Common Services. By default, the Analyzer viewpoint is registered in the instance of Ops Center Common Services bundled with the Analyzer viewpoint. If you want to use the bundled Ops Center Common Services, register Ops Center Analyzer in the instance of the bundled Ops Center Common Services. For details, see [Registering Ops Center Analyzer in Ops Center Common Services \(on page 85\)](#). If you want to use Common Services installed on a different host from Analyzer viewpoint host, register Analyzer viewpoint in the Common Services installed on the different host. For details, see [Registering Analyzer viewpoint in Ops Center Common Services running on a different host \(on page 450\)](#)

### Procedure

1. In Ops Center Common Services, register the data center and associate the data center with Ops Center Analyzer. For details, see the *Ops Center Help*.



**Tip:**

- You can use the following command on the Analyzer viewpoint host to check the list of data centers and Ops Center Analyzer system that are monitored by Analyzer viewpoint.

```
/opt/hitachi/analyzer_viewpoint/etl/list_inventory.sh
```

- After you register the data center and the Ops Center Analyzer system, if you want to manually collect monitoring data, run the `run.sh` command. For details, see [Starting the data collection process \(on page 454\)](#).

## Specifying settings so that the host name of Ops Center Common Services can be resolved

If any of the following conditions is met, specify settings so that the host names of individual Ops Center products can be resolved from client machines and from the Analyzer viewpoint host.

- Ops Center products are registered in Ops Center Common Services with their host names.
- A product installed by using the Ops Center OVA is in use.



**Note:** The products installed in the Ops Center OVA are registered in Ops Center Common Services with their host names.

## Advanced Configuration

### Configuring the network

If you do not want to use VM customization specification, manually configure the network.

#### Before you begin

You must have root privilege.

#### Procedure

1. Start the virtual machine.
2. From a VMware vSphere Client, log on to the Analyzer viewpoint virtual machine.
3. Configure the network by network manager as follows:

- a. To configure the network, run the following command to make sure that device named `ens192` is available.

```
nmcli device
```

- b. Set an IP address, gateway, and DNS server. For example:

```
nmcli connection modify ens192 ipv4.addr 192.0.2.10/24
nmcli connection modify ens192 ipv4.gateway 192.0.2.1
nmcli connection modify ens192 ipv4.dns 192.0.2.2
nmcli general hostname host-name
```

As an option, you can register a second DNS server. For example:

```
nmcli connection modify ens192 +ipv4.dns 192.0.2.3
```

- c. Confirm that your host name can be resolved. If your host name cannot be resolved, run the following command to edit the hosts file.

```
/opt/hitachi/analyzer_viewpoint/bin/edit-hosts
```

- d. Restart the network service.

```
systemctl restart network
```

#### 4. Change the time zone setting to your local time zone.

- a. Run the following command to check the available time zones.

```
timedatectl list-timezones
```

- b. Change the time zone to your time zone. For example:

```
timedatectl set-timezone America/Los_Angeles
```

- c. Confirm the time zone and the current date and time.

```
timedatectl
```

#### 5. (Optional) If you want to specify the NTP server to be synchronized, set up the NTP service.

- a. Modify the configuration file.

```
vi /var/opt/hitachi/analyzer_viewpoint/system/chrony.conf
```

- b. Comment out all servers, and then specify the NTP server that you want to use. For example:

```
server 0.pool.ntp.org iburst
server 1.pool.ntp.org iburst
server 2.pool.ntp.org iburst
```

```
server 3.pool.ntp.org iburst
server NewNTPServer iburst
```

- c. Restart NTP service.

```
systemctl restart chronyd
```

- d. Confirm the settings.

```
chronyc sources
```

6. Restart the virtual machine.

```
reboot
```

## Changing the maximum amount of memory used by the data collection process

If you are monitoring a huge number of resources, you can ensure sufficient memory by changing the maximum amount of memory that can be used by the data collection process.

We recommend allocating about half of the memory of the Analyzer viewpoint virtual machine. For more information, see [Resource requirements for the virtual machine \(on page 440\)](#).

### Before you begin

You must have root privilege.

### Procedure

1. Log on to the Analyzer viewpoint virtual machine.
2. Open the following file.

```
/var/opt/hitachi/analyzer_viewpoint/etl/config/runtime.conf
```

3. Specify the maximum amount of memory (in GB) that can be used by the data collection process.

Example:

```
VIEWPOINT_ETL_MAX_HEAP_IN_GB=128
```

## Making Analyzer viewpoint accessible by using the host name

To make Analyzer viewpoint accessible through the host name, run the **setservicehostname** command.



**Before you begin**

- You must have root privilege.
- The Analyzer viewpoint host must be able to access itself by using its own host name. If the host name cannot be resolved, run the **edit-hosts** command, which is stored in the directory `/opt/hitachi/analyzer_viewpoint/bin`, to edit the hosts file.

**Procedure**

1. Run the following command.

```
/opt/hitachi/analyzer_viewpoint/bin/setservicehostname host-name
```

**Configuring Analyzer viewpoint host name**

If you use an IP address to access Analyzer viewpoint, this procedure is unnecessary. If you use a host name to access Analyzer viewpoint and want to change the host name, perform this procedure.

**Before you begin**

- You must have root privilege.
- If you are using the instance of Ops Center Common Services running on a different host, skip steps 1 to 7.

**Procedure**

1. Run the following command to change the host name set for the Ops Center Common Services:

```
/opt/hitachi/CommonService/utility/bin/cschgconnect.sh -h host-name
```



**Note:** For details about the **cschgconnect.sh** command, see the section about changing host names in the *Hitachi Ops Center Installation and Configuration Guide*. When Ops Center Common Services is running on the same host as Analyzer viewpoint, you cannot use the `-p` option of the **cschgconnect.sh** command. In addition, you do not need to perform the procedure for issuing an Ops Center Common Services server certificate.

2. Restart the Ops Center Common Services.

```
systemctl restart csportal.service
```

3. Stop the Analyzer viewpoint services.

```
systemctl stop analyzer-viewpoint.target
```

4. Start the API gateway services.

```
systemctl start analyzer-viewpoint-apigw.service
```

5. Run the following command:

```
/opt/hitachi/analyzer_viewpoint/bin/setupcommonservice --csUri Common-Services-url --csUsername Common-Services-username --csPassword Common-Services-password
```



**Note:** The Common Services user specified for this command must belong to the **opscenter-administrators** user group.

Example:

```
/opt/hitachi/analyzer_viewpoint/bin/setupcommonservice --csUri https://viewpointhost/ --csUsername sysadmin --csPassword sysadmin
```

6. Start the Analyzer viewpoint services.

```
systemctl start analyzer-viewpoint.target
```

7. Confirm that Analyzer viewpoint can be accessed from the Ops Center Portal by using the following URL.

```
https://host-name-of-the-virtual-machine[:port-number]/portal
```

8. Run the following command:

```
/opt/hitachi/analyzer_viewpoint/bin/setservicehostname host-name
```



**Note:** If you are using the instance of Ops Center Common Services bundled with Analyzer viewpoint, this procedure also changes the host name of Ops Center Common Services. Run the **setupcommonservice** command for the products registered in Ops Center Common Services to set new host names. For details, see the documentation for each product.

## Registering Analyzer viewpoint in Ops Center Common Services running on a different host

By default, the Analyzer viewpoint is registered in the instance of Ops Center Common Services bundled with the Analyzer viewpoint. Perform this procedure only if you want to use Common Services installed on a different host.

### Before you begin

You must have root privilege.

**Procedure**

1. Stop the Analyzer viewpoint services:

```
systemctl stop analyzer-viewpoint.target
```

2. Run the following command to register Analyzer viewpoint in Ops Center Common Services.

```
/opt/hitachi/analyzer_viewpoint/bin/setupcommonservice --csUri Common-Services-url --csUsername Common-Services-username --csPassword Common-Services-password
```



**Note:** The Common Services user specified for this command must belong to the **opscenter-administrators** user group.

Example:

```
/opt/hitachi/analyzer_viewpoint/bin/setupcommonservice --csUri https://192.0.2.1/ --csUsername sysadmin --csPassword sysadmin
```

3. Restart the services.

```
systemctl start analyzer-viewpoint.target
```

## Changing the Analyzer viewpoint port number

**Before you begin**

You must have root privilege.

**Procedure**

1. To change the port number, use the following command:

```
/opt/hitachi/analyzer_viewpoint/bin/changeportnumber port-number
```

2. After running this command, you must use the following URL to access Analyzer viewpoint:

```
https://host-name-or-IP-address-of-the-virtual-machine:port-number/
```



**Note:** If you are using the instance of Ops Center Common Services bundled with Analyzer viewpoint, this command also changes the port number of Ops Center Common Services. Run the **setupcommonservice** command for the products registered in Ops Center Common Services to set new port numbers. For details, see the documentation for each product.

## Changing the HTTPS server certificate of Analyzer viewpoint

Although viewpoint server uses a self-signed certificate by default, you can also register and use a custom certificate.

### Before you begin

You must have root privilege.

### Procedure

1. Copy the certificate and key files that you want to use into the following directory:  
`/var/opt/hitachi/analyzer_viewpoint/apigw/ssl`
2. Log on to the Analyzer viewpoint virtual machine.
3. Open the following file.  
`/var/opt/hitachi/analyzer_viewpoint/apigw/user.conf`
4. Uncomment the `KONG_SSL_CERT` and `KONG_SSL_CERT_KEY` lines and add the path to the certificate and key files.

Example:

```
KONG_SSL_CERT=/var/opt/hitachi/analyzer_viewpoint/apigw/ssl/user.crt
KONG_SSL_CERT_KEY=/var/opt/hitachi/analyzer_viewpoint/apigw/ssl/
user.key
```

5. Restart the API Gateway service.

```
systemctl restart analyzer-viewpoint-apigw.service
```

## Using Analyzer viewpoint

### Creating user accounts

You can create user accounts for the Analyzer viewpoint by using the Ops Center Portal.

### Before you begin

You must have Admin privilege for Ops Center Common Services.



**Note:** By default, the built-in Admin user account of Ops Center Common Services is also registered in the Analyzer viewpoint as a user with Admin privileges. If you disable the built-in Admin user account of Ops Center Common Services, assign Admin privileges for Analyzer viewpoint to another Admin user account in Ops Center Common Services.

## Procedure

1. Log in to the Ops Center Portal by using an Ops Center user account that has permission to create users.  
For details, see the *Ops Center Help*.
2. In the Ops Center Portal user management window, create a user account for using Analyzer viewpoint. Be sure to specify an email address.



**Note:** To register an existing Ops Center Common Services user in Analyzer viewpoint, you do not need to create a new user account. However, be sure to specify an email address.

3. Contact the user whose account you created in the Ops Center Common Services, and ask the user to log in to the Analyzer viewpoint.



**Note:** When an Ops Center Common Services user accesses Analyzer viewpoint for the first time, the user is registered as a user with Viewer role.

## Next steps

Contact the administrator of Analyzer viewpoint, and ask him or her to assign the appropriate role.

## Assigning user roles

The following user roles are available for the Analyzer viewpoint.

- **Viewer:** Users assigned this role can view dashboards.
- **Editor:** Users assigned this role can edit dashboards, in addition to performing the operations that are available to users assigned the Viewer role.
- **Admin:** Users assigned this role can use all the management functions (such as changing user roles), in addition to performing the operations that are available to users assigned the Editor role.

For Ops Center Common Services users except the built-in Admin user, the Viewer role is set when the individual user logs in to the Analyzer viewpoint for the first time. The same applies to Ops Center Common Services users who are externally authenticated by an Active Directory server. After the individual user logs in for the first time, change the user's roles as needed.

## Before you begin

To perform this procedure, you must have administrator permissions for Analyzer viewpoint.

## Procedure

1. Log in to Analyzer viewpoint by using an administrator account.
2. On the screen displayed by clicking **Configuration > Users**, select the **Role** to assign to the user.

3. If you assigned the user the Admin role, click **Server Admin > Users**. On the screen that appears, select the applicable user and then enable **Analyzer viewpoint Admin** under **Permissions**.

## Starting the data collection process

Data is automatically collected every day at 0:15 AM (according to the time zone of the Analyzer viewpoint virtual machine). Run the following command to collect data manually, for example, after initial setup or if the processing to automatically collect data is not performed (because of system maintenance or some other reason).

```
/opt/hitachi/analyzer_viewpoint/etl/run.sh
```

The process collects data from the previous day and normally takes ten or more minutes to complete.

## Collecting log files

### Before you begin

You must have root privilege.

### Procedure

1. To collect log files, use the following command:

```
/opt/hitachi/analyzer_viewpoint/bin/diag
```

The collected log files are output to the current directory.

## Backing up and restoring Analyzer viewpoint

Clone the virtual machine on which Analyzer viewpoint is running, and then back up the cloned virtual machine based on the environment and operation policy. Similarly, when restoring the virtual machine, use the virtual machine you backed up.

---

## Appendix A: Ops Center Analyzer CLI commands

Use CLI commands to run operations and make configuration changes in Ops Center Analyzer.

### List of Commands

The following table lists the Ops Center Analyzer commands.

#### The Analyzer server commands

| Command                 | Description                                                                                                                                                                                                                                                                                                                                           |
|-------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>backupsystem</b>     | Backs up Analyzer server setting information in the folder you specify.                                                                                                                                                                                                                                                                               |
| <b>encryptpassword</b>  | Creates a password file to be specified as an argument of commands in Analyzer server.                                                                                                                                                                                                                                                                |
| <b>hcnds64checkauth</b> | Checks the settings in the <code>exauth.properties</code> file and the connection to the external authentication server when connecting to an external authentication server.                                                                                                                                                                         |
| <b>hcnds64fwcancel</b>  | Registers an exception so that communication between the Analyzer server and the web browser is not blocked by the Windows-based firewall.                                                                                                                                                                                                            |
| <b>hcnds64getlogs</b>   | Collects log files that are output during operation of Analyzer server, and then outputs the log files to an archive file.                                                                                                                                                                                                                            |
| <b>hcnds64intg</b>      | <p>Deletes authentication data registered in the repository of the server that manages user accounts. The command also displays the address of the server in which the authentication data is registered.</p> <p>If you fail to delete authentication data when uninstalling Analyzer server, use this command to delete the authentication data.</p> |

| Command                     | Description                                                                                                                                                                                                                                                                                    |
|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>hcnds64ldapuser</b>      | Registers, in the Analyzer server, a user account used to search user information in external authentication servers when connecting to an external authentication server. This command also deletes user accounts used to search user information that are registered in the Analyzer server. |
| <b>hcnds64prmset</b>        | Registers, changes, and cancels the registration of the host that manages the user accounts used for connection with Ops Center Automator.                                                                                                                                                     |
| <b>hcnds64radiussecret</b>  | When connecting to an external authentication server, registers a shared secret for the RADIUS server in the Analyzer server or deletes a shared secret registered in the Analyzer server.                                                                                                     |
| <b>hcnds64srv</b>           | Starts or stops Analyzer server services and databases. The command also displays the status of Analyzer server services.                                                                                                                                                                      |
| <b>hcnds64ssltool</b>       | Creates private keys, CSRs, and self-signed certificates (including its content files), which are required for SSL connection.                                                                                                                                                                 |
| <b>hcnds64unlockaccount</b> | Unlocks a user account. Use this command when you cannot log on to Analyzer server because all the user accounts are locked.                                                                                                                                                                   |
| <b>reloadtemplate</b>       | Reload the Analyzer server template files during the startup of Analyzer server.                                                                                                                                                                                                               |
| <b>restoresystem</b>        | Restores the backup for Analyzer server settings information that you collected by running the <b>backupsystem</b> command.                                                                                                                                                                    |
| <b>setupcommonservice</b>   | Registers the Ops Center Analyzer to Ops Center Common Services.                                                                                                                                                                                                                               |

### The Analyzer probe server commands

| Command                  | Description                                                                                                                                                                 |
|--------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>collection_config</b> | Changes the data collection intervals for the RAID Agent that is installed with Ops Center Analyzer.                                                                        |
| <b>htmssltool</b>        | Creates private keys, CSRs, and self-signed certificates (including its content files), which are required to establish an SSL connection by using the RAID Agent services. |



## Command usage guidelines

You must consider the following when using commands.

