Hitachi Ops Center Analyzer

10.8.3

Installation and Configuration Guide

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

MK-99ANA001-14
July 2022

Contents

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 10.8.3 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 the Hitachi Vantara Support Website: https://knowledge.hitachivantara.com/Documents.

Referenced documents

The following documents are referenced in this document.

- *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 Infrastructure Management Pack for VMware vRealize Operations User's Guide*, MK-92ADPTR081

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

Document conventions

This document uses the following typographic conventions:

Convention	Description
Bold	▪ Indicates text in a window, including window titles, menus, menu options, buttons, fields, and labels. Example: Click **OK**. ▪ Indicates emphasized words in list items.
Italic	▪ Indicates a document title or emphasized words in text. ▪ Indicates a variable, which is a placeholder for actual text provided by the user or for output by the system. Example: `pairdisplay -g group` (For exceptions to this convention for variables, see the entry for angle brackets.)
`Monospace`	Indicates text that is displayed on screen or entered by the user. Example: `pairdisplay -g oradb`
< > angle brackets	Indicates variables in the following scenarios: ▪ Variables are not clearly separated from the surrounding text or from other variables. Example: `Status-<report-name><file-version>.csv` ▪ Variables in headings.

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

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

Icon	Label	Description
	Note	Calls attention to additional information.
	Tip	Provides helpful information, guidelines, or suggestions for performing tasks more effectively.
	Important	Highlights information that is essential to the completion of a task.
	Caution	Warns the user of adverse conditions and/or consequences (for example, disruptive operations, data loss, or a system crash).
	CAUTION	Warns the user of a hazardous situation that, if not avoided, could result in major or minor injury.
	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

Physical capacity unit	Value
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: ▪ 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 the Hitachi Vantara Support Website: 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

The Hitachi Vantara Support Website is the destination for technical support of products and solutions sold by Hitachi Vantara. To contact technical support, log on to the Hitachi Vantara Support Website for contact information: https://support.hitachivantara.com/en_us/contact-us.html.

Hitachi Vantara Community 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 comments 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:

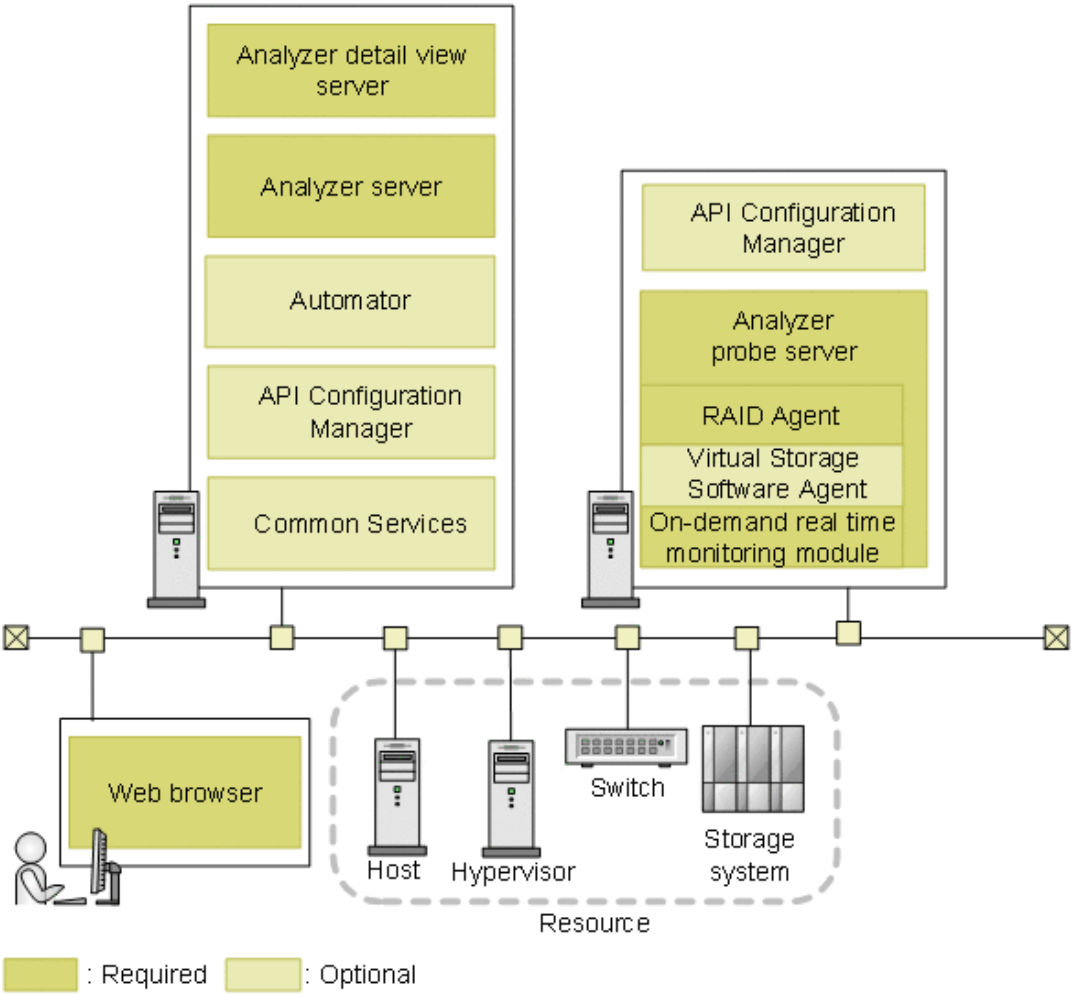
- **Analyzer server:** The primary component that communicates with the Analyzer detail view server. It correlates the configuration and performance data obtained by Analyzer detail view server to generate reports and enable data analytics for performance monitoring and problem resolution in your monitored 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. In both cases, you must also install the Analyzer probe server after installing the Analyzer server and 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. Install the Analyzer probe server on a different host than the one where the Analyzer detail view server is installed. When you install the Analyzer probe server, the following are installed at the same time: RAID Agent, Virtual Storage Software Agent (optional), and the On-demand real time monitoring module.

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 time on the Analyzer host must be synchronized with the time on other hosts running Ops Center products. We recommend configuring an NTP server.
- 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
- The Hitachi Enterprise Storage probe uses RAID Agent or Tuning Manager - Agent for RAID to collect information for the following storage systems: VSP E series, VSP F series, VSP G series, and the VSP 5000 series.
- The Hitachi VSS Block Storage probe uses Virtual Storage Software Agent to collect Virtual Storage Software Block information.
- 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 Analyzer probe server can connect with RAID Agent or Virtual Storage Software Agent installed on another host. Also, the Analyzer probe server can connect to multiple RAID Agents or Virtual Storage Software Agents.

  If you are not using a given instance of Analyzer probe server, RAID Agent, or Virtual Storage Software Agent, stop the relevant services:

  - If you are using RAID Agent or Virtual Storage Software Agent installed on a host other than the Analyzer probe server host, stop the Analyzer probe server services on the other host. For details, see Stopping the Analyzer detail view server or Analyzer probe server services (on page 440).
  - If you are not using the RAID Agent or Virtual Storage Software Agent instances installed on the same host as the Analyzer probe server, stop the RAID Agent and Virtual Storage Software Agent services. For details, see Stopping the RAID Agent services (on page 442) or Stopping the Virtual Storage Software Agent services (on page 443).

If you followed the procedure Starting the RAID Agent services (on page 440) to specify the setting that starts the RAID Agent services automatically when the OS starts, clear that setting.

- You can connect only one RAID Agent or Virtual Storage Agent to a storage system. If you connect two or more RAID Agents or Virtual Storage Software Agents, data collection might fail, some data might be missing, or the load on the storage system might increase.
- For some storage systems, you can select the data collection method. For details, see Selecting the data collection method (on page 154).
- 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.

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 259).

Default installation directory

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

Component name	Default installation directory
Analyzer server	`/opt/hitachi`
Analyzer detail view server	`/data`
Analyzer probe server	`/home`
Analyzer Windows probe	`C:\Program Files\HDCA\HDCA Windows Probe`
Ops Center API Configuration Manager	`/opt/hitachi/ConfManager` If this component was upgraded from a version earlier than 10.0.0, the previous installation path is inherited.
Common component[1]	*`Analyzer-server-installation-destination-directory`*`/Base64` If a Common component was already installed with another product, the new Common component is installed in the same directory.

Notes:

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.

Chapter 2: System requirements

Before installing, you must ensure that your environment meets the system requirements for Hitachi Ops Center Analyzer server, Ops Center Analyzer detail view server, and Analyzer probe server.

The following describes the system requirements when you use the Analyzer OVA, Analyzer probe OVA, or the installer. For details about system requirements for using the Ops Center consolidated OVA, see the *Hitachi Ops Center System Requirements*.

System requirements for using the Analyzer OVA and Analyzer probe OVA

Requirements for the Analyzer OVA

Before you install the Analyzer server and Analyzer detail view server using the Analyzer OVA (stand-alone OVA), review the guest operating system settings, virtualization software, and virtual machine resource settings requirements.

> **Note:**
>
> By default, `iptables` is used instead of the `firewalld` daemon.

Guest operating system settings

- Oracle Linux 8.4 (Architecture x86_64)

  For questions about the Oracle Linux OS that is packaged with this product, contact Oracle customer support.

  > **Note:**
  >
  > Apply operating system patches as needed.

Virtualization software

- VMware vSphere Hypervisor (VMware ESXi) 6.5u1, 6.7, 7.0, or 7.0u2

Resource settings for the virtual machine

The default resource settings assume that you are managing ten storage systems. For larger-scale systems, change the settings for memory, disk size, and virtual memory.

The following table lists the default resource settings for the Analyzer server, the Analyzer detail view server, and the operating system.

Item	Settings
Processor	16 cores
Memory	32 GB
Disk space	800 GB

The following tables list the required resources according to the size of the monitoring target (Small, Medium, Large, and Larger). Change the resources as needed. For details, see Hardware sizing based on system scale (on page 47).

- Hardware requirements for the Analyzer server

Processor (cores)	Memory	Free disk space for installation directory
Small: 4 Medium: 4 Large: 8 Larger: 16 Based on an Intel® Xeon® Processor E5-2670 v2 @ 2.50 GHz.	Small: 8 GB Medium: 8 GB Large: 16 GB Larger: 32 GB If you want to increase the memory from the default value of 8 GB, you must run the **`changememory`** command to change the maximum value that can be set for memory. For details, see changememory (on page 616).	Small: 100 GB Medium: 100 GB Large: 100 GB Larger: 100 GB

- Hardware requirements for the Analyzer detail view server

Processor (cores)	Memory	Free disk space for installation directory		
		Data retention period		
		14 days	32 days	365 days
Small: 2 Medium: 4 Large: 9 Larger: 20	Small: 10 GB Medium: 10 GB Large: 29 GB Larger: 77 GB	Small: 150 GB Medium: 150 GB Large: 150 GB Larger: 300 GB	Small: 150 GB Medium: 150 GB Large: 250 GB Larger: 650 GB	Small: 150 GB Medium: 1,250 GB Large: 2,800 GB

Processor (cores)	Memory	Free disk space for installation directory		
		Data retention period		
		14 days	32 days	365 days
Based on an Intel® Xeon® Processor E5-2670 v2 @ 2.50 GHz.				Larger: 7,100 GB
Note: Values are calculated based on the Hitachi Enterprise Storage system.				

Requirements for the Analyzer probe OVA

Before you install the Analyzer probe server and Ops Center Protector Client using the Analyzer probe OVA, review the guest operating system settings, virtualization software, and virtual machine resource settings requirements.

Note:

By default, `iptables` is used instead of the `firewalld` daemon.

Guest operating system settings

- Oracle Linux 8.4 (Architecture x86_64)

Virtualization software

- VMware vSphere Hypervisor (VMware ESXi) 6.5u1, 6.7, 7.0, or 7.0u2

Resource settings for the virtual machine

The default resource settings assume that you are managing five storage systems.

The following table lists the default resource settings.

Item	Settings
Processor	14 cores
Memory	42 GB
Disk space	200 GB

The following table lists the required resources according to the size of the monitoring target (Small, Medium, Large). Change the resources as needed. For details, see Hardware sizing based on system scale (on page 47).

Processor (cores)	Memory	Free disk space for installation directory
Small: 4 Medium: 6 Large: 12 Based on an Intel® Xeon® Processor E5-2670 v2 @ 2.50 GHz.	Small: 10 GB Medium: 17 GB Large: 24 GB **Note:** If you are monitoring a system that is similar or larger than Large scale, consider installing multiple probe servers.	Small: 150 GB Medium: 200 GB[1] Large: 300 GB[1] (The types of disks used are SAN disks.)

1. If you want to change the data collection interval from 5 minutes to 1 minute, the following free disk space is required:
   - Medium: 300 GB
   - Large: 450 GB

Note:

Values are calculated based on the Hitachi Enterprise Storage system.

OS changes based on security best practices (OVA)

The following OS setting changes are applied to the OVA to strengthen security. You can revert to the original settings if necessary. These OS settings can also be applied for the Ops Center products installed by using the installer.

Note that Hitachi Vantara does not take responsibility for, or support any interactions between, third-party programs and these OS settings.

/etc/modprobe.d/CIS.conf

Additional settings:

- install cramfs /bin/true
- install freevxfs /bin/true
- install jffs2 /bin/true
- install hfs /bin/true
- install hfsplus /bin/true
- install squashfs /bin/true
- install udf /bin/true
- install vfat /bin/true
- install dccp /bin/true
- install sctp /bin/true

- install rds /bin/true
- install tipc /bin/true

/etc/fstab

Original settings:

- /dev/mapper/ol-home /home xfs defaults 0 0

Additional settings:

- /dev/mapper/ol-home /home xfs defaults,nodev 0 0

/etc/sysctl.conf

Additional settings:

- net.ipv4.conf.default.accept_redirects = 0
- net.ipv4.conf.all.accept_redirects = 0
- net.ipv4.conf.default.send_redirects = 0
- net.ipv4.conf.all.send_redirects = 0
- net.ipv4.conf.all.secure_redirects = 0
- net.ipv4.conf.default.secure_redirects = 0
- net.ipv4.icmp_echo_ignore_broadcasts = 1
- net.ipv4.icmp_ignore_bogus_error_responses = 1
- net.ipv4.conf.all.rp_filter = 1
- net.ipv4.conf.default.rp_filter = 1
- net.ipv4.tcp_syncookies = 1
- kernel.randomize_va_space = 2
- net.ipv4.conf.all.log_martians = 1
- net.ipv4.conf.default.log_martians = 1
- fs.suid_dumpable = 0
- net.ipv4.conf.all.accept_source_route = 0
- net.ipv4.conf.default.accept_source_route = 0
- net.ipv4.ip_forward = 0

/etc/motd, /etc/issue, /etc/issue.net

Additional settings:

Authorized uses only. All activity may be monitored and reported.

Note: The default lines that identify the system name and kernel version for the login prompt in /etc/issue and /etc/issue.net have been removed.

Affected OVAs

Item	OVA
/etc/modprobe.d/CIS.conf	Analyzer OVA Analyzer probe OVA
/etc/fstab	Analyzer probe OVA
/etc/sysctl.conf	Analyzer OVA Analyzer probe OVA
/etc/motd, /etc/issue, /etc/issue.net	Analyzer OVA Analyzer probe OVA

System requirements for using the installer

This section provides the system requirements for using the installer.

Analyzer server requirements

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

Supported operating systems

- Red Hat Enterprise Linux 7.1-7.9, 8.1, 8.2, 8.4 (x64)
- Oracle Linux 7.1-7.9, 8.2, 8.4 (Unbreakable Enterprise Kernel) (x64)
- Oracle Linux 7.4-7.9, 8.1, 8.2, 8.4 (Red Hat Compatible Kernel) (x64)

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

▪ alsa-lib 1.0.27.2-3 or later
▪ bc 1.06.95-1 or later
▪ chkconfig.x86_64
▪ coreutils.x86_64
▪ gawk.x86_64
▪ glibc.x86_64
▪ grep.x86_64
▪ gzip.x86_64
▪ iproute
▪ libgcc.x86_64
▪ libselinux-utils.x86_64
▪ libstdc++.x86_64
▪ ncompress.x86_64
▪ ncurses.x86_64
▪ net-tools 1.60-110 or later
▪ net-tools.x86_64
▪ nss-softokn-freebl.i686
▪ policycoreutils 2.2.5-11 or later
▪ policycoreutils.x86_64
▪ procps-ng.x86_64
▪ sed.x86_64
▪ tar
▪ tcsh 6.17-24 or later
For Red Hat Enterprise Linux and Oracle Linux 7 or earlier, the following package is also required:
▪ policycoreutils-python.x86_64
For Red Hat Enterprise Linux and Oracle Linux 8 or later, the following packages are also required:
▪ freetype 2.9.1-4 or later
▪ glibc.i686 2.28-72 or later
▪ libgcc.i686 8.3.1-4.5 or later
▪ libnsl 2.28-72 or later
▪ libnsl.x86_64
	If dashboard reports are sent to users, you must install the following packages and package group:
	▪ package
	  • gtk3-3.22.10 or later
	  • libXScrnSaver 1.2.2-6.1 or later
	  • mesa-libgbm.x86_64
	  • nss-3.22 or later
	▪ package group
	  • fonts

RPM packages	Details
▪ libpng 1.6.34-5 or later ▪ libstdc++.i686 8.3.1-4.5 or later ▪ policycoreutils-python-utils.noarch	

Kernel parameters

Before installing the Analyzer server, 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 + *current-system-value*
`/etc/security/limits.conf`	`soft nofile` `hard nofile`	The larger of 8514 and the following value: 4418 + *current-system-value*
* 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

For details on the number of manageable resources, see Hardware sizing based on system scale (on page 47).

Processor (cores)	Memory	Free disk space for installation directory[1]	Free disk space by directory[1, 2]
Small: 4 Medium: 4 Large: 8 Larger: 16 Based on an Intel® Xeon® Processor E5-2670 v2 @ 2.50 GHz.	Small: 8 GB Medium: 8 GB Large: 16 GB Larger: 32 GB	Small: 100 GB Medium: 100 GB Large: 100 GB Larger: 100 GB To complete the installation, you need a minimum of 2 GB. Do not include any symbolic links in the installation directory. If the Common component is	`/tmp`: 2 GB `/var/opt`: 1 GB `/var/`*`installation-directory-path`*: 3 GB

Processor (cores)	Memory	Free disk space for installation directory[1]	Free disk space by directory[1, 2]
	If you want to increase the memory from the default value of 8 GB, you must run the **`changememory`** command to change the maximum value that can be set for memory. For details, see changememory (on page 616).	already installed, you need at least 2 GB of free space in the directory where the Common component is installed.	

1. Do not create these directories on a Network File System (NFS) partition.
2. The Analyzer server retrieves the partition details and checks the free disk space. Make sure that the required disk space is available.

   For example, if the `/tmp` directory is mounted on the P1 partition, the partition must have a minimum of 2 GB free.

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 7.1-7.9, 8.1, 8.2, 8.4 (x64)
- Oracle Linux 7.1-7.9, 8.2, 8.4 (Unbreakable Enterprise Kernel) (x64)
- Oracle Linux 7.4-7.9, 8.1, 8.2, 8.4 (Red Hat Compatible Kernel) (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.

If you set the `JAVA_HOME` environment variable for the Analyzer detail view server host, specify the OpenJDK or Oracle JDK directory used by the Analyzer detail view server.

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
▪ bc ▪ crontabs ▪ dejavu-sans-fonts ▪ expat-devel ▪ expect ▪ fontconfig 2.13.0-4.3 or later ▪ gcc ▪ initscripts ▪ lsof (recommended) ▪ nc or nmap-ncat (recommended) ▪ nss-3.21.0 or later ▪ openssl-devel (1.0.1e-fips 11 Feb 2013 or later) ▪ parted ▪ perl ▪ perl-CPAN ▪ perl-IO-Socket-SSL ▪ perl-XML-Simple ▪ sudo ▪ sysstat ▪ unzip ▪ xorg-x11-font-utils 7.5-21 or later ▪ xorg-x11-fonts-Type1 ▪ zip For Red Hat Enterprise Linux and Oracle Linux 7 or earlier, the following package is also required: ▪ net-tools ▪ policycoreutils-python	If nc (or nmap-ncat) and lsof are not installed or the path for jstack of the JDK is not set, some maintenance information will be unavailable. For this reason, we recommend you install the optional tool and set the necessary path.

RPM packages	Details
For Red Hat Enterprise Linux and Oracle Linux 8 or later, the following packages are also required: ▪ iproute ▪ policycoreutils-python-utils ▪ tar	

Kernel parameters

Before installing the Analyzer detail view server, 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

For details on the number of manageable resources for each system scale (Small, Medium, Large, and Larger), see Hardware sizing based on system scale (on page 47).

Processor (cores)	Memory	Free disk space for installation directory[1, 2, 3]			Free disk space by directory[3, 4]
		Data retention period			
		14 days	32 days	365 days	
Small: 4 Medium: 4 Large: 9 Larger: 20 Based on an Intel® Xeon® Processor E5-2670 v2 @ 2.50 GHz.	Small: 10 GB Medium: 10 GB Large: 29 GB Larger: 77 GB	Small: 150 GB Medium: 150 GB Large: 150 GB Larger: 300 GB	Small: 150 GB Medium: 150 GB Large: 250 GB Larger: 650 GB	Small: 150 GB Medium: 1,250 GB Large: 2,800 GB Larger: 7,100 GB	`/root`: 300 MB `/home`: 100 MB `/tmp`: 500 MB `/usr/local`: 1 GB

Processor (cores)	Memory	Free disk space for installation directory[1, 2, 3]			Free disk space by directory[3, 4]
		Data retention period			
		14 days	32 days	365 days	
		Do not include any symbolic links in the installation directory.			

1. To complete the installation, you need a minimum of 5 GB and the disk usage must be less than 95%.
2. You must install the Analyzer detail view server on a physical disk. When you run the **`analytics_install.sh`** command, do not install the Analyzer detail view server on the same disk where the operating system is installed.
3. Do not create these directories on a Network File System (NFS) partition.
4. The Analyzer detail view server retrieves the partition details and checks the free disk space. Make sure that the required disk space is available.

   For example, if:

   - the `/tmp` and `/usr/local` directories are mounted on the P1 partition, the partition must have a minimum of 1524 MB free.
   - the `/home` directory is mounted on the P2 partition, the partition must have a minimum of 100 MB free.

Note:

Values are calculated based on the Hitachi Enterprise Storage system.

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 7.1-7.9, 8.1, 8.2, 8.4 (x64)
- Oracle Linux 7.1-7.9, 8.2, 8.4 (Unbreakable Enterprise Kernel) (x64)
- Oracle Linux 7.4-7.9, 8.1, 8.2, 8.4 (Red Hat Compatible Kernel) (x64)

Note: Virtual Storage Software Agent does not support Red Hat Enterprise Linux and Oracle Linux versions 7.1-7.4.

When installing the operating system, select the default software package settings or add a software package with the default settings selected for installation.

Time zone

For the OS time zone, set the canonical time zone.

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.

If you set the `JAVA_HOME` environment variable for the Analyzer probe server host, specify the OpenJDK or Oracle JDK directory used by the Analyzer probe server.

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
▪ alsa-lib.x86_64 ▪ bc ▪ coreutils ▪ crontabs ▪ expat-devel ▪ expect ▪ firewalld ▪ gawk ▪ gcc ▪ glibc.i686 ▪ glibc.x86_64 ▪ grep ▪ initscripts ▪ iproute.x86_64 ▪ libgcc.x86_64 ▪ libstdc++.i686 ▪ libstdc++.x86_64 ▪ libyaml ▪ lsof (recommended) ▪ make	If nc (or nmap-ncat) and lsof are not installed or the path for jstack of the JDK is not set, some maintenance information will be unavailable. For this reason, we recommend you install the optional tool and set the necessary path. **Note:** If you want to use Red Hat Enterprise Linux and Oracle Linux 8 or later, we strongly recommend that after you install the prerequisite packages, you upgrade the following packages to the following versions: ▪ libsemanage 2.9-3 or later ▪ python3-libsemanage 2.9-3 or later

RPM packages	Details
▪ nc or nmap-ncat (recommended) ▪ ncurses ▪ net-tools ▪ nss-softokn-freebl.i686 ▪ nss-softokn-freebl.x86_64 ▪ nss-3.21.0 or later ▪ openssh-clients ▪ openssl-devel (1.0.1e-fips 11 Feb 2013 or later) ▪ openssl-1.0.2k or later ▪ perl ▪ perl-CPAN ▪ perl-Digest-MD5 ▪ perl-IO-Socket-SSL ▪ perl-XML-Simple ▪ policycoreutils ▪ rpm ▪ sed ▪ sysstat ▪ systemd ▪ sudo ▪ tcsh ▪ unzip ▪ which ▪ xinetd ▪ zip For Red Hat Enterprise Linux and Oracle Linux 8 or later, the following packages are also required: ▪ bzip2-libs.x86_64 ▪ glibc-all-langpacks ▪ glibc-locale-source ▪ glibc-minimal-langpack ▪ libnsl.i686 ▪ libnsl.x86_64	

RPM packages	Details
▪ libpng.x86_64 ▪ libxcrypt.i686 ▪ libxcrypt.x86_64 ▪ ncurses-compat-libs ▪ nss_db.i686 ▪ nss_db.x86_64 ▪ policycoreutils ▪ policycoreutils-python-utils ▪ tar ▪ zlib.x86_64	

Kernel parameters

Before installing the Analyzer probe server, 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

For details on the number of manageable resources for each system scale (Small, Medium, and Large), see Hardware sizing based on system scale (on page 47).

Processor (cores)	Memory[1]	Free disk space for installation directory[2]	Free disk space by directory[2]
Small: 6 Medium: 8 Large: 14	Small: 12 GB Medium: 21 GB Large: 30 GB	Small: 150 GB Medium: 200 GB[4] Large: 300 GB[3, 4]	Analyzer probe server: `/etc`: 100 MB `/home`: 100 MB

Processor (cores)	Memory[1]	Free disk space for installation directory[2]	Free disk space by directory[2]
Based on an Intel® Xeon® Processor E5-2670 v2 @ 2.50 GHz.	**Note:** If you are monitoring a system that is similar or larger than Large scale, consider installing multiple probe servers.	To complete the installation, you need a minimum of 5 GB and the disk usage must be less than 95%. Do not include any symbolic links in the installation directory.	`/root`: 300 MB `/tmp`: 100 MB `/usr/local`: 1 GB RAID Agent: `/opt/jp1pc`: Small: 3.1 GB Medium: 6.8 GB Large: 11.5 GB `/tmp`: 350 MB Virtual Storage Software Agent[5]: *`installation-directory-path/`*`VirtualStorageSoftwareAgent`: 1GB `/var/`*`installation-directory-path/`*`VirtualStorageSoftwareAgent`: 1GB `/var/log`: 7GB `/usr/lib/jvm`: 1GB

1. When analyzing Universal Replicator performance, if you perform monitoring with the maximum value of C/T delta set to a value greater than the default (3,600 seconds), the amount of memory used by the Analyzer probe server increases. You can calculate the amount of the increase by using the following formula:

   6,144,000 bytes x ((*maximum-value-of-C/T-delta* - 3600) / 3600) x *number-of-storage-systems-to-be-monitored*

   For details on how to change the maximum value of C/T delta, see Changing the maximum C/T delta value monitored when analyzing Universal Replicator performance (on page 482).

2. The Analyzer probe server retrieves the partition details and checks the free disk space. Make sure that the required disk space is available.

Processor (cores)	Memory[1]	Free disk space for installation directory[2]	Free disk space by directory[2]
For example, if: ▪ the `/tmp` and `/usr/local` directories are mounted on the P1 partition, the partition must have a minimum of 1124 MB free. ▪ the `/home` directory is mounted on the P2 partition, the partition must have a minimum of 100 MB free. ▪ the `/etc` directory is mounted on the P3 partition, the partition must have a minimum of 100 MB free. **3.** The types of disks used are SAN disks. **4.** If you want to change data collection interval from 5 minutes to 1 minute, the following free disk space is required: ▪ Medium: 300 GB ▪ Large: 450 GB **5.** This is the free disk space required to install Virtual Storage Software Agent. **Note:** Values are calculated based on the Hitachi Enterprise Storage system.			

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 Windows Server 2012 R2 Server core and Minimal Server Interface are not supported.	▪ Standard	No SP	x64
Windows Server 2016	▪ Standard	No SP	x64

OS name	Edition	SP	Architecture
Server core and Nano Server are not supported.			
Windows Server 2019 Server core is not supported.	▪ Standard ▪ Datacenter	No SP	x64

Network configuration

The Windows probe supports IPv4 only.

System locale

The Analyzer Windows probe must be installed on an English Windows machine with one of the following English System 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 the 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	▪ HTTP ▪ HTTPS

Hardware requirements

Prerequisites	Minimum
Processor	4 cores
Memory	8 GB
Disk space (system drive)	50 GB

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

Note: If you are using the Analyzer Windows probe, you must use the same version of Analyzer detail view server included in the product package for the probe. For details, see the Release Notes.

Hardware sizing based on system scale

The following table contains guidelines for determining the size of your environment based on the number of monitoring targets. Based on the sizing and scalability guidelines, you can identify the hardware requirements and scale your environment to meet workload demands.

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

The memory and disk space requirements vary depending on the managed resources. For example:

- a large number of volumes require a sizable database.
- if you decrease the interval at which you obtain performance information, the volumes occupy more disk space in the database.

If the Analyzer server and the Analyzer detail view server are installed on the same host and you are monitoring only storage systems, you might be able to decrease the required memory to a value less than the one described in Requirements for the Analyzer OVA (on page 29), Analyzer server requirements (on page 34), or Analyzer detail view server requirements (on page 37). The following table shows the maximum number of resources and the hardware requirements when the required memory is decreased.

Maximum number of resources		Memory requirement (total for the Analyzer server and the Analyzer detail view server)	Processor and disk area requirements
Storage			
Volume	Storage		
4,000	2	8 GB[1]	See the requirements for a medium-scale system.
20,000	5	15 GB[1]	See the requirements for a medium-scale system.
50,000	10	22 GB[2] You must run the **`changememory`** command to change the maximum amount of memory for the Analyzer server to 16 GB.	See the requirements for a large-scale system.

1. You can decrease the value to a value less than 18 GB, which is the amount of memory required for a medium-scale system (Analyzer server: 8 GB, Analyzer detail view server: 10 GB).
2. You can decrease the value to a value less than 45 GB, which is the amount of memory required for a large-scale system (Analyzer server: 16 GB, Analyzer detail view server: 29 GB).

Port requirements

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

Note: By default, `iptables` is used instead of the `firewalld` daemon in the virtual appliance.

Default port number for Analyzer server

Source IP address	Target IP address	Default port	Protocol
User Desktop[1]	Analyzer server	22015[2]	HTTP
		22016[2]	HTTPS
Analyzer server	RAID Agent Server or Tuning Manager - Agent for RAID Server	24221[3]	HTTP
		24222[3]	HTTPS
		22[3]	SSH
	Ops Center Common Services	443	HTTPS
	Common component	22031, 22032, 22035, 22036, 22037, and 22038	TCP
localhost	localhost	27100, 27102, 27103, and 27104 (internal; do not open these ports for external communication.)	TCP

Notes:

1. For virtual appliances, Any is open.
2. By default, HTTP and HTTPS can be used to access the Analyzer server.
3. 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[1]	Target IP address	Default port	Protocol
User Desktop, Analyzer server	Analyzer detail view server	8443	TCP
Analyzer probe server	Analyzer detail view server	9092	HTTP (default) or HTTPS
Analyzer probe server	Analyzer detail view server	22[2]	SFTP
		7443[2]	HTTPS
	Intermediate FTP Server	22[2]	SFTP
		21[2]	FTP
		990[2]	FTPS
Analyzer probe server	Analyzer detail view server	8443[3]	HTTPS
SNMP Manager server	Analyzer detail view server	9191	UDP
Analyzer detail view server	Ops Center Common Services	443	HTTPS
localhost	localhost	22[2]	SFTP
		9999, 8888, 8013, 6379, 6380, 6381, 6382, and 2181 (internal; do not open these ports for external communication.)	TCP

Notes:

1. For virtual appliances, Any is open.
2. This port is required for the data transfer protocol. Close this port if it is not required.
3. This port is required if you want to migrate Tuning Manager data. For details, refer to Migrating Hitachi Tuning Manager historical data (on page 201).

Default port number for Analyzer probe server

Source IP address[1]	Target IP address	Default port	Protocol
User Desktop	Analyzer probe server	8443	TCP
Analyzer probe server	Tuning Manager server	22015[2]	HTTP
		22016[2]	HTTPS
Analyzer detail view server	On-demand real time monitoring module	24262	WSS (WebSocket over TLS)
Analyzer probe server	Ops Center Common Services	443	HTTPS
localhost	localhost	9999 and 8888 (internal; do not open these ports for external communication.)	TCP

Notes:

1. For virtual appliances, Any is open.
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 201).

Probe port and firewall requirements

Probe name	Collection method	Source IP address	Target IP address	Default port	Protocol
Storage systems					
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
		RAID Agent Server or	Storage systems that are managed through SVP	See "Port numbers for each destination storage system" in	TCP

Probe name	Collection method	Source IP address	Target IP address	Default port	Protocol
		Tuning Manager - Agent for RAID Server		the next table.	
	RAID Agent (required if using REST API)	RAID Agent Server	GUM (CTL) (for storage other than VSP 5000 series) or SVP (for VSP 5000 series)	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 Configuratio n Manager Server	23450	HTTP
				23451	HTTPS
Hitachi NAS	RUSC	Analyzer probe server	HNAS SMU	22	SSH
	REST API		HNAS REST API Server	8444	HTTPS
Hitachi VSS Block Storage	Vitural Storage Software Agent (REST API)	Analyzer probe server	Virtual Storage Software Agent Server	24081	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	

Probe name	Collection method	Source IP address	Target IP address	Default port	Protocol
IBM Power Systems	HMC (Hardware Management Console) REST API	Analyzer probe server	IBM Power Systems managed by Hardware Management Console (HMC)	12443	HTTPS
FC Switches					
Brocade FC Switch (BNA)	BNA (REST API)	Analyzer probe server	BNA server	80	HTTP
				443	HTTPS
Brocade FC Switch	Brocade Switch CLI	Analyzer probe server	Brocade FC Switch	22	SSH
	Fabric OS REST API			80	HTTP
				443	HTTPS
Cisco FC Switch (DCNM) (10.0 does not support HTTP)	DCNM (Web Services)	Analyzer probe server	DCNM Server	80	HTTP
				443	HTTPS
	DCNM (REST API)	Analyzer probe server	DCNM Server	443	HTTPS
Cisco FC Switch (CLI)	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 (For virtual appliances, Any is open.)	TCP

Port numbers for destination storage systems

	VSP 5000 series	VSP E990, VSP G/F350, G/F370, G/F700, G/F900, VSP G200, G/F400, G/F600, G/F800	VSP G1000, G1500, and VSP F1500
Default port	443	443	443
	11099	1099	1099
	51099	51099	51099
	51100	51100-51355	51100

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

Analyzer server supports the following browsers:

Web browser/other	Version
Firefox	ESR 91
Internet Explorer	11*
Microsoft Edge	Latest version of stable channel
Chrome Browser for enterprise	Latest version of stable channel
* Browser subwindows may open behind the main (parent) window.	

Analyzer detail view server and Analyzer probe server support the following browsers:

Web browser/other	Version
Firefox	ESR 91
Microsoft Edge	Latest version of stable channel
Chrome Browser for enterprise	Latest version of stable channel

Monitoring target requirements

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

Monitoring target storage systems

You can monitor the following storage systems:

Storage System	Microcode/Firmware version	Analyzer probe
VSP 5100, 5500, 5100H, 5500H	90-02 or later	Hitachi Enterprise Storage probe **Note:** ▪ This probe collects data from storage systems when using the RAID Agent or Tuning Manager - Agent for RAID. ▪ 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.
VSP 5200, 5600, 5200H, 5600H	90-08 or later	
VSP E590, E790	93-03-21 or later	
VSP E590H, E790H	93-05-01 or later	
VSP E990	93-02 or later	
VSP E1090, E1090H	93-06-21 or later	
VSP G1000, G1500, and VSP F1500	80-06-63 or later	
VSP G/F350, G/F370, G/F700, G/F900	88-02-01 or later	
VSP G200, G/F400, G/F600, G/F800	83-05-29 or later	
VSP N400, N600, N800 See "Notes on notation of the VSP N series" following this table.	83-06-01 or later	
Hitachi NAS platform (HNAS) firmware and System management unit (SMU) 3080, 3090, 4040, 4060, 4080, 4100, 5000 series, VSP G/F400, G/F600, G/F800, VSP N400, N600, N800	13.5 or later	HNAS probe **Note:** To view NAS configuration and performance reports, go to the Analyzer detail view server.
Virtual Storage Software Block	1.10 or later	Hitachi VSS Block Storage probe

Note:

- The following storage systems might be referred to as VSP family:
  - VSP E series
  - VSP F series
  - VSP G series
  - VSP 5000 series
- VSP family 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, G/F400, G/F600, G/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	▪ 6.5 ▪ 6.5u2	VMware probe

Product name		Version	Analyzer probe name
		▪ 6.7 ▪ 7.0 ▪ 7.0u2	
	VMware ESXi	▪ 6.5 ▪ 6.5u2 ▪ 6.7 ▪ 6.7u2 ▪ 7.0 ▪ 7.0u2	
Hyper-V	Windows Server 2012 Hyper-V Windows Server 2012 R2 Hyper-V Server core is not supported.	--	Windows probe
	Windows Server 2016 Hyper-V		
	Windows Server 2019 Hyper-V ▪ Standard ▪ Datacenter		
IBM Power Systems	HMC	V9R2	IBM Power Systems probe
	IBM Power Systems	P7-740 (8205-E6C)	

Monitoring target hosts

You can monitor the following hosts:

OS name		Version/Edition	Analyzer probe name
Windows	Windows Server 2012 Windows Server 2012 R2	▪ Standard	Windows probe

OS name		Version/Edition	Analyzer probe name
	Server core is not supported.		
	Windows Server 2016 Server core and Nano Server are not supported.	▪ Standard	
	Windows Server 2019 Server core is not supported.	▪ Standard ▪ Datacenter	
Linux	Red Hat Enterprise Linux	▪ 7.1 - 7.9 ▪ 8.1 ▪ 8.2 ▪ 8.4	Linux probe
	SUSE Linux Enterprise Server	▪ 11 ▪ 12	
	Oracle Linux	▪ 7.0 ▪ 7.3 - 7.9 ▪ 8.1 ▪ 8.2 ▪ 8.4	
	CentOS	▪ 7.1 ▪ 7.2	

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	▪ 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 (CLI)	▪ 6.1.2b1 ▪ 6.2.2d ▪ 6.3.2e8 ▪ 7.0.2e ▪ 7.2.1a ▪ 7.4.1b ▪ 7.4.1d ▪ 8.1.2a ▪ 8.2.0 ▪ 8.2.0a ▪ 8.2.0b ▪ 8.2.1c ▪ 8.2.2 ▪ 8.2.2a	Brocade FC Switch probe
	Brocade Fabric OS (REST API)	▪ 8.2.1a1 ▪ 8.2.2 ▪ 8.2.2a ▪ 8.2.3a ▪ 9.0.1b	

Switch name	Software	Version/Model	Analyzer probe name
Cisco	Cisco Data Center Network Manager (Web Services)	▪ 5.0 ▪ 6.3 ▪ 7.1 ▪ 10.0 ▪ 10.2 ▪ 10.3 ▪ 10.4(2)	Cisco FC Switch (DCNM) probe
	Cisco Data Center Network Manager (REST API)	▪ 11.4 ▪ 11.5(1)	
	Cisco SAN Switch (CLI)	▪ MDS 9124 ▪ MDS 9145 ▪ MDS 9148 ▪ MDS 9148S ▪ MDS 9513	Cisco FC Switch (CLI) probe

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 Ops Center consolidated OVA. For details, see the *Hitachi Ops Center Installation and Configuration Guide*.

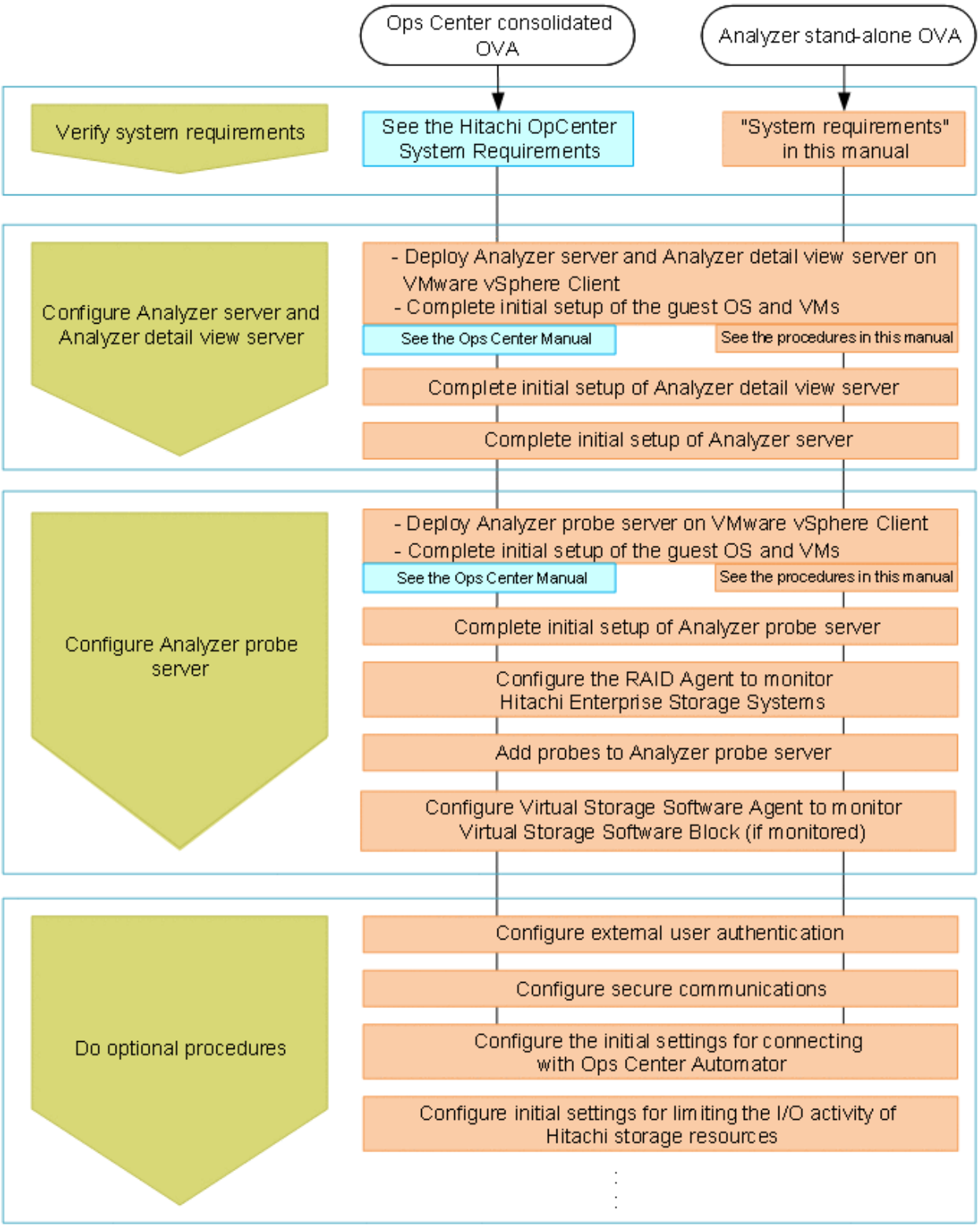
https://knowledge.hitachivantara.com/Documents/Management_Software/Ops_Center

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 install Analyzer using a stand-alone OVA


Ops Center consolidated OVA
Analyzer stand-alone OVA
Verify system requirements
See the Hitachi OpCenter System Requirements
"System requirements" in this manual
Configure Analyzer server and Analyzer detail view server
- Deploy Analyzer server and Analyzer detail view server on VMware vSphere Client
- Complete initial setup of the guest OS and VMs
See the Ops Center Manual
See the procedures in this manual
Complete initial setup of Analyzer detail view server
Complete initial setup of Analyzer server
Configure Analyzer probe server
- Deploy Analyzer probe server on VMware vSphere Client
- Complete initial setup of the guest OS and VMs
See the Ops Center Manual
See the procedures in this manual
Complete initial setup of Analyzer probe server
Configure the RAID Agent to monitor Hitachi Enterprise Storage Systems
Add probes to Analyzer probe server
Configure Virtual Storage Software Agent to monitor Virtual Storage Software Block (if monitored)
Do optional procedures
Configure external user authentication
Configure secure communications
Configure the initial settings for connecting with Ops Center Automator
Configure initial settings for limiting the I/O activity of Hitachi storage resources

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).

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: 172.30.197.99
   - 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. If you want to use Common Services, you must manually register Analyzer, Analyzer detail view and Analyzer probe in Common Services.

Note:

- You can run the setup tool only once. Afterwards, you must change the settings manually.
- 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`**.

   Note:

   This setup tool is stored in `/opt/OpsVM/vmtool` but you can run the tool from any location.

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 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.

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 Requirements for the Analyzer OVA (on page 29).
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 the Analyzer probe server and Protector Client (VMware vSphere Client)

By deploying the OVA file (the Analyzer probe OVA), you can create a virtual machine on which Analyzer probe server, Protector Client, and Ops Center API Configuration Manager are 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 the 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 the 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
    ```

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

    Note: If you do not want to collect performance information using a command device, skip these settings.

    Use a 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 add, 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.
  - 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. The RAID Agent startup might fail in the replicated environment.

Procedure

1. From a VMware vSphere client, log on to the VMware ESXi server.
2. Deploy the Analyzer probe OVA (`dcaprobe_`*`version`*`.ova`) by selecting **File** > **Deploy OVF Template**, and then following the prompts.

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.

   This operation is not required if you are sure that the IP addresses will not conflict.

   When deployment is complete, the following default network settings are used for the virtual machine:

   - **IP address:** 172.30.197.101
   - **Net mask:** 255.255.0.0
   - **Default gateway:** 172.30.0.1

   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 in for the first time, use the following user ID and password:

   User ID: `root`

   Password: `manager`

   After you log in, 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 guest OS initial settings.

> **Note:** When running the Analyzer probe server, Ops Center API Configuration Manager, and Protector Client on the same VM, all components share the same command device, but Ops Center API Configuration Manager and Protector Client must access the storage systems using different credentials. This means they must use different user accounts when accessing the storage system.

> **Tip:** The Analyzer probe server and Protector Client are installed in the following directory on the virtual machine.
>
> - Analyzer probe server: `/home`
> - Protector Client: `/opt/hitachi/protector`

Initial setup of the guest OS or VMs

After deploying the virtual appliance, run the setup tool (**`opsvmsetup`**) to specify the guest OS initial settings. If you want to use Protector, specify settings for Protector. If you want to use Common Services, you must manually register Analyzer probe in Common Services.

Procedure

1. From the VMware vSphere Client, log on to the guest OS.
2. Run the **`opsvmsetup`** command.

   Note:
   - You can run the setup tool only once. To change the settings after running the setup tool, use the operating system commands.
   - This setup tool is stored in `/opt/OpsVM/vmtool` but you can run the tool from any location.

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 available time zone values:

         ```
         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
   - **Protector settings:**
     - Whether to use Protector
     - Protector master host name
     - Protector master IPv4 address

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.

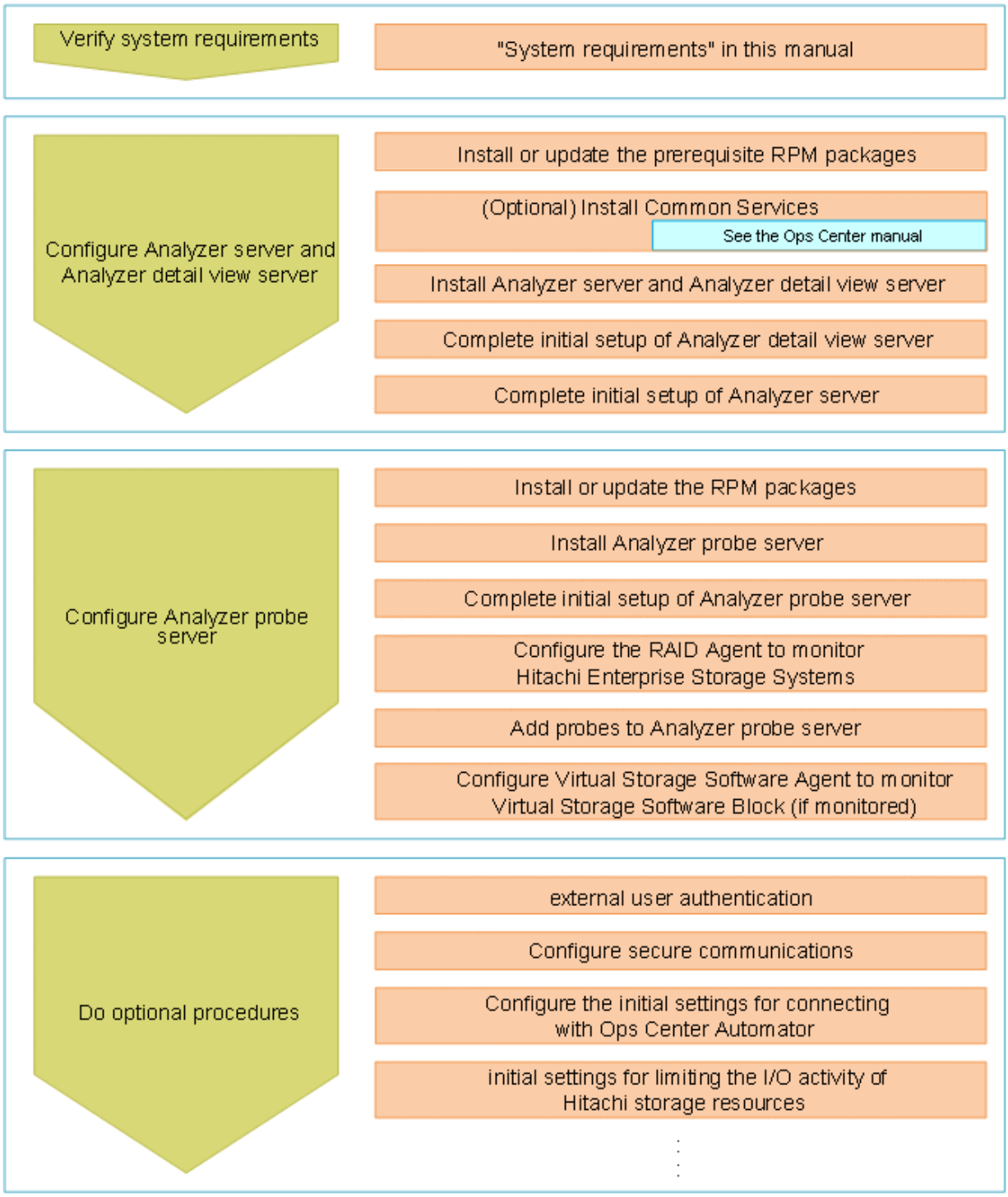
5. If the virtual machine is not connected to the network when deployed, complete the following steps to enable the network adapter:
   a. Log on to the guest OS.
   b. Stop the virtual machine by running the **`shutdown`** command.
   c. Right-click the virtual machine that you want to stop, and then 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. If you want to use Common Services, you must manually register Analyzer, Analyzer detail view, and Analyzer probe in Common Services by performing the procedures described in "Initial setup after installation".



Installing or updating the prerequisite RPM packages

You can obtain the prerequisite RPM packages from the Linux OS media or the distribution website, such as for Red Hat Enterprise Linux.

You can check which RPM packages are missing by running the precheck tool (`analytics_precheck.sh`).

If the `libstdc++` package is already installed in the environment in which the Analyzer probe server:

```
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 the `x86_64` (the 64-bit library), and then retry the installation of `libstdc++.i686`:

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

Installing or updating the RPM packages by using the Linux OS media

The following describes how to install or update the RPM packages by using the Linux OS media.

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

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

2. Configure the yum repository.

   - For Red Hat Enterprise Linux and Oracle Linux 7 or earlier:

     ```
     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
     ```

   - For Red Hat Enterprise Linux and Oracle Linux 8 or later:

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

   - **For the package group:**

     ```
     yum group install package-group-to-install
     ```

4. Unmount the Linux OS media:

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

Installing or updating the RPM packages using the distribution website

The following describes how to install or update the RPM packages by using the distribution website.

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-install
     ```

   - **For the package group:**

     ```
     yum group install package-group-to-install
     ```

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 `20-nproc.conf` file, if it does not exist.

b. Ensure that the following two properties are present in the `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

To install the Analyzer server and Analyzer detail view server, 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, 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.
- Verify that the ports you specify are available for communication. The default ports are 22015 (non-SSL) and 22016 (SSL).
- To prevent an installation error, verify that the ports used by the Common component (27100, 27102, 27103, and 27104) are not used by other processes.
- Verify that you have root permissions to run the installer and the precheck tool.
- Verify that the console and clock properties are set to the same time zone.
- Verify that 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, follow these rules. For the installation location of the Analyzer server, we recommend the `/opt` directory:
  - Specify a directory name of less than 94 bytes.
  - Use the following characters:

    `A-Z a-z 0-9 / _`
  - Do not use spaces.
  - Do not use a path separator (`/`) at the end of a path.
- Do not include any symbolic links in the installation path.
- Make sure that the following directories are not mounted with the `noexec` option:
  - `/opt`
  - `/tmp`
  - `/var/opt`

Before you begin installation of Analyzer detail view server, review the following prerequisites:

- Review the Analyzer detail view server requirements (hardware and software).
- Prepare an unformatted device (physical device or logical device such as an LVM) specifically for installing the Analyzer detail view server. For details about disk space requirements, see the Analyzer detail view server requirements.
- Verify that the ports you specify are available for communication. The default port is 8443.
- Verify that you have root permissions 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.
- Verify that the console and clock properties are set to the same time zone.
- Verify that 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.
- During installation, when prompted to specify the installation directory for the Analyzer detail view server, follow these rules:
  - Specify a directory name of less than 94 bytes.
  - Use the following characters:

    `A-Z a-z 0-9 + ^ , ~ ! # @ { } _ . -`
  - Do not use spaces.
- Do not include any symbolic links in the installation path.

- Check the kernel and system limits on the number of open files and processes. For more information, see Increasing the maximum number of open files (Linux OS) (on page 76).
- If `firewalld` is enabled during installation, settings will be changed for all active zones. If necessary, revise the settings after the installation finishes.

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:
   - You must use only the following characters in the directory path to which the installer is copied: `A-Z a-z 0-9 - . _`
   - Do not use spaces.

   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/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
   ```

   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 following message is shown, refer to the release notes.

```
An Analyzer server earlier than v10.7.0, Hitachi Ops Center Automator earlier
than v10.8.0, or Hitachi Command Suite earlier than v8.8.3 is already installed
on this server. Make sure to upgrade the relevant products by referring to the
Release Notes.
```

Note:

- When you run the precheck tool, it checks the static information of the system environment.
- 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 a root user 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.

Do not change the size of the device window while the command is running. If you change the size of the window, the installation fails.

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 (with a `TYPE` of `lvm`, `mpath`, or `raid`) as displayed in the tree in `<System device information>` (Example: `DCAvg-DCAlv00`)

If you select a partition or a volume group of LVM, all the free disk space is used to create a logical volume for the LVM.

```
[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  200G  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]:

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. When you enter `y`, the firewall rules that are currently applied are saved.

```
[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 firewall,
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 by 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(Mount point) : /data
Device name                         : [create new partition, volume group, and
logical volume] on /dev/sdb
Filesystem                          : xfs
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 change firewall 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. At this time, the firewall rules that are currently applied are saved.

```
[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
```

If the following message is shown, refer to the release notes.

```
An Analyzer server earlier than v10.7.0, Hitachi Ops Center Automator earlier
than v10.8.0, or Hitachi Command Suite earlier than v8.8.3 is already installed
on this server. Make sure to upgrade the relevant products by referring to the
Release Notes.
```

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

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

Installing Analyzer probe server

To install the Analyzer probe server, 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.
- During installation, when prompted to specify the installation directory for the Analyzer probe server, follow these rules:
  - Use the following characters:

    `A-Z a-z 0-9 + [ ] , ~ ! # @ { } _ . -`
  - Do not use spaces.
- Do not include any symbolic links in the installation path.
- 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 76) 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 are not mounted with 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, delete it manually if necessary.
  - The IP address must be resolvable from the host name of the host where RAID Agent is installed. Check the `hosts` file or the domain name system (DNS) server configuration of the host where RAID Agent is installed.
  - The RAID Agent cannot run on hosts that use DHCP to assign IP addresses. 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. You must exclude the domain 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. The following example is an example that sets C for the LANG value and 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
    ```

- If needed, you can install Virtual Storage Software Agent when you install Analyzer probe server.
  - If `firewalld` is enabled, the settings will be changed for the default zone. If required, revise the settings after the installation finishes.

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:
   - You must use only the following characters in the directory path to which the installer is copied: `A-Z a-z 0-9 - . _`
   - Do not use spaces.

   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
   ```

   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]
   ```

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

   Do not change the size of the device window while the command is running. If you change the size of the window, the installation fails.

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. At this time, the firewall rules that are currently applied are saved.

```
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 firewall 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.

12. When you want to monitor Virtual Storage Software Block (VSSB) systems, you need to install the required agent.

```
Do you want to install the Virtual Storage Software Agent server? (y/n) [n]: y
```

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, it makes certain changes to the host environment when you install the Analyzer detail view server or the Analyzer probe server.

Note: The installer does not make any changes to the Analyzer server.

Analyzer detail view server

The installer makes the following changes to the host environment settings.

Change	Details
Addition of users	The following users are added: ▪ megha ▪ meghadata You must change the default passwords. Refer to Changing the megha and meghadata passwords (on page 108) for more information.
Addition of groups	The following group is added: megha.
Changes to the cron settings	A setting that periodically starts the service and monitors resource usage for the Analyzer detail view server is added.
Changes to the ssh settings	The `/etc/ssh/sshd_config` file is edited, and settings are added as follows to allow the meghadata user to access the Analyzer detail view server by using password authentication. ▪ If `sftp /usr/libexec/openssh/sftp-server` is set in the SFTP server subsystem settings: • Match User meghadata • PasswordAuthentication yes ▪ If `sftp internal-sftp` is set in the SFTP server subsystem settings: • Match User meghadata • PasswordAuthentication yes • ForceCommand internal-sftp -u 2 If you want to change the SFTP server subsystem settings, see Default meghadata user settings for Analyzer detail view server (on page 498).

Change	Details

Kernel parameter settings	The following kernel parameters are set:
	▪ 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:
	`/usr/lib/sysctl.d/60-hiaa.conf`
	▪ 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:
	`/etc/security/limits.conf`
	▪ 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:
	`/etc/security/limits.d/20-nproc.conf`
	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 `/etc/rc.local`.
Installation of the Perl module	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

Change	Details
	installed as part of the installation of Analyzer detail view server. ▪ Module::Build ▪ YAML ▪ XML::Simple ▪ Log::Log4perl ▪ LWP::UserAgent ▪ LWP::Protocol::https Required prerequisite perl modules are also installed.

Analyzer probe server

The installer makes the following changes to the host environment settings.

Change	Details
Addition of users	The following user is added: ▪ megha You must change the default password. Refer to Changing the megha and meghadata passwords (on page 108) for more information.
Addition of groups	The following group is added: megha.
Changes to the cron settings	A setting that periodically starts the service and monitors resource usage for the Analyzer probe server is added.

Change	Details

Kernel parameter settings	The following kernel parameters are set:
	▪ 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:
	`/usr/lib/sysctl.d/60-hiaa.conf`
	▪ 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:
	`/etc/security/limits.conf`
	▪ 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:
	`/etc/security/limits.d/20-nproc.conf`
	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 `/etc/rc.local`.
Installation of the Perl module	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. ▪ Module::Build ▪ YAML

Change	Details
	▪ 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 Required prerequisite perl modules are also installed.
Addition of SELinux policy records	If the OS is Red Hat Enterprise Linux/Oracle Linux 8 and Virtual Storage Software Agent is installed, policy records for files in the following directory are added: `/var/Virtual-Storage-Software-Agent-installation-destination-directory/VirtualStorageSoftwareAgent`

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

After installing Analyzer server and the Analyzer detail view server, perform the initial setup of Analyzer detail view.

To use Common Services and single sign-on through the Ops Center Portal, you must also register Analyzer detail view in Common Services and assign Analyzer detail view permissions to Ops Center user groups. If you deployed the Ops Center OVA, Analyzer detail view is already registered in Common Services. If you used the stand-alone OVA or installer, you must register with Common Services manually. If you change the host name, IP address, or port number of the server where Common Services is installed, you must register Analyzer detail view again.

Note:

Products installed with 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 detail view server:

Procedure

1. (Optional) If you want to use Common Services and access Analyzer detail view from the Ops Center Portal, run the `setupcommonservice` command to register Analyzer detail view in Common Services.
2. Perform the initial setup of the Analyzer detail view server.
3. (Optional) If you want to use Common Services, assign Analyzer detail view permissions to the Ops Center user group.

Registering Analyzer detail view server with Common Services

If you want to use Common Services installed on a different host, or you installed Analyzer detail view server using the stand-alone OVA or installer, you must register Analyzer detail view server with Common Services.

If you deployed the Ops Center consolidated OVA, Analyzer detail view is already registered in Common Services.

Before you begin

Verify the following:

- The host name of Common Services is resolvable from the Analyzer detail view server.
- The Analyzer detail view server and Common Services are running.
- SSL is configured for the Analyzer detail view server and Common Services.
- A user account exists with Common Services that has Administrator permissions.

Procedure

1. Log on to the Analyzer detail view server through an SSH client (like **`putty`**) as a root user.
2. Navigate to the following directory:

   ```
   /usr/local/megha/bin
   ```

3. Run the `setupcommonservice` command to register the Analyzer detail view server with Common Services.

   ```
   setupcommonservice -csUri Common-Services-URL -csUsername Common-Services-user-name -appHostname Analyzer-detail-view-server-host-name-or-IP-address -appPort Analyzer-detail-view-server-port -appName product-name-to-display-in-the-portal -appDescription description-todisplay-in-the-portal
   ```

   Use the `-help` option for command usage information.

   The following is an example to register a new instance of Analyzer detail view server in Common Services:

   ```
   setupcommonservice -csUri https://myopscenter.com:443/portal -csUsername sysadmin -appHostname mydetailview.com -appPort 8443 -appName detailview_B -appDescription "detail view B"
   ```

   Note:

   - The *Common-Services-user-name* must not contain greater than and less than signs (< >), Square brackets ([ ]), spaces, double quotation mark ("), colon (:), or ampersand (&).
   - The *Analyzer-detail-view-server-host-name-or-IP-address* must contain the correct host name or IP address.

4. Enter the password of the Common Services user.

Result

Analyzer detail view server is shown in the Common Services.

> **Note:** To remove a Hitachi Ops Center product registered in Common Services, use the Hitachi Ops Center Portal.

Setting up 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

Assigning Analyzer detail view roles to Ops Center user groups

When you use the Ops Center to perform operations in Analyzer detail view, you must assign Analyzer detail view roles to Ops Center user groups to provide required access.

Before you begin

Make sure that Analyzer detail view is registered with Common Services.

Procedure

1. Log in to the Ops Center portal as a member of the administrator group (for example opscenter-administrators) and then launch Analyzer detail view.

   Note: The user name must not contain greater than and less than signs (< >), square brackets ([ ]), spaces, double quotation mark ("), colon (:), and ampersand (&).

2. In the Analyzer detail view, in the application bar, click the **Manage** menu.
3. In the **Manage** window, in the **Administration** section, click the **Manage Ops Center Groups and Roles** link.
4. In the **Manage Ops Center Groups and Roles** window, select the check boxes to assign the Normal and Admin role to user groups and then click **Save**.

Initial setup of Analyzer probe server

After installing Analyzer probe server, perform the initial setup of Analyzer probe.

To use Common Services and single sign-on through the Ops Center Portal, you must also register Analyzer probe in Common Services and assign Analyzer probe permissions to Ops Center user groups. If you used the stand-alone OVA or installer, you must register with Common Services manually. If you change the host name, IP address, or port number of the server where Common Services is installed, you must register Analyzer probe again.

Note:

Products installed with 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 probe server, complete the following tasks on the Analyzer probe server:

Procedure

1. (Optional) If you want to use Common Services and access Analyzer probe from the Ops Center Portal, run the **`setupcommonservice`** command to register Analyzer probe in Common Services.
2. Perform the initial setup of Analyzer probe.
3. (Optional) If you want to use Common Services, make sure that Analyzer probe permissions have been assigned to the Ops Center user group.

Registering Analyzer probe server with Common Services

If you want to use Common Services installed on a different host, or you installed Analyzer probe server using the stand-alone OVA or installer, you must register Analyzer probe server with Common Services.

Before you begin

Verify the following:

- The host name of Common Services is resolvable from the Analyzer probe server.
- The Analyzer probe server and Common Services are running.
- SSL is configured for the Analyzer probe server and Common Services.
- A user account exists with Common Services that has Administrator permissions.

Procedure

1. Log on to the Analyzer probe server through an SSH client (like **`putty`**) as a root user.
2. Navigate to the following directory:

```
/usr/local/megha/bin
```

3. Run the `setupcommonservice` command to register Analyzer probe server with Common Services.

```
setupcommonservice -csUri Common-Services-URL -csUsername Common-Services-user-name -appHostname Analyzer-probe-server-host-name-or-IP-address -appPort Analyzer-probe-server-port -appName product-name-to-display-in-the-portal -appDescription description-todisplay-in-the-portal
```

   Use the `-help` option for command usage information.

   The following is an example to register a new instance of Analyzer probe server in Common Services:

```
setupcommonservice -csUri https://myopscenter.com:443/portal -csUsername sysadmin -appHostname myprobe.com -appPort 8443 -appName probe_B -appDescription "probe B"
```

   Note:

   - The *Common-Services-user-name* must not contain greater than and less than signs (< >), Square brackets ([ ]), spaces, double quotation mark ("), colon (:), and ampersand (&).
   - The *Analyzer-detail-view-server-host-name-or-IP-address* must contain the correct host name or IP address.

4. Enter the password of the Common Services user.

Result

Analyzer probe server is shown in the Common Services.

Note: To remove a Hitachi Ops Center product registered in Common Services, use the Hitachi Ops Center Portal.

Setting up 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 required 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 490).

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

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

  Note:

  - For the SFTP protocol, you can use key-based or password-based authentication. If you plan to use key-based authentication, make sure that it is configured. The key-based authentication is supported for sending the data directly from the Analyzer probe server to the Analyzer detail view server (without an intermediate FTP or FTPS server) using the meghadata user. Refer to Configuring key-based authentication to transfer data directly from Analyzer probe server to Analyzer detail view server (on page 431). After configuring the key-based authentication, select the SFTP protocol and then select the Key-Based button. If you have provided the passphrase, enter the passphrase.
  - If you are using SFTP and HTTPS protocols: refer to Supported ciphers for Analyzer probe (on page 54).
  - If you are using the HTTPS protocol, make sure that the meghadata user can log on to localhost using SSH and a connection from localhost to port 22 can be established on the Analyzer detail view server.
  - The System Diagnostics data for the Analyzer probe server is not collected in case of HTTPS protocol.

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

  If you are using an intermediate FTP server as a primary server, then you must configure the downloader (on page 148) 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, make sure that:

  - The FTP user must have the required permission to create a new directory in the current working directory on the FTP server.

    If the FTP user does not have the required permission, then you must create the directory manually. Refer to Getting the Appliance UUID and configuring the intermediate FTP server (on page 150).

  - The intermediate FTP server supports the following commands: open, rmdir, delete, disconnect, send, pwd, dir, size, modtime, nlist, put, rename, binary, debug, cd, lcd, passive, put

- **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 108) 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 an intermediate FTP server, make sure you provide the Analyzer detail view server IP address that is processing the data of the primary server. In addition, make sure that you are not connecting the Analyzer probe server to the Analyzer detail view server using a proxy.

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

10. Click **Next**.

    In addition to sending Analyzer probe server data to a single (local) Analyzer detail view server, you can configure a secondary (cloud-based or on-premises) Analyzer detail view server, or intermediate FTP 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 data 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 Enterprise Storage probe
- Hitachi NAS probe
- VMware probe
- Brocade FC Switch (BNA) probe
- Brocade FC Switch probe
- Cisco FC Switch (DCNM) probe
- Cisco FC Switch (CLI) probe
- Linux probe

Viewing Ops Center user groups for Analyzer probe

The Analyzer probe only includes the Admin role. Therefore, all Ops Center user groups are assigned the Admin role by default. You can view the list of Ops Center user groups in the Manage Ops Center Groups and Roles window.

Before you begin

Make sure that Analyzer probe is registered with Common Services.

Procedure

1. Log in to the Ops Center portal as a member of the administrator group (for example opscenter-administrators) and then launch Analyzer probe.

   Note: The user name must not contain contain greater than and less than signs (< >), square brackets ([ ]), spaces, double quotation mark ("), colon (:), and ampersand (&).

2. In the Analyzer probe, in the application bar, click the **Manage** menu.
3. In the **Manage** window, in the **Administration** section, click the **Manage Ops Center Groups and Roles** link.
4. In the **Manage Ops Center Groups and Roles** window, the list of Ops Center groups is displayed.

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 and single sign-on through the Ops Center Portal, 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 used the stand-alone OVA or installer, you must register with Common Services manually. 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 with 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 and access Analyzer from the Ops Center Portal, 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 you installed Analyzer using the stand-alone OVA or installer, you must register Analyzer with Common Services. If you deployed the Ops Center consolidated OVA, Analyzer is already registered in Common Services.

Before you begin

Verify the following:

- The host name of Common Services is resolvable from the Analyzer server.
- The Analyzer server and Common Services are running.
- SSL is configured for the Analyzer server and Common Services.

  For details, see Configuring an SSL certificate (Common Services) (on page 404).
- A user account exists with Common Services that has Administrator permissions.

Procedure

1. Access the following directory:
   `Analyzer-server-installation-destination-directory/Analytics/bin`
2. Run the **`setupcommonservice`** command with the `auto` option specified to register Analyzer in Common Services.

   ```
   setupcommonservice -csUri Common-Services-URL [-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]
   ```

   The `help` option shows command usage information. For details, see setupcommonservice (on page 662).
3. Enter the username and password of the Common Services user according to the message output by the command.

Result

Ops Center Analyzer is shown in the Ops Center Portal.

Note: To remove a Hitachi Ops Center product registered in Common Services, use the Hitachi Ops Center Portal.

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 logon 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 Admin permissions for Ops Center Analyzer.
- Use the following settings for Email Notification and Send Test Mail:
  - Protocol: SMTPS, STARTTLS, cleartext
  - Authentication Methods: LOGIN, PLAIN, DIGEST-MD5

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 this procedure if the current megha or meghadata user password has expired.

If a security policy for the maximum number of login attempts is enabled in your environment, you must disable it before changing the megha and meghadata passwords. After completing the procedure, you can re-enable the setting.

Note: If you do not want to stop the **`crond`** service, you can stop 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 440) and Starting the Analyzer detail view server or Analyzer probe server services (on page 439)

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
```

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.

   Note: Passwords can contain uppercase and lowercase letters, numbers, and the following special characters:

   @, !, ~, #, $, `, %, ^, &, *, (,), -, _, =, +, {, }, <, >, [,], \

8. Start the megha service using the following command:

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

9. Start the crond service using the following 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.

Note: If you do not want to stop the **`crond`** service, you can stop 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 440) and Starting the Analyzer detail view server or Analyzer probe server services (on page 439)

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
```

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
```

> **Note:** Passwords can contain uppercase and lowercase letters, numbers, and the following special characters:
>
> @, !, ~, #, $, `, %, ^, &, *, (,), -, _, =, +, {, }, <, >, [,]

5. Start the megha service using the following command:

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

6. Start the crond service using the following 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*.

Connecting to Ops Center Automator when there is no link to 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 and the host running the browser.

Procedure

1. Log on to the host on which Ops Center Automator is installed as a user with root permission.
2. Display the Ops Center Automator URL by running the **`hcmds64chgurl`** command, and check the host name.

   ```
   Automator-installation-destination-directory/Base64/bin/hcmds64chgurl -list
   ```

3. On the Analyzer server host and the host running the browser, verify that you can resolve Ops Center Automator host name reported by **`hcmds64chgurl`** 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, you are required to complete this procedure before you can 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.

The following procedure sets 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 root permission.
2. Run the **`hcmds64prmset`** 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.

```
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 are 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.

Connecting to Ops Center Automator when linked to 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 and the host running the browser.

Procedure

1. Log on to the host on which Ops Center Automator is installed as a user with root permission.
2. Display the Ops Center Automator URL by running the **`hcmds64chgurl`** command, and check the host name.

   ```
   Automator-installation-destination-directory/Base64/bin/hcmds64chgurl -list
   ```

3. On the Analyzer server host and the host running the browser, verify that you can resolve Ops Center Automator host name reported by **`hcmds64chgurl`** 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, you are required to complete this procedure before you can 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 root permission.
2. Run the **`hcmds64prmset`** 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.

   ```
   Common-component-installation-destination-directory/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 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 **`hcmds64prmset`** 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:

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 116).

Procedure

1. Create a definition file corresponding to the service to run 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:

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

3. Restart the Analyzer server or run 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

`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
`SE.automation.template.serviceGroupName.string`	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
`SE.automation.template.serviceName.string`	Specify the service name used in Ops Center Automator.	The same service name as the one used in Ops Center Automator	N/A	Required
`SE.template.filter.resourceName.string`	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.
`SE.template.filter.resourceType.string`	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.
`SE.template.filter.vmHostname.string`	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.

Key name	Setting description	Specifiable values	Default value	Optional or required
`SE.template.filter.ipaddress.string`	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.
`SE.template.filter.upperResourceName.string`	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.
`SE.template.filter.upperResourceType.string`	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.
`SE.template.filter.MultipleResources.boolean`	To complete 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:

1. Settings display only when the **Execute Action** window is called from a resource that matches the specified conditions.

Key name	Setting description	Specifiable values	Default value	Optional or required
2. 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
`%ANALYTICS_VIRTUALMACHINENAME%`	Name of the virtual host	Displays only when the resource is a virtual machine
`%ANALYTICS_RESOURCETYPE%`	Resource type	N/A
`%ANALYTICS_UPPERRESOURCETYPE%`	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 root permission.
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:

   ```
   Common-component-installation-destination-directory/bin/hcmds64intg -delete -
   type component-name
   ```

   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`

   If you are prompted to enter a username, enter a user ID for the primary server that has the User Management permission.
3. Stop and restart the services:
   a. Run the **hcmds64srv** command with the `stop` option to stop the services.
   b. Run the **hcmds64srv** command with the `start` option to start the services.
4. Log on to the host of the secondary server as a user with root permission.
5. Run the **hcmds64prmset** 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:

   ```
   Automator-installation-destination-directory/Base64/bin/hcmds64prmset -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.

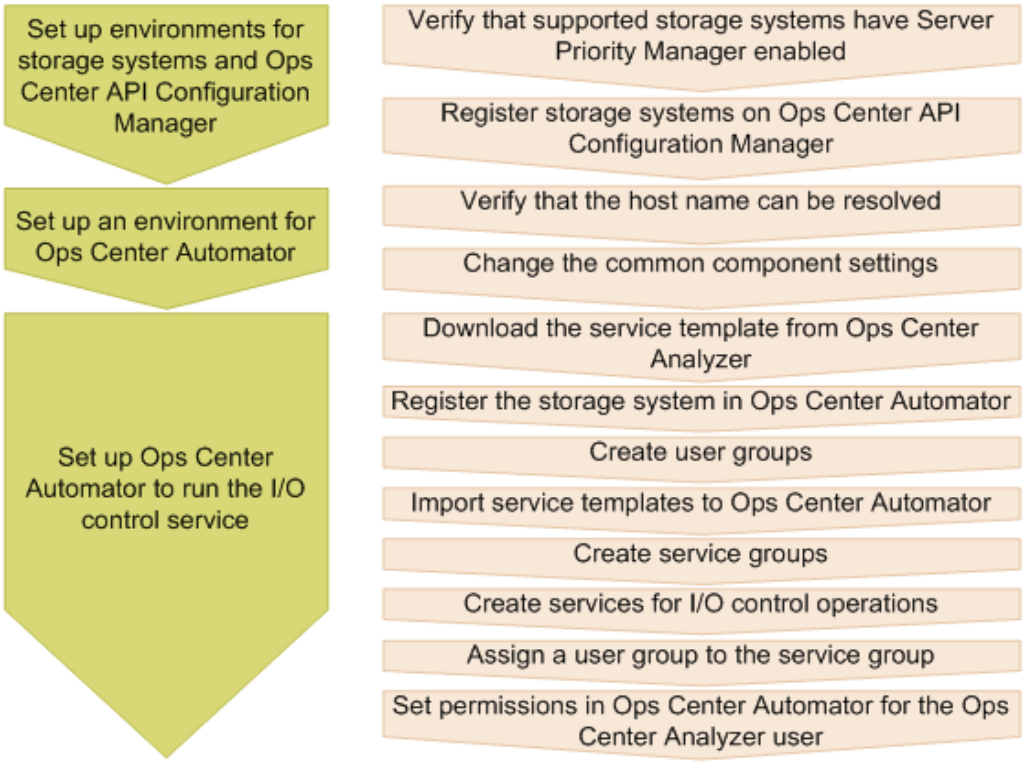
The I/O control feature requires the Server Priority Manager function provided by Hitachi storage systems. To configure Analyzer to work with the Server Priority Manager, use one of the following methods:

- 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.
- You cannot configure I/O controls if volumes use NVMe over Fabrics (NVMe-oF).

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 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 Automation Director version 8.5.1 or later, or Ops Center Automator version earlier than 10.8.0:

        `ServiceTemplate_03.20.00.zip`
      - If you are using Ops Center Automator version 10.8.0 or later:

        `ServiceTemplate_10.00.00.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. From the **Infrastructure Groups** view, click the infrastructure group for which the resource is being assigned. If necessary, you can create a new infrastructure group or edit an existing one.
   b. From the **Service Groups** tab, choose the resource and then click **Assign** to assign to the infrastructure group.
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:

    `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. Running the script is initiated by Ops Center Analyzer after you submit the I/O control task.
5. Check the status of the script 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 run 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 "Content-Type: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 "Content-Type: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 "Content-Type: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 include in 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 "Content-Type: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 "Content-Type: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:

   ```
   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 runs. 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 run 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 running 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":"000000102cceccc9",
"upperLimitForIops":50},
{
"ldevId":102,
"hostWwn":"000000102cceccc0",
"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

You can verify whether the scripts ran successfully. The script 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.

