Hitachi Ops Center

11.0.4

Installation and Configuration Guide

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

MK-99OPS001-24
April 2025

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

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

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

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

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

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

Contents

Preface

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

Product version

This document revision applies to Hitachi Ops Center version 11.0.4.

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 documentation website: https://docs.hitachivantara.com.

Accessing product documentation

Product user documentation is available on: https://docs.hitachivantara.com. Check this site for the most current documentation, including important updates that may have been made after the release of the product.

Getting help

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.feedback@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

The Hitachi Ops Center product enables you to optimize your data center operations through integrated configuration, analytics, automation, and copy data management. These features enable you to administer, automate, optimize, and protect your Hitachi storage infrastructure.

Hitachi Ops Center is a system consisting of multiple products. The following provides an overview of the Hitachi Ops Center product components and an overview of the system configuration.

Overview of the Hitachi Ops Center products

A Hitachi Ops Center system consists of the following software products:

Hitachi Ops Center Common Services

Hitachi Ops Center Common Services provides infrastructure functions common to Hitachi Ops Center that enable you to launch products, manage users, and enable single sign-on (SSO).

Hitachi Ops Center Automator

Hitachi Ops Center Automator provides the tools to automate and simplify end-to-end processes, such as storage provisioning, for storage and data center administrators. The building blocks of the product are prepackaged automation templates known as service templates.

Hitachi Ops Center Analyzer

Hitachi 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.

Hitachi Ops Center Analyzer collects the data to analyze from Hitachi Ops Center Analyzer detail view, which processes performance and configuration data received from probes that connect to monitoring targets.

Hitachi Ops Center Analyzer viewpoint

Hitachi Ops Center Analyzer viewpoint consolidates information from multiple instances of Hitachi Ops Center Analyzer and provides functions for monitoring a system that spans multiple data centers.

Hitachi Ops Center Administrator

Hitachi Ops Center Administrator is a unified software management tool that reduces the complexity of managing storage systems by simplifying the setup, management, and maintenance of storage resources.

Hitachi Ops Center Protector

Hitachi Ops Center Protector provides a modern, holistic approach to data protection, recovery, and retention.

Hitachi Ops Center API Configuration Manager

Hitachi Ops Center API Configuration Manager provides APIs for obtaining information from and performing operations on storage systems.

Overview of Hitachi Ops Center Common Services

Common Services is a component that provides single sign-on functionality and a portal site for Hitachi Ops Center products.

When you log in to the Hitachi Ops Center Portal, the portal shows a list of registered Hitachi Ops Center products. When you click a product-name link, the product UI opens. Because user authentication is centralized, you can access each product without additional logins.

The Hitachi Ops Center products that support the single sign-on functionality are as follows:

- Hitachi Ops Center Automator (version 10.0.1 or later)
- Hitachi Ops Center Analyzer

- Hitachi Ops Center Analyzer detail view (version 10.8.2 or later)
- Hitachi Ops Center Analyzer probe (version 10.8.2 or later)
- Hitachi Ops Center Analyzer viewpoint
- Hitachi Ops Center Administrator (version 10.1.0 or later)
- Hitachi Ops Center Protector (version 7.0 or later)

The single sign-on user information is managed by Common Services, so you can create, delete, and modify user accounts from the portal site.

> **Tip:** You can also use Hitachi Ops Center products without single sign-on. For the installation and setup procedures to use in this case, see the documentation for the specific Hitachi Ops Center products that you are using.

Linking with an Active Directory or LDAP server

By linking Common Services with an external Active Directory or LDAP server, you can consolidate actions related to authenticating Hitachi Ops Center users. You can link Common Services with an Active Directory or LDAP server from the Hitachi Ops Center Portal.

You can link Common Services with one of the following authentication servers:

- Active Directory server
- LDAP server that supports LDAPv3 and LDAPS

You can link Common Services with an Active Directory server or an LDAP server. You cannot link Common Services with both types of servers.

The following conditions apply when you link Common Services with an Active Directory server or LDAP server.

Active Directory server:

- You can link to a maximum of four Active Directory servers.
- Both LDAP(S) and Kerberos are supported as authentication protocols.
- When using Kerberos authentication, you can set only one realm.
- You can register Common Services users for objects that are located under the base DN and with an `objectclass` of `person`.
- To log in to the Hitachi Ops Center Portal, use the Active Directory `sAMAccountName` as the user name.
- You can specify groups under the base DN to import.
- If you link to multiple Active Directory servers, make sure that usernames and email addresses are not duplicated among servers.

LDAP server:

- You can set only one LDAP server.
- Only LDAP(S) is supported as an authentication protocol.

- You can import a maximum of 100 user accounts.

  To narrow down the users to import, you can filter the search conditions by using LDAP attributes.

- Synchronizing user groups between the LDAP server and Common Services is not supported.

> **Note:**
>
> - To use Analyzer viewpoint, you must specify an email address for the `mail` attribute.
> - A user who has the same user name or email address as a local user of Common Services cannot log in to the Hitachi Ops Center Portal.
>
>   Before setting up the linkage, you must delete the local user in the Hitachi Ops Center Portal or change the email address of the local user.
>
> - If the LDAP server certificate has expired, all users (including local users of Common Services) will be unable to log in to the Hitachi Ops Center Portal.
>
>   To avoid this, you must update the LDAP server certificate before it expires, and import the certificate into the Common Services truststore.

For details on how to set up a link with an Active Directory or LDAP server and details on users and user groups, see Configuring a link to an Active Directory or LDAP server (on page 107).

Linking with an identity provider

By linking Common Services with an external identity provider, you can use the identity provider to centrally authenticate Hitachi Ops Center users. You can also use the Multi Factor Authentication (MFA) functionality provided by the identity provider.

By linking with an identity provider, when a user logs in to the Hitachi Ops Center Portal, you can authenticate the user on the identity provider side. If the identity provider successfully authenticates the user, the user is imported as a local user of Common Services.

Common Services supports linking with AD FS (Active Directory Federation Services) or linking with an identity provider registered in Keycloak, which is incorporated in Common Services. The settings required for linking with an identity provider depend on the identity provider type. For details, see Configuring a link to an AD FS identity provider (on page 116) or Configuring a link to a non-AD FS identity provider (on page 136).

Note:

- You can link to either AD FS or a non-AD FS identity provider, but not both.
- You cannot link one Active Directory server to both a directory service and AD FS.
- Identity provider user accounts must have a unique username and email address. If an identity provider user account conflicts with a local user ID or email address, the identity provider user cannot log in. You must remove the local user from the Hitachi Ops Center Portal or change the email address before proceeding.

Installation methods for Hitachi Ops Center

You can use one of the following methods to install Hitachi Ops Center:

- Installation by using an OVA file

  Use this method when you want to easily install the products on a virtual machine.

  Deploy an OVA file on a VMware ESXi server, which creates a virtual machine on which the Hitachi Ops Center product is installed.

  For information about the OVA file provided by Hitachi Ops Center and about products that are installed on the virtual machine, see OVA files provided by Hitachi Ops Center (on page 17).

- Installation by using the Express installer

  Use this method when you want to install or upgrade multiple Hitachi Ops Center products at the same time. The Express installer includes the Server Express installer and the Client Express installer, each of which installs different products. You can select specific products to install.

  The Server Express installer installs the following products and registers them with Common Services:

  - Hitachi Ops Center Common Services
  - Hitachi Ops Center Administrator
  - Hitachi Ops Center API Configuration Manager
  - Hitachi Ops Center Protector
  - Hitachi Ops Center Automator
  - Hitachi Ops Center Analyzer
  - Hitachi Ops Center Analyzer detail view
  - Hitachi Ops Center Analyzer viewpoint

  You can use the Client Express installer to install the following products:

  - Hitachi Ops Center API Configuration Manager
  - Hitachi Ops Center Protector Client
  - Hitachi Ops Center Analyzer probe server

- Installation by using the individual installer

  Use this method when you want to install or upgrade Hitachi Ops Center products individually. Use the installation media for each product to perform installation.

For details on the installation method, see the following descriptions:

- Installing Hitachi Ops Center products by using the OVA file (on page 21)
- Installing or upgrading Hitachi Ops Center products by using the Express installer (on page 36)
- Installing or upgrading Hitachi Ops Center products by using the individual installer (on page 65)

OVA files provided by Hitachi Ops Center

Hitachi Ops Center provides the following OVA files.

OVA name	Installed product
Ops Center OVA	▪ Hitachi Ops Center Common Services ▪ Hitachi Ops Center Automator ▪ Hitachi Ops Center Analyzer* ▪ Hitachi Ops Center Analyzer detail view ▪ Hitachi Ops Center Administrator ▪ Hitachi Ops Center Protector (Master) ▪ Hitachi Ops Center API Configuration Manager
Analyzer OVA	▪ Hitachi Ops Center Analyzer ▪ Hitachi Ops Center Analyzer detail view
Analyzer probe OVA	▪ Hitachi Ops Center Analyzer probe ▪ Hitachi Ops Center Analyzer Virtual Storage Software Agent ▪ Hitachi Ops Center Protector (Client) ▪ Hitachi Ops Center API Configuration Manager
Analyzer viewpoint OVF	▪ Hitachi Ops Center Analyzer viewpoint ▪ Hitachi Ops Center Common Services
* If you are using Analyzer, Analyzer probe is required. Either deploy the Analyzer probe OVA, or install Analyzer probe on another machine.	

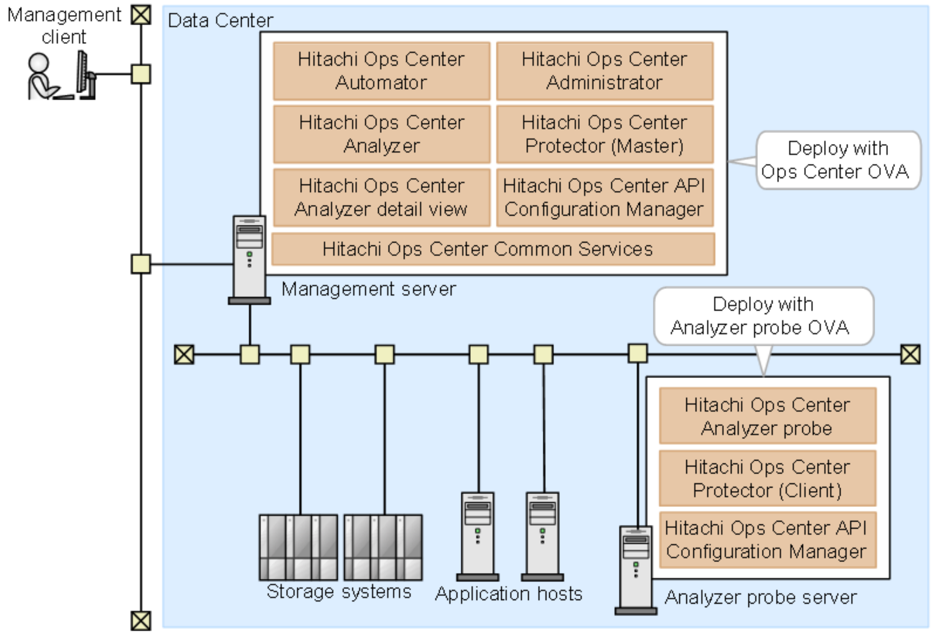
Hitachi Ops Center system configurations

A Hitachi Ops Center system consists of one or more management servers, depending on the software you are using and the scope of resources to manage. Common Services runs on one management server, and products register with Common Services so that they can use common infrastructure functions.

The following provides basic system configuration examples and the recommended installation method for each.

Example configuration running on one management server

The following shows an example system configuration in which Hitachi Ops Center product runs on one management server.

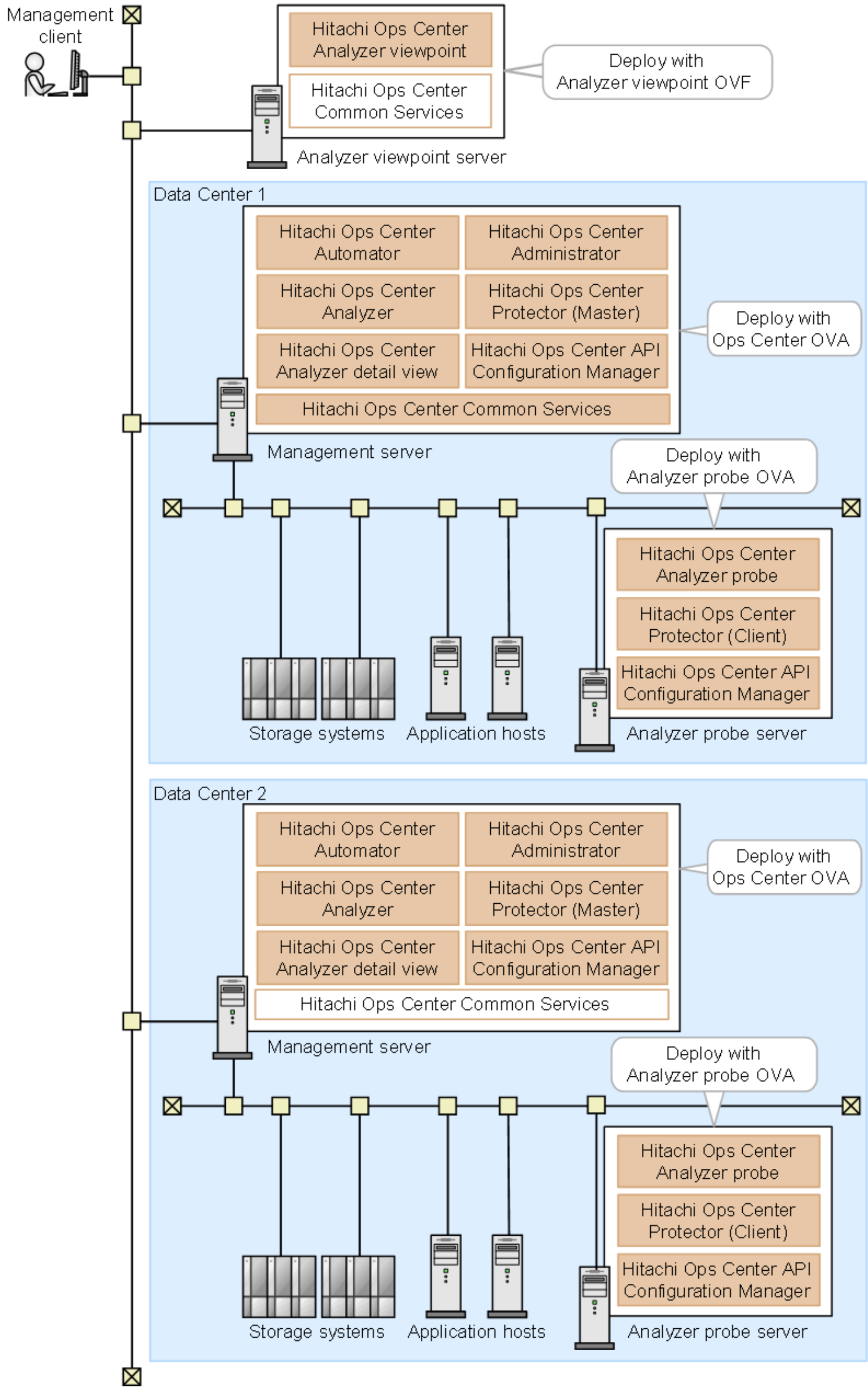

Management client
Data Center
Hitachi Ops Center Automator
Hitachi Ops Center Administrator
Hitachi Ops Center Analyzer
Hitachi Ops Center Protector (Master)
Hitachi Ops Center Analyzer detail view
Hitachi Ops Center API Configuration Manager
Hitachi Ops Center Common Services
Deploy with Ops Center OVA
Management server
Deploy with Analyzer probe OVA
Hitachi Ops Center Analyzer probe
Hitachi Ops Center Protector (Client)
Hitachi Ops Center API Configuration Manager
Storage systems
Application hosts
Analyzer probe server

When building a system with the OVA, it's easiest to use the Ops Center OVA to install the main products, and then add the Analyzer Probe OVA.

When using an individual installer, you use the installer specific to the product. If you want to use the single sign-on functionality, you must also install Common Services.

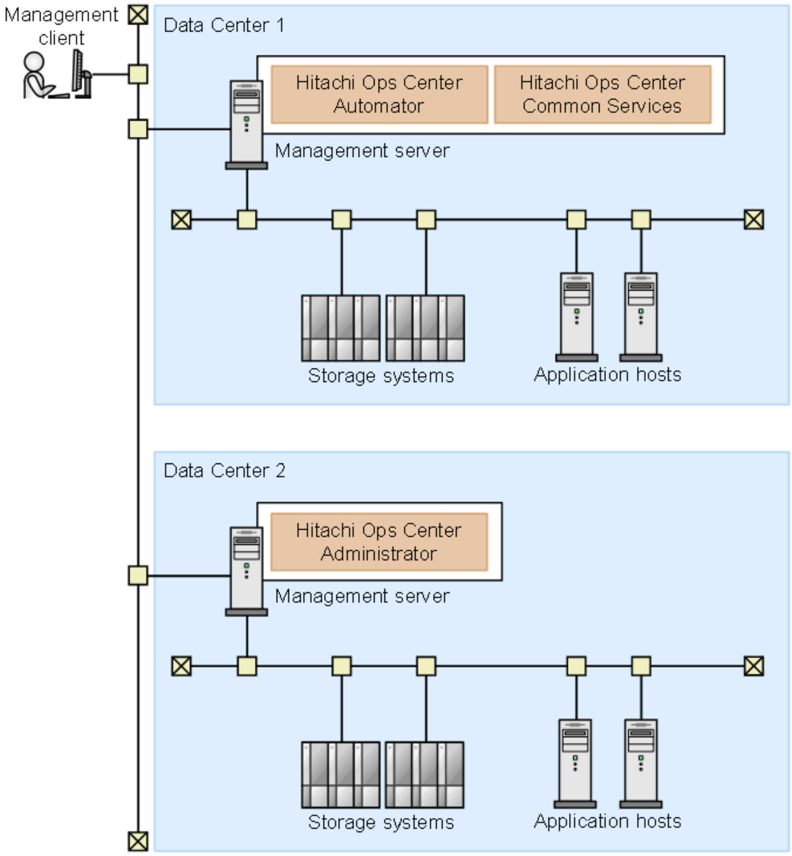
Example configuration running on multiple management servers

When managing resources in a large-scale data center, you can use a configuration that uses multiple management servers. The following shows this type of configuration.


Management client
Hitachi Ops Center Analyzer viewpoint
Hitachi Ops Center Common Services
Deploy with Analyzer viewpoint OVF
Analyzer viewpoint server
Data Center 1
Hitachi Ops Center Automator
Hitachi Ops Center Administrator
Hitachi Ops Center Analyzer
Hitachi Ops Center Protector (Master)
Hitachi Ops Center Analyzer detail view
Hitachi Ops Center API Configuration Manager
Hitachi Ops Center Common Services
Deploy with Ops Center OVA
Management server
Deploy with Analyzer probe OVA
Hitachi Ops Center Analyzer probe
Hitachi Ops Center Protector (Client)
Hitachi Ops Center API Configuration Manager
Storage systems
Application hosts
Analyzer probe server
Data Center 2
Hitachi Ops Center Automator
Hitachi Ops Center Administrator
Hitachi Ops Center Analyzer
Hitachi Ops Center Protector (Master)
Hitachi Ops Center Analyzer detail view
Hitachi Ops Center API Configuration Manager
Hitachi Ops Center Common Services
Deploy with Ops Center OVA
Management server
Deploy with Analyzer probe OVA
Hitachi Ops Center Analyzer probe
Hitachi Ops Center Protector (Client)
Hitachi Ops Center API Configuration Manager
Storage systems
Application hosts
Analyzer probe server

If you deploy multiple OVA files, a Common Services instance is installed on each server, but the system only uses one instance. In this example configuration, the system uses the Common Services instance on the management server running in Data Center 1.

Using an individual installer, you can also manually install optional Hitachi Ops Center products. In this example configuration, Automator, Administrator, and Common Services are installed.



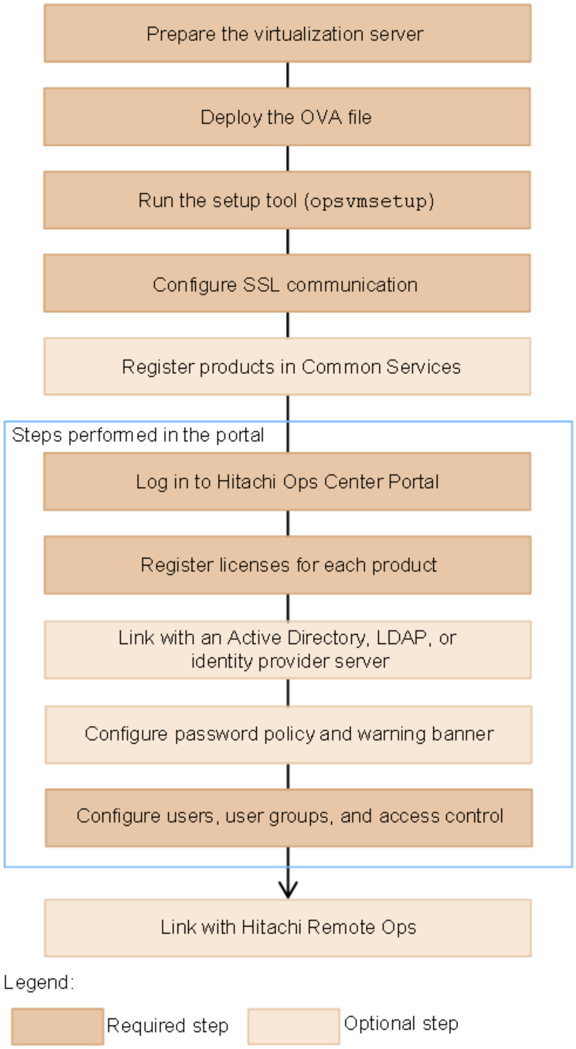
Note: If the Hitachi Ops Center system configuration contains multiple management servers and the system times of the management servers are not the same, you cannot start the products from the Hitachi Ops Center Portal. To keep the time synchronized, we recommend that you use NTP to correct the time automatically.

Chapter 2: Installing Hitachi Ops Center products by using the OVA file

You can install Hitachi Ops Center products on a virtual machine by deploying the Hitachi Ops Center OVA file on a VMware ESXi server.

Workflow for deploying and setting up Hitachi Ops Center

The following figure shows the workflow for installing and setting up the Hitachi Ops Center products by using the OVA file:


Prepare the virtualization server
Deploy the OVA file
Run the setup tool (opsvmsetup)
Configure SSL communication
Register products in Common Services
Steps performed in the portal
Log in to Hitachi Ops Center Portal
Register licenses for each product
Link with an Active Directory, LDAP, or identity provider server
Configure password policy and warning banner
Configure users, user groups, and access control
Link with Hitachi Remote Ops
Legend:
Required step
Optional step

For a complete list of Hitachi Ops Center system requirements, go to the Ops Center documentation site and select Hitachi Ops Center System Requirements.

For details on preparing the virtualization server, see the VMware documentation.

After configuring access control, configure the settings for each product as necessary. For details on how to configure settings, see the documentation for each product.

System configuration of the Hitachi Ops Center virtual machine

This section describes the virtual machine system configuration that is created by using the Hitachi Ops Center OVA file.

Guest operating system

Oracle Linux is installed as the guest operating system.

Installed products

The following products, which are components of the management server, are installed:

- Hitachi Ops Center Automator
- Hitachi Ops Center Analyzer
- Hitachi Ops Center Analyzer detail view
- Hitachi Ops Center Administrator
- Hitachi Ops Center Protector
- Hitachi Ops Center API Configuration Manager
- Hitachi Ops Center Common Services

Note:

- The installation directory is `/opt/hitachi`.
- The installation destination for Common Services is `/opt/hitachi/CommonService`.
- User data for Common Services is stored in the following user data directory:

  `/var/opt/hitachi/CommonService`

API Configuration Manager requires Command Control Interface, so it is also installed as part of the installation. The installation directory is `/opt/hitachi/HORCM`.

Note:

- For products not included in this OVA, install each product by using the individual installer or OVA provided for that product.
- Hitachi Ops Center does not support installing other software products on the management server, but allows for installing software required by corporate policy such as anti-virus programs and third-party monitoring agents. Note that Hitachi Vantara does not take responsibility for or support any interactions between the third-party programs and the Hitachi Ops Center software.

Default settings for the virtual machine and the guest operating system

The OVA deployment sets the virtual machine and operating system settings that Hitachi Ops Center requires by default.

When you deploy the OVA file, a virtual machine with the following default settings is created. Confirm whether the virtualization server has enough resources to create the virtual machine.

Item	Settings
CPU	12 cores
Memory	36 GiB
Disk size	1050 GiB

The default settings assume that you are managing 10 storage systems. For larger-scale systems, change the settings for memory, disk size, and virtual memory, or increase the number of virtual machines.

For details on how to change the settings of virtual machines, go to the Ops Center documentation site and select Hitachi Ops Center System Requirements.

The following table lists the items that are set by default for the guest operating system. To change the settings for Hitachi Ops Center products after the deployment, change the operating system settings as needed.

Item	Settings
Operating system version	Oracle Linux

Item	Settings
	For details about the latest operating system version, see the *Hitachi Ops Center System Requirements*.
Installed libraries	Prerequisite libraries required for the Hitachi Ops Center products included in the OVA.
Kernel parameters	Values required for the Hitachi Ops Center products included in the 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.

Deploying Hitachi Ops Center

By deploying the Hitachi Ops Center OVA file, you can create a virtual machine on which the products are installed.