- You must have Administrator permission (Windows) or root permission (Linux).
- If the Analyzer server is running on Windows, replace the hyphen (-) immediately before each argument with a slash (/).
- To interrupt a running command, press **Ctrl+C**, make sure that you read any messages and check for problems. If necessary, repeat the command. If you interrupt a command, the return value might be undefined.

### In Windows

- If the command is to be run in an environment where User Account Control (UAC) requires Administrator permission, run the command from the administrator console of the Analyzer server.

To display the administrator console:

#### For Windows Server 2012

1. From the desktop, display the **Start** window.
  2. Right-click the **Start** window to display **All apps**.
  3. In the **Hitachi Ops Center Analyzer** folder, select **Analyzer Command**.
- If you enable Quick Edit Mode in the command prompt, and then click the mouse in the window, the window output is stopped until the quick edit mode is canceled. Therefore, do not use the quick edit mode.

### In Linux

- If the maximum output size of the core file is set to 0, core dumps are effectively disabled. To output a core dump when a failure occurs, run the **ulimit** command before running each command, and set the maximum output size to **unlimited**.

## Usable characters for command arguments

You can specify the following characters for command arguments:

- The specification method for command arguments must comply with the specifications of the OS command prompt. Therefore, if an argument value contains a space ( ) or special symbols, you must escape such characters by enclosing each of the characters with double quotation marks (").
- You can use the following types of characters when specifying a path with an argument of a command:

Alphanumeric characters, underscores (\_), periods (.), hyphens (-), spaces ( ), left parentheses ( ( ), right parentheses ( ) ), hash marks (#), at marks (@), colons (:), and backslash (\)

You can use a colon only as a drive delimiter. You can use a backslash (\) only as a folder delimiter.

- When specifying a path in an argument, you cannot use a path in UNC format.
- When specifying a path in an argument, you cannot use a path that has a folder name that begins or ends with a space. Also, you cannot specify a folder name that consists of only spaces.
- When specifying a path in an argument, you cannot use a path that has a folder name that begins or ends with a period (.). Also, you cannot specify a folder name that consists of only periods.
- Unless otherwise stated, the path length is from 1 to 230 characters in the absolute path.
- Unless otherwise stated, each command argument is case-sensitive.
- Do not specify reserved words for the OS as a file name or folder name.

## backupsystem

Use this command to back up Analyzer server setting information in the directory you specified.

### Format

```
backupsystem
 -dir output-directory
 -type {all | Analytics}
 [-auto]
```

### Options

#### **dir** *output-directory*

Specify the directory in which the backup file is stored with the absolute or relative path.

#### **type** {all | Analytics}

Specify the type of information for backup.

##### **all**

Backs up Analyzer server and Common component. Common component manages the user information.

##### **Analytics**

Backs up only Analyzer server.

#### **auto**

Automatically stops or starts services and databases of Analyzer server and products that use Common component. If you omit this option, these services and databases are not automatically stopped or started.

## Location

In Windows

*Analyzer-server-installation-destination-folder\Analytics\bin*

In Linux

*Analyzer-server-installation-destination-directory/Analytics/bin*

## Notes

- Make sure that the directory in which the backup file is to be stored has sufficient free space. Use the following formula to calculate the required amount of free space:

### In Windows

5 GB + Size of *Analyzer-server-installation-destination-folder*  
*\Analytics\data*

### In Linux

5 GB + Size of *Analyzer-server-installation-destination-directory/*  
*Analytics/data*

If products that use Common component are installed on the Analyzer server, add the capacity required to back up information for those products.

- The following files for HTTPS connections are not backed up. If necessary, back up these files manually.

- SSL server certificate file
- Private-key file

In addition, the files for HTTPS connections are defined in the `httpsd.conf` file and the `user_httpsd.conf` file.

- If all of the following conditions are met, use the **hcmds64srv** command to stop the service before running the **backupsystem** command.
  - The `auto` option is not specified.
  - `all` is specified for the `type` option.
- If products that use Common component are installed on the Analyzer server, run the **restoresystem** command by specifying `type Analytics` to restore only Analyzer server. You can back up the data required for restoring only Analyzer server by specifying `type Analytics` for the **backupsystem** command.
- If you specify `Analytics` for the `type` option, the following files are not backed up. If you must back up these files, back them up manually.
  - Security definition file (`security.conf`)
  - File for setting port numbers and host names (`user_httpsd.conf`)

**Return values**

| Return value | Description                                               |
|--------------|-----------------------------------------------------------|
| 0            | The command ran normally.                                 |
| 1            | The argument is invalid.                                  |
| 2            | Command running was interrupted.                          |
| 3            | The service status is invalid.                            |
| 4            | Another command is currently running.                     |
| 7            | The path is invalid.                                      |
| 9            | The path does not exist.                                  |
| 10           | The path cannot be accessed.                              |
| 11           | The directory is not empty.                               |
| 14           | You do not have permission to run this command.           |
| 100          | The backup operation failed.                              |
| 101          | The start or stop of the service failed.                  |
| 255          | Command running was interrupted because of another error. |

**Example**

The following example shows the use of this command to back up information of Analyzer server:

```
backupsystem -dir /tmp -type Analytics -auto
```

**collection\_config**

Use this command to change data collection intervals for all instances of RAID Agent installed with Ops Center Analyzer that have the same `Access Type` (a setting in the instance information). Execute this command on the Analyzer probe server. To change the intervals for collecting data from VSP family or HUS VM, specify the same value as the data collection intervals for both the RAID Agent and the Hitachi Enterprise Storage probe.

**Note:**

- RAID Agent bundled with Ops Center Analyzer can use various methods to collect performance data. These data collection methods have different characteristics, and the time required to collect data varies depending on which method is used. Furthermore, for some methods, the collection interval cannot be changed. Data collection method is determined by the value of `Access Type`, which is specified when an instance is created.

As such, you can use this command to specify a collection interval for each `Access Type` and to check records can be collected based on the `Access Type`.

- For details about how to change data collection intervals for Tuning Manager - Agent for RAID, see the *Hitachi Command Suite Tuning Manager Agent Administration Guide*.

**Format**

```
collection_config
{showinterval -at AccessType |
 changeinterval -at AccessType -r record-ID {-i data-collection-
interval | -reset} [-stop | -restart] |
 showaccesstype {-at AccessType} |
 service {-start | -stop | -status}}
```

**Options****showinterval -at AccessType**

Displays the data collection interval and other information for a specific `Access Type`.

**-at AccessType**

Specifies the `Access Type` for which you want to check the data collection interval.

Out of the execution results, the records with `RW` displayed in the `Mode` column can be changed.

The following table shows the items displayed in the list:

| Item   | Description                 |
|--------|-----------------------------|
| Record | The record ID in RAID Agent |

| Item    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|---------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Mode    | <p>Indicates whether data collection intervals can be changed</p> <ul style="list-style-type: none"> <li>▪ <b>RW:</b> Can be changed.</li> <li>▪ <b>R:</b> Cannot be changed.</li> <li>▪ <b>N/A:</b> Cannot be changed because data cannot be collected.</li> </ul>                                                                                                                                                                                                                                                                                                                          |
| Type    | <p>Details of data collection intervals set for the record</p> <ul style="list-style-type: none"> <li>▪ <b>Collection Interval:</b> The value of the data collection intervals of the record is displayed in the <code>Current</code> column.</li> <li>▪ <b>Sync Collection With:</b> The value of the data collection intervals of the record is synchronized with the record values displayed in the <code>Current</code> column.</li> <li>▪ <b>Not Collectable:</b> This value is displayed when <code>Mode</code> is N/A. This indicates that the record cannot be collected.</li> </ul> |
| Current | <p>The value specified as data collection intervals. The following information is displayed according to the value in the <code>Type</code> column:</p> <ul style="list-style-type: none"> <li>▪ For <b>Collection Interval</b> Data collection intervals (unit: seconds)</li> <li>▪ For <b>Sync Collection With</b> ID of the record with which the value of data collection intervals is to be synchronized</li> <li>▪ For <b>Not Collectable</b> - (hyphen)</li> </ul>                                                                                                                    |
| Default | <p>The default value. The following information is displayed according to the value in the <code>Type</code> column:</p> <ul style="list-style-type: none"> <li>▪ For <b>Collection Interval</b> Data collection intervals (unit: seconds)</li> <li>▪ For <b>Sync Collection With</b> ID of the record with which the value of data collection intervals is to be synchronized</li> <li>▪ For <b>Not Collectable</b> - (hyphen)</li> </ul> <p>Note that, for some records, the default data collection intervals vary depending on the <code>Access Type</code>.</p>                         |

| Item     | Description                                                                                                                                                                                 |
|----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Modified | Information indicating whether the value specified for the data collection interval is customized. <ul style="list-style-type: none"> <li>▪ <b>Y:</b> The setting is customized.</li> </ul> |

**changeinterval -at *AccessType* -r *record-ID* {-i *data-collection-interval* | -reset} [-stop | -restart]**

Specify, for a specific *Access Type*, the record whose data collection interval you want to change and the new data collection interval.

One execution of the command allows you to change the data collection intervals for only one record. When you want to execute this subcommand, stop the RAID Agent service.

**-at *AccessType***

Specifies the *Access Type* whose data collection interval you want to change.

**-r *record-ID***

Specifies the ID of the record for which you want to change data collection intervals.

If the specified record does not exist, or if the data collection intervals for the specified record cannot be changed, an error occurs.

**-i *data-collection-interval***

Specifies a value (unit: seconds) for the data collection interval to use for the specified record after the change.

The values that can be specified vary depending on the record.

The following table shows the requirements for the values to be specified as data collection intervals for each record. Note that this table includes records for which, depending on the *Access Type*, you might not be able to change the collection interval. To check whether the collection interval can be changed for a particular *Access Type*, use the subcommand **showinterval**.

| Record ID                        | Requirement for the values to be specified as data collection intervals                       |
|----------------------------------|-----------------------------------------------------------------------------------------------|
| PD_PLC, PD_PLTC, PD_VVC, PD_VWTC | A value that is a multiple of 3,600 and a divisor of 86,400 in the range from 3,600 to 86,400 |

| Record ID                                                                                                                                                                                                                         | Requirement for the values to be specified as data collection intervals                                                 |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------|
| PD_PEFF, PD_PLF, PD_PLR, PD_PLTR, PD_PLTS, PD_SEFF, PD_VVF                                                                                                                                                                        | A value that is a multiple of 60 and a divisor of 3,600, or a value that is a multiple of 3,600 and a divisor of 86,400 |
| PD_UMS, PI, PI_CHS, PI_CLMS, PI_CLPS, PI_LDA*, PI_LDS*, PI_LDSX, PI_PLS*, PI_PRCs, PI_PTS, PI_PTSX, PI_RGS*                                                                                                                       | A value that is a multiple of 60 and a divisor of 3,600 in the range from 60 to 3,600                                   |
| PI_PLTI, PI_VVTI                                                                                                                                                                                                                  | A value that is a multiple of 300 and a divisor of 3,600 in the range from 300 to 3,600                                 |
| *: Note that if the value of data collection intervals is set to a value smaller than the default value, the KAVE00227-W message might be output continuously. In this case, increase the value of the data collection intervals. |                                                                                                                         |

For details about the default setting of data collection intervals for each record, see the *Hitachi Ops Center Analyzer REST API Reference Guide*.

**-reset**

Returns the data collection interval for the specified record to the default value.

**-stop**

Stops the instance for which the data collection interval is to be updated, as well as the RAID Agent service.

**-restart**

Stops the instance for which the data collection interval is to be updated, as well as the RAID Agent service, and then restarts them after the data collection interval is updated.

**showaccesstype {-at *AccessType*}**

Shows the *Access Type* for each instance.

**-at *AccessType***

Specifies the *Access Type* for which you want to show information. If this option is omitted, information about all instances is shown.

The following table shows the items displayed in the list:



| Item       | Description   |
|------------|---------------|
| AccessType | Access Type   |
| Instance   | Instance name |

**service {-start | -stop | -status}**

Uses RAID Agent services. You can specify the following options:

**-start**

Starts RAID Agent services

**-stop**

Stops RAID Agent services

**-status**

Displays the execution statuses of RAID Agent services

## Location

This command is stored in the following directory on the Analyzer probe server:

/opt/hitachi/Analytics/bin

## Notes

The data collection intervals of the records that have been changed by using this command are applied to all instance environments that have the same `Access Type`.

## Return values

| Return value | Description                                                                                            |
|--------------|--------------------------------------------------------------------------------------------------------|
| 0            | The command ran normally.                                                                              |
| 10           | The specified arguments are invalid.                                                                   |
| 12           | The environment is invalid.                                                                            |
| 13           | The specified record does not exist.                                                                   |
| 14           | The data collection interval cannot be changed for the specified record and <code>Access Type</code> . |
| 15           | The value specified for the data collection interval is invalid.                                       |
| 16           | Execution of the command was suspended because the RAID Agent service is not stopped.                  |
| 17           | The instance to be updated does not exist.                                                             |

| Return value | Description                                    |
|--------------|------------------------------------------------|
| 20           | Failed to stop the RAID Agent service.         |
| 21           | Failed to update the data collection interval. |
| 22           | Failed to start the RAID Agent service.        |
| 23           | Other config commands are running.             |
| 100          | Failed to access the file.                     |
| 254          | The system environment is invalid.             |
| 255          | An unexpected error occurred.                  |

### Example

To display a list of information about all records when the `Access Type` is 1:

```
collection_config showinterval -at 1
```

To change the value of the data collection interval to 7,200 seconds (2 hours) for the record PD\_PLC in all instance environments for which the `Access Type` is 1:

```
collection_config changeinterval -at 1 -r PD_PLC -i 7200 -restart
```

To display the `Access Type` of all instances of RAID Agent:

```
collection_config showaccesstype
```

To start RAID Agent services:

```
collection_config service -start
```

## encryptpassword

Use this command to generate a password file to be specified as the argument of a command in Analyzer server. To generate a password file, the user must be registered in Analyzer server.

### Format

```
encryptpassword
 -user user-ID
 -password password
 -passwordfile password-file-path
```

## Options

### **user** *user-ID*

Specify the user ID of the Analyzer server user for whom you want to create a password file. The user must have the Admin or Modify permission for IAA, or the User Management permission.

You can specify from 1 to 256 characters.

You can use alphanumeric characters and the following characters:

Exclamation marks (!), hash marks, dollar signs (\$), percent signs (%), ampersands (&), single quotation marks ('), left parentheses, right parentheses, asterisks (\*), plus signs (+), hyphens, periods, equal signs (=), at marks, backslashes, carets (^), underscores, and vertical bars (|)

The user ID is not case sensitive.