   The name of the script file is displayed as the command action name.

   Note: You can only track the status of the script on the **Events** tab. The status and 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:

- 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 56).

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 run 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 for Granular Data Collection monitoring

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)	The name of instance that you want collect performance information (in seconds) 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.	Optional
Use of a proxy server	Whether to use a proxy server for communication between the Analyzer server and the RAID Agent host. If a proxy server is available, specify one of the following values: ▪ `noproxy`: Specify this if the server and the host communicate directly with each other without using a proxy server. ▪ `proxy`: Specify this if you use a proxy server. If a proxy server is not available, omit this item.	Optional
URL of the proxy server	The URL of the proxy server. If you use a proxy server, you must specify a value for this item.	Optional
Authentication information for the proxy server	Authentication information for the proxy server. If you use a proxy server that requires user authentication, specify the authentication information in the following format: *`user-name:password`*	Optional

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

- VSP F1500
- VSP G1000

Definition file example

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

```
VSP F1500,123456,10.196.1.2
VSP G1000,7890,10.196.1.3,24221,INSTANCE1
```

Configuring initial settings for enabling the Analyzer server audit log

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 `syslog` file.

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: ▪ Starting or shutting down an OS ▪ Starting 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: ▪ Hardware failures ▪ Software failures (memory error, etc.)
`LinkStatus`	Events indicating link status among devices: ▪ Whether a link is up or down
`ExternalService`	Events indicating the results of communication with external services: ▪ Communication with an external server, such as NTP or DNS ▪ Communication with a management server (SNMP)
`Authentication`	Events indicating that a device, administrator, or end user succeeded or failed in connection or authentication: ▪ Fibre Channel login ▪ Device authentication (Fibre Channel - Security Protocol authentication, iSCSI login authentication, SSL server/client authentication) ▪ Administrator or end user authentication
`AccessControl`	Events indicating that a device, administrator, or end user succeeded or failed in gaining access to resources: ▪ Access control for devices ▪ Access control for the administrator or end users

Categories	Description
`ContentAccess`	Events indicating that attempts to access important data succeeded or failed: ▪ Access to important files on NAS or to contents when HTTP is supported ▪ Access to audit log files
`ConfigurationAccess`	Events indicating that the administrator succeeded or failed in performing an allowed operation: ▪ 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`	Events indicating that a performed maintenance operation succeeded or failed: ▪ Addition or deletion of hardware components ▪ Addition or deletion of software components
`AnomalyEvent`	Events indicating that an anomaly, such as a threshold being exceeded, occurred: ▪ 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
	Events indicating that abnormal communication occurred: ▪ 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 root permission.
2. Open the `auditlog.conf` file, which is located in the following location:

   `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`

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

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 `Log.Facility`	Facility defined in the `syslog.conf` file
1	`user`
2	`mail`*
3	`daemon`
4	`auth`*
6	`lpr`*
16	`local0`
17	`local1`
18	`local2`
19	`local3`
20	`local4`
21	`local5`
22	`local6`
23	`local7`
* Although you can specify this value, we do not recommend doing so.	

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`

Severity of audit events	Severity defined in the `syslog.conf` file
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`

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
```

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

`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 `syslog` file.

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

```
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,FQDN,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
uniform-identifier	Fixed to `CELFSS`.
unified-specification-revision-number	Fixed to `1.1`.
serial-number	Serial number of audit log messages.
message-ID	Message ID.
date-and-time	The date and time when the message was output. This item is output in the format of *yyyy*-*mm*-*dd*`T`*hh*`:`*mm*`:`*ss*`.`*stime-zone*.
detected-entity	Component or process name.
detected-location	Host name.
audit-event-type	Event type.
audit-event-result	Event result.
audit-event-result-subject-identification-information	Account ID, process ID, or IP address corresponding to the event.
hardware- identification-information	Hardware model or serial number.
location-information	Identification information for the hardware component.
location-identification-information	Location identification information.
FQDN	Fully qualified domain name.

Item*	Description
redundancy-identification-information	Redundancy identification information.
agent-information	Agent information.
request-source-host	Host name of the request sender.
request-source-port-number	Port number of the request sender.
request-destination-host	Host name of the request destination.
request-destination-port-number	Port number of the request destination.
batch-operation-identifier	Serial number of operations through the program.
log-data-type-information	Fixed to `BasicLog` or `DetailLog`.
application-identification-information	Program identification information.
reserved-area	Not output. This is a reserved space.
message-text	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**.

   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.
3. In the **Secondary** Analyzer detail view **Server** window, specify the following details:
   - **Protocol**: **FTP**, **FTPS**, **SFTP**, or **HTTPS**.
     - For the SFTP protocol, you can use key-based or password-based authentication. If you plan to use key-based, make sure that it is configured. Key-based authentication is supported for sending data directly from the Analyzer probe server to the Analyzer detail view server (without an intermediate FTP or FTPS server) using the meghadata user. Refer to Configuring key-based authentication to transfer data directly from Analyzer probe server to Analyzer detail view server (on page 431). After configuring key-based authentication, select the SFTP protocol and then click Key-Based. If you have configured a passphrase, enter it when prompted.
     - The Analyzer detail view server supports the SFTP and HTTPS protocols. If you are using FTP or FTPS, make sure that the server is configured and you provide the 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 148) 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 108) 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 data to an intermediate FTP server, the Analyzer detail view server needs the FTP server details to download the data.

Note: Do not follow this procedure if you are sending the data directly from the Analyzer probe server to the Analyzer detail view server (without an intermediate FTP server).

Before you begin

Note: If you do not want to stop the **`crond`** service, you can stop 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 440) and Starting the Analyzer detail view server or Analyzer probe server services (on page 439)

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:

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

     For example:

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

     Note: When the Analyzer probe server sends data to an intermediate FTP server, only password-based authentication is suppported (`--authType Password-Based`).

   - If you want to download the data of the specific Analyzer probe server appliance:

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

     For example:

     ```
     sh /usr/local/megha/bin/createOrUpdateFTPConfiguration.sh --create --authType
     Password-Based --ftpServer 192.168.1.2 --ftpMethod SFTP --ftpPort 22 --
     ftpUsername abc --applianceidOption ApplianceIds --applianceidList 1c5fbdd9-
     8ed3-43fe-8973-e9cba6d103c6,39cfcb01-11b2-46b4-8fce-b4d84ea5acda
     ```

     Note:
     - When the Analyzer probe server sends data to an intermediate FTP server, only password-based authentication is suppported (`--authType Password-Based`).
     - Do not use the **`createOrUpdateFTPConfiguration.sh`** command to change the `meghadata` user password. Instead, use the **`changePassword.sh`** command. See Changing the megha and meghadata passwords (on page 108) for more information.

6. Type the FTP user password and confirm it.
7. Start the megha service using the following command:

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

8. Start the crond service using the following command:

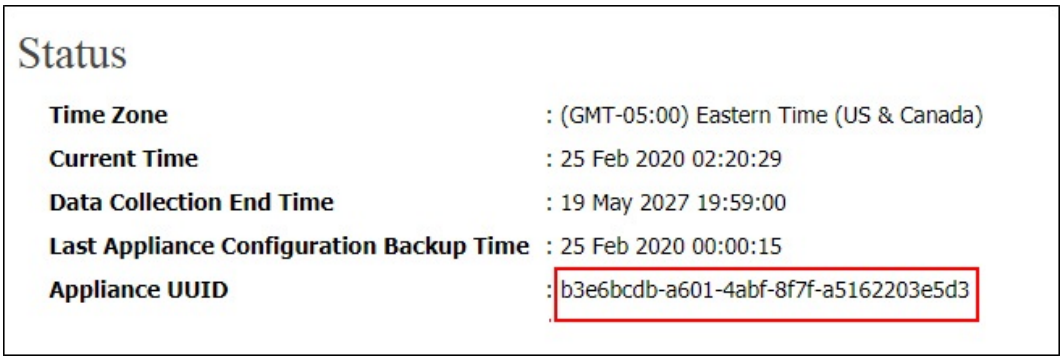
```
service crond start
```

Getting the Appliance UUID and configuring the intermediate FTP server

If the FTP server user does not have sufficient permissions to create the directory automatically, then you must create it manually. The directory name must be the UUID of the Analyzer probe.

Procedure

1. Log on to the Analyzer probe UI.
   The **Status** window opens.
2. Copy the Appliance UUID from the **Status** window as shown in this example.



3. Create the UUID directory on your FTP server.
4. On the Analyzer probe **Status** window, click **Reconfigure**.
   The **Reconfigure Settings** window opens.
5. Click the **Analyzer detail view server** tab.
6. In the **Server Details** section, click the **Edit** corresponding to the primary server.
7. Configure the intermediate FTP server. For more information, refer to “Setting up Analyzer probe server” (from steps 9-12) .

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 storage systems.

Determining the appropriate agent for collecting data

The agent to use depends on your environment. Both agents collect information from storage systems.

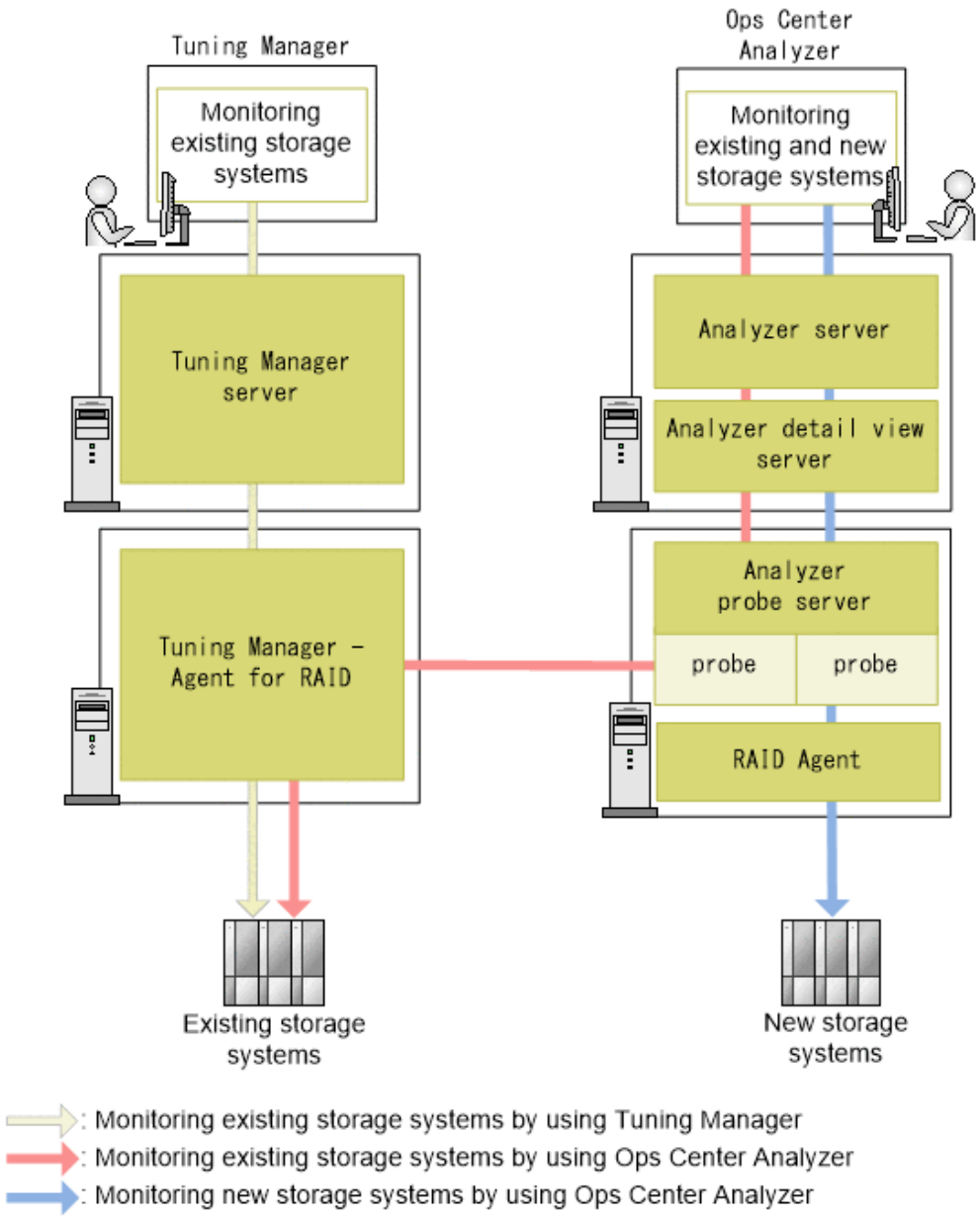
- **RAID Agent:** This agent is installed with Ops Center Analyzer.
- **Tuning Manager - Agent for RAID:** This agent is used in environments where Tuning Manager was previously used to monitor storage system performance.

The following table shows the correspondence between the environment you are using and the agent the Hitachi Enterprise Storage probe uses:

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 153)
Migration from Tuning Manager to Ops Center Analyzer		RAID Agent installed with Ops Center Analyzer	Setting up RAID Agent (on page 153)
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 194)
	Newly installed storage systems to be monitored by Ops Center Analyzer.	RAID Agent installed with Ops Center Analyzer	Setting up RAID Agent (on page 153)

Monitoring environment	Use this Agent	Go to this section
Previous Tuning Manager and Ops Center Analyzer environment now Ops Center Analyzer only	RAID Agent installed with Ops Center Analyzer	Switching from Tuning Manager - Agent for RAID to RAID Agent (on page 204)

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 Manger 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.

If you want to set up Analyzer viewpoint, check which access types can be used by referring to Monitoring target storage systems (on page 562).

Workflow for adding the Hitachi Enterprise Storage probe

To monitor storage systems 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 154).
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 153).
   - 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 194).
   - 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 204).

Setting up RAID Agent

The Hitachi Enterprise Storage probe collects data from the monitored storage systems using RAID Agent, which is bundled with Ops Center Analyzer. RAID Agent temporarily stores the data it collects from the storage system in a database called Hybrid Store, and then provides the data to the Hitachi Enterprise Storage probe.

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`

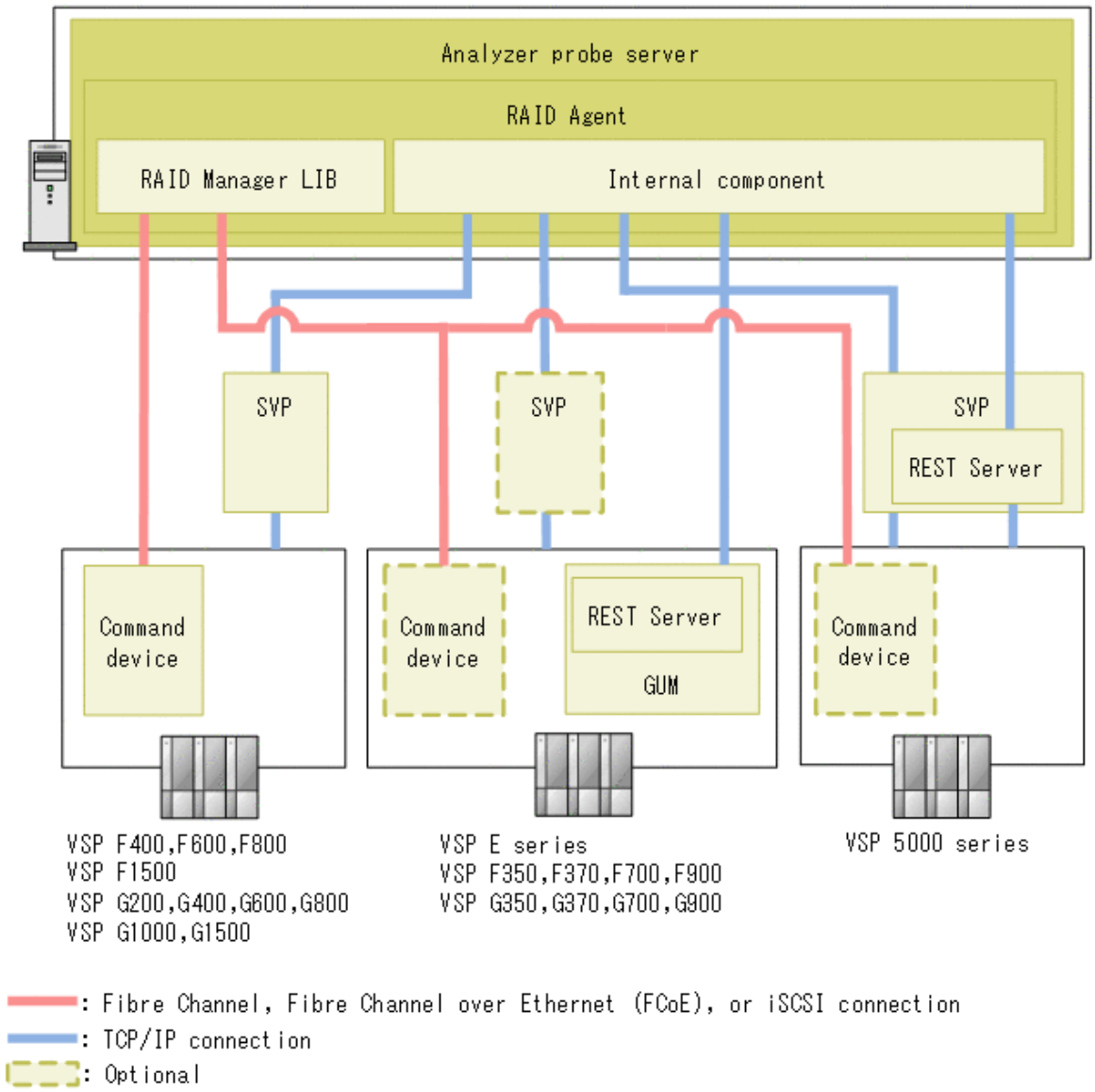
  Data collection using REST API

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`. If you want to set up Analyzer viewpoint, check which access types that you can use by referring to Monitoring target storage systems (on page 562).

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 monitor	Data collection method			Access Type to select
	Command devices	SVP	REST API of the storage system	
VSP F400	Used	Used	--	1

Storage systems to monitor	Data collection method			Access Type to select
	Command devices	SVP	REST API of the storage system	
VSP F600 VSP F800 VSP F1500 VSP G200 VSP G400 VSP G600 VSP G800 VSP G1000 VSP G1500				
VSP E590[2] VSP E790[2] VSP E990 VSP E1090[2] VSP E590H[2] VSP E790H[2] VSP E1090H[2] VSP 5000 series VSP F350[1] VSP F370[1] VSP F700[1] VSP F900[1] VSP G350[1] VSP G370[1] VSP G700[1] VSP G900[1]	Used	Used	--	1
	Used	--	Used	2
	--	Used	Used	3
	--	--	Used	4
Notes:				

Storage systems to monitor	Data collection method			Access Type to select
	Command devices	SVP	REST API of the storage system	

1. The methods for collecting performance data depend on the microcode version:
   - When using the command device and the SVP, microcode version 88-03-22 or later is required.
   - 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 88-03-22 or later is required.
   - When using only the REST API, microcode version 88-02-01 or later is required.
2. You can only select `Access Type` 2 or 4.

Legend:

--: Not used

About selecting the data collection method

Depending on the data collection method, you can collect different types of performance data.

Note:

You can use any `Access Type` to collect storage system performance data and configuration information, the names of pools, and information about the saving capacity and ratio.

If RAID Agent bundled with Ops Center Analyzer will monitor VSP E series, VSP 5000 series, VSP F350, F370, F700, F900, VSP G350, G370, G700, or G900, select the `Access Type` as follows:

Do you use a network that uses Fibre Channel (use a command device)?	Do you use the SVP?	Do you want to monitor the following additional information?	Select this Access Type
Yes	Yes	▪ Virtual IDs for parity groups ▪ Tier information ▪ Current Capacity in License window	`1`
Yes	No	▪ Tier information	`2`

Do you use a network that uses Fibre Channel (use a command device)?	Do you use the SVP?	Do you want to monitor the following additional information?	Select this Access Type
No	Yes	▪ Virtual IDs for parity groups ▪ Current Capacity in License window	`3`
No	No	▪ Current Capacity in License window	`4`

If you use a Fibre Channel network, you can view more detailed information about the storage system. In addition, if you select `Access Type` 1, the storage system is monitored at the same level as the following storage systems:

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*.

To analyze Universal Replicator performance, use `Access Type` 1 for both the primary and secondary storage systems.

If you are using the On-demand real time monitoring module, select either `Access Type` 1 or 2.

If you want to display the volume label, select `Access Type` 1 or 2.

To monitor a VSP 5000 series storage system that uses NVMe-oF, select `Access Type` 1 or 2.

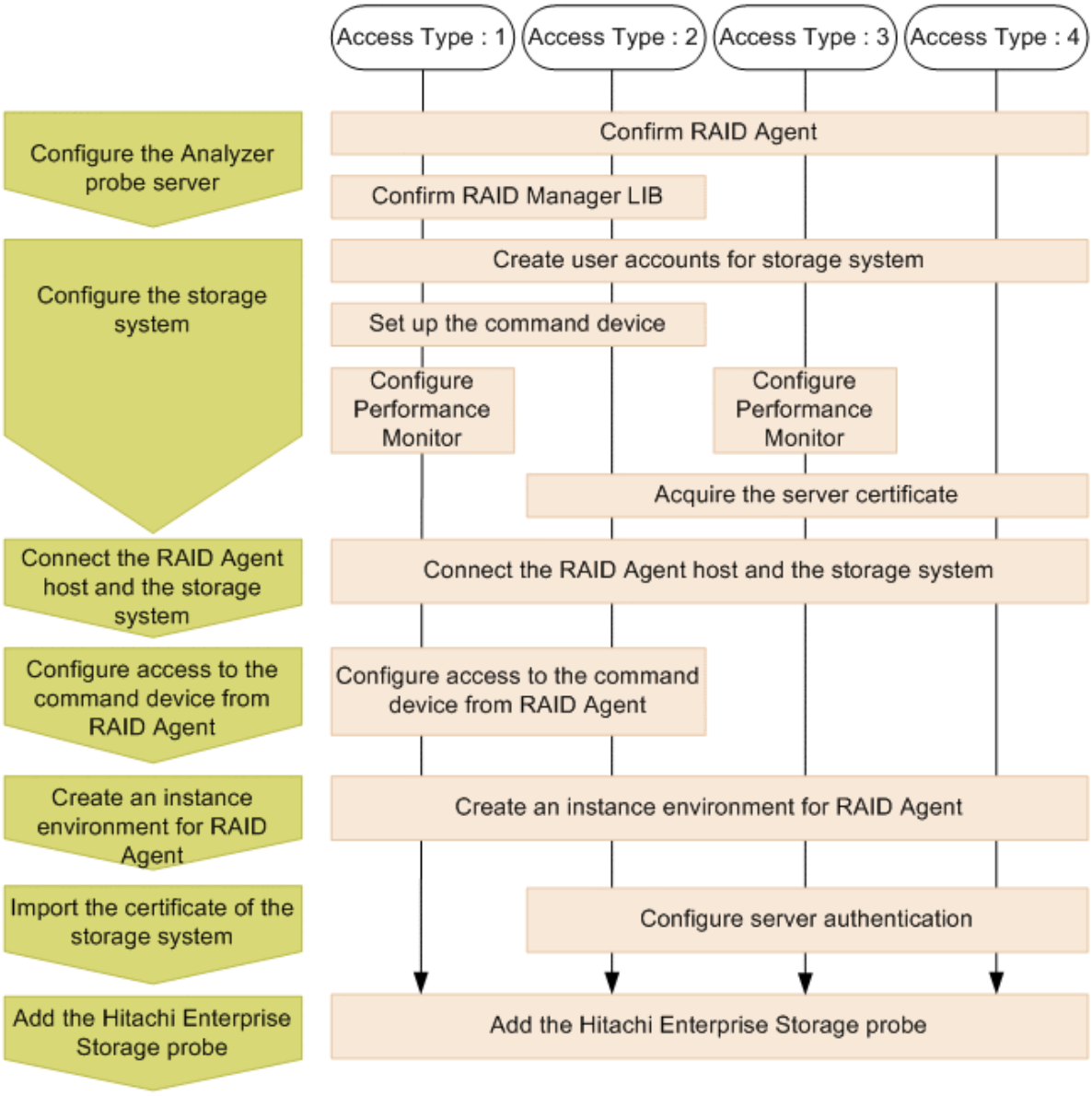
Workflow for setting up the Hitachi Enterprise Storage probe (when using RAID Agent)

To monitor storage systems 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`).

Workflow for setting up the Hitachi Enterprise Storage probe (when using RAID Agent)



Access Type: An item in the instance information for RAID Agent that specifies the combination of methods for collecting performance data:
1: Command device and SVP
2: Command device and REST API
3: SVP and REST API
4: REST API

In the following procedures, only the settings required for each access type are described.

When `Access Type` is `1`: Configuring RAID Agent for data collection using command devices and SVP (on page 161)

When `Access Type` is `2`: Configuring RAID Agent for data collection using command device and REST API (on page 170)

When `Access Type` is `3`: Configuring RAID Agent for data collection using SVP and REST API (on page 179)

When `Access Type` is `4`: Configuring RAID Agent for data collection using REST API (on page 188)

Migrating setting information from Tuning Manager - Agent for RAID to RAID Agent

If you are migrating 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 204).

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 475).
     - 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

  To collect performance data by using a TCP/IP connection, you need to use Storage Navigator to create a user account. Create the user account as a dedicated RAID Agent account. One user account is required for each instance. Assign one of the following roles to the user account:

  - 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 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 available values, see the 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.
Monitoring-target WWNs	Set the performance data collection-target WWNs.
Sampling interval	Set the interval at which Performance Monitor collects performance data. The granularity set here becomes the granularity of data that can be collected by RAID Agent.

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

Notes on collecting performance data by using the SVP

- If you power off a storage system during the monitoring period, the performance data during the power-off period is not collected in the SVP. In addition, the values of the performance data immediately after you again power on the storage system might be extremely large.
- If the load for the input from and output to the host becomes high on a storage system, some of the performance data might go missing, because the storage system prioritizes input/output processing over monitoring processing. If performance data frequently goes missing, specify a larger value for Sample Interval in the Edit Monitoring Switch window. For details, see the documentation about Performance Monitor of each storage system.
- Do not change the SVP time setting. If you do so, the following problems might occur:
  - Invalid performance data is collected in the SVP
  - The SVP cannot collect performance data

  If you changed the SVP time setting, disable the setting of Monitoring Switch, and then enable it again. After doing so, collect the performance data again. For details about the monitoring switch settings, see the documentation about Performance Monitor of each storage system.

- For the SVP on which SVP High Availability Feature is installed, if you switch from the master SVP to the standby SVP, the “short range” performance data will be deleted.
- Some functions cannot be run while performance data is being collected. If you run these functions while performance data is collected using the SVP of RAID Agent, either the data collection or 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 collected:

  - Data migration in Device Manager
  - Displaying the following Storage Navigator windows:
    - Server Priority Manager window
    - Volume Migration window
  - Using the export tools described in the Performance Monitor manuals
- If "SVP regular reboots" or "SVP recovery reboots" is enabled, performance data is not collected while the SVP is restarting.

Notes on Data in Place upgrades or downgrades

When planning a Data in Place upgrade or downgrade, note the following:

- During an upgrade or downgrade, you cannot collect data from the storage system by using a command device in in-band mode while operations are running on the controller belonging to the port connected to the command device. If you want to continue collecting data, complete one of the following before running operations on the controller:
  - If you are not using Analyzer viewpoint, change the value of `Access Type` in the instance settings of RAID Agent to `3` or `4`.
  - Reconfigure the RAID Agent instance to assign a command device that is connected to the server where the RAID Agent is installed by using the port of a different controller.
- During an upgrade or downgrade, some data points might be missing.

Configuring access to the command device from RAID Agent

If you plan to collect performance data by using a command device, make sure that the command device of the monitored storage system can be accessed from the host where 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 where 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 the 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 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 is necessary if RAID Agent is installed on a guest OS of VMware ESXi. For details, see the VMware ESXi documentation.

   Use the VMware vSphere Client to add a device to the guest OS. By doing so, if you designate a command device as the device to add, 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 where RAID Agent is installed.

   Run the **`jpctdlistraid`** command on the host where RAID Agent is installed, and confirm that the information you set on the command device is output:

   ```
   /opt/jp1pc/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/jp1pc/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`.

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/jp1pc/tools/jpcinssetup agtd -inst 35053
```

2. Set up the instance information for the storage system to 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: ▪ `12`: VSP G1000, G1500, VSP F1500 ▪ `13`: VSP 5000 series

Item	Description
	▪ `22`: VSP G200, G400, G600, G800, VSP F400, F600, F800 ▪ `23`: VSP E990 or VSP G/F350, G/F370, G/F700, G/F900
Serial No	Specify the serial number of the storage system.
Access Type	Specify `1`. If a value other than `13` and `23` is specified for `Storage model`, `1` is automatically specified.
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 `/opt/jp1pc/tools/jpctdlistraid` command. RAID Agent uses this command device to collect information about the storage system. The `/dev/sd*` 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. For details, see Configuring access to the command device from RAID Agent (on page 164) .
Unassigned Open Volume Monitoring[1]	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. ▪ 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.
Mainframe Volume Monitoring[1]	Specify `Y` to monitor a logical device for which the emulation type used for a mainframe is set. ▪ 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
	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.
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 `Serial No`.
Storage User ID for SVP	Specify the user ID of the user account that accesses the target storage system using the SVP.
Storage Password for SVP	Specify the password of the user account that accesses the target storage system using the SVP.
SVP Port No	Specify the port number if `Storage model` is set to `22` or `23`. You can specify a value from `0` to `65535`. The default value is `1099`. This value is the same as the initial value for the `RMIIFRegist` 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	If `22` or `23` is specified for `Storage model`, 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`. This value is the same as the initial value for the `MAPPWebServerHttps` 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.
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`.

Item	Description
	However, in a large-scale environment that exceeds an assumed value[2], if you specify `1`, processing might end abnormally because of insufficient memory. For this reason, for a large-scale environment, specify `2`. ▪ 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 create on the target storage system. The required memory size for the Java VM is 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 SVP	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`. ▪ `1`: 0.5 GB ▪ `2`: 1.0 GB ▪ `3`: 2.0 GB ▪ `4`: 4.0 GB ▪ `5`: 8.0 GB
Notes: 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). 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: ▪ Number of LU paths: `0` ▪ Sampling interval (in minutes): `1`	

3. When configuring multiple instances, repeat steps 1 and 2 for each instance.

4. To monitor a storage system by using a command device, RAID Manager LIB is required. 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/jp1pc/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, and VSP F350, F370, F700, F900 storage systems are reported as, `VSP G200 G400 G600 G800 F400 F600 F800` by the **`jpctdchkinst`** command.

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 478). 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/jp1pc/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.

Next steps

Adding Hitachi Enterprise Storage probe (on page 209)

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 by using both the command device and REST API. 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 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
  - VSP 5000 series storage systems: TCP/IP connection with the SVP
  - All other storage systems: TCP/IP connection with the GUM (CTL)
- Fibre Channel, Fibre Channel over Ethernet (FCoE), or iSCSI connection for the command device

Notes on Data in Place upgrades or downgrades

When planning a Data in Place upgrade or downgrade, note the following:

- During an upgrade or downgrade, you cannot collect data from the storage system by using a command device in in-band mode while operations are running on the controller belonging to the port connected to the command device. If you want to continue collecting data, complete one of the following before running operations on the controller:
  - If you are not using Analyzer viewpoint, change the value of `Access Type` in the instance settings of RAID Agent to `3` or `4`.
  - Reconfigure the RAID Agent instance to assign a command device that is connected to the server where the RAID Agent is installed by using the port of a different controller.
- During an upgrade or downgrade, some data points might be missing.

Configuring access to the command device from RAID Agent

If you plan to collect performance data by using a command device, make sure that the command device of the monitored storage system can be accessed from the host where 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 where 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 the 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 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 is necessary if RAID Agent is installed on a guest OS of VMware ESXi. For details, see the VMware ESXi documentation.

Use the VMware vSphere Client to add a device to the guest OS. By doing so, if you designate a command device as the device to add, 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 where RAID Agent is installed.

   Run the **`jpctdlistraid`** command on the host where RAID Agent is installed, and confirm that the information you set on the command device is output:

```
/opt/jp1pc/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/jp1pc/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`.

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/jp1pc/tools/jpcinssetup agtd -inst 35053
```

2. Set up the instance information for the storage system to 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: ▪ `13`: VSP 5000 series ▪ `23`: VSP E590, E790, E990, E1090, E590H, E790H, E1090H, or VSP G/F350, G/F370, G/F700, G/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 `/opt/jp1pc/tools/jpctdlistraid` command. RAID Agent uses this command device to collect information about the storage system. The `/dev/sd*` 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. For details, see Configuring access to the command device from RAID Agent (on page 164) .
Unassigned Open Volume Monitoring[1]	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. ▪ 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]	Specify `Y` to monitor a logical device for which the emulation type used for a mainframe is set. ▪ 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. 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.
SVP IP Address or Host Name	If `13` is specified for `Storage model`, specify the IP address or host name of the SVP that manages the storage system that was specified for `Serial No`.
GUM(CTL) IP Address or Host Name (Primary)	If `23` is specified for `Storage model`, 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 `Serial No`. The default value is blank. Connections with the connection destination set for `GUM(CTL) IP Address or Host Name (Primary)` are prioritized. 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)`.
GUM(CTL) IP Address or Host Name (Secondary)	
Storage User ID for REST-API	Specify the user ID of the user account that accesses the target storage system using the REST API.
Storage Password for REST-API	Specify the password of the user account that accesses 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 `2`. Specify `2` (that is, leave the default value as is). ▪ To use HTTP: `1` ▪ To use HTTPS: `2`

Item	Description
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`, processing might end abnormally because of insufficient memory. For this reason, for a large-scale environment, specify `2`. ▪ 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 create on the target storage system. The required memory size for the Java VM is 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 memory size for the Java VM. The default value is `1`. ▪ `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

Notes:

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).

Item	Description
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: ▪ 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. To monitor a storage system by using a command device, RAID Manager LIB is required. 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/jp1pc/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 478). 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/jp1pc/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 server certificate in RAID Agent, import the storage system 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 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 server certificate to the root certificate authority, must be connected in a chain of trust.
- If the storage system certificate already exists in the truststore, delete the existing certificate before importing new certificate. To delete the existing certificate, run the following command:

```
rm /opt/jp1pc/agtd/agent/instance-name/jssecacerts
```

Procedure

1. Run the following command to import the storage system certificate to the truststore:

```
/opt/jp1pc/htnm/HBasePSB/jdk/bin/keytool -import -alias alias-name -file
certificate-file-name -keystore truststore-file-name -storepass access-password-
for-truststore -storetype JKS
```

   - For *alias-name*, specify a name that makes it possible to determine which storage system will use the server certificate.
   - 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/jp1pc/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/jp1pc/agtd/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.
   - To check the name of the host of an SSL certificate for a VSP 5000 series storage system, specify a host name that can be resolved for `SVP IP Address or Host Name` in the RAID Agent instance information.
   - If the web server certificate is not a wildcard certificate, specify `false`, because the host name cannot be verified.
3. Run the command **`jpctdchkinst`** to confirm the instance settings:

```
/opt/jp1pc/tools/jpctdchkinst -inst instance-name
```

4. Run the following commands to restart the services of the RAID Agent instance:

```
/opt/jp1pc/htnm/bin/htmsrv stop -all
```

```
/opt/jp1pc/htnm/bin/htmsrv start -all
```

Next steps

Adding Hitachi Enterprise Storage probe (on page 209)

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

  To collect performance data by using a TCP/IP connection, you need to use Storage Navigator to create a user account. Create the user account as a dedicated RAID Agent account. One user account is required for each instance. Assign one of the following roles to the user account:

  - 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 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 available values, see the 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.
Monitoring-target WWNs	Set the performance data collection-target WWNs.
Sampling interval	Set the interval at which Performance Monitor collects performance data. The granularity set here becomes the granularity of data that can be collected by RAID Agent.

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:

- VSP 5000 series storage systems: TCP/IP connection with the SVP
- All other storage systems: TCP/IP connection with the GUM (CTL)

Notes on collecting performance data by using the SVP

- If you power off a storage system during the monitoring period, the performance data during the power-off period is not collected in the SVP. In addition, the values of the performance data immediately after you again power on the storage system might be extremely large.
- If the load for the input from and output to the host becomes high on a storage system, some of the performance data might go missing, because the storage system prioritizes input/output processing over monitoring processing. If performance data frequently goes missing, specify a larger value for Sample Interval in the Edit Monitoring Switch window. For details, see the documentation about Performance Monitor of each storage system.
- Do not change the SVP time setting. If you do so, the following problems might occur:
  - Invalid performance data is collected in the SVP
  - The SVP cannot collect performance data

  If you changed the SVP time setting, disable the setting of Monitoring Switch, and then enable it again. After doing so, collect the performance data again. For details about the monitoring switch settings, see the documentation about Performance Monitor of each storage system.

- For the SVP on which SVP High Availability Feature is installed, if you switch from the master SVP to the standby SVP, the “short range” performance data will be deleted.
- Some functions cannot be run while performance data is being collected. If you run these functions while performance data is collected using the SVP of RAID Agent, either the data collection or 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 collected:

  - Data migration in Device Manager
  - Displaying the following Storage Navigator windows:
    - Server Priority Manager window
    - Volume Migration window
  - Using the export tools described in the Performance Monitor manuals
- If "SVP regular reboots" or "SVP recovery reboots" is enabled, performance data is not collected while the SVP is restarting.

Notes on Data in Place upgrades or downgrades

When planning a Data in Place upgrade or downgrade, note the following:

- During an upgrade or downgrade, the model name after the upgrade or downgrade might be displayed as that of the target storage system.
- During an upgrade or downgrade, some data points might be missing.

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/jp1pc/tools/jpcinssetup agtd -inst 35053
   ```

2. Set up the instance information for the storage system to 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: ▪ `13`: VSP 5000 series ▪ `23`: VSP E990 or VSP G/F350, G/F370, G/F700, G/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 `Serial No`.
Storage User ID for SVP	Specify the user ID of the user account that accesses the target storage system using the SVP.
Storage Password for SVP	Specify the password of the user account that accesses the target storage system using the SVP.
SVP Port No	Specify the port number if `Storage model` is set to `22` or `23`. You can specify a value from `0` to `65535`. The default value is `1099`. This value is the same as the initial value for the `RMIIFRegist` 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	If `22` or `23` is specified for `Storage model`, 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`. This value is the same as the initial value for the `MAPPWebServerHttps` 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.

Item	Description
GUM(CTL) IP Address or Host Name (Primary)	If `23` is specified for `Storage model`, 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 `Serial No`. The default value is blank. Connections with the connection destination set for `GUM(CTL) IP Address or Host Name (Primary)` are prioritized. 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)`.
GUM(CTL) IP Address or Host Name (Secondary)	
Storage User ID for REST-API	Specify the user ID of the user account that accesses the target storage system using the REST API.
Storage Password for REST-API	Specify the password of the user account that accesses 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 `2`. Specify `2` (that is, leave the default value as is). ▪ 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*, if you specify `1`, processing might end abnormally because of insufficient memory. For this reason, for a large-scale environment, specify `2`. ▪ 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`

Item	Description
Maximum number of Volumes	If you specified `1` for `Java VM Heap Memory setting Method`, specify the maximum number of volumes to create on the target storage system. The required memory size for the Java VM is 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 SVP	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`. ▪ `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	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`. ▪ `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
* The following values are assumed for the environment when the required memory size is calculated based on the maximum number of volumes. ▪ **If data is collected by using the REST API:** ▪ 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:** ▪ 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/jp1pc/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 478). 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/jp1pc/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 server certificate in RAID Agent, import the storage system 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 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 server certificate to the root certificate authority, must be connected in a chain of trust.
- If the storage system certificate already exists in the truststore, delete the existing certificate before importing new certificate. To delete the existing certificate, run the following command:

```
rm /opt/jp1pc/agtd/agent/instance-name/jssecacerts
```

Procedure

1. Run the following command to import the storage system certificate to the truststore:

```
/opt/jp1pc/htnm/HBasePSB/jdk/bin/keytool -import -alias alias-name -file
certificate-file-name -keystore truststore-file-name -storepass access-password-
for-truststore -storetype JKS
```

   - For *alias-name*, specify a name that makes it possible to determine which storage system will use the server certificate.
   - 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/jp1pc/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/jp1pc/agtd/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.
   - To check the name of the host of an SSL certificate for a VSP 5000 series storage system, specify a host name that can be resolved for `SVP IP Address or Host Name` in the RAID Agent instance information.
   - If the web server certificate is not a wildcard certificate, specify `false`, because the host name cannot be verified.
3. Run the command **`jpctdchkinst`** to confirm the instance settings:

```
/opt/jp1pc/tools/jpctdchkinst -inst instance-name
```

4. Run the following commands to restart the services of the RAID Agent instance:

```
/opt/jp1pc/htnm/bin/htmsrv stop -all
```

```
/opt/jp1pc/htnm/bin/htmsrv start -all
```

Next steps

Adding Hitachi Enterprise Storage probe (on page 209)

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 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 methods:

- VSP 5000 series storage systems: TCP/IP connection with the SVP
- All other storage systems: TCP/IP connection with the GUM (CTL)

Notes on Data in Place upgrades or downgrades

When planning a Data in Place upgrade or downgrade, note the following:

- During an upgrade or downgrade, the model name after the upgrade or downgrade might be displayed as that of the target storage system.
- During an upgrade or downgrade, some data points might be missing.

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/jp1pc/tools/jpcinssetup agtd -inst 35053
   ```

2. Set up the instance information for the storage system to 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: ▪ `13`: VSP 5000 series ▪ `23`: VSP E590, E790, E990, E1090, E590H, E790H, E1090H, or VSP G/F350, G/F370, G/F700, G/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 `Storage model`, specify the IP address or host name of the SVP that manages the storage system that was specified for `Serial No`.
GUM(CTL) IP Address or Host Name (Primary)	If `23` is specified for `Storage model`, 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 `Serial No`. The default value is blank. Connections with the connection destination set for `GUM(CTL) IP Address or Host Name (Primary)` are prioritized. 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)`.
GUM(CTL) IP Address or Host Name (Secondary)	
Storage User ID for REST-API	Specify the user ID of the user account that accesses the target storage system using the REST API.

Item	Description
Storage Password for REST-API	Specify the password of the user account that accesses 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 `2`. Specify `2` (that is, leave the default value as is). ▪ 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*, if you specify `1`, processing might end abnormally because of insufficient memory. For this reason, for a large-scale environment, specify `2`. ▪ 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 create on the target storage system. The required memory size for the Java VM is 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 memory size for the Java VM. The default value is `1`. ▪ `1`: 128 MB ▪ `2`: 256 MB ▪ `3`: 512 MB ▪ `4`: 1.0 GB ▪ `5`: 2.0 GB

Item	Description
	▪ 6: 4.0 GB ▪ 7: 8.0 GB
* 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: ▪ 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/jp1pc/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 478). 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/jp1pc/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 server certificate in RAID Agent, import the storage system 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 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 server certificate to the root certificate authority, must be connected in a chain of trust.
- If the storage system certificate already exists in the truststore, delete the existing certificate before importing new certificate. To delete the existing certificate, run the following command:

```
rm /opt/jp1pc/agtd/agent/instance-name/jssecacerts
```

Procedure

1. Run the following command to import the storage system certificate to the truststore:

```
/opt/jp1pc/htnm/HBasePSB/jdk/bin/keytool -import -alias alias-name -file
certificate-file-name -keystore truststore-file-name -storepass access-password-
for-truststore -storetype JKS
```

   - For *alias-name*, specify a name that makes it possible to determine which storage system will use the server certificate.
   - 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/jp1pc/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/jp1pc/agtd/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.
   - To check the name of the host of an SSL certificate for a VSP 5000 series storage system, specify a host name that can be resolved for `SVP IP Address or Host Name` in the RAID Agent instance information.
   - If the web server certificate is not a wildcard certificate, specify `false`, because the host name cannot be verified.
3. Run the command **`jpctdchkinst`** to confirm the instance settings:

```
/opt/jp1pc/tools/jpctdchkinst -inst instance-name
```

4. Run the following commands to restart the services of the RAID Agent instance:

```
/opt/jp1pc/htnm/bin/htmsrv stop -all
```

```
/opt/jp1pc/htnm/bin/htmsrv start -all
```

Next steps

Adding Hitachi Enterprise Storage probe (on page 209)

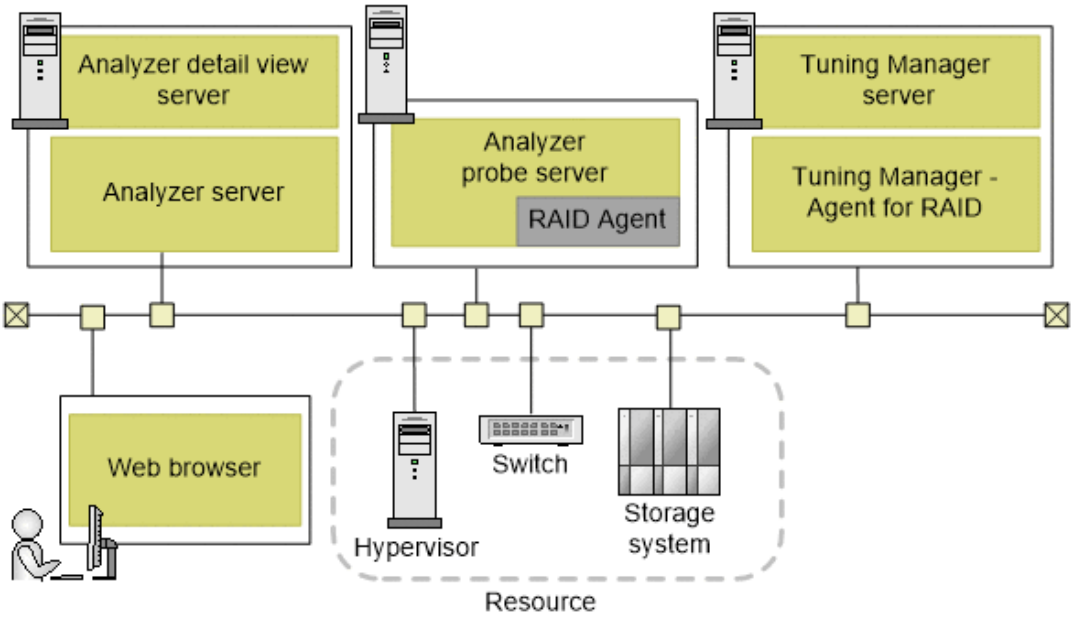
Setting up Tuning Manager - Agent for RAID

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 storage systems.

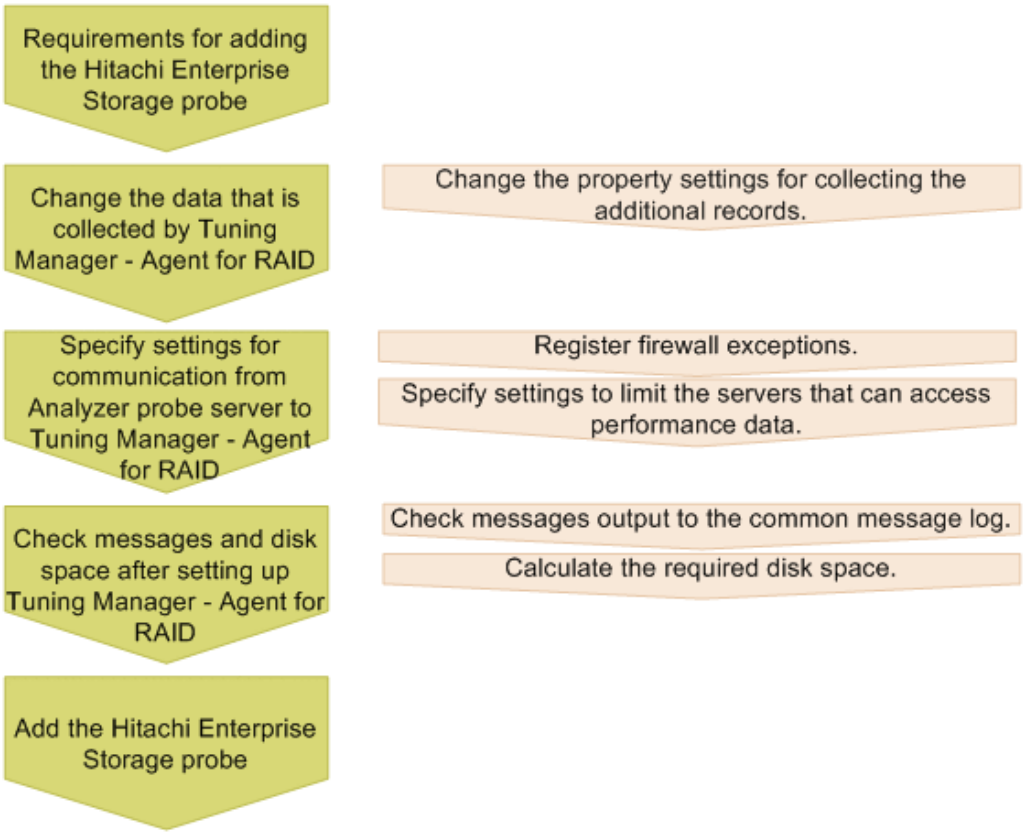
Requirements for adding the Hitachi Enterprise Storage probe (when using Tuning Manager - Agent for RAID)

To use Tuning Manager - Agent for RAID to monitor storage systems, you must complete the following steps 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.
- You use the latest version of Tuning Manager - Agent for RAID.
- 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_NHC
- PD_NNC
- PD_NNPC
- PD_NSPC
- PD_NSSC
- PD_PWPC
- PD_RGD
- PD_RPHC
- PI_CTGS
- PI_JNLS

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** or **Interval 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 the latest 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
- The default record collection interval may differ between Tuning Manager - Agent for RAID and the Hitachi Enterprise Storage probe, so you should adjust to either one.

  If you change the collection interval of the Hitachi Enterprise Storage probe instead of Tuning Manager - Agent for RAID, refer to Changing the data collection intervals of Analyzer detail view performance metrics (on page 474).
- Ops Center Analyzer detail view supports filtering storage ports based on the `Speed` attribute for adding an alert definition. Analyzer detail view uses the `negotiatedPortSpeed` metric for the port speed value. If you are using Tuning Manager - Agent for RAID, the port speed is not available.

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_NHC	Number of NVMe-oF host NQNs
PD_NNC	Number of NVMe-oF namespaces
PD_NNPC	Number of NVMe-oF host-namespace paths
PD_NSPC	Number of NVM subsystem ports
PD_NSSC	Number of NVM subsystems
PD_PWPC	Total number of settings related to ports and the WWNs of host bus adapters*
PD_RGD	Number of parity groups
PD_RPHC	Number of remote paths belonging to path groups for which the storage system at the other end of the path is registered as RCU
PI_CTGS	Number of consistency 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	92	327	--	--
PD_LDD	76	266	--	--
PD_LHGC	68	272	--	--
PD_LWPC	64	619	--	--
PD_MPBC	52	114	--	--
PD_NHC	59	619	--	--
PD_NNC	60	139	--	--
PD_NNPC	65	653	--	--
PD_NSPC	54	203	--	--
PD_NSSC	65	394	--	--
PD_PWPC	80	363	--	--
PD_RGD	80	296	--	--
PD_RPHC	72	456	--	--
PI_CTGS	56	54	50	68

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

Record ID	Retention period (unit: hours)
PD_MPBC	168
PD_NHC	168
PD_NNC	168
PD_NNPC	168
PD_NSPC	168
PD_NSSC	168
PD_PWPC	168
PD_RGD	168
PD_RPHC	168
PI_CTGS	48

Migrating Hitachi Tuning Manager historical data

The Tuning Manager data migration feature copies storage system historical data from Tuning Manager to the Analyzer detail view database. You can obtain the migrated data 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.

The migration data flow for Tuning Manager - Agent for RAID is as follows:

1. The Analyzer probe server connects to Tuning Manager to identify the Tuning Manager - Agent for RAID associated with it.
2. The Analyzer probe server connects to the Tuning Manager - Agent for RAID 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.

To perform this data migration, use the procedures described in the sections that follow.

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.
- Use the latest version of Tuning Manager - Agent for RAID.
- Tuning Manager host settings are accessible 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 for 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:** Host name or 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 Tuning Manager - Agent for RAID instances 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 all frequencies except Minute.
- 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 487).

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 154).)

b. Set up RAID Agent. (For details, see Workflow for setting up the Hitachi Enterprise Storage probe (when using RAID Agent) (on page 158) 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 475).

Note: Collection intervals for Tuning Manager - Agent for RAID are set for each instance. Collection intervals for RAID Agent are set for each host on which RAID Agent is installed. For this reason, it might not be possible to set the same collection intervals.

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 488).

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 487).

Chapter 7: Configuring Virtual Storage Software Agent to monitor Virtual Storage Software Block

Before adding the Hitachi VSS Block Storage probe, configure Virtual Storage Software Agent to monitor Virtual Storage Software Block.

Setting up Virtual Storage Software Agent

Set up Virtual Storage Software Agent as follows:

Before you begin

- If you want to use the web server access control function of Virtual Storage Software Block, you must set the IP addresses of access sources in advance. For details, see the description of how to configure web server access for a storage system.
- When you create Virtual Storage Software Block instances, you need to specify a user who has a storage role or a monitor role.

Procedure

1. Log on as root on the host where Virtual Storage Software Agent is installed.
2. Open the Virtual Storage Software Agent client configuration file:

   `/var/`*`Virtual-Storage-Software-Agent-installation-destination-directory`*`/VirtualStorageSoftwareAgent/config/userconfig-setting.yaml`

3. Change the settings in the file as needed.
   - `protocol`: Protocol of Virtual Storage Software Agent. Specify `http` or `https`.
   - `port`: Port number of Virtual Storage Software Agent. Specify a value from `1` to `65535`.
   - `verifyingSsl`: Whether to verify Virtual Storage Software Block the server certificate. Specify `true` or `false`.

   The following is an example:

```
serverSettings:
  protocol: http
  port: 24080

virtualStorageSoftwareAccessSettings:
  verifyingSsl: false
```

4. Create or update each instance by running the following command:

```
Virtual-Storage-Software-Agent-installation-destination-directory/
VirtualStorageSoftwareAgent/bin/instancesetup [--name instance-name] [--host
host-name-or-IP-address] [--port port-number] [--user username] [--update] [--
skipVerifyConnection]
```

   - `name`: Virtual Storage Software Block instance name. Only alphanumeric characters (A-Z, a-z, 0-9) are allowed.
   - `host`: Host name or IP address of Virtual Storage Software Block. If you want to specify a host name, make sure it can be resolved on the host where Virtual Storage Software Agent is installed. If you specify the IP address, you must use IPv4.
   - `port`: Port number of Virtual Storage Software Block. The default port number is `443`.
   - `user`: User name for connecting to Virtual Storage Software Block.
   - `update`: Specifies to update an existing instance.
   - `skipVerifyConnection`: Specifies to skip verification of the connection with Virtual Storage Software Block.

   Note: If you want to connect with multiple instances of Virtual Storage Software Block, create as many instances as you need. (One instance of Virtual Storage Software Agent can monitor up to 10 instances of Virtual Storage Software Block.)

5. If necessary, you can delete instance by running the following command:

```
Virtual-Storage-Software-Agent-installation-destination-directory/
VirtualStorageSoftwareAgent/bin/instanceunsetup [--name instance-name]
```

6. Restart the Virtual Storage Software Agent services by running the following command:

```
systemctl restart virtualstoragesoftware-agent.service
```

Chapter 8: 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: VSP E series, VSP F series, VSP G series, VSP 5000 series. 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 maximum100 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.

  Note: If you are using the Analyzer REST API functions that access RAID Agent, then make sure that the RAID Agent IP address (provided in this field) is accessible from the Analyzer server.

- **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 numbers are:

  `24221-HTTP`

  `24222-HTTPS`

- **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, the data collection interval are displayed for each record type. This data collection interval is set in Hitachi Enterprise Storage probe for data collection. Click **Next**.

   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 211).
- 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 213).

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: VSP E series, 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.)

  Note: In the case of VSP E590, VSP E790, VSP E1090, VSP E590H, VSP E790H, and VSP E1090H storage systems, the Hitachi Enterprise Storage probe supports data collection for the storage systems with in-band and out-of-band (both) communication modes.
- `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, VSP E990.

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.

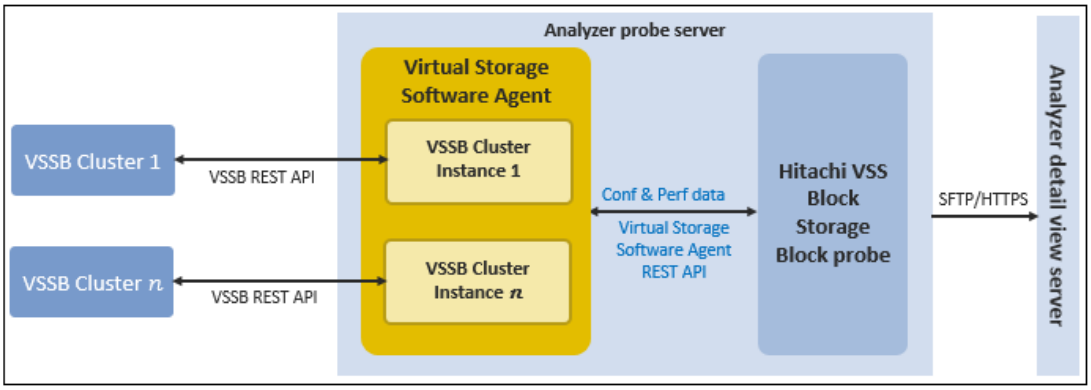
Procedure

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 211).
   - 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 213)

Adding Hitachi VSS Block Storage probe

The Hitachi VSS Block Storage probe collects data from Virtual Storage Software Block (VSSB) systems. The Hitachi VSS Block Storage probe uses the Virtual Storage Software Agent to collect data. The probe connects to the Virtual Storage Software Agent using the Virtual Storage Software Agent REST API and the Virtual Storage Software Agent connects to the VSSB Cluster to collect data using the VSSB REST API.



Note: The Virtual Storage Software Agent can be installed on the Analyzer probe machine or any other machine.

Before you begin

- Make sure that the Virtual Storage Software Agent is installed and the VSSB cluster instances are added to the Virtual Storage Software Agent.

Procedure

1. On the Analyzer probe home page, click **Add Probe**.
2. In the **Add Probe** window, from the **Probes** menu, select **Hitachi VSS Block Storage**.
3. In the **Hitachi Virtual Storage Software Block Probe** window, type the following details, and then click **Next**:
   - **Probe Name**: The probe name must be unique and must consist of 4-100 alphanumeric characters, with no special characters other than hyphen and underscore.
   - **Connection Type**: HTTPS (Only HTTPS connection is supported).

- **VSS Agent IP Address or FQDN**: IP address or FQDN of the machine where the Virtual Storage Software Agent is installed.
- **VSS Agent Port**: Port number used by the Virtual Storage Software Agent on the Virtual Storage Software Agent machine.

  Default: 24081
- **VSSB Cluster Instance**: VSSB Cluster instance name (alias) added to the Virtual Storage Software Agent.

4. Click **Next** and then click **OK**.
5. In the **Status** window, in the **Action** column, click **Start** to begin collecting data.

Editing the Hitachi VSS Block Storage probe

You can change the Virtual Storage Software Agent IP address, Virtual Storage Software Agent port, or VSSB cluster instance if these details have changed.

Procedure

1. Open the Analyzer probe home page
2. In the **Status** window, stop the Hitachi VSS Block Storage probe and then click **Edit**.
3. In the **Edit Hitachi Virtual Storage Software Block Probe** window, enter the Virtual Storage Software Agent IP address, Virtual Storage Software Agent port, or VSSB cluster instance, and then click **Next**.
4. In the **Validation** window, click **Next**, and then click **OK**.
5. In the **Action** column, click **Start** to begin collecting data.

Adding Hitachi NAS probe

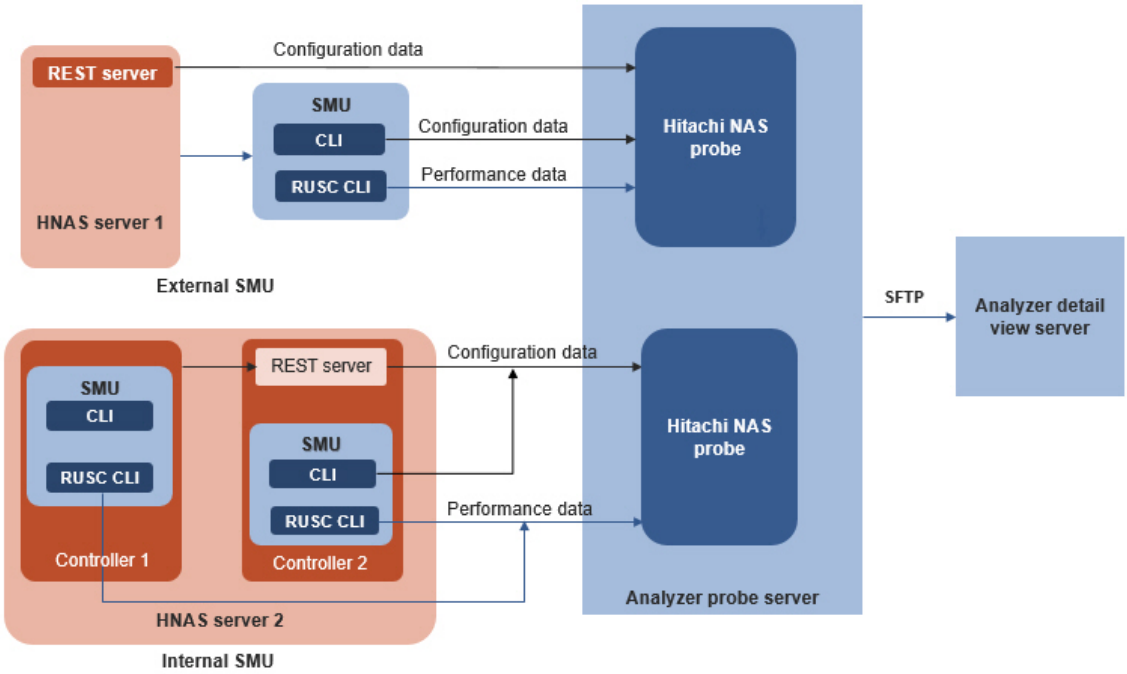
Hitachi NAS probe collects configuration and performance data for the Hitachi NAS platform. There are two types of Hitachi NAS configurations: External SMU and Internal SMU. The Hitachi NAS probe collects configuration data using REST API, and performance data using RUSC CLI.

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. Make sure that following criteria are met for REST API and NAS OS versions:

- REST API v7.1.0: NAS OS v13.5 or higher
- REST API v7.1.3: NAS OS v13.7 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.

> **Note:** If the Hitachi NAS storage system is upgraded for an existing Hitachi NAS probe, make sure you restart that probe in the Analyzer probe UI.

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 use REST API calls.

    A valid Enterprise Virtual Server (EVS) IP address with admin services type (called an Admin EVS IP address) is required to use 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.

- If the SMU OS version is v13.9.6628.07 or higher, make sure that SMU session timeout value is configured to 1 hour. Refer to the Hitachi NAS documentation to configure the session timeout value.
- By default, the Hitachi NAS probe does not collect the Hitachi NAS File System resource snapshot size data from Analyzer probe v10.8.0-00 or later. To collect the snapshot size data, you must enable collection on the Analyzer probe, which might cause a Hitachi NAS system restart problem. Therefore, we only recommend enabling snapshot size data collection if the system restart problem has been fixed in your target Hitachi NAS system. See Enabling snapshot size data collection for Hitachi NAS storage system (on page 456) for more information.

Procedure

1. On the Analyzer probe home page, click **Add Probe**.
2. 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.

     Note: Maximum length for password: 16 characters
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 219) 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 reimport 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 IBM Power Systems probe

The IBM Power Systems probe collects configuration and performance data from one or more IBM Power Systems. It connects to the Hardware Management Console (HMC) using the HMC REST API.

Before you begin

- The HMC FQDN or IP address must be accessible from the Analyzer probe server.
- The user must have the hmcviewer role.
- HMC Performance and Capacity Monitoring (PCM) must be enabled .

Procedure

1. On the Analyzer probe home page, click **Add Probe**.
2. In the **Add Probe** window, from the **Probes** menu, select **IBM Power Systems**.

3. In the **Add IBM Power Systems Probe** window, type the following details, and then click **Next**:
   - **HMC FQDN/IP Address**: IP address or FQDN of the HMC.
   - **User name** and **Password**: User name and password of the HMC.
   - **Connection Type**: HTTPS (Only HTTPS connection is supported)
   - **Connection Port**: 12443 (Default port)
4. In the **Validation** window, click **Next**.
5. In the **Select IBM Power Systems** window, select the target IBM Power Systems for which you want to collect data.
6. Click **Next** and then click **OK**.
7. In the **Status** window, a separate probe is added for each selected IBM Power System. In the **Action** column, click **Start** to begin collecting data.

   Note: If you later add another IBM Power System to the same HMC, add an additional probe using the same procedure.

Editing IBM Power Systems probe details

You can change the username, password, or port if these details change on the target HMC. If you have added probes for multiple IBM Power Systems, make sure you update the details for each probe instance.

Procedure

1. In the **Status** window, stop the IBM Power Systems probe and then click **Edit**.
2. In the **Edit IBM Power Systems Probe** window, edit the username, password, or port and then click **Next**.
3. In the **Validation** window, click **Next**, and then click **OK**.
4. In the **Status** window, in the **Action** column, click **Start** to begin collecting data.

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

Before adding the Brocade FC Switch (BNA) probe, verify the following:

- The user Area of Responsibility includes 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 is installed.

> **Note:** Do not use both the Brocade FC Switch (BNA) probe and Brocade FC Switch 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

     > **Note:** Maximum length for password: 16 characters
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 the 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 219) 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 probe

The Brocade FC Switch probe collects performance and configuration data from the individual Brocade FC switch using one of the following methods:

- CLI (using SSH connection)
- REST API (for supported switches starting with v8.2.0)

  For a list of supported switch versions, see Monitoring target FC switches (on page 60).

Note:

- 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. Do not use both the Brocade FC Switch (BNA) and Brocade FC Switch (CLI) probes to collect data for the same switch.
- When you upgrade the firmware for an existing Brocade FC switch probe, you must restart the probe in the Analyzer probe UI.

Before you begin

- **To collect data using the REST API**
  - A user with “admin” or “user” role-based access control (RBAC) role permissions is required. (FOS REST API function calls are permitted or denied based on user privilege configurations determined by the RBAC functionality in Fabric OS.)
  - Make sure that a valid HTTPS certificate is available on the target switch if you want to collect data using the HTTPS connection.
  - A REST API session is used for data collection. Make sure that the number of sessions are configured accordingly.
- **To collect data using the CLI**
  - A user with read-only permissions on the target switch is required. Additionally, Observer and Modify (OM) permission for "Nocheck" RBAC class is required. (This permission is required to collect the data for virtual switches).

Procedure

1. On the Analyzer probe home page, click **Add Probe**.
2. In the **Add Probe** window, from the **Select Probe Type** menu, select **Brocade FC Switch**.
3. In the **Provide Brocade FC Switch Details** window, select the data collection method (CLI or REST API).
4. 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 Resource 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 Resource 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 of the target switch.
     - **Password:** Password of the user.
     - **Protocol:** Select the communication protocol (HTTP or HTTPS)

       Note: This field is displayed only for the REST API data collection method.
     - **Port:** Depending on the data collection method and protocol, enter the port numbers. The default are:
       - REST API: 80 (HTTP) or 443 (HTTPS)
       - CLI: 22 (SSH)
   - **Upload CSV:** You can add a range of switch IP addresses with different credentials and group the switches based on the data center. When adding multiple data centers, make sure that each has a unique name. (The switches are shown under data center in the Analyzer detail view resource 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**.

   Scroll down to view the list of switches. You can also add more switches or delete a switch before adding the probe.
5. To add more Brocade FC Switch IP addresses, click **Add More**.

> **Note:** You can add multiple switches that use the same data collection method at one time.

6. Click **Next**.
   The system scans the switch IP addresses and adds the valid switches to the system.
7. In the **Switch Validation** window, click **Next**, and then **OK**.
   Each valid switch IP address is added as an individual probe.
8. 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 one of the following methods:

- **REST API**: To collect data from DCNM v11.0 or later by using only the HTTPS protocol.
- **Web Services**: To collect data from DCNM version earlier than v11.0 using the HTTP and HTTPS protocols.

> **Note:**
>
> - If the Cisco DCNM version is upgraded from 10.x (or earlier) to 11.x for an existing probe, the Cisco DCNM probe stops collecting data. You must add the probe again using the REST API data collection method.
> - Do not use both the Cisco FC Switch (DCNM) and Cisco FC Switch (CLI) probe to collect data for the same switch.
> - Cisco DCNM REST API collects the data for the FC port that is part of a port channel or connected to an end device (host or storage).

Before you begin

- **REST API**: To collect data from DCNM by running REST APIs, a DCNM user with “Network-operator” role is required.

  > **Note:** The REST API data collection method only supports the HTTPS protocol.

- **Web Services**: To collect data from DCNM by using the Web services, a user with access to the DCNM client is required.

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, select one of the following Data Collection Methods and then click **Next**:
   - **REST API**: Use this option to collect data from the Cisco switches with DCNM v11.0 or later.
     a. Enter the following details:
        - **IP Address**: IP address of DCNM.
        - **Username** and **password** for DCNM. The user must have access to the DCNM web client.
     b. In the **Validation** window, click **Next**.
     c. 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**.
   - **Web Services**: Use this option to collect data from Cisco switches with DCNM versions earlier than v11.0.
     a. Enter the follwing details:
        - **IP Address**: IP address of DCNM.
        - **Protocol** : Select **HTTP** or **HTTPS**.

          The default ports are:

          `80` - HTTP

          `443` - HTTPS
        - **Port**: The port number used to access web service on the DCNM server.

          Note: In some environments, the port number is optional.
        - **Username** and **password** of DCNM. The user must have access to the DCNM web client.
     b. In the **Validation** window, click **Next**.
     c. 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 subset of switches that you want to monitor. For example, if you want to monitor 60 out of 100 switches, you can specify these switches in the CSV file and import it to the probe.

i. Select **Select switches for data collection using csv file import**.

   The CSV file requires a specific format. Download a sample file by clicking the **Export** option.

ii. Edit the CSV file details based on your requirements. You can add only those switches that you want to monitor, or type `No` for each switch that you do not want to monitor.

iii. To load the CSV file, click **Import**. The imported switches are listed in **Select switches for data collection**.

iv. To track the status of the switches in the **Uploaded Switch CSV Record Status** window, click **Details**. For more information, see Viewing the host CSV file import status (on page 219).

4. Click **Next**, and then click **OK**.
5. In the **Status** window, under **Action**, click **Start** to begin collecting data.

Adding Cisco FC Switch (CLI) probe

Cisco FC Switch (CLI) probe collects 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 one 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 228) 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.

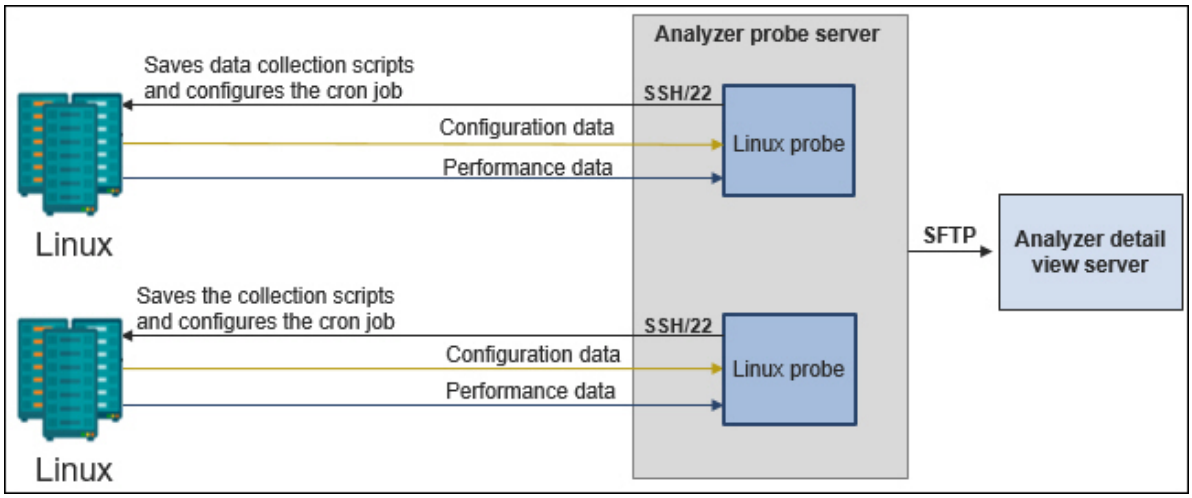
Adding Linux probe

The Linux probe allows you to monitor the overall health of the Linux environment. The Linux probe collects performance and configuration data from individual Linux machines. This can help you analyze performance and configuration related problems.

The Analyzer probe UI requires an IP address, user credentials, and installation directory path of the target Linux machine to add each target machine as an individual probe in the Analyzer probe UI.

The Analyzer probe logs in to the target machine using an SSH connection with user-specified credentials, saves the data collection scripts, and configures a cron job to collect configuration and performance data. The data is saved in the installation directory on the target machine and periodically transferred to theAnalyzer probe server using the `sendRawData.pl` script.

The following diagram illustrates the data collection flow:



Note:

- If you are planning to upgrade the operating system on the Linux host for an existing Linux probe, make sure you stop the Linux probe in the Analyzer probe UI before the upgrade and restart it after the upgrade.
- If you have added a Linux probe for a target where the Analyzer probe or Analyzer detail view application is running, we recommend stopping the application before you upgrade the operating system.

Before you begin

- The following is required on each target machine or host to be monitored:
  - **Packages:**
    - Install the following RPM packages:
      - sysstat
      - perl
      - zip
      - openssh-clients
    - Install the following Perl modules:
      - 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 in a common location (accessible to all users). Refer to Installing the perl module (on page 231) for more information.
  - **Installation directory:** Create an installation directory (where the collection scripts and data will be stored).

    Note: The directory name is restricted to alphanumeric, hyphen, and underscore characters only.
  - **User:**
    - A user account to add the Linux probe with read, write, and execute permissions. This user must also have the following:
      - Privilege to access the cron job on each target machine.
      - Read, write, and execute permissions for the installation directory (that you will create on target machine).
      - Execute permission for Perl modules (that you will install on the target machine).

      Note:
      - As a best practice, set a non-expiring password for the user. If the password on the target Linux machine expires or changes after adding the probe, you must update it immediately in the Analyzer probe UI for the associated Linux probe.
      - Do not remove the account that you will use to add the Linux probe to collect data from the target Linux machine.
    - Data for the following resources are collected only if you add the Linux probe as the root user:

- Host Volume Group
- Host Logical Volume
- Host Physical Volume

Note:

- The Linux probe does not collect multipath information.
- By default, the Linux probe does not collect processes data. See Enabling the Linux host processes data collection (on page 482) for more information.

- The `xinetd` service must be running on the Analyzer probe server.

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**: IP address of the target Linux machine
   - **USERNAME**: User on the target Linux host or machine

     Note: Do not remove the account that was used to add the Linux probe.

   - **PASSWORD**: User password
   - **INSTALLATION DIRECTORY**: Installation directory path on the target machine or host
4. To add multiple targets, click **Add More**. Otherwise, click **Next** to continue.