Procedure

1. From a VMware vSphere client, log in to the VMware ESXi server.
2. From the VMware vSphere client, deploy the Hitachi Ops Center OVA (`OpsCenterVM_`*`version`*`.ova`) by selecting **File** > **Deploy OVF Template**, and then follow the prompts.
3. To avoid IP address conflicts when the virtual machine starts, 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 network settings are set by default for the virtual machine:

   - IP address: 172.30.197.92
   - Network mask: 255.255.0.0
   - Default gateway: 172.30.0.1

   a. Right-click the new virtual machine, and select **Edit Settings**.

   b. In the **Hardware** tab, select **Network adapter 1**, and then clear the **Connect at power on** check box.
4. Start the virtual machine.
5. If you changed the settings in step 3 so that the virtual machine does not connect to the network when it starts, reselect the **Connect at power on** check box.

   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 specify the following settings:

Network settings

- Host name (or FQDN)
- IP address
- Default gateway
- Network mask
- DNS server (up to two servers)
- Password-based SSH root login

Time settings

- Time zone
- NTP server

When you run the initial setup, the following settings are specified: the network and time settings for the guest OS, the single sign-on settings for the selected product, the settings to enable SSL communications, and the firewall settings for service ports.

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 the `/opt/OpsVM/vmtool` directory but you can run the tool from any directory.
- The setup tool specifies an IPv4 address.
- The host name (or FQDN) and IP address specified in this step is used in the URL for accessing the Hitachi Ops Center Portal. To change the host name (or FQDN) or IP address that is used to access the Hitachi Ops Center Portal, run the **`cschgconnect`** command after installation. For details about the **`cschgconnect`** command, see Changing the management server host name, IP address, or port number (on page 159).
- The management server on which Common Services and other relevant products are installed and the web browser used to access the Hitachi Ops Center Portal must be able to resolve and reach the host name (or FQDN) and IP address.
- You cannot specify uppercase characters in the host name (or FQDN). If you do, they are converted to lowercase characters and then registered.
- Specify the time zone in the *`area/location`* format. If you do not know the required 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.

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

   User ID: `root`

   Password: `manager`

   After logging in, you must change the root password.

2. Run the setup tool: **`opsvmsetup`**.
3. Specify the values as indicated in the prompts.
   After you finish all items, a list of the settings is displayed.
4. Check the settings, enter `y`, and then apply the settings.

   After applying 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, complete the following steps to 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**.

Installing Analyzer separately using an OVA

In a large system configuration with multiple Analyzer servers, you can use the Analyzer OVA to deploy only Analyzer and Analyzer detail view. This enables you to use a separate server or add another instance of Analyzer. For information on installing the Analyzer OVA, see the Analyzer installation documentation.

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 One B20 or 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 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:** For best results, select **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
   - **Network 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)
     - Password-based SSH root login
   - **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**.

Upgrading after an OVA installation

The OVA is for new installations only. To perform an upgrade or overwrite installation, perform the procedures described in Installing or upgrading Hitachi Ops Center products by using the Express installer (on page 36) or Installing or upgrading Hitachi Ops Center products by using the individual installer (on page 65).

Configuring SSL communications

By default, Common Services uses SSL/TLS communications. Immediately after installation, the system uses SSL communication by using a self-signed certificate. However, you must set up SSL communications to use a valid server certificate before any of the products can communicate with Common Services and the Hitachi Ops Center Portal.

For details on how to configure SSL communications, see Configuring SSL communications (on page 76).

Next steps

When you finish configuring SSL communications, go to Registering Hitachi Ops Center products with Common Services (on page 32).

Registering Hitachi Ops Center products with Common Services

If you want to use the functions provided by Common Services, such as the Portal window, user management, or single sign-on, run the **setupcommonservice** command to register each product with Common Services.

When you deploy the Hitachi Ops Center OVA file, each product is registered with Common Services. In this case, go to Initial setup using the Hitachi Ops Center Portal (on page 96). In the following cases, you must run the **setupcommonservice** command for each product:

- If you want to use a product that was installed by using a method other than the Ops Center OVA, register the product in Common Services.
- If you deployed the Ops Center OVA to multiple management servers, decide which management server to use as the Common Services host, and then re-register the products installed on the other management servers to the central Common Services instance.

Note: You cannot unregister a Hitachi Ops Center product using the **setupcommonservice** command. To delete products, use the Hitachi Ops Center Portal.

Before you begin

- Change the initial password of the Hitachi Ops Center Portal built-in account (the sysadmin user). When you use the initial password to log in to the Hitachi Ops Center Portal, the Change password window is displayed. Specify a new password. For details, see Logging in to the Hitachi Ops Center Portal (on page 97).
- Ensure that each product can resolve the host name where Common Services is installed. If you want to use a host name that is not a fully qualified domain name (FQDN), set the IP address and the host name in the `/etc/hosts` file for name resolution. If you want to use an IP address instead of a host name, log in to the management server where Common Services is installed and run the **cschgconnect.sh** command.
- Ensure that the Hitachi Ops Center product server and the Common Services server are running.
- For the Common Services account to be specified for the **setupcommonservice** command, specify a user who belongs to the opscenter-administrators group.

Note: If you change the Common Services host name, IP address, or server port number changes, you must register each product again.

The location of the **setupcommonservice** command, command syntax, and command examples for each product are as follows:

Administrator

Default location: `/opt/rainier/bin`

Command syntax:

```
setupcommonservice --csUri CommonService_URL --applicationPort port_number --
applicationHostAddress ip_address --applicationName app_name [--appDescription
app_description] [--csUsername CommonService_Username] [--tlsVerify --csUriCACert
Certificate_FileName]
```

Command example:

```
setupcommonservice --csUri https://example.com/portal --csUsername sysadmin --
tlsVerify --csUriCACert certificate.cer --applicationPort 20961 --
applicationHostAddress 192.0.2.11 --applicationName MyAdministrator1
```

Protector

Default location: `/opt/hitachi/protector/bin/`

Command syntax:

```
setupcommonservice --cs-uri CommonService_URL [--cs-username CommonService_Username] -
-app-scheme protocol --app-hostname host_name --app-port port_number
```

Command example:

```
setupcommonservice --cs-uri https://example.com/portal --cs-username sysadmin --app-
scheme https --app-hostname MyHost --app-port 20964
```

Automator

For Linux:

Default location: `/opt/hitachi/Automation/bin/`

Command syntax:

```
setupcommonservice {[-csUri CommonService_URL | -csUri CommonService_URL -csUsername
CommonServiceUsername] [-appName app_name] [-appDescription app_description] [-auto]
| -help}
```

Command example:

```
setupcommonservice -csUri https://example.com/portal -appName MyAutomator1
```

For Windows:

Default location: `Program-Files-folder\hitachi\Automation\bin`

Command syntax:

```
setupcommonservice {[/csUri CommonService_URL | /csUri CommonService_URL /csUsername
CommonServiceUsername] [/appName app_name] [/appDescription app_description] [/auto]
| /help}
```

Command example:

```
setupcommonservice /csUri https://example.com/portal /appName MyAutomator1
```

Analyzer

Default location: `/opt/hitachi/Analytics/bin/`

Command syntax:

```
setupcommonservice -csUri CommonService_URL [-csUsername CommonService_Username] [-
appPort port_number] [-appHostname ip_address_or_host_name] [-appName app_name] [-
appDescription app_description] [-auto]
```

Command example:

```
setupcommonservice -csUri https://example.com/portal -appPort 22016 -appHostname
192.0.2.10 -appName MyAnalyzer1
```

Analyzer detail view

Default location: `/usr/local/megha/bin/`

Command syntax:

```
setupcommonservice -csUri CommonService_URL -csUsername CommonService_Username -
appHostname ip_address_or_host_name -appPort port_number -appName app_name -
appDescription app_description
```

Command example:

```
setupcommonservice -csUri https://example.com/portal -csUsername sysadmin -
appHostname MyHost -appPort 8443 -appName MyAnalyzerdetailview1 -appDescription ""
```

Analyzer probe

Default location: `/usr/local/megha/bin/`

Command syntax:

```
setupcommonservice -csUri CommonService_URL -csUsername CommonService_Username -
appHostname ip_address_or_host_name -appPort port_number -appName app_name -
appDescription app_description
```

Command example:

```
setupcommonservice -csUri https://example.com/portal -csUsername sysadmin -
appHostname MyHost -appPort 8443 -appName MyAnalyzerprobe1 -appDescription ""
```

Analyzer viewpoint

Default location: `/opt/hitachi/analyzer_viewpoint/bin/`

Command syntax:

```
setupcommonservice --csUri CommonService_URL [--csUsername CommonServiceUsername] [--
applicationName app_name]
```

Command example:

```
setupcommonservice --csUri https://example.com
```

Next steps

When the Hitachi Ops Center products are registered in Common Services, go to Initial setup using the Hitachi Ops Center Portal (on page 96).

Installing OS updates and other products after deployment

The following table outlines the installation tasks for an operating system patch or for Hitachi Ops Center products in an environment in which the OVA is deployed.

Task	Implementation method
Apply operating system patches	Apply as needed.
Update the operating system	You can update the OS as described in Applying Linux security updates using yum (on page 189).
Upgrade of OSS	"Requests" incorporated in the VM image is set for the sample code of API Configuration Manager. If a vulnerability is found in "Requests", upgrade all of them. For details, see the *Hitachi Ops Center API Configuration Manager Release Notes*.
Install additional Hitachi Ops Center products	To install other Hitachi Ops Center products that are not installed on a virtual machine to which the OVA is deployed, install the products by using the installation media. Confirm the system requirements of the products, install prerequisite packages, and reconfigure kernel parameters as necessary. For details on the product system requirements, see the documentation or Release Notes for each product.

Chapter 3: Installing or upgrading Hitachi Ops Center products by using the Express installer

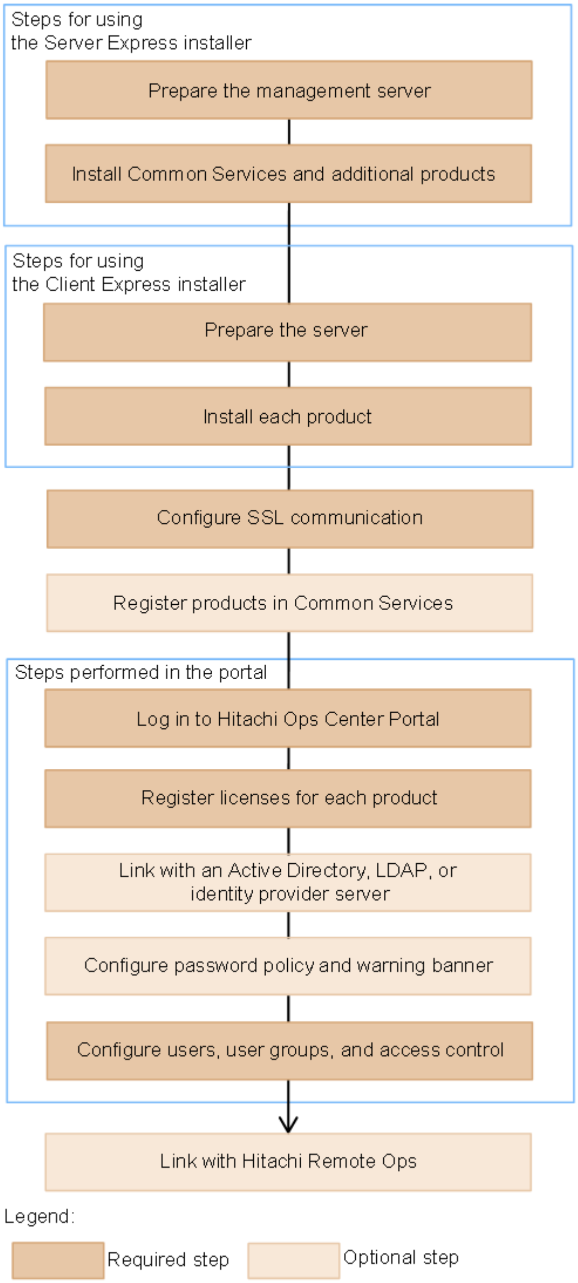
You can simultaneously install or upgrade multiple Hitachi Ops Center products by using the Express installers.

Depending on which products you want to install, you can use the Server Express installer and the Client Express installer. For details, see Using the Server Express installer (on page 38) or Using the Client Express installer (on page 52).

Workflow for installing and setting up Hitachi Ops Center (Express installer)

The following figure shows the workflow for using the Server Express installer and the Client Express installer.

Tip: You use the Client Express installer only when the environment requires it. For example, you use the Client Express installer when you want to configure a separate server to run the Protector Client or Analyzer probe server.


Steps for using the Server Express installer
Prepare the management server
Install Common Services and additional products
Steps for using the Client Express installer
Prepare the server
Install each product
Configure SSL communication
Register products in Common Services
Steps performed in the portal
Log in to Hitachi Ops Center Portal
Register licenses for each product
Link with an Active Directory, LDAP, or identity provider server
Configure password policy and warning banner
Configure users, user groups, and access control
Link with Hitachi Remote Ops
Legend:
Required step
Optional step

When the setup is complete, configure the settings for each product as required. For details, see the documentation for each product.

If you are upgrading, the previous settings are preserved. If you upgrade Hitachi Ops Center products that were registered in Common Services, you do not need to configure SSL communication or perform the subsequent steps.

Using the Server Express installer

Using the Server Express installer, you can simultaneously install or upgrade the following products:

- Hitachi Ops Center Common Services
- Hitachi Ops Center Administrator
- Hitachi Ops Center API Configuration Manager
- Hitachi Ops Center Protector
- Hitachi Ops Center Automator
- Hitachi Ops Center Analyzer
- Hitachi Ops Center Analyzer detail view
- Hitachi Ops Center Analyzer viewpoint

To use API Configuration Manager or Protector, the prerequisite program Command Control Interface is required. If you use the Server Express installer to install API Configuration Manager or Protector, Command Control Interface will also be installed. Do not use this instance of Command Control Interface for other purposes.

Note: If Command Control Interface has already been installed by using one of the following methods, upgrade it by using the Server Express installer:

- Installation by using the Ops Center OVA
- Installation by the Server Express installer
- Individual installation of API Configuration Manager

If the currently installed instance of Command Control Interface is a newer version, it will be left in place.

If Command Control Interface was individually installed by using a different method, it will not be upgraded. If necessary, you can upgrade it manually.

If you do not want to use an individually installed instance of Command Control Interface and want to replace it with an instance of Command Control Interface installed by the Server Express installer, or if you want to replace an instance of Command Control Interface installed by the Server Express installer with an individually installed instance of Command Control Interface, see Replacing Command Control Interface (on page 191).

Preparing the management server

Make sure that the management server on which you plan to install Hitachi Ops Center products meets the system requirements.

For the Common Services system requirements, see the Hitachi Ops Center Release Notes. For the system requirements of other Hitachi Ops Center products, see the documentation or Release Notes for each product.

For a complete list of Hitachi Ops Center system requirements, go to the Ops Center documentation site and select Hitachi Ops Center System Requirements.

Note:

- Hitachi Ops Center does not support installing other software products on the management server, but allows for installing software required by corporate policy such as anti-virus programs and third-party monitoring agents. Note that Hitachi Vantara does not take responsibility for or support any interactions between the third-party programs and the Hitachi Ops Center software.
- When Common Services is installed, the following RPM packages are installed:
  - Amazon Corretto 21
  - PostgreSQL 15
- Common Services starts the Common Services service by using the postgres user and postgres group created on the management server.

  Configurations where postgres users and postgres groups do not exist on the management server are not supported.

  If the users on the management server are managed by an external authentication server, the Common Services service cannot start when the OS starts.

Make sure that you complete the following actions on the installation destination management server:

- To install prerequisite packages, the Server Express installer requires the repository settings for the **`yum`** command. Specify the yum repository settings in advance, or specify the settings by following the message displayed when you run the Server Express installer.
- Administrator requires Podman as a container runtime.

  For Podman-related software (podman, containers-common, conmon, runc), make sure that versions supported by Administrator are installed on the management server.

  If they are not installed, install them by using the following methods:

  - Installation by using the Server Express installer

    When you install by using the Server Express installer, the **`yum`** command is run during the Administrator installation and the Podman-related software is installed. Configure the yum repository settings in advance or when running the Server Express installer so that a supported version of the Podman-related software can be installed.
  - Installation by using the OS media

    If the yum repository does not contain a supported version of the Podman-related software, install a supported version of the Podman-related software by using the OS media.

  For details on supported versions and how to install them, see the *Hitachi Ops Center Administrator Getting Started Guide*.

Note: If you run the Server Express installer, the `iptables` and `firewalld` settings are changed so that required communications can be established. If you use `nftables`, you must make the changes manually.

Installing or upgrading Common Services and additional products

To install or upgrade Common Services and one or more products, use the Server Express installer.

Note:

- If you install Common Services, Amazon Corretto 21 and PostgreSQL 15 are installed. If you upgrade Common Services, Amazon Corretto 8 (version 10.6.0 and earlier), Amazon Corretto 11 (versions 10.6.1 to 10.9.1), Amazon Corretto 17 (versions 10.9.2 to 11.0.2), and PostgreSQL 11 (version 10.9.2 and earlier) that were installed with the previous version are not removed. If you do not need these programs, remove them by using the **`rpm`** command. If you cannot remove the programs by using this command, use the **`rpm`** command with the `--nopreun` option specified.

  The package names are as follows:

  - Amazon Corretto 8: `java-1.8.0-amazon-corretto-devel`
  - Amazon Corretto 11: `java-11-amazon-corretto-devel`
  - Amazon Corretto 17: `java-17-amazon-corretto-devel`
  - PostgreSQL 11: `postgresql11, postgresql11-server, postgresql11-libs`
- If the Analyzer viewpoint server was deployed by using an OVF version earlier than 10.5.1, you cannot use the Server Express installer to upgrade Common Services or Analyzer viewpoint. In this case, deploy the latest version of the Analyzer viewpoint OVF to upgrade.

  For details on how to upgrade Analyzer viewpoint, see the Analyzer documentation.

Before you begin

- For best results, close all other programs, including:
  - Security-monitoring programs
  - Virus-detection programs
  - Process-monitoring programs

  If the Services window is open, close it.
- If you are logged in to the Hitachi Ops Center Portal, close the web browser before beginning the upgrade. If you upgrade Common Services while logged in to the Hitachi Ops Center Portal, an internal server error might occur. If this error occurs, restart the web browser.

- In Common Services version 10.9.1 and later, a special group named support-services has been added as a default user group. This group is used for support services, so it cannot be used for standard purposes. For this reason, if you want to upgrade from version 10.9.0 or earlier, first make sure that the support-services group does not exist.
  - If the support-services group was imported by linking with an Active Directory server, delete the group. In addition, from the Hitachi Ops Center Portal, change the Group entry list setting for user directories so that the support-services group will not be imported.
  - If the system administrator created the support-services group using a method other than linking with an Active Directory server, delete or rename the group before upgrading from version 10.9.0 or earlier.

  > **Note:** If you upgrade Common Services from version 10.9.0 or earlier while the support-services group exists, you must delete or rename the group and then perform an overwrite installation of Common Services.

- For details on the prerequisites for installing each product, see the respective manual.

Procedure

1. Log in to the management server as the root user.

   If you log in as an ordinary user, use the **`sudo`** command to complete the following procedure as the root user.
2. To start the Server Express installer, run `install.sh`, which is in the following location on the installation media:

   `root-directory-of-the-installation-media``/install.sh`

   > **Note:** If one or more products cannot be installed in the same environment as a currently installed product, the Server Express installer will not install the applicable products and a warning message is displayed.
3. If the yum repository settings are not configured or cannot be used, a message appears asking if you want to run the Yum Setup Helper tool. Follow the displayed message to configure the settings.
   a. To configure the settings, enter **y**. The Yum Setup Helper window is displayed.
   b. From **Content in Current Dir**, use the cursor keys and then the **Enter** key to select the directory that includes the OS media file (ISO file).

      > **Note:** The Yum Setup Helper tool uses the OS media file to configure the yum repository settings, so the OS media file must be stored on the management server. If the OS media file does not exist, get it from the distribution website. Click **Help** to see information about the corresponding OS media file.
   c. Select the ISO file. The file name is displayed for **Selected Item**.
   d. Click **OK**. Configuration of the yum repository settings starts, and a processing window is displayed.

      > **Tip:** You can also use the **tab** key to move the cursor between items in the window.

e. When configuration of the yum repository settings is complete, a message is displayed. Select **OK**. If the configuration fails, an error message is displayed. If you select **OK**, the window where you can select an OS media file is displayed again.

4. Choose the product you want to install, and then press **Enter**.

   If you select **1 All**, the products listed within the parentheses are installed.

   To select multiple products, separate the numbers with commas. (Example: 2,3)

   Note: You cannot select products that have ** displayed for the product number.

5. For new Analyzer, Analyzer detail view, or Analyzer viewpoint installations, set the memory size by choosing one of the following scale values:

   - `1`: Small-scale configuration
   - `2`: Medium-scale configuration
   - `3`: Large-scale configuration

   Note: For details on the system requirements for each product based on scale, see *Hitachi Ops Center System Requirements*.

6. Follow the prompts and specify the required information.

   For Common Services:

Setting items	Description

Install directory	For a new installation:
	- Specify the directory in which to install Common Services.
	It will be installed in the following location:
	`*specified-directory*/CommonService`
	The default location is as follows:
	`/opt/hitachi/CommonService`
	- Specify a directory by using 64 or fewer bytes and the following characters:
	A-Z, a-z, 0-9, underscores (_), and forward slashes (/)
	Note: You cannot specify the following paths:
	- `/usr`
	- `/usr/local`
	- `/var`
	- root directory (`/`)

Host name or IP address	For a new installation: - You can specify a host name in FQDN format. - The host name (or FQDN) or IP address specified in this step is used in the URL for accessing the Hitachi Ops Center Portal. To change the host name (or FQDN) or IP address that is used to access the Hitachi Ops Center Portal, run the **`cschgconnect`** command after installation. For details about the **`cschgconnect`** command, see Changing the management server host name, IP address, or port number (on page 159). - The management server on which Common Services and other relevant products are installed and the web browser used to access the Hitachi Ops Center Portal must be able to resolve and reach the host name (or FQDN) and IP address.

Setting items	Description
	▪ If you specify a host name (or FQDN), specify a value using no more than 128 characters. ▪ You cannot specify uppercase characters in the host name (or FQDN). If you do, they are converted to lowercase characters and then registered.
Port number	For a new installation: ▪ Specify a value in the range 1 - 65535. ▪ Default: 443 If you install the following products on the same management server, there will be conflicts with the default port number 443: • Protector • Administrator Change the port number so that it does not conflict between the products. If you want to change the port number for Common Services to a number other than 443, we recommend using port number 20950.
Do you want to access to Hitachi Ops Center Portal by using both host name and IP address ?	For a new installation where a host name or FQDN is specified: ▪ Specify y or n. ▪ Default: n
Do you want to back up the Common Services database first ?	For an upgrade or overwrite installation: ▪ Specify y or n. ▪ Default: y
Database backup location	For an upgrade or overwrite installation where you want to back up the database: ▪ Specify a directory by using 150 or fewer bytes and the following characters: A-Z, a-z, 0-9, underscores (_), and forward slashes (/) **Note:** You cannot specify the root directory (/). ▪ Default: `/var/`*`installation-directory`*`/backup`

Setting items	Description
Admin user name	For a new installation of another product when Common Services has already been installed: Specify the username of the Common Services administrator. Specify a user who belongs to the user group to which the opscenter-system-administrator or the opscenter-security-administrator role is assigned.
Password	For a new installation of another product when Common Services has already been installed: Specify the password of the Common Services administrator.

For Administrator:

Setting items	Description
IP address	For a new installation: ▪ Specify a value in IPv4 format. ▪ Default: IP address of the system
Port number	For a new installation: ▪ Specify a value in the range 1 - 65535. ▪ Default: 20961
User name	For an upgrade installation: Default: sysadmin
Password	For an upgrade installation: Default: None
Network mode	Specify the container network mode by using either of the following: ▪ bridge: Uses the container bridge network. ▪ host: Uses the container host network. Use this mode if you must disable the kernel parameter **`net.ipv4.ip_forward`**. For a new installation: ▪ Specify 1 (bridge) or 2 (host). ▪ Default: 1

Setting items	Description
	For an upgrade installation: If you want to change the current network mode, specify 1 (bridge) or 2 (host).

For API Configuration Manager:

Setting items	Description

Install directory	For a new installation:
	▪ Specify the directory in which to install API Configuration Manager.
	It will be installed in the following location:
	`*specified-directory*/ConfManager`
	The default location is as follows:
	`/opt/hitachi/ConfManager`
	▪ Specify a directory by using 64 or fewer bytes and the following characters:
	A-Z, a-z, 0-9, underscores (_), and forward slashes (/)
	Note: You cannot specify the following paths:
	▪ `/usr`
	▪ `/usr/local`
	▪ `/var`
	▪ root directory (`/`)

Do you want to back up the API Configuration Manager database first ?	For an upgrade installation: ▪ Specify y or n. ▪ Default: y

Setting items	Description
Database backup location	For an upgrade installation where you want to back up the database: ▪ Specify a directory by using 64 or fewer bytes and the following characters: A-Z, a-z, 0-9, underscores (_), and forward slashes (/) **Note:** You cannot specify the following paths: ▪ `/usr` ▪ `/usr/local` ▪ `/var` ▪ root directory (`/`) ▪ Default: `*specified-directory*/backup/bak_CONFIG_MGR`

For Protector:

Setting items	Description

Install directory	For a new installation:
	Specify the directory in which to install Protector.
	It will be installed in the following location:
	`*specified-directory*/protector`
	The default location is as follows:
	`/opt/hitachi/protector`

Node name	For a new installation: Default: Node name of the operating system
User account on the local system	For a new installation: Default: root
Port number	For a new installation: Default: 20964

For Automator:

Setting items	Description

Install directory	For a new installation:
	- Specify the directory in which to install Automator.
	It will be installed in the following location:
	`specified-directory/Automation`
	The default location is as follows:
	`/opt/hitachi/Automation`
	- Specify a directory by using 64 or fewer bytes and the following characters:
	A-Z, a-z, 0-9, underscores (_), and forward slashes (/)
	Note: You cannot specify the following paths:
	- `/usr`
	- `/usr/local`
	- `/var`
	- root directory (`/`)

Host name or IP address	For a new installation: If you specify a host name specify a value using no more than 128 characters.
Database directory	For a new installation: - Specify a directory by using 90 or fewer bytes and the following characters: A-Z, a-z, 0-9, underscores (_), and forward slashes (/) **Note:** You cannot specify the root directory (/). - Default: `/var/specified-directory/database`
Do you want to back up the Automator database first ?	For an upgrade or overwrite installation: - Specify y or n. - Default: y

Setting items	Description
Database backup location	For an upgrade or overwrite installation where you want to back up the database: - Specify a directory by using 150 or fewer bytes and the following characters: A-Z, a-z, 0-9, underscores (_), and forward slashes (/) **Note:** You cannot specify the root directory (/). - Default: `/var/`*`specified-directory`*`/Automation_backup`

For Analyzer:

Setting items	Description
Install directory	For a new installation: - Specify the directory in which to install Analyzer. It will be installed in the following location: *`specified-directory`*`/Analytics` The default location is as follows: `/opt/hitachi/Analytics` - If you specify a directory other than the default, refer to the product manual for the requirements.