### **password** *password*

Specify the password of the user specified in the `user` option.

You can specify from 1 to 256 characters.

Usable character types are the same as for the `user` option.

### **passwordfile** *password-file-path*

Use an absolute or relative path to specify a path of the password file to be created.

## Location

In Windows

*Analyzer-server-installation-destination-folder\Analytics\bin*

In Linux

*Analyzer-server-installation-destination-directory/Analytics/bin*

## Return values

| Return value | Description                                              |
|--------------|----------------------------------------------------------|
| 0            | The command ran normally.                                |
| 1            | The argument is invalid.                                 |
| 2            | Command running was interrupted.                         |
| 3            | The service status is invalid.                           |
| 4            | An exclusion error occurred.                             |
| 5            | Communication failed.                                    |
| 6            | Authentication failed. (The specified value is invalid.) |

| Return value | Description                                               |
|--------------|-----------------------------------------------------------|
| 7            | The path is invalid.                                      |
| 8            | The output destination path exists.                       |
| 9            | The path does not exist.                                  |
| 10           | The path cannot be accessed.                              |
| 14           | You do not have permission to run this command.           |
| 200          | The password file could not be generated.                 |
| 255          | Command running was interrupted because of another error. |

## hcmds64checkauth

When connecting to an external authentication server, use this command to check the settings of the `exauth.properties` file and the connections to the external authentication server.

If you execute this command, the command will perform checks in the following four phases, and then the results will be displayed:

- Phase 1: The command checks whether the property used when connecting to the external authentication server is correctly set in the `exauth.properties` file.
- Phase 2: The command checks whether the properties for the external authentication server and the external authorization server are correctly set in the `exauth.properties` file.
- Phase 3: The command checks whether a connection to the external authentication server can be established.
- Phase 4: If the settings are specified so that an external authorization server is also connected, the command checks whether a connection to the external authorization server can be established, and whether the authorization group can be searched.

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.
```

### Format

```
hcmds64checkauth
 [-user user-ID]
 [-pass password]
 [-summary]
```

## Options

### **user** *user-ID*

Specify the user ID of the user account registered in the external authentication server or the external authorization server for which the connection is to be checked.

If you execute the command without specifying the `user` option, you will be prompted to enter a user ID.

- For LDAP authentication

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

Specify the user ID of the user account registered in the RADIUS server.

- For Kerberos authentication

When connecting to the external authentication server only, specify the user ID of the user account that is registered in the Analyzer server and for which the authentication method to be performed is Kerberos.

When connecting also to the external authorization server, specify the user ID of the user account that is not registered in the Analyzer server.

### **pass** *password*

Specify the password of the user ID specified in the `user` option.

If you execute the command without specifying the `pass` option, you will be prompted to enter a password.

### **summary**

This option simplifies the confirmation message that appears when the command is executed.

If this option is specified, the messages to be displayed are limited to messages indicating whether each processing phase is successful or failed, error messages, and messages indicating the results. However, if an error message similar to the message indicating the results is to appear, the former error message is omitted and only the latter resulting message is displayed.

## Location

### In Windows

*Common-component-installation-destination-folder\bin*

### In Linux

*Common-component-installation-destination-directory/bin*

## Notes

- You cannot specify a user account with a *user-ID* or *password* that begins with a forward slash (/) when using Windows or begins with a hyphen (-) when using Linux.
- If you are using Kerberos authentication and the realm name is specified multiple times in the `exauth.properties` file, check the user account for each realm. In addition, specify the user ID using the following format:
  - When specifying a user who does not belong to the realm specified for `auth.kerberos.default_realm` in the `exauth.properties` file, specify a value in the form of *user-ID@realm-name*.
  - When specifying a user who belongs to the realm specified as the `auth.kerberos.default_realm` in the `exauth.properties` file, you can specify a value for *user-ID* without specifying the realm name.
- When you are using LDAP authentication in a multi-domain configuration and you run the **hcmds64checkauth** command, the authentication is checked for all connected external authentication servers specified in the `exauth.properties` file and the results are displayed for each.
 

If an external authentication server does not have registered user accounts that match the user accounts specified in the **hcmds64checkauth** command, an error message with this information is generated and displayed as a check result in phase 3. In this case, processing might end because of failure during the phase 3 confirmation. In this case, use a user account registered on the external authentication server to check the connection of the external authentication server.
- If Ops Center Automator is connected, run the **hcmds64checkauth** command on the server that is set as the primary server.

## Return values

| Return value | Description                                                                                                                                                                                                                                        |
|--------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 0            | The command ran normally.                                                                                                                                                                                                                          |
| 1 - 99       | This code indicates the total number of syntax errors.                                                                                                                                                                                             |
| 100          | This is the return code when the number of syntax errors exceeds 100 lines.                                                                                                                                                                        |
| 101 - 199    | A connection or authentication error occurred.<br>Unit's place: Number of connection errors<br>Ten's place: Number of authentication errors<br>The maximum number of each place is nine. If more than nine errors occur, each place displays nine. |
| 250          | The command is executed on the secondary server.                                                                                                                                                                                                   |

| Return value | Description                                                                           |
|--------------|---------------------------------------------------------------------------------------|
| 252          | The common item setting in the definition file is incorrect.                          |
| 253          | The settings for connecting to the external authentication server are not configured. |
| 254          | The argument is invalid.                                                              |
| 255          | The command ran abnormally.                                                           |

### Example

The following example shows how to use the command to verify the connection with the external authentication server:

```
hcnds64checkauth -user user01 -pass TTdate00 -summary
```

## Escaping special characters

The following explains how to escape when executing the `hcnds64ldapuser` command, `hcnds64radiussecret` command, or `hcnds64checkauth` 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, ampersands (&), vertical bars (|), carets (^), left angle brackets (<), right angle brackets (>), left parentheses ( ( ), right parentheses ( ) )

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, hash marks (#), ampersands (&), single quotation marks ( ' ), left parentheses ( ( ), right parentheses ( ) ), tildes (~), backslashes (\), grave accent marks ( ` ), left angle brackets (<), right angle brackets (>), semicolons (;), and vertical bars (|)

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 `hcnds64radiussecret` command is `secret01\`, escape it as follows:

**In Windows:**

```
hcnds64radiussecret /set secret01\\ /name ServerName
```

**In Linux:**

Use either of the following formats:

```
hcnds64radiussecret -set secret01\\ -name ServerName
```

```
hcnds64radiussecret -set "secret01\\" -name ServerName
```

## hcnds64fwcancel

Use this command to register an exception so that communication between the Analyzer server and the web browser is not blocked by the Windows-based firewall.

**Format**

```
hcnds64fwcancel
```

**Location**

*Common-component-installation-destination-folder\bin*

**Return values**

This command has no return value. To determine whether the processing ran normally, check whether HBase (Web) is correctly registered in the inbound rules of the Windows-based firewall.

You can check the inbound rules for Windows Firewall in the Windows-based system control panel.

## hcnds64getlogs

Use this command to collect log files that are output during operation of Analyzer server, and then output the log files to an archive file.

**Format**

```
hcnds64getlogs
 -dir output-directory-path
 [-types Analytics]
 [-arc archive-file-name]
 [-logtypes {log | db | csv}]
```



## Options

### **dir** *output-directory-path*

Specify the directory path for outputting the archive file. You can specify only a directory of a local disk.

As the output directory path, specify an empty directory in absolute or relative path format. If the directory path does not exist, the directory is created automatically. The maximum allowable path length is 100 characters. The Write permission is set for the directory you specify in this option.

### **types** *Analytics*

Specify *Analytics* as the product name of the target of log file collection. This is not case-sensitive. If you omit this option, Analyzer server and all Hitachi Command Suite products that have been installed are subject to the command processing. In this case, log collection might take while.

### **arc** *archive-file-name*

Specify the name of the archive file to be created as the result of Common component's material collection tool. If you omit this option, the archive file name is `HiCommand_log_64`. Archive files are output under the directory in the `dir` option.

Characters that can be specified as the archive file name include printable ASCII characters (0x20 to 0x7E), excluding the following special characters: Backslashes (\), slashes (/), colons (:), commas (,), semicolons (;), asterisks (\*), question marks (?), double quotation marks ("), left angle brackets (<), right angle brackets (>), vertical bars (|), dollar signs (\$), percent signs (%), ampersands (&), single quotation marks ('), and grave accent marks (`) You do not need to specify an extension.

### **logtypes** {*log* | *db* | *csv*}

Specify the type of the log file for Common component for which you want to collect logs. The following table shows the correspondence between the log file type and the log files that can be collected:

| Log file type | Archive file to be created                                                                                                                                         |
|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| log           | <ul style="list-style-type: none"> <li><i>Archive-file-name-in-the-arc-option_64.jar</i></li> <li><i>Archive-file-name-in-the-arc-option_64.hdb.jar</i></li> </ul> |
| db            | <i>Archive-file-name-in-the-arc-option_64.db.jar</i>                                                                                                               |
| csv           | <i>Archive-file-name-in-the-arc-option_64.csv.jar</i>                                                                                                              |

If you omit this option, all log files of Common component are collected. Therefore, we recommend that you run the command by omitting the option.

To specify more than one type, use a space as a delimiter (for example, /logtypes log db csv). If you use the `types` option and the `logtypes` option at the same time, specify `log` as the value of the `logtypes` option.

## Output format

The following table lists the log files collected using the **hcmds64getlogs** command.

### In Windows

| Archive file                                                                              | Output result                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>output-destination-folder-in-dir-option\archive-file-name-in-archive-option_64.jar</i> | <ul style="list-style-type: none"> <li>▪ All files in <i>Analyzer-server-installation-destination-folder\Analytics\logs</i></li> <li>▪ All files in <i>Analyzer-server-installation-destination-folder\Analytics\conf</i></li> <li>▪ All files in <i>Analyzer-server-installation-destination-folder\Analytics\work</i></li> <li>▪ All files in <i>Analyzer-server-installation-destination-folder\Analytics\data</i></li> <li>▪ All files in <i>Analyzer-server-installation-destination-folder\Analytics\system</i></li> <li>▪ All files in <i>Windows-folder*\Temp\HITACHI_HICOMMAND_INST_LOG</i></li> <li>▪ List of the files in <i>Analyzer-server-installation-destination-folder\Analytics</i></li> <li>▪ List of the registry keys in <i>HKEY_LOCAL_MACHINE\SOFTWARE\HITACHI\</i></li> <li>▪ hosts file</li> <li>▪ services file</li> <li>▪ Result of running the <b>ipconfig</b> command of the OS</li> <li>▪ Result of running the <b>netstat</b> command of the OS with the <code>na</code> option specified</li> <li>▪ Result of running the <b>msinfo32</b> command of the OS with the <code>report</code> option specified</li> <li>▪ Result of running the <b>systeminfo</b> command of the OS</li> <li>▪ Result of running Common component's material collection tool (<b>hcmdsgetlogs</b>, <b>hcmdsras</b>)</li> </ul> |

| Archive file                                                                              | Output result                                                                         |
|-------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| <i>output-destination-folder-in-dir-option\archive-file-name-in-arc-option_64.hdb.jar</i> | Result of running Common component's material collection tool ( <b>hcmdsgetlogs</b> ) |
| <i>output-destination-folder-in-dir-option\archive-file-name-in-arc-option_64.db.jar</i>  |                                                                                       |
| <i>output-destination-folder-in-dir-option\archive-file-name-in-arc-option_64.csv.jar</i> |                                                                                       |
| *: By default, this is C:\WINDOWS.                                                        |                                                                                       |

## In Linux

| Archive file                                                                                   | Output result                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>output-destination-directory-in-dir-option/archive-file-name-in-arc-option_64.jar</code> | <ul style="list-style-type: none"> <li>▪ All files in <code>Analyzer-server-installation-destination-directory/Analytics/logs</code></li> <li>▪ All files in <code>Analyzer-server-installation-destination-directory/Analytics/conf</code></li> <li>▪ All files in <code>Analyzer-server-installation-destination-directory/Analytics/work</code></li> <li>▪ All files in <code>Analyzer-server-installation-destination-directory/Analytics/data</code></li> <li>▪ All files in <code>Analyzer-server-installation-destination-directory/Analytics/system</code></li> <li>▪ <code>/var/opt/hitachi/HPA/*.log</code> files</li> <li>▪ List of the files in <code>Analyzer-server-installation-destination-directory/Analytics</code></li> <li>▪ Result of running the <b>netstat</b> command of the OS with the <code>-nao</code> option specified</li> <li>▪ Result of running the <b>uname</b> command of the OS with the <code>-a</code> option specified</li> <li>▪ Result of running the <b>free</b> command of the OS</li> </ul> |

| Archive file | Output result                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|--------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|              | <ul style="list-style-type: none"> <li>▪ Result of running the <b>ps</b> command of the OS with the <b>-elfa</b> option specified</li> <li>▪ <code>/var/log/messages*</code> files</li> <li>▪ <code>/etc/hosts</code> file</li> <li>▪ <code>/etc/services</code> file</li> <li>▪ Result of running the <b>env</b> command of the OS</li> <li>▪ Result of running the <b>sysctl</b> command of the OS with the <b>-a</b> option specified</li> <li>▪ Result of running the <b>ulimit</b> command of the OS with the <b>-a</b> option specified</li> <li>▪ Result of running the <b>ipcs</b> command of the OS with the <b>-a</b> option specified</li> <li>▪ Result of running the <b>cat /proc/meminfo</b> command of the OS</li> <li>▪ Result of running the <b>df</b> command of the OS with the <b>-k</b> option specified</li> <li>▪ Result of running the <b>dmesg</b> command of the OS</li> <li>▪ Result of running the <b>rpm</b> command of the OS with the <b>-qa</b> option specified</li> <li>▪ <code>/etc/inittab</code> file</li> <li>▪ <code>/etc/redhat-release</code> file</li> <li>▪ <code>/etc/nsswitch.conf</code> file</li> <li>▪ <code>/etc/resolv.conf</code> file</li> <li>▪ Result of running the <b>ip</b> command of the OS with the <b>-a</b> option specified</li> <li>▪ <code>/etc/.hitachi/Analytics/installInfo</code> file</li> <li>▪ <code>/etc/sysconfig/iptables-config</code> file</li> <li>▪ Result of running the <b>service iptables status</b> command of the OS</li> <li>▪ Result of running Common component's material collection tool (<b>hcmdsgetlogs</b>, <b>hcmdsras</b>)</li> </ul> |

| Archive file                                                                                       | Output result                                                                         |
|----------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| <code>output-destination-directory-in-dir-option/archive-file-name-in-arc-option_64.hdb.jar</code> | Result of running Common component's material collection tool ( <b>hcmdsgetlogs</b> ) |
| <code>output-destination-directory-in-dir-option/archive-file-name-in-arc-option_64.db.jar</code>  |                                                                                       |
| <code>output-destination-directory-in-dir-option/archive-file-name-in-arc-option_64.csv.jar</code> |                                                                                       |

## Location

In Windows

`Common-component-installation-destination-folder\bin`

In Linux

`Common-component-installation-destination-directory/bin`

## Notes

- Do not interrupt the running of this command.
- Do not run more than one instance of this command at the same time.
- If the directory in the `dir` option has insufficient free space, running of the **hcmds64getlogs** command will not be completed. Secure a sufficient amount of space in the directory in the `dir` option, and then rerun this command. Use the following formula to calculate the amount of required free space:

### In Windows

Size of folders and files in `Analyzer-server-installation-destination-folder\Analytics\data` + size of folders and files in `Analyzer-server-installation-destination-folder\Analytics\logs` + 10 GB

### In Linux

Size of directories and files in `Analyzer-server-installation-destination-directory/Analytics/data` + size of directories and files in `Analyzer-server-installation-destination-directory/Analytics/logs` + 10 GB

If products that use Common component are installed on the Analyzer server, add the capacity required for collecting logs for these products in the calculation.

- If you use the same option more than once, only the first option is used.
- You can run this command even if the Analyzer server is not running.

## Return values

| Return value | Description                 |
|--------------|-----------------------------|
| 0            | The command ran normally.   |
| 1            | The argument is invalid.    |
| 2            | The command ran abnormally. |

## Example

The following example shows the use of this command to collect log files in the folder:

```
hcmds64getlogs -dir /tmp/dir01 -types Analytics -arc Analyzer_log
```

## hcmds64intg

Use this command to delete authentication data registered in the repository of the server that manages user accounts. The command also displays the address of the server in which the authentication data is registered.

If you fail to delete authentication data when uninstalling Analyzer server, use this command to delete the authentication data.

## Format

```
hcmds64intg
 {-delete -type Analytics | -print | -primary}
 -user user-ID
 -pass password
```

## Options

### delete

Deletes authentication data.

### type **Analytics**

Specify Analytics as the product name of the server in which the authentication data is registered.

### print

Displays the name of the program in which the authentication data is registered.

### primary

Displays the host name or the IP address of the server in which the authentication data is registered.

**user** *user-ID*

Specify the user ID for connecting with the server in which the authentication data is registered. The user ID you specify must have the User Management permission.

**pass** *password*

Specifies the password of the account that has the User Management permission.

**Location**

In Windows

*Common-component-installation-destination-folder\bin*

In Linux

*Common-component-installation-destination-directory/bin*

**Return values**

| Return value | Description                                                                                                                                                                               |
|--------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 0            | The command ran normally.                                                                                                                                                                 |
| 1            | The authentication data has already been deleted.                                                                                                                                         |
| 2            | Authentication data is registered in the server on which you ran the command.                                                                                                             |
| 3            | Authentication data is not registered in the server on which you ran the command.                                                                                                         |
| 4            | Authentication data is not registered in the server on which you ran the command. In addition, an authentication error occurred on the server in which authentication data is registered. |
| 253          | An authentication error occurred on the server in which authentication data is registered.                                                                                                |
| 254          | Communication with the server in which authentication data is registered failed.                                                                                                          |
| 255          | The command ran abnormally.                                                                                                                                                               |

**Example**

The following example shows the use of this command to delete authentication data from the server that manages the user account:

```
hcmds64intg -delete -type Analytics -user user1 -pass pass1
```

## hcnds64ldapuser

To connect to an external authentication server, use this command to register, in the Analyzer server, a user account used to search user information in external authentication servers. You can also use this command to delete user accounts used to search user information that are registered in the Analyzer server.

If you register a user account by using this command, use the **hcnds64checkauth** command to verify whether the user account can be correctly authenticated.

### Format

#### To register an LDAP search user account:

```
hcnds64ldapuser -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
```

#### To delete an LDAP search user account:

```
hcnds64ldapuser -delete
 -name name
```

#### To display external authentication servers for which LDAP search user accounts have already been registered in the Analyzer server:

```
hcnds64ldapuser -list
```

### Options

#### set

Registers user information

#### dn *DN-of-user-account-used-to-search-for-LDAP-user-info*

Specify the DN of the user used to search information.

Specify the DN in accordance with the rules defined in RFC 4514. For example, if any of the following characters are included in the DN, you must use a backslash (\) to escape each character.

Spaces, hash marks (#), plus signs (+), commas (,), semicolons (;), left angle brackets (<), equal signs (=), right angle brackets (>), and backslashes (\)

#### pass *password-of-user-account-used-to-search-for-LDAP-user-info*

Specify the password for the user specified for the dn option.

The password is case-sensitive and must completely match the password registered in the LDAP directory server. If you execute this command without specifying the pass option, you will be prompted to enter a password.



**delete**

Deletes user information.

Specify this option to delete user information, including the server identification name or the domain name specified for the `name` option.

**name *name***

The items to be specified vary depending on the authentication method.

- For LDAP authentication: Server identification name or the domain name for external authentication servers of the LDAP directory server

Specify the server identification name that was specified for the `auth.server.name` property in the `exauth.properties` file, or specify the domain name specified for `auth.ldap.value-specified-for-auth.server.name.domain.name` property in the `exauth.properties` file.

- For RADIUS authentication: Domain name of the RADIUS server

Specify the domain name specified for `auth.radius.auth.server.name-property-value.domain.name` in the `exauth.properties` file.

- For Kerberos authentication: Realm name of the Kerberos server)

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.

**list**

Displays the external authentication servers for which the user accounts used to search information have already been registered in the Analyzer server.

**Location**

In Windows

*Common-component-installation-destination-folder\bin*

In Linux

*Common-component-installation-destination-directory/bin*

## Notes

- In the LDAP directory server, you can use double quotation marks (") for the DN and password. In the Analyzer server, however, you must 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
```

## Return values

| Return value | Description                                                 |
|--------------|-------------------------------------------------------------|
| 0            | The command ran normally.                                   |
| 1            | The argument is invalid.                                    |
| 2            | The argument includes a character that cannot be specified. |
| 3            | The registered information cannot be found.                 |
| 255          | The command ran abnormally.                                 |

## Example

**To register an LDAP search user account:**

```
hcmds64ldapuser -set -dn "CN=user01,CN=Users,DC=Example,DC=com" -pass
qweasd00 -name example.com
```

**To delete an LDAP search user account:**

```
hcmds64ldapuser -delete -name example.com
```

## hcmds64prmset

Use this command to register, change, and cancel the registration of the host that manages the user accounts used to connect with Ops Center Automator.

If you execute this command, the information about the user accounts in the Common component will be managed by the Common component of the primary server. The host whose user accounts are managed by the primary server is called the secondary server.

Execute this command on the server that is set as the secondary server.

To connect to Ops Center Automator that is linked with Device Manager, execute this command on Analyzer server.

To connect to Ops Center Automator that is not linked with Device Manager, execute this command on Ops Center Automator.

**Format****When registering the primary server or changing information about the registered primary server**

```
hcmds64prmset
 [-host host-name-or-IP-address]
 [-port port-number-for-non-SSL-communication
 | -sslport port-number-for-SSL-communication]
 [-check]
```

**When cancelling the registered primary server**

```
hcmds64prmset -setprimary
```

**When displaying the registered information**

```
hcmds64prmset -print
```

**Options****host *host-name-or-IP-address***

Specify the host name or IP address of the primary server. If SSL communication is enabled on the primary server, specify the same value as that of Common Name (CN) in the server certificate.

If you change the host name of only the registered primary server, you can omit the `port` or `sslport` option.

**port *port-number-for-non-SSL-communication***

Specify the port number of HBase 64 Storage Mgmt Web Service of the primary server. Specify this option if SSL communication is disabled on the primary server. The default port number is 22015.

If you change the port number of only the registered primary server, you can omit the `host` option.

**sslport *port-number-for-SSL-communication***

Specify the port number of HBase 64 Storage Mgmt Web Service of the primary server. Specify this option if SSL communication is enabled on the primary server. The default port number is 22016.

If you change the port number of only the registered primary server, you can omit the `host` option.

**check**

Checks the connection to the primary server.

**setprimary**

Cancels the registered primary server. The host where the command was executed will be changed from the secondary server to the primary server.

**print**

The following information is displayed:

- Role of the host where the command was executed (primary server or secondary server)
  - Host name (IP address) and port number of the primary server
- This information is displayed only if the role of the host is the secondary server.

**Location**

In Windows

*Common-component-installation-destination-folder\bin*

In Linux

*Common-component-installation-destination-directory/bin*

**Notes**

After executing this command, restart the product by executing the **hcmds64srv** command on the host where you executed the command.

**Return values**

| Return value | Description               |
|--------------|---------------------------|
| 0            | The command ran normally. |

| Return value | Description                 |
|--------------|-----------------------------|
| 255          | The command ran abnormally. |

### Example

The following example shows how to use this command to register the primary server:

```
hcmds64prmset -host host01 -port 22015
```

## hcmds64radiussecret

To connect to an external authentication server, use this command to register a shared secret for the RADIUS server in the Analyzer server. You can also use this command to delete shared secrets registered in the Analyzer server.

If you register a shared secret by using this command, execute the **hcmds64checkauth** command to verify whether the shared secret can be correctly authenticated.

### Format

#### To register a shared secret:

```
hcmds64radiussecret
 [-set shared-secret]
 -name RADIUS-server-identification-name
```

#### To delete a shared secret:

```
hcmds64radiussecret
 -delete
 -name RADIUS-server-identification-name
```

#### To display a list of server identification names of the RADIUS servers for which shared secrets are registered:

```
hcmds64radiussecret -list
```

### Options

#### **set *shared-secret***

Registers a shared secret for the RADIUS server in the Analyzer server.

For a *shared-secret*, you can specify printable ASCII characters (0x21 to 0x7E) of 128 bytes or less.

If you execute the command without specifying the **set** option, you will be prompted to enter a shared secret.

**delete**

Deletes a shared secret registered in the Analyzer server.

**name** *RADIUS-server-identification-name*

Specifies a RADIUS server identification name.

The specified name must match a server identification name specified for the `auth.server.name` property in the `exauth.properties` file.

**list**

Displays a list of server identification names of the RADIUS servers for which shared secrets are registered.

**Location**

In Windows

*Common-component-installation-destination-folder\bin*

In Linux

*Common-component-installation-destination-directory/bin*

**Return values**

| Return value | Description                                                 |
|--------------|-------------------------------------------------------------|
| 0            | The command ran normally.                                   |
| 1            | The argument is invalid.                                    |
| 2            | The argument includes a character that cannot be specified. |
| 3            | The registered information cannot be found.                 |
| 255          | The command ran abnormally.                                 |

**Examples****To register a shared secret:**

```
hcmds64radiussecret -set secret01 -name example.com
```

**To delete a shared secret:**

```
hcmds64radiussecret -delete -name example.com
```

## hcmds64srv

Use this command to start or stop Analyzer server services. The command also displays the Analyzer server service status or changes the service start method.

### Format

**To start, stop, or display only the status of a specific service:**

```
hcmds64srv
 {-start | -stop | -check | -status}
 [-server service-name]
```

**To display the status of services of Analyzer server and products that use Common component:**

```
hcmds64srv
 -statusall
```

**To change the start method of a service:**

```
hcmds64srv
 -starttype {auto | manual}
 {-server service-name | -all}
```

### Options

#### start

Starts the service and database you specified in the `server` option.

#### stop

Stops the service and database you specified in the `server` option.

#### status

Displays the status of the server and database you specified in the `server` option.

#### server *service-name*

To start, stop, or display the status of Analyzer server product services only, specify `AnalyticsWebService` as the service name. By running this command by specifying `AnalyticsWebService` in the `server` option, you can start, stop, or display the status of the following services:

| Service display name and process  | Start | Stop | Status display |
|-----------------------------------|-------|------|----------------|
| HAnalytics Engine Web Service     | Y     | Y    | Y              |
| HBase 64 Storage Mgmt Web Service | Y     | N    | N              |

| Service display name and process                                                              | Start | Stop | Status display |
|-----------------------------------------------------------------------------------------------|-------|------|----------------|
| HBase 64 Storage Mgmt Web SSO Service                                                         | Y     | N    | N              |
| Database process*                                                                             | Y     | N    | N              |
| <b>Legend:</b><br>Y: Processed<br>N: Not processed                                            |       |      |                |
| *: An Analyzer server internal process corresponding to the service HiRDB/EmbeddedEdition_HD1 |       |      |                |

If you omit the `server` option, the next service is started, stopped, or the status of the next service displays.

| Service display name and process                                                              | Start | Stop | Status display |
|-----------------------------------------------------------------------------------------------|-------|------|----------------|
| HAnalytics Engine Web Service                                                                 | Y     | Y    | Y              |
| HBase 64 Storage Mgmt SSO Service                                                             | Y     | Y    | Y              |
| HBase 64 Storage Mgmt Web Service                                                             | Y     | Y    | Y              |
| HBase 64 Storage Mgmt Web SSO Service                                                         | Y     | Y    | Y              |
| Database process*                                                                             | Y     | Y    | Y              |
| Service of products that use Common component                                                 | Y     | Y    | Y              |
| <b>Legend:</b><br>Y: Processed                                                                |       |      |                |
| *: An Analyzer server internal process corresponding to the service HiRDB/EmbeddedEdition_HD1 |       |      |                |

### **statusall**

Displays the service and data statuses, and the status of the products registered in Common component. If you omit the `server` option, this argument is used.

### **starttype {auto | manual}**

Specify the start type of the service with the `server` option. Specify `auto` for an automatic start. Specify `manual` for a manual start.



**all**

If you specify this option, the command runs for all services of Analyzer server and other products that use Common component.

**Location**

In Windows

*Common-component-installation-destination-folder\bin*

In Linux

*Common-component-installation-destination-directory/bin*

**Notes**

- If you start or stop Analyzer server services as a daily operation, omit the `server` option to start or stop all the services. To start only Analyzer server services by specifying the `server` option, specify `AnalyticsWebService` for the `server` option to start Common component service.
- If you run the command with the `stop` option and the termination processing does not end within three minutes, an error occurs and a message is displayed to indicate a time-out. In this case, wait a while, and then rerun the command with the `stop` option.
- If you start or stop a service with the `start` or `stop` option, the command might end while the service does not start or stop completely. To confirm that the service has completely started or stopped, use either of the following operations:
  - Confirm that either of the following messages has been output to a disclosed log or the event log:

**At startup**

KNAQ10086-I Application is running.

**When stopped**

KNAQ10089-I Application is stopped.

- Specify the `statusall` option to check the status of the service.

**Return values**

The following table shows the return values of the command with `start` option or `stop` option:

| Return value | Description                                                               |
|--------------|---------------------------------------------------------------------------|
| 0            | The command ran normally.                                                 |
| 1            | <b>With <code>start</code> option</b><br>The service was already started. |

| Return value | Description                                                 |
|--------------|-------------------------------------------------------------|
|              | <b>With stop option</b><br>The service was already stopped. |
| 255          | The command failed.                                         |

The following table shows the return values of the command with the `check`, `status`, or `statusall` option:

| Return value | Description                  |
|--------------|------------------------------|
| 0            | The service has not started. |
| 1            | The service has started.     |
| 255          | The command failed.          |

The following table shows the return values of the command with the `starttype` option:

| Return value | Description               |
|--------------|---------------------------|
| 0            | The command ran normally. |
| 255          | The command failed.       |

## Examples

To start all services:

```
hcnds64srv -start
```

To stop all services:

```
hcnds64srv -stop
```

To check the status of all services:

```
hcnds64srv -status
```

To start the services of only Analyzer server products:

```
hcnds64srv -start -server AnalyticsWebService
```

## hcmds64ssltool

Use this command to create private keys, certificate signing requests (CSRs), self-signed certificates, and content files for self-signed certificates that are required for SSL connections. The created files are used for the following purposes:

- Submitting the CSR to a CA to obtain an SSL server certificate. You can build an SSL-connected environment by combining the obtained SSL server certificate and the private key.
- Building an SSL-connected environment by combining the self-signed certificate with the private key. However, we recommend that you use the environment only for test purposes because security is low.
- Checking the details of the registration of the self-signed certificate from the content file of the self-signed certificate.