   The **Host Validation** section opens and validates the host IP address.
5. Click **Next**.
   The **Script Deployment** section opens and data collection scripts are deployed on the target machine or host.
6. Click **Next**, and then click **OK**.
7. In the **Status** window, in **Action**, click **Start** to start collecting data.

   Each target machine is added as an individual Linux probe in the Analyzer probe.

   Note: If the password on the target Linux machine is expired or changed after adding the probe, you must immediately update it by using the probe UI for the Analyzer probe that monitors the target.

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 a common location that is accessible to all users.

Procedure

1. Verify if the **`perl`** module is installed by using one of the following methods.

   Using the perl command:

   ```
   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.
   ```

   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 **`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.

3. Verify if the installation is successful by using one of the following methods.

   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 Analyzer server UI.

Chapter 9: 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 method

You can use the following method to collect data using the Analyzer Windows probe:

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.
  - The Local Service on the target machine must have read permissions for the following registry key:

    `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg`

- Users designated for this method must be added to the Local Group Policy on the target machine and the machine on which the Analyzer Windows probe is installed:

  Run the Local Group Policy Editor (`gpedit.msc`), select Computer Configuration > Windows Settings > Security Settings > Local Policies > User Rights Assignment, and then add the users to the Log on as a service and Allow log on locally policy settings. In addition, make certain that the users are not present in the Deny log on locally setting (which would prevent them from logging in).

  In addition, make sure that the following default rights (policy settings) are assigned to the designated user:

  - Access this computer from the network
  - Adjust memory quotas for a process
  - Allow log on through Remote Desktop Services
  - Back up files and directories
  - Bypass traverse checking
  - Change the system time
  - Change the time zone
  - Create a pagefile
  - Create global objects
  - Create symbolic links
  - Debug programs
  - Enable computer and user accounts to be trusted for delegation
  - Force shutdown from a remote system
  - Impersonate a client after authentication
  - Increase scheduling priority
  - Load and unload device drivers
  - Log on as a batch job
  - Manage auditing and security log
  - Modify firmware environment values
  - Perform volume maintenance tasks
  - Profile system performance
  - Profile single process
  - Remove computer from docking station
  - Restore files and directories
  - Shut down the system
  - Take ownership of files or other objects

- 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:

  Run **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 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.

  - The 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:

   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 54).
   - **Port**: Port number. The default port for FTP is `21`.
   - **User**: `meghadata`
   - **Password**: 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 108) for more information.

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:** 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 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 10: Upgrade your Ops Center Analyzer environment

You can upgrade Ops Center Analyzer components.

Upgrade workflow

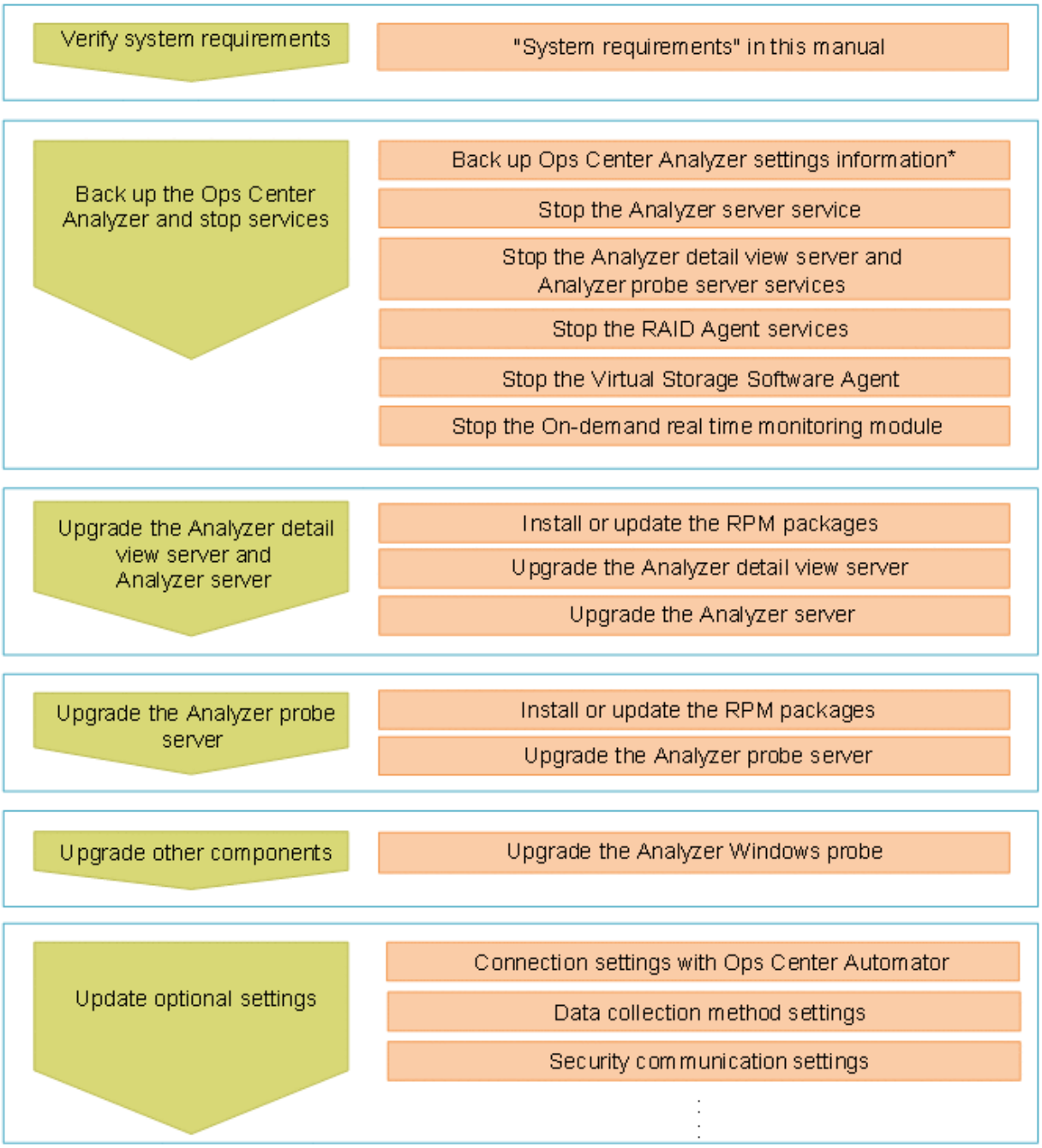
Upgrade the following components:

- Analyzer server
- Analyzer detail view server
- Analyzer probe server (the RAID agent and the Virtual Storage Software Agent on the same host)
- Windows probe

Use the installer to perform an upgrade regardless of whether you used the OVA or the installer when you performed the original installation.

Note: If you want to use Tuning Manager - Agent for RAID, use a version supported by Ops Center Analyzer. For details on the supported versions, see Requirements for adding the Hitachi Enterprise Storage probe (when using Tuning Manager - Agent for RAID) (on page 194). If your current version 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. 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.

Preparing for an upgrade

Before upgrading each component, back up Ops Center Analyzer and stop the services.

Before you begin

Review the requirements for the following components (hardware and software):

- Analyzer server
- Analyzer detail view server
- Analyzer probe server

Procedure

1. Back up Ops Center Analyzer in case the upgrade fails. For details, see Backing up Ops Center Analyzer (on page 510).
2. Stop each service in the following order:
   a. Analyzer server
      Stopping the Analyzer server services (on page 438)
   b. Analyzer detail view server
      Stopping the Analyzer detail view server or Analyzer probe server services (on page 440)
   c. Analyzer probe server
      Stopping the Analyzer detail view server or Analyzer probe server services (on page 440)
   d. RAID Agent
      Stopping the RAID Agent services (on page 442)
   e. Virtual Storage Software Agent
      Stopping the Virtual Storage Software Agent services (on page 443)
   f. On-demand real time monitoring module
      Stopping the On-demand real time monitoring module services (on page 444)
   g. Analyzer Windows probe

Installing or updating the prerequisite RPM packages

You can obtain the prerequisite RPM packages from the Linux OS media or the distribution website, such as for Red Hat Enterprise Linux.

You can check which RPM packages are missing by running the precheck tool (`analytics_precheck.sh`).

If the `libstdc++` package is already installed in the environment in which the Analyzer probe server:

```
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 the `x86_64` (the 64-bit library), and then retry the installation of `libstdc++.i686`:

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

Installing or updating the RPM packages by using the Linux OS media

The following describes how to install or update the RPM packages by using the Linux OS media.

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

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

2. Configure the yum repository.

   - For Red Hat Enterprise Linux and Oracle Linux 7 or earlier:

     ```
     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
     ```

   - For Red Hat Enterprise Linux and Oracle Linux 8 or later:

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

   - **For the package group:**

     ```
     yum group install package-group-to-install
     ```

4. Unmount the Linux OS media:

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

Installing or updating the RPM packages using the distribution website

The following describes how to install or update the RPM packages by using the distribution website.

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-install
   ```

   - **For the package group:**

   ```
   yum group install package-group-to-install
   ```

Upgrading the Analyzer detail view and the Analyzer servers

You can upgrade the Analyzer server and the Analyzer detail view server individually, or upgrade both servers together. (`analytics_install.sh`).

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 Analyzer server and the Analyzer detail view server requirements (hardware and software).
- If you are upgrading the Analyzer detail view server, verify that you have a registered license.
- If the Analyzer detail view server is connected to the Analyzer server, you must upgrade the Analyzer detail view server and the Analyzer server at the same time.
- Regardless of whether the Analyzer detail view server and the Analyzer server are installed on the same host, you must upgrade the Analyzer detail view server before you upgrade the Analyzer server.
- To upgrade from a version earlier than 10.0.0, verify the following:
  - The `/var` directory of the host on which you plan to install the Analyzer server has 5 GB of free space.
  - Both the root directory and the installation directory of the host on which you plan to install the Analyzer detail view server have 5 GB of free space.
- Make sure that the following directories are not mounted with the `noexec` option:
  - `/opt`
  - `/tmp`
  - `/var/opt`
- Check Port requirements (on page 49), and change the firewall and network settings so that the required ports can communicate.

Procedure

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:
   - You must use only the following characters in the directory path to which the installer is copied: `A-Z a-z 0-9 - . _`
   - Do not use spaces.

   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/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
```

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 following message is shown, refer to the release notes.

```
An Analyzer server earlier than v10.7.0, Hitachi Ops Center Automator earlier
than v10.8.0, or Hitachi Command Suite earlier than v8.8.3 is already installed
on this server. Make sure to upgrade the relevant products by referring to the
Release Notes.
```

If the following message is displayed, you must change the JDK used by the Analyzer detail view server. For details, see Resolving a JDK-related error for the Analyzer detail view server (on page 550).

```
JDK environment is invalid (invalid-settings).
```

For *invalid-settings*, one or more of the following values is displayed: `java`, `keytool`, `jstack`, `jre_1.8.0`, or `java_home`.

Note:

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

   Do not change the size of the device window while the command is running. If you change the size of the window, the installation fails.

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
```

   If the following message is shown, refer to the release notes.

```
An Analyzer server earlier than v10.7.0, Hitachi Ops Center Automator earlier
than v10.8.0, or Hitachi Command Suite earlier than v8.8.3 is already installed
on this server. Make sure to upgrade the relevant products by referring to the
Release Notes.
```

   If the following message is displayed, you must change the JDK used by the Analyzer detail view server. For details, see Resolving a JDK-related error for the Analyzer detail view server (on page 550).

```
[ERR]  JDK environment is invalid (invalid-settings).
```

   For *invalid-settings*, one or more of the following values is displayed: `java`, `keytool`, `jstack`, `jre_1.8.0`, or `java_home`.

8. Refresh the browser cache.

Upgrading the Analyzer probe server

When you upgrade the Analyzer probe server, the RAID agent and Virtual Storage Software Agent on the same host are automatically upgraded, but Ops Center API Configuration Manager and other Ops Center products are not upgraded. If you are upgrading the Analyzer probe server from version 10.8.1 or earlier, you can choose whether to perform a new installation of Virtual Storage Software Agent.

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.
- Review the Analyzer probe server requirements (hardware and software).
- When upgrading from a version earlier than 10.0.0, make sure that both the root directory and the installation directory of the host on which you plan to install the Analyzer probe server has 5 GB of free space.
- During the upgrade, `/opt/jp1pc/htnm/HBasePSB/hjdk/jdk` might be deleted. If you have created files under this directory, move them elsewhere before starting the upgrade. If any settings (such as `htnm_httpsd.conf`) reference a file under this directory, revise them to use the new location.
- Make sure that the following directories are not mounted with the `noexec` option:
  - `/tmp`
  - `/var`
- Check Port requirements (on page 49), and change the firewall and network settings so that the required ports can communicate.

Procedure

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:
   - You must use only the following characters in the directory path to which the installer is copied: `A-Z a-z 0-9 - . _`
   - Do not use spaces.

   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
```

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 following message is displayed, you must change the JDK used by the Analyzer probe server. For details, see Resolving a JDK-related error for the Analyzer probe server (on page 552).

```
JDK environment is invalid (invalid-settings).
```

For *invalid-settings*, one or more of the following values is displayed: `java`, `keytool`, `jstack`, `jre_1.8.0`, or `java_home`.

Note:

- When you run the precheck tool, it checks the static information of the system environment.
- 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
```

   - Do not change the size of the device window while the command is running. If you change the size of the window, the installation fails.
   - If the following message is displayed, you must change the JDK used by the Analyzer probe server. For details, see Resolving a JDK-related error for the Analyzer probe server (on page 552).

     ```
     [ERR]  JDK environment is invalid (invalid-settings).
     ```

     For *invalid-settings*, one or more of the following values is displayed: `java`, `keytool`, `jstack`, `jre_1.8.0`, or `java_home`.

   If you are upgrading the Analyzer probe server from version 10.8.1 or earlier, you can choose whether to perform a new installation of Virtual Storage Software Agent.

   ```
   Do you want to install the Virtual Storage Software Agent server?(y/n) [n]:y
   ```

7. Refresh the browser cache.

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.

Procedure

1. Download the Analyzer Windows probe installer to your machine.
2. To upgrade your current Analyzer Windows probe, run each of the `DCA_Windows_Probe_x.x.x-xx.exe` installers in ascending order: where *x.x.x-xx* is the version number.

> **Note:** If you want to confirm your current Analyzer Windows probe version, check the version in **Programs and Features** in **Control Panel** on your Analyzer Windows probe server.

3. Run the `DCA_Windows_Probe.exe` to install the Analyzer Windows probe.

   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 on a Windows 64-bit machine, the upgrade process makes a backup of the current Analyzer Windows probe configuration file in this location: `C:\Program Files\HDCA\HDCA Windows Probe`

4. If you have `DCA_Windows_Probe_Patch.exe`, run it to install the patch version.

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:

- **Refreshing the browser cache:** After upgrading to the Analyzer detail view server and Analyzer probe server, sometimes the UI is distorted. To fix this issue, refresh the browser cache.
- **Initializing the browser settings:** 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 255).
- **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 351) and Configuring an SSL certificate (Common Services) (on page 404). If you enabled SSL communication during the use of Infrastructure Analytics Advisor, see Configuring an SSL certificate (Common Services) (on page 404).
- **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 105) and Assigning Analyzer permissions to Ops Center user groups (on page 106).

If you want to use Common Services with Analyzer detail view after an upgrade, check the following:

- **Initial settings for using Common Services:** When you use Common Services for the first time, perform the procedures in Registering Analyzer detail view server with Common Services (on page 95) and Assigning Analyzer detail view roles to Ops Center user groups (on page 97).

If you want to use Common Services with Analyzer probe after an upgrade, check the following:

- **Initial settings for using Common Services:** When you use Common Services for the first time, perform the procedures in Registering Analyzer probe server with Common Services (on page 98).

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 110).
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:

`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 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 11: 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.

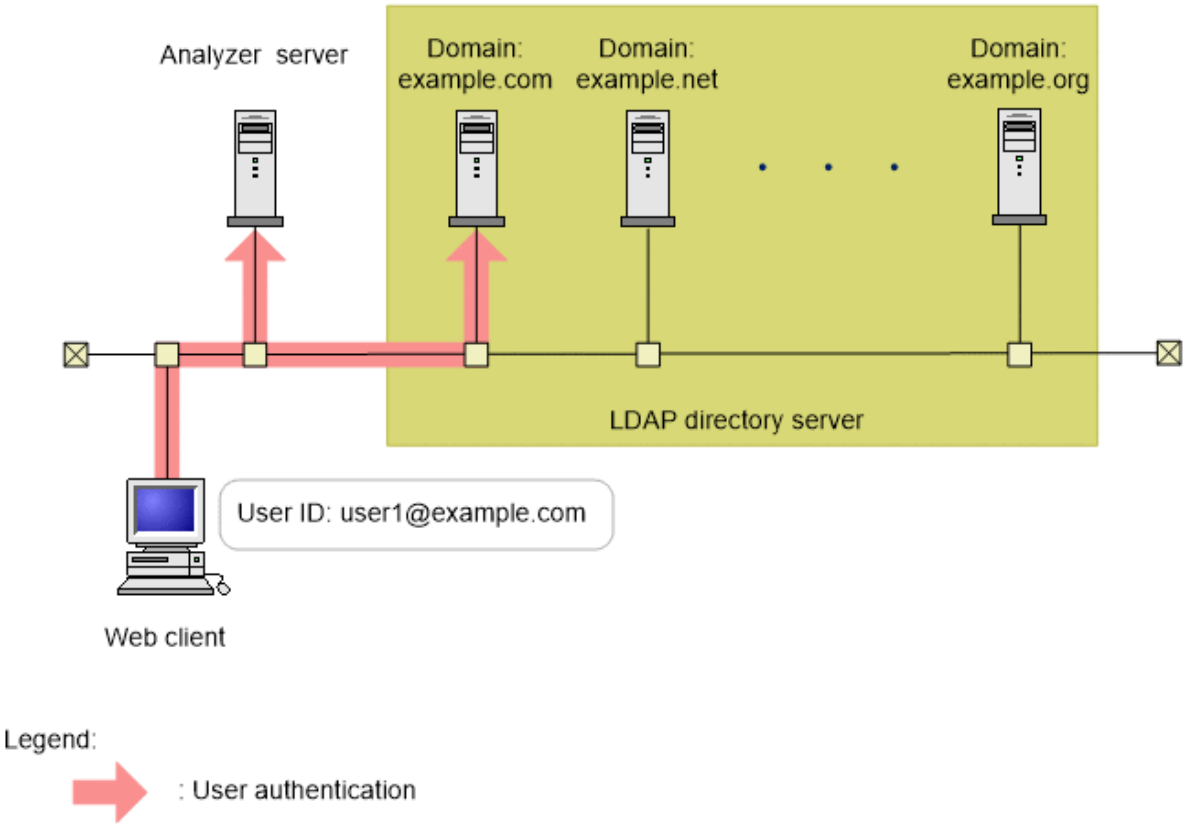
The following table shows external authentication servers for which redundant configurations and multi-domain configurations are supported.

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:**		

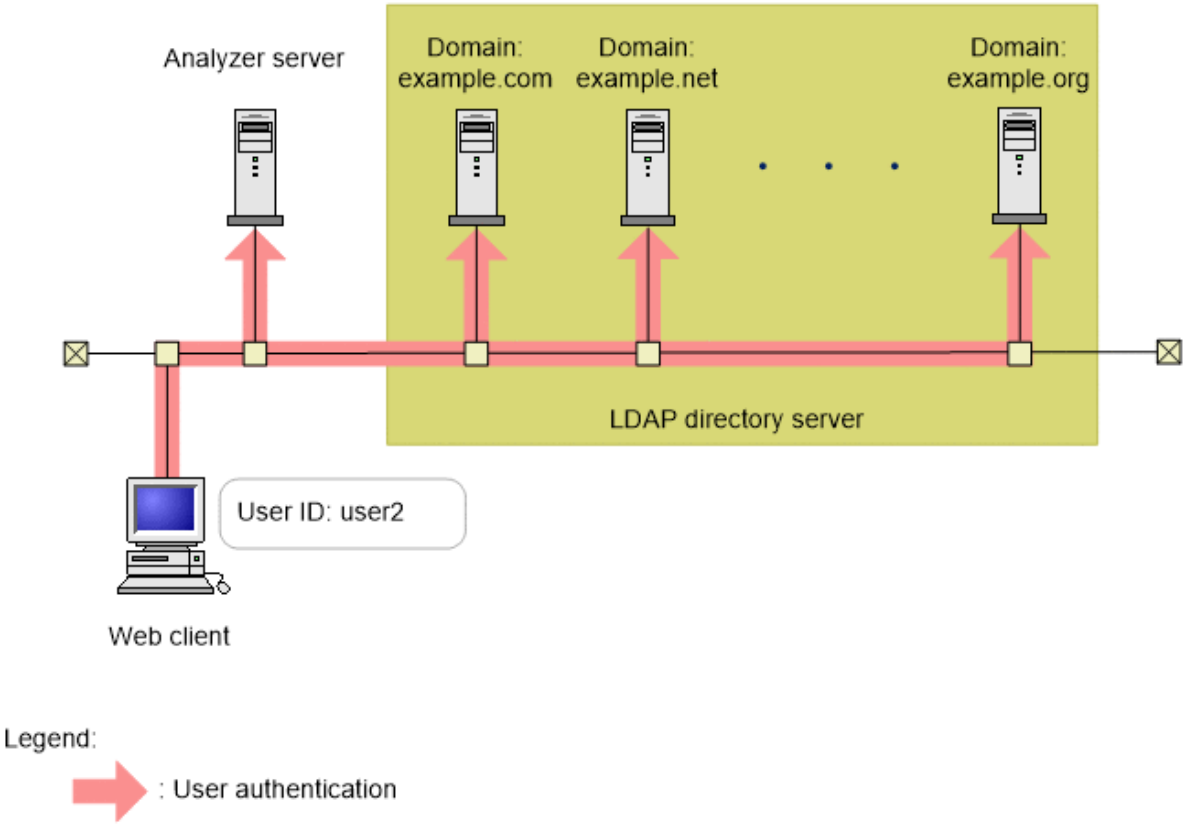
External authentication server	Redundant configuration	Multi-domain configuration
1. You can use either a redundant configuration or a multi-domain configuration. If the global catalog for Active Directory is set, you can use both a redundant configuration and a multi-domain configuration. 2. By managing 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.



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.



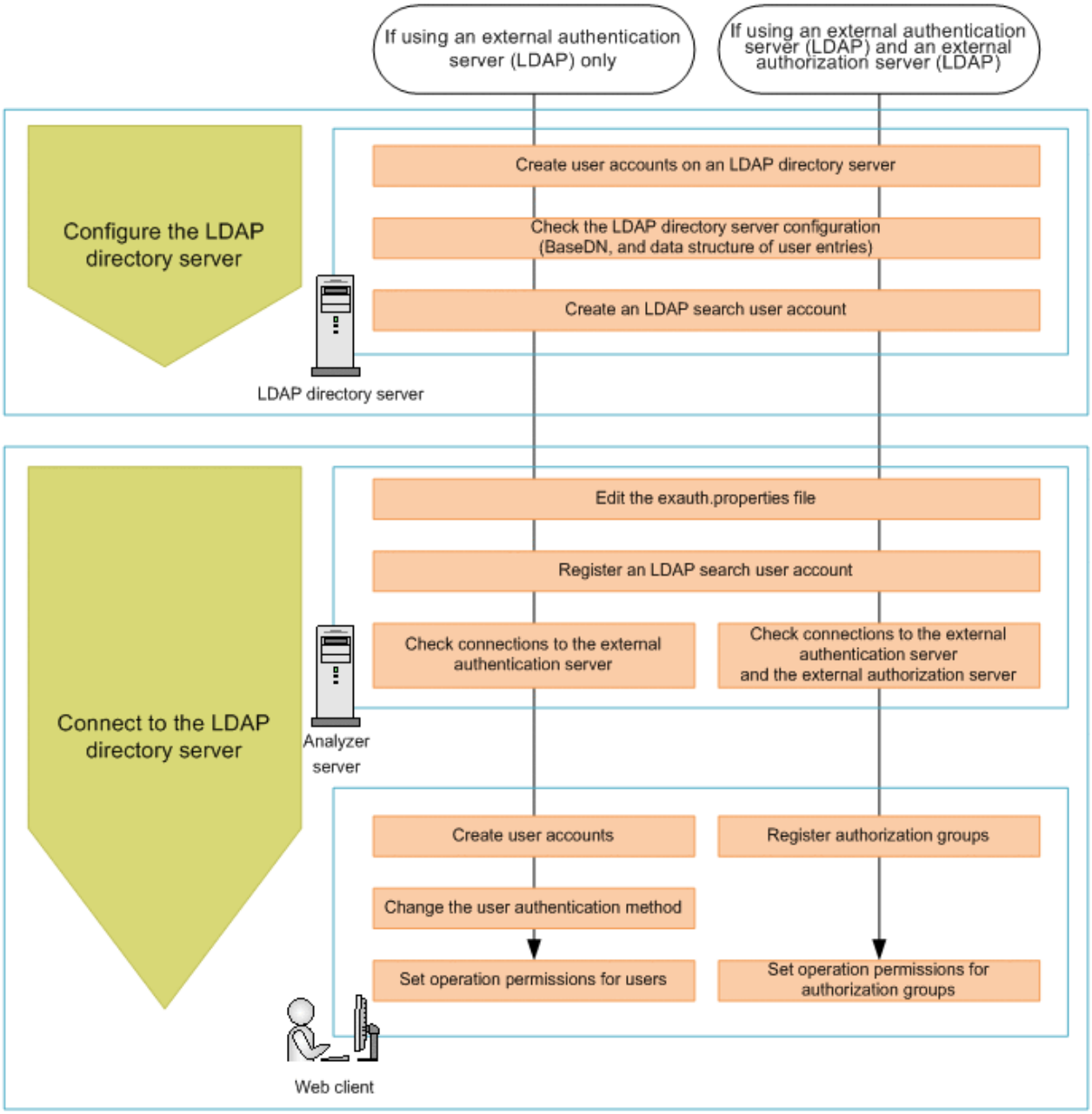
Configuring LDAP authentication for Analyzer server

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.

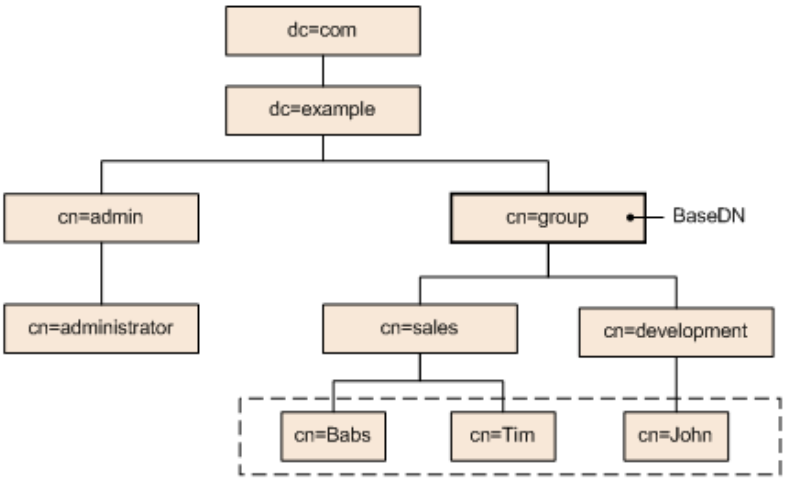
The following describes BaseDN in the hierarchical structure model and in the flat model.

- 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.

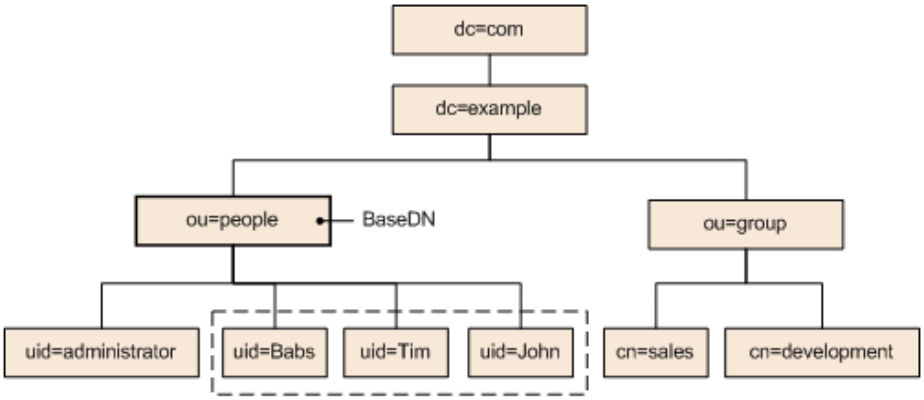
The user entries enclosed by the dotted line can be authenticated. In this example, BaseDN is `cn=group,dc=example,dc=com`, because the target user entries extend across two departments (`cn=sales` and `cn=development`).

- 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 root permission.
- 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 directory.

      `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:

      `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 **hcmds64ldapuser** command to register the LDAP search user account.

```
Common-component-installation-destination-directory/bin/hcmds64ldapuser -
set -dn DN-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.

```
Common-component-installation-destination-directory/bin/hcmds64ldapuser -
list
```

Tip:

To delete the LDAP search user account from the Analyzer server, run the **hcmds64ldapuser** command with the `delete` option.

3. Run the **hcmds64checkauth** command to confirm whether connections to the external authentication server and the external authorization server can be established properly.

```
Common-component-installation-destination-directory/bin/hcmds64checkauth [-
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 271)
	Obtain LDAP directory server information from the DNS server.	Settings for using DNS to connect to an LDAP directory server (on page 275)
Yes	Directly specify information about the LDAP directory server.	Settings for connecting directly to an LDAP directory server and an authorization server (on page 278)
	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 284)

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
`auth.server.type`	Specify an external authentication server type. Specify `ldap`. Default value: `internal` (do not connect to an external authentication server)

`auth.server.name`	Specify the server identification names of LDAP directory servers. You can specify any name for this property in order to identify which LDAP directory servers the settings such as the port number and the protocol for connecting to the LDAP directory server are applied to. `ServerName` has been set as the initial value. You must specify at least one name. To specify multiple server identification names, delimit the server identification names by using commas (`,`). Do not register the same server identification name more than once.
	Specifiable values: No more than 64 bytes of the following characters:
	`A` to `Z`
	`a` to `z`
	`0` to `9`
	`! # ( ) + - . = @ [ ] ^ _ { } ~`
	Default value: none

`auth.ldap.multi_domain`	When specifying multiple server identification names for LDAP directory servers, specify the configuration to use for each server. Specify `true` to use a multi-domain configuration. Specify `false` to use a redundant configuration. Default value: `false`
`auth.ldap.default_domain`	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 `auth.server.name`, a multi-domain configuration will be used, and a redundant configuration will not be used. Default value: none

Property names	Details
`auth.group.mapping`	Specify whether to also connect to an external authorization server (LDAP directory server). Specify `false` (do not connect). Default value: `false` (do not connect)
`auth.ocsp.enable`	Specify whether or not to verify the validity of an LDAP directory server electronic signature certificate by using an OCSP responder when the LDAP directory server and STARTTLS are used for communication. If you want to verify the validity of certificates, specify `true`. To not verify the validity of certificates, specify `false`. Default value: `false`
`auth.ocsp.responderURL`	Specify the URL of an OCSP responder if you want to use an OCSP responder that is not the one written in the AIA field of the electronic signature certificate to verify the validity of the electronic signature certificate. If this value is omitted, the OCSP responder written in the AIA field is used. Default value: none
`auth.ldap.`*`auth.server.name-property-value`*`.protocol`	Specify the protocol for connecting to the LDAP directory server. This attribute is required. When communicating in cleartext, specify `ldap`. When using STARTTLS communication, specify `tls`. Before specifying `tls`, 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. ▪ TLS_RSA_WITH_AES_256_GCM_SHA384 ▪ TLS_RSA_WITH_AES_256_CBC_SHA256 ▪ TLS_RSA_WITH_AES_256_CBC_SHA ▪ TLS_RSA_WITH_AES_128_CBC_SHA256 ▪ TLS_RSA_WITH_AES_128_CBC_SHA Specifiable values: `ldap` or `tls` Default value: none

Property names	Details
`auth.ldap.`*`auth.server.name-property-value`*`.host`	Specify the host name or IP address of the LDAP directory server. If you specify the host name, make sure beforehand that the host name can be resolved to an IP address. If you specify the IP address, you can use either an IPv4 or IPv6 address. When specifying an IPv6 address, enclose it in square brackets (`[ ]`). This attribute is required. To use a redundant configuration when the global catalog is enabled (`auth.ldap.default_domain` is specified), specify multiple host names or IP addresses, delimited by commas. When using STARTTLS as the protocol for connecting to the LDAP directory server, in the `host` attribute specify the same host name as the value of CN in the LDAP directory server certificate. You cannot use an IP address. Default value: none
`auth.ldap.`*`auth.server.name-property-value`*`.port`	Specify the port number of the LDAP directory server. Make sure beforehand that the port you specify is set as the listen port number on the LDAP directory server. To use a redundant configuration when the global catalog is enabled (`auth.ldap.default_domain` 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 `host`. Specifiable values: 1 to 65535 Default value: 389 (when the global catalog is disabled), 3268 (when the global catalog is enabled)
`auth.ldap.`*`auth.server.name-property-value`*`.timeout`	Specify the amount of time to wait before timing out when connecting to the LDAP directory server. If you specify 0, the system waits until a communication error occurs without timing out. Specifiable values: 0 to 120 (seconds) Default value: 15

Property names	Details
`auth.ldap.`*`auth.server.name-property-value`*`.attr`	Specify the attribute (Attribute Type) to use as the user ID during authentication. ▪ For the hierarchical structure model Specify the name of the attribute containing the unique value to 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. 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 `sAMAccountName` in which the Windows logon ID has been defined. ▪ For the flat model Specify the RDN attribute name of the user entry. For example, if the user's DN is `uid=John,ou=People,dc=example,dc=com`, specify the `uid` that is the attribute name of the `uid=John`. `sAMAccountName` has been set as the initial value. This attribute is required. Default value: none
`auth.ldap.`*`auth.server.name-property-value`*`.basedn`	Specify the BaseDN, which is the DN of the entry that will be used as the start point when searching for LDAP user information on the LDAP directory server. The user entries that are located in the hierarchy below this DN will be checked during authentication. If characters that must be escaped are included in the specified BaseDN, escape all of those characters correctly because the specified value will be passed to the LDAP directory server without change. ▪ For the hierarchical structure model Specify the DN of the hierarchy that includes all of the user entries to be searched. ▪ For the flat model Specify the DN of the hierarchy just above the user entries to be searched. This attribute is required. Specify the DN by following the rules defined in RFC4514. For example, if any of the following characters are included in a DN, you must use a backslash (`\`) to escape each character.

Property names	Details
	Spaces `# + ; , < = > \` Default value: none
`auth.ldap.`*`auth.server.name-property-value`*`.retry.interval`	Specify the retry interval (in seconds) for when an attempt to connect to the LDAP directory server fails. Specifiable values: 1 to 60 (seconds) Default value: 1
`auth.ldap.`*`auth.server.name-property-value`*`.retry.times`	Specify the number of retries to attempt when an attempt to connect to the LDAP directory server fails. If you specify 0, no retries are attempted. Specifiable values: 0 to 50 Default value: 20
`auth.ldap.`*`auth.server.name-property-value`*`.domain`	Specify the name of a domain for multi-domain configurations managed by the LDAP directory server, or the domain name for the global catalog. 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. 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. If the global catalog is enabled, be sure to specify the domain name that is specified in `auth.ldap.default_domain` as the default server configuration to use for authentication. This attribute is required when a multi-domain configuration is used. Default value: none
`auth.ldap.`*`auth.server.name-property-value`*`.dns_lookup`	Specify whether to use the DNS server to look up the information about the LDAP directory server. Specify `false` (do not look up the information). Default value: `false` (do not look up the information)

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
`auth.server.type`	Specify an external authentication server type. Specify `ldap`. Default value: `internal` (do not connect to an external authentication server)

`auth.server.name`	Specify the server identification names of LDAP directory servers. You can specify any name for this property in order to identify which LDAP directory servers the settings such as the port number and the protocol for connecting to the LDAP directory server are applied to. `ServerName` 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

`auth.group.mapping`	Specify whether to also connect to an external authorization server (LDAP directory server). Specify `false` (do not connect). Default value: `false` (do not connect)
`auth.ldap.`*`auth.server.name-property-value`*`.protocol`	Specify the protocol for connecting to the LDAP directory server. This attribute is required. Specifiable values: `ldap` Default value: none
`auth.ldap.`*`auth.server.name-property-value`*`.timeout`	Specify the amount of time to wait before timing out when connecting to the LDAP directory server. If you specify 0, the system waits until a communication error occurs without timing out. Specifiable values: 0 to 120 (seconds) Default value: 15

Property names	Details
`auth.ldap.`*`auth.server.name-property-value`*`.attr`	Specify the attribute (Attribute Type) to use as the user ID during authentication. ▪ For the hierarchical structure model Specify the name of the attribute containing the unique value to 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. 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 `sAMAccountName` in which the Windows logon ID has been defined. ▪ For the flat model Specify the RDN attribute name of the user entry. For example, if the user's DN is `uid=John,ou=People,dc=example,dc=com`, specify the `uid` that is the attribute name of the `uid=John`. `sAMAccountName` has been set as the initial value. This attribute is required. Default value: none
`auth.ldap.`*`auth.server.name-property-value`*`.basedn`	Specify the BaseDN, which is the DN of the entry that will be used as the start point when searching for LDAP user information on the LDAP directory server. The user entries that are located in the hierarchy below this DN will be checked during authentication. If characters that must be escaped are included in the specified BaseDN, escape all of those characters correctly because the specified value will be passed to the LDAP directory server without change. ▪ For the hierarchical structure model Specify the DN of the hierarchy that includes all of the user entries to be searched. ▪ For the flat model Specify the DN of the hierarchy just above the user entries to be searched. This attribute is required. Specify the DN by following the rules defined in RFC4514. For example, if any of the following characters are included in a DN, you must use a backslash (`\`) to escape each character.

Property names	Details
	Spaces `# + ; , < = > \` Default value: none
`auth.ldap.`*`auth.server.name-property-value`*`.retry.interval`	Specify the retry interval (in seconds) for when an attempt to connect to the LDAP directory server fails. Specifiable values: 1 to 60 (seconds) Default value: 1
`auth.ldap.`*`auth.server.name-property-value`*`.retry.times`	Specify the number of retries to attempt when an attempt to connect to the LDAP directory server fails. If you specify 0, no retries are attempted. Specifiable values: 0 to 50 Default value: 20
`auth.ldap.`*`auth.server.name-property-value`*`.domain.name`	Specify the name of a domain managed by the LDAP directory server. This attribute is required. Default value: none
`auth.ldap.`*`auth.server.name-property-value`*`.dns_lookup`	Specify whether to use the DNS server to look up the information about the LDAP directory server. Specify `true` (look up the information). However, if the following attribute values are already set, the LDAP directory server will be connected to by using the user-specified values instead of by using the DNS server to look up the information. ▪ `auth.ldap.`*`auth.server.name-property-value`*`.host` ▪ `auth.ldap.`*`auth.server.name-property-value`*`.port` Default value: `false` (do not look up the information)

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
`auth.server.type`	Specify an external authentication server type. Specify `ldap`. Default value: `internal` (do not connect to an external authentication server)

`auth.server.name`	Specify the server identification names of LDAP directory servers. You can specify any name for this property in order to identify which LDAP directory servers the settings such as the port number and the protocol for connecting to the LDAP directory server are applied to. `ServerName` has been set as the initial value. You must specify at least one name. To specify multiple server identification names, delimit the server identification names by using commas (`,`). Do not register the same server identification name more than once.
	Specifiable values: No more than 64 bytes of the following characters:
	`A` to `Z`
	`a` to `z`
	`0` to `9`
	`! # ( ) + - . = @ [ ] ^ _ { } ~`
	Default value: none

`auth.ldap.multi_domain`	When specifying multiple server identification names for LDAP directory servers, specify the configuration to use for each server. Specify `true` to use a multi-domain configuration. Specify `false` to use a redundant configuration. Default value: `false`
`auth.ldap.default_domain`	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 `auth.server.name`, a multi-domain configuration will be used, and a redundant configuration will not be used. Default value: none
`auth.group.mapping`	Specify whether to also connect to an external authorization server (LDAP directory server). Specify `true` (connect). Default value: `false` (do not connect)

Property names	Details
`auth.ocsp.enable`	Specify whether or not to verify the validity of an LDAP directory server electronic signature certificate by using an OCSP responder when the LDAP directory server and STARTTLS are used for communication. If you want to verify the validity of certificates, specify `true`. To not verify the validity of certificates, specify `false`. Default value: `false`
`auth.ocsp.responderURL`	Specify the URL of an OCSP responder if you want to use an OCSP responder that is not the one written in the AIA field of the electronic signature certificate to verify the validity of the electronic signature certificate. If this value is omitted, the OCSP responder written in the AIA field is used. Default value: none
`auth.ldap.`*`auth.server.name-property-value`*`.protocol`	Specify the protocol for connecting to the LDAP directory server. This attribute is required. When communicating in cleartext, specify `ldap`. When using STARTTLS communication, specify `tls`. Before specifying `tls`, 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. ▪ TLS_RSA_WITH_AES_256_GCM_SHA384 ▪ TLS_RSA_WITH_AES_256_CBC_SHA256 ▪ TLS_RSA_WITH_AES_256_CBC_SHA ▪ TLS_RSA_WITH_AES_128_CBC_SHA256 ▪ TLS_RSA_WITH_AES_128_CBC_SHA Specifiable values: `ldap` or `tls` Default value: none
`auth.ldap.`*`auth.server.name-property-value`*`.host`	Specify the host name or IP address of the LDAP directory server. If you specify the host name, make sure beforehand that the host name can be resolved to an IP address. If you specify the IP address, you can use either an IPv4 or IPv6 address. When specifying an IPv6 address, enclose it in square brackets (`[ ]`). This attribute is required.

Property names	Details
	To use a redundant configuration when the global catalog is enabled (`auth.ldap.default_domain` is specified), specify multiple host names or IP addresses, delimited by commas. When using STARTTLS as the protocol for connecting to the LDAP directory server, in the `host` attribute specify the same host name as the value of CN in the LDAP directory server certificate. You cannot use an IP address. Default value: none
`auth.ldap.`*`auth.server.name-property-value`*`.port`	Specify the port number of the LDAP directory server. Make sure beforehand that the port you specify is set as the listen port number on the LDAP directory server. To use a redundant configuration when the global catalog is enabled (`auth.ldap.default_domain` 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 `host`. Specifiable values: 1 to 65535 Default value: 389 (when the global catalog is disabled), 3268 (when the global catalog is enabled)
`auth.ldap.`*`auth.server.name-property-value`*`.timeout`	Specify the amount of time to wait before timing out when connecting to the LDAP directory server. If you specify 0, the system waits until a communication error occurs without timing out. Specifiable values: 0 to 120 (seconds) Default value: 15

Property names	Details
`auth.ldap.`*`auth.server.name-property-value`*`.attr`	Specify the attribute (Attribute Type) to use as the user ID during authentication. ▪ For the hierarchical structure model Specify the name of the attribute containing the unique value to 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. 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 `sAMAccountName` in which the Windows logon ID has been defined. ▪ For the flat model Specify the RDN attribute name of the user entry. For example, if the user's DN is `uid=John,ou=People,dc=example,dc=com`, specify the `uid` that is the attribute name of the `uid=John`. `sAMAccountName` has been set as the initial value. This attribute is required. Default value: none
`auth.ldap.`*`auth.server.name-property-value`*`.basedn`	Specify the BaseDN, which is the DN of the entry that will be used as the start point when searching for LDAP user information on the LDAP directory server. The user entries that are located in the hierarchy below this DN will be checked during authentication. If characters that must be escaped are included in the specified BaseDN, escape all of those characters correctly because the specified value will be passed to the LDAP directory server without change. ▪ For the hierarchical structure model Specify the DN of the hierarchy that includes all of the user entries to be searched. ▪ For the flat model Specify the DN of the hierarchy just above the user entries to be searched. This attribute is required. Specify the DN by following the rules defined in RFC4514. For example, if any of the following characters are included in a DN, you must use a backslash (`\`) to escape each character.

Property names	Details
	Spaces `# + ; , < = > \` Default value: none
`auth.ldap.`*`auth.server.name-property-value`*`.retry.interval`	Specify the retry interval (in seconds) for when an attempt to connect to the LDAP directory server fails. Specifiable values: 1 to 60 (seconds) Default value: 1
`auth.ldap.`*`auth.server.name-property-value`*`.retry.times`	Specify the number of retries to attempt when an attempt to connect to the LDAP directory server fails. If you specify 0, no retries are attempted. Specifiable values: 0 to 50 Default value: 20
`auth.ldap.`*`auth.server.name-property-value`*`.domain.name`	Specify the name of a domain managed by the LDAP directory server. This attribute is required. Default value: none
`auth.ldap.`*`auth.server.name-property-value`*`.domain`	Specify the name of a domain for multi-domain configurations managed by the LDAP directory server, or the domain name for the global catalog. 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. 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. If the global catalog is enabled, be sure to specify the domain name that is specified in `auth.ldap.default_domain` as the default server configuration to use for authentication. This attribute is required when a multi-domain configuration is used. Default value: none
`auth.ldap.`*`auth.server.name-property-value`*`.dns_lookup`	Specify whether to use the DNS server to look up the information about the LDAP directory server. Specify `false` (do not look up the information). Default value: `false` (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
`auth.server.type`	Specify an external authentication server type. Specify `ldap`. Default value: `internal` (do not connect to an external authentication server)

`auth.server.name`	Specify the server identification names of LDAP directory servers. You can specify any name for this property in order to identify which LDAP directory servers the settings such as the port number and the protocol for connecting to the LDAP directory server are applied to. `ServerName` 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

`auth.group.mapping`	Specify whether to also connect to an external authorization server (LDAP directory server). Specify `true` (connect). Default value: `false` (do not connect)
`auth.ldap.`*`auth.server.name-property-value`*`.protocol`	Specify the protocol for connecting to the LDAP directory server. This attribute is required. Specifiable values: `ldap` Default value: none
`auth.ldap.`*`auth.server.name-property-value`*`.timeout`	Specify the amount of time to wait before timing out when connecting to the LDAP directory server. If you specify 0, the system waits until a communication error occurs without timing out. Specifiable values: 0 to 120 (seconds) Default value: 15

Property names	Details
`auth.ldap.`*`auth.server.name-property-value`*`.attr`	Specify the attribute (Attribute Type) to use as the user ID during authentication. ▪ For the hierarchical structure model Specify the name of the attribute containing the unique value to 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. 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 `sAMAccountName` in which the Windows logon ID has been defined. ▪ For the flat model Specify the RDN attribute name of the user entry. For example, if the user's DN is `uid=John,ou=People,dc=example,dc=com`, specify the `uid` that is the attribute name of the `uid=John`. `sAMAccountName` has been set as the initial value. This attribute is required. Default value: none
`auth.ldap.`*`auth.server.name-property-value`*`.basedn`	Specify the BaseDN, which is the DN of the entry that will be used as the start point when searching for LDAP user information on the LDAP directory server. The user entries that are located in the hierarchy below this DN will be checked during authentication. If characters that must be escaped are included in the specified BaseDN, escape all of those characters correctly because the specified value will be passed to the LDAP directory server without change. ▪ For the hierarchical structure model Specify the DN of the hierarchy that includes all of the user entries to be searched. ▪ For the flat model Specify the DN of the hierarchy just above the user entries to be searched. This attribute is required. Specify the DN by following the rules defined in RFC4514. For example, if any of the following characters are included in a DN, you must use a backslash (`\`) to escape each character.

Property names	Details
	Spaces `# + ; , < = > \` Default value: none
`auth.ldap.`*`auth.server.name-property-value`*`.retry.interval`	Specify the retry interval (in seconds) for when an attempt to connect to the LDAP directory server fails. Specifiable values: 1 to 60 (seconds) Default value: 1
`auth.ldap.`*`auth.server.name-property-value`*`.retry.times`	Specify the number of retries to attempt when an attempt to connect to the LDAP directory server fails. If you specify 0, no retries are attempted. Specifiable values: 0 to 50 Default value: 20
`auth.ldap.`*`auth.server.name-property-value`*`.domain.name`	Specify the name of a domain managed by the LDAP directory server. This attribute is required. Default value: none
`auth.ldap.`*`auth.server.name-property-value`*`.dns_lookup`	Specify whether to use the DNS server to look up the information about the LDAP directory server. Specify `true` (look up the information). However, if the following attribute values are already set, the LDAP directory server will be connected to by using the user-specified values instead of by using the DNS server to look up the information. ▪ `auth.ldap.`*`auth.server.name-property-value`*`.host` ▪ `auth.ldap.`*`auth.server.name-property-value`*`.port` Default value: `false` (do not look up the information)

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
```

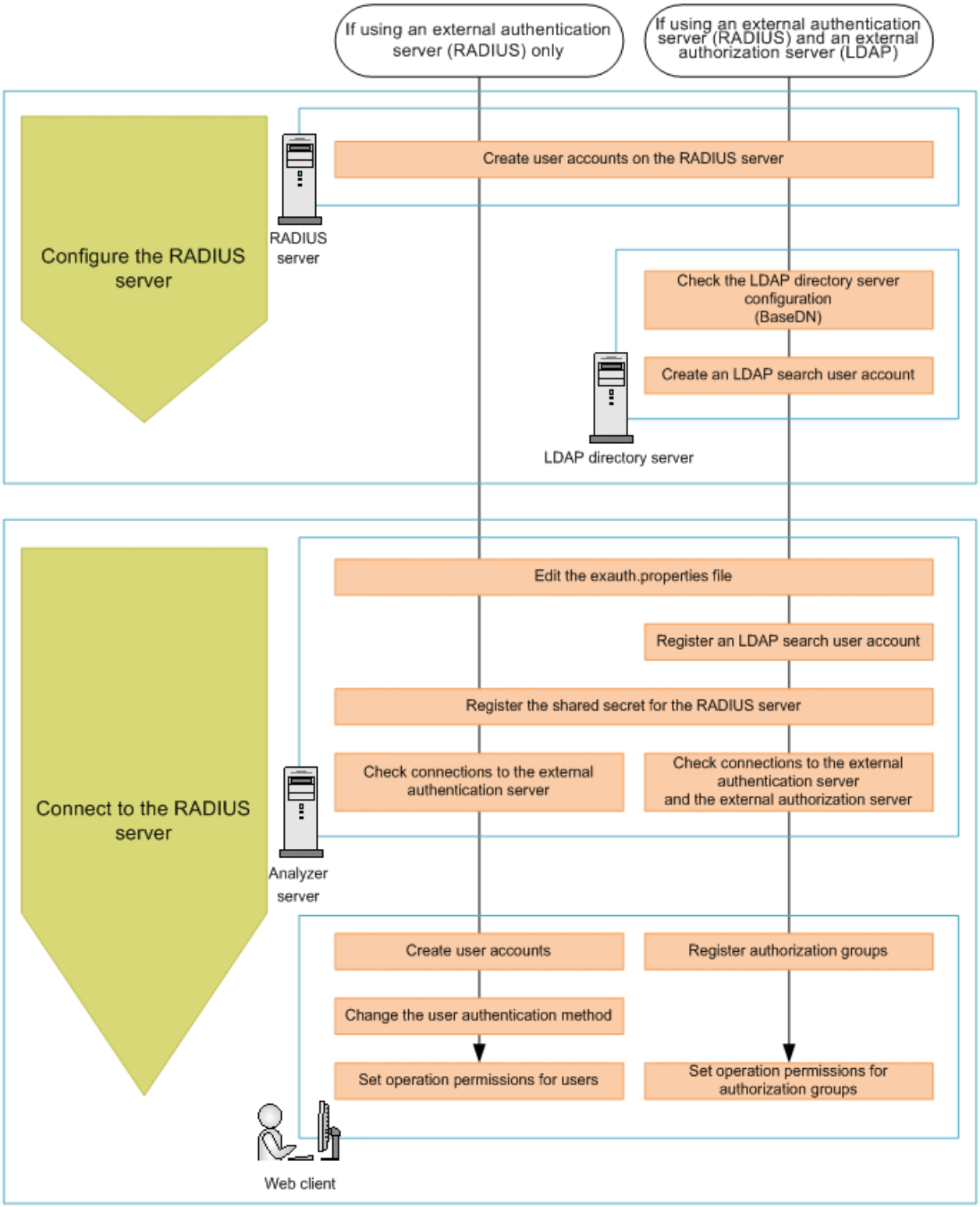
Configuring RADIUS authentication for Analyzer server

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 264)

  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 266)

  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 root permission.
- 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 directory.

      `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:

      `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 **hcmds64ldapuser** command to register the LDAP search user account.

```
Common-component-installation-destination-directory/bin/hcmds64ldapuser -
set -dn DN-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.

```
Common-component-installation-destination-directory/bin/hcmds64ldapuser -
list
```

Tip:

To delete the LDAP search user account from the Analyzer server, run the **hcmds64ldapuser** command with the `delete` option.

3. Register to the Analyzer server a shared secret for communicating with the RADIUS server.

   a. Use the **hcmds64radiussecret** command to register the shared secret of the RADIUS server. When you run the command, enter the shared secret in response to the prompt.

```
Common-component-installation-destination-directory/bin/hcmds64radiussecret
-name RADIUS-server-identification-name
```

   b. You can use the following command to list RADIUS servers for which shared secrets are registered:

```
Common-component-installation-destination-directory/bin/hcmds64radiussecret
-list
```

Tip:

To delete shared secrets that have been registered to the Analyzer server, run the **hcmds64radiussecret** command with the `delete` option specified.

4. Run the **hcmds64checkauth** command to confirm whether connections to the external authentication server and the external authorization server can be established properly.

```
Common-component-installation-destination-directory/bin/hcmds64checkauth [-
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 297)

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 299)
	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 305)

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
`auth.server.type`	Specify an external authentication server type. Specify `radius`. Default value: `internal` (do not connect to an external authentication server)
`auth.server.name`	Specify the server identification names of RADIUS servers. You can specify any name for this property in order to identify which RADIUS servers the settings such as the port number and the protocol for connecting to the RADIUS server are applied to. `ServerName` has been set as the initial value. You must specify at least one name. When configuring a redundant configuration, separate the server identification name of each server with a comma (`,`). Do not register the same server identification name more than once. Specifiable values: No more than 64 bytes of the following characters:

Property names	Details

	`A` to `Z`
	`a` to `z`
	`0` to `9`
	`! # ( ) + - . = @ [ ] ^ _ { } ~`
	Default value: none

`auth.group.mapping`	Specify whether to also connect to an external authorization server (LDAP directory server). Specify `false` (do not connect). Default value: `false` (do not connect)
`auth.radius.`*`auth.server.name-property-value`*`.protocol`	Specify the protocol for RADIUS server authentication. This attribute is required. Specifiable values: `PAP` or `CHAP` Default value: none
`auth.radius.`*`auth.server.name-property-value`*`.host`	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. 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 `host` attribute, specify the same host name as the value of CN in the LDAP directory server certificate. You cannot use an IP address. Default value: none
`auth.radius.`*`auth.server.name-property-value`*`.port`	Specify the port number for RADIUS server authentication. Make sure beforehand that the port you specify is set as the listen port number on the RADIUS server. Specifiable values: 1 to 65535 Default value: 1812
`auth.radius.`*`auth.server.name-property-value`*`.timeout`	Specify the amount of time to wait before timing out when connecting to the RADIUS server. Specifiable values: 1 to 65535 (seconds) Default value: 1
`auth.radius.`*`auth.server.name-`	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.

Property names	Details
property-value.retry.times	Specifiable values: 0 to 50 Default value: 3
auth.radius.*auth.server.name-property-value*.attr.NAS-IP-Address	Specify the IPv4 address of the Analyzer server. The RADIUS server uses this attribute value to identify the Analyzer server. If the format of the address is invalid, this property is disabled. You must specify exactly one of the following: attr.NAS-IP-Address, attr.NAS-IPv6-Address, or attr.NAS-Identifier. Default value: none
auth.radius.*auth.server.name-property-value*.attr.NAS-IPv6-Address	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 ([ ]). If the format of the address is invalid, this property is disabled. You must specify exactly one of the following: attr.NAS-IP-Address, attr.NAS-IPv6-Address, or attr.NAS-Identifier. Default value: none
auth.radius.*auth.server.name-property-value*.attr.NAS-Identifier	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. You must specify exactly one of the following: attr.NAS-IP-Address, attr.NAS-IPv6-Address, or attr.NAS-Identifier. Specifiable values: Specify no more than 253 bytes of the following characters: A to Z a to z 0 to 9 ! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ ` { | } ~ 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
`auth.server.type`	Specify an external authentication server type. Specify `radius`. Default value: `internal` (do not connect to an external authentication server)

`auth.server.name`	Specify the server identification names of RADIUS servers. You can specify any name for this property in order to identify which RADIUS servers the settings such as the port number and the protocol for connecting to the RADIUS server are applied to. `ServerName` has been set as the initial value. You must specify at least one name. When configuring a redundant configuration, separate the server identification name of each server with a comma (`,`). Do not register the same server identification name more than once.
	Specifiable values: No more than 64 bytes of the following characters:
	`A` to `Z`
	`a` to `z`
	`0` to `9`
	`! # ( ) + - . = @ [ ] ^ _ { } ~`
	Default value: none

`auth.group.mapping`	Specify whether to also connect to an external authorization server (LDAP directory server). Specify `true` (connect). Default value: `false` (do not connect)
`auth.ocsp.enable`	Specify whether or not to verify the validity of an LDAP directory server electronic signature certificate by using an OCSP responder when the LDAP directory server and STARTTLS are used for communication. If you want to verify the validity of certificates, specify `true`. To not verify the validity of certificates, specify `false`. Default value: `false`
`auth.ocsp.responderURL`	Specify the URL of an OCSP responder if you want to use an OCSP responder that is not the one written in the AIA field of the electronic signature certificate to verify the validity of the electronic signature certificate. If this value is omitted, the OCSP responder written in the AIA field is used. Default value: none

Property names	Details
`auth.radius.`*`auth.server.name-property-value`*`.protocol`	Specify the protocol for RADIUS server authentication. This attribute is required. Specifiable values: `PAP` or `CHAP` Default value: none
`auth.radius.`*`auth.server.name-property-value`*`.host`	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. 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 `host` attribute, specify the same host name as the value of CN in the LDAP directory server certificate. You cannot use an IP address. Default value: none
`auth.radius.`*`auth.server.name-property-value`*`.port`	Specify the port number for RADIUS server authentication. Make sure beforehand that the port you specify is set as the listen port number on the RADIUS server. Specifiable values: 1 to 65535 Default value: 1812
`auth.radius.`*`auth.server.name-property-value`*`.timeout`	Specify the amount of time to wait before timing out when connecting to the RADIUS server. Specifiable values: 1 to 65535 (seconds) Default value: 1
`auth.radius.`*`auth.server.name-property-value`*`.retry.times`	Specify the number of retries to attempt when an attempt to connect to the RADIUS server fails. If you specify 0, no retries are attempted. Specifiable values: 0 to 50 Default value: 3
`auth.radius.`*`auth.server.name-property-value`*`.attr.NAS-IP-Address`	Specify the IPv4 address of the Analyzer server. The RADIUS server uses this attribute value to identify the Analyzer server. If the format of the address is invalid, this property is disabled. You must specify exactly one of the following: `attr.NAS-IP-Address`, `attr.NAS-IPv6-Address`, or `attr.NAS-Identifier`.

Property names	Details
	Default value: none
`auth.radius.`*`auth.server.name-property-value`*`.attr.NAS-IPv6-Address`	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 (`[ ]`). If the format of the address is invalid, this property is disabled. You must specify exactly one of the following: `attr.NAS-IP-Address`, `attr.NAS-IPv6-Address`, or `attr.NAS-Identifier`. Default value: none

`auth.radius.`*`auth.server.name-property-value`*`.attr.NAS-Identifier`	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.
	You must specify exactly one of the following: `attr.NAS-IP-Address`, `attr.NAS-IPv6-Address`, or `attr.NAS-Identifier`.
	Specifiable values: Specify no more than 253 bytes of the following characters:
	`A` to `Z`
	`a` to `z`
	`0` to `9`
	`! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [ \ ] ^ _ ` { | } ~`
	Default value: none

`auth.radius.`*`auth.server.name-property-value`*`.domain.name`	Specify the name of a domain managed by the LDAP directory server (external authorization server). This attribute is required. Default value: none
`auth.radius.`*`auth.server.name-property-value`*`.dns_lookup`	Specify whether to use the DNS server to look up the information about the LDAP directory server (external authorization server). Specify `false` (do not look up the information). Default value: `false` (do not look up the information)
`auth.group.`*`domain-name`*`.protocol`	Specify the protocol for connecting to the LDAP directory server (external authorization server). When communicating in cleartext, specify `ldap`. When using STARTTLS communication, specify `tls`.

Property names	Details
	Before specifying `tls`, 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. ▪ TLS_RSA_WITH_AES_256_GCM_SHA384 ▪ TLS_RSA_WITH_AES_256_CBC_SHA256 ▪ TLS_RSA_WITH_AES_256_CBC_SHA ▪ TLS_RSA_WITH_AES_128_CBC_SHA256 ▪ TLS_RSA_WITH_AES_128_CBC_SHA Specifiable values: `ldap` or `tls` Default value: `ldap`
`auth.group.`*`domain-name`*`.host`	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 (`[ ]`). If you omit this attribute, the external authentication server and the external authorization server are assumed to be running on the same computer. When the external authentication server and the external authorization server are running on different computers and when using STARTTLS as the protocol for connecting to the LDAP directory server, in the `host` attribute specify the same host name as the value of CN in the LDAP directory server certificate. You cannot use an IP address. Default value: none
`auth.group.`*`domain-name`*`.port`	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. Specifiable values: 1 to 65535 Default value: 389

Property names	Details
`auth.group.`*`domain-name`*`.basedn`	Specify the BaseDN, which is the DN of the entry that will be used as the start point when searching for LDAP user information on the LDAP directory server (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. 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. Spaces `# + ; , < = > \` If characters that must be escaped are included in the specified BaseDN, escape all of those characters correctly because the specified value will be passed to the LDAP directory server without change. If you omit this attribute, the value specified in the `defaultNamingContext` property of Active Directory is assumed as the BaseDN. Default value: none
`auth.group.`*`domain-name`*`.timeout`	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. Specifiable values: 0 to 120 (seconds) Default value: 15
`auth.group.`*`domain-name`*`.retry.interval`	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
`auth.group.`*`domain-name`*`.retry.times`	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 *`domain-name`*, specify the value specified for `auth.radius.`*`auth.server.name-property-value`*`.domain.name`.	

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
`auth.server.type`	Specify an external authentication server type. Specify `radius`. Default value: `internal` (do not connect to an external authentication server)

`auth.server.name`	Specify the server identification names of RADIUS servers. You can specify any name for this property in order to identify which RADIUS servers the settings such as the port number and the protocol for connecting to the RADIUS server are applied to. `ServerName` has been set as the initial value. You must specify at least one name. When configuring a redundant configuration, separate the server identification name of each server with a comma (`,`). Do not register the same server identification name more than once.
	Specifiable values: No more than 64 bytes of the following characters:
	`A` to `Z`
	`a` to `z`
	`0` to `9`
	`! # ( ) + - . = @ [ ] ^ _ { } ~`
	Default value: none

`auth.group.mapping`	Specify whether to also connect to an external authorization server (LDAP directory server). Specify `true` (connect). Default value: `false` (do not connect)
`auth.radius.`*`auth.server.name-property-value`*`.protocol`	Specify the protocol for RADIUS server authentication. This attribute is required. Specifiable values: `PAP` or `CHAP` Default value: none

Property names	Details
`auth.radius.`*`auth.server.name-property-value`*`.host`	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. 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 `host` attribute, specify the same host name as the value of CN in the LDAP directory server certificate. You cannot use an IP address. Default value: none
`auth.radius.`*`auth.server.name-property-value`*`.port`	Specify the port number for RADIUS server authentication. Make sure beforehand that the port you specify is set as the listen port number on the RADIUS server. Specifiable values: 1 to 65535 Default value: 1812
`auth.radius.`*`auth.server.name-property-value`*`.timeout`	Specify the amount of time to wait before timing out when connecting to the RADIUS server. Specifiable values: 1 to 65535 (seconds) Default value: 1
`auth.radius.`*`auth.server.name-property-value`*`.retry.times`	Specify the number of retries to attempt when an attempt to connect to the RADIUS server fails. If you specify 0, no retries are attempted. Specifiable values: 0 to 50 Default value: 3
`auth.radius.`*`auth.server.name-property-value`*`.attr.NAS-IP-Address`	Specify the IPv4 address of the Analyzer server. The RADIUS server uses this attribute value to identify the Analyzer server. If the format of the address is invalid, this property is disabled. You must specify exactly one of the following: `attr.NAS-IP-Address`, `attr.NAS-IPv6-Address`, or `attr.NAS-Identifier`. Default value: none
`auth.radius.`*`auth.server.name-property-`*	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 (`[ ]`). If the format of the address is invalid, this property is disabled.

Property names	Details
value.attr.NAS-IPv6-Address	You must specify exactly one of the following: attr.NAS-IP-Address, attr.NAS-IPv6-Address, or attr.NAS-Identifier. Default value: none
auth.radius.*auth.server.name-property-value*.attr.NAS-Identifier	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. You must specify exactly one of the following: attr.NAS-IP-Address, attr.NAS-IPv6-Address, or attr.NAS-Identifier. Specifiable values: Specify no more than 253 bytes of the following characters: A to Z a to z 0 to 9 ! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ ` { | } ~ Default value: none
auth.radius.*auth.server.name-property-value*.domain.name	Specify the name of a domain managed by the LDAP directory server (external authorization server). This attribute is required. Default value: none
auth.radius.*auth.server.name-property-value*.dns_lookup	Specify whether to use the DNS server to look up the information about the LDAP directory server (external authorization server). Specify true (look up the information). However, if the following attribute values are already set, the LDAP directory server will be connected to by using the user-specified values instead of by using the DNS server to look up the information. ▪ auth.group.*domain-name*.host ▪ auth.group.*domain-name*.port Default value: false (do not look up the information)
auth.group.*domain-name*.protocol	Specify the protocol for connecting to the LDAP directory server (external authorization server). Specifiable values: ldap

Property names	Details
	Default value: `ldap`
`auth.group.`*`domain-name`*`.basedn`	Specify the BaseDN, which is the DN of the entry that will be used as the start point when searching for LDAP user information on the LDAP directory server (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. 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. Spaces `# + ; , < = > \` If characters that must be escaped are included in the specified BaseDN, escape all of those characters correctly because the specified value will be passed to the LDAP directory server without change. If you omit this attribute, the value specified in the `defaultNamingContext` property of Active Directory is assumed as the BaseDN. Default value: none
`auth.group.`*`domain-name`*`.timeout`	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. Specifiable values: 0 to 120 (seconds) Default value: 15
`auth.group.`*`domain-name`*`.retry.interval`	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
`auth.group.`*`domain-name`*`.retry.times`	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 *`domain-name`*, specify the value specified for `auth.radius.`*`auth.server.name-property-value`*`.domain.name`.	

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 264)

  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 266)

  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 root permission.
- 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 directory.

      `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:

      `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 **`hcmds64ldapuser`** command to register the LDAP search user account.

   ```
   Common-component-installation-destination-directory/bin/hcmds64ldapuser -
   set -dn DN-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.

   ```
   Common-component-installation-destination-directory/bin/hcmds64ldapuser -
   list
   ```

   Tip:

   To delete the LDAP search user account from the Analyzer server, run the **`hcmds64ldapuser`** command with the `delete` option.

3. Run the **`hcmds64checkauth`** command to confirm whether connections to the external authentication server and the external authorization server can be established properly.

   ```
   Common-component-installation-destination-directory/bin/hcmds64checkauth [-
   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 316)
	Obtain Kerberos server information from the DNS server.	Settings for using DNS to connect to a Kerberos server (on page 318)
Yes	Directly specify information about the Kerberos server.	Settings for connecting directly to a Kerberos server and an authorization server (on page 319)
	Obtain Kerberos server information from the DNS server.	Settings for using DNS to connect to a Kerberos server and an authorization server (on page 323)

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
`auth.server.type`	Specify an external authentication server type. Specify `kerberos`. Default value: `internal` (do not connect to an external authentication server)
`auth.group.mapping`	Specify whether to also connect to an external authorization server (LDAP directory server). Specify `false` (do not connect). Default value: `false` (do not connect)
`auth.kerberos.default_realm`	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
`auth.kerberos.dns_lookup_kdc`	Specify whether to use the DNS server to look up the information about the Kerberos server. Specify `false` (do not look up the information). Default value: `false` (do not look up the information)
`auth.kerberos.default_tkt_enctypes`	Specify the encryption type used for Kerberos authentication.
`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)

Property names	Details
	Default value: 300
`auth.kerberos.timeout`	Specify the amount of time to wait before timing out when connecting to the Kerberos server. If you specify 0, the system waits until a communication error occurs without timing out. Specifiable values: 0 to 120 (seconds) Default value: 3
`auth.kerberos.realm_name`	Specify the realm identification names. You can specify any name for this attribute in order to identify which realms the property attribute settings are applied to. You must specify at least one name. When specifying multiple realm identification names, separate the names with commas (`,`). Do not register the same realm identification name more than once. Default value: none
`auth.kerberos.`*`auth.kerberos.realm_name-property-value`*`.realm`	Specify the name of the realm set in the Kerberos server. This attribute is required. Default value: none
`auth.kerberos.`*`auth.kerberos.realm_name-property-value`*`.kdc`	Specify the information about the Kerberos server in the following format: *`host-name-or-IP-address`*`[:`*`port-number`*`]` This attribute is required. ***`host-name-or-IP-address`*** If you specify the host name, make sure beforehand that the name can be resolved to an IP address. If you specify the IP address, use an IPv4 address. In an IPv6 environment, you must specify the host name. Note that you cannot specify the loopback address (`localhost` or `127.0.0.1`). 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. ***`port-number`*** Make sure beforehand that the port you specify is set as the listen port number on the Kerberos server. If you do not specify a port number or the specified port number cannot be used in a Kerberos server, `88` is assumed.

Property names	Details
	When configuring the Kerberos server in redundant configuration, separate the servers with commas (`,`) as follows: *host-name-or-IP-address*[:*port-number*],*host-name-or-IP-address*[:*port-number*], ...

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
`auth.server.type`	Specify an external authentication server type. Specify `kerberos`. Default value: `internal` (do not connect to an external authentication server)
`auth.group.mapping`	Specify whether to also connect to an external authorization server (LDAP directory server). Specify `false` (do not connect). Default value: `false` (do not connect)
`auth.kerberos.default_realm`	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
`auth.kerberos.dns_lookup_kdc`	Specify whether to use the DNS server to look up the information about the Kerberos server. Specify `true` (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. ▪ `auth.kerberos.realm_name` ▪ `auth.kerberos.`*auth.kerberos.realm_name-property-value*`.realm` ▪ `auth.kerberos.`*auth.kerberos.realm_name-property-value*`.kdc` Default value: `false` (do not look up the information)

Property names	Details
`auth.kerberos.default_tkt_enctypes`	Specify the encryption type used for Kerberos authentication.
`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.timeout`	Specify the amount of time to wait before timing out when connecting to the Kerberos server. If you specify 0, the system waits until a communication error occurs without timing out. Specifiable values: 0 to 120 (seconds) Default value: 3

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
`auth.server.type`	Specify an external authentication server type. Specify `kerberos`. Default value: `internal` (do not connect to an external authentication server)
`auth.group.mapping`	Specify whether to also connect to an external authorization server (LDAP directory server). Specify `true` (connect). Default value: `false` (do not connect)
`auth.ocsp.enable`	Specify whether or not to verify the validity of an LDAP directory server electronic signature certificate by using an OCSP responder when the LDAP directory server and STARTTLS are used for communication. If you want to verify the validity of certificates, specify `true`. To not verify the validity of certificates, specify `false`. Default value: `false`

Property names	Details
`auth.ocsp.responderURL`	Specify the URL of an OCSP responder if you want to use an OCSP responder that is not the one written in the AIA field of the electronic signature certificate to verify the validity of the electronic signature certificate. If this value is omitted, the OCSP responder written in the AIA field is used. Default value: none
`auth.kerberos.default_realm`	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
`auth.kerberos.dns_lookup_kdc`	Specify whether to use the DNS server to look up the information about the Kerberos server. Specify `false` (do not look up the information). Default value: `false` (do not look up the information)
`auth.kerberos.default_tkt_enctypes`	Specify the encryption type used for Kerberos authentication.
`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.timeout`	Specify the amount of time to wait before timing out when connecting to the Kerberos server. If you specify 0, the system waits until a communication error occurs without timing out. Specifiable values: 0 to 120 (seconds) Default value: 3
`auth.kerberos.realm_name`	Specify the realm identification names. You can specify any name for this attribute in order to identify which realms the property attribute settings are applied to. You must specify at least one name. When specifying multiple realm identification names, separate the names with commas (`,`). Do not register the same realm identification name more than once. Default value: none
`auth.kerberos.`*`auth.kerberos.realm_name-property-value`*`.realm`	Specify the name of the realm set in the Kerberos server. This attribute is required. Default value: none

Property names	Details
`auth.kerberos.`*`auth.kerberos.realm_name-property-value`*`.kdc`	Specify the information about the Kerberos server in the following format: *`host-name-or-IP-address`*`[:`*`port-number`*`]` This attribute is required. ***host-name-or-IP-address*** If you specify the host name, make sure beforehand that the name can be resolved to an IP address. If you specify the IP address, use an IPv4 address. In an IPv6 environment, you must specify the host name. Note that you cannot specify the loopback address (`localhost` or `127.0.0.1`). 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. ***port-number*** Make sure beforehand that the port you specify is set as the listen port number on the Kerberos server. If you do not specify a port number or the specified port number cannot be used in a Kerberos server, `88` is assumed. When configuring the Kerberos server in redundant configuration, separate the servers with commas (`,`) as follows: *`host-name-or-IP-address`*`[:`*`port-number`*`],`*`host-name-or-IP-address`*`[:`*`port-number`*`], ...`
`auth.group.`*`realm-name`*`.protocol`	Specify the protocol for connecting to the LDAP directory server (external authorization server). When communicating in cleartext, specify `ldap`. When using STARTTLS communication, specify `tls`. Before specifying `tls`, 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. ▪ TLS_RSA_WITH_AES_256_GCM_SHA384 ▪ TLS_RSA_WITH_AES_256_CBC_SHA256 ▪ TLS_RSA_WITH_AES_256_CBC_SHA

Property names	Details
	▪ TLS_RSA_WITH_AES_128_CBC_SHA256 ▪ TLS_RSA_WITH_AES_128_CBC_SHA Specifiable values: `ldap` or `tls` Default value: `ldap`
`auth.group.`*`realm-name`*`.port`	Specify the port number of the LDAP directory server. Make sure beforehand that the port you specify is set as the listen port number on the LDAP directory server. Specifiable values: 1 to 65535 Default value: 389
`auth.group.`*`realm-name`*`.basedn`	Specify the BaseDN, which is the DN of the entry that will be used as the start point when searching for LDAP user information on the LDAP directory server (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. 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. Spaces `# + ; , < = > \` If characters that must be escaped are included in the specified BaseDN, escape all of those characters correctly because the specified value will be passed to the LDAP directory server without change. If you omit this attribute, the value specified in the `defaultNamingContext` property of Active Directory is assumed as the BaseDN. Default value: none
`auth.group.`*`realm-name`*`.timeout`	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. Specifiable values: 0 to 120 (seconds) Default value: 15
`auth.group.`*`realm-name`*`.retry.interval`	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)

Property names	Details
	Default value: 1
`auth.group.`*`realm-name`*`.retry.times`	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 *`realm-name`*, specify the value specified for `auth.kerberos.`*`auth.kerberos.realm_name-property-value`*`.realm`.	

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
`auth.server.type`	Specify an external authentication server type. Specify `kerberos`. Default value: `internal` (do not connect to an external authentication server)
`auth.group.mapping`	Specify whether to also connect to an external authorization server (LDAP directory server). Specify `true` (connect). Default value: `false` (do not connect)
`auth.kerberos.default_realm`	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
`auth.kerberos.dns_lookup_kdc`	Specify whether to use the DNS server to look up the information about the Kerberos server. Specify `true` (look up the information). This attribute is required.

Property names	Details
	However, if all the following attributes values are already set, the Kerberos server will not be looked up by using the DNS server. ▪ `auth.kerberos.realm_name` ▪ `auth.kerberos.`*`auth.kerberos.realm_name-property-value`*`.realm` ▪ `auth.kerberos.`*`auth.kerberos.realm_name-property-value`*`.kdc` Default value: `false` (do not look up the information)
`auth.kerberos.default_tkt_enctypes`	Specify the encryption type used for Kerberos authentication.
`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.timeout`	Specify the amount of time to wait before timing out when connecting to the Kerberos server. If you specify 0, the system waits until a communication error occurs without timing out. Specifiable values: 0 to 120 (seconds) Default value: 3

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 must 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.

The supported authentication and communication protocols for Active Directory are:

- Authentication protocol: LDAP
- Communication protocols:
  - TLS/SSL: LDAPS
  - Without SSL: Plain text (non-TLS)

Configuring the SSL port

The SSL port is enabled and the non-SSL port is disabled while connecting to the Active Directory server.

Before you begin

Note: If you do not want to stop the **crond** service, you can stop 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 440) and Starting the Analyzer detail view server or Analyzer probe server services (on page 439)

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. Navigate to the Java keystore directory. For example:

   ```
   cd /usr/java/jdk1.8.0_291-amd64/jre/lib/security
   ```

7. If the `jssecacerts` file does not exist, create it.

8. Import the certificate into the Analyzer detail view server or Analyzer probe server using the command:

```
keytool -importcert -alias Alias_name -keystore Truststore_file_path -storetype
jks -storepass Truststore_file_password -file
Active_Directory_Server_certificate_or_MSPKI_chain_certificate_file_path
```

Note: You can define any unique alias name for the certificate.

For example:

```
keytool -importcert -alias detailviewAD -keystore jssecacerts -storetype jks -
storepass changeit -file /tmp/LAB_chain.cer
```

9. Make sure that the megha user has the read permission for the `jssecacerts` file. If not, change the permission as follows.

   For example:

```
chmod o+r jssecacerts
```

10. Stop the crond service and verify the status:

```
service crond stop
```

```
service crond status
```

11. Stop the megha service and verify the status:

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

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

12. Start the megha service and verify the status:

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

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

13. Start the crond service and verify the status:

```
service crond start
```

```
service crond status
```

> **Note:** If you upgrade the JDK in the future, make sure that the `jssecacerts` file is copied to the upgraded JDK directory.
>
> For example: If you upgrade JDK from v1.7.0 to v1.8.0, copy the `jssecacerts` file from `/usr/java/jdk1.8.0_291-amd64/jre/lib/security` to `/usr/java/jdk1.8.0_251-amd64/jre/lib/security`.
>
> After copying the `jssecacerts` file, make sure that megha user has the read permission for the `jssecacerts` file. If not, set it as in this example:
>
> ```
> chmod o+r jssecacerts
> ```

14. 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`

Note: The `simple` authentication type is supported for `ad.auth.type` property.

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
```

Setting an explicit domain name for Active Directory

To enhance the security, you can use an explicit User Principal Name (UPN) domain name on the Analyzer detail view server and Analyzer probe server.