For Analyzer detail view:

Setting items	Description
Installation-destination device	For a new installation: - A list of devices on the management server is displayed. Default: Devices with enough free space for the installation are displayed. - If you want to use a device other than the default, specify a device name from the displayed list.

Setting items	Description
Directory for storing application data	For a new installation: - Specify the directory where the application data will be stored. The default location is as follows: `/data` - If you specify a directory other than the default, refer to the product manual for the requirements.
HTTP access port for internal communication	For a new installation: If port number 8080 is being used by another program, specify a value from 10000 to 65530.
HTTPS access port	For a new installation: If port number 8443 is being used by another program, specify a value from 10000 to 65530.
Password for the megha and meghadata users	For a new installation: Specify the password for the megha and meghadata users. The specified password will be set for both the megha and meghadata users.

For Analyzer viewpoint:

Setting items	Description
HTTPS access port for internal communication	If port number 25442 is being used by another program, specify a value from 1 to 65535.

For Command Control Interface:

Setting items	Description
Install directory	For a new installation (when installing API Configuration Manager or Protector): - Specify the directory in which to install Command Control Interface. It will be installed in the following location: *specified-directory*/HORCM The default location is as follows: /opt/hitachi/HORCM - Specify a directory by using 64 or fewer bytes and the following characters: A-Z, a-z, 0-9, underscores (_), and forward slashes (/) **Note:** You cannot specify the following paths: - Paths containing /ConfManager/ - Root directory (/)

7. Check the information you entered and the message that appears.

   If both API Configuration Manager and Protector are included as products to install, a message related to Command Control Interface might appear. Check the message and then continue.

   If there are no problems, press **y** to begin the installation.

8. When the installation is complete, the results are displayed:

   - If all installation tasks finished successfully, **Completed successfully.** is displayed.
   - If any task fails, **Failed.** is displayed.

   If Common Services registration displays a **Failed.** status, you must register the product manually after installing all the products and completing the SSL communications configuration.

   Note: When it takes a long time to install Automator, a KNAE04747-E message might be shown on the console even if the installation is successful. If "`Hitachi Ops Center Automator installation completed successfully.`" is output after the KNAE04747-E message, the installation processing might have completed successfully. Wait a while, check whether the Automator service is running, and if the service is running, log in to Automator. If the Automator service is stopped, start the Automator service, and log in to Automator. If the login is successful, the installation processing is done, and you can ignore the KNAE04747-E message.

9. If you are upgrading from Common Services version 10.9.2 or earlier using the SAML protocol to link with AD FS, you must register the metadata re-acquired from Common Services in AD FS when the upgrade is complete.

   For the registration procedure, see:

   - Exporting Common Services metadata (AD FS) (on page 125)
   - Registering Common Services in AD FS as a relying party (on page 125)

10. If you are upgrading Common Services from version 10.9.3 or earlier and Common Services is linked with an Active Directory server, after upgrading check the settings of **Add all users under Base DN to opscenter-users group** in the Hitachi Ops Center Portal Edit user directory service window.

    > **Note:** Active Directory users are displayed in the Hitachi Ops Center Portal Users window. If there are a large number of users, it might take time to display the screen. If necessary, specify a search filter in **Custom user LDAP filter** to narrow down the Active Directory users to display. The search-filter syntax must conform to RFC 2254.

    - If **Enable** is specified, all Active Directory users under the Base DN are retrieved. Specify a search filter in **Custom user LDAP filter**.
    - If **Disable** is specified, the value of **Group entry list** is automatically specified in **Custom user LDAP filter** when you upgrade. Change the setting as needed.

Next steps

Proceed as follows:

- If you are installing API Configuration Manager, Protector Client, or Analyzer probe server on a server other than Common Services, go to Using the Client Express installer (on page 52).
- If you are not installing these products or plan to install them later, go to Configuring SSL communications (on page 61).

Using the Client Express installer

Using the Client Express installer, you can simultaneously install or upgrade the following products:

- Hitachi Ops Center API Configuration Manager
- Hitachi Ops Center Protector Client
- Hitachi Ops Center Analyzer probe server

To use API Configuration Manager or Protector Client, the prerequisite program Command Control Interface is required. If you use the Client Express installer to install API Configuration Manager or Protector Client, Command Control Interface is also installed. Do not use this instance of Command Control Interface for other purposes.

Note: If Command Control Interface was already installed by using one of the following previous installations, upgrade it by using the Client Express installer:

- Analyzer probe OVA
- Client Express installer
- API Configuration Manager individual installer

If the currently installed Command Control Interface instance is a newer version, it will be left in place.

If Command Control Interface was individually installed by using a different method, it will not be upgraded. If necessary, you can upgrade it manually.

If you do not want to use an individually installed instance of Command Control Interface and want to replace it with an instance of Command Control Interface installed by the Client Express installer, or if you want to replace an instance of Command Control Interface installed by the Client Express installer with an individually installed instance of Command Control Interface, see Replacing Command Control Interface (on page 191).

Preparing the server

Make sure that the server on which you plan to install Hitachi Ops Center products meets the system requirements that are described in the manual or Release Notes for each product.

Make sure that you complete the following actions on the installation destination:

- To install prerequisite packages, the Client Express installer requires the repository settings for the **`yum`** command. Specify the yum repository settings in advance, or specify the settings by following the message displayed when you run the Client Express installer.
- When performing a new installation of the Analyzer probe server, do not install Analyzer detail view on the same server.

Note: If you run the Client Express installer, the `iptables` and `firewalld` settings are changed so that required communications can be established. If you use `nftables`, you must make the changes manually.

Installing or upgrading each product

To install or upgrade each product, use the Client Express installer.

Before you begin

For best results, close all other programs, including:

- Security-monitoring programs
- Virus-detection programs
- Process-monitoring programs

If the Services window is open, close it.

Procedure

1. Log in to the server as the root user or use the **`sudo`** command.
2. To start the Client Express installer, run `install.sh`, which is in the following location in the installation media:

   `root-directory-of-the-installation-media/install.sh`

   Note: If one or more products cannot be installed in the same environment as a currently installed product, the Client Express installer will not install the applicable products and a warning message is displayed.

3. If the yum repository settings are not configured or cannot be used, a message appears asking if you want to run the Yum Setup Helper tool. Follow the displayed message to configure the settings.
   a. To configure the settings, enter **y**. The Yum Setup Helper window is displayed.
   b. From **Content in Current Dir**, use the cursor keys and then the **Enter** key to select the directory that includes the OS media file (ISO file).

      Note: The Yum Setup Helper tool uses the OS media file to configure the yum repository settings, so the OS media file must be stored on the management server. If the OS media file does not exist, get it from the distribution website. Click **Help** to see information about the corresponding OS media file.

   c. Select the ISO file. The file name is displayed for **Selected Item**.
   d. Click **OK**. Configuration of the yum repository settings starts, and a processing window is displayed.

      Tip: You can also use the **tab** key to move the cursor between items in the window.

   e. When configuration of the yum repository settings is complete, a message is displayed. Select **OK**. If the configuration fails, an error message is displayed. If you select **OK**, the window where you can select an OS media file is displayed again.
4. Choose the product you want to install, and then press **Enter**.

   If you select **1 All**, the products listed within the parentheses are installed.

   To select multiple products, separate the numbers with commas. (Example: 2,3)

   Note: You cannot select products that have ** displayed for the product number.

5. For new Analyzer probe server installations, set the memory size by choosing one of the following scale values:
   - `1`: Small-scale configuration
   - `2`: Medium-scale configuration
   - `3`: Large-scale configuration

> **Note:** For details on the system requirements for each product based on scale, see *Hitachi Ops Center System Requirements*.

6. Follow the prompts and specify the required information.

   For API Configuration Manager:

Setting items	Description

Install directory	For a new installation:
	▪ Specify the directory in which to install API Configuration Manager.
	It will be installed in the following location:
	`*specified-directory*/ConfManager`
	The default location is as follows:
	`/opt/hitachi/ConfManager`
	▪ Specify a directory by using 64 or fewer bytes and the following characters:
	A-Z, a-z, 0-9, underscores (_), and forward slashes (/)
	Note: You cannot specify the following paths:
	▪ `/usr`
	▪ `/usr/local`
	▪ `/var`
	▪ root directory (`/`)

Whether backup is required	For an upgrade installation: ▪ Specify y or n. ▪ Default: y

Setting items	Description

Backup directory	If you selected y for the setting "Whether backup is required" for an upgrade installation:
	- Specify the directory for the backup of API Configuration Manager.
	It will be backed up in the following location:
	`specified-directory/backup/bak_CONFIG_MGR`
	The default location is as follows:
	`/opt/hitachi/backup/bak_CONFIG_MGR`
	- Specify a directory by using 64 or fewer bytes and the following characters:
	A-Z, a-z, 0-9, underscores (_), and forward slashes (/)
	Note: You cannot specify the following paths:
	- `/usr`
	- `/usr/local`
	- `/var`
	- root directory (`/`)

For Protector Client:

Setting items	Description

Install directory	For a new installation:
	- Specify the directory in which to install Protector Client.
	It will be installed in the following location:
	`specified-directory/protector`
	The default location is as follows:
	`/opt/hitachi/protector`
	- Specify a directory by using 64 or fewer bytes and the following characters:
	A-Z, a-z, 0-9, underscores (_), and forward slashes (/)
	Note: You cannot specify the following paths:
	- `/usr`
	- `/usr/local`
	- `/var`
	- root directory (`/`)

Node name	For a new installation: Default: Node name of the operating system
Master node name	For a new installation: Specify the node name or IP address of the master OS.
Internet connected	For a new installation: Select whether to install a client node as a node connected to the internet. - Specify y or n. - Default: n

For Analyzer probe server:

Setting items	Description
Application data path	For a new installation: - Specify the directory where the application data will be stored. The default location is as follows: `/home` - If you specify a directory other than the default, refer to the product manual for the requirements.
HTTP access port for internal communication	For a new installation: If port number 8080 is being used by another program, specify a value from 10000 to 65530.
HTTPS access port	For a new installation: If port number 8443 is being used by another program, specify a value from 10000 to 65530.
Port used for the on-demand real time monitoring module	For a new installation: If port number 24262 is being used by another program, specify a value from 10000 to 65530.
Password for megha user	For a new installation: Specify the password for megha user.
Do you want to install the Virtual Storage Software Agent?	If the Virtual Storage Software Agent is not installed: When you want to monitor VSP One SDS Block storage systems, you need to install the Virtual Storage Software Agent. - Specify y or n. - Default: n

Setting items	Description

Installation destination directory for the Virtual Storage Software Agent	When installing the Virtual Storage Software Agent:
	- Specify the installation destination directory for the Virtual Storage Software Agent:
	It will be installed in the following location:
	`*specified-directory*/VirtualStorageSoftwareAgent`
	The default location is as follows:
	`/opt/hitachi/VirtualStorageSoftwareAgent`
	- If you specify a directory other than the default, refer to the product manual for the requirements.

IP address of the Analyzer server	When installing the Virtual Storage Software Agent: The IP address specified here is used when configuring the firewall. - Specify a value in IPv4 format. - Default: IP address of the system

For Command Control Interface:

Setting items	Description

Install directory	For a new installation (when installing API Configuration Manager or Protector Client):
	- Specify the directory in which to install Command Control Interface.
	It will be installed in the following location:
	`*specified-directory*/HORCM`
	The default location is as follows:
	`/opt/hitachi/HORCM`
	- Specify a directory by using 64 or fewer bytes and the following characters:
	A-Z, a-z, 0-9, underscores (_), and forward slashes (/)
	Note: You cannot specify the following paths:
	- Paths containing `/ConfManager/`
	- Root directory (`/`)

7. Check the information you entered and the message that appears.

   If both API Configuration Manager and Protector Client are included as products to install, a message related to Command Control Interface might appear. Check the message and then continue.

   If there are no problems, press **y** to begin the installation.

   > **Note:** If you are installing Analyzer probe server, the following message might appear, but you can ignore it.
   >
   > ```
   > root@localhost's password:
   > ```

8. When the installation is complete, the results are displayed:

   - If all installation tasks finished successfully, **Completed successfully.** is displayed.
   - If any task fails, **Failed.** is displayed.

   > **Note:** To use single sign-on or other features provided by Common Services on the installed Analyzer probe server, register the Analyzer probe server in Common Services after configuring SSL communications.

Configuring SSL communications

Configure SSL on the Hitachi Ops Center products to ensure secure communications. Hitachi Ops Center products use a self-signed certificate or a valid server certificate to perform SSL/TLS communications. The self-signed certificate is used when operation checks are performed, so configure SSL communications using a valid server certificate.

To configure SSL communications, use the SSL Setup tool (**`cssslsetup`** command) or configure the settings manually. For details, see Configuring SSL communications (on page 76). Note that you cannot use the SSL Setup tool to configure SSL communications for Protector clients. For details on how to configure SSL communications for Protector clients, see the Protector documentation.

Next steps

After you finish configuring SSL communications, if there is product that must be registered with Common Services, go to Registering Hitachi Ops Center products with Common Services (on page 61). If you do not need to register a product, go to Initial setup using the Hitachi Ops Center Portal (on page 96).

Registering Hitachi Ops Center products with Common Services

If you want to use the functions provided by Common Services, such as the Portal window, user management, or single sign-on, run the **`setupcommonservice`** command to register each product with Common Services.

If you use the Server Express installer, the products are automatically registered in Common Services. However, in the following cases, you must use the **`setupcommonservice`** command to manually register each product.

- If the product that you installed by using the Server Express installer fails to register in Common Services

  If the result of product registration in Common Services is displayed as Failed., the product registration fails.

- If you are registering the Analyzer probe server installed by using the Client Express installer.

If you do not need to register products in Common Services, go to Initial setup using the Hitachi Ops Center Portal (on page 96).

Note: You cannot unregister a Hitachi Ops Center product using the **`setupcommonservice`** command. To delete products, use the Hitachi Ops Center Portal.

Before you begin

- After installing Common Services, change the initial password for the built-in account (the sysadmin user) on the Hitachi Ops Center Portal. If you use the initial password to log in to the Hitachi Ops Center Portal, the Change password window is displayed. Specify a new password. For details, see Logging in to the Hitachi Ops Center Portal (on page 97).
- Ensure that each product can resolve the host name where Common Services is installed. If you want to use a host name that is not a fully qualified domain name (FQDN), set the IP address and the host name in the `/etc/hosts` file for name resolution. If you want to use an IP address instead of a host name, log in to the management server where Common Services is installed and run the **`cschgconnect.sh`** command.
- Ensure that the Hitachi Ops Center product server and the Common Services server are running.
- For the Common Services account to be specified for the **`setupcommonservice`** command, specify a user who belongs to the opscenter-administrators group.

Note: If you change the Common Services host name, IP address, or server port number changes, you must register each product again.

The location of the **`setupcommonservice`** command, command syntax, and command examples for each product are as follows:

Administrator

Default location: `/opt/rainier/bin`

Command syntax:

```
setupcommonservice --csUri CommonService_URL --applicationPort port_number --
applicationHostAddress ip_address --applicationName app_name [--appDescription
app_description] [--csUsername CommonService_Username] [--tlsVerify --csUriCACert
Certificate_FileName]
```

Command example:

```
setupcommonservice --csUri https://example.com/portal --csUsername sysadmin --
tlsVerify --csUriCACert certificate.cer --applicationPort 20961 --
applicationHostAddress 192.0.2.11 --applicationName MyAdministrator1
```

Protector

Default location: `/opt/hitachi/protector/bin/`

Command syntax:

```
setupcommonservice --cs-uri CommonService_URL [--cs-username CommonService_Username] -
-app-scheme protocol --app-hostname host_name --app-port port_number
```

Command example:

```
setupcommonservice --cs-uri https://example.com/portal --cs-username sysadmin --app-
scheme https --app-hostname MyHost --app-port 20964
```

Automator

Default location: `/opt/hitachi/Automation/bin/`

Command syntax:

```
setupcommonservice {[-csUri CommonService_URL | -csUri CommonService_URL -csUsername
CommonServiceUsername] [-appName app_name] [-appDescription app_description] [-auto]
| -help}
```

Command example:

```
setupcommonservice -csUri https://example.com/portal -appName MyAutomator1
```

Analyzer

Default location: `/opt/hitachi/Analytics/bin/`

Command syntax:

```
setupcommonservice -csUri CommonService_URL [-csUsername CommonService_Username] [-
appPort port_number] [-appHostname ip_address_or_host_name] [-appName app_name] [-
appDescription app_description] [-auto]
```

Command example:

```
setupcommonservice -csUri https://example.com/portal -appPort 22016 -appHostname
192.0.2.10 -appName MyAnalyzer1
```

Analyzer detail view

Default location: `/usr/local/megha/bin/`

Command syntax:

```
setupcommonservice -csUri CommonService_URL -csUsername CommonService_Username -
appHostname ip_address_or_host_name -appPort port_number -appName app_name -
appDescription app_description
```

Command example:

```
setupcommonservice -csUri https://example.com/portal -csUsername sysadmin -
appHostname MyHost -appPort 8443 -appName MyAnalyzerdetailview1 -appDescription ""
```

Analyzer probe

Default location: `/usr/local/megha/bin/`

Command syntax:

```
setupcommonservice -csUri CommonService_URL -csUsername CommonService_Username -
appHostname ip_address_or_host_name -appPort port_number -appName app_name -
appDescription app_description
```

Command example:

```
setupcommonservice -csUri https://example.com/portal -csUsername sysadmin -
appHostname MyHost -appPort 8443 -appName MyAnalyzerprobe1 -appDescription ""
```

Analyzer viewpoint

Default location: `/opt/hitachi/analyzer_viewpoint/bin/`

Command syntax:

```
setupcommonservice --csUri CommonService_URL [--csUsername CommonServiceUsername] [--
applicationName app_name]
```

Command example:

```
setupcommonservice --csUri https://example.com
```

Next steps

When the Hitachi Ops Center products are registered in Common Services, go to Initial setup using the Hitachi Ops Center Portal (on page 96).

Installing OS updates and other products after installation

The following table outlines the installation tasks for operating system patches and Hitachi Ops Center updates where the installer is used.

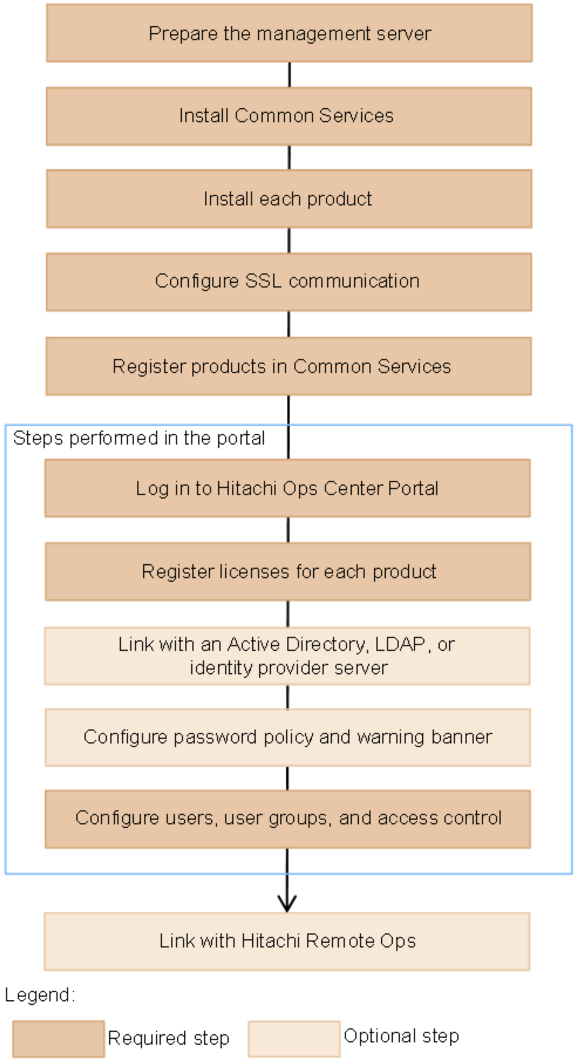
Task	Implementation method
Apply operating system patches	Apply as needed.
Update the operating system	You can update the OS as described in Applying Linux security updates using yum (on page 189).
Upgrade Hitachi Ops Center products	For an upgrade installation or overwrite installation, use the Express installer or individual installers.
Install additional Hitachi Ops Center products	Confirm the system requirements of the products, install prerequisite packages, and reconfigure kernel parameters as necessary. For details on the product system requirements, see the documentation or Release Notes for each product.

Chapter 4: Installing or upgrading Hitachi Ops Center products by using the individual installer

To install or upgrade, or to create a new Hitachi Ops Center system without using the OVA or Express installer, install the products by using the Common Services installer first and then additional products using the individual installer.

Workflow for installing and setting up Hitachi Ops Center (individual installers)

The general workflow for using the individual installer for each product is as follows:


Prepare the management server
Install Common Services
Install each product
Configure SSL communication
Register products in Common Services
Steps performed in the portal
Log in to Hitachi Ops Center Portal
Register licenses for each product
Link with an Active Directory, LDAP, or identity provider server
Configure password policy and warning banner
Configure users, user groups, and access control
Link with Hitachi Remote Ops
Legend:
Required step
Optional step

After setting up access control, configure the settings for each product as necessary. For details, see the documentation for each product.

If you are upgrading, the previous settings are preserved. If you upgrade Hitachi Ops Center products that were registered in Common Services, you do not need to configure SSL communication or perform the subsequent steps.

Preparing the management server

Make sure that the management server on which you plan to install Hitachi Ops Center products meets the system requirements.

For the Common Services system requirements, see the Hitachi Ops Center Release Notes. For the system requirements of other Hitachi Ops Center products, see the documentation or Release Notes for each product.

For a complete list of Hitachi Ops Center system requirements, go to the Ops Center documentation site and select Hitachi Ops Center System Requirements.

Note:

- Hitachi Ops Center does not support installing other software products on the management server, but allows for installing software required by corporate policy such as anti-virus programs and third-party monitoring agents. Note that Hitachi Vantara does not take responsibility for or support any interactions between the third-party programs and the Hitachi Ops Center software.
- When Common Services is installed, the following RPM packages are installed:
  - Amazon Corretto 21
  - PostgreSQL 15
- Common Services starts the Common Services service by using the postgres user and postgres group created on the management server.

  Configurations where postgres users and postgres groups do not exist on the management server are not supported.

  If the users on the management server are managed by an external authentication server, the Common Services service cannot start when the OS starts.

Make sure there are no conflicts among the following port numbers.

Port number used to access Common Services:

443/tcp (default)

Port numbers used for internal communication:

- 20951/tcp
- 20952/tcp
- 20954/tcp
- 20955/tcp
- 20956/tcp

If necessary, register the port number that is used to access Common Services in the firewall exceptions. For details on how to register firewall exceptions, see the OS documentation.

Installing or upgrading Common Services

To install or upgrade Common Services in an existing environment or to create a Hitachi Ops Center system without using the OVA or Express installer, install Common Services by using the individual installer.

Note:

- If you install Common Services, Amazon Corretto 21 and PostgreSQL 15 are installed. If you upgrade Common Services, Amazon Corretto 8 (version 10.6.0 and earlier), Amazon Corretto 11 (versions 10.6.1 to 10.9.1), Amazon Corretto 17 (versions 10.9.2 to 11.0.2), and PostgreSQL 11 (version 10.9.2 and earlier) that were installed with the previous version are not removed. If you do not need these programs, remove them by using the **`rpm`** command. If you cannot remove the programs by using this command, use the **`rpm`** command with the `--nopreun` option specified.

  The package names are as follows:

  - Amazon Corretto 8: `java-1.8.0-amazon-corretto-devel`
  - Amazon Corretto 11: `java-11-amazon-corretto-devel`
  - Amazon Corretto 17: `java-17-amazon-corretto-devel`
  - PostgreSQL 11: `postgresql11, postgresql11-server, postgresql11-libs`
- If the Analyzer viewpoint server was deployed by using an OVF version earlier than 10.5.1, you cannot use the individual installer to upgrade Common Services or Analyzer viewpoint. In this case, deploy the latest version of the Analyzer viewpoint OVF to upgrade.

  For details on how to upgrade Analyzer viewpoint, see the Analyzer documentation.

Before you begin

- Confirm that one of the following settings is configured on the management server installation destination:
  - The management server can access your DNS server.
  - The host name is set in the `hosts` file.