### Format

```
hcmds64ssltool
 [-key private-key-file-name]
 [-csr CSR-file-name]
 [-cert self-signed-certificate-file-name]
 [-certtext name-of-the-content-file-of-the-self-signed-certificate]
 [-validity expiration-date-of-the-self-signed-certificate]
 [-dname distinguished-name (DN)]
 [-sigalg signature-algorithm-of-the-server-certificate-for-RSA-cryptography]
 [-keysize private-RSA key-size]
 [-eccsigalg signature-algorithm-of-the-server-certificate-for-elliptic-curve-cryptography]
 [-ecckeysize size-of-the-private-key-for-elliptic-curve-cryptography]
 [-ext extension-information-for-the-X.509-certificate]
```

### Options

#### **key** *private-key-file-name*

Specifies the absolute path for storing the private key. The private key for RSA cryptography will be output to a file of the specified file name. The private key for elliptic curve cryptography will be output to another file of the specified file name with the prefix `ecc-`.

If you omit this option, the `httpsdkey.pem` file and the `ecc-httpsdkey.pem` file will be output under the *Common-component-installation-destination-folder\uCPSB\httpsd\conf\ssl\server\* (Windows) or the *Common-component-installation-destination-directory/uCPSB/httpsd/conf/ssl/server/* (Linux).

**csr CSR-file-name**

Specifies the filename, and absolute path, for storing the CSR. The CSR for RSA cryptography is output to a file of the specified file name. The CSR for elliptic curve cryptography will be output to another file of the specified file name with the prefix `ecc-`.

If you omit this option, the `httpsd.csr` file and the `ecc-httpsd.csr` file are output under the *Common-component-installation-destination-folder* \uCP SB\httpsd\conf\ssl\server\ (Windows) or the *Common-component-installation-destination-directory*/uCP SB/httpsd/conf/ssl/server/ (Linux).

**cert self-signed-certificate-file-name**

Specifies the filename, and absolute path, for storing the self-signed certificate. The self-signed certificate for RSA cryptography will be output to a file of the specified file name. The self-signed certificate for elliptic curve cryptography is output to another file of the specified file name with the prefix `ecc-`.

If you omit this option, the `httpsd.pem` file and the `ecc-httpsd.pem` file are output under the *Common-component-installation-destination-folder* \uCP SB\httpsd\conf\ssl\server\ (Windows) or the *Common-component-installation-destination-directory*/uCP SB/httpsd/conf/ssl/server/ (Linux).

**certtext name-of-the-content-file-of-the-self-signed-certificate**

Outputs the content of the self-signed certificate in text to a specified path and filename. The content of the self-signed certificate for RSA cryptography is output to a file of the specified file name. The content of the self-signed certificate for elliptic curve cryptography is output to another file of the specified file name with the prefix `ecc-`.

If you omit this option, the `httpsd.txt` file and the `ecc-httpsd.txt` file are output under the *Common-component-installation-destination-folder* \uCP SB\httpsd\conf\ssl\server\ (Windows) or the *Common-component-installation-destination-directory*/uCP SB/httpsd/conf/ssl/server/ (Linux).

**validity expiration-date-of-the-self-signed-certificate**

Specifies the number of days until the self-signed certificate expires. If you specify this option, the same value is specified for RSA cryptography and elliptic curve cryptography. If you omit this option, the certificate expires in 3,650 days.

**dnname distinguished-name (DN)**

Specifies the distinguished-name (DN) described in the SSL server certificate, in the format "*attribute-type=attribute-value*". You can specify some attribute type values using a comma (,) as a delimiter.

Characters specified for attribute types are not case sensitive. You cannot use a double quotation mark (") or a backslash (/) in the attribute type. For details about how to use escape characters, follow the instructions in RFC 2253. To use the following symbols, add a backslash (/) before each symbol as an escape character.

- Plus signs (+), commas (,), semicolons (;), left angle brackets (<), equal signs (=), right angle brackets (>)
- Spaces at the beginning of character strings
- Spaces at the end of character strings
- Hash marks (#) at the beginning of character strings

If you omit this option, you must enter attribute values according to the instructions in the window displayed when you run the command.

The following table lists the attribute types that you can specify for this option:

| Attribute type                  | Definition               | Window response            | Attribute value                                                                           |
|---------------------------------|--------------------------|----------------------------|-------------------------------------------------------------------------------------------|
| CN                              | Common Name              | Server Name                | Distinguished-name* of the Analyzer server, such as host name, IP address, or domain name |
| OU                              | Organizational Unit Name | Organizational Unit        | Lower-level organization name, such as department or section name                         |
| O                               | Organization Name        | Organization Name          | Company or other organization's name*                                                     |
| L                               | Locality Name            | City or Locality           | City name or region name                                                                  |
| ST                              | State or Province Name   | State or Province          | State name or district name                                                               |
| C                               | Country Name             | two-character country-code | Country code                                                                              |
| *: Required in a response entry |                          |                            |                                                                                           |

The following is an example of response input:

```
Enter Server Name [default=MyHostname]:example.com
Enter Organizational Unit:Device Manager Administration
Enter Organization Name [default=MyHostname]:HITACHI
Enter your City or Locality:Santa Clara
Enter your State or Province:California
Enter your two-character country-code:US
```

```
Is CN=example.com,OU=Device Manager Administration,O=HITACHI,L=Santa Clara, ST=California,C=US correct? (y/n) [default=n]:y
```

If the entry is incorrect, you can input again by typing n.

**sigalg *signature-algorithm-of-the-server-certificate-for-RSA-cryptography***

Specifies the signature algorithm of the server certificate for RSA cryptography. You can specify SHA512withRSA, SHA256withRSA, or SHA1withRSA. If you omit this option, the signature algorithm is SHA256withRSA.

**keysize *private-RSA\_key-size***

Specifies the size (in bits) of the private key for RSA cryptography. You can specify 2048, 3072, or 4096. If you omit this option, the size of the private key for RSA cryptography is 2,048 bits.

**eccsigalg *signature-algorithm-of-the-server-certificate-for-elliptic-curve-cryptography***

Specifies the signature algorithm of the server certificate for elliptic curve cryptography. You can specify SHA512withECDSA, SHA384withECDSA, SHA256withECDSA, or SHA1withECDSA. If you omit this option, the signature algorithm is SHA384withECDSA.

**ecckeysize *size-of-the-private-key-for-elliptic-curve-cryptography***

Specifies the size (in bits) of the private key for elliptic curve cryptography. You can specify 256 or 384. If you omit this option, the size of the private key for elliptic curve cryptography is 384 bits.

**ext *extension-information-for-the-X.509-certificate***

Specifies the extension information for the X.509 certificate. The specification method is based on the `ext` option of the `keytool` command in Java. Note, however, that the only extension that can be specified in Ops Center Analyzer is SAN (SubjectAlternativeName).

The following is an example of specifying the extension information.

- To specify `www.example.com` as the host name:

```
hcmds64ssltool -ext san=dns:www.example.com
```

- To specify `www.example.com` and `www.example.net` as multiple host names:

```
hcmds64ssltool -ext san=dns:www.example.com, dns:www.example.net
```

If you specify the `ext` option multiple times, the first specification takes effect.

## Location

In Windows

*Common-component-installation-destination-folder\bin*

In Linux

*Common-component-installation-destination-directory/bin*

## Notes

If the value of the attribute type **CN** of the SSL server certificate does not match the host name, IP address, or domain name as the connection destination of the Analyzer server from the web browser, a message indicates a server mismatch.

## Return values

| Return value | Description                                                         |
|--------------|---------------------------------------------------------------------|
| 0            | The command ran normally.                                           |
| 1            | The argument is invalid.                                            |
| 249          | The file or folder already exists on the specified path.            |
| 250          | Deletion of the key store failed.                                   |
| 251          | Creation of the private key failed.                                 |
| 252          | Creation of the self-signed certificate failed.                     |
| 253          | Creation of the CSR failed.                                         |
| 254          | Creation of the content file of the self-signed certificate failed. |
| 255          | The command ran abnormally.                                         |

# hcnds64unlockaccount

Use this command to unlock user accounts for all users with User Management permission.

You can use this command to unlock user accounts managed by the Common component.

## Format

```
hcnds64unlockaccount
 -user user-ID
 -pass password
```

## Options

### **user** *user-ID*

Specify the user ID of the user account to be unlocked. The user ID you specify must have the User Management permission.

**pass password**

Specify the password of the user account to unlock.

## Location

In Windows

*Common-component-installation-destination-folder\bin*

In Linux

*Common-component-installation-destination-directory/bin*

## Notes

- To run this command, the Common component services (HBase 64 Storage Mgmt Web Service and HBase 64 Storage Mgmt SSO Service) and the database must already be running.
- You can use the **hcmds64unlockaccount** command to unlock only user accounts that have the User Management permission.
- If the user ID or password contains symbols, escape them as shown below:

### In Windows:

If one or more backslashes (\) are contained at the end of the user ID or password, add another backslash (\) as an escape character before each of the backslashes.

If an ampersand (&), vertical bar (|), or carat (^) is contained, enclose each of these symbols in double quotation marks ("), or add a carat (^) as an escape character before each of the symbols.

### In Linux:

Add a backslash (\) as an escape character before each symbol.

For example, if the password is ^a^b^c^ in Windows-based systems, use either of the following:

- `hcmds64unlockaccount /user system /pass "^"a"^"b"^"c"^"`
- `hcmds64unlockaccount /user system /pass ^^a^^b^^c^^`

- If Ops Center Automator is connected, run the **hcmds64unlockaccount** command on the server that is set as the primary server.

## Return values

| Return value | Description                                                       |
|--------------|-------------------------------------------------------------------|
| 0            | The command ran normally.                                         |
| 251          | An authentication error (logon error) occurred.                   |
| 252          | An authentication error (no User Management permission) occurred. |



| Return value | Description                                          |
|--------------|------------------------------------------------------|
| 253          | Communication with the authentication server failed. |
| 254          | The command was run on the secondary server side.    |
| 255          | The command ran abnormally.                          |

### Example

The following example shows how to use this command to unlock a user account:

```
hcmds64unlockaccount -user test01 -pass TTdate00
```

## htmssltool

Create the private keys, certificate signing requests (CSRs), self-signed certificates, and content files for self-signed certificates that are required for SSL connection that uses the RAID Agent services. The created files are used for the following purposes:

- Submitting the CSR to a CA to obtain an SSL server certificate. You can build an SSL-connected environment by combining the obtained SSL server certificate and the private key.
- Building an SSL-connected environment by combining the self-signed certificate with the private key. However, we recommend that you use the environment only for test purposes because security is low.
- Checking the details of the registration of the self-signed certificate from the content file of the self-signed certificate.

### Format

```
htmssltool
 -key private-key-file-name
 -csr CSR-file-name
 -cert self-signed-certificate-file-name
 -certtext name-of-the-content-file-of-the-self-signed-certificate
 [-validity expiration-date-of-the-self-signed-certificate]
 [-dname distinguished-name (DN)]
 [-sigalg signature-algorithm-of-the-server-certificate-for-RSA-cryptography]
 [-keysize private-RSA_key-size]
 [-eccsigalg signature-algorithm-of-the-server-certificate-for-elliptic-curve-cryptography]
 [-ecckeysize size-of-the-private-key-for-elliptic-curve-cryptography]
```

## Options

### **-key *private-key-file-name***

Specifies the absolute path for storing the private key. The private key for RSA cryptography will be output to a file of the specified file name. The private key for elliptic curve cryptography will be output to another file of the specified file name with the prefix `ecc-`.

### **-csr *CSR-file-name***

Specifies the filename, and absolute path, for storing the CSR. The CSR for RSA cryptography is output to a file of the specified file name. The CSR for elliptic curve cryptography will be output to another file of the specified file name with the prefix `ecc-`.

### **-cert *self-signed-certificate-file-name***

Specifies the filename, and absolute path, for storing the self-signed certificate. The self-signed certificate for RSA cryptography will be output to a file of the specified file name. The self-signed certificate for elliptic curve cryptography is output to another file of the specified file name with the prefix `ecc-`.

### **-certtext *name-of-the-content-file-of-the-self-signed-certificate***

Specifies the filename, and absolute path, for the content of the self-signed certificate in text. The content of the self-signed certificate for RSA cryptography is output to a file of the specified file name. The content of the self-signed certificate for elliptic curve cryptography is output to another file of the specified file name with the prefix `ecc-`.

### **-validity *expiration-date-of-the-self-signed-certificate***

Specifies the number of days until the self-signed certificate expires. If you specify this option, the same value is specified for RSA cryptography and elliptic curve cryptography. If you omit this option, the certificate expires in 3,650 days.

### **-dname *distinguished-name (DN)***

Specifies the distinguished-name (DN) described in the SSL server certificate, in the format "*attribute-type=attribute-value*". You can specify some attribute type values using a comma (,) as a delimiter.

Characters specified for attribute types are not case sensitive. You cannot use a double quotation mark (") or a backslash (/) in the attribute type. For details about how to use escape characters, follow the instructions in RFC 2253. To use the following symbols, add a backslash (/) before each symbol as an escape character.

- Plus signs (+), commas (,), semicolons (;), left angle brackets (<), equal signs (=), right angle brackets (>)
- Spaces at the beginning of character strings
- Spaces at the end of character strings
- Hash marks (#) at the beginning of character strings

If you omit this option, you must enter attribute values according to the instructions in the window displayed when you run the command.

The following table lists the attribute types that you can specify for this option:

| Attribute type                  | Definition               | Window response            | Attribute value                                                                                                     |
|---------------------------------|--------------------------|----------------------------|---------------------------------------------------------------------------------------------------------------------|
| CN                              | Common Name              | Server Name                | Distinguished-name* of the host on which RAID Agent is installed, such as the host name, IP address, or domain name |
| OU                              | Organizational Unit Name | Organizational Unit        | Lower-level organization name, such as department or section name                                                   |
| O                               | Organization Name        | Organization Name          | Company or other organization's name*                                                                               |
| L                               | Locality Name            | City or Locality           | City name or region name                                                                                            |
| ST                              | State or Province Name   | State or Province          | State name or district name                                                                                         |
| C                               | Country Name             | two-character country-code | Country code                                                                                                        |
| *: Required in a response entry |                          |                            |                                                                                                                     |

The following is an example of response input:

```
Enter Server Name [default=MyHostname]:example.com
Enter Organizational Unit:Analyzer
Enter Organization Name [default=MyHostname]:HITACHI
Enter your City or Locality:Santa Clara
Enter your State or Province:California
Enter your two-character country-code:US
Is CN=example.com,OU=Analyzer,O=HITACHI,L=Santa Clara,ST=California,
C=US correct? (y/n) [default=n]:y
```

**-sigalg *signature-algorithm-of-the-server-certificate-for-RSA-cryptography***

Specifies the signature algorithm of the server certificate for RSA cryptography. You can specify SHA256withRSA or SHA1withRSA. If you omit this option, the signature algorithm is SHA256withRSA.

**-keysize *private-RSA\_key-size***

Specifies the size (in bits) of the private key for RSA cryptography. You can specify 2048 or 4096. If you omit this option, the size of the private key for RSA cryptography is 2,048 bits.