Note: If you do not want to stop the **crond** service, you can stop 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 440) and Starting the Analyzer detail view server or Analyzer probe server services (on page 439)

Procedure

1. Log on to the Analyzer probe server or 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. Go to the `/usr/local/megha/conf` directory:

```
cd /usr/local/megha/conf
```

6. (If the `custom` directory does not exist) create it as follows:

```
mkdir custom
```

7. (If the `custom.properties` file does not exist), create it in the `custom` directory.
8. Change ownership of the custom directory:

```
chown -R megha:megha /usr/local/megha/conf/custom
```

9. Open the `custom.properties` file and add the `ad.domain.mappings` property with the implicit and explicit domain name:

```
ad.domain.mappings=Explicit_Domain:Implicit_Domain
```

   For example:

```
ad.domain.mappings=marsh.com:domain1.com
```

   To map multiple explicit domain names, separate them with commas:

   For example:

```
ad.domain.mappings=marsh.com:domain1.com,marsh1.com:domain1.com
```

10. Save the changes.

11. Start the megha service using the command:

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

12. Start the crond service using the following command:

```
service crond 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. You must type the username in the following format:

   user-name@FQDN

   For example: `smith@corp.company`

   Note: The Active Directory group user can log in to the Analyzer detail view or Analyzer probe using the *user-name@FQDN* and *FQDN\user-name* formats. The *NetBIOS-Name\user-name* format is not supported.

   All users from the specified Active Directory group are registered with Analyzer detail view (as Normal users) or Analyzer probe (as Admin users) and can access the UI by using the Active Directory logon credentials.
6. Click **Submit**.

Chapter 12: Configure secure communications

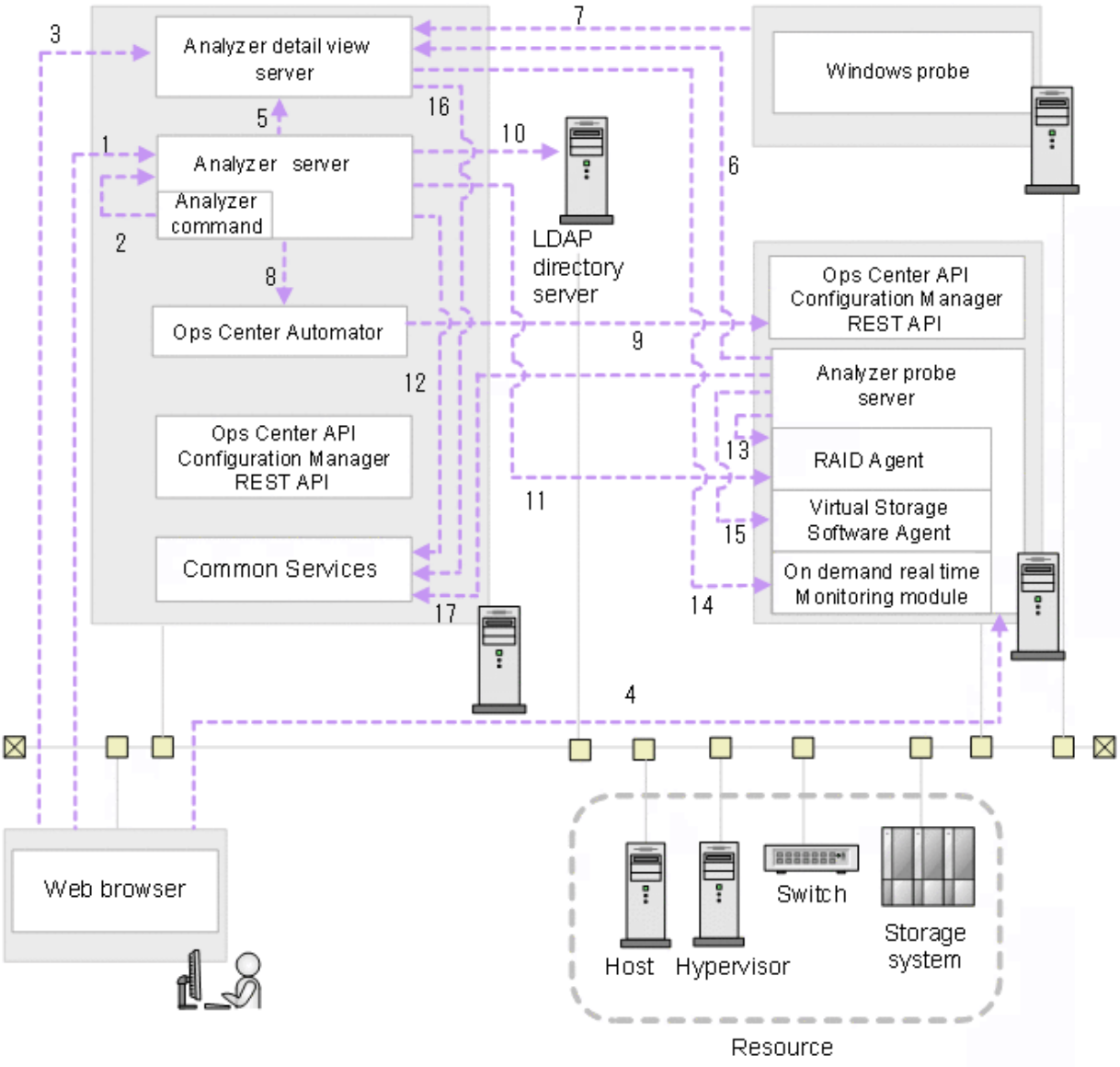
You can configure secure communications between each of the servers and clients.

If you use an instance of Common Services that is installed on the same host, you can use a Common Services command to create a common private key and server certificate, and configure SSL communications for Ops Center products installed on the same host. For details, see the *Hitachi Ops Center Installation and Configuration Guide*.

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[1]	Web client	HTTPS
2	Analyzer server[1]	Analyzer command	HTTPS
3	Analyzer detail view server[1]	Web client	HTTPS
4	Analyzer probe server	Web client	HTTPS
5	Analyzer detail view server[1]	Analyzer server[1]	HTTPS

Route	Server (program)	Client	Protocol
6	Analyzer detail view server[1]	Analyzer probe server	HTTPS SFTP
7	Analyzer detail view server[1]	Windows host	HTTPS
8	Ops Center Automator[1]	Analyzer server[1]	HTTPS
9	Ops Center API Configuration Manager	Ops Center Automator[1]	HTTPS
10	LDAP directory server	Analyzer server[1]	STARTTLS
11	RAID Agent	Analyzer server[1]	HTTPS SSH
12	Ops Center Common Services[1]	Analyzer server[1]	HTTPS
13	RAID Agent	Analyzer probe server	HTTPS
14	On-demand real time monitoring module[2]	Analyzer detail view server[1]	WSS (Web Socket over TLS)
15	Virtual Storage Software Agent	Analyzer probe server	HTTPS
16	Ops Center Common Services[1]	Analyzer detail view server[1]	HTTPS
17	Ops Center Common Services	Analyzer probe server	HTTPS

1. You can configure this component by using the **`cssslsetup`** command if the products are installed on the same management server as Common Services.
2. Certificate validation for the On-demand real time monitoring module cannot be configured by using the **`cssslsetup`** command.

By default, server certificates are not verified. For secure communication, enable verification.

If you use a certificate issued by a certificate authority, use the information in this module to enhance security.

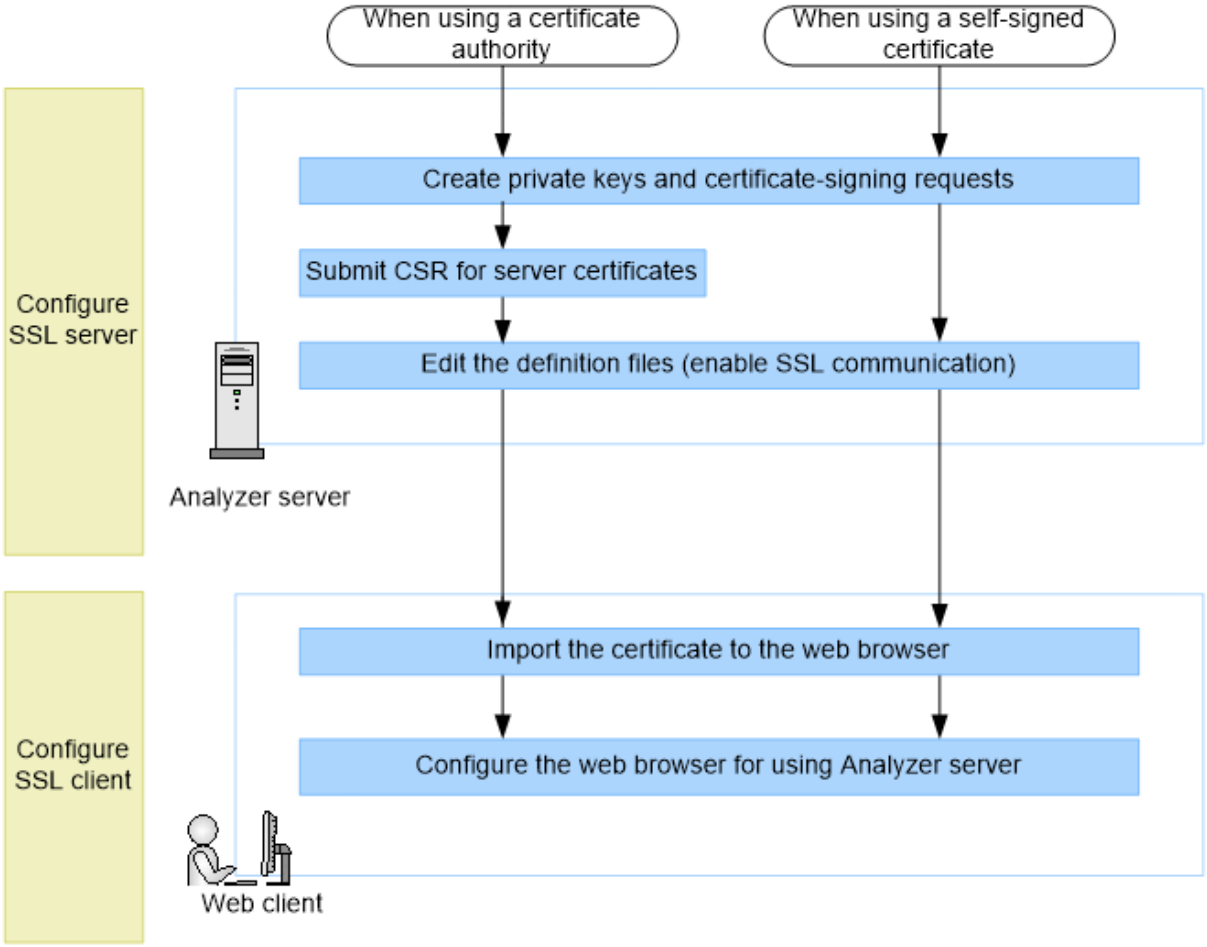
> **Note:**
>
> To use Ops Center Analyzer with security settings enabled, the server certificate must be valid. If the server certificate has expired, you cannot connect to Ops Center Analyzer using a secure connection.

- 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 9, see the *Hitachi Ops Center API Configuration Manager REST API Reference Guide*.
- For security settings for communication route 11, see the Initial setup for enabling Granular Data Collection (on page 134).

Workflow for configuring secure communications

The following figure describes the workflow for configuring secure communication in the Ops Center Analyzer environment.

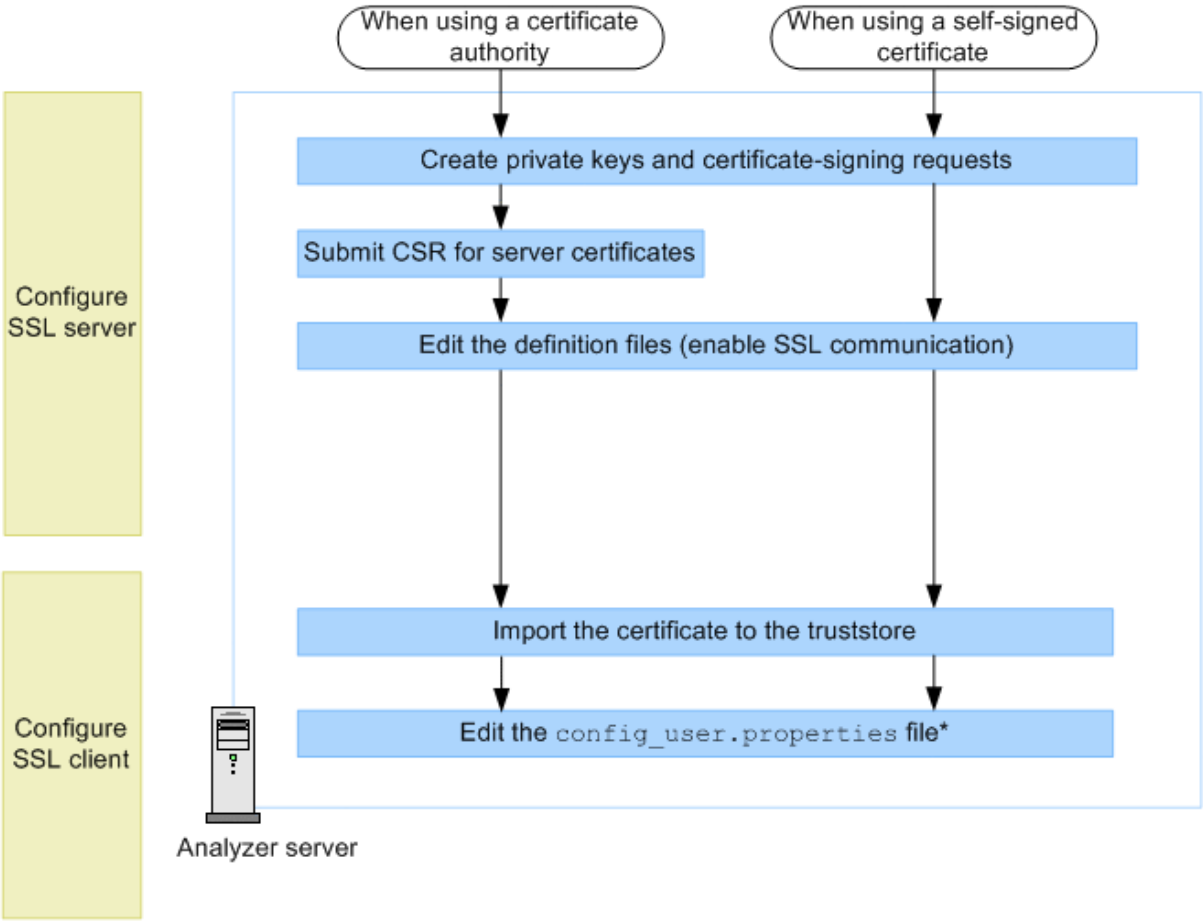
Configuration workflow for secure communication between the Analyzer server and the web client



Analyzer server procedures:

- Creating a private key and a certificate signing request for Analyzer server (on page 352)
- Submitting a certificate signing request (CSR) for Analyzer server (on page 352)
- Enabling SSL communication for Analyzer server (on page 353)

Configuration workflow for secure communication between the Analyzer server and the Analyzer command

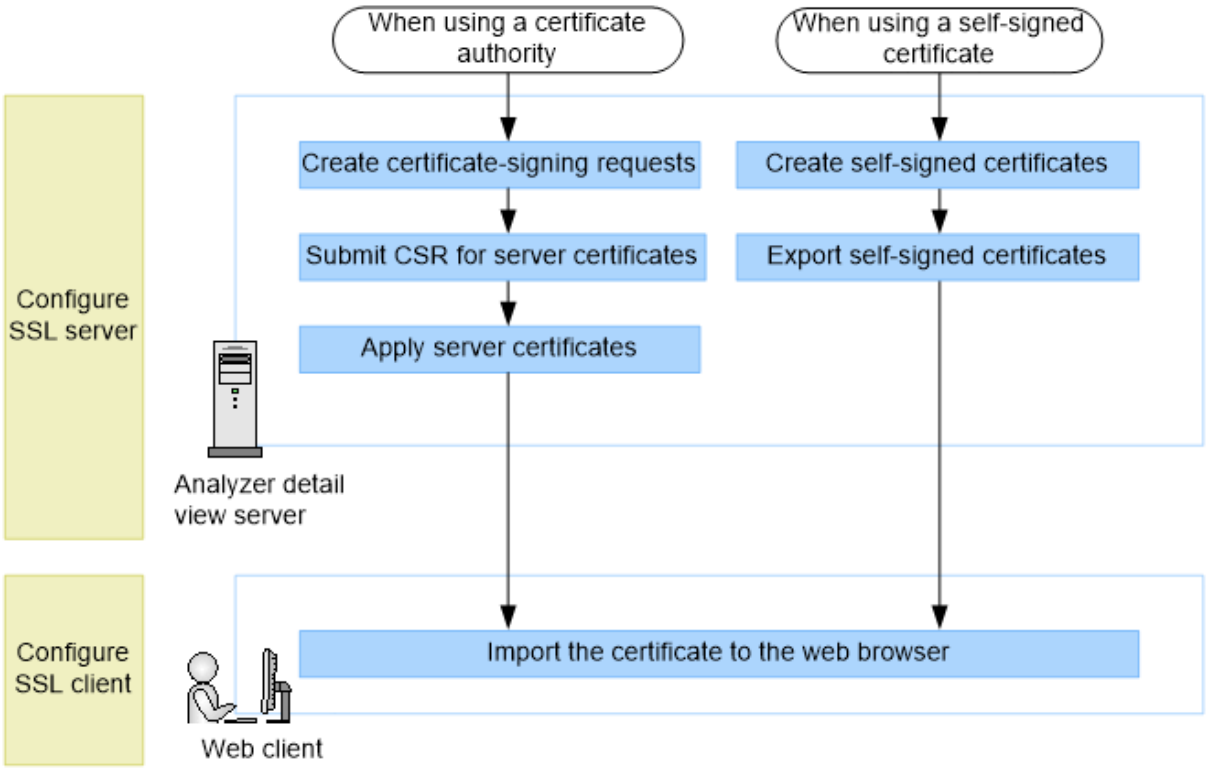


* This procedure is required for enabling verification of the server certificate. This is disabled by default.

Analyzer server procedures:

- Creating a private key and a certificate signing request for Analyzer server (on page 352)
- Submitting a certificate signing request (CSR) for Analyzer server (on page 352)
- Enabling SSL communication for Analyzer server (on page 353)
- Importing Analyzer server certificates to the Analyzer server truststore (on page 357)

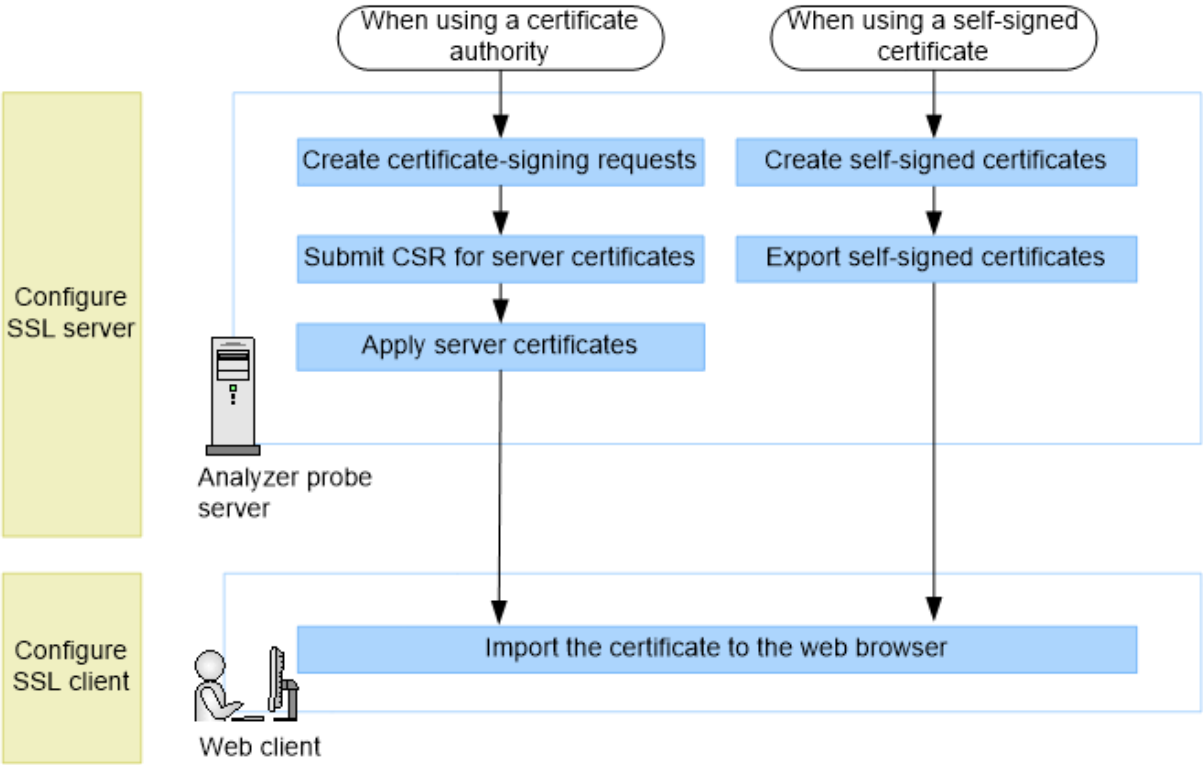
Configuration workflow for secure communication between the Analyzer detail view server and the web client



Analyzer detail view server procedures:

- Configuring a CA signed SSL certificate (Analyzer detail view server) (on page 358)
- Configuring a self-signed SSL certificate (Analyzer detail view server) (on page 362)
- Exporting a self-signed certificate for the Analyzer detail view server (on page 365)

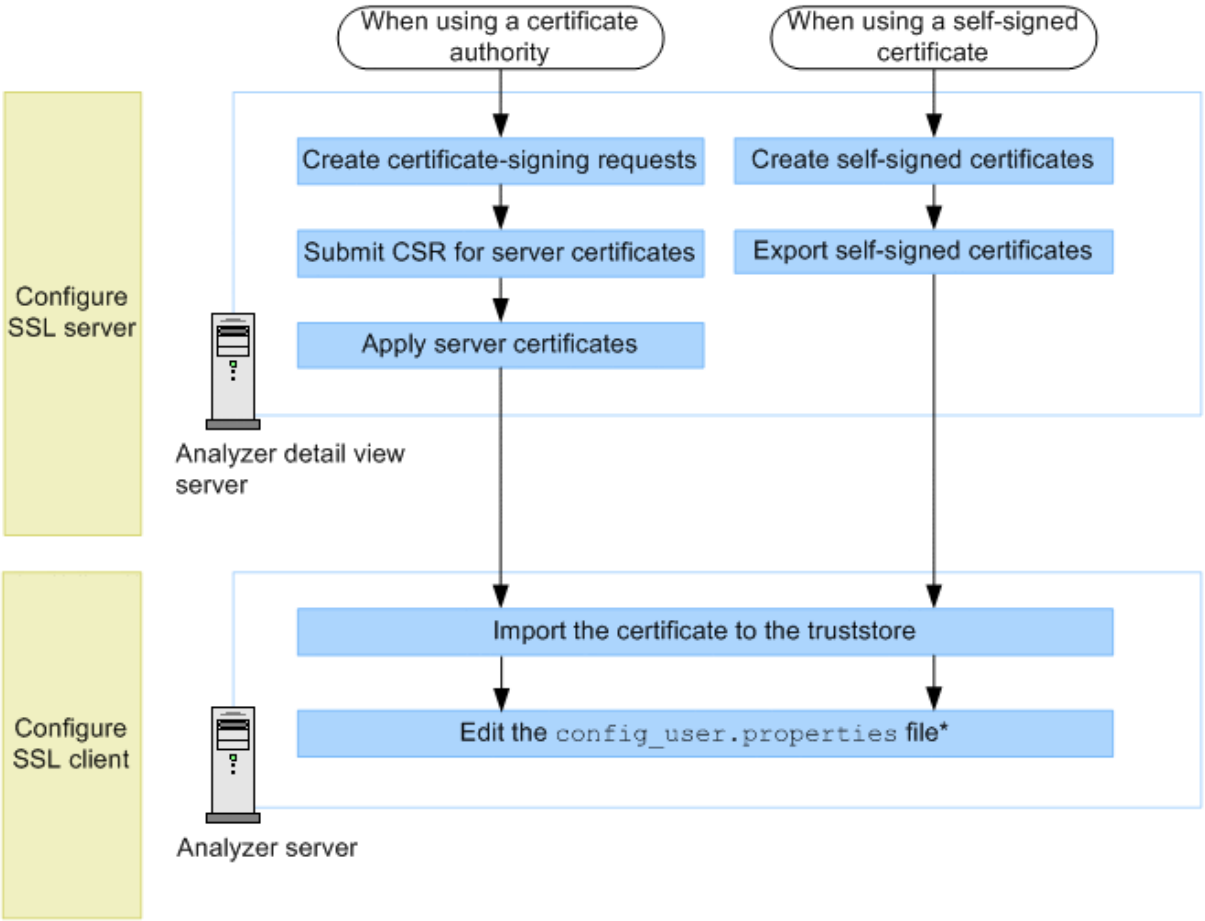
Configuration workflow for secure communication between the Analyzer probe server and the web client



Analyzer probe server procedures:

- Configuring a CA signed SSL certificate (Analyzer probe server) (on page 370)
- Configuring a self-signed SSL certificate (Analyzer probe server) (on page 374)
- Exporting a self-signed certificate for the Analyzer probe server (on page 377)

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.

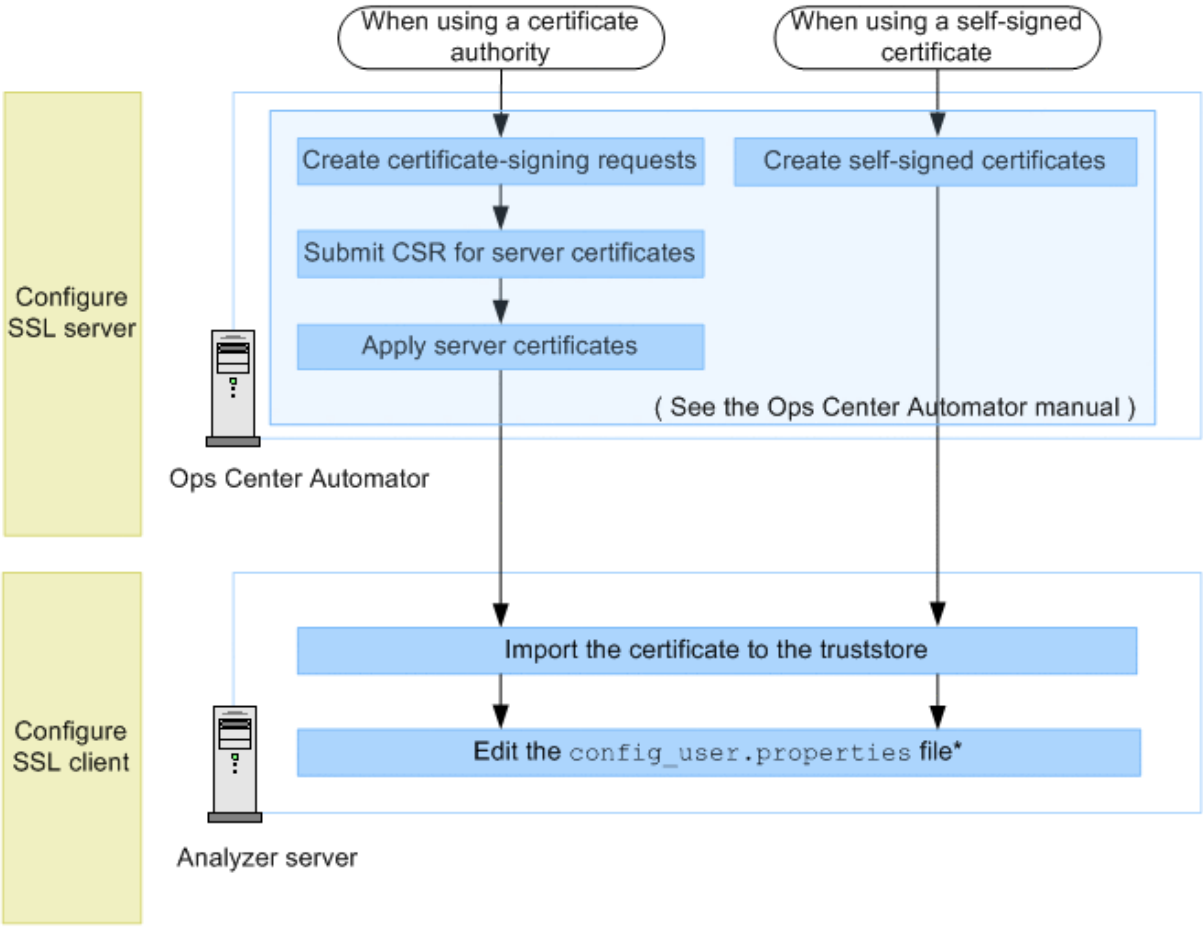
Analyzer detail view server procedures:

- Configuring a CA signed SSL certificate (Analyzer detail view server) (on page 358)
- Configuring a self-signed SSL certificate (Analyzer detail view server) (on page 362)
- Exporting a self-signed certificate for the Analyzer detail view server (on page 365)

Analyzer server procedures:

- Importing Analyzer detail view server certificates to the Analyzer server truststore (on page 368)

Configuration workflow for secure communication between the Ops Center Automator and Analyzer server

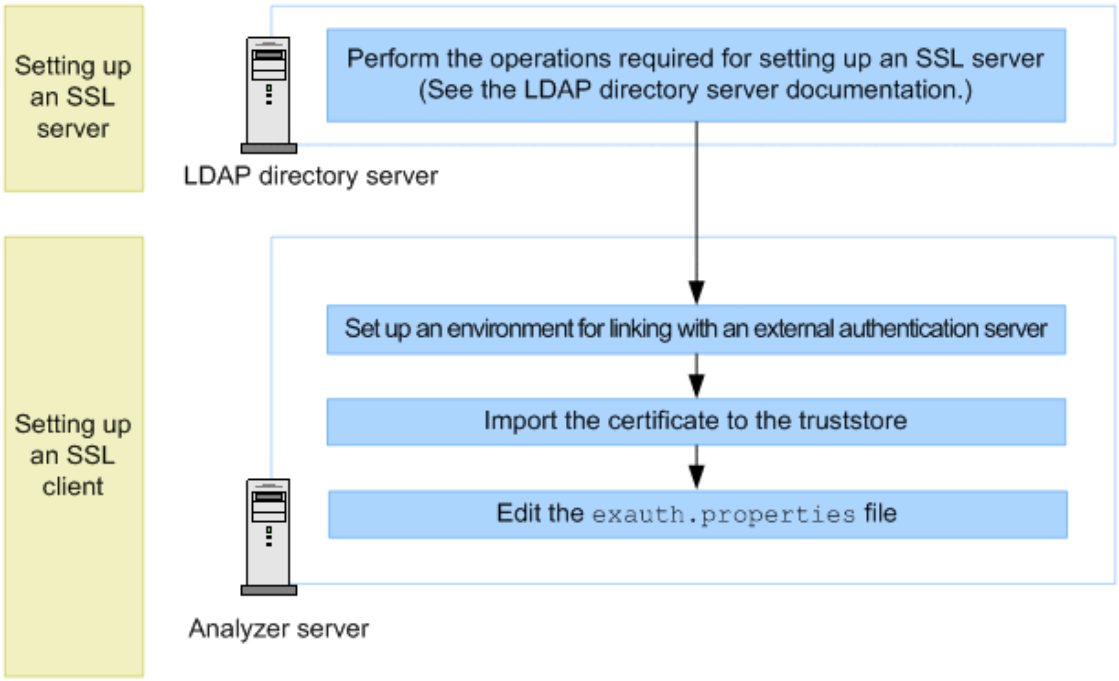


* This procedure is required for enabling verification of the server certificate. This is disabled by default.

Analyzer server procedures:

- Importing Ops Center Automator certificates to the Analyzer server truststore (on page 401)

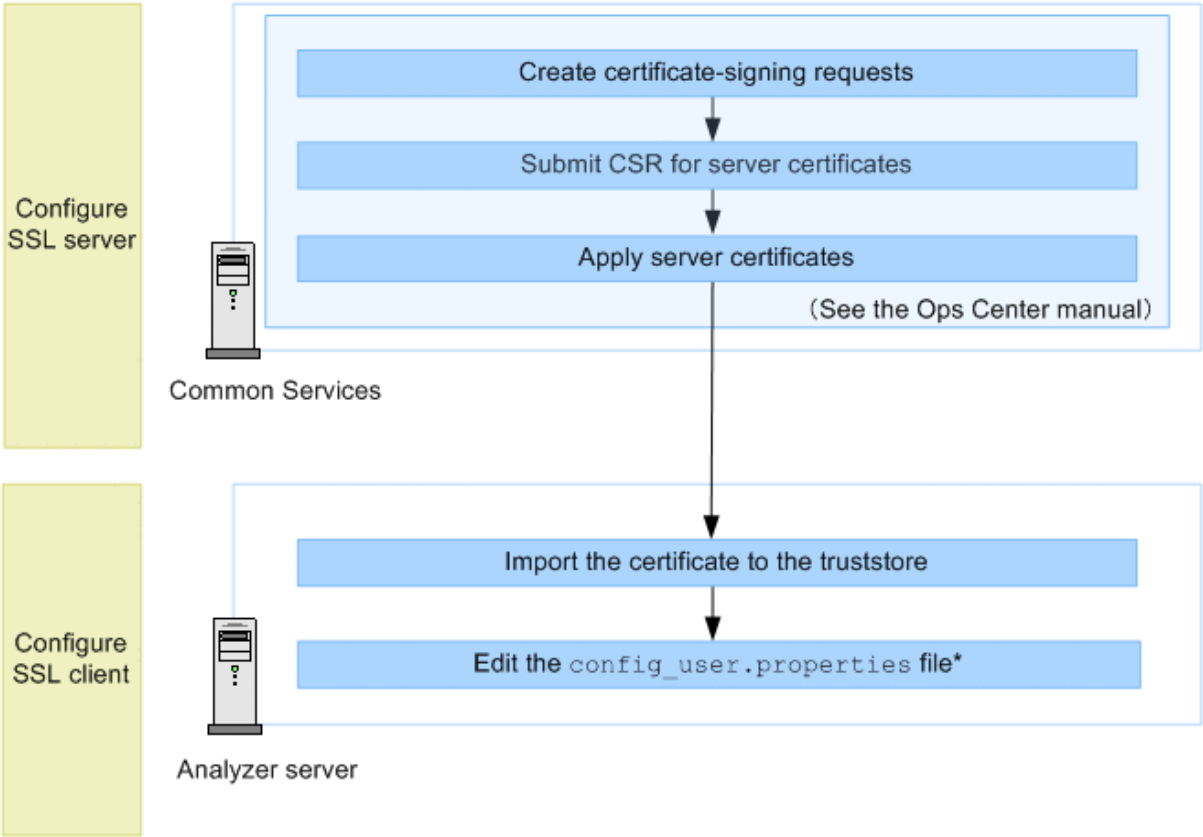
Configuration workflow for secure communication between the LDAP directory server and Analyzer server



Analyzer server procedures:

- Importing LDAP directory server certificates to the Analyzer server truststore (on page 402)

Configuration workflow for secure communication between the Analyzer server and Common Services

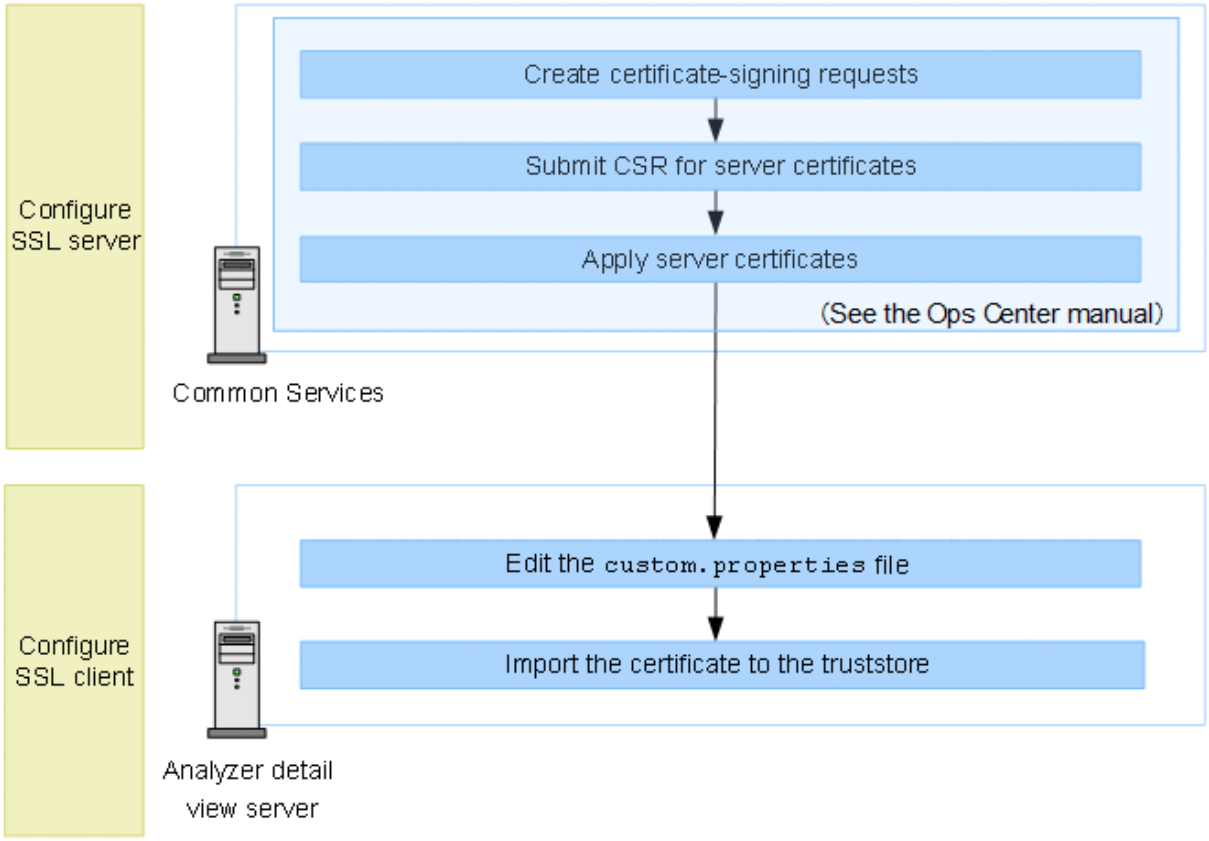


* This procedure is required for enabling verification of the server certificate. This is disabled by default.

Analyzer server procedures:

- Importing Common Services certificates to the Analyzer server truststore (on page 404)

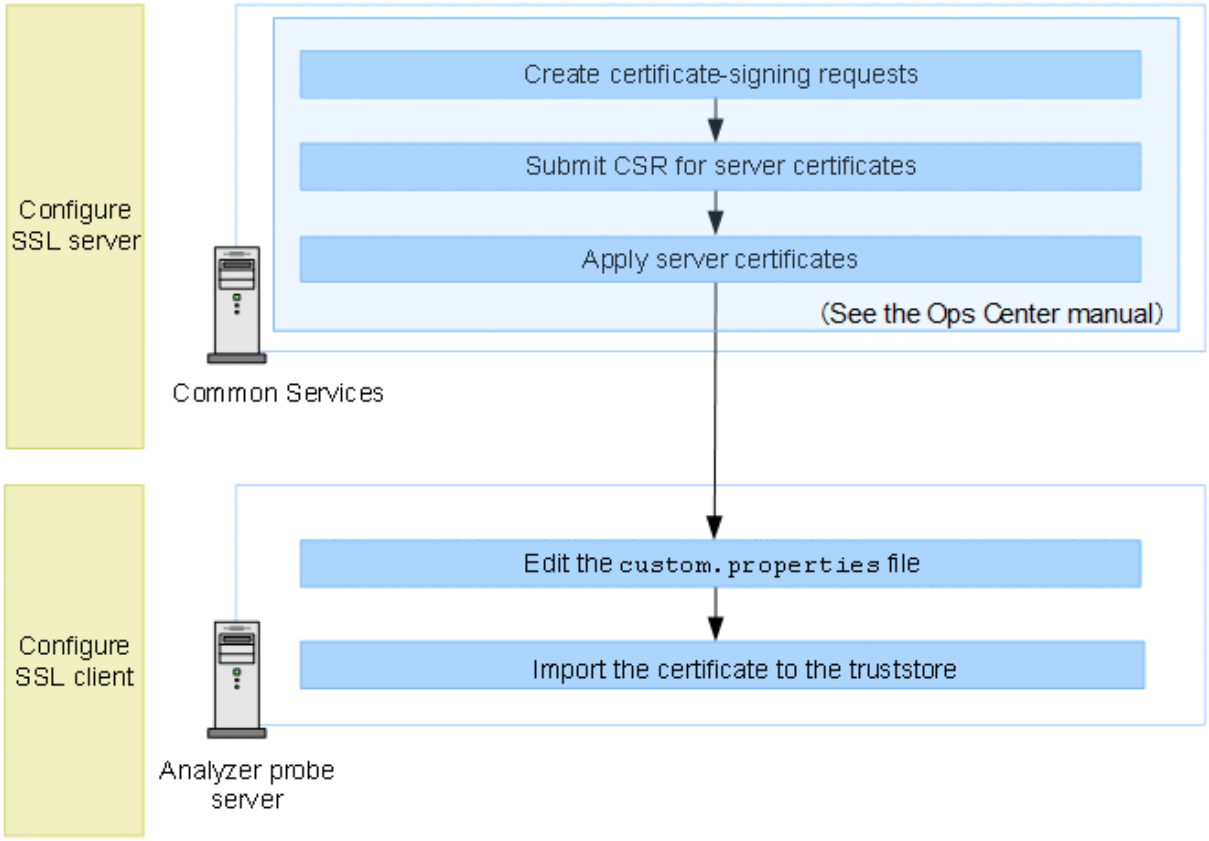
Configuration workflow for secure communication between the Analyzer detail view server and Common Services



Analyzer detail view server procedures:

- Enabling TLS certificate verification for connecting to Common Services (on page 405)

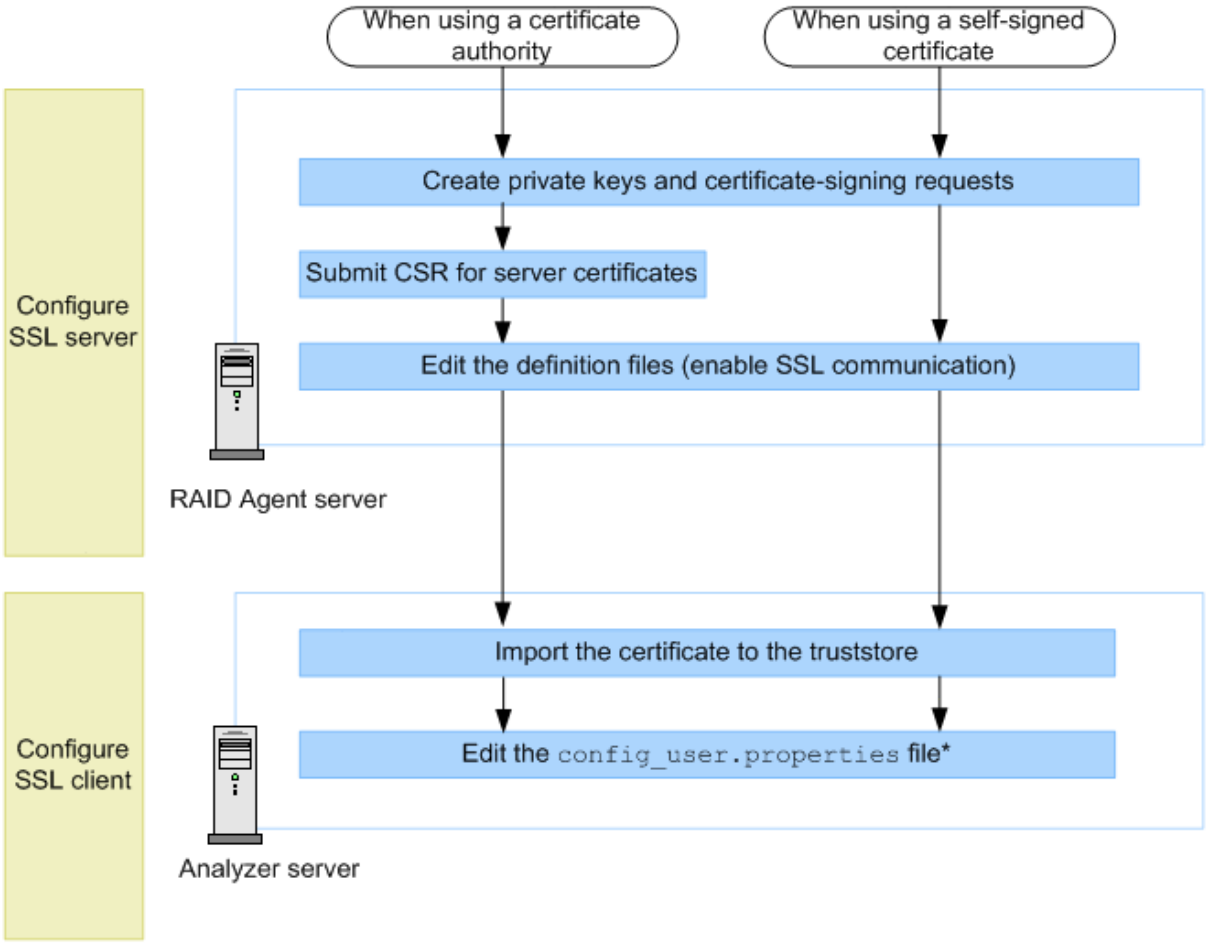
Configuration workflow for secure communication between the Analyzer probe server and Common Services



Analyzer probe server procedures:

- Enabling TLS certificate verification for connecting to Common Services (on page 405)

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.

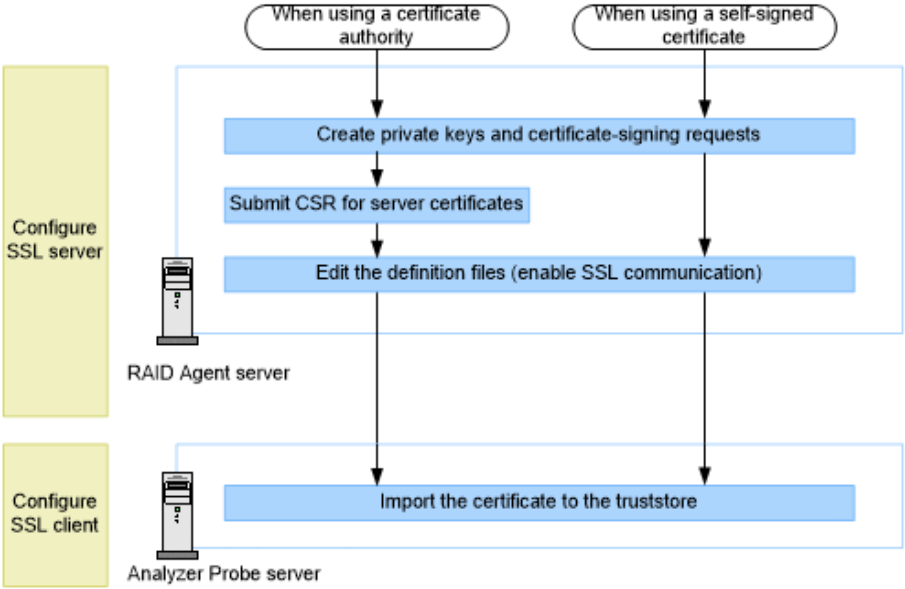
RAID Agent server procedures:

- Creating a private key and a certificate signing request for RAID Agent server (on page 407)
- Submitting a certificate signing request (CSR) for RAID Agent (on page 408)
- Enabling SSL communication for RAID Agent (on page 409)

Analyzer server procedures:

- Importing RAID Agent certificates to the Analyzer server truststore (on page 411)

Configuration workflow for secure communication between the RAID Agent server and Analyzer probe server



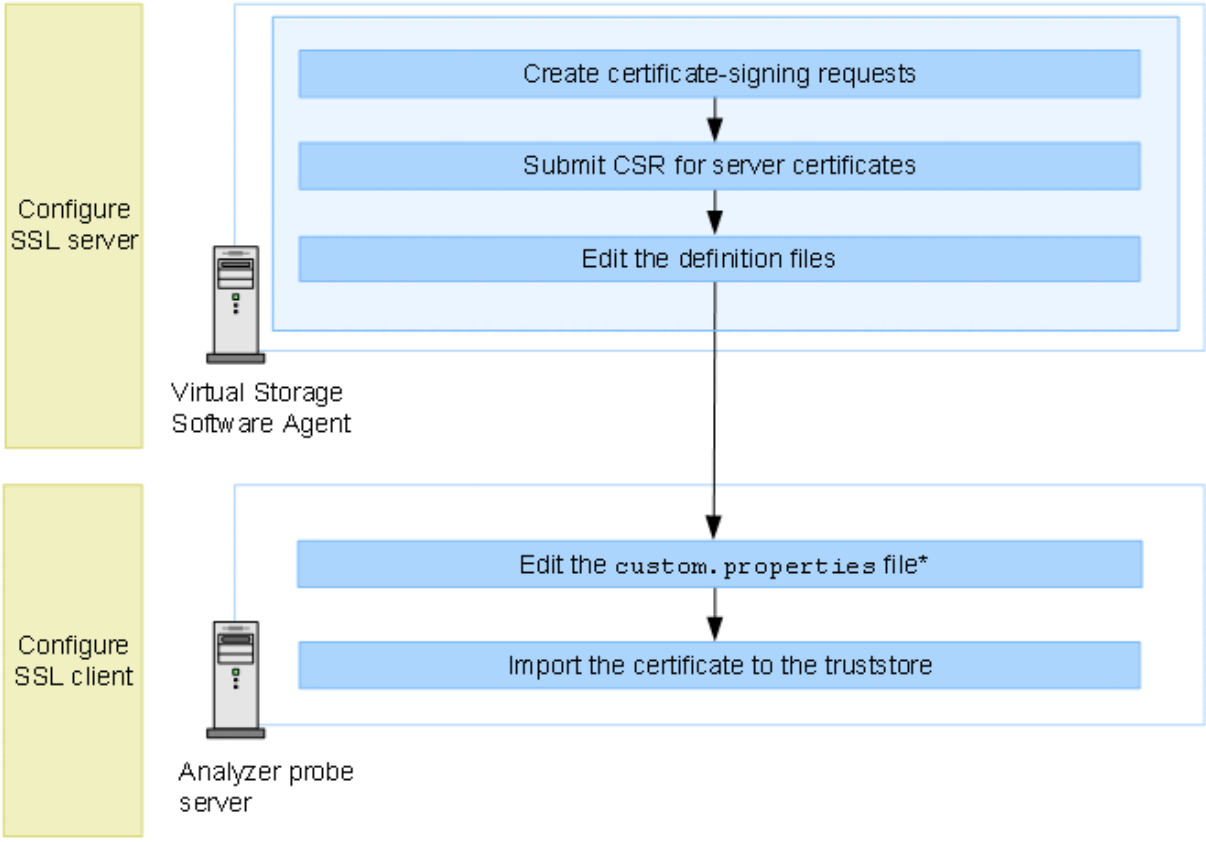
RAID Agent server procedures:

- Creating a private key and a certificate signing request for RAID Agent server (on page 407)
- Submitting a certificate signing request (CSR) for RAID Agent (on page 408)
- Enabling SSL communication for RAID Agent (on page 409)

Analyzer probe server procedures:

- Importing RAID Agent certificates to the Analyzer probe server truststore (on page 412)

Configuration workflow for secure communication between Virtual Storage Software Agent server and Analyzer probe server



* This procedure is required for enabling verification of the server certificate. This is disabled by default.

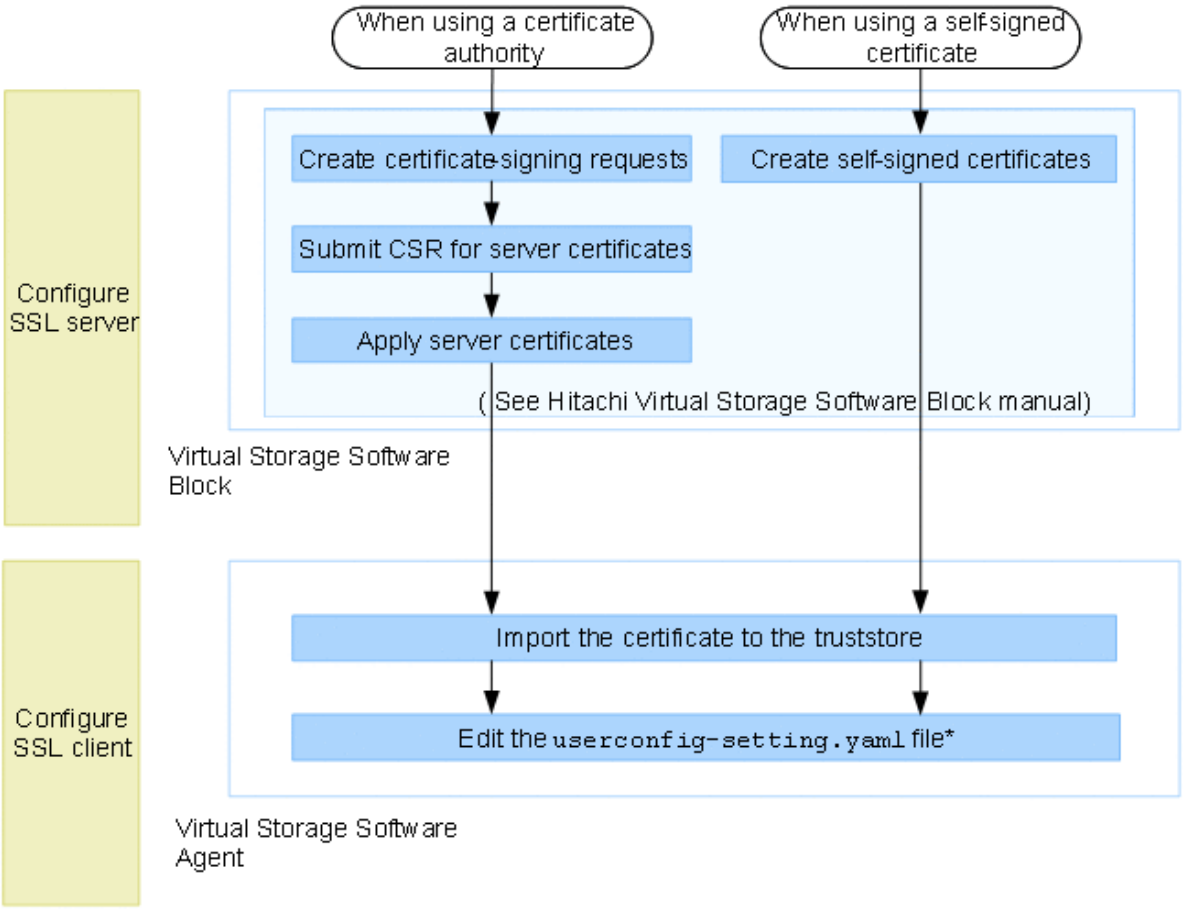
Virtual Storage Software Agent procedures:

- Creating a private key and a certificate signing request for Virtual Storage Software Agent server (on page 414)
- Submitting a certificate signing request (CSR) for Virtual Storage Software Agent (on page 414)
- Enabling SSL communication for Virtual Storage Software Agent (on page 415)

Analyzer probe server procedures:

- Enabling TLS certificate verification for connecting to Virtual Storage Software Agent (on page 416)

Configuration workflow for secure communication between the Virtual Storage Software Block and Virtual Storage Software Agent



* This procedure is required for enabling verification of the server certificate. This is disabled by default.

Virtual Storage Software Agent procedures:

- Importing Virtual Storage Software Block certificates to the Virtual Storage Software Agent truststore (on page 418)

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 **`hcmds64ssltool`** command to create a private key and a certificate signing request (CSR) for Analyzer server.

Before you begin

- You must have root permission.
- 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 recreating 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 recreated.)

Procedure

1. Run the **`hcmds64ssltool`** 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 are created by running the **`hcmds64ssltool`** command with no arguments 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. You must 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 in X.509 PEM format issued by the certificate authority. For details on how to apply, see the website of your certificate authority. In addition, make sure the certificate authority supports the signature algorithm.

Procedure

1. Send the certificate signing request to the certificate authority.
2. Save the server certificate 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 issued by the certificate authority.

  We recommend that you copy the file to the following location:

  Common-component-installation-destination-directory/uCPSB11/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.

   Common-component-installation-destination-directory/uCPSB11/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
SSLEngine Off
#Listen [::]:22016
Listen 22016
<VirtualHost *:22016>
  ServerName Analyzer-server-host-name
  SSLEngine On
  SSLProtocol +TLSv1.2 +TLSv1.3
  SSLCipherSuite TLSv1.3
TLS_AES_128_GCM_SHA256:TLS_AES_256_GCM_SHA384:TLS_CHACHA20_POLY1305_SHA256
#  SSLCipherSuite 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
  SSLCipherSuite ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-GCM-
SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256
  SSLCertificateKeyFile "Common-component-installation-destination-directory/
uCPSB11/httpsd/conf/ssl/server/httpsdkey.pem"
  SSLCertificateFile "Common-component-installation-destination-directory/
```

```
uCPSB11/httpsd/conf/ssl/server/httpsd.pem"
  SSLCertificateKeyFile "Common-component-installation-destination-directory/
uCPSB11/httpsd/conf/ssl/server/ecc-httpsdkey.pem"
  SSLCertificateFile "Common-component-installation-destination-directory/
uCPSB11/httpsd/conf/ssl/server/ecc-httpsd.pem"
#  SSLCACertificateFile "Common-component-installation-destination-directory/
uCPSB11/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 (`#`). For the `SSLCipherSuite` directive, uncomment only one of these lines depending on the encryption set to be used. For example, if you want to use only the encryption set that corresponds to PFS (Perfect Forward Secrecy), uncomment the second of these lines.

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.)
- Specify the absolute paths of the secret key and the server certificate of Analyzer server for the following directives.
  - `SSLCertificateKeyFile`
  - `SSLCertificateFile`
- 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 the Analyzer server was upgraded, `user_httpsd.conf` might not include the required directives. In this case, copy the lines relevant to those directives from the sample file stored in the following location:
>
> *`Common-component-installation-destination-directory/`*`sample/httpsd/conf/user_httpsd.conf`

Note the following:

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

   `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 Ops Center Automator host.

   To apply the changed port number:

   a. Run the **`hcmds64prmset`** command with `sslport` option to change the Common component settings.
   b. Restart Ops Center Automator.

   > **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*.

Checking the expiration date of the certificate for Analyzer server

Use the **`hcmds64checkcerts`** 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 root permission.

Procedure

1. Run the following command:

```
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 `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 root permission.

Procedure

1. Run the following command to delete the certificate that was imported to Analyzer server.

```
Common-component-installation-destination-directory/uCPSB11/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:

  Common-component-installation-destination-directory/uCPSB11/hjdk/jdk/lib/security/jssecacerts

Importing Analyzer server certificates to the Analyzer server truststore

To enable the Analyzer server to verify Analyzer server certificates, import the Analyzer server certificates to the Analyzer server truststore.

Enabling the verification of certificates makes it possible to use HTTPS for communication for the following commands.

- **encryptpassword**
- **reloadtemplate**

Before you begin

- Prepare the Analyzer server certificates.
- You must have root permission.

Procedure

1. Stop the Analyzer server services.
2. Run the following command to import the Analyzer server certificates to the truststore:

   ```
   Common-component-installation-destination-directory/uCPSB11/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 is located.
   - For the *certificate-file-name*, specify the absolute path to the certificate.
   - The truststore file is stored in the following location:

     Common-component-installation-destination-directory/uCPSB11/hjdk/jdk/lib/security/jssecacerts
   - The default truststore password is changeit.
   - You must specify JKS for the keystore type.
3. Change the following properties in the config_user.properties file.

   Location:

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

To enable the verification of server certificates:

- Key: `cert.verify.enabled`
- Value: `true`

4. Change the following properties in the `command_user.properties` file.
   Location:

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

   To set the host name of the Analyzer server that is accessed by Analyzer commands:

   - Key: `command.hostname`
   - Value: *Analyzer-server-host-name*

5. Start the Analyzer server services.

Configuring an SSL certificate (Analyzer detail view server)

Configure an SSL certificate to initiate a secure browser sessions. You can either configure the CA signed or self-signed SSL certificate.

Configuring a CA signed SSL certificate (Analyzer detail view server)

Configure a CA signed SSL certificate to initiate a secure browser sessions 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. Navigate to the `/usr/local/megha/jetty/etc` directory:

```
cd /usr/local/megha/jetty/etc
```

3. Create a private key using one of the following algorithms:

   RSA:

```
openssl genrsa -out jettyPrivate.key
```

   ECDSA:

```
openssl ecparam -out jettyPrivate.key -name prime256v1 -genkey
```

4. Create a certificate signing request (CSR):

```
openssl req -new -key jettyPrivate.key -out /tmp/certreq.csr
```

   Follow the instructions displayed on the console to enter the details for your certificate request. When requested to provide the common name, make sure that you enter a fully qualified host name.

   Enter the default password for CSR: `megha.jeos`

   Note: If you provide a password of your choice, note it. You will need this when applying server certificates.

5. Copy the certificate request file from `/tmp/certreq.csr` and submit it to the certificate authority to create the certificate file.

Applying server certificates

The certificate authority creates the following three certificate files:

- Root
- Intermediate
- Host

Note: If you do not want to stop the **`crond`** service, you can stop 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 440) and Starting the Analyzer detail view server or Analyzer probe server services (on page 439)

Procedure

1. Upload the certificate files to the Analyzer detail view server. (For example, `/usr/local/megha/jetty/etc`).
2. Navigate to the `/usr/local/megha/jetty/etc` directory:

```
cd /usr/local/megha/jetty/etc
```

3. Combine the chain of certificates by concatenating them into a single file (in the order indicated). For example:

```
cat host.cer imd.cer root.cer > cert-chain.cer
```

4. Combine the private key and certificate in the `jetty.pkcs12` file using the following command:

```
openssl pkcs12 -export -inkey jettyPrivate.key -in cert-chain.cer -out
jetty.pkcs12 -name jetty
```

5. Enter the password that you provided when creating the CSR (default: `megha.jeos`).

6. Stop the crond service using the command:

```
service crond stop
```

7. Stop all the running services using the following command:

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

8. Verify that the megha and crond services are stopped by entering these commands:

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

```
service crond status
```

9. Create a backup of the existing keystore file using the following command:

```
cp /usr/local/megha/jetty/etc/keystore /usr/local/megha/jetty/etc/keystore-orig
```

10. Create a backup of an existing `userKeystoreConfig` file using the following command:

```
cp /usr/local/megha/jetty/etc/userKeystoreConfig.xml /usr/local/megha/jetty/etc/
userKeystoreConfig-orig.xml
```

11. Import the `pkcs12` file (using keytool) using the following command:

```
keytool -importkeystore -srckeystore jetty.pkcs12 -srcstoretype PKCS12 -
destkeystore keystore -deststoretype PKCS12
```

12. Enter the password that you provided when creating the CSR (default: `megha.jeos`).

Note: If you provided a password of your choice when creating the CSR, make sure you change the following fields in the `/usr/local/megha/jetty/etc/userKeystoreConfig.xml` file.

```
KeyStorePassword
KeyManagerPassword
TrustStorePassword
```

If the password includes the following special characters, you must replace them as indicated when editing these fields:

- Replace ' " ' with '"'
- Replace ' ' ' with '''
- Replace ' < ' with '<'
- Replace ' > ' with '>'
- Replace ' & ' with '&'

For example:

- Replace `abc"123` with `abc"123`
- Replace `abc'123` with `abc'123`
- Replace `abc&"123` with `abc&"123`

(Optional): If you want an encrypted password for security purpose, you can convert the password into OBF format using the following command and provide the converted password in the `userKeystoreConfig.xml` file:

```
java -cp /usr/local/megha/jetty/lib/jetty-util-<Jetty Version>.jar
org.eclipse.jetty.util.security.Password
"password_provided_when_creating_CSR"
```

For example:

```
java -cp /usr/local/megha/jetty/lib/jetty-util-<Jetty Version>.jar
org.eclipse.jetty.util.security.Password "abc&123"
```

If the password contains " quotation mark, provide the password within ' ' quotation marks in the above command. For example: `'abc"123'`

13. Change the ownership and permission of the keystore file:

```
chown megha:megha /usr/local/megha/jetty/etc/keystore
```

```
chmod og-rwx /usr/local/megha/jetty/etc/keystore
```

14. Start the megha service using the following command:

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

15. Start the crond service using the following command:

```
service crond start
```

16. (Optional) Remove the `certreq.csr`, `cert-chain.cer`, and `jetty.pkcs12` files if you will not need them in the future:

```
rm /tmp/certreq.csr
rm /usr/local/megha/jetty/etc/cert-chain.cer
rm /usr/local/megha/jetty/etc/jetty.pkcs12
```

Configuring a self-signed SSL certificate (Analyzer detail view server)

You can configure a self-signed SSL certificate for browser sessions for test purpose by creating a private key, a certificate signing request (CSR), and applying the server certificate.

Procedure

1. Log on to the Analyzer detail view server through an SSH client (like **`putty`**) as a root user.
2. Create a temporary directory and open it:

```
mkdir /tmp/SelfSignedCertificate
```

```
cd /tmp/SelfSignedCertificate
```

3. Create a private key using one of the following algorithms:

   RSA:

```
openssl genrsa -out jettyPrivate.key
```

   ECDSA:

```
openssl ecparam -out jettyPrivate.key -name prime256v1 -genkey
```

4. Create a certificate signing request (CSR):

```
openssl req -new -key jettyPrivate.key -out certreq.csr
```

   Follow the instructions displayed on the console to enter the details for your certificate request (including the CSR password). For the common name, make sure that you enter the fully qualified host name.

5. Generate a self-signed certificate from the CSR:

```
openssl x509 -req -days 365 -in certreq.csr -signkey jettyPrivate.key -out
certreq.cer
```

6. Combine the private key and certificate in the `jetty.pkcs12` file as shown in the following example:

```
openssl pkcs12 -export -inkey jettyPrivate.key -in certreq.cer -out jetty.pkcs12
-name jetty
```

   Enter the export password. (The default is `megha.jeos`)

Note: If you do not use the default password, you must edit the `userKeystoreConfig.xml` file as follows:

a. Open the `userKeystoreConfig.xml` file:

```
vi /usr/local/megha/jetty/etc/userKeystoreConfig.xml
```

b. Update the following fields and save the file:

```
KeyStorePassword
KeyManagerPassword
TrustStorePassword
```

If the password includes the following special characters, you must replace them as indicated when editing these fields:

- Replace ' " ' with '"'
- Replace ' ' ' with '''
- Replace ' < ' with '<'
- Replace ' > ' with '>'
- Replace ' & ' with '&'

For example:

- Replace `abc"123` with `abc"123`
- Replace `abc'123` with `abc'123`
- Replace `abc&"123` with `abc&"123`

(Optional): If you want an encrypted password for security purpose, you can convert the password into OBF format using the following command and provide the converted password in the `userKeystoreConfig.xml` file:

```
java -cp /usr/local/megha/jetty/lib/jetty-util-<Jetty
Version>.jar org.eclipse.jetty.util.security.Password
"password_provided_when_creating_CSR"
```

For example:

```
java -cp /usr/local/megha/jetty/lib/jetty-util-<Jetty
Version>.jar org.eclipse.jetty.util.security.Password "abc&123"
```

If the password contains " quotation mark, provide the password within ' ' quotation marks in the above command. For example: `'abc"123'`

7. Stop the crond service:

```
service crond stop
```

8. Stop all the running services using the command:

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

9. Create a backup of the existing keystore file using the following command:

```
cp /usr/local/megha/jetty/etc/keystore /usr/local/megha/jetty/etc/keystore-orig
```

10. Import `jetty.pkcs12` into the keystore to import the self-signed certificate using the following command:

```
keytool -importkeystore -srckeystore jetty.pkcs12 -srcstoretype PKCS12 -
destkeystore /usr/local/megha/jetty/etc/keystore -deststoretype PKCS12
```

    Enter the destination and source keystore passwords you used in step 6.

11. Change the ownership and permission of the keystore file:

```
chown megha:megha /usr/local/megha/jetty/etc/keystore
```

```
chmod og-rwx /usr/local/megha/jetty/etc/keystore
```

12. Start the megha service using the command:

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

13. Start the crond service:

```
service crond start
```

14. (Optional) Remove the `SelfSignedCertificate` directory if you will not need it in the future:

```
cd /tmp
```

```
rm -rf /tmp/SelfSignedCertificate
```

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 or HTTPS port number of the Analyzer detail view server

To change the port number for SSL or HTTPS communication, you must change the port numbers specified in the definition file, and then open the new port in the firewall settings.

Before you begin

Note: If you do not want to stop the **`crond`** service, you can stop 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 440) and Starting the Analyzer detail view server or Analyzer probe server services (on page 439)

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
```

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` file:

```
cp /usr/local/megha/jetty/start.ini /usr/local/megha/jetty/org_start.ini.backup
```

6. Change the port number in the `/usr/local/megha/jetty/start.ini` file. For example:

```
jetty.httpConfig.securePort=9443

jetty.ssl.port=9443
```

7. Start the crond service using the following command:

```
service crond start
```

8. Start the megha service using the following command:

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

9. After changing the port number, make sure you change the firewall settings accordingly.

Next steps

If you are using the Common Services, make sure that you also update the port number using the `setupcommonservice` command to update the port number in Common Services.

Deleting an SSL certificate from the Keystore

You can delete a previously imported or exipred SSL certificate from the keystore.

Before you begin

Note: If you do not want to stop the **`crond`** service, you can stop 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 440) and Starting the Analyzer detail view server or Analyzer probe server services (on page 439)

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
```

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 self-signed certificates exported by the Analyzer detail view server or server certificates issued by

a certificate authority to the Analyzer server truststore, and edit the `config_user.properties` file.

Before you begin

You must have root permission.