  If the system cannot resolve the management server host name, it might take a long time for Common Services to start.
- If you are logged in to the Hitachi Ops Center Portal, close the web browser before beginning the upgrade. If you upgrade Common Services while logged in to the Hitachi Ops Center Portal, an internal server error might occur. If this error occurs, restart the web browser.
- In Common Services version 10.9.1 and later, a special group named support-services has been added as a default user group. This group is used for support services, so it cannot be used for standard purposes. For this reason, if you want to upgrade from version 10.9.0 or earlier, first make sure that the support-services group does not exist.
  - If the support-services group was imported by linking with an Active Directory server, delete the group. In addition, from the Hitachi Ops Center Portal, change the Group entry list setting for user directories so that the support-services group will not be imported.
  - If the system administrator created the support-services group using a method other than linking with an Active Directory server, delete or rename the group before upgrading from version 10.9.0 or earlier.

  > **Note:** If you upgrade Common Services from version 10.9.0 or earlier while the support-services group exists, you must delete or rename the group and then perform an overwrite installation of Common Services.

Procedure

1. Log in to the management server as the root user.

   If you log on as an ordinary user, use the **`sudo`** command to complete the following procedure as the root user.
2. Run `install.sh`, which is in the following location on the installation media:

   `*root-directory-of-installation-media*/COMSERV/install.sh`
3. To install Common Services, follow the prompts and specify the required information as follows:

For new installations of Common Services:

- Installation destination for Common Services
  - The default installation destination for Common Services is as follows:

    `/opt/hitachi/CommonService`
  - User data for Common Services is stored in the following user data directory:

    `/var/`*`installation-directory-of-Common-Services`*
- Host name (or FQDN) or IP address
  - The host name (or FQDN) or IP address specified in this step is used in the URL for accessing the Hitachi Ops Center Portal. To change the host name (or FQDN) or IP address that is used to access the Hitachi Ops Center Portal, run the **`cschgconnect`** command after installation. For details about the **`cschgconnect`** command, see Changing the management server host name, IP address, or port number (on page 159).
  - The management server on which Common Services and other relevant products are installed and the web browser used to access the Hitachi Ops Center Portal must be able to resolve and reach the host name (or FQDN) and IP address.
  - If you specify a host name (or FQDN), specify a value using no more than 128 characters.
  - You cannot specify uppercase characters in the host name (or FQDN). If you do, they are converted to lowercase characters and then registered.
- Port number of the access URL

  If you install the following products on the same management server, there will be conflicts with the default port number 443. Change the port number so that it does not conflict between the products. If you want to change the port number for Common Services to a number other than 443, we recommend using port number 20950.
  - Protector
  - Administrator
- Whether access is possible by using an IP address

  Specify whether an IP address can be used to access the Hitachi Ops Center Portal when a host name or FQDN is specified in the access URL.
  - To maintain the default setting of not permitting access by using an IP address, specify `y`.
  - To permit access by using an IP address, specify `n`.

    An IP address acquired from the system is automatically set for the access URL.

For overwrite or upgrade installations of Common Services:

- Whether to back up the existing Common Services database
- If yes, the database backup destination
- If you are upgrading from version 10.9.1 or earlier, whether to continue or interrupt the installation when there is not enough free space on the disk

4. Check the information you entered and any messages displayed. If there are no problems, press **y** to begin the installation.
5. Check the message that appears when installation is complete.
6. Change the initial password for the built-in account (the sysadmin user) on the Hitachi Ops Center Portal.

   If you use the initial password to log in to the Hitachi Ops Center Portal, the Change password window is displayed. Specify a new password. For details, see Logging in to the Hitachi Ops Center Portal (on page 97).
7. If you are upgrading from Common Services version 10.9.2 or earlier using the SAML protocol to link with AD FS, you must register the metadata re-acquired from Common Services in AD FS when the upgrade is complete.

   For the registration procedure, see:

   - Exporting Common Services metadata (AD FS) (on page 125)
   - Registering Common Services in AD FS as a relying party (on page 125)
8. If you are upgrading Common Services from version 10.9.3 or earlier and Common Services is linked with an Active Directory server, after upgrading check the settings of **Add all users under Base DN to opscenter-users group** in the Hitachi Ops Center Portal Edit user directory service window.

   > **Note:** Active Directory users are displayed in the Hitachi Ops Center Portal Users window. If there are a large number of users, it might take time to display the screen. If necessary, specify a search filter in **Custom user LDAP filter** to narrow down the Active Directory users to display. The search-filter syntax must conform to RFC 2254.

   - If **Enable** is specified, all Active Directory users under the Base DN are retrieved. Specify a search filter in **Custom user LDAP filter**.
   - If **Disable** is specified, the value of **Group entry list** is automatically specified in **Custom user LDAP filter** when you upgrade. Change the setting as needed.

Installing or upgrading each product

You install other products after you install Common Services. For details on the installation procedure, see the documentation for the individual product.

If you complete an upgrade or overwrite installation of an existing product, the installation destination is the same as the current installation destination.

Note:

- If the password for the built-in account (the sysadmin user) for the Hitachi Ops Center Portal is set to the initial password, you must change it before installing any products. If you use the initial password to log in to the Hitachi Ops Center Portal, the Change password window is displayed. Specify a new password. For details, see Logging in to the Hitachi Ops Center Portal (on page 97).
- If you upgrade Automator or Analyzer from a version earlier than 10.0, verify that SSL communication is configured.

Configuring SSL communications

By default, Common Services uses SSL/TLS communications. Immediately after installation, the system uses SSL communication by using a self-signed certificate. However, you must set up SSL communications to use a valid server certificate before any of the products can communicate with Common Services and the Hitachi Ops Center Portal.

For details on how to configure SSL communications, see Configuring SSL communications (on page 76).

Next steps

When you finish configuring SSL communications, go to Registering Hitachi Ops Center products with Common Services (on page 71).

Registering Hitachi Ops Center products with Common Services

If you want to use the functions provided by Common Services, such as the Portal window, user management, or single sign-on, run the **`setupcommonservice`** command to register each product with Common Services.

If you used an individual installer to install each product, run the **`setupcommonservice`** command to register each product in Common Services.

If you do not need to register products in Common Services, go to Initial setup using the Hitachi Ops Center Portal (on page 96).

Note: You cannot unregister a Hitachi Ops Center product using the **`setupcommonservice`** command. To delete products, use the Hitachi Ops Center Portal.

Before you begin

- After installing Common Services, change the initial password for the built-in account (the sysadmin user) on the Hitachi Ops Center Portal. If you use the initial password to log in to the Hitachi Ops Center Portal, the Change password window is displayed. Specify a new password. For details, see Logging in to the Hitachi Ops Center Portal (on page 97).
- Ensure that each product can resolve the host name where Common Services is installed. If you want to use a host name that is not a fully qualified domain name (FQDN), set the IP address and the host name in the `/etc/hosts` file for name resolution. If you want to use an IP address instead of a host name, log in to the management server where Common Services is installed and run the **`cschgconnect.sh`** command.
- Ensure that the Hitachi Ops Center product server and the Common Services server are running.
- For the Common Services account to be specified for the **`setupcommonservice`** command, specify a user who belongs to the opscenter-administrators group.

> **Note:** If you change the Common Services host name, IP address, or server port number changes, you must register each product again.

The location of the **`setupcommonservice`** command, command syntax, and command examples for each product are as follows:

Administrator

Default location: `/opt/rainier/bin`

Command syntax:

```
setupcommonservice --csUri CommonService_URL --applicationPort port_number --
applicationHostAddress ip_address --applicationName app_name [--appDescription
app_description] [--csUsername CommonService_Username] [--tlsVerify --csUriCACert
Certificate_FileName]
```

Command example:

```
setupcommonservice --csUri https://example.com/portal --csUsername sysadmin --
tlsVerify --csUriCACert certificate.cer --applicationPort 443 --
applicationHostAddress 192.0.2.11 --applicationName MyAdministrator1
```

Protector

Default location: `/opt/hitachi/protector/bin/`

Command syntax:

```
setupcommonservice --cs-uri CommonService_URL [--cs-username CommonService_Username] -
-app-scheme protocol --app-hostname host_name --app-port port_number
```

Command example:

```
setupcommonservice --cs-uri https://example.com/portal --cs-username sysadmin --app-scheme https --app-hostname MyHost --app-port 443
```

Automator

For Linux:

Default location: `/opt/hitachi/Automation/bin/`

Command syntax:

```
setupcommonservice {[-csUri CommonService_URL | -csUri CommonService_URL -csUsername CommonServiceUsername] [-appName app_name] [-appDescription app_description] [-auto] | -help}
```

Command example:

```
setupcommonservice -csUri https://example.com/portal -appName MyAutomator1
```

For Windows:

Default location: *`Program-Files-folder`*`\hitachi\Automation\bin`

Command syntax:

```
setupcommonservice {[/csUri CommonService_URL | /csUri CommonService_URL /csUsername CommonServiceUsername] [/appName app_name] [/appDescription app_description] [/auto] | /help}
```

Command example:

```
setupcommonservice /csUri https://example.com/portal /appName MyAutomator1
```

Analyzer

Default location: `/opt/hitachi/Analytics/bin/`

Command syntax:

```
setupcommonservice -csUri CommonService_URL [-csUsername CommonService_Username] [-appPort port_number] [-appHostname ip_address_or_host_name] [-appName app_name] [-appDescription app_description] [-auto]
```

Command example:

```
setupcommonservice -csUri https://example.com/portal -appPort 22016 -appHostname 192.0.2.10 -appName MyAnalyzer1
```

Analyzer detail view

Default location: `/usr/local/megha/bin/`

Command syntax:

```
setupcommonservice -csUri CommonService_URL -csUsername CommonService_Username -
appHostname ip_address_or_host_name -appPort port_number -appName app_name -
appDescription app_description
```

Command example:

```
setupcommonservice -csUri https://example.com/portal -csUsername sysadmin -
appHostname MyHost -appPort 8443 -appName MyAnalyzerdetailview1 -appDescription ""
```

Analyzer probe

Default location: `/usr/local/megha/bin/`

Command syntax:

```
setupcommonservice -csUri CommonService_URL -csUsername CommonService_Username -
appHostname ip_address_or_host_name -appPort port_number -appName app_name -
appDescription app_description
```

Command example:

```
setupcommonservice -csUri https://example.com/portal -csUsername sysadmin -
appHostname MyHost -appPort 8443 -appName MyAnalyzerprobe1 -appDescription ""
```

Analyzer viewpoint

Default location: `/opt/hitachi/analyzer_viewpoint/bin/`

Command syntax:

```
setupcommonservice --csUri CommonService_URL [--csUsername CommonServiceUsername] [--
applicationName app_name]
```

Command example:

```
setupcommonservice --csUri https://example.com
```

Next steps

When the Hitachi Ops Center products are registered in Common Services, go to Initial setup using the Hitachi Ops Center Portal (on page 96).

Installing OS updates and other products after installation

The following table outlines the installation tasks for operating system patches and Hitachi Ops Center updates where the installer is used.

Task	Implementation method
Apply operating system patches	Apply as needed.
Update the operating system	You can update the OS as described in Applying Linux security updates using yum (on page 189).
Upgrade Hitachi Ops Center products	For an upgrade installation or overwrite installation, use the Express installer or individual installers.
Install additional Hitachi Ops Center products	Confirm the system requirements of the products, install prerequisite packages, and reconfigure kernel parameters as necessary. For details on the product system requirements, see the documentation or Release Notes for each product.

Chapter 5: Configuring SSL communications

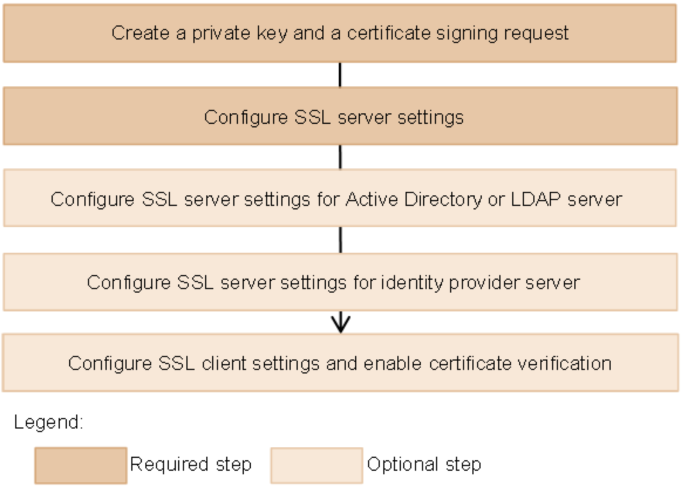
After installation, run the SSL Setup tool (`cssslsetup` command) or manually perform the required procedures to configure SSL communications. By default, Common Services uses SSL/TLS communications by using a self-signed certification. So, you must set up SSL communications to use a valid server certificate.

You can use either of the following methods to configure SSL communications:

- To use the SSL setup tool (the `cssslsetup` command) for each product, perform the procedure described in Configuring SSL communications by using the SSL Setup tool (on page 76).
- To configure SSL communications manually or use both RSA and Elliptic Curve Digital Signature Algorithm (ECDSA) as the public key encryption algorithms, perform the procedure described in Configuring SSL communications without using the SSL Setup tool (on page 89).

Configuring SSL communications by using the SSL Setup tool

The following figure shows the workflow for configuring SSL communications by using the SSL Setup tool (`cssslsetup` command).


Create a private key and a certificate signing request
Configure SSL server settings
Configure SSL server settings for Active Directory or LDAP server
Configure SSL server settings for identity provider server
Configure SSL client settings and enable certificate verification
Legend:
Required step
Optional step

The following Hitachi Ops Center products can be configured for SSL communications by using the `cssslsetup` command:

- Hitachi Ops Center Common Services
- Hitachi Ops Center Automator

- Hitachi Ops Center Analyzer
- Hitachi Ops Center Analyzer detail view
- Hitachi Ops Center Analyzer viewpoint
- Hitachi Ops Center Analyzer probe server
- Hitachi Ops Center Analyzer Virtual Storage Software Agent
- Hitachi Ops Center Administrator
- Hitachi Ops Center Protector (Master)
- Hitachi Ops Center API Configuration Manager

Note:

- You can use the SSL Setup tool for products for which a supported version is installed. If the installed version is not supported, upgrade the product and then use the tool. For details on the versions of each product supported by the SSL Setup tool, see the Hitachi Ops Center Release Notes.
- If API Configuration Manager is installed by a user other than the root user, it is not displayed in the list and SSL communications cannot be configured. Configure the settings manually as described in the *Hitachi Ops Center API Configuration Manager REST API Reference Guide*.
- When specifying a certificate for the **`cssslsetup`** command, specify the certificate in the X.509 PEM format. Make sure that the certificate file specified for the **`cssslsetup`** command contains only text between `-----BEGIN CERTIFICATE-----` and `-----END CERTIFICATE-----`. If the file contains any other text, attempts to set the certificate might fail.

You can run the **`cssslsetup`** command on each management server. For a management server where Common Services is not installed or the Analyzer probe server, obtain the **`cssslsetup`** command from the installation media. The storage locations of the **`cssslsetup`** command are as follows:

- If Common Services is installed on the management server:

  The **`cssslsetup`** command is located

  `*installation-directory-of-Common-Services*/utility/bin`

- If Common Services is not installed on the management server:

  Expand `utility.tar` from the installation media.

  Storage locations of `utility.tar`:

  - `*root-directory-of-the-Common-Services-installation-media*/utility.tar`
  - `*root-directory-of-the-Server-Express-installer-media*/COMMONSERVICES/utility.tar`
  - `*root-directory-of-the-Client-Express-installer-media*/COMMONSERVICES/utility.tar`

  The **`cssslsetup`** command is located

  The **`cssslsetup`** command is stored in the following location after the files are extracted from `utility.tar`:

  `*directory-where-utility.tar-is-extracted*/utility/bin`

The following settings are not configured by the **`cssslsetup`** command:

- Settings using both RSA and Elliptic Curve Digital Signature Algorithm (ECDSA) as public key encryption algorithms

  For details on how to set up such a configuration, see the procedure described in Configuring SSL communications without using the SSL Setup tool (on page 89).

- Settings for storage systems and Active Directory, LDAP, and identity provider servers
- Settings for the Protector clients

  Configure these settings as necessary by referring to the manual for Protector.

SSL Setup tool functionality

The SSL Setup tool provides the following functions.

Creating a private key and a certificate signing request (CSR)

The **`cssslsetup`** command creates a common private key and CSR that can be used by all products.

> **Note:** This command only supports the RSA encryption algorithm. If you want to use both RSA and the Elliptic Curve Digital Signature Algorithm (ECDSA), perform the procedure described in Configuring SSL communications without using the SSL Setup tool (on page 89).

Configuring the SSL server settings

The `cssslsetup` command configures the SSL server settings for the following:

Product	Settings
Common Services	Registers the server certificate and private key.
Automator	▪ Registers the server certificate and private key. ▪ Enables SSL communications.
Analyzer	▪ Registers the server certificate and private key. ▪ Enables SSL communications.
Analyzer detail view	Imports the server certificate (in the PKCS#12 format) into the keystore.
Analyzer viewpoint	Registers the server certificate and private key.
Analyzer probe server	▪ Imports the server certificate (in the PKCS#12 format) into the keystore. ▪ Registers the server certificate and private key (for on-demand real time monitoring and RAID Agent).
Analyzer Virtual Storage Software Agent	Imports the server certificate (in the PKCS#12 format) into the keystore.
Administrator	Registers the server certificate and private key.
Protector	Registers the server certificate and private key.
API Configuration Manager	▪ Registers the server certificate and private key. ▪ Configures notifications for storage system configuration changes.

Configuring the SSL client settings and enabling certificate verification

The `cssslsetup` command configures the SSL communication settings and enables certificate verification.

Product	Settings
Common Services	▪ Imports the root certificate into the truststore. ▪ Imports the root certificate of the server certificate for the Active Directory, LDAP, or an identity provider server into the truststore. ▪ Enables certificate verification.
Automator	▪ Imports the root certificate into the truststore. ▪ Imports the root certificate of the server certificate for the Active Directory server into the truststore. ▪ Enables certificate verification.
Analyzer	▪ Imports the root certificate into the truststore. ▪ Imports the root certificate of the server certificate for the Active Directory server into the truststore. ▪ Enables certificate verification.
Analyzer detail view	▪ Imports the root certificate into the truststore. ▪ Imports the Active Directory server certificate into the truststore. **Note:** To link with Active Directory, you must add an active directory user by using Analyzer detail view. ▪ Enables certificate verification. **Note:** If you want to use a certificate issued by a certificate authority for SSL communication for real time data collection, you must set the following Analyzer detail view server parameters in the `hosts` file on the management server to enable certificate verification: `IP-address hostname` For *hostname*, specify the value obtained by running the **`hostname -f`** command. ▪ Imports the server certificate of the RAID Agent server into the truststore (for on-demand real time monitoring).
Analyzer viewpoint	▪ Registers the trusted certificate into Analyzer viewpoint. ▪ Enables certificate verification.

Product	Settings
Analyzer probe server	▪ Imports the root certificate and the target product's server certificate into the truststore. ▪ Imports the Active Directory server certificate into the truststore. ▪ Imports the root certificate into the Analyzer probe server truststore (for RAID Agent). ▪ Imports the storage system certificate into the truststore of the instance environment (for RAID Agent). ▪ Changes the permissions of the `client.truststore.jks` file, which was copied from the Analyzer detail view server (for real time data collection). ▪ Enables certificate verification.
Analyzer Virtual Storage Software Agent	▪ Imports the root certificate of VSP One SDS Block or the storage system into the truststore. ▪ Enables certificate verification.
Administrator	None **Note:** ▪ You must use the **`setupcommonservice`** command for the following tasks: • Importing the root certificate into the truststore • Enabling certificate verification ▪ If you want to link with Active Directory, you must import the certificate of the Active Directory server into the truststore and register an Active Directory domain that uses the DNS server. For the configuration procedure, see the Administrator documentation.
Protector	Imports the root certificate into the truststore. **Note:** You must use the **`setupcommonservice`** command to enable certificate verification.
API Configuration Manager	▪ Enables certificate verification for SSL communications with the storage system. ▪ Enables SSL communications.

Enabling or disabling certificate verification

You can enable or disable certificate verification for SSL communications maintenance.

Creating a private key and a certificate signing request (SSL Setup tool)

Use the SSL Setup tool to create a private key and a certificate signing request (CSR) for use with all Hitachi Ops Center products.

> **Note:** If the certificate has expired or has been revoked by the certificate authority, you must renew it. Follow the procedure in this section to request a new certificate and overwrite the existing one. You must also perform the procedures in Configuring SSL server settings (SSL Setup tool) (on page 83) and Configuring SSL client settings and enabling certificate verification (SSL Setup tool) (on page 86).

Procedure

1. Log in to the management server as the root user.

   If you log in as an ordinary user, use the **`sudo`** command to complete the following procedure as the root user.

2. Run the **`cssslsetup`** command, which is in the following location:

   If Common Services is installed on the management server:

   `installation-directory-of-Common-Services/utility/bin`

   If Common Services is not installed on the management server:

   `directory-where-utility.tar-is-extracted/utility/bin`

   The main menu is displayed:

```
Main menu   Ver:cssslsetup-command-version
1. Create certificate signing request and private key.
2. Set up SSL server.
3. Set up SSL client.
4. Enable/disable certificate verification(optional).
5. Restart services for each product.
Enter a number or q to quit:
```

3. Enter **1**. You are prompted to provide the required certificate information:

   - Absolute path to the file where the shared private key is output
   - Absolute path to the file where the CSR is output
   - Signature algorithm for RSA
   - Key size
   - Host name (CN)
   - Organizational unit (OU)

- Organization name (O)
- Name of the city or locality (L)
- Name of the state or province (ST)
- 2-letter country code (C)
- Host name (or FQDN), IP address or both of SubjectAltName

> **Note:** When you use the certificate for enabling SSL encryption for real time data collection in the Analyzer detail view server, enter the IP address of SubjectAltName and issue a certificate that includes the IP address specified in the SubjectAltName field.

4. Make sure that the settings are correct. If they are correct, enter **1. Yes**.

   If you want to specify the settings again, enter **2. No (Cancel)** to return to the main menu.
5. When the CSR is successfully created, the results are displayed and the main menu reappears. To exit, enter **q**.
6. Access the CSR from the directory that you specified when creating the request and submit the CSR to the certificate authority requesting that they issue a signed certificate.

   For details, follow the procedure provided by the certificate authority.
7. After obtaining the server certificate signed by the certificate authority, run the following command to check the results:

   If Common Services is installed on the management server:

   ```
   installation-directory-of-Common-Services/openssl/bin/openssl x509 -text -in full-path-of-the-certificate-file
   ```

   If Common Services is not installed on the management server:

   ```
   directory-where-utility.tar-is-extracted/utility/lib/openssl/bin/openssl x509 -text -in full-path-of-the-certificate-file
   ```

Configuring SSL server settings (SSL Setup tool)

Use the SSL Setup tool to specify the server certificate and the private key for the Hitachi Ops Center products on the management server.

> **Note:** When configuring SSL server settings on multiple management servers, use the SSL Setup tool on each management server.

Procedure

1. Log in to the management server as the root user.

   If you log in as an ordinary user, use the **`sudo`** command to complete the following procedure as the root user.
2. Run the **`cssslsetup`** command, which is in the following location:

If Common Services is installed on the management server:

installation-directory-of-Common-Services/utility/bin

If Common Services is not installed on the management server:

directory-where-utility.tar-is-extracted/utility/bin

The main menu is displayed:

```
Main menu   Ver:cssslsetup-command-version
1. Create certificate signing request and private key.
2. Set up SSL server.
3. Set up SSL client.
4. Enable/disable certificate verification(optional).
5. Restart services for each product.
Enter a number or q to quit:
```

3. Enter **2**.

   A list of installed products appears.
4. Specify the target products for which you want to configure the SSL server.

   Use commas to specify multiple products.
5. Enter an absolute path to the file where the shared private key is located.
6. Enter an absolute path to the file where the shared server certificate is located.
7. Specify whether the server certificate specified is issued by an intermediate certificate authority.

   > **Note:** If you specified a server certificate issued by an intermediate certificate authority, create a certificate file by appending -chained to the file name. Do not delete this file.
8. If you specified yes in step 7, specify the absolute path of the certificate of the intermediate certificate authority.
9. To specify settings for Analyzer detail view, Analyzer probe server, or API Configuration Manager, use an absolute path for the root certificate of the server certificate for use with all Hitachi Ops Center products.
10. In the following cases, enter the host name specified when creating the CSR.
    - If you specify settings for Automator
    - If you specify settings for Analyzer
    - If you specify settings for the RAID Agent on the Analyzer probe server
11. To specify settings for Administrator, enter the port number.
12. To specify settings for Administrator, enter the Virtual Appliance Manager credentials.

    The default credentials of the Virtual Appliance Manager are described in the *Hitachi Ops Center Administrator Getting Started Guide*.
13. To specify settings for Analyzer detail view or Analyzer probe server, enter a common password for the truststore, keystore, and key manager.
14. To specify settings for real time data collection of Analyzer detail view, select **1. Yes**.

a. To specify settings, enter a common password for the truststore and keystore.

   The default password is `changeit`. To set a password other than `changeit`, in the following step, select **1. Yes**.

b. When entering the password, if you entered a password other than the default, select **1. Yes**.

   If you selected **1. Yes**, in order to set the password, real time data collection services of Analyzer detail view will be stopped.

15. In the following cases, when ECC encryption certificate settings are enabled, specify whether to leave these settings enabled.

- If you specify settings for Automator
- If you specify settings for Analyzer
- If you specify settings for the RAID Agent on the Analyzer probe server

16. If you specify settings for the Analyzer Virtual Storage Software Agent, import the server certificate to be shared.

a. Specify an absolute path to the file where the keystore that imports the server certificate is located.

b. Specify the password for the keystore.

c. Enter the alias name (server identification name).

17. To implement the SSL server settings, enter **1. Yes**.

After the settings are implemented, a message is displayed and the main menu reappears.