**-eccsigalg *signature-algorithm-of-the-server-certificate-for-elliptic-curve-cryptography***

Specifies the signature algorithm of the server certificate for elliptic curve cryptography. You can specify SHA512withECDSA, SHA384withECDSA, or SHA256withECDSA. If you omit this option, the signature algorithm is SHA384withECDSA.

**-ecckeysize *size-of-the-private-key-for-elliptic-curve-cryptography***

Specifies the size (in bits) of the private key for elliptic curve cryptography. You can specify 256 or 384. If you omit this option, the size of the private key for elliptic curve cryptography is 384 bits.

**Location**

/opt/jplpc/htnm/bin/

**Notes**

Execute this command on the Analyzer probe server. For common name (CN) included in the distinguished name (DN), specify the host name of the host on which RAID Agent is installed. When specifying CN, make sure that the host name can be resolved in the hosts file or DNS of the server connected to RAID Agent.

**Return values**

| Return value | Description                                                         |
|--------------|---------------------------------------------------------------------|
| 0            | The command ran normally.                                           |
| 1            | The argument is invalid.                                            |
| 250          | Deletion of the key store failed.                                   |
| 251          | Creation of the private key failed.                                 |
| 252          | Creation of the self-signed certificate failed.                     |
| 253          | Creation of the CSR failed.                                         |
| 254          | Creation of the content file of the self-signed certificate failed. |
| 255          | An unexpected error occurred.                                       |

## reloadtemplate

Use this command during the startup of the Analyzer server to reload the template files.

The following table describes the types of template files that the command references, and the reference destination directories:

| Type of template file                  | Reference destination folder                                                                                                                                                                                                           |
|----------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Template file for emails               | <p>In Windows</p> <p><i>Analyzer-server-installation-destination-folder\Analytics\conf\template\mail</i></p> <p>In Linux</p> <p><i>Analyzer-server-installation-destination-directory/Analytics/conf/template/mail</i></p>             |
| Template file for commands             | <p>In Windows</p> <p><i>Analyzer-server-installation-destination-folder\Analytics\conf\template\command</i></p> <p>In Linux</p> <p><i>Analyzer-server-installation-destination-directory/Analytics/conf/template/command</i></p>       |
| Template file for Ops Center Automator | <p>In Windows</p> <p><i>Analyzer-server-installation-destination-folder\Analytics\conf\template\automation</i></p> <p>In Linux</p> <p><i>Analyzer-server-installation-destination-directory/Analytics/conf/template/automation</i></p> |

## Format

```
reloadtemplate
 -user user-ID
 -passwordfile password-file
```

## Arguments

### **user** *user-ID*

Specify the Analyzer server user ID to use for command execution. The user must have the Admin or Modify permission for IAA.

### **passwordfile** *path-of-the-password-file*

Specify the path to the password file of the user who is specified for the **user** option. Use the **encryptpassword** command to create the password file.

**Location**

In Windows

*Analyzer-server-installation-destination-folder\Analytics\bin*

In Linux

*Analyzer-server-installation-destination-directory/Analytics/bin*

**Notes**

To run this command, the Analyzer server service must already be running. If the Analyzer server service is not running, you do not have to run this command because the template files are automatically read when the Analyzer server service starts.

**Return values**

| Return value | Description                                                            |
|--------------|------------------------------------------------------------------------|
| 0            | The command ran normally.                                              |
| 1            | The argument is invalid.                                               |
| 2            | Command execution was interrupted.                                     |
| 3            | The service status is invalid.                                         |
| 5            | Communication failed.                                                  |
| 6            | An authentication error occurred.                                      |
| 7            | The specified path is invalid.                                         |
| 9            | The specified path does not exist.                                     |
| 10           | The specified path could not be accessed.                              |
| 14           | You do not have permission to run this command.                        |
| 232          | The reloading of the template files failed.                            |
| 233          | You do not have the necessary permissions to update the template file. |
| 255          | The command terminated abnormally.                                     |

**restoresystem**

Use this command to restore the backup for Analyzer server settings information that you collected by running the **backupsystem** command.

## Format

```
restoresystem
 -dir backup-directory
 -type {all | Analytics}
 [-auto]
```

## Options

### **dir *backup-directory***

Specify the directory in which the backup file is stored with the absolute or relative path.

### **type {all | Analytics}**

Specify the system restore target.

- **all**  
Restores information for both the Analyzer server and the Common component.
- **Analytics**  
Restores only the backup information for the Analyzer server.

### **auto**

Automatically stops or starts services and databases associated with the Analyzer server and products that use Common component. If you omit this option, Analyzer server services and database, as well as products that use Common component, are not automatically stopped or started.

## Location

In Windows

*Analyzer-server-installation-destination-folder\Analytics\bin*

In Linux

*Analyzer-server-installation-destination-directory/Analytics/bin*

## Notes

- When restoring the backup, the directory in which the backup file is stored requires at least 2 GB of free space.
- When you run the **restoresystem** command, for backup, the extension **.original** is appended to the file name of the file in *Analyzer-server-installation-destination-folder\Analytics\conf* (Windows) or *Analyzer-server-installation-destination-directory/Analytics/conf* (Linux). This file is overwritten every time the **restoresystem** is run. If a file with an extension of **.original** exists before the command is executed and you want to save the file, change the file extension before executing the command.

- The following files are not restored by this command. If necessary, manually reset or relocate the files again.

#### Files that require resettings

- Security definition file (`security.conf`)
- File for setting port numbers and host names (`user_httpsd.conf`)

These files are backed up in the following directories:

#### In Windows

- `backup-folder\HBase\base\conf\sec`
- `backup-folder\HBase\base\httpsd.conf`

#### In Linux

- `backup-directory/HBase/base/conf/sec`
- `backup-directory/HBase/base/httpsd.conf`

The definition files are stored in the following locations in the environments where the files are restored:

#### In Windows

- `security.conf`  
`Common-component-installation-destination-folder\conf\sec`
- `user_httpsd.conf`  
`Common-component-installation-destination-folder\uCPSB\httpsd\conf`

#### In Linux

- `security.conf`  
`Common-component-installation-destination-directory/conf/sec`
- `user_httpsd.conf`  
`Common-component-installation-destination-directory/uCPSB/httpsd/conf`

#### Files for HTTPS connections that must be relocated

- SSL server certificate file
- Private-key file

In addition, the settings for HTTPS connections are defined in the `httpsd.conf` file and the `user_httpsd.conf` file. Save each file to the storage destination directory.



- If you do not specify the `auto` option, stop the service by running the `hcnds64srv` command with the `stop` option. The service to be stopped depends on the `type` option.

**If you specified `all` in the `type` option:**

You must stop not only the service of Analyzer server, but also the services of the products that use Common component.

**If you specified `Analytics` in the `type` option:**

You must stop the service only for the Analyzer server.

- Make sure that the following information is the same between the environment where the backup was collected and the environment where the information was restored:
  - Version of Analyzer server
  - Installation directory of Analyzer server
- When products that use Common component are installed on the Analyzer server, if you do a system restore with `all` specified in the `type` option, the definition information for Common component is also restored. In this example, an inconsistency might occur in the definition information between the products that use Common component and Common component itself. Therefore, if products that use Common component are installed on the Analyzer server of the restore destination, do a system restore by using one of the following procedures:

**To restore data for products that use Common component, in addition to Analyzer server data**

1. Run the system restore command for the product that uses Common component.
2. Specify `type Analytics` for the `restoresystem` command of Analyzer server, and then run the command.

**To restore only user information, in addition to Analyzer server data**

1. Specify `type Analytics` for the `restoresystem` command of Analyzer server, and then run the command.
2. Update the user management information.

**To restore data only for the Analyzer server**

1. Specify `type Analytics` for the `restoresystem` command of Analyzer server, and then run the command.

**Return values**

| Return value | Description               |
|--------------|---------------------------|
| 0            | The command ran normally. |
| 1            | The argument is invalid.  |

| Return value | Description                                               |
|--------------|-----------------------------------------------------------|
| 2            | Command running was interrupted.                          |
| 3            | The service status is invalid.                            |
| 4            | Another command is currently running.                     |
| 7            | The path is invalid.                                      |
| 9            | The path does not exist.                                  |
| 10           | The path cannot be accessed.                              |
| 14           | You do not have permission to run this command.           |
| 110          | Running of system restore failed.                         |
| 111          | The start or stop of the service failed.                  |
| 113          | The backup file is invalid.                               |
| 255          | Command running was interrupted because of another error. |

### Example

The following example shows the use of this command to restore information only for the Analyzer server:

```
restoresystem -dir /tmp -type Analytics -auto
```

## setupcommonservice

Use this command to register Analyzer to Ops Center Common Services. This command also updates the Analyzer information that is registered in Common Services.

### Format

#### When registering Analyzer to Common Services

```
setupcommonservice
 -csUri Common-Services-URL
 -csUsername Common-Services-username
 -csPassword Common-Services-user-password
 [-appHostname Analyzer-server-host-name-or-IP-address]
 [-appPort Analyzer-server-port]
 [-appName product-name-to-display-in-the-portal]
 [-appDescription description-to-display-in-the-portal]
 [-auto]
```

## When updating the information of Analyzer that is registered in Common Services

```
setupcommonservice
 [-csUri Common-Services-URL
 -csUsername Common-Services-username
 -csPassword Common-Services-user-password]
 [-appHostname Analyzer-server-host-name-or-IP-address]
 [-appPort Analyzer-server-port]
 [-appName product-name-to-display-in-the-portal]
 [-appDescription description-to-display-in-the-portal]
 [-auto]
```

## When displaying usage information for this command

```
setupcommonservice -help
```

### Options

#### **csUri** *Common-Services-URL*

Specify the Common Services URL (URL for Ops Center Portal).

#### **csUsername** *Common-Services-username*

Specify the username with Security Admin or System Admin role for Common Services.

You can specify from 1 to 256 characters.

You can use alphanumeric characters and the following characters:

Exclamation marks (!), hash marks (#), dollar signs (\$), percent signs (%), ampersands (&), single quotation marks ('), left parentheses ( ( ), right parentheses ( ) ), asterisks (\*), plus signs (+), hyphens (-), periods (.), equal signs (=), at marks (@), carets (^), underscores (\_), and vertical bars (|)

The username is case sensitive.

#### **csPassword** *Common-Services-user-password*

Specify the password of the user specified in the `csUsername` option.

You can specify from 1 to 256 characters.

Usable character types are the same as for the `csUsername` option.

#### **appHostname** *Analyzer-server-host-name-or-IP-address*

Specify the host name or IP address for Analyzer server.

If this option is omitted, the host name of Analyzer server is set.

#### **appPort** *Analyzer-server-port*

Specify the port number for Analyzer server.

If this option is omitted, 22016 (SSL) is set.

#### **appName** *product-name-to-display-in-the-portal*

Specify the Analyzer name to display in the Ops Center Portal.

You can specify from 1 to 255 characters.

If this option is omitted during the registration of a new instance, the host name or IP address of Analyzer server is set.

**appDescription** *description-to-display-in-the-portal*

Specify the Analyzer description to display in the Ops Center Portal.

You can specify from 0 to 255 characters.

If this option is omitted, no description is displayed.

**auto**

Automatically stops and starts Analyzer server services.

**help**

Display usage information for this command.

## Location

In Windows

*Analyzer-server-installation-destination-folder\Analytics\bin*

In Linux

*Analyzer-server-installation-destination-directory/Analytics/bin*

## Notes

If you execute this command without specifying the `auto` option, restart the product by executing the `hcnds64srv` command on the host where you executed the command.

## Return values

| Return value | Description                                                             |
|--------------|-------------------------------------------------------------------------|
| 0            | The command ran normally.                                               |
| 1            | The argument is invalid.                                                |
| 2            | Command running was interrupted.                                        |
| 5            | Communication failed.                                                   |
| 6            | Authentication failed.                                                  |
| 14           | You do not have permission to run this command.                         |
| 16           | An attempt to start or stop the services of the Analyzer server failed. |
| 255          | Command running was interrupted because of another error.               |

## Example

To register a new instance of Analyzer in Common Services:

```
setupcommonservice -csUri https://myopscenter.com:443/portal -csUsername
sysadmin -csPassword sysadmin -appHostname myanalyzer.com -appName
Analyzer_B -appDescription "For managing site B" -auto
```

To reregister Analyzer in an instance of Common Services on another host:

```
setupcommonservice -csUri https://myopscenter2.com:443/portal -csUsername
sysadmin -csPassword sysadmin -appHostname myanalyzer.com -appName
Analyzer_B -appDescription "For managing site B" -auto
```



**Note:** After running the previous command, delete information about Analyzer from the Ops Center Portal that was previously used.

If the host name of the instance of Common Services in which Analyzer is registered was changed to `US_opscenter.com`:

```
setupcommonservice -csUri https://US_opscenter.com:443/portal -csUsername
sysadmin -csPassword sysadmin -auto
```

To change the host name of the Analyzer server that is registered in Common Services to `myanalyzer2.com`:

```
setupcommonservice -appHostname myanalyzer2.com -auto
```

---

## Appendix B: Analyzer server services

After you install Analyzer server on a Windows host, the following services are registered.

| Displayed service name                | Service name                | Startup type | Component        |
|---------------------------------------|-----------------------------|--------------|------------------|
| HAnalytics Engine Web Service         | AnalyticsWebService         | Automatic    | Analyzer server  |
| HBase 64 Storage Mgmt SSO Service     | HBase64StgMgmtSSOService    | Automatic    | Common component |
| HBase 64 Storage Mgmt Web Service     | HBase64StgMgmtWebService    | Automatic    | Common component |
| HBase 64 Storage Mgmt Web SSO Service | HBase64StgMgmtWebSSOService | Manual       | Common component |
| HiRDB/EmbeddedEdition_HD1             | HiRDBEmbeddedEdition_HD1    | Automatic    | Common component |

---

## Appendix C: User-specified properties file (config\_user.properties)

The definition file for configuring public logs and setting values for dynamic thresholds is described and explained.

### Format

*key-name=value*

### Location

For Windows

*Analyzer-server-installation-destination-folder\Analytics\conf*

For Linux

*Analyzer-server-installation-destination-directory/Analytics/conf*

### Timing at which definitions are applied

The definitions are applied when the HAnalytics Engine Web Service starts.

### Content to be specified

Specify each key name and its value on one line. When defining the user-specified properties file, note the following points:

- Any line starting with # is treated as a comment line.
- Blank lines are ignored.
- ISO8859-1 (for Windows) or UTF-8 (for Linux) is used for character encoding.
- Specified values are case-sensitive.
- To include "\" in a specified character string, specify "\\".  
In this situation, "\\" is counted as a single byte.
- If you specify an invalid value, the KNAQ02022-W message is output to the integrated trace logs and public logs, and the default value is used.
- If you specify the same key more than once in the same file, the last specification takes effect.