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:

```
Common-component-installation-destination-directory/uCPSB11/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:

  `Common-component-installation-destination-directory/``uCPSB11/hjdk/jdk/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:

     `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 secure browser sessions. You can either configure the CA signed or self-signed SSL certificate.

Configuring a CA signed SSL certificate (Analyzer probe server)

Configure an SSL certificate to initiate secure browser sessions 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. Navigate to the `/usr/local/megha/jetty/etc` directory:

   ```
   cd /usr/local/megha/jetty/etc
   ```

3. Create a private key using one of the following algorithms:

   RSA:

   ```
   openssl genrsa -out jettyPrivate.key
   ```

   ECDSA:

   ```
   openssl ecparam -out jettyPrivate.key -name prime256v1 -genkey
   ```

4. Create a certificate signing request (CSR):

   ```
   openssl req -new -key jettyPrivate.key -out /tmp/certreq.csr
   ```

   Follow the instructions displayed on the console to enter the details for your certificate request. When requested to provide common name, make sure that you enter a fully qualified host name.

   Enter default password for CSR: `megha.jeos`

   Note: If you provide the password of your choice, note it. You will need this when applying server certificates.

5. Copy the certificate request file from `/tmp/certreq.csr` and submit it to the certificate authority to create the certificate file.

Applying server certificates

The certificate authority creates the following three certificate files:

- Root
- Intermediate
- Host

Note: If you do not want to stop the **crond** service, you can stop 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 440) and Starting the Analyzer detail view server or Analyzer probe server services (on page 439)

Procedure

1. Upload the certificate files to the Analyzer probe server. (For example, `(/usr/local/megha/jetty/etc`).
2. Navigate to the `/usr/local/megha/jetty/etc` directory:

```
cd /usr/local/megha/jetty/etc
```

3. Combine the chain of certificates by concatenating them into a single file (in the order indicated):

```
cat Host-Certificate Intermediate-Certificate Root-Certificate > cert-chain.cer
```

   For example:

```
cat host.cer imd.cer root.cer > cert-chain.cer
```

4. Combine the private key and certificate in the `jetty.pkcs12` file using the following command:

```
openssl pkcs12 -export -inkey jettyPrivate.key -in cert-chain.cer -out
jetty.pkcs12 -name jetty
```

5. Enter the password that you provided when creating the CSR. The default password is: `megha.jeos`
6. Stop the crond service using the command:

```
service crond stop
```

7. Stop all the running services using the command:

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

8. Verify that the megha and crond services are stopped by entering these commands:

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

```
service crond status
```

9. Take a backup of an existing keystore file using the command:

```
cp /usr/local/megha/jetty/etc/keystore /usr/local/megha/jetty/etc/keystore-orig
```

10. Take a backup of an existing `userKeystoreConfig` file using the command:

```
cp /usr/local/megha/jetty/etc/userKeystoreConfig.xml /usr/local/megha/jetty/etc/
userKeystoreConfig-orig.xml
```

11. Import the `pkcs12` file (using keytool) with the following command:

```
keytool -importkeystore -srckeystore jetty.pkcs12 -srcstoretype PKCS12 -
destkeystore keystore -deststoretype PKCS12
```

12. Enter the password that you provided when creating the CSR. The default password is:`megha.jeos`

Note: If you provided a password of your choice when creating the CSR, make sure you change the following fields in the `/usr/local/megha/jetty/etc/userKeystoreConfig.xml` file:

```
KeyStorePassword
KeyManagerPassword
TrustStorePassword
```

If the password includes the following special characters, you must replace them as indicated when editing these fields:

- Replace ' " ' with '"'
- Replace ' ' ' with '''
- Replace ' < ' with '<'
- Replace ' > ' with '>'
- Replace ' & ' with '&'

For example:

- Replace `abc"123` with `abc"123`
- Replace `abc'123` with `abc'123`
- Replace `abc&"123` with `abc&"123`

(Optional): If you want an encrypted password for security purpose, you can convert the password into OBF format using the following command and provide the converted password in the `userKeystoreConfig.xml` file:

```
java -cp /usr/local/megha/jetty/lib/jetty-util-<Jetty Version>.jar
org.eclipse.jetty.util.security.Password
"password_provided_when_creating_CSR"
```

For example:

```
java -cp /usr/local/megha/jetty/lib/jetty-util-<Jetty Version>.jar
org.eclipse.jetty.util.security.Password "abc&123"
```

If the password contains " quotation mark, provide the password within ' ' quotation marks in the above command. For example: `'abc"123'`

13. Change the ownership and permission of the keystore file:

```
chown megha:megha /usr/local/megha/jetty/etc/keystore
```

```
chmod og-rwx /usr/local/megha/jetty/etc/keystore
```

14. Start the megha service using the following command:

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

15. Start the crond service using the following command:

```
service crond start
```

16. (Optional) Remove the `certreq.csr`, `cert-chain.cer`, and `jetty.pkcs12` files if you will not need them in the future:

```
rm /tmp/certreq.csr
rm /usr/local/megha/jetty/etc/cert-chain.cer
rm /usr/local/megha/jetty/etc/jetty.pkcs12
```

Configuring a self-signed SSL certificate (Analyzer probe server)

You can configure a self-signed SSL certificate for browser sessions for test purpose by creating a private key, a certificate signing request (CSR), and applying the server certificate.

Procedure

1. Log on to the Analyzer probe server through an SSH client (like **`putty`**) as a root user.
2. Create a temporary directory and open it:

```
mkdir /tmp/SelfSignedCertificate
```

```
cd /tmp/SelfSignedCertificate
```

3. Create a private key using one of the following algorithms:

   RSA:

```
openssl genrsa -out jettyPrivate.key
```

   ECDSA:

```
openssl ecparam -out jettyPrivate.key -name prime256v1 -genkey
```

4. Create a certificate signing request (CSR):

```
openssl req -new -key jettyPrivate.key -out certreq.csr
```

   Follow the instructions displayed on the console to enter the details for your certificate request including the CSR password. For the common name, make sure that you enter the fully qualified host name.

5. Generate a self-signed certificate from the CSR:

```
openssl x509 -req -days 365 -in certreq.csr -signkey jettyPrivate.key -out
certreq.cer
```

6. Combine the private key and certificate in the `jetty.pkcs12` file as in the following example:

```
openssl pkcs12 -export -inkey jettyPrivate.key -in certreq.cer -out jetty.pkcs12
-name jetty
```

   Enter the export password. (The default is `megha.jeos`)

Note: If you do not use the default password, you must edit the `userKeystoreConfig.xml` file as follows:

a. Open the `userKeystoreConfig.xml` file:

```
vi /usr/local/megha/jetty/etc/userKeystoreConfig.xml
```

b. Update the following fields and save the file:

```
KeyStorePassword
KeyManagerPassword
TrustStorePassword
```

If the password includes the following special characters, you must replace them as indicated when editing these fields:

- Replace ' " ' with '"'
- Replace ' ' ' with '''
- Replace ' < ' with '<'
- Replace ' > ' with '>'
- Replace ' & ' with '&'

For example:

- Replace `abc"123` with `abc"123`
- Replace `abc'123` with `abc'123`
- Replace `abc&"123` with `abc&"123`

(Optional): If you want an encrypted password for security purpose, you can convert the password into OBF format using the following command and provide the converted password in the `userKeystoreConfig.xml` file:

```
java -cp /usr/local/megha/jetty/lib/jetty-util-<Jetty
Version>.jar org.eclipse.jetty.util.security.Password
"password_provided_when creating_CSR"
```

For example:

```
java -cp /usr/local/megha/jetty/lib/jetty-util-<Jetty
Version>.jar org.eclipse.jetty.util.security.Password "abc&123"
```

If the password contains " quotation mark, provide the password within ' ' quotation marks in the above command. For example: `'abc"123'`

7. Stop the crond service:

```
service crond stop
```

8. Stop all the running services using the command:

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

9. Take a backup of the existing keystore file using the command:

```
cp /usr/local/megha/jetty/etc/keystore /usr/local/megha/jetty/etc/keystore-orig
```

10. Import `jetty.pkcs12` into the keystore to import self-signed certificate in keystore with the following command:

```
keytool -importkeystore -srckeystore jetty.pkcs12 -srcstoretype PKCS12 -
destkeystore /usr/local/megha/jetty/etc/keystore -deststoretype PKCS12
```

    Enter the destination and source keystore passwords you used in step 6.

11. Change the ownership and permission of the keystore file:

```
chown megha:megha /usr/local/megha/jetty/etc/keystore
```

```
chmod og-rwx /usr/local/megha/jetty/etc/keystore
```

12. Start the megha service using the command:

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

13. Start the crond service:

```
service crond start
```

14. (Optional) Remove the `SelfSignedCertificate` directory if you will not need it in the future:

```
cd /tmp
```

```
rm -rf /tmp/SelfSignedCertificate
```

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 or HTTPS port number of the Analyzer probe server

To change the port number for SSL or HTTPS communication, you must change the port numbers specified in the definition file, and then open the new port in the firewall settings.

Before you begin

Note: If you do not want to stop the **`crond`** service, you can stop 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 440) and Starting the Analyzer detail view server or Analyzer probe server services (on page 439)

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 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` file:

```
cp /usr/local/megha/jetty/start.ini /usr/local/megha/jetty/org_start.ini.backup
```

6. Change the port number in the `/usr/local/megha/jetty/start.ini` file. For example:

```
jetty.httpConfig.securePort=9443

jetty.ssl.port=9443
```

7. Start the crond service using the following command:

```
service crond start
```

8. Start the megha service using the following 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.

Next steps

If you are using the Common Services, make sure that you also update the port number using the `setupcommonservice` command to update the port number in Common Services.

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 Setting up Analyzer probe server (on page 99).

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 500).

Note: If you do not want to stop the **`crond`** service, you can stop 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 440) and Starting the Analyzer detail view server or Analyzer probe server services (on page 439)

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 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 following 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.

Note: If you do not want to stop the **`crond`** service, you can stop 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 440) and Starting the Analyzer detail view server or Analyzer probe server services (on page 439)

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 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 following command:

```
service crond start
```

Deleting an SSL certificate from the Keystore

You can delete a previously imported or exipred SSL certificate from the keystore.

Before you begin

Note: If you do not want to stop the **`crond`** service, you can stop 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 440) and Starting the Analyzer detail view server or Analyzer probe server services (on page 439)

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
```

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. Navigate to the `/usr/local/httpProxy/jetty/etc` directory:

```
cd /usr/local/httpProxy/jetty/etc
```

3. Create a private key:

```
openssl genrsa -out jettyPrivate.key
```

4. Create a certificate signing request (CSR):

```
openssl req -new -key jettyPrivate.key -out /tmp/certreq.csr
```

   Follow the instructions displayed to enter the details for your certificate request. When requested to provide common name, make sure that you enter a fully qualified host name.

   Enter the default password for the CSR: `megha.jeos`.

   Note: If you provide the password of your choice, note it. You will need this when applying server certificates.

5. Copy the certificate request file from `/tmp/certreq.csr` and submit it to the certificate authority to create the certificate file.

Applying server certificates

The certificate authority creates the following three certificate files:

- Root
- Intermediate
- Host

Note: If you do not want to stop the **`crond`** service, you can stop 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 440) and Starting the Analyzer detail view server or Analyzer probe server services (on page 439)

Procedure

1. Upload the certificate files to the Analyzer detail view server. (For example, `cd /usr/local/httpProxy/jetty/etc/keystore`).
2. Navigate to the `/usr/local/httpProxy/jetty/etc` directory:

```
cd /usr/local/httpProxy/jetty/etc
```

3. Combine the chain of certificates by concatenating them into a single file (in the order indicated):

```
cat Host-Certificate Intermediate-Certificate Root-Certificate > cert-chain.cer
```

   For example:

```
cat host.cer imd.cer root.cer > cert-chain.cer
```

4. Combine the private key and certificate in the `jetty.pkcs12` file using the following command:

```
openssl pkcs12 -export -inkey jettyPrivate.key -in cert-chain.cer -out
jetty.pkcs12 -name jetty
```

5. Enter the password that you provided when creating the CSR. The default password is: `megha.jeos`
6. Stop the crond service using the command:

```
service crond stop
```

7. Stop all the running services using the command:

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

8. Verify that the httpProxy and crond services are stopped by entering these commands:

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

```
service crond status
```

9. Take a backup of an existing keystore file using the command:

```
cp /usr/local/httpProxy/jetty/etc/keystore /usr/local/httpProxy/jetty/etc/
keystore-orig
```

10. Import the `pkcs12` file (using keytool) with the following command:

```
keytool -importkeystore -srckeystore jetty.pkcs12 -srcstoretype PKCS12 -
destkeystore keystore -deststoretype PKCS12
```

11. Take a backup of an existing `userKeystoreConfig` file using the command:

```
cp /usr/local/httpProxy/jetty/etc/userKeystoreConfig.xml /usr/local/httpProxy/
jetty/etc/userKeystoreConfig-orig.xml
```

12. Enter the password that you provided when creating the CSR. The default password is: `megha.jeos`

Note: If you provided a password of your choice when creating the CSR, make sure you change the following fields in the `/usr/local/httpProxy/jetty/etc/userKeystoreConfig.xml` file:

```
KeyStorePassword
KeyManagerPassword
TrustStorePassword
```

If the password includes the following special characters, you must replace them as indicated when editing these fields:

- Replace ' " ' with '"'
- Replace ' ' ' with '''
- Replace ' < ' with '<'
- Replace ' > ' with '>'
- Replace ' & ' with '&'

For example:

- Replace `abc"123` with `abc"123`
- Replace `abc'123` with `abc'123`
- Replace `abc&"123` with `abc&"123`

(Optional): If you want an encrypted password for security purpose, you can convert the password into OBF format using the following command and provide the converted password in the `userKeystoreConfig.xml` file:

```
java -cp /usr/local/megha/jetty/lib/jetty-util-<Jetty Version>.jar
org.eclipse.jetty.util.security.Password "password_provided_when
creating_CSR"
```

For example:

```
java -cp /usr/local/megha/jetty/lib/jetty-util-<Jetty Version>.jar
org.eclipse.jetty.util.security.Password "abc&123"
```

If the password contains " quotation mark, provide the password within ' ' quotation marks in the above command. For example: `'abc"123'`

13. Change the ownership and permission of the keystore file:

```
chown megha:megha /usr/local/httpProxy/jetty/etc/keystore
```

```
chmod og-rwx /usr/local/httpProxy/jetty/etc/keystore
```

14. Start the megha service using the following command:

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

15. Start the crond service using the following command:

```
service crond start
```

16. (Optional) Remove the `certreq.csr`, `cert-chain.cer`, and `jetty.pkcs12` files if you will not need them in the future:

```
rm /tmp/certreq.csr
rm /usr/local/httpProxy/jetty/etc/cert-chain.cer
rm /usr/local/httpProxy/jetty/etc/jetty.pkcs12
```

Configuring an SSL certificate (real time data collection)

Enable SSL encryption to securely collect the real time data. You can either configure the CA signed or self-signed SSL certificate.

Enabling SSL encryption for real time data collection using a CA signed certificate

Follow these procedures as a root user to enable SSL encryption for real-time data communication between the Analyzer probe server to Analyzer detail view server using a CA signed certificate:

1. Stop the services and data collection on the servers (on page 387)
2. Configure the Analyzer detail view server (on page 387)
3. Configure the Analyzer probe server (on page 393)
4. Restart the services (on page 394)

Stop the services and data collection on the servers

Follow these steps on both the Analyzer probe server and Analyzer detail view server:

1. Stop the crond services:

```
service crond stop
```

2. Stop all the services using the command:

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

3. Stop the data collection for System Diagnostics:

```
/usr/local/megha/dbgUtils/bin/hdebug.sh setSystemDiagnosticsConfig --key
sds.enabled --value false
```

Configure the Analyzer detail view server

Follow these steps on the Analyzer detail view server:

1. Make backup copies of the following files located in `/usr/local/megha/kafka/config`:
   - `consumer.properties`
   - `producer.properties`
   - `server.properties`
2. (Optional) Enable host name verification as follows:
   a. Create new entries in the following property files:
      - `/usr/local/megha/conf/sys/server.realtime.properties`:

        ```
        server.realtime.ssl.endpoint.identification.algorithm=https
        ```

      - `/usr/local/megha/dbgUtils/conf/sds.realtime.properties`:

        ```
        sds.realtime.ssl.endpoint.identification.algorithm=https
        ```

   b. Run the following command to identify the FQDN:

      ```
      hostname -f
      ```

   c. Add the Analyzer detail view server FQDN and IP address to the `/etc/hosts` file in the following format:

      ```
      IP-address output-of-the-command-in-step-b
      ```

      For example:

      ```
      192.168.10.11 ssltest.company.com
      ```

3. Create a certificate signing request on the Analyzer detail view server:
   a. Create a temporary directory and open it:

      ```
      mkdir /tmp/RealtimeSSLCertificate
      ```

      ```
      chmod og-rwx /tmp/RealtimeSSLCertificate
      ```

      ```
      cd /tmp/RealtimeSSLCertificate
      ```

   b. Run the following command to identify the FQDN:

      ```
      hostname -f
      ```

   c. Create the `san.cnf` file to define Subject Alternate Name (SAN) and add the details.

      ```
      # san.cnf file to define Subject alternative Name
      [req]
      ```

```
req_extensions = v3_req
distinguished_name = req_distinguished_name

[req_distinguished_name]
C = Country Name
ST = State or Province
L = City
O = Company Name
OU = Department
CN = Common Name

[ v3_req ]
# Extensions to add to a certificate request
basicConstraints = CA:FALSE
keyUsage = nonRepudiation, digitalSignature, keyEncipherment
extendedKeyUsage = serverAuth, clientAuth
subjectAltName = @SAN

[SAN]
DNS.1 = Analyzer_detail_view_server_host_name
IP.1 = Analyzer_detail_view_server_IP_address
```

For example:

```
# san.cnf file to define Subject alternative Name
[req]
req_extensions = v3_req
distinguished_name = req_distinguished_name

[req_distinguished_name]
C = Country Name
ST = State or Province
L = City
O = Company Name
OU = Department
CN = Common Name

[ v3_req ]
# Extensions to add to a certificate request
basicConstraints = CA:FALSE
keyUsage = nonRepudiation, digitalSignature, keyEncipherment
extendedKeyUsage = serverAuth, clientAuth
subjectAltName = @SAN

[SAN]
DNS.1 = ssltest.company.com
IP.1 = 192.168.33.198
```

d. Create a certificate signing request using the following command:

```
openssl req -newkey rsa:Length_of_RSA -nodes -keyout /tmp/
RealtimeSSLCertificate/private.key -Length_of_SHA -out /tmp/
RealtimeSSLCertificate/Certificate_File_Name -config SAN_file_Name
```

For example:

```
openssl req -newkey rsa:2048 -nodes -keyout /tmp/RealtimeSSLCertificate/
private.key -SHA256 -out /tmp/RealtimeSSLCertificate/detail-view-server.csr
-config /tmp/RealtimeSSLCertificate/san.cnf
```

e. Submit the certificate request file to the certificate authority.

The certificate authority creates the following certificate files:

- Host
- Intermediate1
- Intermediate2

Note: Some authorities might issue only one intermediate file.

f. Upload the certificate files to the `/tmp/RealtimeSSLCertificate` directory on the Analyzer detail view server.

g. Combine the chain of certificates by concatenating them into a single file (in the order indicated). For example:

```
cat host.cer imd-1.cer imd-2.cer > certChain.cer
```

Note: Some authorities might issue root CA certificate file also. In such instance, the root CA certificate file name must be part of the command. For example:

```
cat host.cer imd-1.cer root.cer > certChain.cer
```

h. Combine the chain of certificates without the `host.cer` into a single file (in the order indicated). For example:

```
cat imd-1.cer imd-2.cer > certChain_WithoutHostCert.cer
```

Note: Some authorities might issue root CA certificate file also. In such instance, the root CA certificate file name must be part of the command. For example:

```
cat imd-1.cer root.cer > certChain_WithoutHostCert.cer
```

i. Combine the private key and certificate in the `keystore.pkcs12` file using the following command:

```
openssl pkcs12 -export -name localhost -in certChain.cer -inkey private.key
-out keystore.pkcs12
```

> **Note:** For the password, enter `changeit` (default). If you provide a password of your choice, note it. You will need it in next steps. Also, do the following to update it:
>
> i. Run the following command:
>
> ```
> /usr/local/megha/bin/changeSSLCertificatePassword.sh
> ```
>
> ii. Enter the password and confirm.

In rest of this procedure, when prompted for the keystore password or for the the PEM pass phrase, make sure you enter the password configured in this step.

j. Import the CA signed certificate into the keystore:

```
keytool -importkeystore -destkeystore server.keystore.jks -deststoretype
JKS -srckeystore keystore.pkcs12 -srcstoretype pkcs12 -alias localhost
```

k. Add the CA certificate to the clients truststore so that client can trust this certificate:

```
keytool -keystore client.truststore.jks -storetype JKS -alias CARoot -
import -file certChain_WithoutHostCert.cer
```

For trusting the certificate, enter `Yes`.

```
keytool -keystore server.truststore.jks -storetype JKS -alias CARoot -
import -file certChain_WithoutHostCert.cer
```

For trusting the certificate, enter `Yes`.

l. Copy the generated truststore (client and server) and keystore to `/usr/local/megha/conf/kafka`:

```
cp client.truststore.jks server.keystore.jks server.truststore.jks /usr/
local/megha/conf/kafka/
```

m. Change the ownership to megha and permissions of the following files:

```
chown megha:megha /usr/local/megha/conf/kafka/client.truststore.jks
```

```
chown megha:megha /usr/local/megha/conf/kafka/server.truststore.jks
```

```
chown megha:megha /usr/local/megha/conf/kafka/server.keystore.jks
```

```
chmod og-rwx /usr/local/megha/conf/kafka/server.truststore.jks
```

```
chmod og-rwx /usr/local/megha/conf/kafka/client.truststore.jks
```

```
chmod og-rwx /usr/local/megha/conf/kafka/server.keystore.jks
```

```
chmod og-rwx /usr/local/megha/kafka/config/server.properties
```

```
chmod og-rwx /usr/local/megha/kafka/config/consumer.properties
```

```
chmod og-rwx /usr/local/megha/kafka/config/producer.properties
```

4. Edit the property files as follows:

- `/usr/local/megha/conf/sys/server.realtime.properties`:

  Change the value of the `server.realtime.security.protocol` property to `SASL_SSL`.

- `/usr/local/megha/dbgUtils/conf/sds.realtime.properties`:

  Change the value of the `sds.realtime.security.protocol` property to `SASL_SSL`.

- Change the permissions:

```
chmod og-rwx /usr/local/megha/conf/sys/server.realtime.properties
```

```
chmod og-rwx /usr/local/megha/dbgUtils/conf/sds.realtime.properties
```

5. Delete temporary directory and files:

```
cd /tmp
```

```
rm -rf /tmp/RealtimeSSLCertificate
```

Configure the Analyzer Probe server

Follow these steps on the Analyzer probe server:

1. (Optional) Do the following if you have enabled host name verification on the Analyzer detail view server.
   a. Add new entries to the following property files to enable hostname verification.
      - `/usr/local/megha/conf/sys/probe.realtime.properties`:

        ```
        probe.realtime.ssl.endpoint.identification.algorithm=https
        ```

      - `/usr/local/megha/dbgUtils/conf/sds.realtime.properties`:

        ```
        sds.realtime.ssl.endpoint.identification.algorithm=https
        ```

   b. Add the host name and IP address of the Analyzer detail view server to the `/etc/hosts` file in the following format:

      ```
      IP-address host-name
      ```

2. Copy the `client.truststore.jks` from the Analyzer detail view server to the `/usr/local/megha/conf/kafka` directory on the Analyzer probe server.

   Note: The `client.truststore.jks` file is available at the `/usr/local/megha/conf/kafka/` on the Analyzer detail view server.

3. If you have configured the password of your choice in Analyzer detail view server when combining private key and certificate in the `keystore.pkcs12` file (**step 3h**), make sure you configure the same password in Analyzer probe server also. Do the following:
   a. Run the following command:

      ```
      /usr/local/megha/bin/changeSSLCertificatePassword.sh
      ```

   b. Enter the same password that you have provided in Analyzer detail view server when combining private key and certificate in the `keystore.pkcs12` file.

4. Change the ownership of the truststore file to megha and change its permission:

   ```
   chown megha:megha /usr/local/megha/conf/kafka/client.truststore.jks
   ```

   ```
   chmod og-rwx /usr/local/megha/conf/kafka/client.truststore.jks
   ```

5. Edit the property files as follows:
   - `/usr/local/megha/conf/sys/probe.realtime.properties`:

     Remove the # symbol from the beginning of the `probe.realtime.security.protocol` property.
   - `/usr/local/megha/dbgUtils/conf/sds.realtime.properties`:

     Change the value of the `sds.realtime.security.protocol` property to `SASL_SSL`.
   - Change the permissions:

```
chmod og-rwx /usr/local/megha/conf/sys/probe.realtime.properties
```

```
chmod og-rwx /usr/local/megha/dbgUtils/conf/sds.realtime.properties
```

Restart the services

1. On the Analyzer probe server and Analyzer detail view server:
   a. Start the megha service and verify the status:

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

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

   b. The megha service also starts the real time service. Run the following command on the Analyzer detail view server to verify the status:

```
/usr/local/megha/bin/manage-kafka.sh status
```

   c. Start the crond service and verify the status:

```
service crond start
```

```
service crond status
```

   d. Enable the data collection for System Diagnostics and verify the status:

```
/usr/local/megha/dbgUtils/bin/hdebug.sh setSystemDiagnosticsConfig --key
sds.enabled --value true
```

```
/usr/local/megha/dbgUtils/bin/manage-sds.sh start
```

```
/usr/local/megha/dbgUtils/bin/manage-sds.sh status
```

Enabling SSL encryption for real time data collection using a self-signed certificate

Follow these procedures while logged on as a root user:

1. Stop the services and data collection on the servers (on page 395)
2. Configure the Analyzer detail view server (on page 395)
3. Configure the Analyzer Probe server (on page 399)
4. Restart the services (on page 400)

Stop the services and data collection on the servers

Follow these steps on both the Analyzer probe server and Analyzer detail view server:

1. Stop the crond service using the command:

```
service crond stop
```

2. Stop all services using the command:

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

3. Stop the data collection for System Diagnostics:

```
/usr/local/megha/dbgUtils/bin/hdebug.sh setSystemDiagnosticsConfig --key
sds.enabled --value false
```

Configure the Analyzer detail view server

Follow these steps on the Analyzer detail view server:

1. Make backup copies of the following files located in `/usr/local/megha/kafka/config`:
   - `consumer.properties`
   - `producer.properties`
   - `server.properties`
2. (Optional) Enable host name verification as follows:
   a. Create new entries in the following property files:
      - `/usr/local/megha/conf/sys/server.realtime.properties`:

```
server.realtime.ssl.endpoint.identification.algorithm=https
```

      - `/usr/local/megha/dbgUtils/conf/sds.realtime.properties`:

```
sds.realtime.ssl.endpoint.identification.algorithm=https
```

   b. Run the following command to identify the FQDN:

```
hostname -f
```

c. Add the Analyzer detail view server FQDN and IP address to the `/etc/hosts` file in the following format:

```
IP-address output-of-the-command-in-step-b
```

3. Create the keystore file on the Analyzer detail view server:

   a. Create a temporary directory, change the permissions, and open it:

```
mkdir /tmp/RealtimeSSLCertificate
```

```
chmod og-rwx /tmp/RealtimeSSLCertificate
```

```
cd /tmp/RealtimeSSLCertificate
```

   b. Identify the FQDN:

```
hostname -f
```

   c. Create the keystore file:

```
keytool -keystore server.keystore.jks -storetype JKS -alias localhost -
validity validity_in_days -genkey -keyalg RSA -ext
SAN=DNS:Analyzer_detail_view_server_host_name,
IP:Analyzer_detail_view_server_IP_address
```

   For example:

```
keytool -keystore server.keystore.jks -storetype JKS -alias localhost -
validity 365 -genkey -keyalg RSA -ext SAN=DNS:test.ssl.com,IP:192.168.33.123
```

   Respond to the prompts as follows:

   - For the password, enter `changeit` (default). If you change this password, make a note of it because you will need it in next steps. To update the password:

     i. Run the following command:

```
/usr/local/megha/bin/changeSSLCertificatePassword.sh
```

     ii. Enter the password and confirm.

     In rest of this procedure, when prompted for the keystore password or for the the PEM pass phrase, make sure you enter the password configured in this step.

   - For the common name (first and last name), enter a fully qualified host name.
   - For the key password for common name, press **Enter**.

d. Create a CA certificate:

```
openssl req -new -x509 -keyout ca-key -out ca-cert -days validity-in-days
```

For example:

```
openssl req -new -x509 -keyout ca-key -out ca-cert -days 365
```

When prompted for the common name, enter a fully qualified host name.

e. Create the truststore for the real time data collection client (Analyzer probe server) and add the generated certificate to the client truststore:

```
keytool -keystore client.truststore.jks -storetype JKS -alias CARoot -
import -file ca-cert
```

When prompted for trusting the certificate, enter `Yes`.

f. Create the truststore on the Analyzer detail view server and import the public certificate of the CA into the truststore:

```
keytool -keystore server.truststore.jks -storetype JKS -alias CARoot -
import -file ca-cert
```

When prompted for trusting the certificate, enter `Yes`

g. Create a certificate signing request (CSR) using the keystore:

```
keytool -keystore server.keystore.jks -alias localhost -certreq -file cert-
file
```

h. Sign the certificate signing request (cert-file) with the root:

```
openssl x509 -req -CA ca-cert -CAkey ca-key -in cert-file -out cert-signed -
days validity-in-days -CAcreateserial
```

For example:

```
openssl x509 -req -CA ca-cert -CAkey ca-key -in cert-file -out cert-signed -
days 365 -CAcreateserial
```

i. Import the CA (`ca-cert`) into the keystore:

```
keytool -keystore server.keystore.jks -alias CARoot -import -file ca-cert
```

j. Import the signed certificate (`cert-signed`) into the keystore:

```
keytool -keystore server.keystore.jks -alias localhost -import -file cert-
signed
```

k. Copy the generated truststore (client and server) and keystore to `/usr/local/megha/conf/kafka`:

```
cp client.truststore.jks server.keystore.jks server.truststore.jks /usr/local/megha/conf/kafka/
```

l. Change the ownership to megha and also change the permissions for the following files:

```
chown megha:megha /usr/local/megha/conf/kafka/client.truststore.jks
```

```
chown megha:megha /usr/local/megha/conf/kafka/server.truststore.jks
```

```
chown megha:megha /usr/local/megha/conf/kafka/server.keystore.jks
```

```
chmod og-rwx /usr/local/megha/conf/kafka/server.truststore.jks
```

```
chmod og-rwx /usr/local/megha/conf/kafka/client.truststore.jks
```

```
chmod og-rwx /usr/local/megha/conf/kafka/server.keystore.jks
```

```
chmod og-rwx /usr/local/megha/kafka/config/server.properties
```

```
chmod og-rwx /usr/local/megha/kafka/config/consumer.properties
```

```
chmod og-rwx /usr/local/megha/kafka/config/producer.properties
```

4. Edit the property files and change the permissions as follows:

- `/usr/local/megha/conf/sys/server.realtime.properties`:

  Change the value of the `server.realtime.security.protocol` property to `SASL_SSL`.

- `/usr/local/megha/dbgUtils/conf/sds.realtime.properties`:

  Change the value of the `sds.realtime.security.protocol` property to `SASL_SSL`.

- Change the permissions:

```
chmod og-rwx /usr/local/megha/conf/sys/server.realtime.properties
```

```
chmod og-rwx /usr/local/megha/dbgUtils/conf/sds.realtime.properties
```

5. Delete the temporary directory and files:

```
cd /tmp
```

```
rm -rf /tmp/RealtimeSSLCertificate
```

Configure the Analyzer Probe server

Follow these steps on the Analyzer probe server:

1. (Optional) If you have enabled host name verification on the Analyzer detail view server, do the following:
   a. Add new entries to the following property files to enable hostname verification.
      - `/usr/local/megha/conf/sys/probe.realtime.properties`:

        ```
        probe.realtime.ssl.endpoint.identification.algorithm=https
        ```

      - `/usr/local/megha/dbgUtils/conf/sds.realtime.properties`:

        ```
        sds.realtime.ssl.endpoint.identification.algorithm=https
        ```

   b. Add the host name and IP address of the Analyzer detail view server to the `/etc/hosts` file in the following format:

      ```
      IP-address host-name
      ```

2. Copy the `client.truststore.jks` from the Analyzer detail view server to the `/usr/local/megha/conf/kafka` directory on the Analyzer probe server.

   Note: The `client.truststore.jks` file is available on the Analyzer detail view server in the `/usr/local/megha/conf/kafka/` directory.

3. Change the ownership to megha and also the permissions for the truststore file:

   ```
   chown megha:megha /usr/local/megha/conf/kafka/client.truststore.jks
   ```

   ```
   chmod og-rwx /usr/local/megha/conf/kafka/client.truststore.jks
   ```

4. If you changed the default password for the Analyzer detail view server Keystore file in the previous procedure (**step 3C**), make sure that you also configure the same password on the Analyzer probe server as follows:
   a. Run the following command:

      ```
      /usr/local/megha/bin/changeSSLCertificatePassword.sh
      ```

   b. Enter the same password.

5. Edit the property files and change their permissions as follows:
   - `/usr/local/megha/conf/sys/probe.realtime.properties`:

     Remove the # symbol from the beginning of the `probe.realtime.security.protocol` property.
   - `/usr/local/megha/dbgUtils/conf/sds.realtime.properties`:

     Change the value of the `sds.realtime.security.protocol` property to `SASL_SSL`.
   - Change the permissions:

     ```
     chmod og-rwx /usr/local/megha/conf/sys/probe.realtime.properties
     ```

     ```
     chmod og-rwx /usr/local/megha/dbgUtils/conf/sds.realtime.properties
     ```

Restart the services

1. On the Analyzer probe server and Analyzer detail view server:
   a. Start the megha service and verify the status:

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

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

      The megha service also starts the real time service.

   b. Run the following command on the Analyzer detail view server to verify the status:

      ```
      /usr/local/megha/bin/manage-kafka.sh status
      ```

   c. Start the crond service and verify the status:

      ```
      service crond start
      ```

      ```
      service crond status
      ```

   d. Enable System Diagnostics data collection and verify the status:

      ```
      /usr/local/megha/dbgUtils/bin/hdebug.sh setSystemDiagnosticsConfig --key
      sds.enabled --value true
      ```

      ```
      /usr/local/megha/dbgUtils/bin/manage-sds.sh start
      ```

      ```
      /usr/local/megha/dbgUtils/bin/manage-sds.sh status
      ```

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 Ops Center Automator 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 root permission.

Procedure

1. Stop the Analyzer server services.
2. Run the following command to import the Ops Center Automator certificates to the truststore:

```
Common-component-installation-destination-directory/uCPSB11/jdk/bin/keytool -import -alias alias-name -file certificate-file-name -keystore truststore-file-name -storepass truststore-password -storetype JKS
```

Note:

Note the following when specifying 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.

- For the *alias-name*, specify the name of the host on which the certificate is located.
- For the *certificate-file-name*, specify the absolute path to the certificate.

- The truststore file is stored in the following location:

  Common-component-installation-destination-directory/uCPSB11/hjdk/jdk/lib/security/jssecacerts

- Specify a password for the *truststore-password*.
- You must specify JKS for the keystore type.

3. To enable the verification of server certificates, change the following properties in the config_user.properties file.
   - Location:

     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 LDAP directory server certificates to the Analyzer server truststore.

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 262).
- 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 root permission.

Procedure

1. Stop the Analyzer server services.
2. Run the following command to import certificates for the LDAP directory server to the truststore:

```
Common-component-installation-destination-directory/uCPSB11/jdk/bin/keytool -
import -alias alias-name -file certificate-file-name -keystore truststore-file-
name -storepass truststore-password -storetype JKS
```

> **Note:**
>
> Note the following when specifying 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.

- 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`

    `Common-component-installation-destination-directory``/conf/sec/ldapcacerts`

  - `jssecacerts`

    `Common-component-installation-destination-directory``/uCPSB11/hjdk/jdk/lib/security/jssecacerts`

- Specify a password for the *`truststore-password`*.
- You must specify `JKS` for the keystore type of the truststore.

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 Common Services 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 root permission.

Procedure

1. Stop the Analyzer server services.
2. Run the following command to import the Common Services certificates to the truststore:

```
Common-component-installation-destination-directory/uCPSB11/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 is located.
- For the *certificate-file-name*, specify the absolute path to the certificate.
- The truststore file is stored in the following location:

  Common-component-installation-destination-directory/uCPSB11/hjdk/jdk/lib/security/jssecacerts
- The default truststore password is `changeit`.
- You must specify `JKS` for the keystore type.

3. To enable the verification of server certificates, change the following properties in the `config_user.properties` file.
   - Location:

     Analyzer-server-installation-destination-directory/Analytics/conf
   - Key: `cert.verify.enabled`
   - Value: `true`
4. Start the Analyzer server services.

Enabling TLS certificate verification for connecting to Common Services

The TLS certificate verification enables secure communication between the Analyzer detail view server or Analyzer probe server and the Common Services server.

Before you begin

- Obtain a valid TLS certificate from the Common Services server and save it in the `/tmp` directory on the Analyzer detail view server or Analyzer probe server.
- Identify and note the Java keystore path on the Analyzer detail view server or Analyzer probe server machine.

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
```

3. Stop the megha service using the command:

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

4. Make a backup of the `custom.properties` file:

```
cp /usr/local/megha/conf/custom.properties /usr/local/megha/conf/
custom_orig.properties
```

5. Edit the `custom.properties` file.

```
vi /usr/local/megha/conf/custom.properties
```

6. Add a new entry in the property file:

```
commonservice.verify.tls.certificate=true
```

7. Save the `custom.properties` file.
8. Navigate to the Java keystore directory. For example:

```
cd /usr/java/jdk1.8.0_291-amd64/jre/lib/security
```

9. If the `jssecacerts` file does not exist, create it.
10. Import the Common Services server TLS certificate into the Analyzer detail view server or Analyzer probe server using the command:

```
keytool -importcert -alias Alias_name -keystore Truststore_file_path -storetype
jks -storepass Truststore_file_password -file TLS_certificate_file_path
```

> **Note:** You can define any unique alias name for TLS certificate.

For example:

```
keytool -importcert -alias CSServerCert -keystore jssecacerts -storetype jks -
storepass changeit -file /tmp/server.cer
```

11. Make sure that the megha user has the read permission for the `jssecacerts` file. If not, change the permissions as follows:

    For example:

    ```
    chmod o+r jssecacerts
    ```

12. Start the megha service and verify the status:

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

13. Start the crond service and verify the status:

    ```
    service crond start
    service crond status
    ```

Note: If you upgrade the JDK in the future, make sure that the `jssecacerts` file is copied in the upgraded JDK directory.

For example: If you upgrade JDK from v1.7.0 to v1.8.0, copy the `jssecacerts` file from `/usr/java/jdk1.7.0_291-amd64/jre/lib/security` to `/usr/java/jdk1.8.0_251-amd64/jre/lib/security`.

After copying the `jssecacerts` file, make sure that megha user has the read permission for the `jssecacerts` file. If megha user does not have read permission, provide the permission.

For example:

```
chmod o+r jssecacerts
```

Setting up SSL communication (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 **`htmssltool`** 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 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 command will fail.)

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/jp1pc/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/jp1pc/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:

As a best practice, you should only use a self-signed certificate to test encrypted communications.

Submitting a certificate signing request (CSR) for RAID Agent

In general, applications for server certificates are submitted online. You must 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 in X.509 PEM format issued by the certificate authority. For details on how to apply, see the website of your certificate authority. In addition, make sure the certificate authority supports the signature algorithm.

Procedure

1. Send the certificate signing request to the certificate authority.
2. Save the server certificate 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 411).

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 issued by the certificate authority for RAID Agent.

  We recommend that you copy the file to the following location:

  - Private key file for RAID Agent

    `/opt/jp1pc/htnm/HBasePSB/httpsd/conf/ssl/server`

  - Server certificate for RAID Agent (if you are using a certificate issued by a certificate authority)

    `/opt/jp1pc/htnm/HBasePSB/httpsd/conf/ssl/cacert`

  - Server certificate for RAID Agent (if you are using a self-signed certificate*)

    `/opt/jp1pc/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/jp1pc/htnm/bin/htmsrv stop -all
   ```

2. Edit the `/opt/jp1pc/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 `SSLEngine Off` to comment out these lines.

```
ServerName RAID-Agent-server-host-name
#Listen 24221
#Listen [::]:24221
#SSLEngine Off
Listen 24222
#Listen [::]:24222
SSLEngine On
SSLProtocol TLSv1.2
SSLCipherSuite ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-
RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256
SSLCertificateFile /opt/jp1pc/htnm/HBasePSB/httpsd/conf/ssl/server/httpsd.pem
SSLCertificateKeyFile /opt/jp1pc/htnm/HBasePSB/httpsd/conf/ssl/server/
httpsdkey.pem
SSLCertificateFile /opt/jp1pc/htnm/HBasePSB/httpsd/conf/ssl/server/ecc-httpsd.pem
SSLCertificateKeyFile /opt/jp1pc/htnm/HBasePSB/httpsd/conf/ssl/server/ecc-
httpsdkey.pem
#SSLCACertificateFile /opt/jp1pc/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.)
- Specify the absolute paths of the secret key and the server certificate of RAID Agent for the following directives.
  - `SSLCertificateKeyFile`
  - `SSLCertificateFile`
- 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` , `hsso_httpsd.conf`, or `user_hsso_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/jp1pc/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/jp1pc/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 RAID Agent certificates to the Analyzer server truststore, and edit the `config_user.properties` file.

Before you begin

You must have root permission.

Procedure

1. Stop the Analyzer server services.
2. Run the following command to import the certificates for RAID Agent to the truststore file:

```
Common-component-installation-destination-directory/uCPSB11/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:

  Common-component-installation-destination-directory/uCPSB11/hjdk/jdk/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:

     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 RAID agent certificates to the Analyzer probe server truststore.

Before you begin

You must have root permission.

Note: If you do not want to stop the **crond** service, you can stop 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 440) and Starting the Analyzer detail view server or Analyzer probe server services (on page 439)

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
   ```
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 file password of the Analyzer probe server.

   ```
   keytool -import -alias alias-name -keystore /usr/local/megha/jetty/etc/keystore -
   trustcacerts -file certificate-file-name -storetype JKS
   ```

   Example:

   ```
   keytool -import -alias RAIDAgent -keystore /usr/local/megha/jetty/etc/keystore -
   trustcacerts -file htnmcert.crt -storetype JKS
   ```

   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.
   - The keystore file default password of the Analyzer probe server is `megha.jeos`.

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
   ```

Setting up SSL communication (Virtual Storage Software Agent)

To initiate a secure session with a host that uses Virtual Storage Software Agent services, you must create a private key and a certificate signing request (CSR), apply the server certificate, and configure secure communications. When performing a new installation of Virtual Storage Software Agent or upgrading it from version 10.8.2 or earlier, create and revise the server certificate.

Creating a private key and a certificate signing request for Virtual Storage Software Agent server

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 request.
- When re-creating a private key or certificate signing request, send the output to a new location. (If a file of the same name exists in the output location, the command will fail.)

Procedure

1. Log on to the Analyzer probe server.
2. Run the **`keytool`** command to create a keystore file containing the private key for Virtual Storage Software Agent, and a server certificate.

```
/usr/lib/jvm/java-1.8.0-amazon-corretto/jre/bin/keytool -genkeypair -keystore
keystore-file-name -alias alias-name -v -keyalg RSA [-keysize key-size] [-
validity expiration-date]
```

   For example:

```
/usr/lib/jvm/java-1.8.0-amazon-corretto/jre/bin/keytool -genkeypair -keystore
keystore -alias virtualstoragesoftwareagent -v -keyalg RSA -keysize 2048 -
validity 365
```

3. Run the **`keytool`** command to create a certificate signing request (CSR).

```
/usr/lib/jvm/java-1.8.0-amazon-corretto/jre/bin/keytool -certreq -keystore
keystore-file-name -alias alias-name -file CSR-file-name -ext san=dns:host-name
```

Submitting a certificate signing request (CSR) for Virtual Storage Software Agent

In general, applications for server certificates are submitted online. You must create a certificate signing request (CSR) for Virtual Storage Software Agent and send it to the certificate authority to obtain a digital signature.

Before you begin

Create a certificate signing request for Virtual Storage Software Agent.

You must have a server certificate in X.509 PEM format issued by the certificate authority. For details on how to apply, see the website of your certificate authority. In addition, make sure the certificate authority supports the signature algorithm.

Procedure

1. Send the certificate signing request to the certificate authority.
2. Run the following command to import the server certificate to the keystore file:

```
/usr/lib/jvm/java-1.8.0-amazon-corretto/jre/bin/keytool -import -keystore
keystore-file-name -alias alias-name -file certificate-file-name
```

Enabling SSL communication for Virtual Storage Software Agent

To enable SSL communication that uses Virual Storage Software Agent services, edit the `userconfig-setting.yaml` file.

Procedure

1. Check and, if necessary, revise the settings in the following definition file:

```
/var/Virtual-Storage-Software-Agent-installation-destination-directory/
VirtualStorageSoftwareAgent/config/userconfig-setting.yaml
```

   - protocol: The protocol for Virtual Storage Software Agent. Make sure this setting is set to https.
   - port: The port number for Virtual Storage Software Agent. Specify a number in the range 1-65535. The specified port will be used as the port for Virtual Storage Software Agent to which the Hitachi VSS Block Storage probe connects.
   - keyStorePath: The file path of the keystore to which the server certificate was imported.
   - keyStorePassword: The password for the keystore to which the server certificate was imported.

   For example:

```
serverSettings:
  protocol: https
  port: 24081
  keyStorePath: /home/usr/.ssh/keystore
  keyStorePassword: pass!23

virtualStorageSoftwareAccessSettings:
  verifyingSsl: false
```

2. Restart the Virtual Storage Software Agent services by running the following command:

```
systemctl restart virtualstoragesoftware-agent.service
```

Enabling TLS certificate verification for connecting to Virtual Storage Software Agent

The TLS certificate verification enables secure communication between the Analyzer probe server and the Virtual Storage Software Agent for collecting data using the Hitachi VSS Block Storage probe.

Before you begin

- Obtain a valid TLS certificate (for example, `server.crt` file) for Virtual Storage Software Agent and save it in the `/tmp` directory on the Analyzer probe server.

  TLS certificate verification is a global setting. If there are multiple Virtual Storage Software Agents, make sure you obtain TLS certificates for all the Virtual Storage Software Agents.

  Note: If the TLS certificate is created using the IP address and hostname, you can add the Hitachi VSS Block Storage probe using either an IP address or hostname. However, if the TLS certificate is created using only the IP address or hostname, you must add the Hitachi VSS Block Storage probe using only the IP address or hostname, respectively.

- Identify and note the Java keystore path on the Analyzer probe server machine.

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. Make a backup of the `custom.properties` file:

   ```
   cp /usr/local/megha/conf/custom.properties /usr/local/megha/conf/
   custom_orig.properties
   ```

5. Edit the `custom.properties` file.

   ```
   vi /usr/local/megha/conf/custom.properties
   ```

6. Add a new entry in the property file:

   ```
   vssb.verify.tls.certificate=true
   ```

7. Save the `custom.properties` file.
8. Navigate to the Java keystore directory. For example:

   ```
   cd /usr/java/jdk1.8.0_291-amd64/jre/lib/security
   ```

9. If the `jssecacerts` file does not exist, create it.

10. Import the TLS certificate into the Analyzer probe server using the command:

```
keytool -importcert -alias Alias_name -keystore Truststore_file_path -storetype
jks -storepass Truststore_file_password -file TLS_certificate_file_path
```

> **Note:** You can define any unique alias name for TLS certificate.

For example:

```
keytool -importcert -alias vssbCert -keystore jssecacerts -storetype jks -
storepass changeit -file /tmp/server.cer
```

11. If there are multiple Virtual Storage Software Agents, repeat step 10 for each Virtual Storage Software Agent.
12. Make sure that the megha user has the read permission for the `jssecacerts` file. If not, set it as in this example:

```
chmod o+r jssecacerts
```

13. Start the megha service and verify the status:

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

14. Start the crond service and verify the status:

```
service crond start
service crond status
```

> **Note:** If you upgrade the JDK in the future, make sure that the `jssecacerts` file is copied in the upgraded JDK directory.
>
> For example: If you upgrade JDK from v1.7.0 to v1.8.0, copy the `jssecacerts` file from `/usr/java/jdk1.7.0_291-amd64/jre/lib/security` to `/usr/java/jdk1.8.0_251-amd64/jre/lib/security`.
>
> After copying the `jssecacerts` file, make sure that megha user has the read permission for the `jssecacerts` file.

Configuring an SSL certificate (Virtual Storage Software Block)

To use Virtual Storage Software Agent for SSL communication with Virtual Storage Software Block, you must first enable SSL. For details, see the section describing how to set up SSL in the documentation for your storage system.

Importing Virtual Storage Software Block certificates to the Virtual Storage Software Agent truststore

To enable Virtual Storage Software Agent to verify the Virtual Storage Software Block certificates, import the Virtual Storage Software Block certificates to the Virtual Storage Software Agent truststore.

Before you begin

- Prepare the Virtual Storage Software Block certificates. For details, see the section describing how to set up SSL in the documentation for your storage system.
- You must have root permission.

Procedure

1. Run the following command to import the Virtual Storage Software Block certificates to the truststore:

```
keytool -import -alias alias-name -file certificate-file-name -keystore
truststore-file-name -storepass truststore-password -storetype JKS
```

Note:

Note the following when specifying 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.

- For the *`alias-name`*, specify the name of the host on which the certificate is located.
- For the *`certificate-file-name`*, specify the absolute path to the certificate.
- The truststore file is stored in the following location:

  `/usr/lib/jvm/java-1.8.0-amazon-corretto/jre/lib/security/jssecacerts`

- Specify a password for the *`truststore-password`*.
- You must specify `JKS` for the keystore type.

2. To enable the verification of server certificates, change the following properties in the `userconfig-setting.yaml` file.
   - Location: `/var/`*`Virtual-Storage-Software-Agent-installation-destination-directory`*`/VirtualStorageSoftwareAgent/config`
   - Key: `verifyingSsl`
   - Value: `true`
3. Restart the Virtual Storage Software Agent services by running the following command:

```
systemctl restart virtualstoragesoftware-agent.service
```

Enabling TLS certificate verification for the On-demand real time monitoring

The TLS certificate verification enables secure communication between the Analyzer detail view server and the RAID Agent server (usually, the host on which the Analyzer probe server is installed) for On-demand real time monitoring.

Before you begin

- Obtain a valid TLS certificate (for example, `server.crt` file) from the RAID Agent server and save it in the `/tmp` directory on the Analyzer detail view server.

  TLS certificate verification is a global setting. If there are multiple RAID Agent servers available in the Analyzer detail view server, make sure you obtain the TLS certificates for all the RAID Agent servers.
- Identify and note the Java keystore path on the Analyzer detail view server machine.

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. Make a backup of the `custom.properties` file:

```
cp /usr/local/megha/conf/custom.properties /usr/local/megha/conf/
custom_orig.properties
```

5. Edit the `custom.properties` file.

```
vi /usr/local/megha/conf/custom.properties
```

6. Add a new entry in the property file:

```
realtimemonitoring.verify.tls.certificate=true
```

7. Save the `custom.properties` file.
8. Navigate to the Java keystore directory. For example:

```
cd /usr/java/jdk1.8.0_291-amd64/jre/lib/security
```

9. If the `jssecacerts` file does not exist, create it.
10. Import the TLS certificate into the Analyzer detail view server using the **`keytool`** command:

```
keytool -importcert -alias Alias_name -keystore Truststore_file_path -storetype
jks -storepass Truststore_file_password -file TLS_certificate_file_path
```

Note: You can define any unique alias name for TLS certificate.

For example:

```
keytool -importcert -alias aliasName -keystore jssecacerts -storetype jks -
storepass changeit -file /tmp/server.crt
```

11. If there are multiple RAID Agent servers, repeat step 10 for each RAID Agent server.
12. Make sure that the megha user has the read permission for the `jssecacerts` file. If not, change the permissions as in this example:

```
chmod o+r jssecacerts
```

13. Start the megha service and verify the status:

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

14. Start the crond service and verify the status:

```
service crond start
service crond status
```

Note: If you upgrade the JDK in the future, make sure that the `jssecacerts` file is copied in the upgraded JDK directory.

For example: If you upgrade JDK from v1.7.0 to v1.8.0, copy the `jssecacerts` file from `/usr/java/jdk1.7.0_291-amd64/jre/lib/security` to `/usr/java/jdk1.8.0_251-amd64/jre/lib/security`.

After copying the `jssecacerts` file, make sure that megha user has read permission for the `jssecacerts` file.

Replacing the HTTPS server certificate of the On-demand real time monitoring module

The On-demand real time monitoring module uses a self-signed certificate by default. Before using the module, change the setting to use a certificate issued by a certificate authority.

Before you begin

- You must have root permissions.
- Acquire a certificate and a key file issued by a certificate authority.

Procedure

1. Log on to the Analyzer probe server.
2. Stop the On-demand real time monitoring module service:

```
systemctl stop analyzer-granular-data-collection-api
```

3. Change the certificate and key file issued by the certificate authority:
   - If you are using the default location:
     a. Copy the acquired certificate and key file into the following directory:

        `/opt/hitachi/Analytics/granular-data-collection-api/cert`

     b. Use the following file names:
        - `server.crt`: Server certificate
        - `server.key`: Private key
   - If you are using another location:
     a. Open the following `user-granular-data-collection-api.conf` file:

        `/opt/hitachi/Analytics/granular-data-collection-api/conf/user-granular-data-collection-api.conf`

     b. Change the following properties, which specify the server certificate and private key:
        - `GRANULAR_DATA_COLLECTION_API_TLS_CRT_FILE`
        - `GRANULAR_DATA_COLLECTION_API_TLS_KEY_FILE`
4. Start the On-demand real time monitoring module service:

```
systemctl start analyzer-granular-data-collection-api
```

Enabling TLS certificate verification for connecting to HMC

The TLS certificate verification enables secure communication between the Analyzer probe server and the Hardware Management Console (HMC).

Before you begin

- Obtain a valid TLS certificate (for example, `server.cer` file) for HMC in x509 format and save it in the `/tmp` directory on the Analyzer probe server.

  TLS certificate verification is a global setting. If there are multiple HMCs, make sure you obtain the TLS certificates for all the HMCs.

  Note: If the TLS certificate is created using the IP address and hostname, you can add the IBM Power Systems probe using either an IP address or hostname. However, if the TLS certificate is created either using only the IP address or hostname, you must add the IBM Power Systems probe using only the IP address or hostname, respectively.

- Identify and note the Java keystore path on the Analyzer probe server machine.

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. Make a backup of the `custom.properties` file:

   ```
   cp /usr/local/megha/conf/custom.properties /usr/local/megha/conf/
   custom_orig.properties
   ```

5. Edit the `custom.properties` file.

   ```
   vi /usr/local/megha/conf/custom.properties
   ```

6. Add a new entry in the property file:

   ```
   ips.verify.ssl.certificate=true
   ```

7. Save the `custom.properties` file.
8. Navigate to the Java keystore directory. For example:

   ```
   cd /usr/java/jdk1.8.0_291-amd64/jre/lib/security
   ```

9. If the `jssecacerts` file does not exist, create it.
10. Import the TLS certificate into the Analyzer probe server using the command:

    ```
    keytool -importcert -alias Alias_name -keystore Truststore_file_path -storetype
    jks -storepass Truststore_file_password -file TLS_certificate_file_path
    ```

Note: You can define any unique alias name for TLS certificate.

For example:

```
keytool -importcert -alias aliasName -keystore jssecacerts -storetype jks -
storepass changeit -file /tmp/server.cer
```

11. If there are multiple HMCs, repeat step 10 for each HMC.
12. Make sure that the megha user has the read permission for the `jssecacerts` file. If not, set it as in this example:

```
chmod o+r jssecacerts
```

13. Start the megha service and verify the status:

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

14. Start the crond service and verify the status:

```
service crond start
service crond status
```

Note: If you upgrade the JDK in the future, make sure that the `jssecacerts` file is copied in the upgraded JDK directory.

For example: If you upgrade JDK from v1.7.0 to v1.8.0, copy the `jssecacerts` file from `/usr/java/jdk1.7.0_291-amd64/jre/lib/security` to `/usr/java/jdk1.8.0_251-amd64/jre/lib/security`.

After copying the `jssecacerts` file, make sure that megha user has the read permission for the `jssecacerts` file.

Setting an SSL cipher suite

You can set an SSL cipher suites for communication.

Setting an SSL cipher suite for the Analyzer detail view server or Analyzer probe server

The Analyzer detail view server and Analyzer probe server use SSL cipher suites for communication. You can include or exclude cipher suites on the Analyzer probe server or Analyzer detail view server as described here.

Note: If you do not want to stop the **crond** service, you can stop 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 440) and Starting the Analyzer detail view server or Analyzer probe server services (on page 439)

Procedure

1. Log on to the Analyzer probe server or 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 Analyzer detail view server or Analyzer probe server using the command:

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

4. Verify that the services (including `crond`) are stopped using the commands:

```
service crond status
```

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

5. Make a backup of the `/usr/local/megha/jetty/etc/userCipherConfig.xml` file:

```
cp /usr/local/megha/jetty/etc/userCipherConfig.xml /usr/local/megha/jetty/etc/
userCipherConfig.xml.orig
```

6. Edit the `/usr/local/megha/jetty/etc/userCipherConfig.xml` file.

```
vi /usr/local/megha/jetty/etc/userCipherConfig.xml
```

7. Do the following:
   - To exclude enabled ciphers:
     a. In the `addExcludeCipherSuites` set, remove the `<!--` from the beginning and `-->` from the end of the `Item` tag.
     b. Add or update the cipher suites in the `Item` tag:

        Examples:

```
<Item>SSL_RSA_WITH_DES_CBC_SHA</Item>

<Item>SSL_DHE_RSA_WITH_DES_CBC_SHA</Item>
```

        You can also exclude the cipher suites (with the same pattern) using regular expressions.

Example:

```
<Item>TLS_RSA.*</Item>
```

The above entry excludes the cipher suites such as TLS_RSA_WITH_AES_128_CBC_SHA, TLS_RSA_WITH_AES_128_CBC_SHA256, TLS_RSA_WITH_AES_128_GCM_SHA256 and so on.

Note: The following cipher suites cannot be used for the Analyzer detail view server and Analyzer probe server:

- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_RSA_WITH_AES_128_GCM_SHA256

- To set the ciphers for communication:

  a. Remove the `<!--` from the beginning and `-->` from the end of the `IncludeCipherSuites` set.

  b. Add or update the cipher suites in the `Item` tag:

  Examples:

```
<Item>TLS_DHE_DSS_WITH_AES_256_GCM_SHA384</Item>

<Item>TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256</Item>
```

  You can also add the cipher suites (with the same pattern) using regular expressions.

  Example:

```
<Item>TLS_ECDHE.*</Item>
```

  The above entry excludes the cipher suites, such as TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA, TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256, and so on.

  Note: Either of the following cipher suites must be enabled on the Analyzer detail view server:

  - TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
  - TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
  - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
  - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

8. Start the Analyzer detail view server or Analyzer probe server using the command:

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

9. Start the crond service using the following command:

```
service crond start
```

Setting an SSL cipher suite for the HTTP proxy service

The HTTP proxy service uses SSL cipher suites for communication. You can include or exclude cipher suites on the Analyzer detail view server as described here.

> **Note:** If you do not want to stop the **crond** service, you can stop 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 440) and Starting the Analyzer detail view server or Analyzer probe server services (on page 439)

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. Stop the HTTP proxy service using the command:

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

5. Verify that the `crond`, `megha`, and `HTTP proxy` services are stopped using the commands:

```
service crond status
```

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

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

6. Make a backup of the `/usr/local/httpProxy/jetty/etc/userCipherConfig.xml` file:

```
cp /usr/local/httpProxy/jetty/etc/userCipherConfig.xml /usr/local/httpProxy/
jetty/etc/userCipherConfig.xml.orig
```

7. Edit the `/usr/local/httpProxy/jetty/etc/userCipherConfig.xml` file.

```
vi /usr/local/httpProxy/jetty/etc/userCipherConfig.xml
```

8. Do the following:
   - To exclude enabled ciphers:
     a. In the `addExcludeCipherSuites` set, remove the `<!--` from the beginning and `-->` from the end of the `Item` tag.
     b. Add or update the cipher suites in the `Item` tag:

        Examples:

```
<Item>SSL_RSA_WITH_DES_CBC_SHA</Item>

<Item>SSL_DHE_RSA_WITH_DES_CBC_SHA</Item>
```

        You can also exclude the cipher suites (with the same pattern) using regular expressions.

        Example:

```
<Item>TLS_RSA.*</Item>
```

        The above entry excludes the cipher suites such as TLS_RSA_WITH_AES_128_CBC_SHA, TLS_RSA_WITH_AES_128_CBC_SHA256, TLS_RSA_WITH_AES_128_GCM_SHA256 and so on.

   - To set the ciphers for communication:
     a. Remove the `<!--` from the beginning and `-->` from the end of the `IncludeCipherSuites` set.
     b. Add or update the cipher suites in the `Item` tag:

        Examples:

```
<Item>TLS_DHE_DSS_WITH_AES_256_GCM_SHA384</Item>

<Item>TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256</Item>
```

        You can also add the cipher suites (with the same pattern) using regular expressions.

        Example:

```
<Item>TLS_ECDHE.*</Item>
```

        The above entry excludes the cipher suites, such as TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA, TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256, and so on.

9. Start the megha service using the command:

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

10. Start the HTTP proxy service using the command:

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

11. Start the crond service using the following command:

```
service crond start
```

Setting an SSL cipher suite for the real time data collection service

You can include or exclude SSL cipher suites for real-time data collection service on the Analyzer detail view server as described here.

Note: If you do not want to stop the **crond** service, you can stop 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 440) and Starting the Analyzer detail view server or Analyzer probe server services (on page 439)

Before you begin

Make sure that the SSL encryption is enabled for real-time data import. Refer to Enabling SSL encryption for real time data collection using a self-signed certificate (on page 395) for more information.

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. Stop the real time data collection service using the command:

```
/usr/local/megha/bin/manage-kafka.sh stop
```

5. Verify that the `crond`, `megha`, and real time data collection services are stopped using the commands:

```
service crond status
```

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

```
/usr/local/megha/bin/manage-kafka.sh status
```

6. Make a backup of the `/usr/local/megha/kafka/config/server.properties` file:

```
cp /usr/local/megha/kafka/config/server.properties /usr/local/megha/kafka/config/
server.properties.orig
```

7. Edit the `/usr/local/megha/kafka/config/server.properties` file.

```
vi /usr/local/megha/kafka/config/server.properties
```

8. (If the `ssl.cipher.suites` property does not exist), add it and enter one or comma separated values of cipher suites:

   For example:

```
ssl.cipher.suites=TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
```

9. Start the megha service using the command:

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

10. Start the crond service using the following command:

```
service crond start
```

11. Start the real-time data collection service:

```
/usr/local/megha/bin/manage-kafka.sh start
```

Enabling host header validation for the Analyzer probe or Analyzer detail view servers

To enhance security, you can enable host header validation. This ensures the Analyzer probe server or Analyzer detail view server can only be accessed by the IP address (where they are installed). In addition, you can enable access using host name or domain name by defining them in the allowlist.

Note: If you do not want to stop the **crond** service, you can stop 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 440) and Starting the Analyzer detail view server or Analyzer probe server services (on page 439)

Procedure

1. Log on to the Analyzer probe server or 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. Go to the `/usr/local/megha/conf/custom.properties` file, add the following properties, and save the file:
   - To enable host header validation and allow access with IP address and port:

```
host.header.validation.enabled=true
```

   - [Optional]: To allow access with `host-name or domain-name`, add the following additional property:

```
host.header.whitelist=host-name or domain-name
```

6. Start the megha service using the command:

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

7. Start the crond service using the following command:

```
service crond start
```

Configuring key-based authentication

You can configure the key-based authentication to transfer data directly (without an intermediate FTP or FTPS server) from the Analyzer probe server to the Analyzer detail view server using the SFTP protocol with the meghadata user. You can also configure key-based authentication to download this data to the Analyzer detail view server.

Configuring key-based authentication to transfer data directly from Analyzer probe server to Analyzer detail view server

Key-based authentication helps you to transfer data directly (without an intermediate FTP or FTPS server) from the Analyzer probe server to the Analyzer detail view server using the SFTP protocol with the meghadata user.

Note: It is recommended that you use unique SSH host keys for every host that is using SSH and also implement SSH key management solution.

Follow these procedures to configure key-based authentication:

1. Configure the Analyzer probe server (on page 431)
2. Configure the Analyzer detail view server (on page 432)

Configure the Analyzer Probe server

Follow these steps:

1. Log on to the Analyzer probe server through an SSH client (like putty) as a root user.
2. Change ownership and permission of the `.ssh` directory available under the Analyzer probe server installation directory.

   ```
   chown megha:megha /Installation_directory/megha/.ssh

   chmod 700 /Installation_directory/megha/.ssh
   ```

   For example:

   ```
   chown megha:megha /home/megha/.ssh

   chmod 700 /home/megha/.ssh
   ```

3. Switch to the megha user:

   ```
   su - megha
   ```

4. Generate a key for the megha user:

   ```
   ssh-keygen -t rsa -b key_length
   ```

   Note: Key length can be 2048 or 4096.

   For example:

   ```
   ssh-keygen -t rsa -b 2048
   ```

5. Press **Enter** to save the key in the folllowing location:

   ```
   /Installation_directory/megha/.ssh/id_rsa
   ```

For example:

```
/home/megha/.ssh/id_rsa
```

6. (Optional) Enter a passphrase and confirm it.

   Note: If you decide to use a passphrase, make sure you note it. You will need this when configuring the following settings on the Analyzer probe server to transfer data:

   - Configuring data transfer settings when setting up the Analyzer probe server
   - Adding a secondary Analyzer detail view server
   - Editing an Analyzer detail view server (primary and secondary)

7. Copy the public key to the Analyzer detail view server:

   ```
   ssh-copy-id meghadata@Analyzer_detail_view_server_IP_address_or_hostname
   ```

   For example:

   ```
   ssh-copy-id meghadata@192.168.35.31
   ```

8. When prompted for the password, enter the meghadata user password (default: `meghadata123`).

Configure the Analyzer detail view server

Follow these steps on the Analyzer detail view server:

1. Log on to the Analyzer detail view server through an SSH client (like putty) as a root user.
2. Configure the SELinux security context in the `/etc/selinux/targeted/contexts/files/file_contexts.local` file for the following directories available under the Analyzer detail view server installation directory (default: `/data`).

   a. `/Installation_directory/meghadata/.ssh` directory:

      For example:

      ```
      semanage fcontext -a -t ssh_home_t /data/meghadata/.ssh
      ```

   b. `/Installation_directory/meghadata/.ssh/authorized_keys` file:

      For example:

      ```
      semanage fcontext -a -t ssh_home_t /data/meghadata/.ssh/authorized_keys
      ```

3. Change file type to `ssh_home_t` for the following directories available under the Analyzer detail view server installation directory (default: `/data`):

   a. `/Installation_directory/meghadata/.ssh directory`:

For example:

```
restorecon -R -v /data/meghadata/.ssh
```

b. `/Installation_directory/meghadata/.ssh/authorized_keys` file:

For example:

```
restorecon -R -v /data/meghadata/.ssh/authorized_keys
```

c. Verify if the type has been changed to ssh_home_t:

```
ls -Z -a /Installation_directory/meghadata/.ssh
```

Next steps

Make sure that you switch to the key-based authentication and SFTP protocol in the Analyzer probe UI > Reconfigure > Analyzer detail view server > Server Details.

Configuring key-based authentication for the Analyzer detail view server

You can configure the key-based authentication to download data on the Analyzer detail view server when data is directly uploaded to the Analyzer detail view server (without an intermediate FTP server).

Note: It is recommended that you use unique SSH host keys for every host that is using SSH and also implement SSH key management solution.

Before you begin

If the SFTP server subsystem setting is configured as `sftp internal-sftp` in the `/etc/ssh/sshd_config` file, make sure that the following entry is also present in this file:

```
Match User meghadata
        ForceCommand internal-sftp -u 2
```

Procedure

1. Log on to the Analyzer detail view server through an SSH client (like putty) as a root user.
2. Switch to the megha user:

   ```
   su - megha
   ```

3. Generate a key for the megha user:

   ```
   ssh-keygen -t rsa -b key_length
   ```

Note: Key length can be 2048 or 4096.

4. Press **Enter** to save the key in the folllowing directory under the installation directory (default: `/data`):

```
/Installation_directory/megha/.ssh/id_rsa
```

For example:

```
/data/megha/.ssh/id_rsa
```

5. (Optional) Enter a passphrase and confirm it.

Note:

- You cannot use quotation marks or spaces at the beginning or end of a passphrase, nor can you use contiguous multiple spaces within a passphrase.
- If you decide to use a passphrase, make sure you note it. You will need it when updating the data download settings.
- If you do not want to enter passphrase, press **Enter** and confirm it. A blank value is set.

6. Copy the public key:

```
ssh-copy-id meghadata@localhost
```

7. When prompted for the password, enter the meghadata user password (default: `meghadata123`).
8. Switch to the root user:

```
su - root
```

9. Configure the SELinux security context in the `/etc/selinux/targeted/contexts/files/file_contexts.local` file for the following directories available under the Analyzer detail view server installation directory (default: `/data`).
   - `/Installation_directory/meghadata/.ssh` directory:

     For example:

     ```
     semanage fcontext -a -t ssh_home_t /data/meghadata/.ssh
     ```

   - `/Installation_directory/meghadata/.ssh/authorized_keys` file:

     For example:

     ```
     semanage fcontext -a -t ssh_home_t /data/meghadata/.ssh/authorized_keys
     ```

10. Use the `restorecon` command to change file type to `ssh_home_t` for the following directories available under the Analyzer detail view server installation directory (default: `/data`):
    - `/Installation_directory/meghadata/.ssh directory`:

      For example:

      ```
      restorecon -R -v /data/meghadata/.ssh
      ```

    - `/Installation_directory/meghadata/.ssh/authorized_keys` file:

      For example:

      ```
      restorecon -R -v /data/meghadata/.ssh/authorized_keys
      ```

    - Verify the type has been changed to ssh_home_t:

      ```
      ls -Z -a /Installation_directory/meghadata/.ssh
      ```

      For example:

      ```
      ls -Z -a /data/meghadata/.ssh
      ```

11. Restart the sshd service:

    ```
    service sshd restart
    ```

Next steps

By default, password-based authentication is configured for downloading data to the Analyzer detail view server. If you want to switch to key-based authentication, see Updating the downloader on the Analyzer detail view server (on page 490).

Restricting SMTPS and STARTTLS TLS versions

Follow this procedure if you want to use a specific TLS version for SMTPS and STARTTLS communication.

Note:

- The Analyzer detail view server supports TLS versions 1, 1.1, and 1.2 for SMTPS and STARTTLS.
- The following communicatiom methods are supported:
  - SSL: SMTPS
  - TLS: STARTTLS

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 that the crond and megha services are stopped:

```
service crond status
```

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

5. Create a backup of the `custom.properties` file using the following command:

```
cp /usr/local/megha/conf/custom.properties /usr/local/megha/conf/
backup_custom_backup.properties
```

6. Edit the `custom.properties` file.

```
vi /usr/local/megha/conf/custom.properties
```

7. Add the following properties as required:
   - If you want to use the SMTPS protocol, add the following property:

     ssl.mail.smtp.encryption.protocols=*Protocol_version_1 Protocol_version_n*

     For example:

     ssl.mail.smtp.encryption.protocols=TLSv1.1 TLSv1.2

   - If you want to use the STARTTLS protocol, add the following property:

     tls.mail.smtp.encryption.protocols=*Protocol_version_1 Protocol_version_n*

     For example:

     tls.mail.smtp.encryption.protocols=TLSv1.2

8. Save the file and exit.
9. Start the megha service using the command:

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

10. Start the crond service using the following command:

```
service crond start
```

11. Confirm the crond and megha services have been started using the commands:

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

```
service crond status
```

Changing the Analyzer detail view server UI session timeout

By default, Analyzer detail view server UI sessions are closed after 30 minutes.

Note: If you do not want to stop the **crond** service, you can stop 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 440) and Starting the Analyzer detail view server or Analyzer probe server services (on page 439)

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. Add the following property to the `/usr/local/megha/conf/custom.properties` file:

```
user.session.expiry.timeout.in.secs=Time-in-seconds
```

6. Start the megha service using the command:

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

7. Start the crond service using the following command:

```
service crond start
```

Chapter 13: 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 **hcmds64srv** command.

Starting the Analyzer server services

To start the Analyzer server services, run the **hcmds64srv** command.

Before you begin

You must have root permission.

Procedure

1. Run the following command:

```
Common-component-installation-destination-directory/bin/hcmds64srv -start
```

Note:

- 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 **hcmds64srv** command.

Before you begin

You must have root permission.

Procedure

1. Run the following command:

```
Common-component-installation-destination-directory/bin/hcmds64srv -stop -server
server-name
```

Note:

- 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

- Make sure that the following disk space is available:
  - Analyzer probe server:
    - Installation directory: More than 5 GB or 5% available of the total disk space
    - `/etc`: 100 MB (Available)
    - `/tmp`: 100 MB (Available)

    Note: The Analyzer probe server retrieves the partition details where the directories are mounted and checks the free disk space. Make sure that the required disk space is available on partition in case multiple directories are mounted on it.
  - Analyzer detail view server:
    - Installation directory: More than 5 GB or 5% of the total disk space
    - `/tmp`: 500 MB (Available)
- 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
*/5 * * * * F=/usr/local/megha/bin/sysstat.sh; test -f $F && (bash $F >> /usr/
```

```
local/megha/logs/sys/`date +\%Y\%m\%d`.log; chown -R megha:megha /usr/local/
megha/logs/sys)
```

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
# */5 * * * * F=/usr/local/megha/bin/sysstat.sh; test -f $F && (bash $F >> /usr/
local/megha/logs/sys/`date +\%Y\%m\%d`.log; chown -R megha:megha /usr/local/
megha/logs/sys)
```

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 applies to 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/jp1pc/htnm/bin/htmsrv start -all
```

2. If you are starting the services after performing a restore operation, check the RAID Agent log file `htmRestDbEngineMessage#.log` (`#` refers to the log file number) to make sure that the KATR13248-E message is not logged before the KATR13244-I message is generated.

   Note that it might take about one hour from when the RAID Agent service starts until the KATR13244-I message is generated.

   If the KATR13248-E message is logged, RAID Agent restoration 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` file is located in `/opt/jp1pc/htnm/logs`.

To start services automatically:

1. Go to the required directory:

```
cd /opt/jp1pc
```

2. Set up the service automatic start script file (`jpc_start`) for the RAID Agent by copying the `.model` file (`jpc_start.model`) of the service automatic start script and adding execute permission as follows:

```
cp -p jpc_start.model jpc_start
chmod 555 jpc_start
```

3. Register the RAID Agent services in the OS.

a. Edit the service automatic start script (`/etc/rc.d/init.d/jp1_pc`):

```
#!/bin/sh
## Copyright (C) 2004, Hitachi, Ltd.
## Licensed Material of Hitachi, Ltd.
### BEGIN INIT INFO
# Provides: jp1_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. Run the following command:

```
chkconfig jp1_pc on
```

Stopping the RAID Agent services

Stop the RAID Agent services.

Note:

This procedure applies to 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 stop services manually:

Run the following command:

```
/opt/jp1pc/htnm/bin/htmsrv stop -all
```

To stop services automatically:

1. Go to the required directory:

```
cd /opt/jp1pc
```

2. Set up the service automatic stop script file (`jpc_stop`) for the RAID Agent by copying the `.model` file (`jpc_stop.model`) of the service automatic stop script and adding execute permission as follows:

```
cp -p jpc_stop.model jpc_stop
chmod 555 jpc_stop
```

3. Enable automatic service start. For details, see the section that describes starting services automatically in Starting the RAID Agent services (on page 440).
4. To ensure that the services can stop automatically, start the RAID Agent services by using one of the following methods depending on whether the services are running:
   - When the services are stopped:

     Use the **`systemctl`** command to start the services.

     ```
     systemctl start jp1_pc
     ```

   - When the services are running:

     When automatic service start is disabled, use the **`jpcspm`** command to stop the services and then use the **`systemctl`** command to start them.

     ```
     /opt/jp1pc/tools/jpcspm stop -key all
     systemctl start jp1_pc
     ```

     When automatic service start is enabled, you do not need to run any commands.

Starting the Virtual Storage Software Agent services

To start the Virtual Storage Software Agent services:

Procedure

1. Log on as root on the host where Virtual Storage Software Agent is installed.
2. Run the following command:

```
systemctl start virtualstoragesoftware-agent.service
```

Stopping the Virtual Storage Software Agent services

To stop the Virtual Storage Software Agent services:

Procedure

1. Log on as root on the host where Virtual Storage Software Agent is installed.

2. Run the following command:

```
systemctl stop virtualstoragesoftware-agent.service
```

Starting the On-demand real time monitoring module services

To start the On-demand real time monitoring services:

Before you begin

You must have root permissions.

Procedure

1. Log on to the Analyzer probe server.
2. Start the On-demand real time monitoring module services:

```
systemctl start analyzer-granular-data-collection-api
```

Stopping the On-demand real time monitoring module services

To stop the On-demand real time monitoring services:

Procedure

1. Log on to the Analyzer probe server.
2. Stop the On-demand real time monitoring module services:

```
systemctl stop analyzer-granular-data-collection-api
```

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 connecting with the Analyzer server.

Changing the Analyzer server host name

After stopping Analyzer server services by running the **`hcmds64srv`** command, change the host name of the Analyzer server.

Before you begin

You must have root permission.

Procedure

1. To stop the Analyzer server services, run the **`hcmds64srv`** command with the `stop` option.

2. Change the host name on the OS of the Analyzer server.
3. Change the host name specified in `ServerName` in the following file.

   Common-component-installation-destination-directory/uCPSB11/httpsd/conf/user_httpsd.conf

4. Change the host name specified in `command.hostname` in the following file.

   Analyzer-server-installation-directory/Analytics/conf/command_user.properties

5. If Ops Center Analyzer is registered with Common Services by using a host name, run the **setupcommonservice** command to update the host name:

   ```
   setupcommonservice -appHostname new-host-name
   ```

6. Restart the OS of the host on which the Analyzer server is installed.
7. Verify that the IP address can be resolved from the host name of the Analyzer server.
8. 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:

   Common-component-installation-destination-directory/conf/exauth.properties

9. 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 **hcmds64prmset** 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 **hcmds64srv** command, change the IP address of the Analyzer server.

Before you begin

You must have root permission.

Procedure

1. To stop Analyzer server services, run the **hcmds64srv** command with the `stop` option.
2. Change the IP address on the OS of the Analyzer server.
3. If Ops Center Analyzer is registered with 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. 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:

   `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 **`hcmds64prmset`** command to change the Common component settings.
   b. Restart Ops Center Automator.

Changing the port number used between Analyzer server and the web browser

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.

If SSL communication is used between the Analyzer server and the web browser, see Changing the SSL port number between the Analyzer server and a web browser (on page 447).

Before you begin

You must have the root permission.

Procedure

1. To stop Analyzer server services, run the **`hcmds64srv`** command with the `stop` option.
2. Change the port numbers in the following definition files:
   - *`Common-component-installation-destination-directory`*`/uCPSB11/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.

Use the **`firewall-cmd`** command to specify the port number used by the Analyzer server for the port that has the zone applied.

a. Specify the service name to enable 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`.

b. For the port that has the zone applied, specify a combination of the port number to use for the Analyzer server and the protocol.

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`.

4. To start the Analyzer server services, run the **`hcmds64srv`** command with the `start` option.

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.

a. To change the Common component settings, run the **`hcmds64prmset`** command.

b. Restart Ops Center Automator.

Changing the SSL port number between the Analyzer server and a web browser

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. To stop the Analyzer server services, run the **`hcmds64srv`** command with the `stop` option.

2. Change the port numbers in the following definition files:
   - *Common-component-installation-destination-directory*/uCPSB11/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.

   Use the **firewall-cmd** command to specify the port number used by the Analyzer server for the port that has the zone applied.

   a. Specify the service name to enable 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`.

   b. For the port that has the zone applied, specify a combination of the port number to use for the Analyzer server and the protocol.

      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`.

4. If you are using Common Services, run the **setupcommonservice** command to update the port number.

   ```
   setupcommonservice -appPort new-port-number
   ```

5. To start the Analyzer server services, run the **`hcmds64srv`** command with the `start` option.
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 **`hcmds64prmset`** 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 definition files.

Before you begin

You must have root permission.

Procedure

1. To stop the Analyzer server services, run the **`hcmds64srv`** command with the `stop` option.
2. Edit the following definition files:
   - *`Common-component-installation-destination-directory`*`/uCPSB11/httpsd/conf/reverse_proxy.conf`

     Change the port number (27100) in the following lines to a port number that is not used for anything else:

     ```
     ProxyPass /Analytics/ http://127.0.0.1:27100/Analytics/ timeout=3600
     ProxyPassReverse /Analytics/ http://127.0.0.1:27100/Analytics/
     ```

   - *`Common-component-installation-destination-directory`*`/uCPSB11/CC/server/usrconf/ejb/AnalyticsWebService/usrconf.properties`

     Change the port numbers (27100, 27102, 27103, and 27104) in the following lines to a port number that is not used for anything else:

     ```
     webserver.connector.nio_http.port=27100
     ejbserver.http.port=27102
     ejbserver.rmi.remote.listener.port=27103
     ejbserver.rmi.naming.port=27104
     ```

3. To start the Analyzer server services, run the **`hcmds64srv`** command with the `start` option.

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 root permission.

Procedure

1. To stop the Analyzer server services, run the **`hcmds64srv`** command with the `stop` option.
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. To start the Analyzer server services, run the **`hcmds64srv`** command with the `start` option.

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

You can use the backup and restore functions to migrate Analyzer components to a different host.

For details, see Overview of Ops Center Analyzer backup and restore (on page 509).

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 root permission.

Procedure

1. Run the **`hcmds64prmset`** command to change the settings of the Common component.
   - When changing the host name or IP address:

     ```
     Common-component-installation-destination-directory/bin/hcmds64prmset -host
     host-name-or-IP-address-of-Device-Manager
     ```

   - When changing the port number:

     ```
     Common-component-installation-destination-directory/bin/hcmds64prmset {-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 **`hcmds64srv`** command with the `stop` option to stop the Analyzer server services.
   b. Run the **`hcmds64srv`** 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:

   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 the Analyzer detail view server

You can change the IP address of the host on which Analyzer detail view server is installed, or the port number that is used to connect to Analyzer probe server.

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 root permission.

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 445).
   - 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 Analyzer detail view server connection details on the Analyzer probe server (on page 453).
3. Reconfigure the connection with the Analyzer server. For details, see Reconfiguring the connection with Analyzer detail view server (on page 454).
4. If Analyzer detail view server is registered with Common Services by using an IP address, run the **`setupcommonservice`** command to update the IP address.