18. Enter **5** to restart the services for each product.

> **Note:** If you want to use the real time data collection of Analyzer detail view, restart the Analyzer detail view services. You must also configure the SSL client settings for the Analyzer probe server. For details, see the Configuring SSL client settings and enabling certificate verification (SSL Setup tool) (on page 86).

Configuring SSL server settings for an Active Directory or LDAP server

To use LDAPS for communication with an Active Directory or LDAP server, configure SSL server settings on the Active Directory or LDAP server. For details on how to configure these settings, see the Active Directory or LDAP server documentation.

Configuring SSL communication settings for an identity provider server

To link with an identity provider, configure SSL communication settings on the identity provider server. For details on how to configure these settings, see the identity provider documentation.

> **Note:** If you want to use the Relying Party Trust Monitoring function of AD FS, import the root certificate of the certificate authority that signed the Common Services server certificate into the Trusted Root Certification Authorities Certificate Store of the AD FS server.

Configuring SSL client settings and enabling certificate verification (SSL Setup tool)

Use the SSL Setup tool to configure the required SSL client settings on the management server and enable certificate verification.

> **Note:** When configuring SSL client settings on multiple management servers, use the SSL Setup tool on each management server.

Before you begin

- To configure real time data collection for the Analyzer probe server, create the `client.truststore.jks` file on the Analyzer detail view server in advance, and then copy it to `/usr/local/megha/conf/kafka` on the Analyzer probe server. For details, see the Analyzer manual.
- To configure SSL communications between the RAID Agent on the Analyzer probe server and your storage systems, create an instance environment in advance. For details, see the Analyzer manual.

Procedure

1. Log in to the management server as the root user.

   If you log in as an ordinary user, use the **`sudo`** command to complete the following procedure as the root user.
2. Run the **`cssslsetup`** command, which is in the following location:

   If Common Services is installed on the management server:

   `*installation-directory-of-Common-Services*/utility/bin`

   If Common Services is not installed on the management server:

   `*directory-where-utility.tar-is-extracted*/utility/bin`

   The main menu is displayed:

   ```
   Main menu   Ver:cssslsetup-command-version
   1. Create certificate signing request and private key.
   2. Set up SSL server.
   3. Set up SSL client.
   4. Enable/disable certificate verification(optional).
   5. Restart services for each product.
   Enter a number or q to quit:
   ```
3. Enter **3**.

4. Specify the target products for which you want to configure SSL client settings.

   Use commas to specify multiple products.
5. Import the root certificate for common use.

   If you only want to configure the settings for linking with Active Directory, LDAP, or an identity provider server, press **Enter** without specifying anything.

   Note: You must import the root certificate of the server certificate for Common Services.

   a. Specify an absolute path to the file where the root certificate is located.
   b. When the truststore file name is displayed, enter the truststore password. However, the truststore file name is not displayed for Analyzer viewpoint.
   c. Enter the alias name (server identification name).

      If you specify an alias name that is already used for the truststore, you are asked whether you want to re-register the alias name. Alias names are not case-sensitive. Run the following command to verify the alias name:

      ```
      keytool -v -list -keystore path-to-truststore-file
      ```
6. Import the server certificate or the root certificate of the product that establishes SSL communication with the Analyzer probe server.
   a. Specify an absolute path to the file where the server certificate or the root certificate of the target product is located.
   b. When the truststore file name is displayed, enter the truststore password.
   c. Enter the alias name (server identification name).

      If you specify an alias name that is already used for the truststore, you are asked whether you want to re-register the alias name. Alias names are not case-sensitive. Run the following command to verify the alias name:

      ```
      keytool -v -list -keystore path-to-truststore-file
      ```
   d. If you have other certificates to import, enter **1. Yes**. If not, enter **2. No**.
   e. Repeat this procedure until you finish importing all certificates for products that require SSL communications. For the second time and later, you do not need to enter the truststore password.
7. If you are configuring settings for Analyzer Virtual Storage Software Agent, import the root certificate of VSP One SDS Block.
   a. Specify an absolute path to the file where the root certificate of VSP One SDS Block is located.
   b. When the truststore file name is displayed, enter the truststore password.
   c. Enter the alias name (server identification name).

      If you specify an alias name that is already used for the truststore, you are asked whether you want to re-register the alias name. Alias names are not case-sensitive. Run the following command to verify the alias name:

      ```
      keytool -v -list -keystore path-to-truststore-file
      ```

8. If you want to link with Active Directory, LDAP, or an identity provider server, import the certificate associated with the server.

   a. Enter, as an absolute path, the file name of the certificate for the Active Directory, LDAP, or identity provider server.

      If you do not want to link with Active Directory, LDAP, or identity provider server, just press **Enter**.

   b. When the truststore file name is displayed, enter the truststore password.

   c. Enter the alias name (server identification name).

      If you specify an alias name that is already used for the truststore, you are asked whether you want to re-register the alias name. Alias names are not case-sensitive. Run the following command to verify the alias name:

      ```
      keytool -v -list -keystore path-to-truststore-file
      ```

9. For API Configuration Manager, configure SSL communications with your storage systems.

   a. If you want to configure SSL communications, enter **1. Yes**.

   b. Enter the storage device ID of the target storage system and use an absolute path for the server certificate.

   c. To configure SSL communications for additional storage systems, enter **1. Yes**. If not, enter **2. No**.

   d. Repeat this procedure until you finish registering all your storage systems.

10. If you use the on-demand real time monitoring of Analyzer detail view, configure SSL communications for the Analyzer detail view server and the RAID Agent server.

    To configure the settings, perform the following steps:

    a. Enter **1. Yes**.

    b. When the truststore file name is displayed, specify the truststore password.

    c. Enter the alias name (server identification name).

       If you specify an alias name that is already used for the truststore, you are asked whether you want to re-register the alias name. Alias names are not case-sensitive. Run the following command to verify the alias name:

       ```
       keytool -v -list -keystore path-to-truststore-file
       ```

    d. Enter the file name of the server certificate of the target RAID Agent server by using the absolute path.

    e. To configure SSL communications for an additional RAID Agent server, enter **1. Yes**. If not, enter **2. No**.

    f. Repeat this procedure until you finish registering all your RAID Agent servers.

11. Configure SSL communications between the RAID Agent on the Analyzer probe server and your storage systems. Create a truststore for the instance environment of the RAID Agent, and then import the storage system certificates into the truststore.

    a. Select the instance environment to configure.

       To specify multiple instance environments, separate the instance environments with commas.

> **Note:** If a truststore file already exists, it is deleted and a new truststore file is created.

   b. When the truststore name for the instance environment is displayed, enter the file name of the storage system certificate to be imported by using the absolute path.

   c. Enter the truststore password.

   d. Enter the alias name (server identification name).

   e. If you selected multiple instance environments, repeat this procedure for each instance environment until you finish importing all the certificates.

12. If you are configuring real time data collection for the Analyzer probe server, enter **1. Yes**.
13. Specify whether to enable certificate verification.

    > **Note:** If you want to enable certificate verification, you must import the certificate. Perform steps 5 to 12.
    >
    > Even if you disable certificate verification, if you are using Common Services to link with Active Directory, an LDAP, or an identity provider server, you must import the root certificate of the server to which you are linking to perform authentication.

14. To implement the SSL client settings, enter **1. Yes**.

    After the settings are implemented, a message is displayed and the main menu reappears.

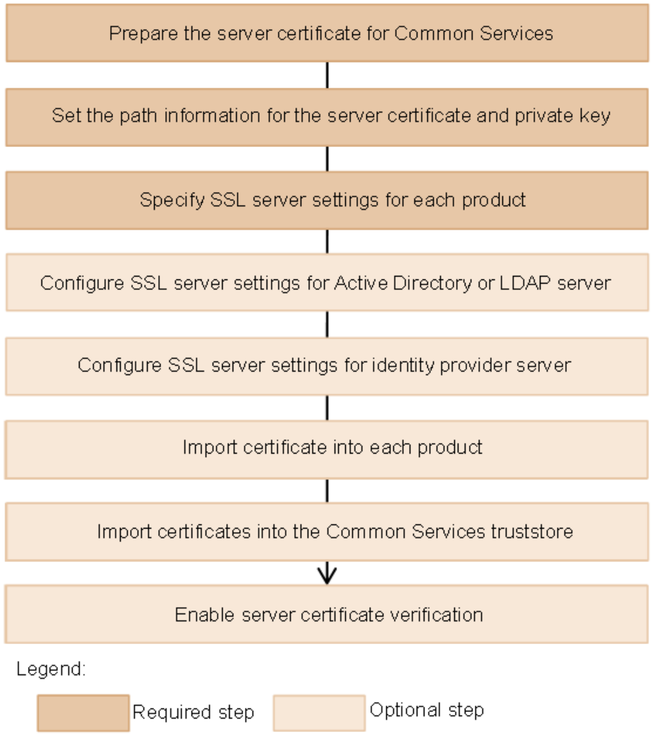
15. Enter **5** to restart the services for each product.

Result

The SSL communication configuration is complete.

Configuring SSL communications without using the SSL Setup tool

The following figure shows the workflow for configuring SSL communications without using the SSL Setup tool:


Prepare the server certificate for Common Services
Set the path information for the server certificate and private key
Specify SSL server settings for each product
Configure SSL server settings for Active Directory or LDAP server
Configure SSL server settings for identity provider server
Import certificate into each product
Import certificates into the Common Services truststore
Enable server certificate verification
Legend:
Required step
Optional step

Preparing the server certificate for Common Services

Prepare the server certificate for Common Services. Make sure the certificate has not expired. For details on how to check this, see Checking the validity period of the server certificate (on page 153). Common Services supports both RSA and Elliptic Curve Digital Signature Algorithm (ECDSA). You cannot configure ECDSA alone. Prepare secret keys and server certificates for RSA only or for both RSA and ECDSA.

Procedure

1. Log in to the management server as the root user.

   If you log in as an ordinary user, use the **sudo** command to complete the following procedure as the root user.
2. Run the following command to create a private key (in X.509 PEM format) and a certificate signing request (CSR).

   > **Note:** When you use the certificate for enabling SSL encryption for real time data collection in the Analyzer detail view server, enter the IP address of SubjectAltName and issue a certificate that includes the IP address specified in the SubjectAltName field.

   Example of the command for RSA:

   ```
   installation-directory-of-Common-Services/openssl/bin/openssl req -new -
   newkey rsa:4096 -nodes -keyout privateRSA.pem -sha256 -out serverRSA.csr -
   subj "/C=ww/ST=xx/L=yy/O=zz/CN=host-name-or-IP-address" -addext
   'subjectAltName = {DNS:host-name|IP:IP-address|DNS:host-name,IP:IP-
   ```

```
address}' -config installation-directory-of-Common-Services/openssl/
openssl.cnf
```

Example of the command for ECDSA:

```
installation-directory-of-Common-Services/openssl/bin/openssl req -new -
newkey ec:<(installation-directory-of-Common-Services/openssl/bin/openssl
ecparam -name secp384r1) -nodes -keyout privateECDSA.pem -sha256 -out
serverECDSA.csr -subj "/C=ww/ST=xx/L=yy/O=zz/CN=host-name-or-IP-address" -
addext 'subjectAltName = {DNS:host-name|IP:IP-address|DNS:host-name,IP:IP-
address}' -config installation-directory-of-Common-Services/openssl/
openssl.cnf
```

When running the command, specify parameters according to the Cipher Suite supported by Common Services. For details on the Cipher Suite supported by Common Services, see the Hitachi Ops Center Release Notes.

Specify `/C=`*`ww`*`/ST=`*`xx`*`/L=`*`yy`*`/O=`*`zz`* according to your environment. For `CN`, specify a host name (or FQDN) or IP address that can be used to access the Hitachi Ops Center Portal.

If you specify a host name for `CN`, specify `DNS:`*`host-name`* for `subjectAltName`. If you specify an IP address for `CN`, specify `IP:`*`IP-address`* for `subjectAltName`. If you specify a host name for `CN`, and specify that an IP address can also be used to access the Hitachi Ops Center Portal, specify `DNS:`*`host-name`*`,IP:`*`IP-address`* for `subjectAltName`.

To create a CSR by using the **`openssl`** command in the Common Services installation directory, you must specify the `-config` option to load the settings file.

3. Run the following command to check the results of creating the CSR:

```
installation-directory-of-Common-Services/openssl/bin/openssl req -text -in CSR-
file -config installation-directory-of-Common-Services/openssl/openssl.cnf
```

4. Access the CSR from the directory that you specified when creating the request and submit the CSR to the certificate authority requesting that they issue a signed certificate.

   For details, follow the procedure provided by the certificate authority.

5. After obtaining a server certificate signed by the certificate authority, run the following command to check the results of creating the server certificate:

```
installation-directory-of-Common-Services/openssl/bin/openssl x509 -text -in
server-certificate-signed-by-certificate-authority
```

Setting the path information for the server certificate and private key

In the Common Services properties file, specify the settings for the signed server certificate obtained from the certificate authority and the settings for the private key.

Before you begin

Concatenate the signed server certificate obtained from the certificate authority and the certificate from the intermediate certificate authority into a single file as follows. If there are multiple certificates from intermediate certificate authorities, concatenate all certificates in a chain.

```
awk 1 server-certificate-signed-by-certificate-authority certificate-from-an-
intermediate-certificate-authority [certificate-from-an-intermediate-certificate-
authority ...] > chained-server-certificate
```

Procedure

1. Log in to the management server as the root user.

   If you log in as an ordinary user, use the **`sudo`** command to complete the following procedure as the root user.
2. Transfer the signed server certificate obtained from the certificate authority and the private key to the management server in a secure manner.
3. Store the server certificate and the private key in the following location:

   ```
   /var/installation-directory-of-Common-Services/tls/
   ```

   For example, for an OVA install uses the following directory:

   ```
   /var/opt/hitachi/CommonService/tls/
   ```
4. In the following properties file, specify the absolute paths to the server certificate file and private key file, and then save the file.

   Properties file location

   ```
   /var/installation-directory-of-Common-Services/userconf/
   config_user.properties
   ```

   For example, for an OVA install uses the following file:

   ```
   /var/opt/hitachi/CommonService/userconf/
   config_user.properties
   ```

   Settings

   - RSA settings:

     ```
     CS_GW_SSL_CERTIFICATE=absolute-path-of-the-certificate-(RSA)-file
     CS_GW_SSL_CERTIFICATE_KEY=absolute-path-of-the-private-key-(RSA)-file
     ```

   - ECDSA settings:

     ```
     CS_GW_SSL_CERTIFICATE_ECDSA=absolute-path-of-the-certificate-(ECDSA)-
     file
     CS_GW_SSL_CERTIFICATE_KEY_ECDSA=absolute-path-of-the-private-key-
     (ECDSA)-file
     ```
5. If this is the first time configuring SSL, restart the Common Services service.

Note: In an environment where SSL communication settings have already been configured, if you want to change the settings in `config_user.properties` by adding ECDSA settings or reissuing a server certificate, complete the following procedures to configure SSL communication by configuring the settings for each product and Common Services, and then restarting the Common Services service. If you restart the Common Services service before configuring the settings, a communication error might occur.

Specifying SSL server settings for each product

Configure SSL communications for each product that links with Common Services. As you did with Common Services, you must prepare the signed certificate from the certificate authority, and specify the SSL server settings.

For details on how to specify the SSL server settings, see the documentation for each product.

Configuring SSL server settings for an Active Directory or LDAP server

To use LDAPS for communication with an Active Directory or LDAP server, configure SSL server settings on the Active Directory or LDAP server. For details on how to configure these settings, see the Active Directory or LDAP server documentation.

Configuring SSL communication settings for an identity provider server

To link with an identity provider, configure SSL communication settings on the identity provider server. For details on how to configure these settings, see the identity provider documentation.

Note: If you want to use the Relying Party Trust Monitoring function of AD FS, import the root certificate of the certificate authority that signed the Common Services server certificate into the Trusted Root Certification Authorities Certificate Store of the AD FS server.

Importing certificates into each product

Import the root certificate of the server certificate for Common Services into each product that links with Common Services. In addition, if you import the Common Services metadata into an identity provider over the network when linking with an identity provider, import the root certificate of the server certificate for Common Services into the identity provider server. In some cases, the certificate might already be imported.

For details on how to import a certificate, see the documentation for each product.

Importing certificates into the Common Services truststore

Import the root certificate of the server certificate for Common Services and for each product into the Common Services truststore. If the system is linked with an Active Directory, LDAP, or identity provider server, you can also import the root certificates of these server certificates.

Before you begin

Transfer the certificates to the management server in a secure manner.

Procedure

1. Log in to the management server as the root user.

   If you log in as an ordinary user, use the **`sudo`** command to complete the following procedure as the root user.
2. Run the following command to import the root certificate of the server certificate for Common Services into the truststore.

   In some cases, the certificate might already be imported.

   Format

   ```
   keytool -importcert -alias alias-name -keystore path-to-truststore-file -
   file path-of-the-certificate-to-be-imported
   ```

   Options

   `-alias` ***`alias-name`***

   Specify the name so that the certificate can be identified in the truststore.

   `-keystore` ***`path-to-truststore-file`***

   Specify the following absolute path as the path to the truststore file:

   `/var/`*`installation-directory-of-Common-Services`*`/tls/cacerts`

   For example, for an OVA install uses the following file:

   `/var/opt/hitachi/CommonService/tls/cacerts`

   Note: When you run the command, you will be asked to enter a password. The default password for the truststore is `changeit`. We recommend that you change the password.

   `-file` ***`path-of-the-certificate-to-be-imported`***

   Specify the absolute path of the certificate to import.
3. In the same way, import the root certificate of the server certificate for each product into the truststore.
4. When you use LDAPS for communication with the Active Directory or LDAP server, import the root certificate of the server certificate for the Active Directory or LDAP server.
5. If you link Common Services with an identity provider, import the root certificate of the server certificate for the identity provider server.

6. Restart the Common Services service and the services for each product.

   For details on how to restart the Common Services service, see Starting or stopping the Common Services service (on page 152). For details on how to restart the service of each product, see the documentation for each product.

Enabling server certificate verification

After the initial installation of Common Services, there is no verification for server certificates from communication partners when Common Services is the SSL client. Therefore, to strengthen security, enable certificate verification immediately so that all server certificates are verified and your environment is protected from threats such as spoofing.

Procedure

1. Log in to the management server as the root user.

   If you log in as an ordinary user, use the **`sudo`** command to complete the following procedure as the root user.
2. Change the following property file to enable server certificate verification:

   Property file location

   `/var/`*`installation-directory-of-Common-Services`*`/userconf/config_user.properties`

   For example, for an OVA install uses the following file:

   `/var/opt/hitachi/CommonService/userconf/config_user.properties`

   Setting

   ```
   CS_PORTAL_SSL_CERTIFICATE_CHECK=true
   ```
3. Restart the Common Services service.

Result

The SSL communication configuration is complete.

Chapter 6: Initial setup using the Hitachi Ops Center Portal

After installing the Hitachi Ops Center products, apply the licenses for each product, and then complete the required configuration, such as creating users and user groups for controlling access.

Initial setup workflow

If you used the OVA to deploy a Hitachi Ops Center product or used an installer to perform a new installation, log in to the Hitachi Ops Center Portal, and then configure the settings described in the following section.

> **Note:** If you perform an upgrade installation, the previous settings are inherited.

1. Log in to the portal as described in Logging in to the Hitachi Ops Center Portal (on page 97).
2. Apply Hitachi Ops Center product licenses as described in Applying Ops Center product licenses (on page 98).

   You must apply the product licenses before using the products.
3. (Optional) Link with an Active Directory, LDAP, or identity provider server.

   For details, see the following topics:

   - Configuring a link to an Active Directory or LDAP server (on page 107)
   - Configuring a link to an AD FS identity provider (on page 116)
   - Configuring a link to a non-AD FS identity provider (on page 136)
4. (Optional) Configure the following settings as needed:

   - Changing the password policy (on page 104)

     Based on your security requirements, you can configure user account password complexity and controls for locking user accounts after consecutive failed authentication attempts.
   - Adding a login warning banner for the Ops Center Portal (on page 106)

     You can display a message in the login window of the Hitachi Ops Center Portal.
5. Control access by Managing local users and groups (on page 98).

   You must configure access control to the Hitachi Ops Center Portal and Hitachi Ops Center products by creating users and configuring settings for user groups.

6. (Optional) Linking with Hitachi Remote Ops (on page 217)

   By linking with Hitachi Remote Ops, when an error occurs in a Hitachi Ops Center product, log files are automatically collected and sent to support personnel.

Logging in to the Hitachi Ops Center Portal

Log in to the Hitachi Ops Center Portal from your browser.

Before you begin

To avoid issues with windows not displaying correctly, configure your browser settings as follows:

- Accept cookies, or register the portal URL as a trusted site.
- Enable active scripting in the security settings.

Procedure

1. In a web browser, access the following URL:

   `https://`*`host-name-or-IP-address-of-Portal`*`:`*`port-number`*`/portal`

   When entering the URL to access the portal, enter the host name or IP address and the port number that were specified during installation.

   The default port number is 443.

   Tip: If you used the OVA to deploy Hitachi Ops Center products, you can access the Hitachi Ops Center Portal by using both the host name and IP address by default. To change the settings so that users can only access the Hitachi Ops Center Portal by using the host name, or to change the host name or IP address used to access the Hitachi Ops Center Portal, use the **`cschgconnect`** command. For details, see Changing the management server host name, IP address, or port number (on page 159).

2. Use the built-in account to log in:

   If you are logging in for the first time, use the following user ID and password:

   User name: `sysadmin`

   Password: `sysadmin`

   If the Change password window is displayed, enter a new password and then click **Submit**.

   If the login is successful, the Hitachi Ops Center Portal main window opens.

   Note: If you want to log in to the Portal by using the IP address, specify the settings so that the management server host name can also be resolved from client machines.

Applying Ops Center product licenses

You must apply Hitachi Ops Center product licenses before use.

Procedure

1. Log in to the Ops Center portal as `sysadmin` or a user with opscenter-administrators membership.
2. From the navigation bar, click **Inventory**.
3. In the **Inventory** window, find products with a status of **License Not Activated** or **License Warning**.
4. Click the status link to access the **License** window for the product.
5. Apply the license, and then verify that the status has changed to **Ready**.

Managing local users and groups

Local refers to user accounts and groups that are created and managed by Ops Center instead of an Active Directory or LDAP server.

Creating and editing Ops Center user accounts

You can create user accounts in Hitachi Ops Center.

Procedure

1. Log in to the Ops Center portal as `sysadmin` or a user with opscenter-administrators membership.
2. From the navigation bar, click **Manage users** and select **Users** from the Asset type list.

   To change a user account, locate the entry and then click the edit (pencil) icon. You can view the details of an account by clicking on the name.
3. In the **Users** window, click **+**.
4. Provide the account information and then click **Submit**.

   The **Change password** window opens.
5. Enter a password, confirm it, and then click **Submit**

Changing a local user password

You can change the passwords for Ops Center portal users.

> **Note:**
>
> - Local users can change their own passwords by clicking the User icon in the upper-right corner and selecting Profile > Password. (The Profile menu is not available for external identity provider users, Active Directory users, or LDAP users.)
> - External identity provider users, Active Directory users, and LDAP users do not include the lock or edit icons.

Procedure

1. Log in to the Ops Center portal as `sysadmin` or a user with opscenter-administrators membership.
2. From the navigation bar, click **Manage users** and select **Users** from the Asset type list.
3. In the **Users** window, locate the entry and then click the **Change password** icon (lock) associated with the user account.
4. Enter the new password, confirm it, and then click **Submit**.

Adding Ops Center groups

You can create a maximum of 100 groups of Hitachi Ops Center users.

> **Note:** Ops Center has two built-in groups that control access to portal functions: opscenter-users and opscenter-administrators. See Assigning privileges to local (non-AD) Ops Center users (on page 105) for details.

Procedure

1. Log in to the Ops Center portal as `sysadmin` or a user with opscenter-administrators membership.
2. From the navigation bar, click **Manage users** and select **Groups** from the Asset type list.

   To change the group name or description, click the edit (pencil) icon. You can view the details of a group by clicking on the name.
3. In the **Groups** window, click **+**.
4. Provide a name and description, and then click **Submit** or **Submit and add another group**.
5. You can assign roles to a group by clicking the icon.

   All groups are automatically assigned the opscenter-user role. You can also can also assign opscenter-system-administrator or opscenter-security-administrator roles. See Assigning portal-level roles to Ops Center groups (on page 100) for details.

Ops Center roles (privileges)

Rather than use a single `sysadmin` account to administer Ops Center, you can assign local users to a group that has administrative privileges. For Active Directory users, you can assign appropriate roles to the group. For local users only, the built-in opscenter-administrators group grants full administrative privileges.

The portal has two types of roles (also known as privileges):

- **Portal-level:** global roles that control access to functions within the Ops Center portal. The opscenter-user role permits users to log in to the Ops Center portal and access the Inventory tab. The opscenter-system-administrator role permits users to access all the portal tabs and create local users, add groups, and assign roles (even at the product-level). This role should not be assigned lightly.
- **Product-level:** roles specific to each product. For example, Administrator has roles called StorageAdministrator, SystemAdministrator, and SecurityAdministrator that control access to different functions in the Administrator UI. Members of the local opscenter-administrators group have default roles assigned that permit access to all Ops Center products.

Assigning portal-level roles to Ops Center groups

As an alternative to using the built-in local opscenter-administrators group, you can assign portal-level roles to local and Active Directory groups.

Before you begin

Note: Local users are automatically members of the opscenter-users group. By default, Active Directory users who are under the Base DN but not members a group are not allowed to log in to the portal. (This is controlled by the Add all users under Base DN to opscenter-users group option described in Configuring Active Directory as a directory service for Ops Center (on page 107).) Instead, only AD group users are allowed to log in (because they are assigned the opscenter-user role).