## Settings

| Category                              | Key name                              | Setting                                                                                                                                                                                                                             | Specifiable values                                              | Default value |
|---------------------------------------|---------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------|---------------|
| Public logs                           | logger.sysloglevel                    | Specify a threshold value for outputting an event log (in Windows) or syslog (in Linux).                                                                                                                                            | <ul style="list-style-type: none"> <li>0</li> <li>10</li> </ul> | 0             |
|                                       | logger.message.server.MaxBackupIndex  | Maximum number of log backup files for the server.                                                                                                                                                                                  | 1 to 16                                                         | 7             |
|                                       | logger.message.server.MaxFileSize     | Maximum size of log files for the server. (unit: KB)                                                                                                                                                                                | 4 to 2,097,151                                                  | 10240         |
|                                       | logger.message.command.MaxBackupIndex | Maximum number of log backup files for commands.                                                                                                                                                                                    | 1 to 16                                                         | 7             |
|                                       | logger.message.command.MaxFileSize    | Maximum size of log files for commands. (unit: KB)                                                                                                                                                                                  | 4 to 2,097,151                                                  | 1024          |
| Dynamic threshold values (parameters) | dynamicThreshold.calculateTime        | Time when the calculation of dynamic threshold values starts.                                                                                                                                                                       | 00:00:00 to 23:59:59                                            | 00:00:00      |
|                                       | dynamicThreshold.startLatencyDay      | <p>Period (unit: days) for which to check the number of performance values that are required to start the calculation of dynamic threshold values.</p> <p>To specify more than one value, use commas (,) to delimit the values.</p> | Single-byte numerals and commas (,)                             | 1, 3, 7, 14   |



| Category                          | Key name                                         | Setting                                                                                                                                                                                                                                                                                                                                                                                                       | Specifiable values | Default value |
|-----------------------------------|--------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|---------------|
|                                   | <code>dynamicThreshold.minimumDataN</code>       | Specify the minimum number of performance values that is required to start the calculation of dynamic threshold values.<br><br>The calculation of dynamic threshold values starts when the number of performance values in the period specified for <code>dynamicThreshold.startLatencyDay</code> exceeds the minimum number of performance values specified for <code>dynamicThreshold.minimumDataN</code> . | 1 to 2,147,483,647 | 150           |
| Dynamic threshold values (margin) | <code>dynamicThreshold.margin.Severe.plus</code> | Specify the margin for addition when the value of Margin is Severe.                                                                                                                                                                                                                                                                                                                                           | 0 to 2,147,483,647 | 1             |
|                                   | <code>dynamicThreshold.margin.Severe.rate</code> | Specify the margin for multiplication (unit: %) when the value of Margin is Severe.                                                                                                                                                                                                                                                                                                                           | 0 to 100           | 1             |
|                                   | <code>dynamicThreshold.margin.Normal.plus</code> | Specify the margin for addition when the value of Margin is Normal.                                                                                                                                                                                                                                                                                                                                           | 0 to 2,147,483,647 | 5             |
|                                   | <code>dynamicThreshold.margin.Normal.rate</code> | Specify the margin for multiplication (unit: %) when the value of Margin is Normal.                                                                                                                                                                                                                                                                                                                           | 0 to 100           | 5             |

| Category                                                    | Key name                              | Setting                                                                                                          | Specifiable values                                                                                                             | Default value           |
|-------------------------------------------------------------|---------------------------------------|------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------|-------------------------|
|                                                             | dynamicThreshold.margin.Rough.plus    | Specify the margin for addition when the value of Margin is Rough.                                               | 0 to 2,147,483,647                                                                                                             | 10                      |
|                                                             | dynamicThreshold.margin.Rough.rate    | Specify the margin for multiplication (unit: %) when the value of Margin is Rough.                               | 0 to 100                                                                                                                       | 10                      |
| Security                                                    | cert.verify.enabled                   | Specify whether to enable the verification of a server certificate.                                              | true or false                                                                                                                  | false                   |
| Controlling resources by using Storage I/O controls feature | automation.parameter.productName      | Specify the name that was set for Category in the <b>Web Service Connections</b> window of Ops Center Automator. | A value from 1 to 32 characters, using only single-byte alphanumeric characters, underscores (_), periods (.), and hyphens (-) | Analytics               |
|                                                             | automation.parameter.serviceGroupName | Specify the service group name that was set in Ops Center Automator for Ops Center Analyzer.                     | A value from 1 to 80 characters, using only single-byte alphanumeric characters and underscores (_)                            | Analytics Service Group |

| Category | Key name                                          | Setting                                                                                                                                                           | Specifiable values               | Default value                         |
|----------|---------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------|---------------------------------------|
|          | automation.parameter.serviceName.ioControl.modify | Specify the service name that was set when the service was created by using the service template "Modify IO Control Settings for Volume" in Ops Center Automator. | A value from 1 to 128 characters | Modify IO Control Settings for Volume |
|          | automation.parameter.serviceName.ioControl.delete | Specify the service name that was set when the service was created by using the service template "Delete IO Control Settings for Volume" in Ops Center Automator. | A value from 1 to 128 characters | Delete IO Control Settings for Volume |
|          | iocontrol.history.maxcount                        | Specify the maximum number of log entries to be retained for I/O control tasks.                                                                                   | 30 to 10,000                     | 5000                                  |
|          | iocontrol.cmd.parameterFile.maxCount              | Specify the maximum number of files that are used as the parameter file for I/O controls by using script files.                                                   | 1 to 5,000                       | 100                                   |
|          | iocontrol.cmd.parameterFile.minRetention.minute   | Specify the minimum retention of files that are used as the parameter file for I/O controls by using script files.                                                | 1 to 14,400                      | 5                                     |
| Event    | event.maxcount                                    | Specify the maximum number of events.                                                                                                                             | 1 to 1,000,000                   | 1000000                               |

| Category | Key name                   | Setting                                  | Specifiable values | Default value |
|----------|----------------------------|------------------------------------------|--------------------|---------------|
|          | event.retentionperiod.hour | Specify the retention period for events. | 1 to 2,880         | 2880          |

## Examples

```

logger.sysloglevel = 0
logger.message.server.MaxBackupIndex = 7
logger.message.server.MaxFileSize = 10240
logger.message.command.MaxBackupIndex = 7
logger.message.command.MaxFileSize = 1024
dynamicThreshold.calculateTime = 00:00:00
dynamicThreshold.startLatencyDay = 1, 3, 7, 14
dynamicThreshold.minimumDataN = 150
dynamicThreshold.margin.Severe.plus = 1
dynamicThreshold.margin.Severe.rate = 1
dynamicThreshold.margin.Normal.plus = 5
dynamicThreshold.margin.Normal.rate = 5
dynamicThreshold.margin.Rough.plus = 10
dynamicThreshold.margin.Rough.rate = 10
cert.verify.enabled = false
automation.parameter.productName = Analytics
automation.parameter.serviceGroupName = Analytics Service Group
automation.parameter.serviceName.ioControl.modify = Modify IO Control
Settings for Volume
automation.parameter.serviceName.ioControl.delete = Delete IO Control
Settings for Volume
iocontrol.history.maxcount = 5000
iocontrol.cmd.parameterFile.maxCount = 100
iocontrol.cmd.parameterFile.minRetention.minute = 5
event.maxcount = 1000000
event.retentionperiod.hour = 2880

```

---

## Appendix D: Analyzer server audit events that are output to the audit log

In Analyzer server, the following categories of audit events are output to the audit log:

- `StartStop`
- `ExternalService`
- `Authentication`
- `ConfigurationAccess`

Each audit event is assigned a severity level. You can filter the audit log data to be output according to the severity levels of events.

The following four tables describe, for each type, the audit events that are output to the audit log by the Analyzer server.

For details on the audit log data generated by other products that use the Common component, see the manuals for the relevant products.

The following table describes the audit events when the type is `StartStop`.

| Type description           | Audit event                 | Severity | Message ID  |
|----------------------------|-----------------------------|----------|-------------|
| Start and stop of software | Successful SSO server start | 6        | KAPM00090-I |
|                            | Failed SSO server start     | 3        | KAPM00091-E |
|                            | SSO server stop             | 6        | KAPM00092-I |

The following table describes the audit events when the type is `ExternalService`.

| Type description                                      | Audit event                                             | Severity | Message ID  |
|-------------------------------------------------------|---------------------------------------------------------|----------|-------------|
| Communication with the external authentication server | Successful communication with the LDAP directory server | 6        | KAPM10116-I |
|                                                       | Failed communication with the LDAP directory server     | 3        | KAPM10117-E |
|                                                       | Successful communication with the RADIUS server         | 6        | KAPM10118-I |

| Type description                                         | Audit event                                                                                  | Severity | Message ID  |
|----------------------------------------------------------|----------------------------------------------------------------------------------------------|----------|-------------|
|                                                          | Failed communication with the RADIUS server (no response)                                    | 3        | KAPM10119-E |
|                                                          | Successful communication with the Kerberos server                                            | 6        | KAPM10120-I |
|                                                          | Failed communication with the Kerberos server (no response)                                  | 3        | KAPM10121-E |
|                                                          | Successful communication with the DNS server                                                 | 6        | KAPM10122-I |
|                                                          | Failed communication with the DNS server (no response)                                       | 3        | KAPM10123-E |
| Authentication with an external authentication server    | Successful TLS negotiation with the LDAP directory server                                    | 6        | KAPM10124-I |
|                                                          | Failed TLS negotiation with the LDAP directory server                                        | 3        | KAPM10125-E |
|                                                          | Successful authentication of the user for an information search on the LDAP directory server | 6        | KAPM10126-I |
|                                                          | Failed authentication of the user for an information search on the LDAP directory server     | 3        | KAPM10127-W |
| User authentication on an external authentication server | Successful user authentication on the LDAP directory server                                  | 6        | KAPM10128-I |
|                                                          | User not found on the LDAP directory server                                                  | 4        | KAPM10129-W |
|                                                          | Failed user authentication on the LDAP directory server                                      | 4        | KAPM10130-W |
|                                                          | Successful user authentication on the RADIUS server                                          | 6        | KAPM10131-I |
|                                                          | Failed user authentication on the RADIUS server                                              | 4        | KAPM10132-W |
|                                                          | Successful user authentication on the Kerberos server                                        | 6        | KAPM10133-I |
|                                                          | Failed user authentication on the Kerberos server                                            | 4        | KAPM10134-W |

| Type description                                                  | Audit event                                                               | Severity | Message ID  |
|-------------------------------------------------------------------|---------------------------------------------------------------------------|----------|-------------|
| Acquisition of information from an external authentication server | Successful acquisition of user information from the LDAP directory server | 6        | KAPM10135-I |
|                                                                   | Failed acquisition of user information from the LDAP directory server     | 3        | KAPM10136-E |
|                                                                   | Successful acquisition of the SRV record from the DNS server              | 6        | KAPM10137-I |
|                                                                   | Failed acquisition of the SRV record from the DNS server                  | 3        | KAPM10138-E |
| Sending of a test email                                           | Successful sending of a test email                                        | 6        | KNAQ38002-I |
|                                                                   | Failed to send a test email                                               | 3        | KNAQ38003-E |
| Execution of an action defined in the command definition file     | Successful execution of an action defined in the command definition file  | 6        | KNAQ38058-I |
|                                                                   | Failed execution of an action defined in the command definition file      | 3        | KNAQ38059-E |
|                                                                   | Successful execution of an action defined in the command definition file  | 6        | KNAQ38062-I |
|                                                                   | Failed execution of action an defined in the command definition file      | 3        | KNAQ38063-E |
| Connection to the Analyzer detail view server                     | Successful connection to the Analyzer detail view server                  | 6        | KNAQ38064-I |
|                                                                   | Failed to connect to the Analyzer detail view server                      | 3        | KNAQ38065-E |
| Configuration of I/O control settings for a storage system        | Successful configuration of I/O control settings for a storage system     | 6        | KNAQ38068-I |
|                                                                   | Failed to configure I/O control settings for a storage system             | 3        | KNAQ38069-E |
| Connection to Ops Center Automator                                | Successful connection to Ops Center Automator                             | 6        | KNAQ38072-I |

| Type description                  | Audit event                                  | Severity | Message ID  |
|-----------------------------------|----------------------------------------------|----------|-------------|
|                                   | Failed to connect to Ops Center Automator    | 3        | KNAQ38073-E |
| Execution of an event action      | Successful execution of an event action      | 6        | KNAQ38078-I |
|                                   | Failed execution of an event action          | 3        | KNAQ38079-E |
| Start of a predictive task        | Successful start of a predictive task        | 6        | KNAQ38086-I |
|                                   | Failed start of a predictive task            | 3        | KNAQ38087-E |
| Interruption of a predictive task | Successful interruption of a predictive task | 6        | KNAQ38088-I |
|                                   | Failed interruption of a predictive task     | 3        | KNAQ38089-E |

The following table describes the audit events when the type is `Authentication`.

| Type description                         | Audit event                                              | Severity | Message ID  |
|------------------------------------------|----------------------------------------------------------|----------|-------------|
| Administrator or end user authentication | Successful login                                         | 6        | KAPM01124-I |
|                                          | Successful login (to the external authentication server) | 6        | KAPM02450-I |
|                                          | Failed login (wrong user ID or password)                 | 4        | KAPM02291-W |
|                                          | Failed login (logged in as a locked user)                | 4        | KAPM02291-W |
|                                          | Failed login (logged in as a nonexistent user)           | 4        | KAPM02291-W |
|                                          | Failed login (no permission)                             | 4        | KAPM01095-E |
|                                          | Failed login (authentication failure)                    | 4        | KAPM01125-E |
|                                          | Failed login (to the external authentication server)     | 4        | KAPM02451-W |
|                                          | Successful logout                                        | 6        | KAPM08009-I |
|                                          | Failed logout                                            | 4        | KAPM01126-W |



| Type description       | Audit event                                                                       | Severity | Message ID  |
|------------------------|-----------------------------------------------------------------------------------|----------|-------------|
| Automatic account lock | Automatic account lock (repeated authentication failure or expiration of account) | 4        | KAPM02292-W |

The following table describes the audit events when the type is `ConfigurationAccess`.