```
setupcommonservice -appHostname new-IP-address -appPort port-number
```

Updating Analyzer detail view server connection details 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. You can also update the authentication type to switch between password-based authentication and key-based authentication.

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**.

     Note:
     - For the SFTP protocol, you can use key-based or password-based authentication. If you plan to use key-based, make sure that it is configured. Key-based authentication is supported for sending data directly from the Analyzer probe server to the Analyzer detail view server (without an intermediate FTP or FTPS server) using the meghadata user. Refer to Configuring key-based authentication to transfer data directly from Analyzer probe server to Analyzer detail view server (on page 431). After configuring key-based authentication, select the SFTP protocol and then click Key-Based. If you have configured a passphrase, enter it when prompted.
     - The System Diagnostics data for the Analyzer probe server is not collected in case of HTTPS protocol.
   - **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.

Changing the default SSH port on the Analyzer detail view server

When you are using the HTTPS protocol to transfer data from the Analyzer probe server to the Analyzer detail view server, if you have configured non-default SSH port on the machine where the Analyzer detail view server is installed, make sure that you configure the same non-default port in Analyzer detail view server to download the Analyzer probe server data.

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. Open the `ftp.properties` file:

```
vi /usr/local/httpProxy/conf/target/ftp.properties
```

5. Enter the non-default SSH port.

```
FtpPort=Non-default-SSH-Port
```

For exmaple:

```
FtpPort=23
```

6. Start the HTTP proxy service by using the command:

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

7. Confirm whether the HTTP proxy service has started by using the command:

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

Enabling snapshot size data collection for Hitachi NAS storage system

By default, the Hitachi NAS probe does not collect the Hitachi NAS File System resource snapshot size data from Analyzer probe v10.8.0-00 or later. To collect the snapshot size data, you need to enable data collection on the Analyzer probe. However, enabling the data collection might cause the Hitachi NAS system reboot problem. Therefore, we only recommend enabling snapshot size data collection if the system reboot problem has been fixed in your target Hitachi NAS system.

To enable the snapshot size data collection, configure the properties described here.

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 all the services using the command:

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

4. Confirm the crond and megha services have been stopped using the commands:

   ```
   service crond status
   ```

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

5. Create a backup of the `custom.properties` file using the following command:

   ```
   cp /usr/local/megha/conf/custom.properties /usr/local/megha/conf/
   backup_custom_backup.properties
   ```

6. Edit the `custom.properties` file.

   ```
   vi /usr/local/megha/conf/custom.properties
   ```

7. Add the following property:

   ```
   hnas_snapshot-size.data.collection=true
   ```

8. Save the file and exit.
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
```

11. Confirm the crond and megha services have been started using the commands:

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

Changing the port for On-demand real time monitoring of Hitachi Enterprise Storage

By default, port 24262 is used for communication between the Analyzer detail view server and RAID Agent server for On-demand real time monitoring. To change this default, you must configure properties in the Analyzer detail view server.

Before you begin

If the Analyzer detail view server is receiving data from multiple RAID Agent servers and you want to configure a separate port for each server, you need to know the RAID Agent server IP addresses available in the Analyzer detail view server. To identify those RAID Agent server IP addresses, do the following:

1. Log on to the Analyzer detail view UI.
2. From the left pane, click **Reports** > **Build**.

   The **Build** window opens.
3. Click **Create Using MQL**.
4. Enter the following query in the **MQL** box using the following format:

   ```
   raidStorage[=serialNumber rx serialNumber]/raidAgentInstance[=raHost rx .*]
   ```

   For example:

   ```
   raidStorage[=serialNumber rx 421358]/raidAgentInstance[=raHost rx .*]
   ```
5. Click **View Result**.

   The **View Result** window opens.
6. In the **View Result** window, click the desired resource in the **Resource** column.

   The RAID Agent server IP address is displayed in the **RAID Agent Host** column.
7. Copy the IP address.

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. Make a backup of the `custom.properties` file:

```
cp /usr/local/megha/conf/custom.properties /usr/local/megha/conf/
custom_orig.properties
```

5. Edit the `custom.properties` file.

```
vi /usr/local/megha/conf/custom.properties
```

6. Change the port as follows:
   - If you want to use one port to communicate with all RAID Agent servers available in Analyzer detail view server, add the following property:

     ```
     default.raidAgent.port=port_Number
     ```

     For example:

     ```
     default.raidAgent.port=25663
     ```

   - If you want to use a different port to communicate with each RAID Agent server, add a separate entry for each server as follows:

     ```
     RAID_Agent_Server_IP_address.raidAgent.port=Port_Number
     ```

     For example:

     ```
     192.168.100.52.raidAgent.port=80
     192.168.20.27.raidAgent.port=89
     ```

7. Save the `custom.properties` file.
8. Start the megha service and verify the status:

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

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

9. Start the crond service and verify the status:

```
service crond start
```

```
service crond status
```

Changing the system information of the Analyzer probe server

Use these procedures to 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, or 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, you must also change the host name by performing the following procedure if the Hitachi Enterprise Storage probe is added.

Note:

This procedure applies to the RAID Agent installed with Ops Center Analyzer. If you are using Tuning Manager - Agent for RAID, see the *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 repeat 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 standard 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
   # */5 * * * * F=/usr/local/megha/bin/sysstat.sh; test -f $F && (bash $F
   >> /usr/local/megha/logs/sys/`date +\%Y\%m\%d`.log; chown -R
   megha:megha /usr/local/megha/logs/sys)
   ```

   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/jp1pc/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.

   Run the **`jpcconf host hostname`** command to change the monitoring host name.

   The following example of the command changes the physical host name to `host02`:

   ```
   /opt/jp1pc/tools/jpcconf host hostname -newhost host02 -d /root/backup
   ```

   Do not run any other commands while running the **`jpcconf host hostname`** command.

   Tip: If the command fails, the RAID Agent configuration file is stored in the directory specified for the **`-d`** option of the **`jpcconf host hostname`** command. If 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/jp1pc/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. If Analyzer probe server is registered with Common Services by using a host name, run the **`setupcommonservice`** command to update the host name:

   ```
   setupcommonservice -appHostname new-host-name -appPort port-number
   ```

9. 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/jp1pc/htnm/bin/htmsrv start -all
   ```

10. 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 standard schedule that generates output for the Analyzer probe server:

```
*/5 * * * * F=/usr/local/megha/cron.5min; 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; chown -R
megha:megha /usr/local/megha/logs/sys)
```

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
```

11. 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.

12. 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*.

13. 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.

14. 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 when the Hitachi Enterprise Storage probe is not added

Use this procedure only if the 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 standard 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
   # */5 * * * * F=/usr/local/megha/bin/sysstat.sh; test -f $F && (bash $F
   >> /usr/local/megha/logs/sys/`date +\%Y\%m\%d`.log; chown -R
   megha:megha /usr/local/megha/logs/sys)
   ```

   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/jp1pc/htnm/Rest/config/htnm_httpsd.conf
   ```

4. If Analyzer probe server is registered with Common Services by using a host name, run the **`setupcommonservice`** command to update the host name:

   ```
   setupcommonservice -appHostname new-host-name -appPort port-number
   ```

5. 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 standard schedule that generates output for the Analyzer probe server:

   ```
   */5 * * * * F=/usr/local/megha/cron.5min; 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; chown -R
megha:megha /usr/local/megha/logs/sys)
```

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
```

6. 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.

7. 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 standard 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
# */5 * * * * F=/usr/local/megha/bin/sysstat.sh; test -f $F && (bash $F
>> /usr/local/megha/logs/sys/`date +\%Y\%m\%d`.log; chown -R
megha:megha /usr/local/megha/logs/sys)
```

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/jp1pc/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. If Analyzer probe server is registered with Common Services by using an IP address, run the **`setupcommonservice`** command to update the IP address.

```
setupcommonservice -appHostname new-IP-address -addPort port-number
```

8. Run the following command to start the RAID Agent services.

```
/opt/jp1pc/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 standard schedule that generates output for the Analyzer probe server:

```
*/5 * * * * F=/usr/local/megha/cron.5min; 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; chown -R
megha:megha /usr/local/megha/logs/sys)
```

c. Run the following command:

```
/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 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.

11. 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.

12. 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 standard 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
# */5 * * * * F=/usr/local/megha/bin/sysstat.sh; test -f $F && (bash $F
```

```
>> /usr/local/megha/logs/sys/`date +\%Y\%m\%d`.log; chown -R
megha:megha /usr/local/megha/logs/sys)
```

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. If Analyzer probe server is registered with Common Services by using an IP address, run the **setupcommonservice** command to update the IP address.

```
setupcommonservice -appHostname new-IP-address -addPort Port Number
```

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 standard schedule that generates output for the Analyzer probe server:

```
*/5 * * * * F=/usr/local/megha/cron.5min; 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; chown -R
megha:megha /usr/local/megha/logs/sys)
```

   c. Run the following command:

```
/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.

Setting the time zone on the Analyzer probe server

You must set the Canonical/Standard time zone on the Analyzer probe server.

Procedure

1. Log on to the Analyzer probe server through an SSH client (like **`putty`**) as a root user.
2. Run the following command to check the time zone:

   ```
   timedatectl status | grep "Time zone"
   ```

   Sample output:

   ```
   Time zone: Asia/Bahrain (+03, +0300)
   ```

   The `Asia/Bahrain` time zone in the above sample output is not a Standard/Canonical time zone. Its corresponding Canonical/Standard time zone is `Asia/Qatar`.
3. Run the following command to set the Canonical/Standard time zone:

   ```
   sudo timedatectl set-timezone Canonical_Standard_time_zone
   ```

   For example:

   ```
   sudo timedatectl set-timezone Asia/Qatar
   ```
4. Run the following command to verify whether the time zone is changed to Canonical/Standard time zone:

   ```
   timedatectl status | grep "Time zone"
   ```

   Sample output:

   ```
   Time zone: Asia/Qatar (+03, +0300)
   ```
5. Stop the crond service:

   ```
   service crond stop
   ```
6. Stop the megha service:

   ```
   /usr/local/megha/bin/megha-jetty.sh stop
   ```
7. Verify the stopped status of the megha service:

   ```
   /usr/local/megha/bin/megha-jetty.sh status
   ```
8. Start the megha service:

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

9. Start the crond service:

```
service crond start
```

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/jp1pc/htnm/bin/htmsrv stop -all
```

2. Run the **`jpcnsconfig port`** command:

```
/opt/jp1pc/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: ▪ 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/jp1pc/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/jp1pc/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: `/opt/jp1pc/htnm/Rest/config/htnm_httpsd.conf`
24222 (Access port for RAID Agent REST Web Service for SSL communication)	
24223 (Port number for RAID Agent REST Application Service)	Change the values for the following properties. You must specify the same value for both properties: ▪ The `ProxyPass` and `ProxyPassReverse directive` property in the `/opt/jp1pc/htnm/Rest/config/htnm_httpsd.conf` file ▪ The `webserver.connector.nio_http.port` property in the `/opt/jp1pc/htnm/HBasePSB/CC/server/usrconf/ejb/AgentRESTService/usrconf.properties` file
24224 (Port number of RMI registry used by RAID Agent REST Application Service)	Change the value of the following property: The `ejbserver.rmi.naming.port` property in the `/opt/jp1pc/htnm/HBasePSB/CC/server/usrconf/ejb/AgentRESTService/usrconf.properties` file
24225 (Port number server management commands used to communicate with RAID Agent REST Application Service)	Change the value for the following property: The `ejbserver.rmi.remote.listener.port` property in the `/opt/jp1pc/htnm/HBasePSB/CC/server/usrconf/ejb/AgentRESTService/usrconf.properties` 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 `ejbserver.http.port` property in the `/opt/jp1pc/htnm/HBasePSB/CC/server/usrconf/ejb/AgentRESTService/usrconf.properties` file

3. Run the following command to start the RAID Agent services:

```
/opt/jp1pc/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 438).

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/jp1pc/htnm/bin/htmsrv stop -all
```

2. Open the `htnm_httpsd.conf` file.

   The `htnm_httpsd.conf` file is located in the following directory:

   `/opt/jp1pc/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/jp1pc/htnm/bin/htmsrv start -all
```

Changing the data collection intervals of Analyzer detail view performance metrics

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. Refer to Changing the RAID Agent record collection interval for Hitachi Enterprise Storage probe (on page 474).
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 475).

Changing the RAID Agent record collection interval for Hitachi Enterprise Storage probe

You might need to change the RAID Agent record collection interval for the Hitachi Enterprise Storage probe (for example, to match the interval defined for RAID Agent). In this case, you must edit the Hitachi Enterprise Storage probe.

Procedure

1. In the **Status** window, stop the instance of the Hitachi Enterprise Storage probe.
2. Click the **Edit** link.
3. In the **Edit Hitachi Enterprise Storage Probe** window, click the **Edit Collection Interval** link and change the RAID Agent record collection interval.
4. Click **Save** and then click **Next**.
5. In the **Validation** window, click **Next**, and then click **OK**.

6. In the **Status** window, in **Action**, click **Start**.

Changing data collection intervals for RAID Agent

Use the **`collection_config`** command to change data collection intervals for RAID Agent. The data collection interval for the Hitachi Enterprise Storage probe must be the same as for RAID Agent.

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. Run 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. Run the following command to change data collection intervals:

```
/opt/hitachi/Analytics/bin/collection_config changeinterval  -at AccessType -r
record-ID -i deta-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 = Agent REST Web Service).
KATR15101-I The service is stopping. (service = 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. Run 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/jp1pc/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/jp1pc/htnm/bin/htmsrv stop -all
```

4. Delete the instance environment using this command:

```
/opt/jp1pc/tools/jpcinsunsetup agtd -inst instance-name
```

The following example shows how to delete the instance environment 35053:

```
/opt/jp1pc/tools/jpcinsunsetup agtd -inst 35053
```

5. Run the following command to start the RAID Agent services:

```
/opt/jp1pc/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 data collection. If you observe problems after enabling the data collection for these metrics, you can change the collection interval for all metrics collected by the Brocade Network Advisor probe. Contact customer support for the procedure of changing data collection interval.

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 following command:

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

11. Start the crond service using the following command:

```
service crond start
```

Changing the configuration information collection time

If RAID Agent fails to collect performance information 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 longer than a minute, the performance data 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 skipped even if the configuration information collection takes a minute or more.

Note:

- RAID Agent collects, performance data from storage systems as follows: configuration information is collected as PD 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`).

If you do so, 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 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	1300

To change the timing of configuration information collection, you must review the disk space allocated to Analyzer probe server. For each storage system being monitored, the /opt/jp1pc directory must have 350 MB free disk space.

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
- PD_ELC
- PD_HGC
- PD_HHGC
- PD_LDC
- PD_LHGC
- PD_LSEC
- PD_LWPC

- PD_NHC
- PD_NNC
- PD_NNPC
- PD_NSPC
- PD_NSSC
- PD_PTC
- PD_PWPC
- PD_RGC

By default, data collection starts on an hourly basis. The collected configuration information is stored in PD records that are generated at the same time.

When the collection time definition file is used, the on-the-hour collection 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 hourly and for the real-time report until the next time configuration information is collected.

Example:

Even if configuration information is collected twice a day at 00:00 and 12:00, the PD records are generated hourly. 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 of PI records. The timing of changes 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 changes 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.

  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 value, 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 a file for each instance.)

The the collection time definition files are saved in this directory:

`/opt/jp1pc/agtd/agent/`*`instance-name/`*

You can create the collection time definition file using the sample file (`conf_refresh_times.ini.sample`) contained in the same directory.

Specify collection times in `hh:mm` format.

Rules for specifying times in the collection time definition file

- You can only use single-byte characters.
- Hours (`hh`) and minutes (`mm`) must be specified as two digits.
- The time must be specified in 24-hour format (00:00 to 23:59).
- One entry per line.
- There is a maximum 48 entries (times).
- Anything beyond five characters (`hh:mm`) is 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 the above rules are ignored.
- If the collection time definition file does not contain any valid lines, collection occurs only once when RAID Agent starts and data 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 following directories:

`/opt/jp1pc/log/jpclog01`

`/opt/jp1pc/log/jpclog02`

If the collection of performance information is skipped, the KAVE00213-W message is output to the log file. If you see this message, revise the settings in the collection time definition file.

The definitions in the collection time definition file are not run if you save the file while RAID Agent is being started or after RAID Agent has started.

Changing the maximum C/T delta value monitored when analyzing Universal Replicator performance

By default, the maximum value of C/T delta is set to 3,600 seconds. If you perform monitoring with the maximum value of C/T delta set to a value greater than the default value, the amount of memory used by the Analyzer probe server increases. To change the maximum value of C/T delta, edit the `collectcommonconfig.ini` file.

Procedure

1. Check the amount of increase in memory usage.

   You can calculate the amount of the increase by using the following formula:

   6,144,000 bytes x ((*maximum-value-of-C/T-delta* - 3600) / 3600) x *number-of-storage-systems-to-be-monitored*

2. Open the `collectcommonconfig.ini` file.

   The `collectcommonconfig.ini` file is stored in the following location:

   `/opt/jp1pc/agtd/agent`

3. Specify the maximum value of C/T delta (in seconds).

   Specify the following setting and value:

   - Setting: `MAX_VALUE`
   - Specifiable values: 3600 to 86400

   For example:

```
[CT_DELTA]
MAX_VALUE=3600
```

Enabling the Linux host processes data collection

By default, the Linux probe does not collect the processes data for a new installation of the Analyzer probe server v10.8.0-00 and later. To collect the processes data, you need to enable their data collection on the Analyzer probe. However, enabling the processes data collection might impact the Linux probe data collection and importing on the Analyzer detail view server. Therefore, it is recommended to enable the processes data collection if the processes running on the Linux host are not changed frequently and the total process count is not more than 1000.

Note:

- When you upgrade to the Analyzer probe server v10.8.0-00 or later and if a Linux probe is already added in the previous versions, the Linux host processes data collection is enabled by default. Disable it, if you observe the Linux probe data collection problem.
- When you upgrade to the Analyzer probe server v10.8.0-00 or later and if a Linux probe is not added in the previous versions, the Linux host processes data collection is disabled by default. You can enable it, if required.

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 that the crond and megha services are stopped:

   ```
   service crond status
   ```

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

5. Create a backup of the `custom.properties` file using the following command:

   ```
   cp /usr/local/megha/conf/custom.properties /usr/local/megha/conf/
   backup_custom_backup.properties
   ```

6. Edit the `custom.properties` file.

   ```
   vi /usr/local/megha/conf/custom.properties
   ```

7. Add one of the following property as required:
   - To enable the Linux host processes data collection, add the following property:

     ```
     collectHostProcessResource=true
     ```

   - To disable the Linux host processes data collection, add the following property:

     ```
     collectHostProcessResource=false
     ```

8. Save the file and exit.
9. Start the megha service using the command:

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

10. Start the crond service using the following command:

```
service crond start
```

11. Confirm the crond and megha services have been started using the commands:

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

```
service crond status
```

Changing the port number of the On-demand real time monitoring module

To change the port number of the On-demand real time monitoring module, perform the following procedure.

Before you begin

You must have root permissions.

Procedure

1. Log on to the Analyzer probe server.
2. Stop the On-demand real time monitoring module service:

```
systemctl stop analyzer-granular-data-collection-api
```

3. Modify the following file:
   `/opt/hitachi/Analytics/granular-data-collection-api/conf/user-granular-data-collection-api.conf`

   Change the port specified in the `GRANULAR_DATA_COLLECTION_API_PORT` property to the one you want to use.
4. If necessary, configure the firewall to allow use of the port.
5. Start the On-demand real time monitoring module service:

```
systemctl start analyzer-granular-data-collection-api
```

Restricting the servers that can access the On-demand real time monitoring module

To enhance security, you can specify that only trusted servers can access the On-demand real time monitoring module. To specify the name of the servers permitted to access the module, edit the `user-granular-data-collection-api.conf` file.

Before you begin

You must have root permissions.

Procedure

1. Log on to the Analyzer probe server.
2. Stop the On-demand real time monitoring module service:

```
systemctl stop analyzer-granular-data-collection-api
```

3. For the following property file, specify the IP address of each Analyzer detail view server that can access the On-demand real time monitoring module:

   `/opt/hitachi/Analytics/granular-data-collection-api/conf/user-granular-data-collection-api.conf`

   Specify the IP addresses as shown in the following example. You can also use CIDR notation for each network. To specify multiple IP addresses, separate them with commas.

   Example:

```
GRANULAR_DATA_COLLECTION_API_ALLOWED_IP_ADDRESS=127.0.0.1, 127.0.0.2
```

   If you specify 0.0.0.0/0, access from all hosts is permitted.

4. Start the On-demand real time monitoring module service:

```
systemctl start analyzer-granular-data-collection-api
```

Upgrading the JDK for Virtual Storage Software Agent

If you want to use a newer version of Amazon Corretto 8, complete the following procedure to upgrade.

Before you begin

Check the release notes for the Amazon Corretto 8 versions supported by Virtual Storage Software Agent.

Procedure

1. Check the Amazon Corretto 8 version installed on the Virtual Storage Software Agent host.
   - If the version is the latest supported by Virtual Storage Software Agent, you do not need to do anything.
   - If the version is not the latest, continue to the next step.
2. From the Amazon Corretto site, download the latest JDK version, and then install it on the host where Virtual Storage Software Agent is installed.
3. Run the RPM command to upgrade Amazon Corretto 8.

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 More Actions menu. Certain management tasks require logging into the Analyzer detail view server as the `admin` user instead of using the More Actions 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	The probe status is displayed in any one of the following four colors: Stopped (Grey): Probe is stopped. Running (Green): Probe is collecting data from targets. Error (Red): Probe has abruptly stopped collecting data. Processing delay (Yellow): Probe is running behind schedule.

	Stopping/Monitoring Stopped (Black): Probe has stopped monitoring targets or probe is stopping .
ACTION	Displayed when the probe is stopped or started. You can perform the following tasks using links in this column: Stop: Stops the probe Start: Starts data collection Edit: Let you edit the probe Delete: Deletes the probe
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

You must update the downloader details on the Analyzer detail view server if any of the following conditions apply:

- You are currently downloading the data from an intermediate FTP server and you need to update the connection details for the Analyzer detail view server or intermediate FTP server.
- You are directly uploading data to the Analyzer detail view server (without an intermediate FTP server) and you want to switch between password-based authentication and key-based authentication.

Before you begin

Note: If you do not want to stop the **crond** service, you can stop 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 440) and Starting the Analyzer detail view server or Analyzer probe server services (on page 439)

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. Run the update FTP configuration script to update the FTP server details:

- If you are downloading the data from an intermediate FTP server using the password-based authentication and you want to update the connection details for the Analyzer detail view server or intermediate FTP server:
  - To download data of all the Analyzer probe server appliances:

    ```
    sh /usr/local/megha/bin/createOrUpdateFTPConfiguration.sh --update --
    authType Password-Based --ftpServer FTP-server-hostname-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 --update --
    authType Password-Based --ftpServer 192.168.1.2 --ftpMethod SFTP --ftpPort
    22 --ftpUsername abc --ftpPassword
    ```

    Note:

    - The `authType`, `ftpServer`, and `ftpUsername` parameters are mandatory.
    - You cannot update the value of the `ftpServer` and `ftpUsername` parameters.
    - The value for the `authType` parameter must be `Password-Based` to download the data from an intermediate FTP server.
    - 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.

  - To download the data of the specific Analyzer probe server appliance:

    ```
    sh /usr/local/megha/bin/createOrUpdateFTPConfiguration.sh --update --
    authType Password-Based --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 --
    authType Password-Based --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 `authType`, `ftpServer`, and `ftpUsername` parameters are mandatory.
- You cannot update the value of the `ftpServer` and `ftpUsername` parameters.
- The value for the `authType` parameter must be `Password-Based` to download the data from an intermediate FTP server.
- 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.
- You should use the `ftpPassword` parameter if you are downloading the data from an intermediate FTP server. 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.

- To switch between password-based authentication and key-based authentication:
  - Switching to key-based authentication:

    ```
    sh /usr/local/megha/bin/createOrUpdateFTPConfiguration.sh --update --
    authType Key-Based --ftpServer localhost --ftpMethod SFTP --ftpPort FTP-
    Port --ftpUsername meghadata --keyPassphrase
    ```

    For example:

    ```
    sh /usr/local/megha/bin/createOrUpdateFTPConfiguration.sh --update --
    authType Key-Based --ftpServer localhost --ftpMethod SFTP --ftpPort 22 --
    ftpUsername meghadata --keyPassphrase
    ```

  - Switching to password-based authentication:

    ```
    sh /usr/local/megha/bin/createOrUpdateFTPConfiguration.sh --update --
    authType Password-Based --ftpServer localhost --ftpMethod FTP-method-(FTP/
    FTPS/SFTP) --ftpPort FTP-Port --ftpUsername meghadata --ftpPassword
    ```

    For example:

    ```
    sh /usr/local/megha/bin/createOrUpdateFTPConfiguration.sh --update --
    authType Password-Based --ftpServer localhost --ftpMethod SFTP --ftpPort
    22 --ftpUsername meghadata --ftpPassword
    ```

Note:

- The `authType`, `ftpServer` and `ftpUsername` parameters are mandatory.
- You cannot update the value of the `ftpServer`, `ftpUsername`, and `ftpPassword` parameters. If you want to change the `ftpPassword` of the meghadata user, use the **`changePassword.sh`** command. See Changing the megha and meghadata passwords (on page 108) for more information.
- Key-based authentication only supports the SFTP method
- You must enter the `keyPassphrase` parameter when switching to key-based authentication for the first time. When configuring key-based authentication to download data to Analyzer detail view server:
  - If you have provided a passphrase, you must enter it when prompted.
  - If you set a blank passphrase, press Enter when prompted.

    See Configuring key-based authentication for the Analyzer detail view server (on page 433) for more information.

6. Enter the passphrase or blank value if you have provided the `keyPassphrase` parameter or enter the meghadata user password if you have provided the `ftpPassword` parameter.

7. Start the megha service using the following command:

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

8. Start the crond service using the following 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	Contains the logs of the following activities: ▪ Operating system upgrade ▪ Data export using Custom Reports ▪ Time zone settings ▪ Manage menu settings **Note:** On the Analyzer probe server, the time zone details are not logged.	✓	✓
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 `20-nproc.conf` file, if it does not exist.

   b. Ensure that the following two properties are present in the `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.

Default meghadata user settings for Analyzer detail view server

During the RPM installation, the Analyzer detail view server checks the existing SFTP server subsystem settings in the `/etc/ssh/sshd_config` file and updates the settings as follows:

- If the SFTP server subsystem setting is configured as `sftp /usr/libexec/openssh/sftp-server`, the Analyzer detail view server adds the following entries at the end of the file:

```
Match User meghadata
PasswordAuthentication yes
```

- If the SFTP server subsystem setting is configured as `sftp internal-sftp`, the Analyzer detail view server adds the following entries at the end of the file:

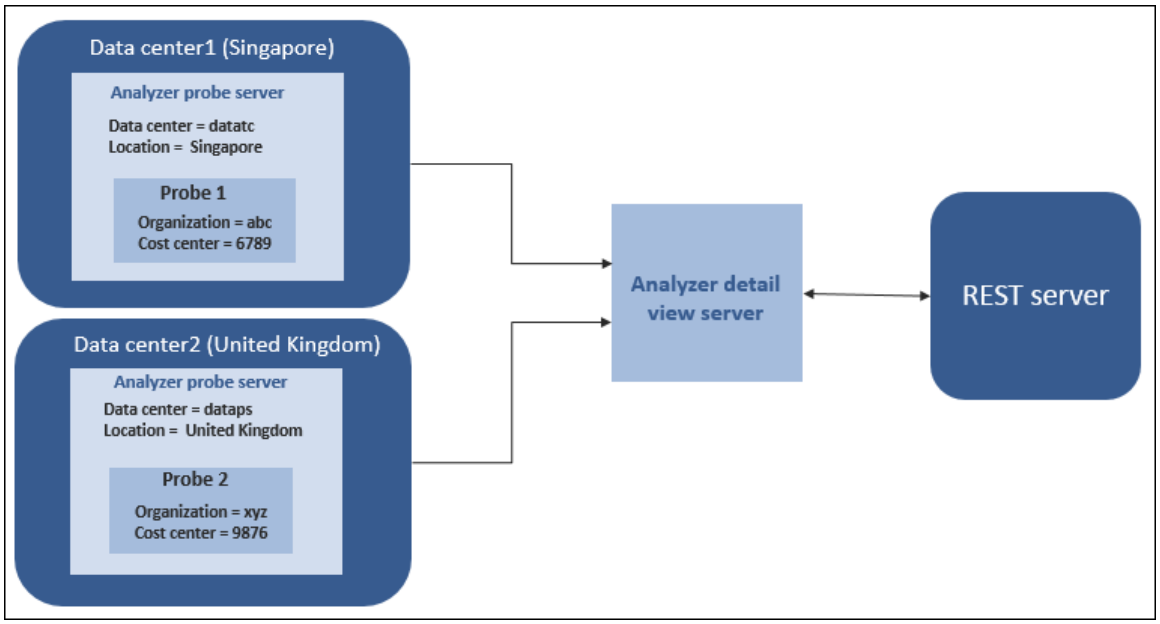
```
Match User meghadata
PasswordAuthentication yes
ForceCommand internal-sftp -u 2
```

Note: If you make any changes for the SFTP server subsystem setting, make sure that the meghadata entries in the `sshd_config` file match the account settings for the meghadata user on the Analyzer detail view server. Restart the Secure Shell Daemon (sshd) service if you make any changes in the `sshd_config` file.

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.

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
```

Changing UID and GID on the Analyzer detail view server and Analyzer probe server

You can change the User Identifier (UID) and Group Identifier (GID) for the `megha` and `meghadata` users. When installing the Analyzer detail view server and Analyzer probe server, the UID and GID are assigned to these users by the operating system.

This is an optional procedure to enhance security.

Note:

- The `megha` user is created for the Analyzer detail view server and Analyzer probe server.
- The `meghadata` user is created only for the Analyzer detail view server.

Changing UID and GID on the Analyzer detail view server

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 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 using the commands:

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

```
service crond status
```

5. Change the UID and GID of the `megha` and `meghadata` users using the commands:

```
usermod -u UID megha
```

```
usermod -u UID meghadata
```

```
groupmod -g GID megha
```

Note:

- Make sure that the new UID and GID is available (not assigned to any other existing user or group).
- The group of the `megha` and `meghdata` users is `megha`.

For example:

```
usermod -u 1005 megha
```

```
usermod -u 1006 meghadata
```

```
groupmod -g 1005 megha
```

6. Verify the UID and GID of the `megha` and `meghdata` users:

```
id megha
```

```
id meghadata
```

7. Change ownership:

   a. Run the following commands to change the ownership of the directories present under installation directory. By default, the Analyzer detail view server is installed at: `/data`. (The `megha` and `meghadata` directories are created in it.) You must change the ownership of both directories:

      - `megha` directory:

        ```
        chown -R megha:megha Installation-directory/megha
        ```

        `Installation-directory`: Type the installation directory that was provided at the time of installation.

        For example:

        ```
        chown -R megha:megha /data/megha
        ```

      - `meghadata` directory:

        ```
        chown -R meghadata:megha Installation-directory/meghadata
        ```

        For example:

        ```
        chown -R meghadata:megha /data/meghadata
        ```

b. Change the ownership of the following directoies:

```
chown -R meghadata:megha /home/meghadata
```

```
chown -R megha:megha /usr/local/megha
```

```
chown -R meghadata:megha /usr/local/megha/db/probe/data/*
```

```
chown -R meghadata:megha /usr/local/megha/db/probe/raw/*.zip
```

```
chown -R meghadata:megha /usr/local/megha/db/probe/raw/*.txt
```

```
chown -R megha:megha /usr/local/httpProxy
```

c. Change the ownership of files in the `/tmp` directory:

i. Navigate to the `/tmp` directory:

```
cd /tmp
```

ii. Run the following command to change ownership:

```
chown megha:megha importStatus.properties.old
probeDataDownloadConfig_localhost_meghadata.properties.old
RealtimeDataImportStatus.properties.old
rollup.custom.task.properties.old rollup.status.properties.old
```

Note: If any of these files is not available, an error message is displayed; ignore it.

8. Verify the ownership of all the above directories:

For example:

```
ls -lrt /usr/local/megha
```

9. Start the megha service and check if it is started:

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

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

10. Start the crond service using the command:

```
service crond start
```

Changing UID and GID on the Analyzer probe server

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 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 using the commands:

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

```
service crond status
```

5. Stop the Xinetd service:

```
service xinetd stop
```

6. Change the UID and GID of the `megha` user using the commands:

```
usermod -u UID megha
```

```
groupmod -g GID megha
```

> **Note:** Make sure that the new UID and GID is available (not assigned to any other existing user or group).

For example:

```
usermod -u 1005 megha
```

```
groupmod -g 1005 megha
```

7. Verify the UID and GID of the `megha` user:

```
id megha
```

8. Change ownership:
   a. Run the following command to change the ownership of the directory present under installation directory. By default, the Analyzer probe server is installed at: `/home`. (The `megha` directory is created in it.) Change the ownership of this directory:

```
chown -R megha:megha Installation-directory/megha
```

Installation-directory: Type the installation directory provided at the time of installation.

For example:

```
chown -R megha:megha /home/megha
```

b. Change the ownership of the `/usr/local/megha` directory:

```
chown -R megha:megha /usr/local/megha
```

c. Change the ownership of files in the `/tmp` directory:

i. Navigate to the `/tmp` directory:

```
cd /tmp
```

ii. Run the following command to change ownership:

```
chown megha:megha probeCustomAttribute.properties.old
uploadServerConfig.xml.old
```

Note: If any of these files is not available, an error message is displayed; ignore it.

9. Verify the ownership of all the above directories:

For example:

```
ls -lrt /usr/local/megha
```

10. Start the megha service and check if it is started:

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

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

11. Start the crond service using the command:

```
service crond start
```

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:

   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.

Settings required when using a virus detection program

If a virus detection program accesses database-related files used by Ops Center Analyzer, operations such as I/O delays or file locks can cause errors. To prevent these problems, exclude the following directories and files from the targets scanned by the virus detection program.

Analyzer server

Exclude the following directories:

- *Analyzer-server-installation-destination-directory*/Analytics
- *Analyzer-server-installation-destination-directory*/Base64
- *Analyzer-server-installation-destination-directory*/common
- *Analyzer-server-installation-destination-directory*/HNTRLib2
- /var/*Analyzer-server-installation-destination-directory*
- /var/opt/HPA
- /etc/.hitachi

Analyzer detail view server

Exclude the following directories:

- *Analyzer-detail-view-server-installation-destination-directory*
- /usr/local/httpProxy
- /tmp/hsperfdata_megha

Exclude the following files:

- `/var/spool/cron/root`
- `/var/spool/cron/megha`
- `/var/spool/cron/meghadata`
- `/var/mail/megha`
- `/var/mail/meghadata`
- Files that are in the `/tmp` directory and whose owners are the megha user

Analyzer probe server

Exclude the following directory:

- *`Analyzer-probe-server-installation-destination-directory`*`/megha`

Exclude the following files:

- `/etc/xinetd.d/dataReceiverDaemon`
- `/var/spool/cron/root`
- `/var/spool/cron/megha`
- `/etc/cron.d/cleanupRawData_*.cron`
- `/etc/cron.d/hnasFCPerfDataGenerator_*.cron`
- `/etc/cron.d/hnasPerfDataGenerator_*.cron`
- `/etc/cron.d/ibmxivPerfDataGenerator_*.cron`
- `/etc/cron.d/processConfRawData_*.cron`
- `/etc/cron.d/processRawData_1*.cron`
- `/etc/cron.d/vnxFileConfDataGenerator_*.cron`
- Files that are in the `/tmp` directory and whose owners are the megha user

Analyzer Windows probe

Exclude the following folders:

- *`Analyzer-Windows-probe-installation-destination-folder`*
- `C:\Temp\HDCA`

RAID Agent

Exclude the following directories:

- `/opt/jp1pc`
- `/home/RAIDAgent`

Exclude the following files:

- `/etc/rc.htnm_agent_rest_app`
- `/etc/rc.htnm_agent_rest_webservice`

- `/etc/init.d/htnm_agent_rest_app`
- `/etc/init.d/htnm_agent_rest_webservice`
- `/etc/rc.d/init.d/htnm_agent_rest_app`
- `/etc/rc.d/init.d/htnm_agent_rest_webservice`
- `/etc/rc.d/rc0.d/K01htnm_agent_rest_app`
- `/etc/rc.d/rc0.d/K01htnm_agent_rest_webservice`
- `/etc/rc.d/rc3.d/S99htnm_agent_rest_app`
- `/etc/rc.d/rc3.d/S99htnm_agent_rest_webservice`
- `/etc/rc.d/rc3.d/S[xx]htnm_agent_rest_app`
- `/etc/rc.d/rc3.d/S[xx]htnm_agent_rest_webservice`
- `/etc/rc.d/rc3.d/K[xx]htnm_agent_rest_app`
- `/etc/rc.d/rc3.d/K[xx]htnm_agent_rest_webservice`
- `/etc/rc.d/rc5.d/S99htnm_agent_rest_app`
- `/etc/rc.d/rc5.d/S99htnm_agent_rest_webservice`
- `/etc/rc.d/rc5.d/S[xx]htnm_agent_rest_app`
- `/etc/rc.d/rc5.d/S[xx]htnm_agent_rest_webservice`
- `/etc/rc.d/rc5.d/K[xx]htnm_agent_rest_app`
- `/etc/rc.d/rc5.d/K[xx]htnm_agent_rest_webservice`
- `/etc/rc.d/rc6.d/K01htnm_agent_rest_app`
- `/etc/rc.d/rc6.d/K01htnm_agent_rest_webservice`
- `/sbin/init.d/htnm_agent_rest_app`
- `/sbin/init.d/htnm_agent_rest_webservice`
- `/sbin/rc1.d/K090htnm_agent_rest_app`
- `/sbin/rc1.d/K090htnm_agent_rest_webservice`
- `/sbin/rc2.d/K910htnm_agent_rest_app`
- `/sbin/rc2.d/K910htnm_agent_rest_webservice`

Chapter 14: 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 Ops Center Analyzer components 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
- Virtual Storage Software Agent
- On-demand real time monitoring module

> **Note:** The backup and restore procedures described 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 of these components, or any of the components selectively. However, to prevent data inconsistency, be sure to back up and restore both Analyzer server and Analyzer detail view server at the same time.

Use cases

- 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.
- Re-installation of the OS or a component on the same host: Migrate settings and accumulated data to the new environment.
- Migration to a different host: You can use the backup and restore functions to migrate Analyzer components to a different host. Settings and accumulated data can also be inherited.

Ops Center Analyzer does not support periodic automatic backup. Create a backup schedule that fits your requirements.

You can back up and restore components in a virtual or physical environment by performing the same procedure.

Backing up Ops Center Analyzer

You can back up the entire Ops Center Analyzer system as described in the following workflow or select individual components back up.

The general backup workflow for Ops Center Analyzer components is as follows:

1. Stop each service in the following order:
   a. Analyzer server

      If the Analyzer server is linked to Ops Center Automator, make sure that no tasks are running for the Analyzer server, and then stop the Analyzer server services. Do not run any tasks for the Analyzer server before the backup processing finishes.

      Stopping the Analyzer server services (on page 438)

   b. Analyzer detail view server

      Stopping the Analyzer detail view server or Analyzer probe server services (on page 440)

   c. Analyzer Windows probe
   d. Analyzer probe server

      Stopping the Analyzer detail view server or Analyzer probe server services (on page 440)

   e. RAID Agent

      Stopping the RAID Agent services (on page 442)

   f. Virtual Storage Software Agent

      Stopping the Virtual Storage Software Agent services (on page 443)

   g. On-demand real time monitoring module

      Stopping the On-demand real time monitoring module services (on page 444)

2. Back up data for each of the following components:
   - Backing up the RAID Agent (on page 511)
   - Backing up Virtual Storage Software Agent (on page 512)
   - Backing up the On-demand real time monitoring module (on page 512)
   - Backing up the Analyzer probe server (on page 513)
   - Backing up the Analyzer detail view server (on page 514)
   - Backing up the Analyzer server (on page 515)

   Do not start any of these services before the backup processing finishes.

3. Start each service in the following order:

a. RAID Agent

   Starting the RAID Agent services (on page 440)

b. Virtual Storage Software Agent

   Starting the Virtual Storage Software Agent services (on page 443)

c. On-demand real time monitoring module

   Starting the On-demand real time monitoring module services (on page 444)

d. Analyzer probe server

   Starting the Analyzer detail view server or Analyzer probe server services (on page 439)

e. Analyzer Windows probe

   Starting the Analyzer Windows probe service (on page 240)

f. Analyzer detail view server

   Starting the Analyzer detail view server or Analyzer probe server services (on page 439)

g. Analyzer server

   Starting the Analyzer server services (on page 438)

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/jp1pc/htnm/bin/htmhsbackup -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/jp1pc/jpchosts`
- `/opt/jp1pc/*.ini`
- `/opt/jp1pc/bin/action/*.ini`
- `/opt/jp1pc/bin/statsvr/*.ini`

Backing up Virtual Storage Software Agent

You can back up the connection settings files of Virtual Storage Software Agent.

Before you begin

- Stop all services of Virtual Storage Software Agent.

Procedure

1. Back up the following files by manually copying them to a directory of your choice.
   - `/var/`*`Virtual-Storage-Software-Agent-installation-destination-directory`*`/VirtualStorageSoftwareAgent/system/access-points.yaml`
   - `/var/`*`Virtual-Storage-Software-Agent-installation-destination-directory`*`/VirtualStorageSoftwareAgent/config/userconfig-setting.yaml`
2. Start Virtual Storage Software Agent as needed.

Backing up the On-demand real time monitoring module

You can back up the configuration files and certificate files of the On-demand real time monitoring module.

Before you begin

- You must have the root permission.
- Stop the service of the On-demand real time monitoring module.

Procedure

1. Log on to the Analyzer probe server.
2. Create a directory for the backup.

   Example:

   ```
   mkdir ./backup
   ```

3. Copy the configuration files and certificate files to the backup directory.

   ```
   cp -p /opt/hitachi/Analytics/granular-data-collection-api/conf/user-granular-data-collection-api.conf ./backup
   ```

```
cp -p /opt/hitachi/Analytics/granular-data-collection-api/conf/system-granular-
data-collection-api.conf ./backup
cp -p /opt/hitachi/Analytics/granular-data-collection-api/cert/server.crt ./
backup
cp -p /opt/hitachi/Analytics/granular-data-collection-api/cert/server.key ./
backup
```

4. Compress the backup directory into a `tar.gz` file.

   Example:

```
tar -zcvf backup.tar.gz ./backup
```

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. The following settings information is not backed up by `backupAndRestore.sh`. Write down this information (or record it by other means) because, after the restore, the settings must be manually revised.
   - 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 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.
- Stop all services for the Analyzer probe server, the Analyzer Windows probe, and the Analyzer server that are connected to the Analyzer detail view server.
- If the Analyzer detail view server is connected to the Analyzer server, make sure that the version of the Analyzer server is the same as that of the Analyzer detail view server.
- 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. The following settings information is not backed up by `backupAndRestore.sh`. Write down this information (or record it by other means) because, after the restore, the settings must be manually revised.
   - 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)
5. If the Analyzer detail view server is connected to the Analyzer server, back up the Analyzer server, because you will need the backup data to perform restore.

Backing up the Analyzer server

You can back up the settings information of the Analyzer server.

Before you begin

- You must have root permission.
- Stop all Analyzer server and Analyzer detail view server services.
- Back up the Analyzer detail view server at the same time, because you will need the backup data to perform restore.
- Make sure that the version of the Analyzer server is the same as that of the Analyzer detail view server.

Procedure

1. Run the **`backupsystem`** command to back up the Analyzer server settings information.

Example:

```
Analyzer-server-installation-destination-directory/Analytics/bin/backupsystem -
dir output-directory -type all
```

To back up the data needed to perform a restore, specify `all` for the `type` option.

Do not specify the `auto` option, because this option starts the services of the Analyzer server.

Restoring Ops Center Analyzer

You can restore the entire Ops Center Analyzer system or individual components according to the following workflow.

The general restore workflow for Ops Center Analyzer components is as follows:

1. Stop the following services in this order:
   a. Analyzer server

      If the Analyzer server is linked to Ops Center Automator, make sure that no tasks are running for the Analyzer server, and then stop the Analyzer server services. Do not run any tasks for the Analyzer server before the restore processing finishes.

      Stopping the Analyzer server services (on page 438)

   b. Analyzer detail view server

      Stopping the Analyzer detail view server or Analyzer probe server services (on page 440)

   c. Analyzer Windows probe
   d. Analyzer probe server

      Stopping the Analyzer detail view server or Analyzer probe server services (on page 440)

   e. RAID Agent

      Stopping the RAID Agent services (on page 442)

   f. Virtual Storage Software Agent

      Stopping the Virtual Storage Software Agent services (on page 443)

   g. On-demand real time monitoring module

      Stopping the On-demand real time monitoring module services (on page 444)

2. Restore data for each of the following components:
   - Restoring the RAID Agent (on page 517)
   - Restoring Virtual Storage Software Agent (on page 518)
   - Restoring the On-demand real time monitoring module (on page 519)
   - Restoring the Analyzer probe server (on page 520)

- Restoring the Analyzer detail view server (on page 521)
- Restoring the Analyzer server (on page 523)

Do not start any of these services before the restore processing finishes.

3. Start the following services in this order:
   a. RAID Agent

      Starting the RAID Agent services (on page 440)

   b. Virtual Storage Software Agent

      Starting the Virtual Storage Software Agent services (on page 443)

   c. On-demand real time monitoring module

      Starting the On-demand real time monitoring module services (on page 444)

   d. Analyzer probe server

      Starting the Analyzer detail view server or Analyzer probe server services (on page 439)

   e. Analyzer Windows probe

      Starting the Analyzer Windows probe service (on page 240)

   f. Analyzer detail view server

      Starting the Analyzer detail view server or Analyzer probe server services (on page 439)

   g. Analyzer server

      Starting the Analyzer server services (on page 438)

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:
  - 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/jp1pc/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 **`jpcinssetup`** 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/jp1pc/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/jp1pc/htnm/Rest/config/htnm_httpsd.conf`
      - `/opt/jp1pc/htnm/HBasePSB/CC/server/usrconf/ejb/AgentRESTService/usrconf.properties`

Restoring Virtual Storage Software Agent

You can restore the connection settings files of Virtual Storage Software Agent.

Before you begin

- Stop all services of Virtual Storage Software Agent.
- The versions of Virtual Storage Software Agent on the backup source and on the restoration destination must be the same.

Procedure

1. Copy the backup files to the following directory on the restoration destination, overwriting the existing files.

File name	Restoration-destination directory
`access-points.yaml`	`/var/`*`Virtual-Storage-Software-Agent-installation-destination-directory/`*`VirtualStorageSoftwareAgent/system/`
`userconfig-setting.yaml`	`/var/`*`Virtual-Storage-Software-Agent-installation-destination-directory/`*`VirtualStorageSoftwareAgent/config/`

2. Start Virtual Storage Software Agent as needed.

Restoring the On-demand real time monitoring module

You can restore the configuration files and certificate files of the On-demand real time monitoring module.

Before you begin

- You must have the root permission.
- The versions of the On-demand real time monitoring modules on the backup source and on the restoration destination must be the same.

Procedure

1. Log on to the host where the Analyzer probe server is installed.
2. Copy the backup data to a directory of your choice on the restoration destination.
3. Stop the On-demand real time monitoring module service:

```
systemctl stop analyzer-granular-data-collection-api
```

4. Decompress the backup file (a `tar.gz` file), and then copy it to the directory on the restoration destination.

   Example:

```
tar -zxvf /root/backup.tar.gz ./backup
cp -p ./backup/user-granular-data-collection-api.conf /opt/hitachi/Analytics/
granular-data-collection-api/conf
cp -p ./backup/system-granular-data-collection-api.conf /opt/hitachi/Analytics/
granular-data-collection-api/conf
cp -p ./backup/server.crt /opt/hitachi/Analytics/granular-data-collection-api/
cert
cp -p ./backup/server.key /opt/hitachi/Analytics/granular-data-collection-api/
cert
```

5. Start the On-demand real time monitoring module service:

```
systemctl start analyzer-granular-data-collection-api
```

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 a restore, delete the Linux probe and then add it back to the Analyzer probe server.
6. If the Analyzer probe server on the backup source host was using Common Services, run the **`setupcommonservice`** command to update the connection settings.
7. If you are using key-based authentication to transfer data, make sure that you re-configure it. Refer to Configuring key-based authentication to transfer data directly from Analyzer probe server to Analyzer detail view server (on page 431) for more information. When re-configuring the key-based authentication, if you provide a new passphrase, make sure you update the passphrase in the Analyzer probe server UI for primary (and secondary, if applicable) Analyzer detail view server.
8. If you are using the Common Services, make sure that you re-register the Analyzer probe server with Common Services. Refer to Registering Analyzer probe server with Common Services (on page 98) for more information.

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.
- Stop all services for the Analyzer probe server, the Analyzer Windows probe, and the Analyzer server that are connected to the Analyzer detail view server on the restore destination host.
- If the Analyzer detail view server is connected to the Analyzer server, make sure that the version of the Analyzer server is the same as that of the Analyzer detail view server 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 the Analyzer detail view server is connected to the Analyzer server, restore the Analyzer server by using the backup data that was acquired at the same time as that of the Analyzer detail view server.
5. 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)
6. Verify the settings of the SMTP server, the Syslog server, and the SNMP Manager.

7. 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 connecting 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
8. If the Analyzer detail view server on the backup source host was using Common Services, run the **`setupcommonservice`** command to update the connection settings.
9. If you are using the key-based authentication to transfer data, make sure that you re-configure the key-based authentication. Refer to Configuring key-based authentication to transfer data directly from Analyzer probe server to Analyzer detail view server (on page 431) and Configuring key-based authentication for the Analyzer detail view server (on page 433) for more information. When re-configuring the key-based authentication, if you provide a new passphrase, make sure you update the passphrase in the Analyzer probe server UI for primary (and secondary, if applicable) Analyzer detail view server.
10. If you are using the Common Services, make sure that you re-register Analyzer detail view server with Common Services and re-assign the Analyzer detail view roles to Ops Center user groups. Refer to Registering Analyzer detail view server with Common Services (on page 95) for more information.

Restoring the Analyzer server

You can restore the settings information of the Analyzer server. This procedure varies depending on the destination environment. Be sure to perform the procedure appropriate for your configuration.

Restoring the Analyzer server to the same host:

Restoring the Analyzer server to the same host (on page 523)

Restoring the Analyzer server to a different host:

- Restoring the Analyzer server to a different host when Analyzer is not linked to Ops Center Automator (on page 525)
- Restoring the Analyzer server to a different host when Analyzer is linked to Ops Center Automator (on the same host) (on page 526)
- Restoring the Analyzer server to a different host when Analyzer is linked to Ops Center Automator (on another host) that is not linked to Device Manager (on page 528)
- Restoring the Analyzer server to a different host when Analyzer is linked to Ops Center Automator (on another host) that is linked to Device Manager (on page 530)

Restoring the Analyzer server to the same host

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 root permission.
- Stop all Analyzer server and Analyzer detail view server services on the restore destination host.
- Make sure that the version of the Analyzer server on the restore destination host is the same as that of the Analyzer detail view server.
- Make sure that the Analyzer detail view server has been restored by using the backup data that was acquired at the same time as the backup data of the Analyzer server.
- 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
  - IP address
  - System locale

Procedure

1. Run the **`restoresystem`** command to restore the settings information of Analyzer server.

   Example:

   ```
   Analyzer-server-installation-destination-directory/Analytics/bin/restoresystem -
   dir output-directory -type Analytics
   ```

   Do not specify the `auto` option, because this option starts the services of the 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.

   - 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`*`/uCPSB11/httpsd/conf`

3. If the maximum amount of memory that can be used by the Analyzer server was changed on the backup-source host, use the **`changememory`** command to set the maximum amount of memory again.
4. In the restore destination environment, if HTTPS connections are used between Analyzer server and the web client, enable HTTPS connections.
5. In the restore destination environment, if you changed the port number for communication between Analyzer server and the web client, reset the port number.
6. 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 server to a different host when Analyzer is not linked to Ops Center Automator

If, on the backup source host, Analyzer server does not link with Ops Center Automator, you can restore settings and accumulated data of the Analyzer server to a different host by using this procedure.

Before you begin

- You must have root permission.
- Stop all Analyzer server and common component services on the restore destination host.
- The versions of the Analyzer server on the backup source and restore destination hosts must be the same.

Procedure

1. Transfer the settings information of the Analyzer server and the common component (information that was collected by the backup source host) to the restore destination host.
2. On the restore destination host, perform the following procedure:
   a. Run the **`restoresystem`** command to restore the settings information of Analyzer server and the common component.

   ```
   Analyzer-server-installation-destination-directory/Analytics/bin/
   restoresystem -dir backup-data-output-directory -type all
   ```

   The user information registered in the common component on the restore destination is overwritten. If you want to retain the user information on the restore destination, specify `Analytics` for the `type` option so that the user information registered in the common component on the backup source is not restored.

   Do not specify the `auto` option, because this option starts the services of the Analyzer server.

b. Revise the following definition files on the restore destination host based on the content that was changed on the backup source host. If you already specified settings on the restore destination host, this step is unnecessary.

   - Security definition file

     `Common-component-installation-directory/conf/sec/security.conf`

   - Configuration file that sets the port number and the host name

     `Common-component-installation-directory/uCPSB11/httpsd/conf/user_httpsd.conf`

     Note: For details on how to edit the `user_httpsd.conf` file, see Enabling SSL communication for Analyzer server (on page 353).

c. Set up a connection with the Analyzer detail view server. For details, see Setting up a connection with Analyzer detail view server (on page 107).

d. If the Analyzer server on the backup source host was using Common Services, run the **`setupcommonservice`** command to update the connection settings for Common Services.

   Tip:

   After the restoration is complete, if you cannot log in to the Analyzer server, restart the server because the new authentication information might not have been applied.

Next steps

Be sure to uninstall the Analyzer server on the backup source host. Configurations where multiple instances of Analyzer reference the same Analyzer detail view server are not supported. For details, see Removing Ops Center Analyzer and Analyzer detail view servers (on page 532).

Restoring the Analyzer server to a different host when Analyzer is linked to Ops Center Automator (on the same host)

If, on the backup source host, Analyzer server links with Ops Center Automator on the same host, you can restore settings and accumulated data of the Analyzer server to a different host by using this procedure.

Before you begin

- You must have root permission.
- Stop all Analyzer server and common component services on the restore destination host.
- The versions of the Analyzer server on the backup source and restore destination hosts must be the same.

Procedure

1. Transfer the settings information of the Analyzer server and the common component (information that was collected by the backup source host) to the restore destination host.
2. On the restore destination host, perform the following procedure:
   a. Reconfigure the primary server settings and the secondary server settings for the Common component.

   ```
   Common-component-installation-directory/bin/hcmds64prmset -host host-name-or-IP-address-of-the-primary-server {-port port-number-of-the-primary-server-(non-SSL-communication) | -sslport port-number-of-the-primary-server-(SSL-communication)}
   ```

   b. Run the **`restoresystem`** command to restore the settings information of Analyzer server.

   ```
   Analyzer-server-installation-destination-directory/Analytics/bin/restoresystem -dir backup-data-output-directory -type Analytics
   ```

   Do not specify the `auto` option, because this option starts the services of the Analyzer server.

   c. Revise the following definition files on the restore destination host based on the content that was changed on the backup source host. If you already specified settings on the restore destination host, this step is unnecessary.
      - Security definition file

        `Common-component-installation-directory/conf/sec/security.conf`

      - Configuration file that sets the port number and the host name

        `Common-component-installation-directory/uCPSB11/httpsd/conf/user_httpsd.conf`

        Note: For details on how to edit the `user_httpsd.conf` file, see Enabling SSL communication for Analyzer server (on page 353).

   d. Set up a connection with the Analyzer detail view server. For details, see Setting up a connection with Analyzer detail view server (on page 107).
   e. If the Analyzer server on the backup source host was using Common Services, run the **`setupcommonservice`** command to update the connection settings for Common Services.

   > **Tip:**
   > After the restoration is complete, if you cannot log in to the Analyzer server, restart the server because the new authentication information might not have been applied.

3. Remove the Analyzer server on the backup source host.

a. Run the following command to back up the Analyzer server authentication data:

```
Common-component-installation-directory/bin/hcmds64authmove -export -
datapath backup-data-output-directory
```

b. Stop any security monitoring, antivirus, and process monitoring software.

c. Run the following command to remove the Analyzer server:

```
/opt/hitachi/Analytics/installer/analytics_uninstall.sh SYS
```

d. When prompted, select the components you want to remove, and then complete the removal process.

e. Run the following command to restore the Analyzer server authentication data:

```
Common-component-installation-directory/bin/hcmds64authmove -import -
datapath backup-data-output-directory
```

Restoring the Analyzer server to a different host when Analyzer is linked to Ops Center Automator (on another host) that is not linked to Device Manager

If, on the backup source host, Analyzer server links with Ops Center Automator on a different host that does not link with Device Manager, you can restore settings and accumulated data of the Analyzer server to a different host by using this procedure.

Note: If the Analyzer server is configured as secondary server, your next step is Restoring the Analyzer server to a different host when Analyzer is linked to Ops Center Automator (on another host) that is linked to Device Manager (on page 530).

Before you begin

- You must have root permission.
- Stop all Analyzer server and common component services on the restore destination host.
- The versions of the Analyzer server on the backup source and restore destination hosts must be the same.

Procedure

1. Migrate the user information to the Common component of Ops Center Automator.

   Note: If Ops Center Automator is running on Windows, perform the following steps but replace – with / immediately before each argument.

   a. Run the **hcmds64srv** command to stop all services.

```
Automator-installation-destination-directory/Base64/bin/hcmds64srv -stop
```

b. Run the **hcmds64prmset** command to set the Common component of Ops Center Automator as the primary server.

```
Automator-installation-destination-directory/Base64/bin/hcmds64prmset -
setprimary
```

c. Run the **hcmds64dbconvert** command to migrate the user information that was backed up.

```
Automator-installation-destination-directory/Base64/bin/hcmds64dbconvert -
auth -workpath working-folder-path -file import-file-path -auto
```

d. Run the **hcmds64srv** command to start the services.

```
Automator-installation-destination-directory/Base64/bin/hcmds64srv -start
```

2. Transfer the settings information of the Analyzer server and the common component (information that was collected by the backup source host) to the restore destination host.
3. On the restore destination host, perform the following procedure:

a. Reconfigure the primary server settings and the secondary server settings for the Common component.

```
Common-component-installation-directory/bin/hcmds64prmset -host host-name-
or-IP-address-of-the-primary-server {-port port-number-of-the-primary-
server-(non-SSL-communication) | -sslport port-number-of-the-primary-server-
(SSL-communication)}
```

b. Run the **restoresystem** command to restore the settings information of Analyzer server.

```
Analyzer-server-installation-destination-directory/Analytics/bin/
restoresystem -dir backup-data-output-directory -type Analytics
```

Do not specify the `auto` option, because this option starts the services of the Analyzer server.

c. Revise the following definition files on the restore destination host based on the content that was changed on the backup source host. If you already specified settings on the restore destination host, this step is unnecessary.

- Security definition file

  Common-component-installation-directory`/conf/sec/security.conf`

- Configuration file that sets the port number and the host name

  Common-component-installation-directory`/uCPSB11/httpsd/conf/user_httpsd.conf`

  Note: For details on how to edit the `user_httpsd.conf` file, see Enabling SSL communication for Analyzer server (on page 353).

d. Set up a connection with the Analyzer detail view server. For details, see Setting up a connection with Analyzer detail view server (on page 107).

e. If the Analyzer server on the backup source host was using Common Services, run the **`setupcommonservice`** command to update the connection settings for Common Services.

> **Tip:**
>
> After the restoration is complete, if you cannot log in to the Analyzer server, restart the server because the new authentication information might not have been applied.

Next steps

Be sure to uninstall the Analyzer server on the backup source host. Configurations where multiple instances of Analyzer reference the same Analyzer detail view server are not supported. For details, see Removing Ops Center Analyzer and Analyzer detail view servers (on page 532).

Restoring the Analyzer server to a different host when Analyzer is linked to Ops Center Automator (on another host) that is linked to Device Manager

If, on the backup source host, Analyzer server links with Ops Center Automator on a different host that links with Device Manager, you can restore settings and accumulated data of the Analyzer server to a different host by using this procedure.

Before you begin

- You must have root permission.
- Stop all Analyzer server and common component services on the restore destination host.
- The versions of the Analyzer server on the backup source and restore destination hosts must be the same.

Procedure

1. Transfer the settings information of the Analyzer server and the common component (information that was collected by the backup source host) to the restore destination host.
2. On the restore destination host, perform the following procedure:
   a. Reconfigure the primary server settings and the secondary server settings for the Common component.

```
Common-component-installation-directory/bin/hcmds64prmset -host host-name-
or-IP-address-of-the-primary-server {-port port-number-of-the-primary-
server-(non-SSL-communication) | -sslport port-number-of-the-primary-server-
(SSL-communication)}
```

b. Run the **`restoresystem`** command to restore the settings information of Analyzer server.

```
Analyzer-server-installation-destination-directory/Analytics/bin/
restoresystem -dir backup-data-output-directory -type Analytics
```

Do not specify the `auto` option, because this option starts the services of the Analyzer server.

c. Revise the following definition files on the restore destination host based on the content that was changed on the backup source host. If you already specified settings on the restore destination host, this step is unnecessary.

- Security definition file

  `Common-component-installation-directory/conf/sec/security.conf`

- Configuration file that sets the port number and the host name

  `Common-component-installation-directory/uCPSB11/httpsd/conf/user_httpsd.conf`

  Note: For details on how to edit the `user_httpsd.conf` file, see Enabling SSL communication for Analyzer server (on page 353).

d. Set up a connection with the Analyzer detail view server. For details, see Setting up a connection with Analyzer detail view server (on page 107).

e. If the Analyzer server on the backup source host was using Common Services, run the **`setupcommonservice`** command to update the connection settings for Common Services.

Tip:

After the restoration is complete, if you cannot log in to the Analyzer server, restart the server because the new authentication information might not have been applied.

Next steps

Be sure to uninstall the Analyzer server on the backup source host. Configurations where multiple instances of Analyzer reference the same Analyzer detail view server are not supported. For details, see Removing Ops Center Analyzer and Analyzer detail view servers (on page 532).

Chapter 15: 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

You can remove Analyzer server and Analyzer detail view server. You can choose to remove Analyzer server, Analyzer detail view server, or both.

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. When prompted, select the components you want to remove, and then complete the removal process.

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 16: 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 log message.

   If the following log entry 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.
5. If the web browser is set to refuse the use of cookies, change the settings to allow the use of cookies for Analyzer server.

6. Restart the web browser.

   If you cannot access the web client even after performing the preceding steps, delete the cookies related to the IP address and host name of Analyzer server, and then restart the web browser.

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 the 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 the 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`.

   Refer to Configuring an SSL certificate (Analyzer detail view server) (on page 358) for more information.

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.

Connection to RAID Agent fails when the on-demand real time monitoring function is used

When the On-demand real time monitoring function is used in the GUI of the Analyzer detail view server, the connection to RAID Agent might fail and the following message might be displayed.

```
Cannot connect to the RAID Agent server 'IP-address'.
```

Perform the following procedure to verify that communication is possible between Analyzer detail view server and the On-demand real time monitoring module:

Procedure

1. Verify that the On-demand real time monitoring module on the Analyzer probe server has started.

   For details, see Starting the On-demand real time monitoring module services (on page 444).

2. Change the firewall and network settings to enable access from the Analyzer detail view server to the On-demand real time monitoring module on the Analyzer probe server.

   The default port number of the On-demand real time monitoring module is 24262.

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 **hcmds64getlogs** 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 root permission.
2. Run the **hcmds64getlogs** command to collect the log file for the Analyzer server.

```
Common-component-installation-destination-directory/bin/hcmds64getlogs -dir
output-directory-path
```

   An archive file is output to the specified output destination.

   For details about the **hcmds64getlogs** 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.

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/jp1pc/tools/jpcras output-directory-path all all
   ```

   An archive file named `jpcrasYYMMDD.tar.gz` or `jpcrasYYMMDD.tar.Z` is output to the specified output destination.

Collecting the log files of Virtual Storage Software Agent

To collect the Virtual Storage Software Agent log files:

Procedure

1. Log on as root on the host where Virtual Storage Software Agent is installed.
2. To collect the log files, use the following command:

   ```
   rpm -qa > rpm_list.txt && tar -cvzf agent_diag.tar.gz directory-from-which-to-collect-log-file ./rpm_list.txt
   ```

For Example:

```
rpm -qa > rpm_list.txt && tar -cvzf agent_diag.tar.gz -C / opt/hitachi/
VirtualStorageSoftwareAgent var/opt/hitachi/VirtualStorageSoftwareAgent var/log/
hitachi/VirtualStorageSoftwareAgent ${PWD#/}/rpm_list.txt
```

Note: When specifying multiple directories from which to collect log files, separate each directory with a space.

Log files are collected from these locations:

- *Virtual-Storage-Software-Agent-installation-destination-directory*/VirtualStorageSoftwareAgent
- /var/*Virtual-Storage-Software-Agent-installation-destination-directory*/VirtualStorageSoftwareAgent
- /var/log/hitachi/VirtualStorageSoftwareAgent

An archive file named agent_diag.tar.gz is output to the directory from which you ran the command.

Collecting the log file for the On-demand real time monitoring module

Run the **diag** command to collect the log file for the On-demand real time monitoring module.

Procedure

1. As a user with root permission, log on to the host where Analyzer probe server is installed.
2. Run the **diag** command to collect the log file for the On-demand real time monitoring module.

```
/opt/hitachi/Analytics/granular-data-collection-api/bin/diag
```

An archive file named diag.*yyyymmdd-hhmmss*.tgz is output to the directory in which you ran the command.

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.

Note: The System Diagnostics data is not collected for the Analyzer probe server if the HTTPS protocol is used to upload data from the Analyzer probe server to the Analyzer detail view server.

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.

Before you begin

Note: If you do not want to stop the **crond** service, you can stop 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 440) and Starting the Analyzer detail view server or Analyzer probe server services (on page 439)

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. 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 following 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 following 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:

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`

Enabling debug logs in Analyzer detail view server and Analyzer probe server

By default, the Analyzer detail view server and the Analyzer probe server create `info` logs to track various activities. When you report a problem to customer support, they may request more details about specific log messages for investigating the problem. In this case, log level should be changed from `info` to `debug`.

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. Navigate to the `conf` directory.

```
cd /usr/local/megha/conf
```

3. Take a backup of the `log.xml` file.

```
cp log.xml bkp_log.xml_org
```

4. Open the `log.xml` file.

```
vi log.xml
```

5. Search for the log name and change the log level from `info` to `debug`.

   For example, if the transaction log needs to be updated, then check the `name="transaction"` tag. The entry will be similar to this,

   Edit the entry to change `level="info"` to `level="debug"`.

6. Save the file.
7. Log on to the Analyzer detail view server or Analyzer probe server UI (approximately after two hours), download the diagnostic data (**Manage** > **Download Diagnostic Data**) and send it to customer support for troubleshooting.

Next steps

When the problem is resolved, make sure that you change the log level from `debug` back to `info`.

Analyzer probe server is unable to connect to SMU

When you are unable to add Hitachi NAS probe, it is important to verify whether the Analyzer probe server can connect to the SMU. Use the solutions in this section to resolve the connection issue.

Username or password for SMU user is incorrect

Verify whether you have entered the correct username and password when adding the Hitachi NAS probe:

Procedure

1. Log on to the SMU UI:
   `https://`*`SMU-IP-Address`*`/mgr/app`
2. On the Login window, enter the same SMU credentials that you used when adding the Hitachi NAS probe.
3. If you cannot log in, contact the storage administrator.

User does not have SMU CLI access

Verify whether the SMU user has SMU CLI access. The following procedure applies to an external SMU. Similar procedure should be followed for internal SMU.

Procedure

1. Log on to the SMU UI:
   `https://SMU-IP-Address/mgr/app`
2. Enter the same SMU credentials that you used when adding the Hitachi NAS probe.
3. In the **SMU Administration** section, click the **SMU Users** link.
4. Check the **Allow CLI Access** column and verify whether or not the user has CLI access.

SMU IP is not accessible from the Analyzer probe server

Verify whether the Analyzer probe server can connect to the SMU.

Procedure

1. Log on to the Analyzer probe server through an SSH client (like **`putty`**) as a root user.
2. Run the following command to verify the connection:
   `ssh HNAS-SMU-user-name@HNAS-SMU-IP`
   If the Analyzer probe server is unable to connect the SMU, contact the network administrator.

High network latency between Analyzer probe server and SMU

Verify the network latency between the Analyzer probe server and SMU.

Procedure

1. Log on to the Analyzer probe server through an SSH client (like **`putty`**) as a root user.
2. Run the following command:
   ```
   /usr/local/megha/lib/hnas/hnasGetConnectionData.sh SMU SMU-IP-Address username
   password
   ```
   If there is no response from the Analyzer probe server within 30 seconds, then do the following to change the connection timeout value:
   a. Navigate to the hnas directory:
      ```
      cd /usr/local/megha/lib/hnas
      ```
   b. Open the `hnasGetConnectionData.sh` file.
   c. Change the `set timeout` property value to 60.
   d. Save the file.
3. Run the following command to re-check the connection:
   ```
   /usr/local/megha/lib/hnas/hnasGetConnectionData.sh SMU SMU-IP-Address username
   password
   ```

If you do not get response even after changing the timeout value to 60, contact the network administrator to investigate the high latency between the SMU and the Analyzer probe server.

Cannot collect performance information from Hitachi NAS platform even after adding the Hitachi NAS probe

If you want to monitor Hitachi NAS platform release 13.9.6628.07 or later but cannot collect performance information from Hitachi NAS platform even after adding the Hitachi NAS probe, revise the SSH session timeout value for the SMU.

Procedure

1. Check the SSH session timeout setting for the SMU.
2. Set the SSH session timeout value for the SMU to 3,600 seconds or longer.

   To configure the session timeout value, refer to the Hitachi NAS documentation.

Hitachi Enterprise Storage probe shows Processing delay status

In the Analyzer probe server **Status** window, sometimes Hitachi Enterprise Storage probe shows the Processing delay status. One reason could be that it is collecting data for a large number of resources from the target. To resolve this problem, you can increase the default data polling interval, export interval, and wait time threshold.

Note: By default, the performance data collection interval for the Hitachi Enterprise Storage probe is 300 seconds (5 minutes). Use the following procedure to update the interval that the Analyzer probe server collects data from the target and uploads it to the Analyzer detail view server. For example, if you increase the data collection and export intervals from 5 minutes to 15, the data is reflected in reports after 15 minutes.

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 all the services using the command:

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

4. Confirm the crond and megha services have been stopped using the commands:

```
service crond status
```

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

5. Create a backup of the Hitachi Enterprise Storage probe instance property file for which you have observed the Processing delay problem.

   For example:

```
cp /usr/local/megha/conf/probe/
HitachiEnterpriseStorage_80001_VSP5200_80001.properties /usr/local/megha/conf/
probe/backup_HitachiEnterpriseStorage_80001_VSP5200_80001_backup.properties
```

6. Open the Hitachi Enterprise Storage probe instance property file.

   For example:

```
vi /usr/local/megha/conf/probe/
HitachiEnterpriseStorage_80001_VSP5200_80001.properties
```

7. Add the following properties in the instance property file:

```
probe.perf.collection.interval.secs=performance_data_collection_interval
_in_seconds
probe.perf.export.interval.secs=performance_data_export_interval
_in_seconds
perf.threshold.time.limit.minutes=performance_data_threshold_in_minutes
```

   For example:

```
probe.perf.collection.interval.secs=900
   probe.perf.export.interval.secs=900
   perf.threshold.time.limit.minutes=30
```

   Note: Make sure that the value for `probe.perf.collection.interval.secs` and `probe.perf.export.interval.secs` is greater than default value (300 seconds).

8. Save the file and exit.

   Note: If you have observed the problem for multiple Hitachi Enterprise Storage probes, repeat step 5 to 8.

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
```

11. Confirm the crond and megha services have been started using the commands:

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

```
service crond status
```

Reducing performance spike events

For the Analyzer server, if the performance metric for a monitoring target exceeds a threshold which equal to or more than a presrcibed number of times during the threshold monitoring period, an event is issued.

A spike is a sudden rise or drop in performanice value. By default, the event is issued when the spike exceeds the threshold 1 time per 5-minute period. If these values result in an excessive number of events being issued, you can adjust the threshold monitoring period and the number of spikes to issue the event.

For static thresholds, Analyzer maintains separate counts for the number of times critical and warning thresholds are exceeded. When a value exceeds both the critical and warning thresholds, only the critical threshold is counted. For example, assume a performance metric data threshold is triggered twice in 10 minutes. If the value exceeds both the critical and warning thresholds the first time, but only exceeds the warning threshold the second time, the event is not issued. If you do not need to distinguish between the severity of spikes, we recommend setting the same value for critical and warning thresholds. Otherwise, we do not recommend suppressing these events.

Procedure

1. Open the user-specified properties file (`config_user.properties`).

   The file is stored in the following location:

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

2. Add the key corresponding to the Analyzer metric for which you want to suppress the issuance of events by performance spikes.

   For details about the Analyzer metrics that apply, see "Event issuance conditions" in User-specified properties file (config_user.properties) (on page 666).

   For example, to configure settings so that an event is issued when the Hitachi Storage Total IOPS (LDEV) metric exceeds the threshold twice in 10 minutes (the threshold monitoring period), add a key as follows:

```
dynamicThreshold.alertCondition.RAID_VOLUME_RAIDLDEV_TOTALIOPS.number = 2
dynamicThreshold.alertCondition.RAID_VOLUME_RAIDLDEV_TOTALIOPS.period = 10
```

Note: Set the threshold monitoring period as an integer multiple of the data collection interval.

3. Restart the Analyzer server services.

RAID Agent services startup on Red Hat Enterprise Linux/ Oracle Linux 8

When the OS is Red Hat Enterprise Linux/Oracle Linux version 8 or later, if you log in to the GUI of the OS, start the RAID Agent services, and install the Analyzer probe server, the RAID Agent services will stop when you log out of the OS.

To perform the following operations, use an SSH client to remotely connect to the Linux host:

- Run either of the following commands to start the RAID Agent services:
  - The **`htmsrv start`** command
  - The **`jpcstart`** command
- Install the Analyzer probe server.

If you accidentally start the RAID Agent services from the GUI of the OS and the services continue to run even after you log out from the OS, perform the following steps.

Procedure

1. Run the following command to stop the RAID Agent services:

```
/opt/jp1pc/htnm/bin/htmsrv stop -all
```

2. Start the RAID Agent services by using either of the following methods:
   - Use an SSH client to remotely connect to the Linux host, and then run the command for starting services.
   - Restart the OS to automatically start the services. Note that this method can be used only when both of the following conditions are met:
     - Settings are configured so that RAID Agent services start automatically.
     - The following instances are the same:
       - The instance of the RAID Agent that is started by the automatic startup script (jpc_start)
       - The instance of the RAID Agent that you want to start

A JDK-related error occurs during upgrade

When you upgrade a Data Center Analytics server or an Analytics probe server that was configured by using a virtual appliance with a version from 3.0.0-01 to 3.3.0-02, you may receive a JDK-related error message. If you receive an error message while running the

precheck tool or during the upgrade, complete the following procedure to change the JDK that is used by the Analyzer detail view server or the Analyzer probe server.

Resolving a JDK-related error for the Analyzer detail view server

Change the JDK used by the Analyzer detail view server to OpenJDK or Oracle JDK by performing the following procedure.