Procedure

1. Log in to the Ops Center portal as `sysadmin` or a user with opscenter-administrators membership.
2. From the navigation bar, click **Manage users** and select **Groups** from the Asset type list.
3. In the **Groups** window, find the entry for the group and then click the role (profile with star) icon.

   You can assign the following roles:

   opscenter-user

   The default role assigned to users that grants access to the Ops Center portal. These users can start products, but they cannot view other users or groups, add products, or change portal settings.

opscenter-system-administrator

Manage portal users, groups, product registration, user federation (Active Directory/LDAP), and access all admin functions within the component products.

opscenter-security-administrator

Similar to the system-administrator role, except that it does not grant full access to admin functions within the component products. Instead, this role grants access to the **Access product-level roles** link in the **Inventory** tab. This controls the mapping of component-level roles to the roles defined in the Ops Center portal. For example, a member of a group with the opscenter-security-administrator role connecting to Automator will only see the **Administration** tab with Resources and Permissions; none of the other Administration categories (or other dashboard tabs) are visible.

4. From the **Available roles** list, select the role you want to assign and then click the left arrow. To remove a role from a group, select the role from the **Assigned roles** list and then click the right arrow.
5. When you are finished, click < in the upper left corner of the window to return to the list of groups.

Assigning product-level roles from the Ops Center portal

Because each Ops Center product includes a unique set of roles or permissions that determine what users can do within each product UI, the portal includes a direct link to access these roles and associate them with groups.

To simplify the process of assigning roles associated with each product, the Ops Center portal includes links for each entry in the Inventory tab. The Access product-level roles link takes you directly to the product window where roles are assigned or access to resources is configured. Where applicable, defaults are pre-assigned to members of the opscenter-administrators group (local only). You can also use this link to assign product-level roles to local and AD groups.

Note: Ops Center includes a special role, opscenter-security-administrator, that gives a user or group access to the Access product-level roles link (without access to any other admin functions). See Assigning portal-level roles to Ops Center groups (on page 100) for details.

Ops Center Product	Destination of "Access product-level role" link	Default roles assigned to opscenter-administrators group
Administrator	Dashboard > Security Settings	StorageAdministrator, SystemAdministrator, SecurityAdministrator
Analyzer	Administration > User Group Management > User Groups and Permissions	Admin, Modify, StorageOps

Ops Center Product	Destination of "Access product-level role" link	Default roles assigned to opscenter-administrators group
Analyzer detail view	Manage > Administration > Manage Ops Center Groups and Roles	Normal, Admin
Analyzer probe	The Admin role is assigned automatically; no action is necessary.	Admin
Analyzer viewpoint	Configuration > Users	Admin
Automator	The link opens the Administration tab. Select User Groups under Resources and Permissions.	Admin, plus access to all service groups
Protector	Dashboard > Access Control	Protector Admin (assigned under ACP Association "opscenter Administrators")

Procedure

1. Log in to the Ops Center portal as `sysadmin` or a user with opscenter-administrators membership.
2. From the navigation bar, click **Inventory**.
3. Click the **Access product-level roles** link for the product.
4. See the procedures that follow for the product you selected.

For Administrator

Procedure

1. In the Ops Center **Security Management** window, enter the group name and select it.
2. Select the permissions to be assigned and then click **Submit**.

For Analyzer

Procedure

1. In the **Administration** window, click **User Groups and Permissions** under **User Group Management**.
2. Select the group name and then click **Edit Permission Mapping**.
3. In the "Edit User Groups" section, select all permissions and then click **OK**.

For Analyzer detail view

Before you begin

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

Procedure

1. Log in to the Ops Center portal with a user which belongs to the administrator group (for example opscenter-administrators) and then start Analyzer detail view.
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**.

For Analyzer viewpoint

Before you begin

Make sure that Analyzer viewpoint is registered with Common Services.

Procedure

1. Log in to the Ops Center portal with a user which belongs to the administrator group (for example opscenter-administrators) and then start Analyzer viewpoint.
2. Select **Users** from the **Configuration** menu.
3. In the **Role** column for the login, select **Admin**.

For Automator

Procedure

1. In the **Administration** window, click **User Groups** under **Resources and Permissions**.
2. Select the group and then click **Assign** under "Service Groups."
3. Select "All Service Groups" and then click **Add** to move it to "Assigned Service Groups."
4. Change the Role from **Submit** to **Admin** and then click **OK**.

For Protector

Instead of assigning a role to a group, you must create an association that connects a group with a profile (that has a defined role and access to resources).

Procedure

1. In the **Access Control** window, click **Manage ACP Associations**.
2. Click the plus (**+**) icon.
3. Enter a name for the association and then click **Next**.
4. Select **Group**, and then select "opscenter" from the **Space** list.
5. Click **Browse** and select the Group Name.

6. Click **Next**.
7. Click a profile under "Available Profiles" to add it to "Selected Profiles."
8. Click **Finish**.

Controlling local portal access

You can configure the security settings that are applied when a local user logs in, controlling access to the Hitachi Ops Center portal with the following settings:

- Password requirements
- Account lock settings
- User groups
- Login banner

Changing the password policy

You can set restrictions (such as password length and valid characters) on the passwords for login accounts.

Procedure

1. Log in to the Ops Center portal as `sysadmin` or a user with opscenter-administrators membership.
2. Click the **Settings** (gear) icon in the upper right corner and select **Password Policy**.

   The following table describes the password controls. For best results, change the default values to be more restrictive.

Item	Description	Default value
Minimum length	Minimum length of a password (1-256).	12
Uppercase characters	Minimum number of uppercase alphabetic characters (0-256).	1
Lowercase characters	Minimum number of lowercase alphabetic characters (0-256).	1
Digits	Minimum number of numeric characters (0-256).	1
Special characters	Minimum number of symbols (0-256).	1

Item	Description	Default value
	The following symbols can be used: !, #, $, %, &, ', (,), *, +, -, ., =, @, \, ^, _, |	
Brute force prevention	Limits the number of unsuccessful login attempts (to prevent so-called brute force attacks). Click **Enable** and enter a **Max Login Failures** value to specify the number of login attempts permitted before an account is automatically locked (1-256).	Enabled

3. Click **Submit** when the changes are complete.

Assigning privileges to local (non-AD) Ops Center users

You can assign administrative privileges by adding local users to the opscenter-administrators group.

Note: This procedure is for accounts created locally in the Ops Center portal and does not apply to Active Directory users.

The following default groups are available:

opscenter-users

The default group assigned to users that grants access to the Ops Center portal. These users can start products, but they cannot view other users or groups, add products, or change portal settings.

opscenter-administrators

Members of the this group can access all portal management functions in the Ops Center, including managing users, groups, or products, and changing portal settings.

support-services

This group is for support services and will not be used without the customer's permission.

If you use this group for support services, note the following:

- External authentication users cannot be assigned to this group.
- Local users assigned to this group cannot be assigned to any other group.
- Do not assign product-level roles to this group.

You can also assign special privileges (roles) to a group that you have created. See Assigning portal-level roles to Ops Center groups (on page 100) for details.

Procedure

1. Log in to the Ops Center portal as `sysadmin` or a user with opscenter-administrators membership.
2. From the navigation bar, click **Manage users** and select **Users** from the Asset type list.
3. Click the 👥 icon for the user account. (Use the search box if the user account is not visible.)

   The group selection window appears.
4. From the **Available Groups** list, select the group you want to assign and then click the left arrow. To remove a user from a group, select the group from the **Group Membership** list and then click the right arrow.
5. When you are finished, click < in the upper left corner of the window to return to the list of users.

Enabling or disabling login accounts

You can disable accounts to prevent them from being used and enable accounts that have been locked.

Procedure

1. Log in to the Ops Center portal as `sysadmin` or a user with opscenter-administrators membership.
2. From the navigation bar, click **Manage users** and select **Users** from the Asset type list.
3. Locate the user account that you want to enable or disable in the **Users** window and then click the **Edit User** icon.
4. Click **Disable** or **Enable**, and then click **Submit**.

Adding a login warning banner for the Ops Center Portal

You can add a warning banner to display information about system access on the portal login page.

Procedure

1. Log in to the Ops Center portal as `sysadmin` or a user with opscenter-administrators membership.
2. Click the **Settings** icon and select **Warning banner**.
3. You can customize the default message or compose a new one. Click **Submit** when the changes are complete.

Chapter 7: Configuring a link to an Active Directory or LDAP server

By linking Hitachi Ops Center with an external Active Directory or LDAP server, you can perform centralized user authentication on the Active Directory or LDAP server. To link with an Active Directory or LDAP server, configure the settings on the Hitachi Ops Center Portal.

Configuring Active Directory as a directory service for Ops Center

You can add a directory service and configure authentication for the Ops Center portal so that AD groups can access portal functions and products with a single sign-in.

Before you begin

- For LDAP configurations, verify you completed the procedure described in Importing certificates into the Common Services truststore (on page 94).
- For Kerberos configurations, see Setting up Kerberos authentication for Ops Center (on page 110) before following this procedure.

About using multiple Active Directory servers

- You can configure a maximum of four Active Directory servers.
- The Users screen of the Ops Center portal is designed to display up to 200 users. If the total number of local users and Active Directory users exceeds 200, the excess users will be able to log in to Ops Center, but will not be displayed on the Users screen.
- User names and email addresses must be unique and not duplicated across multiple Active Directory servers.
- If the BIND password is invalid on one of several Active Directory servers registered with Common Services, or if a connection cannot be made to an Active Directory server, the following operations are not possible:
  - Create new local user
  - Display local user list
  - Update user profile

Note: Whenever you make changes to existing Active Directory settings, you must do the following:

- Click Sync groups to apply the changes to Active Directory groups configured in Ops Center.
- Click Test connection and Test authentication.

If any errors are reported, confirm the changes are valid.

Procedure

1. Log in to the Ops Center portal as `sysadmin` or a user with opscenter-administrators membership.
2. From the navigation bar, click **Manage users** and select **User directories** from the Asset type list.
3. Click the **+** (plus) icon.

   The **Add user directory service** window opens.
4. Enter a name for the service.
5. Select **Active directory** for the **Directory service** type.
6. Select the **Authentication protocol**.

   LDAP is the default protocol. If you choose **Kerberos**, select the **Realm** name from the displayed list.
7. Enter the **Connection URL** (for example: `ldaps://ldaps.example.com`) and then click **Test connection**.

   Note: Specify the same host name as the CN or SANs in the Active Directory server certificate.
8. Enter the **BIND user DN** (for example: `CN=bind-user,OU=foo,OU=bar,DC=example,DC=com`) and the password and then click **Test authentication**.

   Note: The BIND User DN only requires read permissions (not admin or modify).
9. Enter the **Base DN** (for example: `OU=foo,OU=bar,DC=example,DC=com`).

   Note: To have portal access, users must be included in the subtree of the DN specified in the Base DN.
10. You can import a maximum of 100 AD users. Click **Pre-check the number of imported users**. If you exceed this limit, you can decrease the number of users to be imported by using a **Custom user LDAP filter**. For best results, use a filter to specify a user or group. Here are some examples:

    Note: The following search conditions are set automatically and cannot be changed:

    ```
    objectclass="person,organizationalPerson,user"
    scope=2(subtree)
    ```

To select the sAMAccountName `t_brady`:

```
(sAMAccountName=t_brady)
```

To select multiple sAMAccountName instances:

```
(|(sAMAccountName=t_brady)(sAMAccountName=p_manning)(sAMAccountName=a_rodgers))
```

To select users belonging to `group1`:

```
(memberOf=cn=group1,ou=example)
```

To select users belonging to `group1` or `group2`:

```
(|(memberOf=cn=group1,ou=example)(memberOf=cn=group2,ou=example))
```

For information on how to query a user or group DN from Active Directory, see Using dsquery to obtain user or group DN (on page 110).

11. By default, the **Add all users under Base DN to opscenter-users group** option is not available. This means that only members of groups (next step) are permitted to log in to the portal. If you enable this option, all users under the Base DN are assigned to the opscenter-users group and can also log in.
12. Provide entries for the **Group entry list**. For example, if you created AD groups named `sanadmin` and `sanoperator`, you can eventually assign roles and permissions appropriate to each group, as in this example:

```
"CN=sanadmin,CN=Users,DC=home,DC=us"
"CN=sanoperator,CN=Users,DC=home,DC=us"
```

Click **+Add Group DN** to add entries.

> **Note:** The group DN must be included in the subtree of the DN specified in the **Base DN**.

13. Click **Submit** when the settings are complete. If the "Number of users outside of range" error is still displayed, change the **Custom user LDAP filter** to reduce the number of users to be added. You can use the **Pre-check the number of users (filter)** to confirm the results before resubmitting.

> **Note:** If a group name collides with an existing group name, a KAOP20008-E error is displayed, possibly including "Failed to sync groups" along with name of the directory service. If this occurs, change the name of the existing user group on the Groups screen.

Result

- The Active Directory entries are added to Manage users > Groups and are displayed with the DN designation.
- AD users cannot be added to local (non-AD) groups.

Next steps

- By default, AD group users are assigned the opscenter-user role, which permits them to log in to the Ops Center portal and access the Inventory tab, but not start Ops Center products. To assign a role to an AD group that permits users access to administrative functions outside the Inventory tab and log in to all Ops Center products with full admin privileges, you can assign the opscenter-system-administrator role. See Assigning portal-level roles to Ops Center groups (on page 100) for more information.
- To assign product-level roles to an AD group that permit members to access individual Ops Center products, see Assigning product-level roles from the Ops Center portal (on page 101) for more information.
- Confirm the Active Directory entries appear in Manage users > Groups.
- Verify Active Directory users can log in. AD users must log in using the `sAMAccoutName` (no domain).

Using dsquery to obtain user or group DN

You can use the following PowerShell commands to obtain the DN for a user or group.

To get the user DN:

```
dsquery user
```

To retrieve the user details (all attributes):

```
dsquery * user_DN -scope base -attr *
```

To get the group DN:

```
dsquery group
```

To retrieve the group details (all attributes):

```
dsquery * group_DN -scope base -attr *
```

Setting up Kerberos authentication for Ops Center

You can configure Kerberos authentication for the Ops Center directory service.

> **Note:** Whenever you make changes to Kerberos authentication, make sure to retest the authentication for the Directory service (in Manage users > User directories).

Procedure

1. Log in to the Ops Center portal as `sysadmin` or a user with opscenter-administrators membership.
2. From the navigation bar, click **Manage users** and select **User directories** from the Asset type list.

3. Click **Kerberos connection settings**.
4. To use DNS instead of KDC to look up the Kerberos server, enable **DNS lookup KDC**.
5. Use **Clock skew** to control the maximum time difference between the system clocks on the Ops Center server and the Kerberos server (default: 300 seconds). When this value is exceeded, an authentication error occurs.
6. Enter the **Realm name** that identifies the Kerberos domain. The Realm name is case-sensitive and must match the realm to which you are linking. Although the realm can be any ASCII string, the convention is to make it the same as the domain name in upper-case letters (such as EXAMPLE.COM).
7. If you are not using DNS, click **+Add KDC** to provide a list of Kerberos **KDC** server entries.
8. Click **Submit** when the settings are complete.

Configuring a non-AD directory service for Ops Center (LDAP server)

You can configure any directory service that supports the LDAP authentication protocol (such as Tivoli) for the Ops Center portal and import users from the server. This permits the users to access portal functions and products with a single sign-in. (Only LDAP is supported for non-AD directory services.)

Before you begin

- Verify you completed the procedure described in Importing certificates into the Common Services truststore (on page 94).

Note: Whenever you make changes to LDAP server settings, you must do the following:

- Click Sync users to apply the changes to the users configured in Ops Center.
- Click Test connection and Test authentication.
- Click Pre-check the number of imported users.

If any errors are reported, confirm the changes are valid.

Procedure

1. Log in to the Ops Center portal as `sysadmin` or a user with opscenter-administrators membership.
2. From the navigation bar, click **Manage users** and select **User directories** from the Asset type list.
3. Click the **+** (plus) icon.

   The **Add user directory service** window opens.
4. Enter a name for the service.
5. Select **Other** for the **Directory service** type.

   The LDAP **Authentication protocol** is automatically selected.

6. Enter the **Connection URL** (for example: `ldaps://ldaps.example.com`) and then click **Test connection**.

   > **Note:** Specify the same host name as the CN or SANs in the LDAP server certificate.

7. Enter the **BIND user DN** (for example: `CN=bind-user,OU=foo,OU=bar,DC=example,DC=com`) and the password and then click **Test authentication**.

   > **Note:** The BIND User DN only needs read permissions (not admin or modify).

8. Enter the **Base DN** (for example: `OU=foo,OU=bar,DC=example,DC=com`).

   > **Note:** To have portal access, users must be included in the subtree of the DN specified in the Base DN.

9. Configure the following LDAP settings:

Item	Description	Default value
User object classes	Object class of the imported user	Examples: inetOrgPerson, organizationalPerson **Note:** Use commas to separate entries.
Search scope	One level (flat), or Subtree.	Subtree
Custom user LDAP filter (optional)	Search filter to narrow results. (Must be specified in rfc2254 format.) The filter only applies to user entry attributes (not DN objects).	Examples: (|(cn=t_brady)(cn=j_smith)(cn=orion_admin)) (ou=Storage management)
LDAP attribute for username	Attribute that uniquely identifies the imported user.	uid

10. You can import a maximum of 100 users. Click **Pre-check the number of imported users**. If you exceed the limit, you can decrease the number of users by using the **Custom user LDAP filter**.
11. Configure the following attributes to be used when importing the users:

Item	Description	Default value
LDAP attribute for first name	Imported user's first name. Select **Full name** or **First name**.	For Full name, cn is the default value. For First name, givenName is the default value.
LDAP attribute for last name	Imported user's last name	sn
LDAP attribute for email	Imported user's email address	mail
LDAP attribute for RDN	Attribute used as RDN (top attribute) of typical user DN (usually the same as Username LDAP attribute).	uid
LDAP attribute for UUID	Attribute used for UUID	entryUUID

12. By default, the **Add all users under Base DN to opscenter-users group** option is not available. If you enable this option, all users under the Base DN are automatically assigned to the opscenter-users group and can also log in. If the option is not available, you have to add the imported users to a local group manually and assign the opscenter-user role to permit them to log in.
13. Click **Submit** when the settings are complete.
14. When you are returned to the **User directories** window, click **Sync users**. The LDAP server users are then imported into the Ops Center portal.

Result

The imported LDAP server users are added to Manage users > Users and are displayed with the DN designation.

- If you enabled the Add all users under Base DN to opscenter-users group option, the imported LDAP server users can log in to the Ops Center portal and access the Inventory tab. To assign a role to a group that permits access to administrative functions outside the Inventory tab and log in to all Ops Center products with full admin privileges, you can assign the opscenter-system-administrator role. See Assigning portal-level roles to Ops Center groups (on page 100) for more information.
- To assign product-level roles to a group that permits members to access individual Ops Center products, refer to Assigning product-level roles from the Ops Center portal (on page 101) for more information.
- Confirm the LDAP server entries appear in Manage users > Users.
- Verify the LDAP server users can log in.

Determining the parameters for LDAP server registration

If you want to link with an LDAP server, when you register the link with the LDAP server in Common Services, you must set parameters to import users.

Run the **`ldapsearch`** command, and then determine the parameters based on the information returned by the search.

Procedure

1. From the management server, run the **`ldapsearch`** command.

   Example of the command syntax:

   ```
   ldapsearch -h host-name-or-IP-address-of-the-LDAP-server -b base-DN-to-be-
   found -D bind-dn -w password-of-the-bind-DN -L -s scope-of-the-search
   ["ldap-filter"]
   ```

   For details, see the LDAP server documentation.

   Example of running command:

   ```
   ldapsearch -h example.com -b "CN=Users,DC=example,DC=com" -D "CN=admin,
   CN=Users,DC=example,DC=com" -w sysadmin -L -s sub "(objectclass=*)"
   ```

   Example of LDIF data:

   ```
   dn: CN=John Smith,CN=Users,DC=example,DC=com
   objectClass: person
   objectClass: organizationalPerson
   uid: j_smith
   cn: John Smith
   sn: Smith
   givenName: John
   distinguishedName: CN=John Smith,CN=Users,DC=example,DC=com
   whenCreated: 20200710022002.0Z
   whenChanged: 20210603075422.0Z
   memberOf: CN=opscenter_users,CN=Users,DC=example,DC=com
   mail: j_smith@example.com
   objectGUID:: hMekv/PMMkyVnykQ5AeMyQ==
   description: type1

   dn: CN=Tom Brady,CN=Users,DC=example,DC=com
   objectClass: person
   objectClass: organizationalPerson
   uid: t_brady
   cn: Tom Brady
   sn: Brady
   givenName: Tom
   distinguishedName: CN=Tom Brady,CN=Users,DC=example,DC=com
   whenCreated: 20200710022057.0Z
   ```

```
whenChanged: 20210601074245.0Z
memberOf: CN=hcs_users,CN=Users,DC=example,DC=com
mail: t_brady@example.com
objectGUID:: pZtOMo29j0CSoFnJrkL3EQ==
description: type2
```

2. Based on the displayed LDIF data, determine the parameter information to set in Common Services.

   The following table shows an example of the correspondence between the settings in Common Services and the LDAP attributes.

Setting in Common Services	LDAP user attribute
LDAP attribute for username	`uid`
LDAP attribute for email	`mail`
LDAP attribute for last name	`sn`
Full name*	`cn`
First name*	`givenName`
LDAP attribute for RDN	`cn`
LDAP attribute for UUID	`objectGUID`
User object classes	`organizationalPerson`
Custom user LDAP filter	`(description=type1)`
*: Set one of these settings.	

   You can specify a search filter in **Custom User LDAP Filter** to narrow down the users to be imported. (The syntax must conform to RFC 2254.)

Chapter 8: Configuring a link to an AD FS identity provider

By linking Common Services with an identity provider, you can delegate Hitachi Ops Center Portal authentication. You can also use the Multi Factor Authentication (MFA) functionality provided by the identity provider.

The procedure for configuring a link differs depending on the type of identity provider. You can configure a link to AD FS by following the steps listed in the Workflow for linking with AD FS (on page 116) to workflow topic. For details on the procedure for configuring a link to an identity provider other than AD FS, see Configuring a link to a non-AD FS identity provider (on page 136).

Supported AD FS

Common Services supports the following for AD FS.

Item	Description
Identity provider	Active Directory Federation Services (AD FS)
Protocol	▪ OpenID Connect (OIDC) ▪ Security Assertion Markup Language (SAML)
OS	The supported AD FS must support the following operating systems: ▪ Windows Server 2016 Datacenter ▪ Windows Server 2019 Datacenter ▪ Windows Server 2022 Datacenter ▪ Windows Server 2025 Datacenter
Maximum number of linked providers	1 If a link is already established with AD FS, you cannot configure links to other identity providers.

Workflow for linking with AD FS

Use the following workflow to specify settings for AD FS:

The workflow for specifying settings depends on the protocol being used.

If you want to use OIDC:

1. Register Common Services in AD FS as an application group.
2. Set up an issuance transform rule for AD FS.
3. Check the OpenID Connect Discovery endpoint of AD FS.
4. Register AD FS with Common Services.
5. Log in to the Hitachi Ops Center Portal as an AD FS user.

If you want to use SAML:

1. Check the AD FS metadata endpoint.
2. Register AD FS with Common Services.
3. Export Common Services metadata.
4. Register Common Services in AD FS as a relying party.
5. Set up a claim issuance policy.
6. Log in to the Hitachi Ops Center Portal as an AD FS user.

Before using Common Services to specify the settings to link with AD FS, you must install and configure AD FS.

To link with AD FS, you must specify SSL communication settings in advance for the route from Common Services to the AD FS server. For details, see Configuring SSL communications (on page 76).

Note: If you are using a host name for the Common Services access URL, the host name of the management server must be resolvable by the AD FS server.

Configuring settings to link with AD FS (OIDC)

To link with AD FS by using the OIDC protocol, configure settings as follows.

Registering Common Services in AD FS as an application group

By registering Common Services in AD FS as an application group, you can transfer authentication for the Hitachi Ops Center Portal to AD FS.

Before you begin

The following settings are also necessary for registering AD FS in Common Services and must be determined in advance:

- AD FS alias name

  The alias name is an identifier that uniquely identifies AD FS in Common Services. You can specify up to 64 characters consisting of halfwidth alphabetic characters (lowercase only), numeric characters, hyphens, and underscores. You cannot change the registered value later.

  Example:

  ```
  adfs_oidc_ad5
  ```

- URI of the Web API identifier

  The Web API identifier is an identifier that AD FS uses to uniquely identify Common Services. Although you can specify any valid character string, a good practice is to use a name that is easy to identify (such as the host name of the Common Services management server).

  Example:

  ```
  https://common_services_host
  ```

Procedure

1. Log in to the AD FS server.
2. Select **Start** > **Windows Administrative Tools** > **AD FS Management**.
3. From the tree on the left side, select **AD FS** > **Application Groups**. In the pane on the right side, click **Application Groups** > **Add Application Group**.
4. In the Welcome window, complete the following information, and then click **Next**:

   Name

   A name of your choice.

   Template

   Select **Server application accessing a web API**.

5. In the Server application window, complete the following information, and then click **Next**:

   Client Identifier

   Record this information for when you register AD FS in Common Services.

   Redirect URI

   Specify the host name and port number of the Common Services management server, along with the AD FS alias name:

   `https://`*`host-name`*`:`*`port-number`*`/auth/realms/opscenter/broker/`*`alias-name`*`/endpoint`

   For *alias-name*, specify the AD FS alias name that you determined in advance.

6. In the Configure Application Credentials window, select the **Generate a shared secret** check box.

   Make a note of the Secret for when you register AD FS in Common Services.
7. Click **Next**.
8. In the Configure Web API window, for **Identifier**, specify the URI of the Web API identifier that you determined in advance, click **Add**, and then click **Next**.
9. In the Choose Access Control Policy window, specify an access control policy, and then click **Next**.
10. In the Configure Application Permissions window, select the following check boxes for **Permitted scopes**, and then click **Next**.
    - **allatclaims**
    - **email**
    - **openid**
    - **profile**
11. In the Summary window, make sure that the settings are correct, and then click **Next**.
12. In the Finish window, click **Close**.