| Type description                                | Audit event                                                                 | Severity | Message ID  |
|-------------------------------------------------|-----------------------------------------------------------------------------|----------|-------------|
| User registration (GUI)                         | Successful user registration                                                | 6        | KAPM07230-I |
|                                                 | Failed user registration                                                    | 3        | KAPM07240-E |
| User deletion (GUI)                             | Successful single user deletion                                             | 6        | KAPM07231-I |
|                                                 | Failed single user deletion                                                 | 3        | KAPM07240-E |
|                                                 | Successful multiple user deletion                                           | 6        | KAPM07231-I |
|                                                 | Failed multiple user deletion                                               | 3        | KAPM07240-E |
| Password change (from the administrator window) | Successful password change by the administrator                             | 6        | KAPM07232-I |
|                                                 | Failed password change by the administrator                                 | 3        | KAPM07240-E |
| Password change (from the user's own window)    | Failed authentication processing for verifying old password                 | 3        | KAPM07239-E |
|                                                 | Successful change of login user's own password (from the user's own window) | 6        | KAPM07232-I |
|                                                 | Failed change of login user's own password (from the user's own window)     | 3        | KAPM07240-E |
| Profile change                                  | Successful profile change                                                   | 6        | KAPM07233-I |
|                                                 | Failed profile change                                                       | 3        | KAPM07240-E |
| Permission change                               | Successful permission change                                                | 6        | KAPM02280-I |
|                                                 | Failed permission change                                                    | 3        | KAPM07240-E |
| Account lock                                    | Successful account lock <sup>1</sup>                                        | 6        | KAPM07235-I |

| Type description                            | Audit event                                                                         | Severity | Message ID  |
|---------------------------------------------|-------------------------------------------------------------------------------------|----------|-------------|
|                                             | Failed account lock                                                                 | 3        | KAPM07240-E |
| Account lock release                        | Successful account lock release <sup>2</sup>                                        | 6        | KAPM07236-I |
|                                             | Failed account lock release                                                         | 3        | KAPM07240-E |
|                                             | Successful account lock release using the <code>hcnds64unlockaccount</code> command | 6        | KAPM07236-I |
|                                             | Failed account lock release using the <code>hcnds64unlockaccount</code> command     | 3        | KAPM07240-E |
| Authentication method change                | Successful authentication method change                                             | 6        | KAPM02452-I |
|                                             | Failed authentication method change                                                 | 3        | KAPM02453-E |
| Authorization group addition (GUI)          | Successful addition of an authorization group                                       | 6        | KAPM07247-I |
|                                             | Failed addition of an authorization group                                           | 3        | KAPM07248-E |
| Authorization group deletion (GUI)          | Successful deletion of one authorization group                                      | 6        | KAPM07249-I |
|                                             | Failed deletion of one authorization group                                          | 3        | KAPM07248-E |
|                                             | Successful deletion of multiple authorization groups                                | 6        | KAPM07249-I |
|                                             | Failed deletion of multiple authorization groups                                    | 3        | KAPM07248-E |
| Authorization group permission change (GUI) | Successful change of an authorization group's permission                            | 6        | KAPM07250-I |
|                                             | Failed change of an authorization group's permission                                | 3        | KAPM07248-E |
| User registration (GUI and CLI)             | Successful registration of user                                                     | 6        | KAPM07241-I |
|                                             | Failed to register user                                                             | 3        | KAPM07242-E |

| Type description                                       | Audit event                                                                                           | Severity | Message ID  |
|--------------------------------------------------------|-------------------------------------------------------------------------------------------------------|----------|-------------|
| User information update<br>(GUI and CLI)               | Successful update of user information                                                                 | 6        | KAPM07243-I |
|                                                        | Failed to update user information                                                                     | 3        | KAPM07244-E |
| User deletion<br>(GUI and CLI)                         | Successful deletion of user                                                                           | 6        | KAPM07245-I |
|                                                        | Failed to delete user                                                                                 | 3        | KAPM07246-E |
| Authorization group registration<br>(GUI and CLI)      | Successful registration of an authorization group                                                     | 6        | KAPM07251-I |
|                                                        | Failed registration of an authorization group                                                         | 3        | KAPM07252-E |
| Authorization group deletion<br>(GUI and CLI)          | Successful deletion of an authorization group                                                         | 6        | KAPM07253-I |
|                                                        | Failed deletion of an authorization group                                                             | 3        | KAPM07254-E |
| Authorization group permission change<br>(GUI and CLI) | Successful change of an authorization group's permission                                              | 6        | KAPM07255-I |
|                                                        | Failed change of an authorization group's permission                                                  | 3        | KAPM07256-E |
| Database backup or restore                             | Successful backup using the <code>hcnds64backups</code> command or the <code>hcnds64db</code> command | 6        | KAPM05561-I |
|                                                        | Failed backup using the <code>hcnds64backups</code> command or the <code>hcnds64db</code> command     | 3        | KAPM05562-E |
|                                                        | Successful full restore using the <code>hcnds64db</code> command                                      | 6        | KAPM05563-I |
|                                                        | Failed full restore using the <code>hcnds64db</code> command                                          | 3        | KAPM05564-E |
|                                                        | Successful partial restore using the <code>hcnds64db</code> command                                   | 6        | KAPM05565-I |
|                                                        | Failed partial restore using the <code>hcnds64db</code> command                                       | 3        | KAPM05566-E |

| Type description                   | Audit event                                                           | Severity | Message ID  |
|------------------------------------|-----------------------------------------------------------------------|----------|-------------|
| Database export or import          | Successful database export                                            | 6        | KAPM06543-I |
|                                    | Failed database export                                                | 3        | KAPM06544-E |
|                                    | Successful database import                                            | 6        | KAPM06545-I |
|                                    | Failed database import                                                | 3        | KAPM06546-E |
| Database area creation or deletion | Successful database area creation                                     | 6        | KAPM06348-I |
|                                    | Failed database area creation                                         | 3        | KAPM06349-E |
|                                    | Successful database area deletion                                     | 6        | KAPM06350-I |
|                                    | Failed database area deletion                                         | 3        | KAPM06351-E |
| Authentication data input/output   | Successful data output using the <code>hcnds64authmove</code> command | 6        | KAPM05832-I |
|                                    | Failed data output using the <code>hcnds64authmove</code> command     | 3        | KAPM05833-E |
|                                    | Successful data input using the <code>hcnds64authmove</code> command  | 6        | KAPM05834-I |
|                                    | Failed data input using the <code>hcnds64authmove</code> command      | 3        | KAPM05835-E |
| Update of the mail server settings | Successful update of the mail server settings                         | 6        | KNAQ38000-I |
|                                    | Failed update of the mail server settings                             | 3        | KNAQ38001-E |
| Creation of a user account         | Successful creation of a user account                                 | 6        | KNAQ38004-I |
|                                    | Failed creation of a user account                                     | 3        | KNAQ38005-E |
| Update of user information         | Successful update of user information                                 | 6        | KNAQ38006-I |
|                                    | Failed update of user information                                     | 3        | KNAQ38007-E |
| Deletion of a user account         | Successful deletion of a user account                                 | 6        | KNAQ38008-I |
|                                    | Failed deletion of a user account                                     | 3        | KNAQ38009-E |
| Creation of a threshold profile    | Successful creation of a threshold profile                            | 6        | KNAQ38010-I |

| Type description                                              | Audit event                                                                               | Severity | Message ID  |
|---------------------------------------------------------------|-------------------------------------------------------------------------------------------|----------|-------------|
|                                                               | Failed creation of a threshold profile                                                    | 3        | KNAQ38011-E |
| Update of a threshold profile                                 | Successful update of a threshold profile                                                  | 6        | KNAQ38012-I |
|                                                               | Failed update of a threshold profile                                                      | 3        | KNAQ38013-E |
| Deletion of a threshold profile                               | Successful deletion of a threshold profile                                                | 6        | KNAQ38014-I |
|                                                               | Failed deletion of a threshold profile                                                    | 3        | KNAQ38015-E |
| Settings for resources to be allocated to a threshold profile | Successful configuration of settings for resources to be allocated to a threshold profile | 6        | KNAQ38016-I |
|                                                               | Failed to configure settings for resources to be allocated to a threshold profile         | 3        | KNAQ38017-E |
| Settings for dynamic threshold values                         | Successful configuration of settings for dynamic threshold values                         | 6        | KNAQ38018-I |
|                                                               | Failed to configure settings for dynamic threshold values                                 | 3        | KNAQ38019-E |
| Consumer creation                                             | Successful creation of a consumer                                                         | 6        | KNAQ38020-I |
|                                                               | Failed creation of a consumer                                                             | 3        | KNAQ38021-E |
| Consumer update                                               | Successful update of a consumer                                                           | 6        | KNAQ38022-I |
|                                                               | Failed update of a consumer                                                               | 3        | KNAQ38023-E |
| Consumer deletion                                             | Successful deletion of a consumer                                                         | 6        | KNAQ38024-I |
|                                                               | Failed deletion of a consumer                                                             | 3        | KNAQ38025-E |
| Settings for resources to be allocated to a consumer          | Successful configuration of settings for resources to be allocated to a consumer          | 6        | KNAQ38026-I |
|                                                               | Failed to configure settings for resources to be allocated to a consumer                  | 3        | KNAQ38027-E |
| Creation of email address information                         | Successful creation of email address information                                          | 6        | KNAQ38028-I |
|                                                               | Failed creation of email address information                                              | 3        | KNAQ38029-E |

| Type description                                                                 | Audit event                                                                                                  | Severity | Message ID  |
|----------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------|----------|-------------|
| Update of email address information                                              | Successful update of email address information                                                               | 6        | KNAQ38030-I |
|                                                                                  | Failed update of email address information                                                                   | 3        | KNAQ38031-E |
| Deletion of email address information                                            | Successful deletion of email address information                                                             | 6        | KNAQ38032-I |
|                                                                                  | Failed deletion of email address information                                                                 | 3        | KNAQ38033-E |
| Change to the status of email address information                                | Successful change to the status of email address information                                                 | 6        | KNAQ38034-I |
|                                                                                  | Failed to change the status of email address information                                                     | 3        | KNAQ38035-E |
| Settings for a condition profile to be allocated to email address information    | Successful configuration of settings for a condition profile to be allocated to email address information    | 6        | KNAQ38036-I |
|                                                                                  | Failed to configure settings for a condition profile to be allocated to email address information            | 3        | KNAQ38037-E |
| Creation of a condition profile                                                  | Successful creation of a condition profile                                                                   | 6        | KNAQ38038-I |
|                                                                                  | Failed creation of a condition profile                                                                       | 3        | KNAQ38039-E |
| Update of a condition profile                                                    | Successful update of a condition profile                                                                     | 6        | KNAQ38040-I |
|                                                                                  | Failed update of a condition profile                                                                         | 3        | KNAQ38041-E |
| Deletion of a condition profile                                                  | Successful deletion of a condition profile                                                                   | 6        | KNAQ38042-I |
|                                                                                  | Failed deletion of a condition profile                                                                       | 3        | KNAQ38043-E |
| Settings for notification email addresses to be allocated to a condition profile | Successful configuration of settings for notification email addresses to be allocated to a condition profile | 6        | KNAQ38044-I |
|                                                                                  | Failed to configure settings for notification email addresses to be allocated to a condition profile         | 3        | KNAQ38045-E |

| Type description                                                                      | Audit event                                                                                      | Severity | Message ID  |
|---------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------|----------|-------------|
| Creation of resource allocation rules                                                 | Successful creation of resource allocation rules                                                 | 6        | KNAQ38046-I |
|                                                                                       | Failed creation of resource allocation rules                                                     | 3        | KNAQ38047-E |
| Update of resource allocation rules                                                   | Successful update of resource allocation rules                                                   | 6        | KNAQ38048-I |
|                                                                                       | Failed update of resource allocation rules                                                       | 3        | KNAQ38049-E |
| Deletion of resource allocation rules                                                 | Successful deletion of resource allocation rules                                                 | 6        | KNAQ38050-I |
|                                                                                       | Failed deletion of resource allocation rules                                                     | 3        | KNAQ38051-E |
| Priority of resource allocation rules                                                 | Successful change to the priority of resource allocation rules                                   | 6        | KNAQ38052-I |
|                                                                                       | Failed to change the priority of resource allocation rules                                       | 3        | KNAQ38053-E |
| Allocation of resources to a threshold profile based on the resource allocation rules | Successful allocation of resources to a threshold profile based on the resource allocation rules | 6        | KNAQ38054-I |
|                                                                                       | Failed allocation of resources to a threshold profile based on the resource allocation rules     | 3        | KNAQ38055-E |
| Update of information about conditions of the resource allocation rules               | Successful update of information about conditions of the resource allocation rules               | 6        | KNAQ38056-I |
|                                                                                       | Failed update of information about conditions of the resource allocation rules                   | 3        | KNAQ38057-E |
| Reloading of a definition file                                                        | Successful reloading of a definition file                                                        | 6        | KNAQ38060-I |
|                                                                                       | Failed to reload a definition file                                                               | 3        | KNAQ38061-E |
| Update of connection settings for the Analyzer detail view server                     | Successful update of connection settings for the Analyzer detail view server                     | 6        | KNAQ38066-I |

| Type description                                                             | Audit event                                                                             | Severity | Message ID  |
|------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------|----------|-------------|
|                                                                              | Failed update of connection settings for the Analyzer detail view server                | 3        | KNAQ38067-E |
| Update of the status of I/O control configuration tasks for a storage system | Successful update of the status of I/O control configuration tasks for a storage system | 6        | KNAQ38070-I |
|                                                                              | Failed update of the status of I/O control configuration tasks for a storage system     | 3        | KNAQ38071-E |
| Update of the connection settings for Ops Center Automator                   | Successful update of the connection settings for Ops Center Automator                   | 6        | KNAQ38074-I |
|                                                                              | Failed update of the connection settings for Ops Center Automator                       | 3        | KNAQ38075-E |
| Deletion of the connection settings for Ops Center Automator                 | Successful deletion of the connection settings for Ops Center Automator                 | 6        | KNAQ38076-I |
|                                                                              | Failed deletion of the connection settings for Ops Center Automator                     | 3        | KNAQ38077-E |
| Backup of server configuration information                                   | Successful backup of server configuration information                                   | 6        | KNAQ38082-I |
|                                                                              | Failed backup of server configuration information                                       | 3        | KNAQ38083-E |
| Restore of server configuration information                                  | Successful restore of server configuration information                                  | 6        | KNAQ38084-I |
|                                                                              | Failed to restore server configuration information                                      | 3        | KNAQ38085-E |
| Deletion of the predictive history                                           | Successful deletion of the predictive history                                           | 6        | KNAQ38090-I |
|                                                                              | Failed to delete the predictive history                                                 | 3        | KNAQ38091-E |
| Update of the status of the predictive history                               | Successful update of the status of the predictive history                               | 6        | KNAQ38092-I |
|                                                                              | Failed to update the status of the predictive history                                   | 3        | KNAQ38093-E |



| Type description                                                                                                                                                                                                                                                                                                                                                  | Audit event                                 | Severity | Message ID  |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------|----------|-------------|
| Creation of a predictive profile                                                                                                                                                                                                                                                                                                                                  | Successful creation of a predictive profile | 6        | KNAQ38094-I |
|                                                                                                                                                                                                                                                                                                                                                                   | Failed to create a predictive profile       | 3        | KNAQ38095-E |
| Editing of a predictive profile                                                                                                                                                                                                                                                                                                                                   | Successful editing of a predictive profile  | 6        | KNAQ38096-I |
|                                                                                                                                                                                                                                                                                                                                                                   | Failed to edit a predictive profile         | 3        | KNAQ38097-E |
| Deletion of a predictive profile                                                                                                                                                                                                                                                                                                                                  | Successful deletion of a predictive profile | 6        | KNAQ38098-I |
|                                                                                                                                                                                                                                                                                                                                                                   | Failed to delete a predictive profile       | 3        | KNAQ38099-E |
| Creation of a predictive report                                                                                                                                                                                                                                                                                                                                   | Successful creation of a predictive report  | 6        | KNAQ38100-I |
|                                                                                                                                                                                                                                                                                                                                                                   | Failed to create a predictive report        | 3        | KNAQ38101-E |
| Editing of a predictive report                                                                                                                                                                                                                                                                                                                                    | Successful editing of a predictive report   | 6        | KNAQ38102-I |
|                                                                                                                                                                                                                                                                                                                                                                   | Failed to edit a predictive report          | 3        | KNAQ38103-E |
| Deletion of a predictive report                                                                                                                                                                                                                                                                                                                                   | Successful deletion of a predictive report  | 6        | KNAQ38104-I |
|                                                                                                                                                                                                                                                                                                                                                                   | Failed to delete a predictive report        | 3        | KNAQ38105-E |
| <b>Notes:</b> <ol style="list-style-type: none"> <li>1. If an account is locked because the authentication method was changed for a user whose password is not set, this information is not recorded in the audit log.</li> <li>2. If an account is unlocked because a password was set for a user, this information is not recorded in the audit log.</li> </ol> |                                             |          |             |

## Hitachi Vantara



Corporate Headquarters

2535 Augustine Drive

Santa Clara, CA 95054 USA

[HitachiVantara.com](http://HitachiVantara.com) | [community.HitachiVantara.com](http://community.HitachiVantara.com)

Contact Information

USA: 1-800-446-0744

Global: 1-858-547-4526

[HitachiVantara.com/contact](http://HitachiVantara.com/contact)