Procedure

1. Stop the Analyzer server services.
2. Log on as the root user to the Analyzer detail view server through an SSH client (like **`putty`**).
3. Use the following command to stop the crond service:

```
service crond stop
```

4. Stop all Analyzer detail view server services:

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

5. Upload the RPM package for OpenJDK or Oracle JDK to the `/tmp` directory.
6. Install the uploaded package:

```
rpm -ivh /tmp/package-name
```

7. Switch to the OpenJDK or Oracle JDK that you installed. Perform one or more of the required actions based on the description of invalid settings in the message.
   - If the error message displayed `java`:
     a. Display the list of java versions:

```
alternatives --config java
```

     b. When prompted, enter the version number of the OpenJDK or Oracle JDK that you installed:

     Example of output when the Java version is changed:

```
There are 2 programs which provide 'java'.

  Selection    Command
-----------------------------------------------
 + 1           /opt/hitachi/Base64/uCPSB/jdk/bin/java
*  2           java-1.8.0-openjdk.x86_64 (/usr/lib/jvm/java-1.8.0-
openjdk-devel-1.8.0.262.b08-1.el7_6.x86_64/bin/java)

Enter to keep the current selection[+], or type selection number: 2
```

     c. Run the command again, and confirm that a plus mark (+) appears next to the

java version that you want to use:

```
alternatives --config java
```

- If the error message displayed `jre_1.8.0`:
  a. Display the list of jre_1.8.0 versions:

  ```
  alternatives --config jre_1.8.0
  ```

  b. When prompted, enter the version number of the OpenJDK or Oracle JDK that you installed:

  ```
  Enter to keep the current selection[+], or type selection number:
  ```

  If the OpenJDK or Oracle JDK that you added does not appear, run the following command to delete the existing jre_1.8.0 settings.

  ```
  alternatives --remove jre_1.8.0 /opt/hitachi/Base64/uCPSB/jdk/jre
  ```

  c. Run the command again, and confirm that a plus mark (+) appears next to the jre_1.8.0 version that you want to use:

  ```
  alternatives --config jre_1.8.0
  ```

- If the error message displayed `jstack`:
  a. Display the list of jstack versions:

  ```
  alternatives --config jstack
  ```

  b. When prompted, enter the version number of the OpenJDK or Oracle JDK that you installed:

  ```
  Enter to keep the current selection[+], or type selection number:
  ```

  c. Run the command again, and confirm that a plus mark (+) appears next to the jstack version that you want to use:

  ```
  alternatives --config jstack
  ```

- If the error message displayed `keytool`:

  Run the following command to delete the keytool settings:

  ```
  alternatives --remove keytool /opt/hitachi/Base64/uCPSB/jdk/bin/keytool
  ```

- If the error message displayed `java_home`:

  Run the following command to delete the java_home settings:

  ```
  alternatives --remove java_home /opt/hitachi/Base64/uCPSB/jdk
  ```

8. Run the following command to apply the settings to the OS:

```
alternatives --auto java
```

9. Run the precheck tool (`analytics_precheck.sh`) and confirm that no error occurs for the Java environment:

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

Resolving a JDK-related error for the Analyzer probe server

Change the JDK used by the Analyzer probe server to OpenJDK or Oracle JDK by performing the following procedure.

Procedure

1. Log on as the root user to the Analyzer probe server through an SSH client (like **`putty`**).
2. Use the following command to stop the crond service:

```
service crond stop
```

3. Stop all Analyzer probe server services:

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

4. Upload the RPM package for OpenJDK or Oracle JDK to the `/tmp` directory.
5. Install the uploaded package:

```
rpm -ivh /tmp/package-name
```

6. Switch to the OpenJDK or Oracle JDK that you installed. Perform one or more of the required actions based on the description of invalid settings in the message.
   - If the error message displayed `java`:
     a. Display the list of java versions:

     ```
     alternatives --config java
     ```

     b. When prompted, enter the version number of the OpenJDK or Oracle JDK that you installed:

Example of output when the Java version is changed:

```
There are 2 programs which provide 'java'.

  Selection    Command
-----------------------------------------------
 + 1           /opt/jp1pc/htnm/HBasePSB/jdk/bin/java
*  2           java-1.8.0-openjdk.x86_64 (/usr/lib/jvm/java-1.8.0-
openjdk-devel-1.8.0.262.b08-1.el7_6.x86_64/bin/java)

Enter to keep the current selection[+], or type selection number: 2
```

c. Run the command again, and confirm that a plus mark (+) appears next to the java version that you want to use:

```
alternatives --config java
```

- If the error message displayed `jre_1.8.0`:

  a. Display the list of jre_1.8.0 versions:

  ```
  alternatives --config jre_1.8.0
  ```

  b. When prompted, enter the version number of the OpenJDK or Oracle JDK that you installed:

  ```
  Enter to keep the current selection[+], or type selection number:
  ```

  If the OpenJDK or Oracle JDK that you added does not appear, run the following command to delete the existing jre_1.8.0 settings.

  ```
  alternatives --remove jre_1.8.0 /opt/jp1pc/htnm/HBasePSB/jdk/jre
  ```

  c. Run the command again, and confirm that a plus mark (+) appears next to the jre_1.8.0 version that you want to use:

  ```
  alternatives --config jre_1.8.0
  ```

- If the error message displayed `jstack`:

  a. Display the list of jstack versions:

  ```
  alternatives --config jstack
  ```

  b. When prompted, enter the version number of the OpenJDK or Oracle JDK that you installed:

  ```
  Enter to keep the current selection[+], or type selection number:
  ```

  c. Run the command again, and confirm that a plus mark (+) appears next to the jstack version that you want to use:

  ```
  alternatives --config jstack
  ```

- If the error message displayed `keytool`:

  Run the following command to delete the keytool settings:

  ```
  alternatives --remove keytool /opt/jp1pc/htnm/HBasePSB/jdk/bin/keytool
  ```

- If the error message displayed `java_home`:

  Run the following command to delete the java_home settings:

  ```
  alternatives --remove java_home /opt/jp1pc/htnm/HBasePSB/jdk
  ```

7. Run the following command to apply the settings to the OS:

```
alternatives --auto java
```

8. Run the precheck tool (`dcaprobe_precheck.sh`) and confirm that no error occurs for the Java environment:

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

Chapter 17: Installing Ops Center Analyzer viewpoint

Install Ops Center Analyzer viewpoint 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.

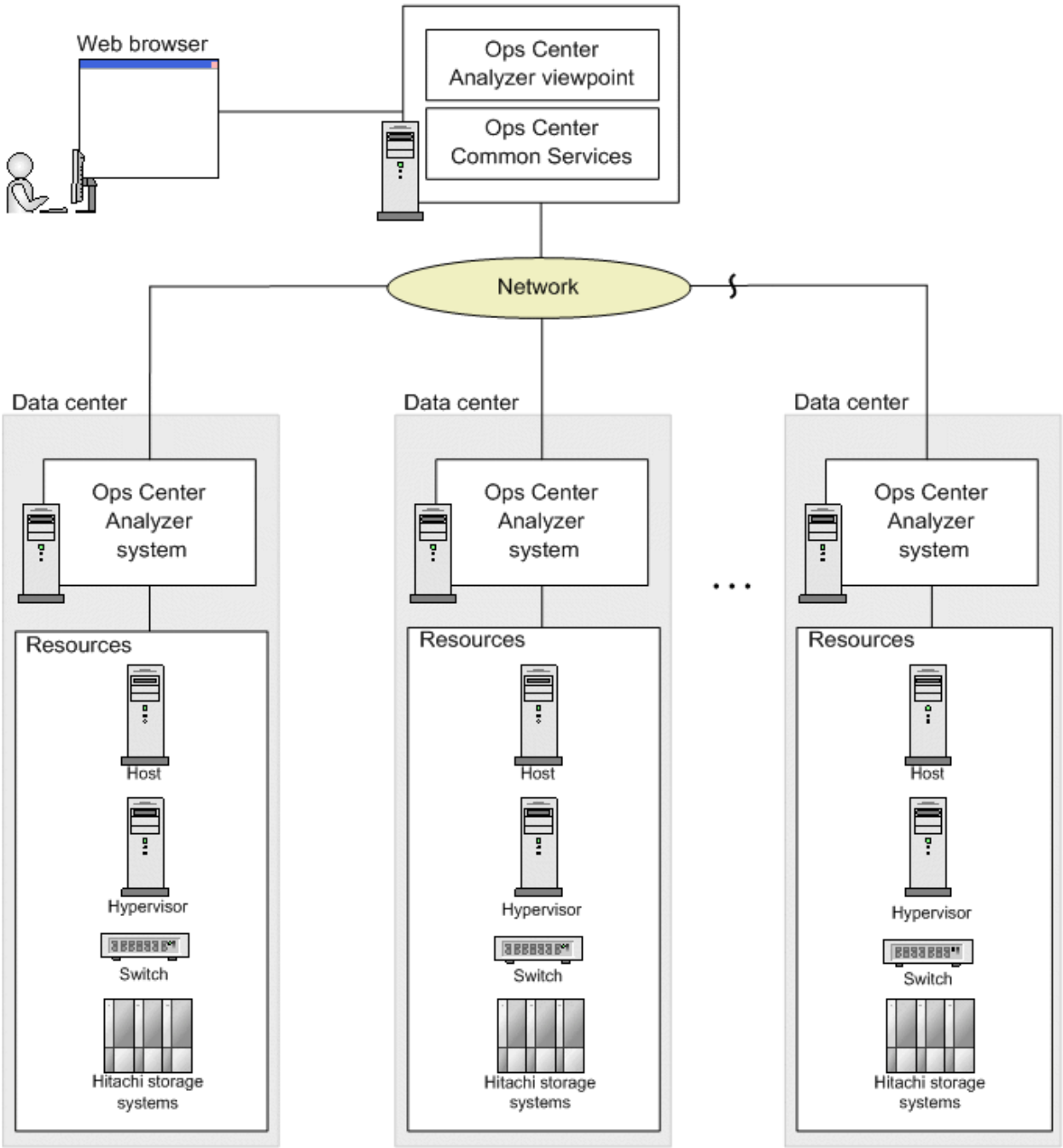
- Easily analyze problems related to resources.

  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, you can launch the Ops Center Analyzer UI from Analyzer viewpoint, and quickly perform the tasks needed to resolve the problem.

Analyzer viewpoint system configuration

The following shows an example of an Analyzer viewpoint system configuration. You can also configure Common Services and Analyzer viewpoint on different hosts. Analyzer viewpoint periodically collects information about each resource from Ops Center Analyzer servers running at multiple data centers. The RAID Agent of the Ops Center Analyzer system collects the data from storage systems. The Analyzer detail view collects the data from hypervisors, hosts, and switches.



Prerequisites

To use Analyzer viewpoint, confirm the following prerequisites:

- Ops Center Analyzer version is 10.6.1 or later.

If you want to monitor hypervisors, hosts, and switches, use Ops Center Analyzer version 10.8.0-01 or later.

System requirements

The following provides the Analyzer viewpoint system requirements.

System requirements for using the Analyzer viewpoint OVF

Guest operating system settings

- Oracle Linux 8.4 (Architecture x86_64)

Virtualization software

Product name		Version
VMware	vCenter Server	6.5u1, 6.7, 7.0, or 7.0u2
	ESXi	Use the same version as the vCenter Server.

OS changes based on security best practices (Analyzer viewpoint OVF)

The following OS setting changes are applied to the OVF to strengthen security. You can revert to the original settings if necessary. These OS settings can also be applied for the Ops Center products installed by using the installer.

Note that Hitachi Vantara does not take responsibility for, or support any interactions between, third-party programs and these OS settings.

/etc/modprobe.d/CIS.conf

Additional settings:

- install cramfs /bin/true
- install freevxfs /bin/true
- install jffs2 /bin/true
- install hfs /bin/true
- install hfsplus /bin/true
- install squashfs /bin/true
- install udf /bin/true
- install dccp /bin/true
- install sctp /bin/true
- install rds /bin/true
- install tipc /bin/true

/etc/sysctl.conf

Additional settings:

- net.ipv4.conf.default.accept_redirects = 0
- net.ipv4.conf.all.accept_redirects = 0
- net.ipv4.conf.default.send_redirects = 0
- net.ipv4.conf.all.send_redirects = 0
- net.ipv4.conf.all.secure_redirects = 0
- net.ipv4.conf.default.secure_redirects = 0
- net.ipv6.conf.all.accept_redirects = 0
- net.ipv6.conf.default.accept_redirects = 0
- net.ipv4.icmp_echo_ignore_broadcasts = 1
- net.ipv4.icmp_ignore_bogus_error_responses = 1
- net.ipv4.conf.all.rp_filter = 1
- net.ipv4.conf.default.rp_filter = 1
- net.ipv4.tcp_syncookies = 1
- net.ipv6.conf.all.accept_ra = 0
- net.ipv6.conf.default.accept_ra = 0
- kernel.randomize_va_space = 2
- net.ipv4.conf.all.log_martians = 1
- net.ipv4.conf.default.log_martians = 1
- fs.suid_dumpable = 0
- net.ipv4.conf.all.accept_source_route = 0
- net.ipv4.conf.default.accept_source_route = 0
- net.ipv4.ip_forward = 0

/etc/motd, /etc/issue, /etc/issue.net

Additional settings:

Authorized uses only. All activity may be monitored and reported.

Note: The default lines that identify the system name and kernel version for the login prompt in /etc/issue and /etc/issue.net have been removed.

System requirements for using the Analyzer viewpoint installer

The requirements for operating systems, network configuration, and RPM packages are as follows:

Supported operating systems

- Red Hat Enterprise Linux 7.5-7.9, 8.1, 8.2, 8.4 (x64)
- Oracle Linux 7.5-7.9, 8.2, 8.4 (Unbreakable Enterprise Kernel) (x64)
- Oracle Linux 7.5-7.9, 8.1, 8.2, 8.4 (Red Hat Compatible Kernel) (x64)

Network

Analyzer viewpoint only supports IPv4 communication. If an IPv6 environment is included as a communication destination for Analyzer viewpoint, configure the system so that Analyzer viewpoint establishes all communication in IPv4.

Prerequisite RPM packages

Install the following RPM packages before you install Analyzer viewpoint. You can run the precheck tool provided by Analyzer viewpoint (`viewpoint_precheck.sh`) to identify missing RPM packages.

- at 3.1.13 or later
- bash-completion 2.1 or later
- expect 5.45 or later
- fontconfig 2.10.95 or later
- freetype 2.4.11 or later
- gdb 7.6.1 or later
- libicu 50.1.2 or later
- lsof 4.87 or later
- ltrace 0.7.91 or later
- perl 5.16.3 or later
- perl-Time-HiRes 1.9725 or later
- policycoreutils
- sos 3.5 or later
- strace 4.12 or later
- sysstat 10.1.5 or later
- systemtap-runtime 3.2 or later
- tcpdump 4.9.2 or later
- trace-cmd 2.6.0 or later
- unzip 6 or later
- wget 1.14 or later
- zip 3 or later
- zlib-devel 1.2.7 or later

For Red Hat Enterprise Linux and Oracle Linux 7 or earlier, the following packages are also required:

- net-tools 2 or later
- systemd-sysv 219 or later

For Red Hat Enterprise Linux and Oracle Linux 8 or later, the following packages are also required:

- jq
- oniguruma
- policycoreutils-python-utils
- sqlite
- tar

Note: If you want to use Red Hat Enterprise Linux or Oracle Linux 8 or later, we strongly recommend that after you install the prerequisite packages, you upgrade the following packages to the following versions:

- libsemanage 2.9-3 or later
- python3-libsemanage 2.9-3 or later

Hardware requirements

Hardware requirements for Analyzer viewpoint for monitoring storage systems only

System scale (number of LDEVs)	Processor (cores)	Memory	Disk space*	Disk type
40,000 or less	8	64 GB	1 TB	SSD (1,000 IOPS)
greater than 40,000 and less than 270,000	12	128 GB	4 TB	SSD (10,000 IOPS, 1GB/sec)
greater than 270,000 and less than 640,000	16	256 GB	8 TB	SSD (10,000 IOPS, 1GB/sec)
* Analyzer viewpoint retains historical data for 378 days.				

Hardware requirements for Analyzer viewpoint for monitoring storage systems, hypervisors, hosts, and switches

For details on the number of manageable resources, see Hardware sizing based on system scale (on page 561).

System scale	Processor (cores)	Memory	Disk space*	Disk type
Extra Small	8	24 GB	1 TB	SSD (1,000 IOPS)
Small	8	48 GB	1 TB	SSD (1,000 IOPS)
Medium	12	64 GB	4 TB	SSD (10,000 IOPS, 1GB/sec)
Large	12	96 GB	4 TB	SSD (10,000 IOPS, 1GB/sec)
Extra Large	16	192 GB	4 TB	SSD (10,000 IOPS, 1GB/sec)
* Analyzer viewpoint retains historical data for 378 days.				

Hardware sizing based on system scale

The following table contains guidelines for determining the size of your environment based on the number of monitoring targets. Based on the sizing and scalability guidelines, you can identify the hardware requirements and scale your environment to meet workload demands.

System scale	Maximum number of resources					
	Hypervisor		Storage		FC Switch	FC Switch port
	VM	ESX	Volume	Storage		
Extra Small	100	6	1,500	3	2	128
Small	300	20	25,000	10	4	256
Medium	1,500	100	80,000	20	10	640
Large	4,500	300	120,000	30	28	1,792
Extra Large	7,500	500	200,000	50	40	2,560

Port requirements

The port requirements are as follows.

Source IP address	Target IP address	Default port	Protocol
User Desktop	Analyzer viewpoint	OVF: 443 installer: 25442*	HTTPS
Analyzer viewpoint	Analyzer server	22016	HTTPS
Ops Center Common Services	Analyzer viewpoint	443	HTTPS
localhost	localhost	25080, 25081, 25082, 25083, 25085, 25432, 25443, 8086, 8088 (internal; it is strongly recommended that you do not open these ports for external communication.)	HTTPS
* If you are using the installer, you can choose this port during installation.			

Supported browsers

The following browsers are supported:

Web browser	Version
Firefox	ESR 91
Microsoft Edge	Latest version of stable channel
Chrome Browser for enterprise	Latest version of the stable channel

Monitoring target storage systems

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 E series
- VSP F series
- VSP G series
- VSP 5000 series

Storage system data is collected by using one of the following methods:

- Command device and SVP (`Access Type`: 1)
- Command device and REST API (`Access Type`: 2)

For details on these data collection methods, see Selecting the data collection method (on page 154).

For VSP E590, E790, E1090, E590H, E790H, and E1090H storage systems, use `Access Type` 2.

To analyze Universal Replicator performance, use `Access Type` 1 for both the primary and secondary storage systems.

Analyzer viewpoint supports the analysis of Universal Replicator performance for individual consistency groups. However, configurations where one consistency group includes multiple journal groups are not supported.

To view the performance information of NVM Host in Analyzer viewpoint, use Ops Center Analyzer 10.8.1 or later.

If you use Tuning Manager - Agent for RAID to collect information, you must change the settings so that the system uses the RAID Agent included with Ops Center Analyzer. For details, see Determining the appropriate agent for collecting data (on page 151).

Monitoring target hypervisors, host, and switches

Analyzer viewpoint supports the same hypervisors, hosts, and switches that are monitored by the Ops Center Analyzer system.

For details, see the system requirements of Ops Center Analyzer.

Monitoring target hypervisors (on page 58)

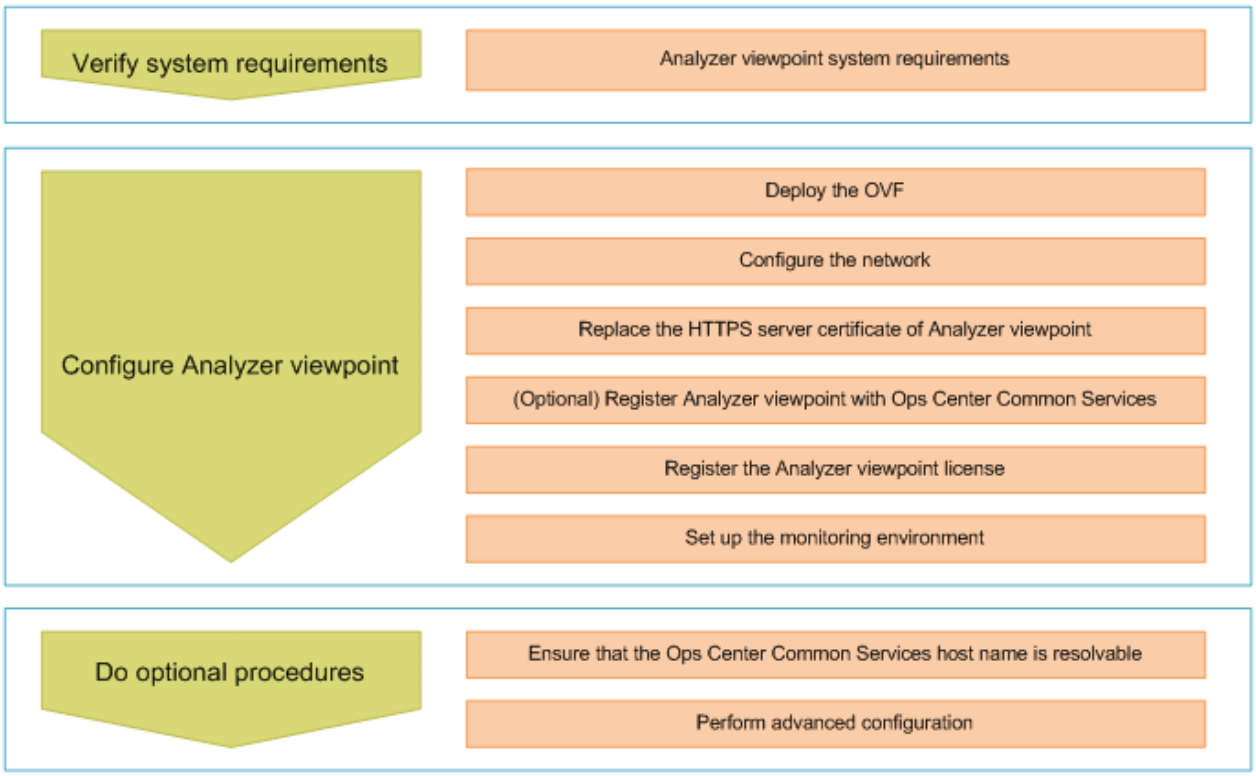
Monitoring target hosts (on page 59)

Monitoring target FC switches (on page 60)

Installing Analyzer viewpoint using a virtual appliance

Workflow for installing Analyzer viewpoint by using a virtual appliance

The following figure shows the workflow for setting up Analyzer viewpoint when using the OVF file (Analyzer viewpoint OVF).



Deploying the OVF

By deploying the OVF, you create a virtual machine on which the viewpoint server is installed.

Before you begin

Verify the System requirements (on page 557).

Also, before you install Analyzer viewpoint, be aware of the following:

- The virtual machine you create in the following procedure is to be used as the host for Analyzer viewpoint excluding Common Services. Do not use this virtual machine for any other purpose.
- After installation, do not change the system time to an earlier time, because this may cause Analyzer viewpoint to malfunction.
- The time on the Analyzer viewpoint host must be synchronized with the time on other hosts running Ops Center products. 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 Manually configuring the network of the virtual machine (on page 566).

Note: When Analyzer viewpoint is installed, the following RPM packages are installed:

- Amazon Corretto 11
- Kong
- PostgreSQL 11

If another product that uses these RPM packages is installed on the same host as Analyzer viewpoint, check the versions of the RPM packages supported by that product and make sure that the upgrade will not cause any problems. If the upgrade might cause a problem, install Analyzer viewpoint on a different host than that product.

Procedure

1. From a VMware vSphere client, log in to the VMware ESXi server.
2. Deploy the Analyzer viewpoint OVF by selecting **File** > **Deploy OVF Template** and selecting the Analyzer viewpoint files.
   - For vCenter v6.7 or v7.0:

     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:

     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, right-click the newly deployed virtual machine and select **Edit Settings**.

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.

Tip:

- By default, the format of virtual disks is set to thick provisioning. However, you can also select thin provisioning.
- Analyzer viewpoint is installed in the following directory on the virtual machine.

  `/opt/hitachi/analyzer_viewpoint`

Using VM customization specification to configure the network

We recommend that you configure the network with VM customization specification of the virtual machine. However, if you prefer not to use this specification, you can skip this procedure and configure the network manually as described in Manually configuring the network of the virtual machine (on page 566).

Procedure

1. From a VMware vSphere client, log in to the VMware ESXi server.
2. Create a VM customization specification.
   a. Select **Menu** > **Policies and Profiles**. In the **VM Customization Specifications** window, click **New**.
   b. Follow the instructions in the **New VM Guest Customization Spec** window.

      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 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**.

Manually configuring the network of the virtual machine

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 using the network manager as follows:
   a. Run the following command to make sure that the device named `ens192` is available.

   ```
   nmcli device
   ```

   b. Set an IP address, gateway, DNS server, and host name. 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. Activate the connection profile.

   ```
   nmcli connection up ens192
   ```

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 local 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 synchronize, set up the NTP service.
   a. Modify the configuration file.

   ```
   vi /var/opt/hitachi/analyzer_viewpoint/system/chrony.conf
   ```

b. Specify the NTP server or the NTP Pool that you want to use. For example:

```
#pool 2.pool.ntp.org iburst
server NewNTPServer iburst
```

c. Restart the NTP service.

```
systemctl restart chronyd
```

d. Confirm the settings.

```
chronyc sources
```

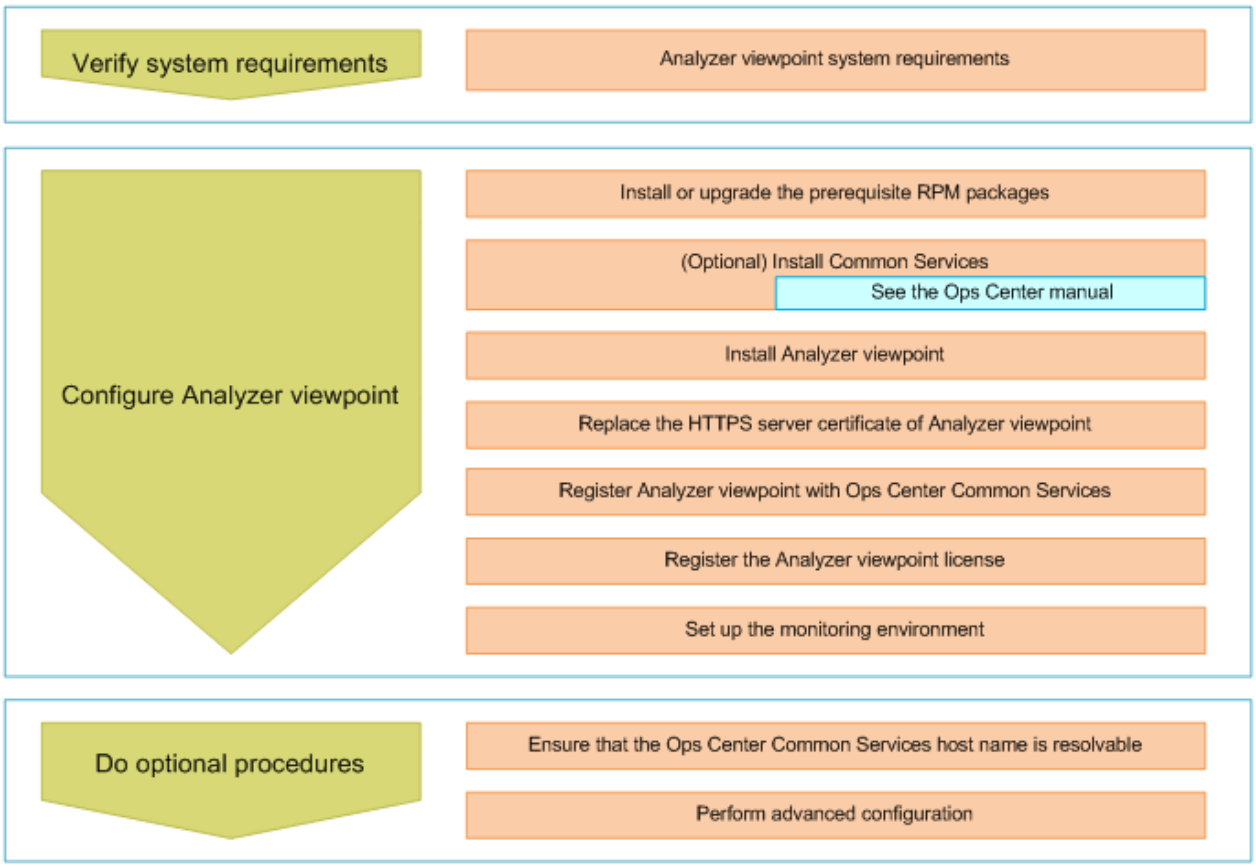
6. Restart the virtual machine.

```
reboot
```

Installing Analyzer viewpoint by using the installer

Workflow for installing Analyzer viewpoint by using the installer

The following figure shows the workflow for setting up Analyzer viewpoint when using the installer. As part of the initial setup, you must register Analyzer viewpoint with Common Services.



Installing or updating the prerequisite RPM packages

You can obtain the prerequisite RPM packages from the Linux OS media or the distribution website, such as for Red Hat Enterprise Linux.

You can check which RPM packages are missing by running the precheck tool (`viewpoint_precheck.sh`).

Installing or updating the RPM packages by using the Linux OS media

The following describes how to install or update the RPM packages by using the Linux OS media.

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

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

2. Configure the yum repository.
   - For Red Hat Enterprise Linux and Oracle Linux 7 or earlier:

```
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
```

   - For Red Hat Enterprise Linux and Oracle Linux 8 or later:

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

   - **For the package group:**

```
yum group install package-group-to-install
```

4. Unmount the Linux OS media:

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

Installing or updating the RPM packages using the distribution website

The following describes how to install or update the RPM packages by using the distribution website.

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-install
   ```

   - **For the package group:**

   ```
   yum group install package-group-to-install
   ```

Installing Analyzer viewpoint (installer)

To install Analyzer viewpoint, complete the following procedure.

Before you begin

- Review the Analyzer viewpoint requirements (hardware and software).
- Verify that you can resolve the IP address from the host name where you plan to install Analyzer viewpoint.

  Check the `hosts` file or the domain name system (DNS) server configuration of the host where you plan to install Analyzer viewpoint.
- Make sure that the ports you specify are available for communication. (The default port is 25442.)
- Verify that you have root permission to run the installer and the precheck tool.
- After installation, do not change the system time to an earlier time, because this may cause Analyzer viewpoint to malfunction. If time is synchronized by using an NTP server, use slew mode.
- The time on the Analyzer viewpoint host must be synchronized with the hosts running Ops Center products. We recommend configuring an NTP server.

- To install Analyzer viewpoint on the same host as Common Services, use Common Services version 10.5.1 or a later.
- If `firewalld` is enabled, during installation, settings will be changed for the default zone. If necessary, revise the settings after installation finishes.

Note: When Analyzer viewpoint is installed, the following RPM packages are installed:

- Amazon Corretto 11
- Kong
- PostgreSQL 11

If another product that uses these RPM packages is installed on the same host as Analyzer viewpoint, check the versions of the RPM packages that are supported by that product and make sure that the upgrade will not cause any problems. If the upgrade might cause a problem, install Analyzer viewpoint on a different host than that product.

Procedure

1. Stop any security monitoring software, antivirus software, and process monitoring software.
2. Mount the Analyzer viewpoint installation media.
3. Move to the root directory of the installer.

   ```
   cd mounted-directory/VIEWPOINT
   ```

4. Run the precheck tool as the root user to check whether Analyzer viewpoint can be installed.

   ```
   bash viewpoint_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.

   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 the root user to start the installation:

   ```
   bash viewpoint_install.sh NEW
   ```

   Do not forcibly stop the host during or immediately after the installation of Analyzer viewpoint. To stop or restart the host, wait until the installation is complete, and then perform the correct procedure (for example, by running an OS command).

6. Enter the required values according to the prompts, and complete the installation.

Note: When you specify the port, if the default port number (25442) is in use, specify a different port number. For details, see Port requirements (on page 561).

Tip: Analyzer viewpoint is installed in the following directory.

`/opt/hitachi/analyzer_viewpoint`

Changing a Linux host environment by using the installer

If you run the Analyzer viewpoint installer, the internal processing of the installer changes the environment of the host on which Analyzer viewpoint is installed as follows.

Change	Details
Addition of users	The following users are added: ▪ analyzer ▪ influxdb ▪ kong ▪ postgres ▪ rattlesnake
Addition of groups	The following groups are added: ▪ analyzer ▪ influxdb ▪ kong ▪ postgres ▪ rattlesnake
Addition of SELinux policy records	For Red Hat Enterprise Linux/Oracle Linux 8, policy records for files in the following directory are added: `/var/opt/hitachi/analyzer_viewpoint`
Changes to the cron settings	The periodic data collection processing settings of Analyzer viewpoint are added.

Replacing the HTTPS server certificate of Analyzer viewpoint

Analyzer viewpoint uses a self-signed certificate by default. Change the setting to use a certificate issued by a certificate authority before using Analyzer viewpoint.

> **Note:** If an instance of Analyzer viewpoint is on the same host as Ops Center Common Services, you can use the **`cssslsetup`** command to create a common certificate and key file for all Ops Center products. For details, see the *Hitachi Ops Center Installation and Configuration Guide*.

Before you begin

- You must have root privilege.
- Acquire a certificate and a key file issued by a certificate authority.

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 server.
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.

   Set permissions so that the certificate and key files can be read by the OS user root. A good practice is to grant only the necessary permissions for the 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
   ```

Enabling certificate verification for Analyzer viewpoint

You can enable certificate verification during secure communication for Analyzer viewpoint.

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 enable certificate verification:

```
/opt/hitachi/analyzer_viewpoint/bin/config-cert --enable
```

   For details on the command, see config-cert command (on page 599).

3. Run the following command to import a certificate to the truststore. To import multiple certificates, run the command separately for each certificate.

```
/opt/hitachi/analyzer_viewpoint/bin/config-cert --register certificate-file-name
registration-name-of-the-certificate
```

   You must import the following certificates or the root certificate:

   - Analyzer server
   - Analyzer viewpoint
   - Common Services

   If you are using the instance of Common Services bundled with Analyzer viewpoint that was installed by using the OVF, you do not need to import the Common Services certificate.

   Note: If you are using a certificate that contains a host name in a SAN (Subject Alternative Name), use the **setupcommonservice** command to specify settings so that the link with Common Services uses the host name. Also, use the **setservicehostname** command to specify settings so that Analyzer viewpoint is accessed by the host name.

4. Start the Analyzer viewpoint services:

```
systemctl start analyzer-viewpoint.target
```

Deleting a certificate registered in the Analyzer viewpoint truststore

You can delete a certificate that is used for verification from the Analyzer viewpoint truststore.

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 delete a certificate from the truststore. To delete multiple certificates, run the command separately for each certificate.

```
/opt/hitachi/analyzer_viewpoint/bin/config-cert --delete registration-name-of-
the-certificate
```

For details on the command, see config-cert command (on page 599).

3. Start the Analyzer viewpoint services:

```
systemctl start analyzer-viewpoint.target
```

Registering Analyzer viewpoint with Ops Center Common Services

If you installed Analyzer viewpoint by using the virtual appliance, it is automatically registered with the instance of Ops Center Common Services. Therefore, you only need to complete this procedure if you want to register Analyzer viewpoint with a different instance of Common Services (for example, if you want to register with an existing instance of Common Services running on another server).

If you installed Analyzer viewpoint by using the installer, you must follow this procedure.

Before you begin

You must have root privilege.

Procedure

1. Stop the Analyzer viewpoint services:

```
systemctl stop analyzer-viewpoint.target
```

2. To Register Analyzer viewpoint in Ops Center Common Services, run the following command:

```
/opt/hitachi/analyzer_viewpoint/bin/setupcommonservice --csUri Common-Services-
url
```

Example:

```
/opt/hitachi/analyzer_viewpoint/bin/setupcommonservice --csUri https://
myopscenter.com/
```

3. Enter the username and password of the Common Services user when prompted.

Note: The Common Services user specified for this command must belong to the **opscenter-administrators** user group.

4. Restart the services.

```
systemctl start analyzer-viewpoint.target
```

Note: To remove a Hitachi Ops Center product registered in Common Services, use the Hitachi Ops Center Portal.

Registering the Analyzer viewpoint license

You register an Analyzer viewpoint license by using the Ops Center Portal. You must complete this procedure for a new installation 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 **Inventory** tab to open the **Products** window, find the Analyzer viewpoint instance that you want to use, and then click the product status link. Usually, **Ready** appears as the product 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 and 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 **Inventory** tab to open the **Products** window, find the Analyzer viewpoint instance that you want to use, and then click the product status link. Usually, **Ready** appears as the product 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

If Analyzer viewpoint was installed by using the OVF, you can log in 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 access Analyzer viewpoint by using the following address:

```
https://IP-address-of-the-Analyzer-viewpoint-server:port-number/
```

Note: The default port number for an instance of Analyzer viewpoint that was installed by using the installer is 25442.

Setting up the monitoring environment

Before you begin

Ensure that Analyzer viewpoint and Ops Center Analyzer are registered with the same Ops Center Common Services instance. For details, see Registering Ops Center Analyzer in Ops Center Common Services (on page 105).

Procedure

1. Access the Ops Center Portal.
2. Add the data center and associate the related data with Ops Center Analyzer. For details, see the *Ops Center Portal Help*.

Tip:

- To view a list of monitored data centers and Ops Center Analyzer systems, run the following command on the Analyzer viewpoint server:

```
/opt/hitachi/analyzer_viewpoint/etl/list_inventory.sh
```

- After registering the data center and the Ops Center Analyzer system, you can start data collection manually with the **`run.sh`** command. For details, see Manually collecting data for a specific period (on page 587).

Ensuring that the Ops Center Common Services host name is resolvable

In the following cases, ensure that you specify the required settings so that the host names of individual Ops Center products are resolvable 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

Changing the maximum amount of memory used by the data collection process

If you are monitoring a large number of resources or the data collection interval is long, you should consider 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 host on which Analyzer viewpoint is installed. For more information, see Hardware requirements (on page 560).

Before you begin

You must have root permissions.

Procedure

1. Log on to the Analyzer viewpoint server.
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 by setting the following parameters.

   The amount of memory used for data collection from storage systems:

   `VIEWPOINT_ETL_SCHEDULE_MAX_HEAP_IN_GB`

   The maximum amount of memory to be used for regular data collection.

   `VIEWPOINT_ETL_ONDEMAND_MAX_HEAP_IN_GB`

   The maximum amount of memory to be used for manual data collection.

   The amount of memory used for data collection from hypervisors, hosts, and switches:

   `VIEWPOINT_ETL_DETAILVIEW_SCHEDULE_MAX_HEAP_IN_GB`

   The maximum amount of memory to be used for regular data collection.

   `VIEWPOINT_ETL_DETAILVIEW_ONDEMAND_MAX_HEAP_IN_GB`

   The maximum amount of memory to be used for manual data collection.

   Example:

   ```
   VIEWPOINT_ETL_SCHEDULE_MAX_HEAP_IN_GB=12
   VIEWPOINT_ETL_ONDEMAND_MAX_HEAP_IN_GB=24
   VIEWPOINT_ETL_DETAILVIEW_SCHEDULE_MAX_HEAP_IN_GB=12
   VIEWPOINT_ETL_DETAILVIEW_ONDEMAND_MAX_HEAP_IN_GB=24
   ```

Setting the URL for accessing Analyzer viewpoint

In the following cases, use the **`setservicehostname`** command to set the URL for accessing Analyzer viewpoint.

- To access Analyzer viewpoint by using the host name
- To change the IP address that you are using to access Analyzer viewpoint, which was installed by using the installer

Before you begin

- You must have root privilege.
- The Analyzer viewpoint host must be able to access itself by using the host name. If the host name cannot be resolved, edit the `hosts` file so that the host can be accessed by using its host name. If Analyzer viewpoint was installed by using the OVF, edit the `hosts` file by running the **`edit-hosts`** command, which is stored in the `/opt/hitachi/analyzer_viewpoint/bin` directory.

Procedure

1. Log on to the Analyzer viewpoint server.
2. Run the following command:

```
/opt/hitachi/analyzer_viewpoint/bin/setservicehostname host-name
```

Configuring the 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, complete this procedure.

Before you begin

- You must have root privilege.
- If Analyzer viewpoint was installed by using the installer or you are using an instance of Ops Center Common Services running on a different host, skip steps 1 through 7.

Procedure

1. Run the following command to change the Ops Center Common Services host name:

```
/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*. If Analyzer viewpoint was installed by using the OVF, you cannot use the `-p` option of the **`cschgconnect.sh`** command for an instance of Ops Center Common Services that is running on the same host as Analyzer viewpoint. 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
```

   Example:

```
/opt/hitachi/analyzer_viewpoint/bin/setupcommonservice --csUri https://
viewpointhost/
```

6. Enter the username and password of the Common Services user according to the message output by the command.

   Example:

```
Authenticate with Common Services to set up the application.
Username:sysadmin
Password:
```

   The Common Services user specified for this command must belong to the **opscenter-administrators** user group.

7. Start the Analyzer viewpoint services.

```
systemctl start analyzer-viewpoint.target
```

8. Confirm that you can access Analyzer viewpoint from the Ops Center Portal by using the following URL:

```
https://host-name-of-the-Analyzer-viewpoint-server[:port-number]/portal/
```

9. 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 that was installed by using the OVF, 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.

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
```

   If `firewalld` is enabled, when you run the **`changeportnumber`** command, settings will be changed for the default zone. (Revise the settings if necessary.)

2. After running this command, you must use the following URL to access Analyzer viewpoint:

```
https://IP-address-or-host-name-of-the-Analyzer-viewpoint-server:port-number/
```

> **Note:** If you are using the instance of Ops Center Common Services bundled with Analyzer viewpoint that was installed by using the OVF, 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.

Upgrading the JDK for Analyzer viewpoint

Amazon Corretto 11 is installed on the host on which Analyzer viewpoint is installed. If you want to use a newer version of Amazon Corretto, complete the following procedure to upgrade.

Before you begin

- Check the release notes for the Amazon Corretto 11 versions supported by Analyzer viewpoint.
- Before upgrading the JDK, obtain a backup of the instance of Analyzer viewpoint that you are using.

Procedure

1. Check the Amazon Corretto 11 version installed on the Analyzer viewpoint host. If another product on the same host also uses Amazon Corretto 11, verify which versions are supported and whether an upgrade will cause any issues. If a problem might occur, do not upgrade Amazon Corretto. Alternatively, install Analyzer viewpoint on a different host than the product.
   - If the latest version is already installed, you do not to need to perform the following steps.
   - If the version is not the latest, continue to the next step.
2. From the Amazon Corretto site, download the latest JDK version, and then install it on the host where Analyzer viewpoint is installed.
3. If Common Services v10.6.1 or later is installed on the same host as Analyzer viewpoint, stop the services of Common Services. If another product that uses Amazon Corretto 11 is installed on the same host, stop it as needed.

   ```
   systemctl stop csportal
   ```

4. Disable the regular data collection for Analyzer viewpoint:

   ```
   /opt/hitachi/analyzer_viewpoint/etl/change-etl-config --disable
   ```

5. Run the RPM command to upgrade Amazon Corretto 11:

   ```
   rpm -Uv --nopost the-Amazon-Corretto-11-rpm-file-path
   ```

6. Enable the regular data collection for Analyzer viewpoint:

   ```
   /opt/hitachi/analyzer_viewpoint/etl/change-etl-config --enable
   ```

7. If Common Services v10.6.1 or later is installed on the same host as Analyzer viewpoint, start the services of Common Services. If another product that uses Amazon Corretto 11 is installed on the same host, start it as needed.

   ```
   systemctl start csportal
   ```

Settings required when using a virus detection program

If a virus detection program accesses database-related files used by Analyzer viewpoint, operations such as I/O delays or file locks can cause errors. To prevent these problems, exclude the following directories and files from the targets scanned by the virus detection program.

Exclude the following directories:

- `/opt/hitachi/analyzer_viewpoint/`
- `/var/log/hitachi/analyzer_viewpoint/`
- `/var/opt/hitachi/analyzer_viewpoint/`

Exclude the following files:

- `/etc/systemd/system/multi-user.target.wants/analyzer-viewpoint-bootstrapper.service`
- `/etc/systemd/system/multi-user.target.wants/postgresql-11@analyzer-viewpoint-apigw-db.service`
- `/etc/systemd/system/multi-user.target.wants/analyzer-viewpoint-apigw.service`
- `/etc/systemd/system/multi-user.target.wants/influxdb@analyzer-viewpoint-metrics-db.service`
- `/etc/systemd/system/multi-user.target.wants/analyzer-viewpoint-webconsole.service`
- `/etc/systemd/system/multi-user.target.wants/analyzer-viewpoint.target`
- `/etc/systemd/system/postgresql-11@analyzer-viewpoint-apigw-db.service.d`
- `/etc/systemd/system/postgresql-11@analyzer-viewpoint-apigw-db.service.d/override.conf`
- `/etc/systemd/system/analyzer-viewpoint-apigw-bootstrapper.service`
- `/etc/systemd/system/analyzer-viewpoint-apigw.service`
- `/etc/systemd/system/analyzer-viewpoint-apigw.service.d`
- `/etc/systemd/system/analyzer-viewpoint-apigw.service.d/override_kong.conf`
- `/etc/systemd/system/analyzer-viewpoint-apigw.service.d/override.conf`
- `/etc/systemd/system/influxdb@analyzer-viewpoint-metrics-db.service.d`
- `/etc/systemd/system/influxdb@analyzer-viewpoint-metrics-db.service.d/override.conf`
- `/etc/systemd/system/analyzer-viewpoint-webconsole.service.d`
- `/etc/systemd/system/analyzer-viewpoint-webconsole.service.d/override.conf`
- `/etc/systemd/system/analyzer-viewpoint.target`
- `/etc/systemd/system/analyzer-viewpoint-bootstrapper.service.d`
- `/etc/systemd/system/analyzer-viewpoint-bootstrapper.service.d/override.conf`

- /etc/systemd/system/analyzer-viewpoint.target.d
- /etc/systemd/system/analyzer-viewpoint.target.d/override.conf
- /etc/systemd/system/analyzer-viewpoint-bootstrapper.service
- /etc/systemd/system/analyzer-viewpoint-license-manager.service
- /etc/systemd/system/analyzer-viewpoint-iaa-launcher.service
- /etc/systemd/system/analyzer-viewpoint-inventory.service
- /etc/systemd/system/analyzer-viewpoint-api-proxy.service
- /etc/systemd/system/multi-user.target.wants/vm-initializer.service
- /etc/systemd/system/vm-initializer.service
- /etc/systemd/system/graphical.target.wants/vm-initializer.service
- /etc/systemd/system/vm-initializer.service.d
- /etc/systemd/system/vm-initializer.service.d/override.conf
- /etc/systemd/system/multi-user.target.wants/re-eruption.service
- /etc/systemd/system/graphical.target.wants/re-eruption.service

Note: Depending on the environment, some of the files might not exist.

Using Analyzer viewpoint

Creating user accounts

You can create user accounts for 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 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 Common Services user account that has permission to create users.

   For details, see the *Ops Center Portal 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 them to log in to 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 the Viewer role.

Next steps

Contact the Analyzer viewpoint administrator and ask them to assign the required role.

Assigning user roles

The following user roles are available for 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 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. Click **Configuration** > **Users** and select the **Role** to assign to the user.
3. If you assigned the user the Admin role, click **Server Admin** > **Users**. Select the applicable user and then under **Permissions**, enable **Viewpoint Admin**.

Changing the default data collection interval

By default, Analyzer viewpoint collects data every five minutes from the RAID Agent, and every 20 minutes from the Analyzer detail view. To change this interval, use the **`change-etl-config`** command.

Before you begin

You must have root permissions.

Procedure

1. Log on to the Analyzer viewpoint server.
2. Run the following command:

```
/opt/hitachi/analyzer_viewpoint/etl/change-etl-config --minutes data-collection-interval
```

For details, see change-etl-config command (on page 597).

Manually collecting data for a specific period

If you want to manually collect data for a specific period of time after the initial setup or when the regular data collection process does not run because of system maintenance or other reasons, use the **`run.sh`** command.

Before you begin

You must have root permissions.

Procedure

1. Log on to the Analyzer viewpoint server.
2. Run the following command:

```
/opt/hitachi/analyzer_viewpoint/etl/run.sh --startTime start-time --endTime end-time --dataSource source-from-which-data-is-collected
```

- By specifying the `dataSource` option, you can select the source from which data is to be collected. The specifiable values are `all`, `agent`, and `detail_view`. If you omit this option, `all` is assumed.
- Specify *start-time* and *end-time* in `yyyyMMddHHmm` format.
- Specify *start-time* and *end-time* so that the period defined by these times is in the range from one minute to 24 hours. If you specify `detail_view` for the `dataSource` option, you can specify a collection interval longer than 24 hours.

Note:

- You can collect data from the past 48 hours.
- Depending on the scope of data to collect, it might take 10 minutes or longer for the processing to finish.
- The longer the data collection period, the more memory the data collection process requires. If you want to change the maximum value for the amount of memory that the data collection process can use, see Changing the maximum amount of memory used by the data collection process (on page 579).
- To manually collect data in a time zone that uses daylight saving time, specify the scope of data to collect, taking into account the following effects that changing the time period might have:
  - During the switch to daylight saving time, if the time changes, for example, from 1:59 in standard time to 3:00 in daylight saving time and you specify a time that was skipped (between 2:00 and 2:59), the command assumes 3:00 was specified.
  - When daylight saving time ends, if the time changes, for example, from 1:59 in daylight saving time to 1:00 in standard time and you specify a time in the time period that is duplicated (between 1:00 and 1:59), the command always assumes the time during the period from 1:00 to 1:59 in daylight saving time was specified.

Setting the C/T delta value to monitor when Universal Replicator performance is analyzed

When you analyze Universal Replicator performance, the write delay time for the consistency group (C/T delta) is monitored. You can set a maximum value and threshold values for C/T delta. For details, see **Changing the maximum C/T delta value monitored when analyzing Universal Replicator performance (on page 482)**. To set the C/T delta threshold values (for the critical threshold and the warning threshold), edit the `ctdelta.threshold.properties` file as described here.

Before you begin

You must have root privilege.

Procedure

1. Log on to the Analyzer viewpoint server.
2. Open the following file:

```
/var/opt/hitachi/analyzer_viewpoint/etl/threshold/ctdelta.threshold.properties
```

3. Specify the C/T delta threshold value (warning or critical threshold) in units of seconds. You can specify the same value for all consistency groups, or specify values for each consistency group.

To specify the same value for all consistency groups, use the following settings:

- global.critical
- global.warning

To specify values for each consistency group, use the following settings:

- specific.critical.*primary-storage-system-serial-number.consistency-group-ID-(hexadecimal)*
- specific.warning.*primary-storage-system-serial-number.consistency-group-ID-(hexadecimal)*

Example settings:

```
global.warning=1500
global.critical=1800
specific.warning.123456.0=300
specific.critical.123456.0=600
specific.warning.123456.1F=1800
specific.critical.123456.1F=2700
```

Collecting Analyzer viewpoint 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.

Upgrading Analyzer viewpoint

The method for upgrading Analyzer viewpoint depends on your environment.

- When upgrading from version 10.5.0 or earlier:
  - Upgrade by using the virtual appliance.
- When upgrading from version 10.5.1 or later:
  - If Analyzer viewpoint was installed by using a virtual appliance, you can upgrade by using a virtual appliance or by using the installer.
  - If Analyzer viewpoint was installed by using the installer, you must upgrade by using the installer.

Note: You can upgrade Analyzer viewpoint either before or after upgrading Analyzer server and Analyzer detail view server.

Upgrading Analyzer viewpoint by using the virtual appliance

To upgrade Analyzer viewpoint by using the virtual appliance, deploy the OVF file from the installation media and import the data from the old virtual machine. You must reimport any Analyzer viewpoint plug-ins.

You cannot use the virtual appliance to upgrade an instance of Analyzer viewpoint that was installed or upgraded by using the installer.

Note: When Analyzer viewpoint is upgraded, the following RPM packages are upgraded:

- Amazon Corretto 11
- PostgreSQL 11

If another product that uses these RPM packages is installed on the same host as Analyzer viewpoint, check the versions of the RPM packages that are supported by that product and make sure that the upgrade will not cause any problems. If the upgrade might cause a problem, install Analyzer viewpoint on a different host than that product.

Procedure

1. Back up Analyzer viewpoint in case the upgrade fails. For details, see Backing up and restoring Analyzer viewpoint by using the VMware functionality (on page 593).
2. From a VMware vSphere client, log in to the VMware ESXi server.
3. Deploy the Analyzer viewpoint OVF by selecting **File** > **Deploy OVF Template** and selecting the Analyzer viewpoint files to create a new virtual machine.

   Tip: By default, the format of virtual disks is set to thick provisioning. However, you can also select thin provisioning.
4. Right-click the old virtual machine and select **Power** > **Shutdown Guest OS**.
5. If you did not create a snapshot on the old virtual machine, skip this step. If you created and retained a snapshot on the old virtual machine, 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.
6. Copy the old virtual disk to the newly deployed virtual machine.
   a. Open the **Storage** tree view.
   b. From **datastore**, select the directory where you stored the data from the old virtual machine.
   c. Select the old virtual machine vmdk and click **Copy to**.

      Note: If there is more than one file named **`Analyzer_viewpoint_`***xx.yy.zz_N*.vmdk, select and copy the file for which the value of *N* is greatest.
   d. Select the directory where you store the new virtual machine, and click **OK**.

7. Specify the settings required to add the existing hard disk to the new virtual machine.
   a. 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 **ADD NEW DEVICE**, and then select **Existing Hard Disk**.
   d. From **datastore**, select the directory where you store the new virtual machine.
   e. Select the old virtual machine vmdk, and click **OK**.
   f. Select **Hard disk 2**, click **×**, and then click **OK** to delete the disk.
8. To configure the network of the new virtual machine, refer to Using VM customization specification to configure the network (on page 566).
9. If you are using vCenter version 6.5, change the boot option to EFI:
   a. Right-click the new virtual machine and select **Edit Settings**.
   b. Go to the **VM Options** tab.
   c. Under **Boot Options**, from **Choose which firmware should be used to boot the virtual machine**, select **EFI** and click **OK**.
10. Right-click the new virtual machine and select **Power** > **Power ON**.
11. Reimport 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 **Re-import** for each dashboard.
12. Refresh the browser cache.

Next steps

If you changed the port number for Analyzer viewpoint on the old virtual machine, the firewall settings are not inherited. Specify the firewall settings again as needed to use the same port on the new virtual machine.

Upgrading Analyzer viewpoint by using the installer

To upgrade Analyzer viewpoint by using the installer, complete the following procedure.

If you installed Analyzer viewpoint by using the installer, you upgrade Analyzer viewpoint by using the installer. If you installed Analyzer viewpoint by using an OVF file equivalent to or later than version 10.5.1, you can upgrade Analyzer viewpoint by using the installer.

Before you begin

Before starting the upgrade, check the following requirements:

- Review the Analyzer viewpoint requirements (hardware and software). Make sure that the prerequisite packages are installed.
- Verify that you have root permission to run the installer and the precheck tool.

Note: When Analyzer viewpoint is upgraded, the following RPM packages are upgraded:

- Amazon Corretto 11
- PostgreSQL 11

If another product that uses these RPM packages is installed on the same host as Analyzer viewpoint, check the versions of the RPM packages that are supported by that product and make sure that the upgrade will not cause any problems. If the upgrade might cause a problem, install Analyzer viewpoint on a different host than that product.

Procedure

1. Back up Analyzer viewpoint in case the upgrade fails. For details, see Backing up and restoring Analyzer viewpoint (on page 593).
2. Log in to the host on which you want to complete the upgrade.
3. Stop the Analyzer viewpoint services:

   ```
   systemctl stop analyzer-viewpoint.target
   ```

4. Mount the Analyzer viewpoint installation media.
5. Move to the root directory of the installer.

   ```
   cd mounted-directory/VIEWPOINT
   ```

6. Run the precheck tool as the root user to check whether you are ready to install Analyzer viewpoint.

   ```
   bash viewpoint_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.

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

7. Run the following command as the root user to start the upgrade:

   ```
   bash viewpoint_install.sh VUP
   ```

   Do not forcibly stop the host during or immediately after an upgrade installation of Analyzer viewpoint. To stop or restart the host, wait until the upgrade installation is complete, and then perform the correct procedure (for example, by running an OS command).

8. Enter the required values according to the prompts, and complete the upgrade.
9. Reimport 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 **Re-import** for each dashboard.

10. Refresh the browser cache.

Backing up and restoring Analyzer viewpoint

To back up or restore Analyzer viewpoint, you can use one of two methods: VMware functions or commands. If you cannot use the VMware functions, perform backup and restore by using the commands. Decide which method to use based on your environment.

Backing up and restoring Analyzer viewpoint by using the VMware functionality

To back up and restore the Analyzer viewpoint virtual machine, complete the following procedure.

Procedure

1. Clone the Analyzer viewpoint virtual machine.
2. Back up the cloned virtual machine based on the environment backup policies.
3. When you want to restore, use the virtual machine you backed up.

Backing up Analyzer viewpoint by using a command

You can back up the settings information and data of Analyzer viewpoint.

Before you begin

You must have root permission.

Procedure

1. Stop the Analyzer viewpoint services.

```
systemctl stop analyzer-viewpoint.target
```

2. Run the **backup** command to back up the settings information and data of Analyzer viewpoint.

```
/opt/hitachi/analyzer_viewpoint/bin/backup --dir output-directory
```

For details, see backup command (on page 596).

3. After the backup finishes, start the Analyzer viewpoint services as needed.

```
systemctl start analyzer-viewpoint.target
```

Restoring Analyzer viewpoint by using a command

You can restore the settings information and data of Analyzer viewpoint.

Before you begin

Before you start restoring Analyzer viewpoint, verify the following:

- You must have root permission.
- The following items must be the same between the backup source host and the restore destination host:
  - Version number of the installed instance of Analyzer viewpoint
  - Host name

    If the host name is used to access Analyzer viewpoint on the backup source host, you must use the same host name for the restore destination host.
  - IP address
  - System locale

Procedure

1. Stop the Analyzer viewpoint services on the restore destination host.

   ```
   systemctl stop analyzer-viewpoint.target
   ```

2. Run the **`restore`** command to restore the settings information and data of Analyzer viewpoint.

   ```
   /opt/hitachi/analyzer_viewpoint/bin/restore --file backup-file-name
   ```

   For details, see restore command (on page 601).

3. Configure the firewall settings.

   If necessary, configure the settings so that the firewall allows the ports used to access Analyzer viewpoint.
4. To connect to an instance of Common Services other than the one where the backup destination was connected, re-register Analyzer viewpoint in Common Services.
5. If Analyzer viewpoint access on the backup source host used the host name, make sure that the host name can be resolved.
   - If the environment on the restore destination host was configured by using the installer, edit the `hosts` file.
   - If the Analyzer viewpoint environment on the backup source host was configured by using the installer, but the Analyzer viewpoint environment on the restore destination host was configured by using the OVF, make sure that the host name can be resolved by using the **`edit-hosts`** command.
6. In Analyzer viewpoint on the backup source host, if the SSL certificate was changed from the default self-signed certificate and stored in a location other than `/var/opt/hitachi/analyzer_viewpoint/`, manually migrate the SSL certificate.

7. After the restore finishes, start the Analyzer viewpoint services as needed.

```
systemctl start analyzer-viewpoint.target
```

Removing Analyzer viewpoint

Use the `viewpoint_uninstall.sh` command to remove the instance of Analyzer viewpoint that was installed by using the installer.

You cannot use this command to remove an instance of Analyzer viewpoint that was installed by deploying an OVF file.

Before you begin

You must have root privilege.

Procedure

1. Log on to the Analyzer viewpoint server.
2. Stop any security monitoring software, antivirus software, and process monitoring software.
3. Run the following commands:

```
cd /opt/hitachi/analyzer_viewpoint/uninstaller
bash viewpoint_uninstall.sh SYS
```

   Do not forcibly stop the host during or immediately after the removal of Analyzer viewpoint. To stop or restart the host, wait until the removal is complete, and then perform the correct procedure (for example, by running an OS command).

4. Enter the required values according to the prompts, and then complete the removal process.

Next steps

When you use the `viewpoint_uninstall.sh` command to remove Analyzer viewpoint, SELinux policy records that were added for Red Hat Enterprise Linux/Oracle Linux 8 are not deleted. Delete them as needed. Do not forcibly stop the host immediately after the deletion of the SELinux policy records. Similarly, the following rpm packages will not be removed. Remove them as needed by using the `rpm` command. If the command fails, run the `rpm` command with the `--nopreun` option specified.

- Amazon Corretto 11
- PostgreSQL 11
- Kong[#1]
- InfluxDB
- jq[#2]
- oniguruma[#2]

If you use Red Hat Enterprise Linux or Oracle Linux version 8 or later, do not remove jq and oniguruma, because they are prerequisite packages for the operating system.

#1: Before you remove Kong, delete the Lua modules in the following order.

```
/usr/local/bin/luarocks remove kong-oidc-viewpoint
```

```
/usr/local/bin/luarocks remove lua-resty-openidc
```

```
/usr/local/bin/luarocks remove lua-resty-jwt
```

#2: If you use Red Hat Enterprise Linux or Oracle Linux version 7 or earlier, remove jq before oniguruma.

Analyzer viewpoint commands

The following describes the Analyzer viewpoint commands.

backup command

Use this command to back up the settings information and data of Analyzer viewpoint to the specified directory.

You can back up the following information:

- Customized Analyzer viewpoint dashboard reports
- Historical data
- Information registered in Common Services
- Information about changes to port numbers
- Host name settings information
- Settings information such as data collection intervals and the maximum amount of memory
- Setting information for whether to enable or disable certificate verification and the certificates registered in the truststore

Format

```
backup --dir output-directory
```

Options

`dir` *`output-directory`*

Specify, as an absolute path, the directory in which to store the backup file.

The backup file is output in the format `viewpoint-backup-`*`viewpoint-version-backup-start-date-and-time`*`.tgz`.

Example

```
viewpoint-backup-105000-20201021-053210.tgz
```

Location

`/opt/hitachi/analyzer_viewpoint/bin/`

Notes

Make sure that the back up file storage directory has as much free space as the directory `/var/opt/hitachi/analyzer_viewpoint/`.

change-etl-config command

This command changes the settings for the Analyzer viewpoint process that collects data. You can use this command to change the data collection interval and enable or disable data collection.

Format

To change the data collection interval:

```
change-etl-config --minutes data-collection-interval [--dataSource {all | agent |
detail_view}]
```

To enable or disable data collection:

```
change-etl-config [--enable | --disable] [--dataSource {all | agent | detail_view}]
```

To check the data collection settings:

```
change-etl-config --display
```

Options

`minutes`

The data collection interval (in minutes). You can specify the following values: 1, 5, 10, 15, 20, 30, 60, 120, 180, 240, 360, 480, 720, and 1440.

We strongly recommend that you specify 20 minutes or longer for the data collection interval of Analyzer detail view.

`dataSource {all | agent | detail_view}`

The data source from which data is to be collected. Specify `agent` to collect data from the RAID Agent, `detail_view` to collect data from the Analyzer detail view, or `all` to collect data from both. If you omit this option, `agent` is assumed.

`enable`
Enables data collection.

`disable`
Disables data collection.

`display`
Display data collection settings:

Item	Description
ETL_COLLECTION_INTERVAL_IN_MINUTES	Currently configured data collection interval for the RAID Agent (in minutes)
ETL_COLLECTION_ENABLED	Status of data collection from the RAID Agent true: enable false: disable
ETL_DETAILVIEW_COLLECTION_INTERVAL_IN_MINUTES	Currently configured data collection interval for the Analyzer detail view (in minutes)
ETL_DETAILVIEW_COLLECTION_ENABLED	Status of data collection from the Analyzer detail view true: enable false: disable

Location

`/opt/hitachi/analyzer_viewpoint/etl`

Example

To change the interval for data collection from the RAID Agent to 10 minutes:

```
change-etl-config --minutes 10 --dataSource agent
```

To check the data collection settings:

```
change-etl-config --display
```

Output example:

```
ETL_COLLECTION_INTERVAL_IN_MINUTES=5
ETL_COLLECTION_ENABLED=false
```

```
ETL_DETAILVIEW_COLLECTION_INTERVAL_IN_MINUTES=5
ETL_DETAILVIEW_COLLECTION_ENABLED=true
```

Note: The longer the data collection interval, the more memory the data collection process requires. If you want to change the maximum value for the amount of memory that the data collection process can use, see Changing the maximum amount of memory used by the data collection process (on page 579).

config-cert command

Use this command to enable or disable certificate verification in Analyzer viewpoint and import certificates to the truststore.

Format

To enable or disable certification verification:

```
/opt/hitachi/analyzer_viewpoint/bin/config-cert [--enable | --disable]
```

To import a certificate to the truststore:

```
/opt/hitachi/analyzer_viewpoint/bin/config-cert --register certificate-file-name
registration-name-of-the-certificate
```

To delete a certificate from the truststore:

```
/opt/hitachi/analyzer_viewpoint/bin/config-cert --delete registration-name-of-the-
certificate
```

To check whether certificate verification is enabled and to check the certificates that were imported to the truststore:

```
/opt/hitachi/analyzer_viewpoint/bin/config-cert --status
```

To display details of the certificate imported to the truststore:

```
/opt/hitachi/analyzer_viewpoint/bin/config-cert --show-cert registration-name-of-the-
certificate
```

Options

enable
Enables certificate verification.

disable
Disables certificate verification.

register ***certificate-file-name registration-name-of-the-certificate***

Imports a certificate. Specify an absolute path to the certificate to import. To run the command, you need the password for the truststore. If the specified certificate is already registered, the command ends in an error. To import multiple certificates, run the command separately for each certificate.

Specify the registration name of the certificate by using no more than 64 bytes. You can use the following types of characters:

Halfwidth alphanumeric characters, _ - ( ) [ ] @ { }

You cannot use spaces. The value is not case-sensitive. If the argument contains a left "(" or right ")" parenthesis character, enclose the argument in double quotation marks.

delete ***registration-name-of-the-certificate***

Deletes an imported certificate. To delete multiple certificates, run the command separately for each certificate.

status

Checks whether certificate verification is enabled and check the certificates that were imported to the trustsrore.

show-cert ***registration-name-of-the-certificate***

Displays details of the certificate imported to the truststore.

Location

`/opt/hitachi/analyzer_viewpoint/bin/`

Return value

Return value	Description
0	The command ran normally.
1	The argument is invalid.
2	The specified file is invalid.
3	The registered name specified for the certificate includes invalid characters.
4	The registered name specified for the certificate is already being used.
5	There are no certificates corresponding to the specified registered name.
6	An attempt to run an internal command failed.
7	Invalid environment.

Example

```
/opt/hitachi/analyzer_viewpoint/bin/config-cert --register /root/cert/server.crt
commonservice
```

restore command

Use this command to restore the backup file for the settings information and data of Analyzer viewpoint that was obtained by using the **`backup`** command.

Format

```
restore --file backup-file-name
```

Options

`file` ***`backup-file-name`***

Specify, as an absolute path, the file name of the backup file.

Location

`/opt/hitachi/analyzer_viewpoint/bin/`

Notes

- The restore destination directory (`/var/opt/hitachi/analyzer_viewpoint/`) must have as much free space as the backup source directory (`/var/opt/hitachi/analyzer_viewpoint/`).
- If you run this command, the Analyzer viewpoint user data on the restore destination host is deleted. Manually back up the necessary user data and then recreate the data.
- The following settings and file are not restored. If necessary, manually reconfigure the settings or relocate the file.

  Firewall settings
  Configure the settings so that the firewall allows the ports used to access Analyzer viewpoint.

  Registration in Common Services
  To connect to an instance of Common Services other than the one where the backup destination was connected, re-register Analyzer viewpoint in Common Services.

  `hosts` file
  If name resolution on the Analyzer viewpoint backup source host uses the `hosts` file, the `hosts` file settings are not inherited.

  - If the Analyzer viewpoint environment on the restore destination host was configured by using the OVF, use the **`edit-hosts`** command to reconfigure the settings.
  - If the Analyzer viewpoint environment on the restore destination host was configured by using the installer, use the `hosts` file to reconfigure the settings.

  Settings configured by using the `edit-hosts` command
  If the Analyzer viewpoint restore destination host was configured by using the installer, the configured settings are not inherited by the **`edit-hosts`** command. If all of the following conditions are met, edit the `hosts` file so that the host name can be resolved.

  - The host name is resolved by using the **`edit-hosts`** command on the backup source host.
  - The Analyzer viewpoint environment on the backup source host was configured by using the OVF.

  SSL server certificate file
  If the backup source host has specified its own SSL certificate and the SSL certificate is stored in a location other than `/var/opt/hitachi/analyzer_viewpoint/`, manually migrate the SSL certificate.

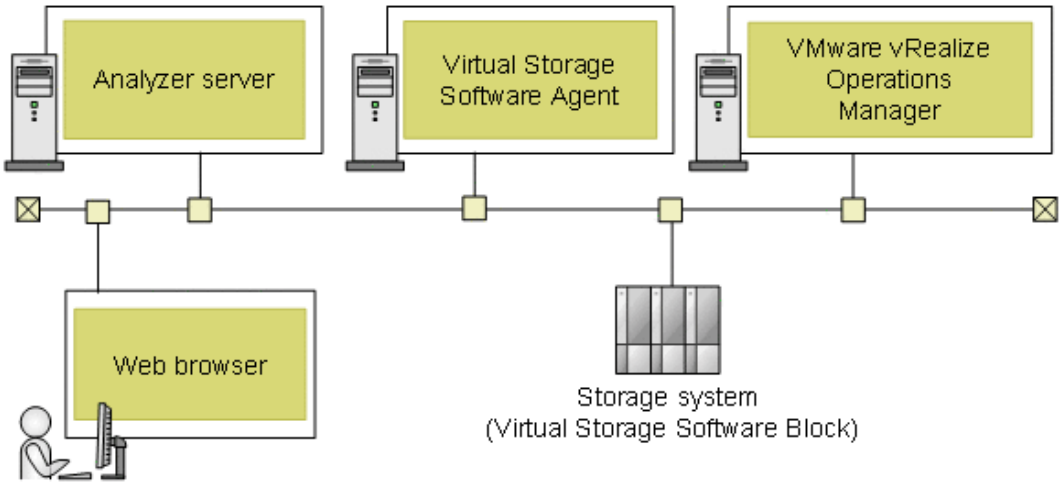
Chapter 18: Installing Virtual Storage Software Agent used by VMware vRealize Operations Manager

The following describes how to install Ops Center Analyzer Virtual Storage Software Agent and complete the initial setup. For details, see the *Hitachi Infrastructure Management Pack for VMware vRealize Operations User's Guide*.

Virtual Storage Software Agent system configuration

Virtual Storage Software Agent is required if you want to monitor Virtual Storage Software Block by using VMware vRealize Operations Manager.

The following shows an example of a Virtual Storage Software Agent system configuration.



Virtual Storage Software Agent requirements

The requirements for operating systems, network configuration, RPM packages, hardware, software, and ports are as follows:

Supported operating systems

- Red Hat Enterprise Linux 7.5-7.9, 8.1, 8.2 , 8.4 (x64)
- Oracle Linux 7.5-7.9, 8.2, 8.4 (Unbreakable Enterprise Kernel) (x64)
- Oracle Linux 7.5-7.9, 8.1, 8.2, 8.4 (Red Hat Compatible Kernel) (x64)

Network configuration

Virtual Storage Software Agent supports IPv4 only.

Prerequisite RPM packages

Install the following RPM packages before you install Virtual Storage Software Agent:

- coreutils
- firewalld
- gawk
- grep
- rpm
- sed
- systemd
- which

For Red Hat Enterprise Linux and Oracle Linux 8 or later, the following packages are also required:

- policycoreutils
- policycoreutils-python-utils

Note: If you want to use Red Hat Enterprise Linux or Oracle Linux 8 or later, we strongly recommend that after you install the prerequisite packages, you upgrade the following packages to the following versions:

- libsemanage 2.9-3 or later
- python3-libsemanage 2.9-3 or later

Hardware requirements

Item	Requirements
Processor	4 cores
Memory	8 GB
Disk space	10 GB

Software requirements

To use Virtual Storage Software Agent, your environment must meet the following requirements:

- The Ops Center Analyzer version must be 10.8.1 or later. Follow the procedure described in Initial setup of Analyzer server (on page 103).
- The Virtual Storage Software Block version must be 1.10 or later.

Port requirements

Source IP address	Target IP address	Default port	Protocol
Analyzer server	Virtual Storage Software Agent	24081	HTTPS
Virtual Storage Software Agent	Virtual Storage Software Block	443	HTTPS

Installing Virtual Storage Software Agent

The Virtual Storage Software Agent installation installs Amazon Corretto 8. If an earlier version of Amazon Corretto is already installed, you are prompted whether to upgrade.

Before you begin

- Review the system requirements.
- If `firewalld` is enabled, the settings will be changed for the default zone. If required, revise the settings after the installation finishes.

Procedure

1. Stop all security monitoring software, antivirus software, and process monitoring software.
2. Mount the Hitachi Ops Center installation media, go to the TOOLS directory, and copy the `VirtualStorageSoftwareAgent.zip` file to a directory on the Linux host.

   Note:
   - You must use only the following characters in the directory path to which the installer is copied: `A-Z a-z 0-9 - . _`
   - Do not use spaces.

3. Unzip the file and move to the `VirtualStorageSoftwareAgent` directory:

```
cd directory-where-you-unzipped-file/VirtualStorageSoftwareAgent
```

4. To start the installation, run the following command as the root user:

```
sh ./install.sh NEW
```

Do not forcibly stop the host during or immediately after the installation of Virtual Storage Software Agent. To stop or restart the host, wait until the installation is complete, and then perform the correct procedure (for example, by running an OS command).

Note:

- The default installation directory of Virtual Storage Software Agent is `/opt/hitachi`.
- For a repair installation, run the following command:

```
sh ./install.sh VUP
```

- To check the version of Virtual Storage Software Agent, run the following command:

```
cat Virtual-Storage-Software-Agent-installation-destination-directory/VirtualStorageSoftwareAgent/system/product_version
```

Changing the Linux host environment with the installer

If you run the Virtual Storage Software Agent installer, the internal processing of the installer changes the environment of the host on which Virtual Storage Software Agent is installed as follows.

Change	Details
Addition of SELinux policy records	For Red Hat Enterprise Linux/Oracle Linux 8, policy records for files in the following directory are added: `/var/Virtual-Storage-Software-Agent-installation-destination-directory/VirtualStorageSoftwareAgent`

Setting up Analyzer server to use Virtual Storage Software Agent

Set up the Analyzer server to use the Virtual Storage Software Agent as follows:

Procedure

1. Log on to the Analyzer server as root.
2. Open the Analyzer server connection definition file with a text editor:

   `Analyzer-server-installation-destination-directory/Analytics/conf/virtualstoragesoftware-access-points.yaml`

3. Edit the file to specifying the following settings:
   - `agentHostOrIpAddress`: Host name or IP address of Virtual Storage Software Agent. If you want to specify a host name, make sure it can be resolved on the host where the Analyzer server is installed. If you specify the IP address, you must use IPv4.
   - `protocol`: Protocol for connecting to Virtual Storage Software Agent. Specify `http` or `https`. Set the same value as the `protocol` specified in the `userconfig-setting.yaml` file on Virtual Storage Software Agent.
   - `agentHostName`: Virtual Storage Software Agent host name. Make sure that the host name can be resolved from the Analyzer server.
   - `port`: Port number for connecting to Virtual Storage Software Agent. Set the same value as the `port` specified in the `userconfig-setting.yaml` file on Virtual Storage Software Agent.

   The following is an example:

   ```
   agentHostOrIpAddress: host1
   protocol: https
   agentHostName: host1
   port: 24081
   ```

   Note: If you want to connect with multiple instances of Virtual Storage Software Agent, create a separate `agentHostOrIpAddress` entry for each host.

4. Restart the Analyzer server. For details, see Starting and stopping the Ops Center Analyzer services (on page 438).

Configuring Virtual Storage Software Agent settings

Follow this procedure to configure the Virtual Storage Software Agent settings.

Procedure

1. Configure Virtual Storage Software Agent.

   Setting up Virtual Storage Software Agent (on page 207)

2. Change the settings of Virtual Storage Software Agent.
   - Setting up SSL communication (Virtual Storage Software Agent) (on page 413)
     - Creating a private key and a certificate signing request for Virtual Storage Software Agent server (on page 414)
     - Submitting a certificate signing request (CSR) for Virtual Storage Software Agent (on page 414)
     - Enabling SSL communication for Virtual Storage Software Agent (on page 415)
     - Importing Virtual Storage Software Agent certificates to Analyzer server truststore (on page 608)
   - Configuring an SSL certificate (Virtual Storage Software Block) (on page 417)
     - Importing Virtual Storage Software Block certificates to the Virtual Storage Software Agent truststore (on page 418)
   - Collecting the log files of Virtual Storage Software Agent (on page 539)
   - Starting the Virtual Storage Software Agent services (on page 443)
   - Stopping the Virtual Storage Software Agent services (on page 443)
   - Upgrading the JDK for Virtual Storage Software Agent (on page 485)
   - Backing up Virtual Storage Software Agent (on page 512)
   - Restoring Virtual Storage Software Agent (on page 518)

Importing Virtual Storage Software Agent certificates to Analyzer server truststore

To enable the Analyzer server to verify Virtual Storage Software Agent certificates, import Virtual Storage Software Agent certificates to the Analyzer server truststore, and edit the `config_user.properties` file.

Before you begin

You must have root permission.

Procedure

1. Save the server certificates for Virtual Storage Software Agent on the Analyzer server.
2. Stop the Analyzer server services.

3. Run the **`keytool`** command to import the certificates for Virtual Storage Software Agent to the truststore file:

```
Common-component-installation-destination-directory/uCPSB11/jdk/bin/keytool -
import -alias alias-name -file certificate-file-name -keystore truststore-file-
name -storepass truststore-password -storetype JKS
```

Note:

Note the following when specifying 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.

- For the *`alias-name`*, specify a name that identifies whether the certificate is the certificate for Virtual Storage Software Agent.
- For the *`certificate-file-name`*, specify the absolute path.
- The truststore file is stored in the following location:

  `Common-component-installation-destination-directory``/uCPSB11/hjdk/jdk/lib/security/jssecacerts`

- Specify a password for the *`truststore-password`*.
- You must specify `JKS` for the keystore type of the truststore.

4. Enable the verification of server certificates, change the following properties in the `config_user.properties` file:
   - Location:

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

   - Key: `cert.verify.enabled`
   - Value: `true`
5. Run the following command to start the Analyzer server services.

Removing Virtual Storage Software Agent

To remove Virtual Storage Software Agent:

Procedure

1. Log on as root on the host where Virtual Storage Software Agent is installed.

2. Stop any security monitoring software, antivirus software, and process monitoring software.
3. Run the following command:

```
cd /Virtual-Storage-Software-Agent-installation-destination-directory/
VirtualStorageSoftwareAgent/uninstaller
sh ./uninstall.sh SYS
```

Next steps

When you use the `uninstall.sh` command to remove Virtual Storage Software Agent, SELinux policy records that were added for Red Hat Enterprise Linux/Oracle Linux 8 are not deleted. Delete them as needed. Do not forcibly stop the host immediately after the deletion of the SELinux policy records.

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
`backupsystem`	Backs up Analyzer server setting information in the folder you specify.
`changememory`	Changes the maximum amount of memory that can be used by the Analyzer server.
`encryptpassword`	Creates a password file to be specified as an argument of commands in Analyzer server.
`hcmds64checkauth`	Checks the settings in the `exauth.properties` file and the connection to the external authentication server when connecting to an external authentication server.
`hcmds64getlogs`	Collects log files that are output during operation of Analyzer server, and then outputs the log files to an archive file.
`hcmds64intg`	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. If you fail to delete authentication data when uninstalling Analyzer server, use this command to delete the authentication data.

Command	Description
hcmds64ldapuser	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.
hcmds64prmset	Registers, changes, and cancels the registration of the host that manages the user accounts used for connection with Ops Center Automator.
hcmds64radiussecret	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.
hcmds64srv	Starts or stops Analyzer server services and databases. The command also displays the status of Analyzer server services.
hcmds64ssltool	Creates private keys, CSRs, and self-signed certificates (including its content files), which are required for SSL connection.
hcmds64unlockaccount	Unlocks a user account. Use this command when you cannot log on to Analyzer server because all the user accounts are locked.
reloadtemplate	Reload the Analyzer server template files during the startup of Analyzer server.
restoresystem	Restores the backup for Analyzer server settings information that you collected by running the **backupsystem** command.
setupcommonservice	Registers the Ops Center Analyzer to Ops Center Common Services.

The Analyzer probe server commands

Command	Description
collection_config	Changes the data collection intervals for the RAID Agent that is installed with Ops Center Analyzer.
htmsrv	Starts or stops services, checks the operating status, and changes the type of startup method for the RAID Agent.
htmssltool	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	Description
jpcinslist	Displays the instance names that have been set up by the RAID Agent.

Command usage guidelines

You must consider the following when using commands.

- You must have root permission.
- 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.
- 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 line. If an argument value contains a space or special symbols, you must escape such characters by enclosing each 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 (\)

- 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.

backupsystem

Use this command to back up Analyzer server setting information in the directory you specified.

Format

```
backupsystem
     -dir output-directory
     -type {all | Analytics}
```

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.

Location

`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:

  10 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.

- Stop the service by running the **`hcmds64srv`** command with the `stop` option. The service to stop 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.

- 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`)
- If the **`changememory`** command was used to change the maximum amount of memory that can be used by the Analyzer server, when you restore the system, run the **`changememory`** command again.

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.

Return value	Description
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
```

changememory

Change the maximum amount of memory that can be used by the Analyzer server.