Setting up an issuance transform rule for AD FS

Set up an issuance transform rule for the Common Services instance registered as an application group in AD FS. The login information for the Hitachi Ops Center Portal is transmitted to Common Services based on these settings.

Procedure

1. Log in to the AD FS server.
2. Select **Start** > **Windows Administrative Tools** > **AD FS Management**.
3. From the tree on the left, select **AD FS** > **Application Groups**. In the middle pane, select the application group for Common Services, and then in the right pane, click **Properties**.

   The properties window for the application group appears.
4. For **Applications**, select ***application-group-name*- Web API** and then click **Edit**.

   The properties window for the Web API appears.
5. On the Issuance Transform Rules tab, click **Add Rule**.

   The Add Transform Claim Rule Wizard dialog box opens.
6. In the Select Rule Template window, select **Send LDAP Attributes as Claims** for **Claim rule template**, and then click **Next**.
7. In the Configure Rule window, complete the following information, and then click **Finish**.

   Claim rule name

   A name of your choice

   Attribute store

   Select **Active Directory**.

Mapping of LDAP attributes to outgoing claim types

Set the following values.

Value to specify for LDAP Attribute	Value to specify for Outgoing Claim Type
Either of the following LDAP attributes for which an email address is registered in the system: ▪ User-Principal-Name ▪ E-Mail-Addresses	E-Mail Address
Given-Name	Given Name
Surname	Surname
Token-Groups - Qualified by Domain Name	Group

> **Note:** For the Active Directory user for the Hitachi Ops Center Portal, make sure that the email address, surname, and given name are set for the LDAP attributes that you specify. If this information is not set, the user cannot log in.

8. Verify that the Claim rule has been added to the Issuance Transform Rules tab, and then click **OK**.

Checking the OpenID Connect Discovery endpoint of AD FS

Obtain the OpenID Connect Discovery endpoint needed to register AD FS in Common Services.

Procedure

1. Log in to the AD FS server.
2. Select **Start** > **Windows Administrative Tools** > **AD FS Management**.
3. Check the OpenID Connect Discovery endpoint of AD FS.

   From the tree on the left side, select **AD FS** > **Service** > **Endpoints**. From the displayed endpoint information, check the value of **URL Path** in the row where the Type is OpenID Connect Discovery.

   To obtain the endpoint, simply append the base URI of AD FS to the displayed URL.

   Example:

   ```
   https://adfs.example.com/adfs/.well-known/openid-
   configuration
   ```

   Make a note of the OpenID Connect Discovery endpoint because you will need it when you register AD FS in Common Services.

Registering AD FS with Common Services

You must register AD FS with Common Services as an identity provider.

Procedure

1. Log in to the Hitachi Ops Center Portal as the sysadmin user or as a user who belongs to the opscenter-administrators group.
2. From the navigation bar, click **Manage users**.
3. In the Users window, from the Asset type, click **Identity providers**.
4. In the Identity Providers window, click ＋.
5. In the wizard, enter and register the following information.

Item	Value
Provider type	Active Directory Federation Services
Federation protocol	OpenID connect 1.0
Display name	Name of the identity provider (up to 64 characters).
Alias	Alias name that was decided on in Registering Common Services in AD FS as an application group (on page 117)
OpenID connect discovery endpoint	The endpoint that was verified in Checking the OpenID Connect Discovery endpoint of AD FS (on page 120).
Enabled	If you specify **Enable**, the identity provider is enabled and the **Log in using external identity provider** link appears in the login window.
Client ID	The AD FS client identifier that was displayed in Registering Common Services in AD FS as an application group (on page 117).
Client secret	The AD FS secret name that was displayed in Registering Common Services in AD FS as an application group (on page 117).
Web API identifier	URI of the Web API identifier used in Registering Common Services in AD FS as an application group (on page 117).
Allowed clock skew	Acceptable time difference between the management server where Common Services is installed and the AD FS server. If the time difference between the servers exceeds this value, you cannot use AD FS to log in. Valid values are 0 to 300 (seconds). Default: 300

Item	Value
Default group mappers	Local user group used as the default. (Optional) When AD FS user authentication succeeds, the user is imported into Common Services as a local user, and the local user group specified for this item is assigned. Maximum number of groups is 10.
Custom group mappers	A pair consists of an AD FS user group and a local user group. (Optional) When AD FS user authentication succeeds, the user is imported into Common Services as a local user. If the user belongs to an AD FS user group specified in the Custom group mappers, the corresponding local user group is assigned. Maximum number of pairs is 10. Specify the AD FS user group name in Windows Domain Qualified Name format. **Example:** `domain\cs_admin_group`

Tip: When the default group mapper is defined, all users that belong to AD FS are assigned to that group when they log in.

By contrast, the custom group mapper requires that each AD FS user be assigned to the group before they can log in.

AD FS users are assigned whatever privileges belong to the local group to which they are mapped. For this reason, you should not use the opscenter-administrators as the default group mapper.

An Ops Center administrator can assign group membership individually to AD FS users instead of depending on the group mappers.

Logging in to the Hitachi Ops Center Portal as an AD FS user

After completing the settings for linking with the AD FS, confirm that you can log in to the Hitachi Ops Center Portal from a browser as an AD FS user.

Procedure

1. In a web browser, access the following URL:

   `https://`*`host-name-or-IP-address-of-Portal`*`:`*`port-number`*`/portal`

2. In the login window, click **Log in using external identity provider**.

   The AD FS login window opens.

3. Log in as an AD FS user.

   When the AD FS user is successfully authenticated, you are logged in to the Hitachi Ops Center Portal.
4. Log in again as the sysadmin user or as a user who is a member of the opscenter-administrators group. Then, select **Manage users** > **Users**, and check whether the following items of the AD FS user are set correctly: the username, last name, first name, email address, and the user group specified for Default group mappers and Custom group mappers.

Result

This completes the settings for linking with the AD FS.

Configuring settings to link with AD FS (SAML)

To link with AD FS by using the SAML protocol, configure settings as follows.

Checking the AD FS metadata endpoint

Check the metadata endpoint required to register AD FS in Common Services.

Procedure

1. Log in to the AD FS server.
2. Select **Start** > **Windows Administrative Tools** > **AD FS Management**.
3. Check the AD FS metadata endpoints.

   From the tree on the left side, select **AD FS** > **Service** > **Endpoints**. From the displayed endpoint information, check the value of URL Path in the row where the Type is Federation Metadata.

   The string obtained by adding the AD FS base URI to the above URL is the AD FS metadata endpoint.

   Example:

   ```
   https://adfs.example.com/FederationMetadata/2007-06/
   FederationMetadata.xml
   ```

   Make note of the endpoint because you need it for registering AD FS with Common Services.

Registering AD FS with Common Services

You must register AD FS with Common Services as an identity provider.

Procedure

1. Log in to the Hitachi Ops Center Portal as the sysadmin user or as a user who is a member of the opscenter-administrators group.

2. From the navigation bar, click **Manage users**.
3. In the Users window, from the Asset type, click **Identity providers**.
4. In the Identity Providers window, click ＋.
5. In the wizard, enter and register the following information.

Item	Value
Provider type	Active Directory Federation Services
Federation protocol	SAML 2.0
Display name	Name of the identity provider (up to 64 characters).
Alias	Alias name used to uniquely identify the identity provider (up to 64 characters). Valid character types are half-width alphabetical characters (lowercase only), numbers, hyphens, and underscores. You cannot change the registered value later.
AD FS endpoint metadata URI	Endpoint defined in Checking the AD FS metadata endpoint (on page 123).
Enabled	If you specify **Enable**, the identity provider is enabled and the **Log in using external identity provider** link appears in the login window.
NameID Policy Format	Format used for the username when the AD FS user is imported as a Common Services local user: ▪ Windows Domain Qualified Name ▪ Email ▪ Unspecified
Allowed clock skew	Acceptable time difference between the management server where Common Services is installed and the AD FS server. If the time difference between the servers exceeds this value, you cannot use AD FS to log in. Valid values are 0 to 300 (seconds). Default: 300
Default group mappers	Local user group used as the default. (Optional) When AD FS user authentication succeeds, the user is imported into Common Services as a local user, and the local user group specified for this item is assigned. Maximum number of groups is 10.
Custom group mappers	A pair consists of an AD FS user group and a local user group. (Optional)

Item	Value
	When AD FS user authentication succeeds, the user is imported into Common Services as a local user. If the user belongs to an AD FS user group specified in the Custom group mappers, the corresponding local user group is assigned. Maximum number of pairs is 10. Specify the AD FS user group name in Windows Domain Qualified Name format. **Example:** `domain\cs_admin_group`

Tip: When the default group mapper is defined, all users that belong to AD FS are assigned to that group when they log in.

By contrast, the custom group mapper requires that each AD FS user be assigned to the group before they can log in.

AD FS users are assigned whatever privileges belong to the local group to which they are mapped. For this reason, you should not use the opscenter-administrators as the default group mapper.

An Ops Center administrator can assign group membership individually to AD FS users instead of depending on the group mappers.

Exporting Common Services metadata (AD FS)

To link with AD FS, you must register Common Services metadata into AD FS. From the Hitachi Ops Center Portal, output the metadata to a file, and then send the file to the AD FS server.

Procedure

1. Log in to the Hitachi Ops Center Portal as the sysadmin user or as a user who is a member of the opscenter-administrators group.
2. In the navigation bar, click **Manage users**.
3. In Asset type in the Users window, click **Identity providers**.
4. In the Identity Providers window, click the target AD FS.
5. In the Identity provider details window, click **Download metadata**.

   The Common Services metadata file is downloaded. Transfer this file to the AD FS server.

Registering Common Services in AD FS as a relying party

By registering Common Services in AD FS as a relying party, you can transfer authentication for the Hitachi Ops Center Portal to AD FS.

Procedure

1. Log in to the AD FS server.
2. Select **Start** > **Windows Administrative Tools** > **AD FS Management**.
3. From the tree on the left side, select **AD FS** > **Relying Party Trusts**. In the pane on the right side, click **Relying Party Trusts** > **Adding Relying Party Trust**.
4. In the Welcome window, select **Claims aware**, and then click **Start**.
5. In the Select Data Source window, select **Import data about the relying party from file**. For **Federation metadata file location**, specify the file to which the Common Services metadata was exported, and then click **Next**.
6. In the Specifying Display Name window, specify a display name, and then click **Next**.
7. In the Choose Access Control Policy window, specify an access control policy, and then click **Next**.
8. In the Ready to Add Trust window, make sure that the settings are correct, and then click **Next**.
9. In the Finish window, select the **Configure claims issuance policy for this application** check box, and then click **Close**.

Setting up a claim issuance policy

Set up a claim issuance policy for the Common Services instance registered as a relying party in AD FS. The user attribute information imported when the user logs in to the Hitachi Ops Center Portal is transmitted to Common Services based on the claim issuance policy settings.

Procedure

1. Log in to the AD FS server.
2. Select **Start** > **Windows Administrative Tools** > **AD FS Management**.
3. From the tree on the left, select **AD FS** > **Relying Party Trusts**. In the middle pane, select the relying party trust for Common Services, and then in the right pane, click **Edit Claim Issuance Policy...**.

   The Edit Claim Issuance Policy dialog box opens.
4. On the Issuance Transform Rules tab, click **Add Rule**.

   The Add Transform Claim Rule Wizard dialog box opens.
5. Select **Transform an Incoming Claim** for the claim rule template, and then click **Next**.
6. Specify the following items:

   Claim rule name

   A name of your choice

   Outgoing claim type

   The **Name ID**

   Incoming claim type and Outgoing name ID format

   Depending on the value specified for NameID Policy Format in Registering AD FS with Common Services (on page 123), specify the values as follows:

Value specified for NameID Policy Format	Value to specify for Incoming claim type	Value to specify for Outgoing name ID format
Windows Domain Qualified Name	Windows account name	Windows Qualified Domain Name
Email	Either of the following LDAP attributes for which an email address is registered in the system: ▪ UPN (User-Principal-Name) ▪ E-Mail Address	Email
Unspecified	UPN	UPN

Pass through all claim values

Select this item to turn it on.

7. Click **Finish**.

   The claim rule is added to the Edit Claim Issuance Policy dialog box. The values specified here are transmitted to Common Services upon the following claim:

   ```
   http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier
   ```

8. In the Edit Claim Issuance Policy dialog box, click **Add Rule** again.

   The Add Transform Claim Rule Wizard dialog box opens.

9. Select **Send LDAP Attributes as Claims** for the claim rule template, and then click **Next**.

10. Specify the following items:

    Claim rule name

    A name of your choice

    Attribute Store

    Active Directory

    Mapping of LDAP attributes to outgoing claim types

    Specify values for the following attributes:

LDAP Attribute	Value
Either of the following LDAP attributes for which an email address is registered in the system: ■ User-Principal-Name ■ E-Mail-Addresses	E-Mail Address
Given-Name	Given Name
Surname	Surname
Token-Groups - Qualified by Domain Name	Group

> **Note:** Make sure that the email address, surname, and given name of the Active Directory user for the Hitachi Ops Center Portal are set for the LDAP attributes that you specify. If this information is not set, the user cannot log in.

11. Click **Finish**.

    The claim rule is added to the Edit Claim Issuance Policy dialog box. The values specified are transmitted to Common Services through the following claims:

    - E-Mail Address:

      ```
      http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress
      ```

    - Given Name:

      ```
      http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname
      ```

    - Surname:

      ```
      http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname
      ```

    - Group:

      ```
      http://schemas.xmlsoap.org/claims/Group
      ```

12. In the Edit Claim Issuance Policy dialog box, change the order of priority to the following, and then click **OK**.

    a. The rule specified for the **Send LDAP Attributes as Claims**

    b. The rule specified for the **Transform an Incoming Claim**

13. To make sure the specified information is correct, select **AD FS** > **Service** > **Claim Descriptions**.

Logging in to the Hitachi Ops Center Portal as an AD FS user

After completing the settings for linking with the AD FS, confirm that you can log in to the Hitachi Ops Center Portal from a browser as an AD FS user.

Procedure

1. In a web browser, access the following URL:

   `https://host-name-or-IP-address-of-Portal:port-number/portal`

2. In the login window, click **Log in using external identity provider**.

   The AD FS login window opens.

3. Log in as an AD FS user.

   When the AD FS user is successfully authenticated, you are logged in to the Hitachi Ops Center Portal.

4. Log in again as the sysadmin user or as a user who is a member of the opscenter-administrators group. Then, select **Manage users** > **Users**, and check whether the following items of the AD FS user are set correctly: the username, last name, first name, email address, and the user group specified for Default group mappers and Custom group mappers.

Result

This completes the settings for linking with the AD FS.

> **Note:** If you link with AD FS by using the SAML protocol, you must periodically update the certificate used for user authentication. For details, see Updating the authentication certificates used with an AD FS (SAML) (on page 130).

Updating an identity provider configuration

You can update the identity provider configuration in the Hitachi Ops Center Portal.

Procedure

1. Log in to the Hitachi Ops Center Portal as sysadmin or a user with opscenter-administrators membership.
2. From the navigation bar, click **Manage users**.
3. In the **Users** window, from the Asset type, click **Identity providers**.
4. Click the edit icon (pencil) for the identity provider.
5. Update the information and then click **Next** to proceed through all the entry windows.
6. Click **Submit** when you reach the last window and your changes are complete.

Removing an identity provider

You can remove an identity provider from Ops Center.

Procedure

1. Log in to the Hitachi Ops Center Portal as sysadmin or a user with opscenter-administrators membership.
2. From the navigation bar, click **Manage users**.
3. In the **Users** window, from the Asset type, click **Identity providers**.
4. Click the delete icon (trash can) for the identity provider.
5. Click **Submit** in the Delete dialog box.

Updating the authentication certificates used with an AD FS (SAML)

This section explains how to check the date of the next update of a certificate, update a certificate, and change the number of days set as the update interval of the Common Services authentication key and AD FS Token certificates that are used with AD FS.

If you link with AD FS by using the OIDC protocol, you do not need to perform this procedure.

Overview of updating authentication certificates (AD FS)

For AD FS, Common Services and AD FS certificates are used during user authentication.

Common Services certificates are called authentication keys, and AD FS certificates are called Token certificates.

Each certificates has an expiration date and certificates are automatically updated according to a defined interval (in days).

However, when a certificate is automatically updated, a discrepancy arises between the new certificate and the certificate that was registered when the link with AD FS was configured. For this reason, you will no longer be able to log in to Common Services by using the AD FS user account. To prevent this problem, you must check the date of the next update of the certificate and update the certificate before the expiration date.

If it is inconvenient to update the authentication key of Common Services immediately, you can temporarily suppress the update by increasing the number of days set as the update interval. Although you can also change the update interval of AD FS Token certificates, the change is not applied to the certificates currently used. The new update interval is applied to the certificates that will be updated next time.

> **Tip:** If you manually update the Common Services certificate, we recommend that you specify the same update interval for the Common Services authentication key and for the AD FS Token certificates, because this enables you to update both on the same day. Update certificates during a time when no user is logged in (such as on a holiday or during the night).

Checking the next update for the Common Services certificates

Check the date of the next update of the authentication key for Common Services.

Procedure

1. Log in to the Hitachi Ops Center Portal as the sysadmin user or as a user who is a member of the opscenter-administrators group.

   Note: If the date of the next update of the authentication key will occur within 30 days, a message to that effect is displayed when you log in.

2. Select **Settings** > **Authentication key**, and then check the value displayed for **Authentication key next update date (UTC)**.

Checking the dates of the next update of the AD FS certificates

Check the dates of the next update of the Token certificates of AD FS.

Procedure

1. Log in to the AD FS server.
2. Select **Start** > **Windows Administrative Tools** > **AD FS Management**.
3. From the tree on the left side, select **AD FS** > **Service** > **Certificates**.
4. Check the value of **Expiration Date** for **Token-decrypting** and **Token-signing** in the middle pane.

Updating the Common Services certificates (AD FS)

Common Services certificates are automatically updated to prevent revocation due to expiration. When a certificate is automatically updated, you need to update the Common Services certificate registered on the AD FS server. There are two ways to update certificates: automatically or manually.

Automatically updating the Common Services certificates

To automatically update Common Services certificates, perform the following procedure. Use the Relying Party Trust Monitoring function of AD FS to ensure that Common Services metadata is updated automatically.

Note: After the certificate is automatically updated in Common Services, it might take up to 24 hours until the certificate is updated by the AD FS Monitoring function. Until it is updated, you will not be able to log in to the Hitachi Ops Center Portal as an AD FS user.

Before you begin

Verify that the following settings are configured:

- If the Windows Server version is 2019 or earlier, verify that Common Services certificates are signed with ECDSA.
- Verify that TLS 1.2 or higher is enabled in the .NET Framework settings of the AD FS server.

Procedure

1. Log in to the Hitachi Ops Center Portal as the sysadmin user or as a user who is a member of the opscenter-administrators group.
2. From the navigation bar, click **Manage users**.
3. In **Asset type** in the Users window, click **Identity providers**. In the target identity provider details window, check the value of **SAML SP metadata URI**.
4. Log in to the AD FS server.
5. Select **Start** > **Windows Administrative Tools** > **AD FS Management**.
6. From the tree on the left side, select **AD FS** > **Relying Party Trusts**. In the middle pane, select the target Relying Party Trust, and then in the right pane, click **Properties**.
7. In the properties window, select the **Monitoring** tab, and enter the value of **SAML SP metadata URI** that you checked in the identity provider details window of the Hitachi Ops Center Portal in **Relying party's federation metadata URL**.
8. Click **Test URL** to confirm. If an error occurs, review the SSL/TLS settings of Windows.
9. Select the check box for **Monitoring relying party**.
10. Select the check box for **Automatically update relying party**.
11. Click **Apply**.

Manually updating the Common Services certificates

To manually update Common Services certificates, perform the following procedure. If the date of the next update of the authentication key of Common Services is approaching, update the authentication key and the metadata. You can also change the update interval of the authentication key without actually updating the key.

Procedure

1. Log in to the Hitachi Ops Center Portal as the sysadmin user or as a user who is a member of the opscenter-administrators group.
2. Select **Settings** > **Authentication key**.

   The Authentication key window appears.

3. To change the update interval of the authentication key, change the value of **Authentication Key update interval (days)**.

   The default value is 180 days (with a range of 90 to 3,650). From a security standpoint, we recommend 90-180 days.

4. For **Update Authentication key now**, select **Yes**.

   If you want to change the update interval without updating the authentication key, select **No**.

5. Click **Submit**.

   If you selected **No** for **Update Authentication key now**, skip the remaining.

6. Export the metadata of Common Services.
   For details, see Exporting Common Services metadata (AD FS) (on page 125).
7. Log in to the AD FS server.

8. Select **Start** > **Windows Administrative Tools** > **AD FS Management**.
9. From the tree on the left side, select **AD FS** > **Relying Party Trusts**.
10. In **Relying Party Trusts**, check the value of **Identifier** for the Common Services instance that is registered.
11. Run the following command in PowerShell:

    ```
    Update-AdfsRelyingPartyTrust -MetadataFile absolute-path-of-the-metadata-file -
    TargetIdentifier ID-of-the-relying-party
    ```

    For *ID-of-the-relying-party*, specify the value of **Identifier** for Common Services (checked in the previous step).

    Example of running the command:

    ```
    Update-AdfsRelyingPartyTrust -MetadataFile C:\temp\metadata.xml -
    TargetIdentifier https://www.example.com:8443/auth/realms/opscenter
    ```

    For details on the command, see the AD FS documentation.

Updating the AD FS certificates

Run the AD FS command `Update-AdfsCertificate` to update the Token certificates. After updating the certificates, you must specify the metadata endpoint for AD FS from the Hitachi Ops Center Portal, and then update the information about AD FS registered in Common Services.

Note: For details about Token certificates and the command, see the AD FS documentation.

Procedure

1. Log in to the AD FS server.
2. To change the update interval of Token certificates, run the following command in PowerShell:

    ```
    Set-AdfsProperties -CertificateDuration update-interval-(number-of-days)
    ```

    The change will take effect the next time the Token certificates are updated after you change the update interval.

    Example of 3 years:

    ```
    Set-AdfsProperties -CertificateDuration 1095
    ```

3. If you want the change to take effect immediately, run the following command in PowerShell to update the Token certificates:

    ```
    Update-AdfsCertificate -CertificateType Token-Decrypting -Urgent
    Update-AdfsCertificate -CertificateType Token-Signing -Urgent
    ```

4. Log in to the Hitachi Ops Center Portal as the sysadmin user or as a user who is a member of the opscenter-administrators group.
5. In the navigation bar, click **Manage users**.
6. In Asset type in the Users window, click **Identity providers**.
7. Click the **Edit identity provider** icon for the registered identify provider.
8. For **AD FS endpoint metadata URI**, set the metadata endpoint for AD FS.

   For details on how to check the metadata endpoint, see Checking the AD FS metadata endpoint (on page 123).
9. Click **Next** without changing any other values.
10. In the **Edit identity provider - confirmation** window, click **Submit**.

If you cannot sign on with an identity provider (AD FS)

If you cannot sign on using AD FS, there are two possibilities:

- Certificates for Common Services were updated.

  In this scenario, if you cannot log in using AD FS, the following message is output to Applications and Services Logs > AD FS > Admin in the AD FS event log:

  ```
  ID6013: The signature verification failed
  ```

  For details on what to do when this message is output, see Updating the Common Services metadata by using AD FS (on page 134).
- Certificates for AD FS were updated.

  In this scenario, if you cannot log in using AD FS, the following message is output Common Services log file (default: `/var/log/hitachi/CommonService/idp/log/server.log`):

  ```
  ERROR [org.keycloak.broker.saml.SAMLEndpoint] (default task-14)
  validation failed
  ```

  For details on what to do when this message is output, see Specifying the AD FS metadata endpoint by using Common Services (on page 135).

Updating the Common Services metadata by using AD FS

You can update the Common Services metadata by using AD FS.

Procedure

1. Export the metadata of Common Services.

   For details, see Exporting Common Services metadata (AD FS) (on page 125).
2. Log in to the AD FS server.
3. Select **Start** > **Windows Administrative Tools** > **AD FS Management**.
4. From the tree on the left side, select **AD FS** > **Relying Party Trusts**.
5. In **Relying Party Trusts**, check the value of **Identifier** for the Common Services instance that is registered.

6. Run the following command in PowerShell:

   ```
   Update-AdfsRelyingPartyTrust -MetadataFile absolute-path-of-the-metadata-file -
   TargetIdentifier ID-of-the-relying-party
   ```

   For *ID-of-the-relying-party*, specify the value of **Identifier** for Common Services (checked in the previous step).

   Example:

   ```
   Update-AdfsRelyingPartyTrust -MetadataFile C:\temp\metadata.xml -
   TargetIdentifier https://www.example.com:8443/auth/realms/opscenter
   ```

   For details on the command, see the AD FS documentation.

Specifying the AD FS metadata endpoint by using Common Services

You can specify the AD FS metadata endpoint by using Common Services.

Procedure

1. Log in to the Hitachi Ops Center Portal as the sysadmin user or as a user who is a member of the opscenter-administrators group.
2. In the navigation bar, click **Manage users**.
3. In Asset type in the Users window, click **Identity providers**.
4. Click the **Edit identity provider** icon for the registered identity provider.
5. For **AD FS endpoint metadata URI**, set the metadata endpoint for AD FS.

   For details on how to check the metadata endpoint, see Checking the AD FS metadata endpoint (on page 123).
6. Click **Next** without changing any other values.
7. In the **Edit identity provider - confirmation** window, click **Submit**.