Format

```
changememory
     {-set memory-size [-auto] | -status}
```

Options

`set` *`memory-size`*

Specify the maximum amount of memory (in GB) that can be used by the Analyzer server. You can specify a value in the range from 8 to 256. Note that the specified value must be less than the total memory of the OS.

`auto`

Automatically stops and starts Analyzer server services.

`status`

Displays the setting status for the maximum amount of memory that can be used by the Analyzer server.

Location

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

Notes

If you run this command without specifying the `auto` option, you must restart the product by running the **`hcmds64srv`** command on the host where you ran the **`changememory`** command.

Return values

Return value	Description
0	The command ran normally.
1	The argument is invalid.
2	Command running was interrupted.
4	Another command is currently running.
13	An attempt to write to the file 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.
18	An attempt to read the file failed.
255	Command running was interrupted because of another error.

Example

To change the maximum amount of memory that can be used by the Analyzer server to 32 GB:

```
changememory -set 32 -auto
```

To check the setting status for the maximum amount of memory that can be used by the Analyzer server:

```
changememory -status
```

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). Run this command on the Analyzer probe server. To change the intervals for collecting data, 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.

In the 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`	Indicates whether data collection intervals can be changed ▪ **RW:** Can be changed. ▪ **R:** Cannot be changed. ▪ **N/A:** Cannot be changed because data cannot be collected.
`Type`	Details of data collection intervals set for the record ▪ **Collection Interval:** The value of the data collection intervals of the record is displayed in the `Current` column. ▪ **Sync Collection With:** The value of the data collection intervals of the record is synchronized with the record values displayed in the `Current` column. ▪ **Not Collectable:** This value is displayed when `Mode` is N/A. This indicates that the record cannot be collected.
`Current`	The value specified as data collection intervals. The following information is displayed according to the value in the `Type` column: ▪ For **`Collection Interval`** Data collection intervals (unit: seconds) ▪ For **`Sync Collection With`** ID of the record with which the value of data collection intervals is to be synchronized ▪ For **`Not Collectable`** **-** (hyphen)
`Default`	The default value. The following information is displayed according to the value in the `Type` column: ▪ For **`Collection Interval`** Data collection intervals (unit: seconds) ▪ For **`Sync Collection With`** ID of the record with which the value of data collection intervals is to be synchronized ▪ For **`Not Collectable`** **-** (hyphen) Note that, for some records, the default data collection intervals vary depending on the `Access Type`.

Item	Description
`Modified`	Information indicating whether the value specified for the data collection interval is customized. ▪ **Y:** The setting is customized.

`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.

Running the command allows you to change the data collection intervals for only one record. When you want to run 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_VVTC	A value that is a multiple of 3,600 and a divisor of 86,400 in the range from 3,600 to 86,400
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

Record ID	Requirement for the values to be specified as data collection intervals
PD_UMS, PI, PI_CHS, PI_CLMS, PI_CLPS, PI_CTGS, PI_JNLS, 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 to update, as well as the RAID Agent service.

`-restart`
Stops the instance for which the data collection interval to update, 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 status 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 `Access Type`.
15	The value specified for the data collection interval is invalid.
16	Running the command was suspended because the RAID Agent service is not stopped.
17	The instance to be updated does not exist.
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.

Return value	Description
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]
     -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. Enter the password in response to the prompt.

If you omit the `user` option, you can enter a user ID in response to the prompt.

`passwordfile` *`password-file-path`*

Use an absolute or relative path to specify a path of the password file to be created.

Location

`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.)
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.
18	An attempt to read the file failed.
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 run 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]
     [-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. Enter the password in response to the prompt.

If you omit the `user` option, you can enter a user ID in response to the prompt.

- 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.

summary

This option simplifies the confirmation message that appears when you run the command.

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

Common-component-installation-destination-directory/bin

Notes

- You cannot specify a user account with a user-ID or password that begins with a hyphen (-).
- 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.

Return value	Description
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. Unit's place: Number of connection errors Ten's place: Number of authentication errors The maximum number of each place is nine. If more than nine errors occur, each place displays nine.
250	The command is run on the secondary server.
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:

```
hcmds64checkauth -summary
```

Escaping special characters

The following explains how to escape when running the `hcmds64ldapuser` command, `hcmds64radiussecret` command, or `hcmds64checkauth` command.

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.

hcmds64getlogs

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

```
hcmds64getlogs
     -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	▪ *Archive-file-name-in-the-arc-option*_64.jar ▪ *Archive-file-name-in-the-arc-option*_64.hdb.jar
db	*Archive-file-name-in-the-arc-option*_64.db.jar
csv	*Archive-file-name-in-the-arc-option*_64.csv.jar

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.

Archive file	Output result
output-destination-directory-in-dir-option/*archive-file-name-in-arc-option*_64.jar	▪ All files in *Analyzer-server-installation-destination-directory*/Analytics/logs ▪ All files in *Analyzer-server-installation-destination-directory*/Analytics/conf ▪ All files in *Analyzer-server-installation-destination-directory*/Analytics/work ▪ All files in *Analyzer-server-installation-destination-directory*/Analytics/data ▪ All files in *Analyzer-server-installation-destination-directory*/Analytics/system ▪ /var/opt/hitachi/HPA/*.log files ▪ List of the files in *Analyzer-server-installation-destination-directory*/Analytics ▪ Result of running the **`netstat`** command of the OS with the `-nao` option specified

Archive file	Output result
	▪ Result of running the **`uname`** command of the OS with the `-a` option specified ▪ Result of running the **`free`** command of the OS ▪ Result of running the **`ps`** command of the OS with the `-elfa` option specified ▪ `/var/log/messages*` files ▪ `/etc/hosts` file ▪ `/etc/services` file ▪ Result of running the **`env`** command of the OS ▪ Result of running the **`sysctl`** command of the OS with the `-a` option specified ▪ Result of running the **`ulimit`** command of the OS with the `-a` option specified ▪ Result of running the **`ipcs`** command of the OS with the `-a` option specified ▪ Result of running the **`cat /proc/meminfo`** command of the OS ▪ Result of running the **`df`** command of the OS with the `-k` option specified ▪ Result of running the **`dmesg`** command of the OS ▪ Result of running the **`rpm`** command of the OS with the `-qa` option specified ▪ `/etc/inittab` file ▪ `/etc/redhat-release` file ▪ `/etc/nsswitch.conf` file ▪ `/etc/resolv.conf` file ▪ Result of running the **`ip`** command of the OS with the `-a` option specified ▪ `/etc/.hitachi/Analytics/installInfo` file ▪ `/etc/sysconfig/iptables-config` file ▪ Result of running the **`service iptables status`** command of the OS ▪ Result of running Common component's material collection tool (**`hcmdsgetlogs`**, **`hcmdsras`**)

Archive file	Output result
	▪ Result of running the **`systemctl status firewalld.service`** command of the OS ▪ Result of running the **`firewall-cmd`** command of the OS with the `--list-all-zones` option specified ▪ Result of running the **`ss`** command of the OS with the `-nao` option specified
*output-destination-directory-in-dir-option/archive-file-name-in-arc-option*_64.hdb.jar	Result of running Common component's material collection tool (**`hcmdsgetlogs`**)
*output-destination-directory-in-dir-option/archive-file-name-in-arc-option*_64.db.jar	
*output-destination-directory-in-dir-option/archive-file-name-in-arc-option*_64.csv.jar	

Location

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:

  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]
```

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. Enter the password in response to the prompt. If you omit the `user` option, you can enter a user ID in response to the prompt.

Location

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
```

hcmds64ldapuser

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 **`hcmds64checkauth`** command to verify whether the user account can be correctly authenticated.

Format

To register an LDAP search user account:

```
hcmds64ldapuser -set
     -dn DN-of-user-account-used-to-search-for-LDAP-user-info
     -name name
```

To delete an LDAP search user account:

```
hcmds64ldapuser -delete
     -name name
```

To display external authentication servers for which LDAP search user accounts have already been registered in the Analyzer server:

```
hcmds64ldapuser -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 (`\`)

Enter the password in response to the prompt.

`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

`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 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:

```
hcmds64ldapuser -set -dn "cn=administrator,cn=admin,dc=example\\,com" -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" -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 run 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.

Run this command on the server that is set as the secondary server.

To connect to Ops Center Automator that is linked with Device Manager, run this command on Analyzer server.

To connect to Ops Center Automator that is not linked with Device Manager, run 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 run 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 run (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

`Common-component-installation-destination-directory``/bin`

Notes

After running this command, restart the product by using the **`hcmds64srv`** command.

Return values

Return value	Description
0	The command ran normally.
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.

When you run the command, enter a shared secret in response to the prompt. For a shared secret, you can specify printable ASCII characters (`0x21` to `0x7E`) of 128 bytes or less.

If you register a shared secret by using this command, run the **`hcmds64checkauth`** command to verify whether the shared secret can be correctly authenticated.

Format

To register a shared secret:

```
hcmds64radiussecret
     -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

`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

`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 -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
HBase 64 Storage Mgmt Web SSO Service	Y	N	N
Database process*	Y	N	N
Legend: Y: Processed 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

Service display name and process	Start	Stop	Status display
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
Legend: 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

`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 `syslog`:

    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	**With `start` option** The service was already started. **With `stop` option** 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.

Return value	Description
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:

```
hcmds64srv -start
```

To stop all services:

```
hcmds64srv -stop
```

To check the status of all services:

```
hcmds64srv -status
```

To start the services of only Analyzer server products:

```
hcmds64srv -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-directory`*`/uCPSB11/httpsd/conf/ssl/server/`.

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-directory/`*`uCPSB11/httpsd/conf/ssl/server/`.

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-directory/`*`uCPSB11/httpsd/conf/ssl/server/`.

`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-directory/`*`uCPSB11/httpsd/conf/ssl/server/`.

`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 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*

Attribute type	Definition	Window response	Attribute value
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

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 directory 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.

hcmds64unlockaccount

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

```
hcmds64unlockaccount
     [-user user-ID]
```

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. Enter the password in response to the prompt. If you omit the `user` option, you will be prompted to enter a user ID.

Location

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, add a backslash (\) as an escape character before each symbol.
- 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.
253	Communication with the authentication server failed.
254	The command was run on the secondary server side.

Return value	Description
255	The command ran abnormally.

Example

The following example shows how to use this command to unlock a user account:

```
hcmds64unlockaccount
```

htmsrv

Use the **htmsrv** command to start or stop services, check the operating status, and change the type of startup method for the RAID Agent. This command must be run by a user with root permissions on the Analyzer probe server host.

- `start`: Specify this to start the services.
- `stop`: Specify this to stop the services.
- `status`: Specify this to check the operating status of the services.
- `starttype`: Specify this to specify how the services are to start.

Format (to start or stop the services)

```
htmsrv
     { start | stop } {-all | -webservice | -key agtd [-inst instance-name]}
```

Format (to check the operating status)

```
htmsrv
    status  {-all | -webservice | -key agtd | -id service-ID}
```

Format (to change the type of startup method)

```
htmsrv
    starttype  { auto | manual } -webservice
```

Options

`-all`

Specify this option to run the following services.

- RAID Agent REST Web Service
- RAID Agent REST Application Service
- Agent Collector, Agent Store, Status Server, Action Handler

`-webservice`

Specify this option to run the following services.

- RAID Agent REST Web Service
- RAID Agent REST Application Service

`-key agtd`

Specify this option to run the following services.

- Agent Collector, Agent Store, Status Server, Action Handler

`-inst` *`instance-name`*

Specify this option to run the following services for a specific instance.

- Agent Collector, Agent Store

`-id` *`service-ID`*

Specify this option to run the following services for a specific service ID.

- Agent Collector, Agent Store, Status Server, Action Handler

`auto`

Specify this option to automatically start the RAID Agent REST Web Service and the RAID Agent REST Application Service.

`manual`

Specify this option to manually start the RAID Agent REST Web Service and the RAID Agent REST Application Service.

Location

This command is stored in the following directory on the Analyzer probe server:

`/opt/jp1pc/htnm/bin/`

Return values

Return value	Description
0	**When an option other than the `status` option is specified:** The command ran normally.

Return value	Description
	When the `status` option is specified: The command ran normally. (All the services to be checked are running.)
1	**When the `start` option is specified:** The command ran normally. (The specified services are already running.) **When the `stop` option is specified:** The command ran normally. (The specified services have already stopped.) **When the `status` option is specified:** The command ran normally. (All the services to be checked have already stopped.)
2	**When the `start` option is specified:** The command ran normally. (Some of the services to be checked are running, and some have stopped.)
10	The specified option is invalid.
255	An unexpected error occurred.

Example

To check the status of all services:

```
htmsrv status -all
```

```
KATR10032-I The specified service is already running. (service=Status Server,
serviceid=PT1hostA)
KATR10032-I The specified service is already running. (service=Action Handler,
serviceid=PH1hostA)
KATR10032-I The specified service is already running. (service=Agent Store,
serviceid=DS1testinst[hostA])
KATR10032-I The specified service is already running. (service=Agent Collector,
serviceid=DA1testinst[hostA])
KATR10032-I The specified service is already running. (service=Agent REST Application
Service)
KATR10032-I The specified service is already running. (service=Agent REST Web Service)
```

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

Attribute type	Definition	Window response	Attribute value
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/jp1pc/htnm/bin/`

Notes

Run 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.

Example

```
htmssltool -key /root/htnmkey.key -csr /root/htnmkey.csr -cert /root/htnmkey.cert -
certtext /root/htnmkey.cert.txt
```

jpcinslist

Use the **`jpcinslist`** command to display the instance names that have been set up by the RAID Agent. This command must be run by a user with root permissions on the Analyzer probe server host.

Format

```
jpcinslist agtd
```

Location

This command is stored in the following directory on the Analyzer probe server:

`/opt/jp1pc/tools/`

Notes

- If you have not created an instance, nothing is output when you run the command.
- If you interrupt the command by using the `Ctrl+C` key or a signal, certain return values are not returned. Therefore, if you interrupt the command by using the `Ctrl+C` key or a signal, ignore the return value.

Return values

Return value	Description
0	The command ran normally.
1	The specified option is invalid.
5	The specified option is invalid.
10	The command is running in another session.
100	The RAID Agent environment is invalid.
102	The specified option is invalid.
200	Memory is insufficient.
210	There is not enough disk space.
211	The file or directory cannot be accessed.
230	The internal command could not be run.
255	An unexpected error occurred.

Example

```
jpcinslist agtd
```

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	*Analyzer-server-installation-destination-directory*/Analytics/conf/template/mail

Type of template file	Reference destination folder
Template file for commands	*Analyzer-server-installation-destination-directory*/Analytics/conf/template/command
Template file for Ops Center Automator	*Analyzer-server-installation-destination-directory*/Analytics/conf/template/automation

Format

```
reloadtemplate
     -user user-ID
     -passwordfile password-file
```

Arguments

user *user-ID*

Specify the Analyzer server user ID to use when running the command. 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

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	The command was interrupted.
3	The service status is invalid.
5	Communication failed.

Return value	Description
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.
18	An attempt to read the file failed.
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}
```

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.

Location

`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-directory`*`/Analytics/conf`. This file is overwritten every time the **`restoresystem`** is run. If a file with an extension of `.original` exists before running the command and you want to save the file, change the file extension before using the command.
- The settings for connecting to the Analyzer detail view server and those for connecting to Common Services are always restored. For this reason, if you are performing a migration to a different host, manually reconfigure these settings after they are restored.
- 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:

  - *`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:

  - `security.conf`

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

  - `user_httpsd.conf`

    `Common-component-installation-destination-directory``/uCPSB11/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.

- Stop the service by running the **`hcmds64srv`** command with the `stop` option. The service to stop 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

    If you are performing the restore as part of the procedure for migrating the system to a different host name, the installation directories on the backup source host and restore destination host do not need to match.

- 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.

Return value	Description
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.
14	You do not have permission to run this command.
18	An attempt to read the file failed.
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
```

setupcommonservice

Use this command to register Analyzer with Ops Center Common Services. This command also updates the Analyzer information that is registered in Common Services. This command requires a secure connection between Common Services and Analyzer. See the *Hitachi Ops Center Installation and Configuration Guide* for more information.

Format

When registering Analyzer with Common Services

```
setupcommonservice
      -csUri Common-Services-URL
     [-csUsername Common-Services-username]
     [-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 Analyzer information registered in Common Services

```
setupcommonservice
     [-csUri Common-Services-URL
      -csUsername Common-Services-username]
     [-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 command usage information

```
setupcommonservice -help
```

Options

csUri *Common-Services-URL*

Specify the Common Services URL (URL for Ops Center Portal).

csUsername *Common-Services-username*

Specify a username with Security Admin or System Admin role for Common Services. Enter the password in response to the prompt.

If you omit this option, you can enter a Common Services username in response to the prompt.

appHostname *Analyzer-server-host-name-or-IP-address*

Specify the host name or IP address for the Analyzer server.

If this option is omitted, the host name of Analyzer server is set.

appPort *Analyzer-server-port*

Specify the port number for the 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 the 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 command usage information.

Location

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

Notes

If you run this command without specifying the `auto` option, you must restart the product by running the **`hcmds64srv`** command on the host where you ran the **`setupcommonservice`** 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.
13	An attempt to write to the file 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.
18	An attempt to read the file 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 -appHostname
myanalyzer.com -appName Analyzer_B -appDescription "For managing site B" -auto
```

To reregister Analyzer with an instance of Common Services on another host:

```
setupcommonservice -csUri https://myopscenter2.com:443/portal -csUsername sysadmin -
appHostname myanalyzer.com -appName Analyzer_B -appDescription "For managing site B" -
auto
```

Note: After running the command, delete the Analyzer information from the original Ops Center Portal.

If the host name of the Common Services instance in which Analyzer is registered was changed to `US_opscenter.com`:

```
setupcommonservice -csUri https://US_opscenter.com:443/portal -auto
```

To change the Analyzer server host name that is registered in Common Services to `myanalyzer2.com`:

```
setupcommonservice -appHostname myanalyzer2.com -auto
```

Appendix B: 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

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.
- UTF-8 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	Corresponding Analyzer metric
Public logs	`logger.syslog level`	Specify a threshold value for outputting syslog.	▪ 0 ▪ 10	`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`	Period (unit: days) for which to check the number of performance values that are required to start the calculation of dynamic threshold values. To specify more than one value, use commas (,) to delimit the values.	Single-byte numerals and commas (,)	`1, 3, 7, 14`	--

Category	Key name	Setting	Specifiable values	Default value	Corresponding Analyzer metric
	`dynamicThreshold.minimumDataN`	Specify the minimum number of performance values that is required to start the calculation of dynamic threshold values. The calculation of dynamic threshold values starts when the number of performance values in the period specified for `dynamicThreshold.startLatencyDay` exceeds the minimum number of performance values specified for `dynamicThreshold.minimumDataN`.	1 to 2,147,483,647	`150`	--
Dynamic threshold values (margin)	`dynamicThreshold.margin.Severe.plus`	Specify the margin for addition when the value of Margin is Severe.	0 to 2,147,483,647	`1`	--
	`dynamicThreshold.margin.Severe.rate`	Specify the margin for multiplication (unit: %) when the value of Margin is Severe.	0 to 100	`1`	--
	`dynamicThreshold.margin.Normal.plus`	Specify the margin for addition when the value of Margin is Normal.	0 to 2,147,483,647	`5`	--

Category	Key name	Setting	Specifiable values	Default value	Corresponding Analyzer metric
	`dynamicThreshold.margin.Normal.rate`	Specify the margin for multiplication (unit: %) when the value of Margin is Normal.	0 to 100	`5`	--
	`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`	--
Event issuance conditions	`dynamicThreshold.alertCondition.RAID_VOLUME_RAIDLDEV_TOTALIOPS.numberInPeriod.number`	Specify the number of times that a spike exceeds a threshold to issue an event of the Hitachi Storage Total IOPS (LDEV) metric during the threshold monitoring period.	1 to the number of samples during the period	`1`	`Hitachi Storage Total IOPS (LDEV)`
	`dynamicThreshold.alertCondition.RAID_VOLUME_RAIDLDEV_TOTALIOPS.numberInPeriod.period`	Specify the threshold monitoring period (in minutes) for the Hitachi Storage Total IOPS (LDEV) metric.	0 < period <= 60 and a multiple of the data collection interval	`5`	

Category	Key name	Setting	Specifiable values	Default value	Corresponding Analyzer metric
	dynamicThreshold.alertCondition.RAID_VOLUME_RAIDLDEV_TRANSFERRATE.numberInPeriod.number	Specify the number of times that a spike exceeds a threshold to issue an event of the Hitachi Storage Transfer Rate (LDEV) metric during the threshold monitoring period.	1 to the number of samples during the period	1	Hitachi Storage Transfer Rate (LDEV)
	dynamicThreshold.alertCondition.RAID_VOLUME_RAIDLDEV_TRANSFERRATE.numberInPeriod.period	Specify the threshold monitoring period (in minutes) for the Hitachi Storage Transfer Rate (LDEV) metric.	0 < period <= 60	5	
	dynamicThreshold.alertCondition.RAID_VOLUME_RAIDLDEV_RESPONSETIME.numberInPeriod.number	Specify the number of times that a spike exceeds a threshold to issue an event of the Hitachi Storage Total Response Time (LDEV) metric during the threshold monitoring period.	1 to the number of samples during the period	1	Hitachi Storage Total Response Time (LDEV)
	dynamicThreshold.alertCondition.RAID_VOLUME_RAIDLDEV_RESPONSETIME.numberInPeriod.period	Specify the threshold monitoring period (in minutes) for the Hitachi Storage Total Response Time (LDEV) metric.	0 < period <= 60	5	

Category	Key name	Setting	Specifiable values	Default value	Corresponding Analyzer metric
	dynamicThreshold.alertCondition.ESX_VM_VM_CPUREADY.numberInPeriod.number	Specify the number of times that a spike exceeds a threshold to issue an event of the VMware CPU Ready (VMware virtual Machine) metric during the threshold monitoring period.	1 to the number of samples during the period	1	VMware CPU Ready (VMware virtual Machine)
	dynamicThreshold.alertCondition.ESX_VM_VM_CPUREADY.numberInPeriod.period	Specify the threshold monitoring period (in minutes) for the VMware CPU Ready (VMware virtual Machine) metric.	0 < period <= 60	5	
	dynamicThreshold.alertCondition.ESX_VM_VDISK_VIRTUALDISKTOTALREADLATENCY.numberInPeriod.number	Specify the number of times that a spike exceeds a threshold to issue an event of the VMware Virtual Disk Total Read Latency (Virtual Disk) metric during the threshold monitoring period.	1 to the number of samples during the period	1	VMware Virtual Disk Total Read Latency (Virtual Disk)
	dynamicThreshold.alertCondition.ESX_VM_VDISK_VIRTUALDISKTOTALREADLATENCY.numberInPeriod.period	Specify the threshold monitoring period (in minutes) for the VMware Virtual Disk Total Read Latency (Virtual Disk) metric.	0 < period <= 60	5	

Category	Key name	Setting	Specifiable values	Default value	Corresponding Analyzer metric
	dynamicThreshold.alertCondition.ESX_VM_VDISK_VIRTUALDISKTOTALWRITELATENCY.numberInPeriod.number	Specify the number of times that a spike exceeds a threshold to issue an event of the VMware Virtual Disk Total Write Latency (Virtual Disk) metric during the threshold monitoring period.	1 to the number of samples during the period	1	VMware Virtual Disk Total Write Latency (Virtual Disk)
	dynamicThreshold.alertCondition.ESX_VM_VDISK_VIRTUALDISKTOTALWRITELATENCY.numberInPeriod.period	Specify the threshold monitoring period (in minutes) for the VMware Virtual Disk Total Write Latency (Virtual Disk) metric.	0 < period <= 60	5	
	dynamicThreshold.alertCondition.ESX_VM_VM_NETDROPPEDRX.numberInPeriod.number	Specify the number of times that a spike exceeds a threshold to issue an event of the VMware Dropped Rx (VMware Virtual Machine) metric during the threshold monitoring period.	1 to the number of samples during the period	1	VMware Dropped Rx (VMware Virtual Machine)
	dynamicThreshold.alertCondition.ESX_VM_VM_NETDROPPEDRX.numberInPeriod.period	Specify the threshold monitoring period (in minutes) for the VMware Dropped Rx (VMware Virtual Machine) metric.	0 < period <= 60	5	

Category	Key name	Setting	Specifiable values	Default value	Corresponding Analyzer metric
	dynamicThreshold.alertCondition.ESX_VM_VM_NETDROPPEDTX.numberInPeriod.number	Specify the number of times that a spike exceeds a threshold to issue an event of the VMware Dropped Tx (VMware Virtual Machine) metric during the threshold monitoring period.	1 to the number of samples during the period	1	VMware Dropped Tx (VMware Virtual Machine)
	dynamicThreshold.alertCondition.ESX_VM_VM_NETDROPPEDTX.numberInPeriod.period	Specify the threshold monitoring period (in minutes) for the VMware Dropped Tx (VMware Virtual Machine) metric.	0 < period <= 60	5	
	dynamicThreshold.alertCondition.LINUX_LHOST_L_MEMUSED.numberInPeriod.number	Specify the number of times that a spike exceeds a threshold to issue an event of the Linux Memory Used % (Linux Host) metric during the threshold monitoring period.	1 to the number of samples during the period	1	Linux Memory Used % (Linux Host)
	dynamicThreshold.alertCondition.LINUX_LHOST_L_MEMUSED.numberInPeriod.period	Specify the threshold monitoring period (in minutes) for the Linux Memory Used % (Linux Host) metric.	0 < period <= 60	5	

Category	Key name	Setting	Specifiable values	Default value	Corresponding Analyzer metric
	dynamicThreshold.alertCondition.LINUX_LHOST_L_FREE.numberInPeriod.number	Specify the number of times that a spike exceeds a threshold to issue an event of the Linux Available KB (Linux Host) metric during the threshold monitoring period.	1 to the number of samples during the period	1	Linux Available KB (Linux Host)
	dynamicThreshold.alertCondition.LINUX_LHOST_L_FREE.numberInPeriod.period	Specify the threshold monitoring period (in minutes) for the Linux Available KB (Linux Host) metric.	0 < period <= 60	5	
	dynamicThreshold.alertCondition.LINUX_LHOST_L_CPULOAD.numberInPeriod.number	Specify the number of times that a spike exceeds a threshold to issue an event of the Linux Processor Time % (Linux Host) metric during the threshold monitoring period.	1 to the number of samples during the period	1	Linux Processor Time % (Linux Host)
	dynamicThreshold.alertCondition.LINUX_LHOST_L_CPULOAD.numberInPeriod.period	Specify the threshold monitoring period (in minutes) for the Linux Processor Time % (Linux Host) metric.	0 < period <= 60	5	

Category	Key name	Setting	Specifiable values	Default value	Corresponding Analyzer metric
	dynamicThreshold.alertCondition.LINUX_LHOSTCPU_L_IDLE.numberInPeriod.number	Specify the number of times that a spike exceeds a threshold to issue an event of the Linux Processor Time Idle % (Linux Host CPU) metric during the threshold monitoring period.	1 to the number of samples during the period	1	Linux Processor Time Idle % (Linux Host CPU)
	dynamicThreshold.alertCondition.LINUX_LHOSTCPU_L_IDLE.numberInPeriod.period	Specify the threshold monitoring period (in minutes) for the Linux Processor Time Idle % (Linux Host CPU) metric.	0 < period <= 60	5	
	dynamicThreshold.alertCondition.WINDOWS_WHOST_PERCENTCOMMITTEDBYTESINUSE.numberInPeriod.number	Specify the number of times that a spike exceeds a threshold to issue an event of the Windows Committed Bytes In Use % (Windows Host) metric during the threshold monitoring period.	1 to the number of samples during the period	1	Windows Committed Bytes In Use % (Windows Host)
	dynamicThreshold.alertCondition.WINDOWS_WHOST_PERCENTCOMMITTEDBYTESINUSE.numberInPeriod.period	Specify the threshold monitoring period (in minutes) for the Windows Committed Bytes In Use % (Windows Host) metric.	0 < period <= 60	5	

Category	Key name	Setting	Specifiable values	Default value	Corresponding Analyzer metric
	dynamicThreshold.alertCondition.WINDOWS_WHOST_AVAILABLEMBYTES.numberInPeriod.number	Specify the number of times that a spike exceeds a threshold to issue an event of the Windows Available MB (Windows Host) metric during the threshold monitoring period.	1 to the number of samples during the period	1	Windows Available MB (Windows Host)
	dynamicThreshold.alertCondition.WINDOWS_WHOST_AVAILABLEMBYTES.numberInPeriod.period	Specify the threshold monitoring period (in minutes) for the Windows Available MB (Windows Host) metric.	0 < period <= 60	5	
	dynamicThreshold.alertCondition.WINDOWS_WHOST_PERCENTPROCESSORTIME.numberInPeriod.number	Specify the number of times that a spike exceeds a threshold to issue an event of the Windows Processor Time % (Windows Host) metric during the threshold monitoring period.	1 to the number of samples during the period	1	Windows Processor Time % (Windows Host)
	dynamicThreshold.alertCondition.WINDOWS_WHOST_PERCENTPROCESSORTIME.numberInPeriod.period	Specify the threshold monitoring period (in minutes) for the Windows Processor Time % (Windows Host) metric.	0 < period <= 60	5	

Category	Key name	Setting	Specifiable values	Default value	Corresponding Analyzer metric
	dynamicThreshold.alertCondition.WINDOWS_WPROCESSOR_PERCENTPROCESSORTIME.numberInPeriod.number	Specify the number of times that a spike exceeds a threshold to issue an event of the Windows Processor Time % (Windows Processor) metric during the threshold monitoring period.	1 to the number of samples during the period	1	Windows Processor Time % (Windows Processor)
	dynamicThreshold.alertCondition.WINDOWS_WPROCESSOR_PERCENTPROCESSORTIME.numberInPeriod.period	Specify the threshold monitoring period (in minutes) for the Windows Processor Time % (Windows Processor) metric.	0 < period <= 60	5	
	dynamicThreshold.alertCondition.VSSB_VOLUME_VSSBVOLUME_READIOPS.numberInPeriod.number	Specify the number of times that a spike exceeds a threshold to issue an event of the Virtual Storage Software Block Read IOPS (VSSB Volume) metric during the threshold monitoring period.	1 to the number of samples during the period	1	Virtual Storage Software Block Read IOPS (VSSB Volume)

Category	Key name	Setting	Specifiable values	Default value	Corresponding Analyzer metric
	dynamicThreshold.alertCondition.VSSB_VOLUME_VSSBVOLUME_READIOPS.numberInPeriod.period	Specify the threshold monitoring period (in minutes) for the Virtual Storage Software Block Read IOPS (VSSB Volume) metric.	0 < period <= 60 and a multiple of the data collection interval	5	
	dynamicThreshold.alertCondition.VSSB_VOLUME_VSSBVOLUME_READRESPONSETIME.numberInPeriod.number	Specify the number of times that a spike exceeds a threshold to issue an event of the Virtual Storage Software Block Read Response Time (VSSB Volume) metric during the threshold monitoring period.	1 to the number of samples during the period	1	Virtual Storage Software Block Read Response Time (VSSB Volume)
	dynamicThreshold.alertCondition.VSSB_VOLUME_VSSBVOLUME_READRESPONSETIME.numberInPeriod.period	Specify the threshold monitoring period (in minutes) for the Virtual Storage Software Block Read Response Time (VSSB Volume) metric.	0 < period <= 60	5	

Category	Key name	Setting	Specifiable values	Default value	Corresponding Analyzer metric
	dynamicThreshold.alertCondition.VSSB_VOLUME_VSSBVOLUME_READTRANSFERRATEINMIB.numberInPeriod.number	Specify the number of times that a spike exceeds a threshold to issue an event of the Virtual Storage Software Block Read Transfer Rate (VSSB Volume) metric during the threshold monitoring period.	1 to the number of samples during the period	1	Virtual Storage Software Block Read Transfer Rate(VSSB Volume)
	dynamicThreshold.alertCondition.VSSB_VOLUME_VSSBVOLUME_READTRANSFERRATEINMIB.numberInPeriod.period	Specify the threshold monitoring period (in minutes) for the Virtual Storage Software Block Read Transfer Rate (VSSB Volume) metric.	0 < period <= 60	5	
	dynamicThreshold.alertCondition.VSSB_VOLUME_VSSBVOLUME_WRITEIOPS.numberInPeriod.number	Specify the number of times that a spike exceeds a threshold to issue an event of the Virtual Storage Software Block Write IOPS (VSSB Volume) metric during the threshold monitoring period.	1 to the number of samples during the period	1	Virtual Storage Software Block Write IOPS (VSSB Volume)

Category	Key name	Setting	Specifiable values	Default value	Corresponding Analyzer metric
	dynamicThreshold.alertCondition.VSSB_VOLUME_VSSBVOLUME_WRITEIOPS.numberInPeriod.period	Specify the threshold monitoring period (in minutes) for the Virtual Storage Software Block Write IOPS (VSSB Volume) metric.	0 < period <= 60	5	
	dynamicThreshold.alertCondition.VSSB_VOLUME_VSSBVOLUME_WRITERESPONSETIME.numberInPeriod.number	Specify the number of times that a spike exceeds a threshold to issue an event of the Virtual Storage Software Block Write Response Time (VSSB Volume) metric during the threshold monitoring period.	1 to the number of samples during the period	1	Virtual Storage Software Block Write Response Time (VSSB Volume)
	dynamicThreshold.alertCondition.VSSB_VOLUME_VSSBVOLUME_WRITERESPONSETIME.numberInPeriod.period	Specify the threshold monitoring period (in minutes) for the Virtual Storage Software Block Write Response Time (VSSB Volume) metric.	0 < period <= 60	5	

Category	Key name	Setting	Specifiable values	Default value	Corresponding Analyzer metric
	`dynamicThreshold.alertCondition.VSSB_VOLUME_VSSBVOLUME_WRITETRANSFERRATEINMIB.numberInPeriod.number`	Specify the number of times that a spike exceeds a threshold to issue an event of the Virtual Storage Software Block Write Transfer Rate (VSSB Volume) metric during the threshold monitoring period.	1 to the number of samples during the period	`1`	`Virtual Storage Software Block Write Transfer Rate (VSSB Volume)`
	`dynamicThreshold.alertCondition.VSSB_VOLUME_VSSBVOLUME_WRITETRANSFERRATEINMIB.numberInPeriod.period`	Specify the threshold monitoring period (in minutes) for the Virtual Storage Software Block Write Transfer Rate (VSSB Volume) metric.	0 < period <= 60	`5`	
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 **Web Service Connections** window of Ops Center Automator.	A value from 1 to 32 characters, using only single-byte alphanumeric characters, underscores (_), periods (.), and hyphens (-)	`Analytics`	--

Category	Key name	Setting	Specifiable values	Default value	Corresponding Analyzer metric
	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	--
	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	--

Category	Key name	Setting	Specifiable values	Default value	Corresponding Analyzer metric
	`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`	--
System monitoring of the Analyzer server	`fileSystemCheck.alert.usable.threshold.warn`	Specify the threshold used to issue a Warning event when the Usable Ratio of the free space falls below this value (%).	1 to 99	`30`	--
	`fileSystemCheck.alert.usable.threshold.critical`	Specify the threshold used to issue a Critical event when the Usable Ratio of the free space falls below this value (%).	1 to 99	`15`	
Event	`event.maxcount`	Specify the maximum number of events.	1 to 1,000,000	`1000000`	--
	`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
dynamicThreshold.alertCondition.RAID_VOLUME_RAIDLDEV_TRANSFERRATE.numberInPeriod.numbe
r = 2
dynamicThreshold.alertCondition.RAID_VOLUME_RAIDLDEV_TRANSFERRATE.numberInPeriod.perio
d = 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 C: 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
An action defined in the command definition file	Success of an action defined in the command definition file	6	KNAQ38058-I
	Failure of an action defined in the command definition file	3	KNAQ38059-E
	Success of an action defined in the command definition file	6	KNAQ38062-I
	Failure of an action 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
	Failed to connect to Ops Center Automator	3	KNAQ38073-E
An event action	Success of an event action	6	KNAQ38078-I
	Failure of an event action	3	KNAQ38079-E

Type description	Audit event	Severity	Message ID
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 nonexisting 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
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	KAPM07237-E KAPM07238-E 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[1]	6	KAPM07235-I
	Failed account lock	3	KAPM07240-E
Account lock release	Successful account lock release[2]	6	KAPM07236-I
	Failed account lock release	3	KAPM07240-E
	Successful account lock release using the `hcmds64unlockaccount` command	6	KAPM07236-I

Type description	Audit event	Severity	Message ID
	Failed account lock release using the `hcmds64unlockaccount` 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
User information update (GUI and CLI)	Successful update of user information	6	KAPM07243-I
	Failed to update user information	3	KAPM07244-E
User deletion (GUI and CLI)	Successful deletion of user	6	KAPM07245-I
	Failed to delete user	3	KAPM07246-E
Authorization group registration (GUI and CLI)	Successful registration of an authorization group	6	KAPM07251-I
	Failed registration of an authorization group	3	KAPM07252-E

Type description	Audit event	Severity	Message ID
Authorization group deletion (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 (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 `hcmds64backups` command or the `hcmds64db` command	6	KAPM05561-I
	Failed backup using the `hcmds64backups` command or the `hcmds64db` command	3	KAPM05562-E
	Successful full restore using the `hcmds64db` command	6	KAPM05563-I
	Failed full restore using the `hcmds64db` command	3	KAPM05564-E
	Successful partial restore using the `hcmds64db` command	6	KAPM05565-I
	Failed partial restore using the `hcmds64db` command	3	KAPM05566-E
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

Type description	Audit event	Severity	Message ID
Authentication data input/ output	Successful data output using the `hcmds64authmove` command	6	KAPM05832-I
	Failed data output using the `hcmds64authmove` command	3	KAPM05833-E
	Successful data input using the `hcmds64authmove` command	6	KAPM05834-I
	Failed data input using the `hcmds64authmove` 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
	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

Type description	Audit event	Severity	Message ID
	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
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

Type description	Audit event	Severity	Message ID
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
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

Type description	Audit event	Severity	Message ID
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
	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

Type description	Audit event	Severity	Message ID
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
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

Type description	Audit event	Severity	Message ID
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

Notes:

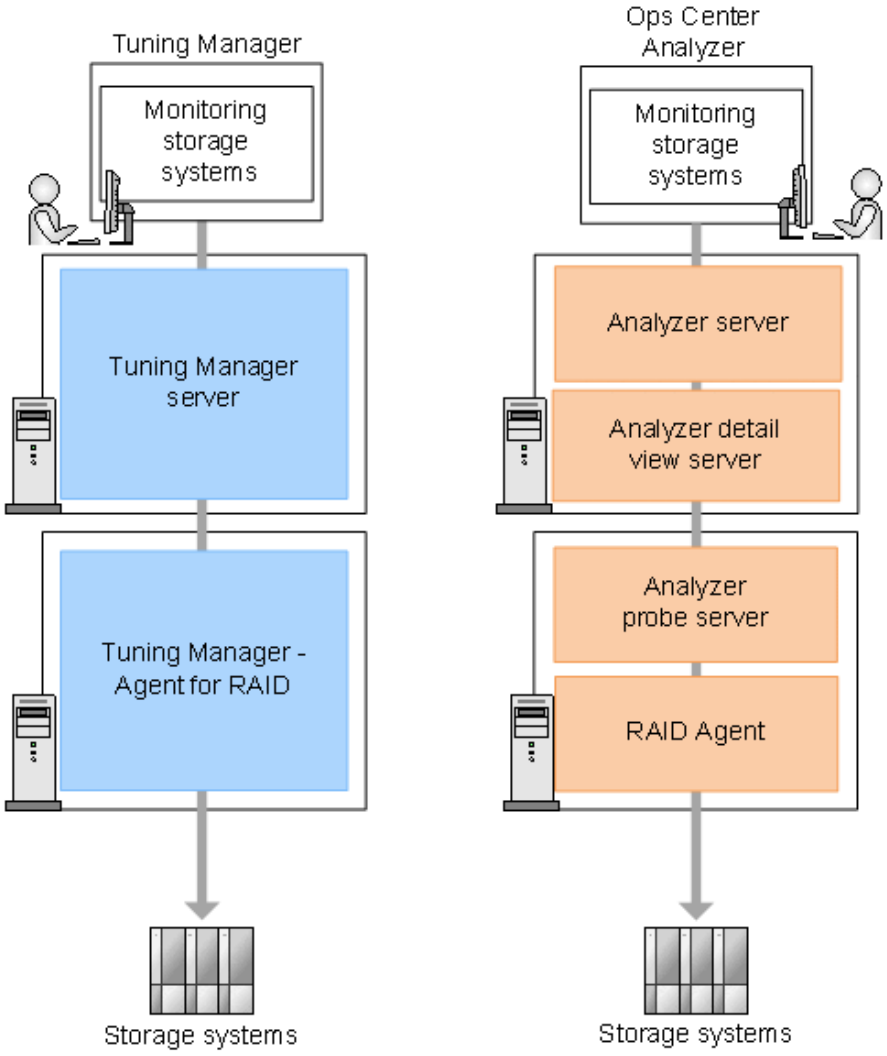
1. If an account is locked because the authentication method was changed for a user whose password is not set, this information is not recorded in the audit log.
2. If an account is unlocked because a password was set for a user, this information is not recorded in the audit log.

Appendix D: Migrating Tuning Manager to Ops Center Analyzer

This chapter explains how to migrate Tuning Manager to Ops Center Analyzer.

Server architecture

Ops Center Analyzer requires at least two servers. The first is for the Analyzer server and Analyzer detail view servers that replace the Tuning Manager server. The second server is for Analyzer probe server and RAID Agent which replace Tuning Manager - Agent for RAID.



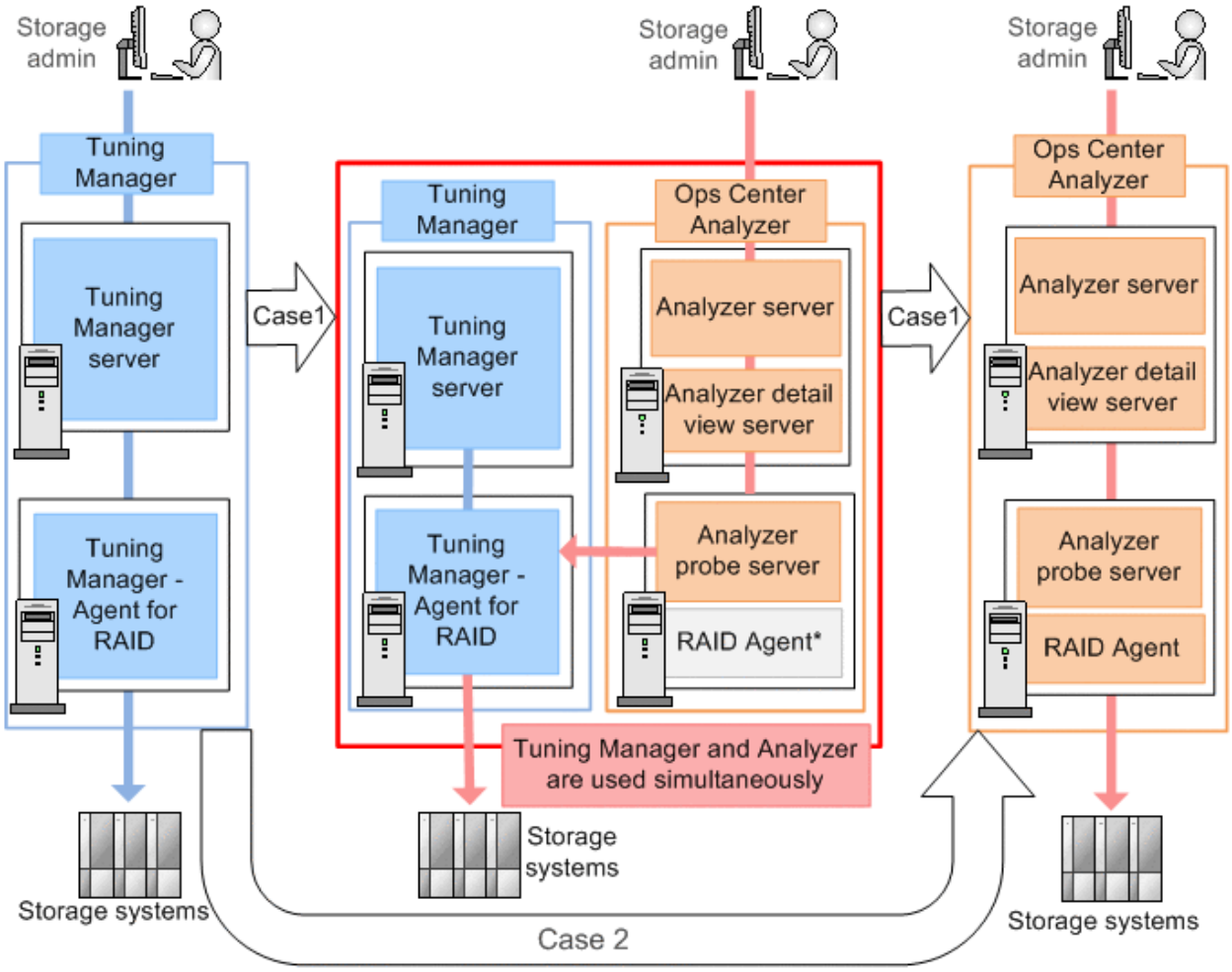
Migration overview

There are two options for performing the migration to Ops Center Analyzer:

Case 1: The move is performed in stages. Tuning Manager and Ops Center Analyzer are used simultaneously for a temporary period, and the complete move to Ops Center Analyzer is made after operations have been evaluated.

Case 2: The move is performed in a single operation. This case applies to customers who have already evaluated Ops Center Analyzer.

In the middle stage (the red box), Ops Center Analyzer collects information from the storage systems using Tuning Manager - Agent for RAID rather than RAID Agent.

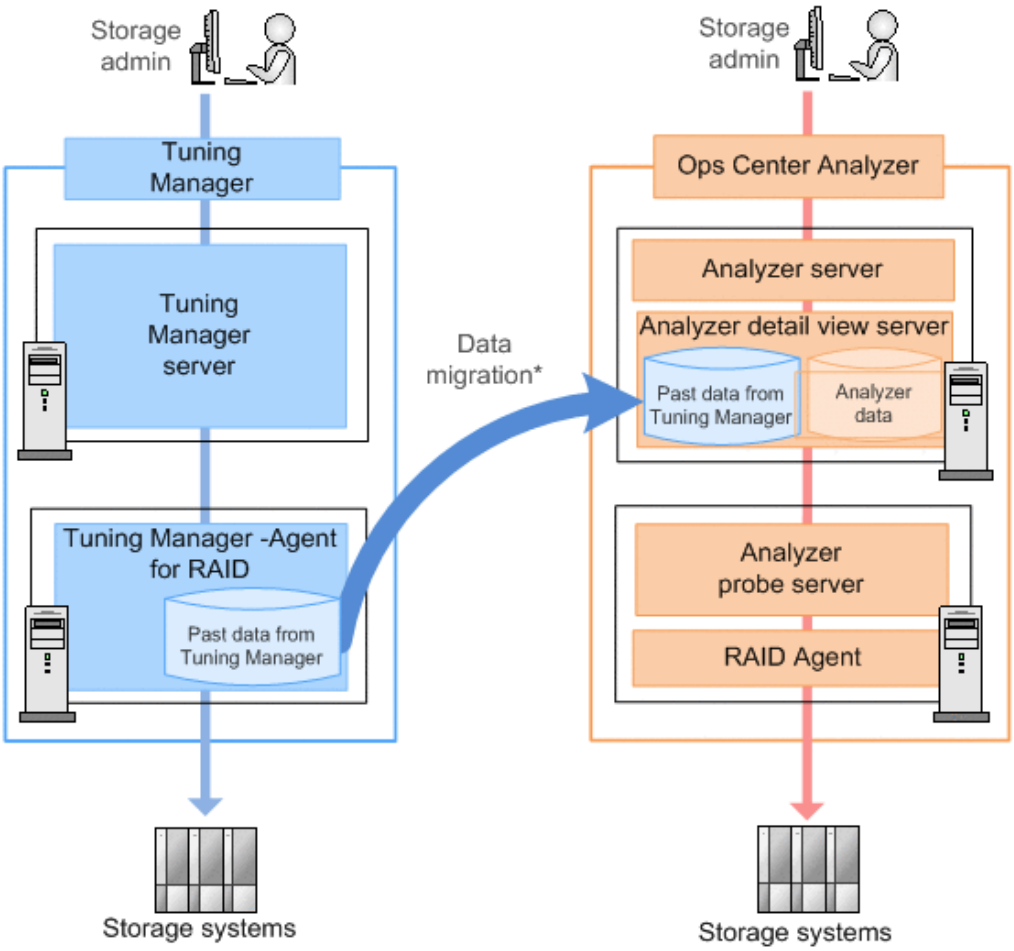


Case 1: Moving in stages
Case 2: Complete move (all at once)
* : If Tuning Manager and Analyzer are to be used simultaneously, use Tuning Manager - Agent for RAID instead of RAID Agent.

Tuning Manager data migration

Ops Center Analyzer supports the migration of data that was created by Tuning Manager:

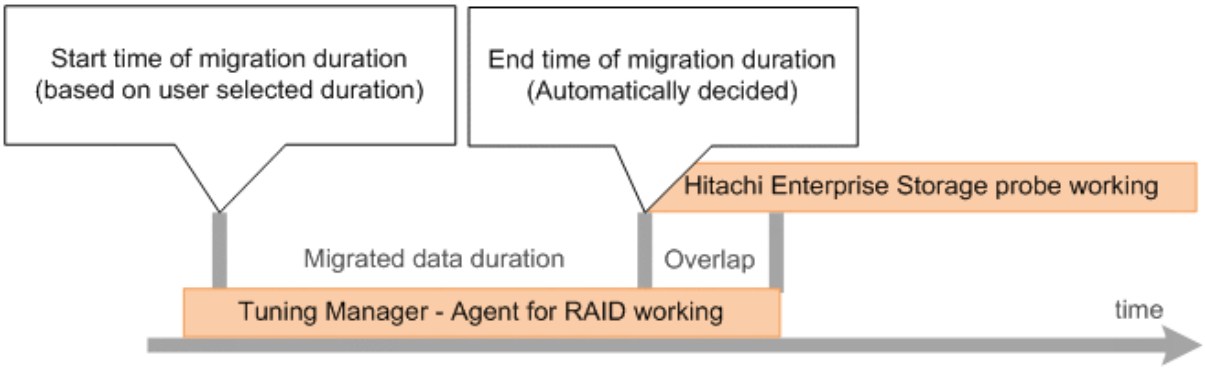
- You can back up the historical monitoring data from Tuning Manager to Ops Center Analyzer.
- You can use the REST API to access the historical data.



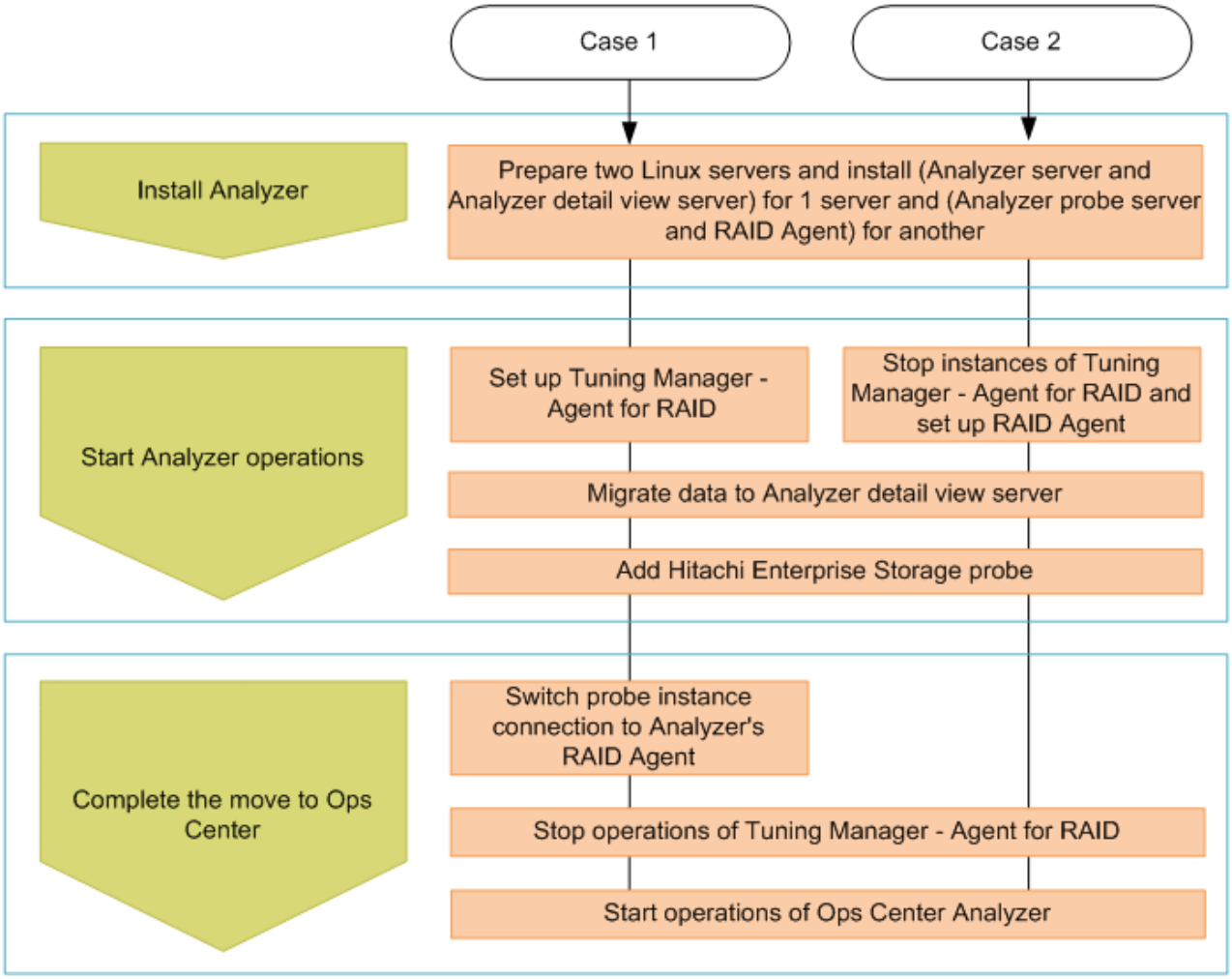
* : You can migrate historical data that was acquired hourly or on a less frequent basis.

About the migration process

- The duration of the migration process depends on the number of volumes and the amount of data (the interval over which data was collected).
- If Tuning Manager - Agent for RAID and Hitachi Enterprise Storage probe overlap collection times, the end time of migration duration will be adjusted to avoid the overlap.

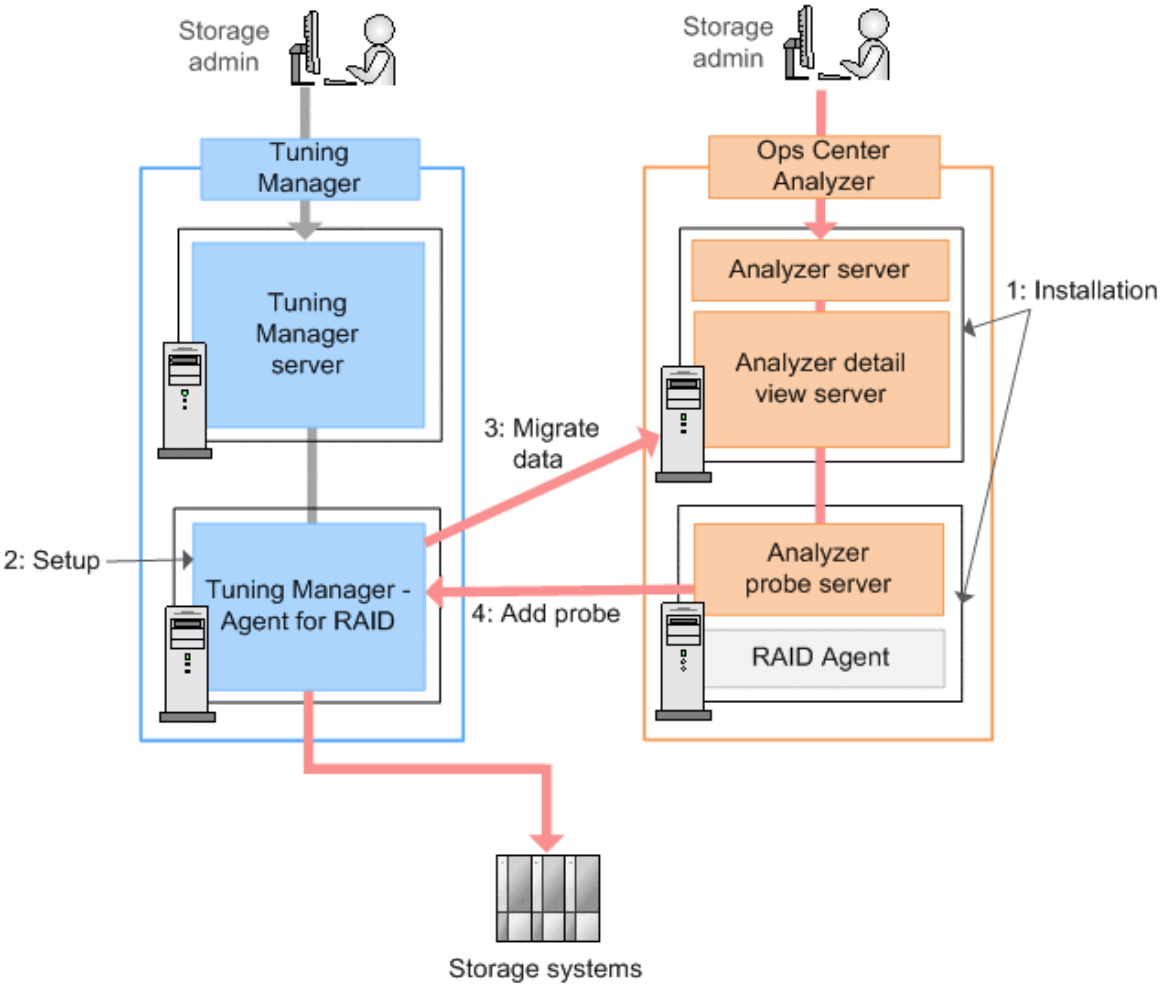


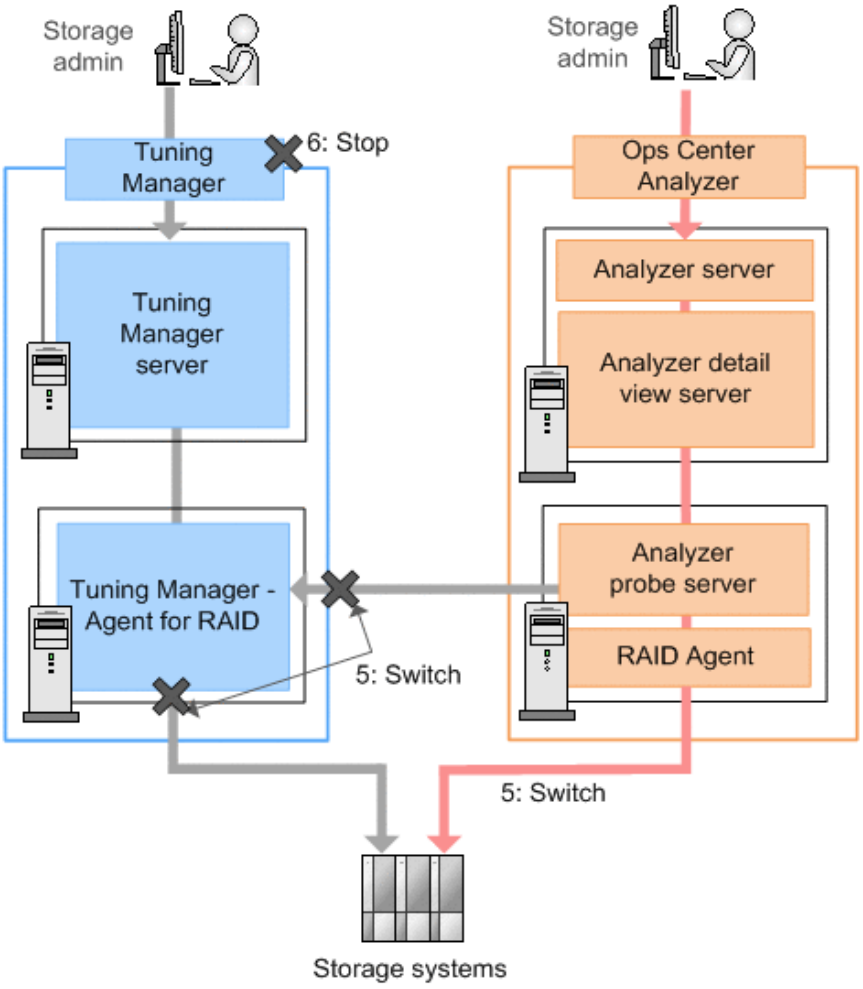
Workflow for Migrating



Case 1: Staged move (Tuning Manager and Ops Center Analyzer used)

The following figure shows the flow of tasks for migration.


Storage admin
Storage admin
Tuning Manager
Tuning Manager server
Tuning Manager - Agent for RAID
Ops Center Analyzer
Analyzer server
Analyzer detail view server
Analyzer probe server
RAID Agent
1: Installation
2: Setup
3: Migrate data
4: Add probe
Storage systems



Installing the Ops Center Analyzer

Perform the following procedures to install the Analyzer server, Analyzer detail view server, and Analyzer probe server:

- Installing Ops Center Analyzer and Analyzer detail view servers (VMware vSphere Client) (on page 65)
- Running the setup tool (opsvmsetup) (on page 65)
- Installing the Analyzer probe server and Protector Client (VMware vSphere Client) (on page 67)
- Initial setup of the guest OS or VMs (on page 69)

You can also install the Analyzer server and Analyzer detail view server using the Ops Center consolidated OVA.

You cannot install the Analyzer probe server on the same host as Tuning Manager - Agent for RAID.

Starting Ops Center Analyzer operations (simultaneous operations with Tuning Manager - Agent for RAID to RAID Agent used)

Perform the following tasks in order:

1. Setting up Tuning Manager - Agent for RAID (on page 194)
2. Migrating Hitachi Tuning Manager historical data (on page 201)
3. Adding Hitachi Enterprise Storage probe (on page 209)

Completing the move to Ops Center

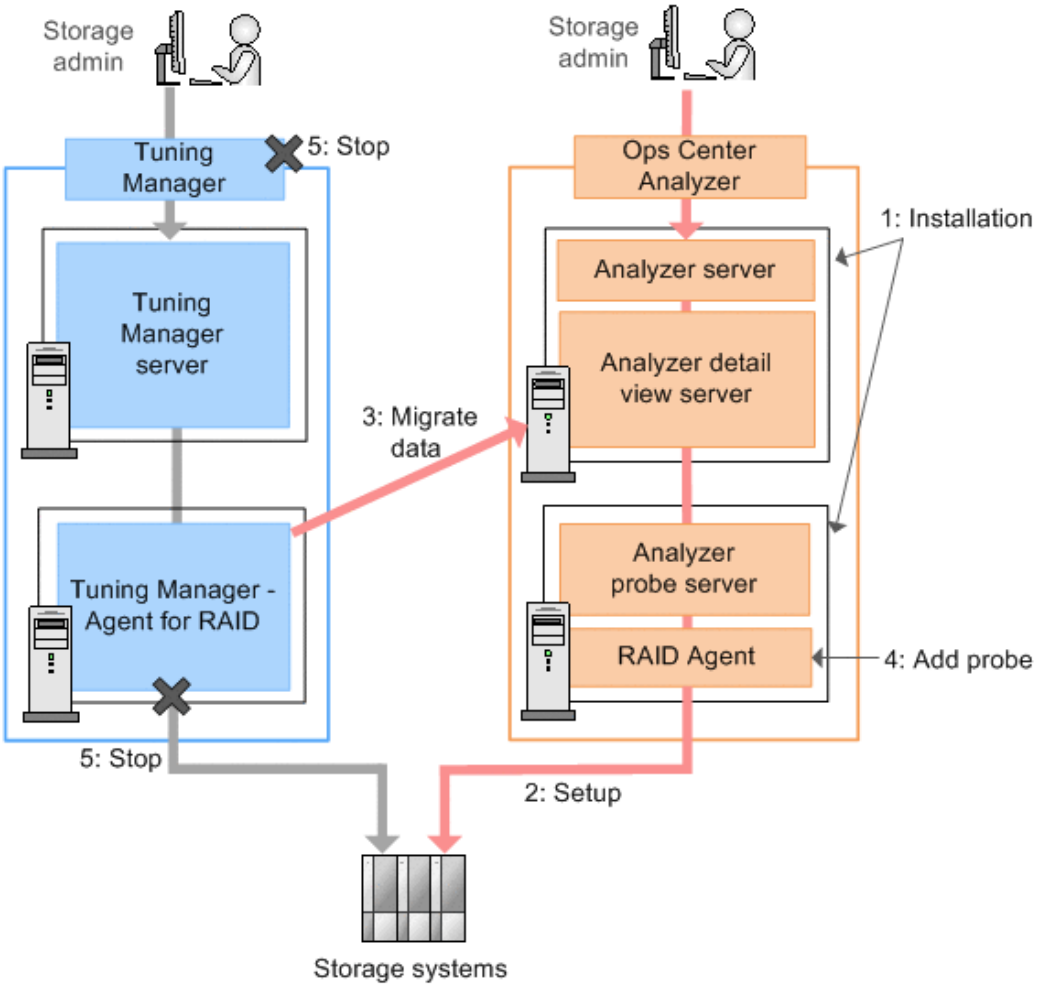
Cease using Tuning Manager when the procedures are complete.

Perform the following tasks in order:

1. Perform the procedure for Switching from Tuning Manager - Agent for RAID to RAID Agent (on page 204).
2. Stop operations of Tuning Manager.
   a. After stopping Tuning Manager, do not start an instance of Tuning Manager - Agent for RAID. To prevent Tuning Manager - Agent for RAID from starting automatically, see the descriptions of manually starting services in the *Hitachi Command Suite Tuning Manager Agent Administration Guide*, and clear the setting.
   b. Uninstall Tuning Manager - Agent for RAID. For details, see the *Hitachi Command Suite Tuning Manager Installation Guide*.
3. Start operations of Ops Center Analyzer.

Case 2: Straight move to Ops Center Analyzer

The following figure shows the flow of tasks for migration.



Installing the Ops Center Analyzer

Perform the following procedures to install the Analyzer server, Analyzer detail view server, and Analyzer probe server:

- Installing Ops Center Analyzer and Analyzer detail view servers (VMware vSphere Client) (on page 65)
- Running the setup tool (opsvmsetup) (on page 65)
- Installing the Analyzer probe server and Protector Client (VMware vSphere Client) (on page 67)
- Initial setup of the guest OS or VMs (on page 69)

You can also install the Analyzer server and Analyzer detail view server using the Ops Center consolidated OVA.

You cannot install the Analyzer probe server on the same host as Tuning Manager - Agent for RAID.

Starting Ops Center Analyzer operations (setup Analyzer probe server and RAID Agent)

Perform the following tasks in order:

1. Stopping instances of Tuning Manager - Agent for RAID and setting up RAID Agent (on page 707)
2. Migrating Hitachi Tuning Manager historical data (on page 201)
3. Adding Hitachi Enterprise Storage probe (on page 209)

Stopping instances of Tuning Manager - Agent for RAID and setting up RAID Agent

Change the agent monitoring a storage system from Tuning Manager - Agent for RAID to RAID Agent that was provided 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 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
   ```

3. Set up RAID Agent.
   a. Determine `Access Type`. (For details, see Selecting the data collection method (on page 154).)
   b. Set up RAID Agent. (For details, see Workflow for setting up the Hitachi Enterprise Storage probe (when using RAID Agent) (on page 158) 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.

4. 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 475).

Completing the move to Ops Center

Cease using Tuning Manager when the procedures are complete.

Perform the following tasks in order:

1. Stop operations of Tuning Manager.

a. After stopping Tuning Manager, do not start an instance of Tuning Manager - Agent for RAID. To prevent Tuning Manager - Agent for RAID from starting automatically, see the descriptions of manually starting services in the *Hitachi Command Suite Tuning Manager Agent Administration Guide*, and clear the setting.

b. Uninstall Tuning Manager - Agent for RAID. For details, see the *Hitachi Command Suite Tuning Manager Installation Guide*.

2. Start operations of Ops Center Analyzer.

Notices

This product includes software developed by the Apache Software Foundation (http://www.apache.org/).

Portions of this software were developed at the National Center for Supercomputing Applications (NCSA) at the University of Illinois at Urbana-Champaign.

This product includes software developed by the University of California, Berkeley and its contributors.

This software contains code derived from the RSA Data Security Inc. MD5 Message-Digest Algorithm, including various modifications by Spyglass Inc., Carnegie Mellon University, and Bell Communications Research, Inc (Bellcore).

Regular expression support is provided by the PCRE library package, which is open source software, written by Philip Hazel, and copyright by the University of Cambridge, England. The original software is available from ftp://ftp.csx.cam.ac.uk/pub/software/programming/pcre/

1. This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)

2. This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)

3. This product includes software written by Tim Hudson (tjh@cryptsoft.com)

4. This product includes the OpenSSL Toolkit software used under OpenSSL License and Original SSLeay License. OpenSSL License and Original SSLeay License are as follow:

LICENSE ISSUES

==========

The OpenSSL toolkit stays under a double license, i.e. both the conditions of

the OpenSSL License and the original SSLeay license apply to the toolkit.

See below for the actual license texts.

OpenSSL License

/* ==========

* Copyright (c) 1998-2019 The OpenSSL Project. All rights reserved.

*

* Redistribution and use in source and binary forms, with or without

* modification, are permitted provided that the following conditions

* are met:

*

* 1. Redistributions of source code must retain the above copyright

* notice, this list of conditions and the following disclaimer.

*

* 2. Redistributions in binary form must reproduce the above copyright

* notice, this list of conditions and the following disclaimer in

* the documentation and/or other materials provided with the

* distribution.

*

* 3. All advertising materials mentioning features or use of this

* software must display the following acknowledgment:

* "This product includes software developed by the OpenSSL Project

* for use in the OpenSSL Toolkit. (http://www.openssl.org/)"

*

* 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to

* endorse or promote products derived from this software without

* prior written permission. For written permission, please contact

* openssl-core@openssl.org.

*

* 5. Products derived from this software may not be called "OpenSSL"

* nor may "OpenSSL" appear in their names without prior written
* permission of the OpenSSL Project.
*
* 6. Redistributions of any form whatsoever must retain the following
* acknowledgment:
* "This product includes software developed by the OpenSSL Project
* for use in the OpenSSL Toolkit (http://www.openssl.org/)"
*
* THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY
* EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
* PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR
* ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
* SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
* NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
* LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
* STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
* ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
* OF THE POSSIBILITY OF SUCH DAMAGE.
* ==
*
* This product includes cryptographic software written by Eric Young
* (eay@cryptsoft.com). This product includes software written by Tim
* Hudson (tjh@cryptsoft.com).
*
*/

Original SSLeay License

/* Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)
* All rights reserved.
*
* This package is an SSL implementation written
* by Eric Young (eay@cryptsoft.com).
* The implementation was written so as to conform with Netscapes SSL.
*
* This library is free for commercial and non-commercial use as long as
* the following conditions are aheared to. The following conditions
* apply to all code found in this distribution, be it the RC4, RSA,
* lhash, DES, etc., code; not just the SSL code. The SSL documentation
* included with this distribution is covered by the same copyright terms
* except that the holder is Tim Hudson (tjh@cryptsoft.com).
*
* Copyright remains Eric Young's, and as such any Copyright notices in
* the code are not to be removed.
* If this package is used in a product, Eric Young should be given attribution
* as the author of the parts of the library used.
* This can be in the form of a textual message at program startup or
* in documentation (online or textual) provided with the package.
*

Other company and product names mentioned in this document may be the trademarks of their respective owners.

Hitachi Vantara

Corporate Headquarters
2535 Augustine Drive
Santa Clara, CA 95054 USA
HitachiVantara.com | community.HitachiVantara.com

Contact Information
USA: 1-800-446-0744
Global: 1-858-547-4526
HitachiVantara.com/contact