Chapter 9: Configuring a link to a non-AD FS identity provider

By linking Common Services with an identity provider, you can delegate Hitachi Ops Center Portal authentication. You can also use the Multi Factor Authentication (MFA) functionality provided by the identity provider.

The procedure for configuring a link differs depending on the type of identity provider. You can configure a link to an identity provider other than AD FS by following the steps listed in the Workflow for linking with a non-AD FS identity provider (on page 136) to workflow topic. For details on the procedure for configuring a link to AD FS, see Configuring a link to an AD FS identity provider (on page 116).

Workflow for linking with a non-AD FS identity provider

The following explains the workflow for configuring a link to an identity provider other than AD FS.

Keycloak is a built-in user authentication function in Common Services. To configure a link to a non-AD FS identity provider, use Keycloak, which is incorporated in Common Services. To establish a connection to the identity provider, you can use OIDC (OpenID Connect) or SAML (Security Assertion Markup Language) as the federation protocol.

For details on how to use Keycloak and how to configure identity providers, see the relevant documentation. Before accessing the Keycloak documentation, determine the Keycloak version by opening and reading the following file, then refer to the same documentation version.

```
installation-directory-of-Common-Services/keycloak/version.txt
```

The workflow for configuring a link to an identity provider other than AD FS consists of the following steps:

1. **Preparing the identity provider.**

   Install the identity provider software so that the identity provider is ready for use.

2. Enabling the function for linking with a non-AD FS identity provider (on page 137)
3. Registering a non-AD FS identity provider (on page 138)
4. Mapping user attributes (on page 138) (Optional)
5. Specifying a mapping to a user group (on page 141)
6. Configuring the authentication settings on the identity provider.

   Configure the settings required for Common Services user authentication, such as registering Common Services as a relying party.

7. Logging in to the Hitachi Ops Center Portal as an identity provider user.

Note:

- "Keycloak" refers to the Keycloak interface incorporated in Common Services.
- Users are responsible for configuring identity providers in Keycloak. Any issues that arise between Keycloak and identity providers are outside the scope of our support.
- When you register an identity provider in Keycloak or change settings after registration, Common Services might not run properly depending on the settings. We recommend that you use the **csbackup** command to back up Common Services in advance. For details, see Backing up Common Services (on page 177).
- If an identity provider other than AD FS is already linked with Common Services, you cannot link Common Services with AD FS.

Enabling the function for linking with a non-AD FS identity provider

To establish a link with an identity provider other than AD FS, you must run the **csembeddedkeycloak** command to enable the linking function.

When you run the **csembeddedkeycloak** command, a configuration change occurs that enables you to access Keycloak from the Hitachi Ops Center Portal. This command also creates a user who has permission log in to Keycloak (idpadmin).

After you enable the linking function, you cannot disable it.

Procedure

1. Log in to the management server as the root user.

   If you log in as an ordinary user, use the **sudo** command to complete the following procedure as the root user.
2. Run the following command:

```
installation-directory-of-Common-Services/utility/bin/csembeddedkeycloak -enable
```

3. When you are prompted whether to enable the setting, enter **y** (for yes).

   If you enter **n** (for no), the process ends.
4. Specify the password for the idpadmin user that will be created.

   Specify a password that follows the password policy for Common Services.
5. When the configuration is complete, the Common Services service is restarted.

Registering a non-AD FS identity provider

Log in to Keycloak from the Hitachi Ops Center Portal to register a non-AD FS identity provider.

Before you begin

Configure SSL communications between Common Services and the identity provider server. You must register the identity provider server certificate or the root certificate of the server certificate in the Common Services truststore. For details, see Configuring SSL communications (on page 76).

Procedure

1. Log in to the Hitachi Ops Center Portal as the sysadmin user or as a user who belongs to the opscenter-administrators group.
2. From the navigation bar, click **Manage users**.
3. In the Users window, from the Asset type, click **Identity providers (Other)**.
4. In the Identity providers (Other) window, click **Embedded Keycloak**.
5. Log in to Keycloak as the idpadmin user.
6. In the Identity providers window, click the identity provider with which you want to link.
7. Follow the instructions in the window to register the identity provider.

   > **Note:** The registered identity provider is not displayed in the ID provider window of the Hitachi Ops Center Portal. To view, update, or delete the identity provider configuration, you must log in to Keycloak. For details on using Keycloak, see the Keycloak documentation.

Mapping user attributes

To synchronize email addresses, last names, and first names of users of an identity provider other than AD FS with those of Common Services, you must map identity provider user attributes to Keycloak user attributes. Note that this mapping is required only when synchronization is needed.

The settings differ depending on the federation protocol used for linking with the identity provider.

- Linking by using the OIDC protocol (on page 138)
- Linking by using the SAML protocol (on page 139)

Linking by using the OIDC protocol

To synchronize email addresses, last names, and first names of users of an identity provider other than AD FS with those of Common Services, you must configure the identity provider to ensure that the ID token issued by the identity provider includes claims that correspond to Keycloak user attributes. You do not need to configure Keycloak. You can choose which attributes to map for users. For details on configuring claims for an identity provider, see the documentation for the identity provider that you are using.

The following table below provides the correspondence between Keycloak user attributes and claims in the ID token of the identity provider.

Keycloak user attribute	Claim in the ID token of the identity provider
email	email
lastName	family_name
firstName	given_name

Linking by using the SAML protocol

To synchronize email addresses, last names, and first names of users of an identity provider other than AD FS with those of Common Services, you must specify mappings between assertion attributes for the identity provider and Keycloak user attributes. You can choose which attributes to map for users.

Before you begin

Configure the assertion attributes for the identity provider. The assertion sent from the identity provider must include attributes required for Keycloak user attributes. For details on assertion attribute settings for the identity provider, see the documentation for the identity provider that you are using.

The following table below provides the correspondence between Keycloak user attributes and assertion attributes for an identity provider.

Keycloak user attribute	Example of assertion attributes for an identity provider
email	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress
lastName	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname
firstName	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname

Procedure

1. Log in to the Hitachi Ops Center Portal as the sysadmin user or as a user who belongs to the opscenter-administrators group.
2. From the navigation bar, click **Manage users**.
3. In the Users window, from the Asset type, click **Identity providers (Other)**.
4. In the Identity providers (Other) window, click **Embedded Keycloak**.

5. Log in to Keycloak as the idpadmin user.
6. In the Identity providers window, click the registered identity provider.
7. In the Provider details window, click the **Mappers** tab.
8. For each attribute to be synchronized, specify the item required for mapping.
   a. Click **Add mapper**.
   b. In the Add Identity Provider Mapper window, specify the following items.
      - When specifying an email address:

Item	Value to be specified	Example of value to be specified
Name	Any Name	email-mapper
Sync mode override	Value that can be selected from the list	Force
Mapper type	Attribute Importer	Attribute Importer
Attribute Name	Assertion attribute for the identity provider	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress
Name Format	ATTRIBUTE_FORMAT_BASIC	ATTRIBUTE_FORMAT_BASIC
User Attribute Name	email	email

      - When specifying a last name:

Item	Value to be specified	Example of value to be specified
Name	Any Name	lastName-mapper
Sync mode override	Value that can be selected from the list	Force
Mapper type	Attribute Importer	Attribute Importer
Attribute Name	Assertion attribute for the identity provider	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname
Name Format	ATTRIBUTE_FORMAT_BASIC	ATTRIBUTE_FORMAT_BASIC
User Attribute Name	lastName	lastName

- When specifying a first name:

Item	Value to be specified	Example of value to be specified
Name	Any Name	firstName-mapper
Sync mode override	Value that can be selected from the list	Force
Mapper type	Attribute Importer	Attribute Importer
Attribute Name	Assertion attribute for the identity provider	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname
Name Format	ATTRIBUTE_FORMAT_BASIC	ATTRIBUTE_FORMAT_BASIC
User Attribute Name	firstName	firstName

c. After configuration is complete, click **Save**.

d. Repeat this procedure until all the attributes to be synchronized are specified.

Specifying a mapping to a user group

Specify a mapping to a user group to assign Hitachi Ops Center access privileges to users of an identity provider other than AD FS.

By using a Keycloak group mapper, you can automatically map users authenticated by the identity provider to the specified Common Services user group. If you do not use a group mapper, you can manually assign a user group to each user on the Hitachi Ops Center Portal.

Based on the following examples, you can create a mapping between users of an identity provider and a user group.

- Assigning Hitachi Ops Center access privileges to all users:

  Using the Hardcoded Group mapper (on page 142)

- Assigning Hitachi Ops Center permissions to specific users:

  Using the Advanced Claim to Group mapper or the Advanced Attribute to Group mapper (on page 143)

- Using the identity provider to perform user authentication only, and using Common Services to manage access privileges:

  Assigning users to a user group by using the Hitachi Ops Center Portal (on page 145)

Note: If you use group mappers, do not specify the following group mappers for the mapper type:

- Orion OIDC Custom Group Mapper
- Orion OIDC Default Group Mapper
- Orion SAML Custom Group Mapper
- Orion SAML Default Group Mapper

Using the Hardcoded Group mapper

By using the Hardcoded Group mapper, you can automatically map all the users authenticated by an identity provider other than AD FS to a specific user group. Use this mapper to assign the same privileges to all identity provider users.

Procedure

1. Log in to the Hitachi Ops Center Portal as the sysadmin user or as a user who belongs to the opscenter-administrators group.
2. From the navigation bar, click **Manage users**.
3. In the Users window, from the Asset type, click **Identity providers (Other)**.
4. In the Identity providers (Other) window, click **Embedded Keycloak**.
5. Log in to Keycloak as the idpadmin user.
6. In the Identity providers window, click the registered identity provider.
7. In the Provider details window, click the **Mappers** tab.
8. Click **Add mapper** and specify the following items in the Add Identity Provider Mapper window:

Item	Value to be specified	Example of value to be specified
Name	Any Name	hardcoded-group
Sync mode override	Value that can be selected from the list	Force
Mapper type	Hardcoded Group	Hardcoded Group
Group	Name of the Common Services user group to which the user is assigned	opscenter-users

9. After configuration is complete, click **Save**.

Using the Advanced Claim to Group mapper or the Advanced Attribute to Group mapper

By using the Advanced Claim to Group mapper or the Advanced Attribute to Group mapper, you can automatically map users authorized by an identity provider other than AD FS to user groups based on the specified conditions. You can use these mappers, for example, to limit users who can log in to Hitachi Ops Center or to assign administrator privileges to a specific user.

These group mappers perform mapping based on user information provided by the identity provider. Specifically, a Key and Value pair is used to specify a condition, as indicated in the following procedure. Multiple conditions can be specified.

- When configuring a link by using the OIDC protocol: For Key, specify the Claim of the ID token. For Value, specify the value of Claim.
- When configuring a link by using the SAML protocol: For Key, specify the assertion attribute. For Value, specify the attribute value.

Procedure

1. Log in to the Hitachi Ops Center Portal as the sysadmin user or as a user who belongs to the opscenter-administrators group.
2. From the navigation bar, click **Manage users**.
3. In the Users window, from the Asset type, click **Identity providers (Other)**.
4. In the Identity providers (Other) window, click **Embedded Keycloak**.
5. Log in to Keycloak as the idpadmin user.
6. In the Identity providers window, click the registered identity provider.
7. In the Provider details window, click the **Mappers** tab.
8. Click **Add mapper** and specify the following items in the Add Identity Provider Mapper window:

- When configuring a link by using the OIDC protocol

Item	Value to be specified	Example of value to be specified
Name	Any Name	Advanced-Claim-to-Group-mapper
Sync mode override	Value that can be selected from the list	Force
Mapper type	Advanced Claim to Group	Advanced Claim to Group
Claims - Key	Key of the identity provider	Claim equivalent to a group The OIDC protocol does not support Claim indicating a group by default. You must specify Claim specific to the identity provider.
Claims - Value	A value that corresponds to Key	Storage Administrators
Regex Claim Values	On (if a regular expression is used for Claims - Value), Off (if no regular expression is used)	Off
Group	Name of the Common Services user group to which the user is assigned	opscenter-administrators

- When configuring a link by using the SAML protocol

Item	Value to be specified	Example of value to be specified
Name	Any Name	Advanced-Attribute-to-Group-mapper
Sync mode override	Value that can be selected from the list	Force
Mapper type	Advanced Attribute to Group	Advanced Attribute to Group
Attributes - Key	Key of the identity provider	http://schemas.xmlsoap.org/claims/Group
Attributes - Value	A value that corresponds to Key	Storage Administrators
Regex Attribute Values	On (if a regular expression is used for Attributes - Value), Off (if no regular expression is used)	Off
Group	Name of the Common Services user group to which the user is assigned	opscenter-administrators

9. After configuration is complete, click **Save**.

Assigning users to a user group by using the Hitachi Ops Center Portal

Without using any group mappers, you can assign users of an identity provider other than AD FS to the Common Services user group and then assign access privileges. The identity provider is used only to authenticate users, and Common Services is used, for example, to manage access privileges.

Procedure

1. As an identity provider user that you want to assign to the user group, perform a login attempt on the Hitachi Ops Center Portal.

   At this time, the user does not have access privileges for Hitachi Ops Center, so the login attempt will fail. However, the user will be registered as a local user in Common Services.

2. Log in to the Hitachi Ops Center Portal as the sysadmin user or as a user who belongs to the opscenter-administrators group.
3. From the navigation bar, click **Manage users** and select **Users** from the Asset type list.
4. Click the **User groups** icon for the identity provider user account.

   (Use the search box if the user account is not visible.)

   The group selection window appears.
5. From the **Available Groups** list, select the group you want to assign and then click the left arrow.
6. When you are finished, click < in the upper left corner of the window to return to the list of users.

Logging in to the Hitachi Ops Center Portal as a non-AD FS identity provider user

After completing the settings for linking with the non-AD FS identity provider, confirm that you can log in to the Hitachi Ops Center Portal from a browser as an identity provider user.

Procedure

1. In a web browser, access the following URL:

   `https://`*`host-name-or-IP-address-of-Portal`*`:`*`port-number`*`/portal`
2. In the login window, click **Log in using external identity provider**.

   The identity provider login window opens.
3. Log in as an identity provider user.

   When the identity provider user is successfully authenticated, you are logged in to the Hitachi Ops Center Portal.
4. Log in again as the sysadmin user or as a user who is a member of the opscenter-administrators group. Then, select **Manage users** > **Users**, and check whether the following items of the identity provider user are set correctly: the username, last name, first name, email address, and the user group specified for Default group mappers and Custom group mappers.

Result

This completes the settings for linking with the identity provider.

Note: If you link with an identity provider by using the SAML protocol, you must periodically update the certificate used for user authentication. For details, see Updating the certificate for authenticating a non-AD FS identity provider (SAML) (on page 147).

Updating the certificate for authenticating a non-AD FS identity provider (SAML)

If signature or encryption is configured for SAML protocol assertions when linking with an identity provider, you must perform one of the following actions if the Common Services certificate or the identity provider certificate is updated:

- If the Common Services certificate is updated, update the Common Services certificate registered in the identity provider.
- If the identity provider certificate is updated, update the identity provider certificate registered in Keycloak.

If you link with an identity provider by using the OIDC protocol, you do not need to perform this procedure.

Updating the Common Services certificates

The Common Services certificates are automatically updated to prevent expiration. After an automatic update, you must update the registered Common Services certificates on identity provider servers other than AD FS.

Before updating the Common Services certificates, you must output metadata from Keycloak to a file and import it to the identity provider.

Procedure

1. From the Hitachi Ops Center Portal, log in to Keycloak.
2. Open the Provider details window for the registered identity provider.
3. In **Endpoints**, from the link **SAML 2.0 Service Provider Metadata**, acquire the metadata.
4. Import the acquired metadata to the identity provider.

   For details on how to import metadata to the identity provider, see the documentation for the identity provider.

Updating the certificate of a non-AD FS identity provider

If the certificate of an identity provider is updated for any reason (for example, the expiration date is approaching), you must update the certificate of the identity provider registered in Keycloak.

For details on how to update the certificate, see the documentation for Keycloak and for the identity provider.

Output logs of operations for establishing linkage with non-AD FS identity providers

Keycloak operation logs are output when operations are performed to establish linkage with identity providers other than AD FS. If a linkage error occurs, verify the displayed message or log during the Keycloak operation and identify the cause of the error.

Keycloak log files are output to the following directory:

Storage location of log files:

```
/var/log/hitachi/CommonService/idp/log/
```

Chapter 10: Maintaining Hitachi Ops Center

The Hitachi Ops Center system administrator performs various system and maintenance tasks such as starting or stopping a service, backing up and restoring user data, and modifying URLs.

Checking the status of Ops Center services

Product	Command
Ops Center Common Services	`systemctl status csportal`
Ops Center Analyzer	*`Common-Component-installation-destination`*`/bin/hcmds64srv -status`
Ops Center Analyzer detail view Analyzer probe server	`/usr/local/megha/bin/megha-jetty.sh status`
Ops Center Analyzer RAID Agent	`/opt/jp1pc/htnm/bin/htmsrv status -all`
Ops Center Analyzer viewpoint	`systemctl status analyzer-viewpoint.target`
Ops Center Administrator	`systemctl status rainier`

Ops Center Automator	**Windows:**
	`Common-Component-installation-destination``\bin\hcmds64srv /status`
	Linux:
	`Common-Component-installation-destination``/bin/hcmds64srv -status`

Ops Center Protector	-
Ops Center API Configuration Manager	**Windows:** *`REST-API-installation-destination`*`\status.bat`

Product	Command
	Linux: *REST-API-installation-destination*/`status.sh`

Starting and stopping Ops Center services

Product	Command

Ops Center Common Services	To stop the service:
	`systemctl stop csportal`
	To start the service:
	`systemctl start csportal`
	or
	`systemctl restart csportal`

Ops Center Analyzer	To stop the service: *Common-Component-installation-destination*/`bin/hcmds64srv -stop` To start the service: *Common-Component-installation-destination*/`bin/hcmds64srv -start`

Ops Center Analyzer detail view	To stop the service:
	`/usr/local/megha/bin/megha-jetty.sh stop`
	To start the service:
	`/usr/local/megha/bin/megha-jetty.sh start`

Analyzer probe server	
Ops Center Analyzer RAID Agent	**Windows:** To stop the service: *RAID-Agent-installation-destination*`\jp1pc\htnm\bin\htmsrv stop -all` To start the service:

Product	Command

	RAID-Agent-installation-destination`\jp1pc\htnm\bin\htmsrv start -all`
	Linux:
	To stop the service:
	`/opt/jp1pc/htnm/bin/htmsrv stop -all`
	To start the service:
	`/opt/jp1pc/htnm/bin/htmsrv start -all`

Ops Center Analyzer viewpoint	To stop the service:
	`systemctl stop analyzer-viewpoint.target`
	To start the service:
	`systemctl restart analyzer-viewpoint.target`

Ops Center Administrator	To stop the service:
	`systemctl stop rainier`
	To start the service:
	`systemctl start rainier`

Ops Center Automator	**Windows:** To stop the service: *Common-Component-installation-destination*`\bin\hcmds64srv /stop` To start the service: *Common-Component-installation-destination*`\bin\hcmds64srv /start` **Linux:** To stop the service: *Common-Component-installation-destination*`/bin/hcmds64srv -stop` To start the service: *Common-Component-installation-destination*`/bin/hcmds64srv -start`

Product	Command

Ops Center Protector	To stop all services:
	`/bin/diagdata --stop hub`
	To start all services:
	`/bin/diagdata --start all`

Ops Center API Configuration Manager	**Windows:** To stop the service: *`REST-API-installation-destination`*`\stop.bat` To start the service: *`REST-API-installation-destination`*`\start.bat` **Linux:** To stop the service: *`REST-API-installation-destination`*`/stop.sh` To start the service: *`REST-API-installation-destination`*`/start.sh`

Starting or stopping the Common Services service

To start or stop the Common Services service, use the **`systemctl`** command.

Procedure

1. Log in to the management server as the root user.

   If you log in as an ordinary user, use the **`sudo`** command to complete the following procedure as the root user.
2. Run the **`systemctl`** command.

   To start the service:

   ```
   systemctl start csportal
   ```

   To stop the service:

   ```
   systemctl stop csportal
   ```

To restart the service:

```
systemctl restart csportal
```

Checking the validity period or revocation status of certificates

Certificates have expiration dates. Also, certificates might be revoked by the certification authority for security reasons. If the certificate for Hitachi Ops Center is expired or revoked, Hitachi Ops Center products will no longer be able to conduct SSL communication normally, so regularly check the validity period and revocation status of certificates by using the following methods.

Method for checking the validity period of a certificate

- Checking the validity period of a certificate in the truststore (on page 153)
- Checking the validity period of the server certificate (on page 153)

Method for checking the revocation status of a certificate

- Checking the revocation status of the server certificate (on page 154)

Checking the validity period of a certificate in the truststore

You can check whether the validity period of a certificate in the truststore has expired.

Procedure

1. Run the following command and provide the keystore password when prompted:

```
installation-directory-of-Common-Services/jdk/bin/keytool -list -v -keystore /var/installation-directory-of-Common-Services/tls/cacerts
```

Checking the validity period of the server certificate

You can check whether the validity period of the server certificate for the management server has expired.

Note: If the certificate has expired, you must renew it. Follow the procedure in Creating a private key and a certificate signing request (SSL Setup tool) (on page 82) to request a new certificate and overwrite the existing one. You must also reconfigure the SSL server settings and SSL client settings.

Procedure

1. Run the following command:

```
installation-directory-of-Common-Services/jdk/bin/keytool -printcert -file path-of-server-certificate
```

Checking the revocation status of the server certificate

You can check the revocation status of the server certificate for a Hitachi Ops Center product by using the Online Certificate Status Protocol (OCSP).

Note: If the certificate has been revoked, you must renew it. Follow the procedure in Creating a private key and a certificate signing request (SSL Setup tool) (on page 82) to request a new certificate and overwrite the existing one. You must also reconfigure the SSL server settings and SSL client settings.

Before you begin

Verify that the following settings are configured on the management server:

- The OCSP responder is functioning. If you are unsure whether it is functioning, contact the certificate authority.
- The server certificate has the Authority Information Access (AIA) record that includes the correct address of the OCSP responder.
- The management server can access the OCSP responder and access is not blocked by a proxy.

To check whether the AIA record includes the correct address of the OCSP responder, you can use the **`openssl`** command. Check the address of the `OCSP-URI` field of the AIA record. If no address is set, contact the certificate authority that signed the server certificate. The following is the command syntax and an example of the command:

Command syntax:

```
echo "Q" | installation-directory-of-Common-Services/openssl/bin/openssl s_client -
connect host-name-or-ip-address-of-product-URL:port-number-of-product-URL 2> /dev/
null | openssl x509 -noout -text
```

Command example:

```
echo "Q" | /opt/hitachi/CommonService/openssl/bin/openssl s_client -connect
example.com:443 2> /dev/null | openssl x509 -noout -text
```

You can check the revocation status of the server certificate in one of the following ways:

- Web browser: Checking the revocation status of the server certificate by using a web browser (on page 154)
- **`openssl`** command: Checking the revocation status of the server certificate by using a command (on page 155)
- Automatically by using cron: Checking the revocation status of the server certificate on a regular basis (on page 155)

Checking the revocation status of the server certificate by using a web browser

You can use the OCSP check function of your web browser to check the revocation status of the server certificate. For details on how to check the status, see the documentation for your browser.

For Firefox, you can check the status by using the following procedure.

Procedure

1. In the settings window of Firefox, select **Privacy & Security**, and then select the **Query OCSP responder servers to confirm the current validity of certificates** check box.
2. Use Firefox to access the URL for the target product, and then check whether an error appears.

   If the server certificate has expired, the `SEC_ERROR_REVOKED_CERTIFICATE` error appears.

   > **Note:** For API Configuration Manager and other products that do not have a web GUI, you cannot use a web browser to check the revocation status. In such cases, see Checking the revocation status of the server certificate by using a command (on page 155).

Checking the revocation status of the server certificate by using a command

You can check the revocation status of the server certificate by using the OCSP check function of the **`openssl`** command. For more details, see the openssl documentation.

Procedure

1. On the management server, run the following **`openssl`** command.

   Command syntax:

   ```
   installation-directory-of-Common-Services/openssl/bin/openssl ocsp -no_nonce -
   issuer issuer-certificate -cert server-certificate -url OCSP-Responder-URI -text
   ```

   The *issuer certificate* is either the root certificate or, if there is an intermediate certificate, specify the PEM-format certificate that combines the root and intermediate certificates.

   Command example:

   ```
   /opt/hitachi/CommonService/openssl/bin/openssl ocsp -no_nonce -issuer cacert.cer
   -cert httpsd.cer -url http://ad.example.com/ocsp -text
   ```

2. Check whether the value of `Cert Status` is `good`. If the value is `revoked`, the server certificate has expired.

Checking the revocation status of the server certificate on a regular basis

On the management server where Hitachi Ops Center products are installed, use cron to check the revocation status of the server certificate on a regular basis. The revocation status check results can be output to a file or to `syslog`.

Sending the revocation status check results to a file

Send the revocation status of a server certificate to a file as follows. Register a command in cron and send the check results to a file.

Procedure

1. Log in to the management server as the root user.

   If you log in as an ordinary user, use the **sudo** command to complete the following procedure as the root user.

2. Modify the crontab file. Run the following command.

   For details on the command, see the crontab documentation.

   ```
   crontab -u root -e
   ```

3. Add a command to the crontab file for each product for which you want to check revocation status.

   The command you set differs depending on how the server certificate of the product is referenced.

   If you check by downloading the certificate file from the URL of the Hitachi Ops Center product:

   Specify the time to download, the command to download the server certificate, and the command to query the OCSP responder in the following format.

   ```
   * * * * * command-to-download-the-server-certificate;command-to-query-the-
   OCSP-responder
   ```

   - Command syntax for downloading the server certificate:

     ```
     installation-directory-of-Common-Services/openssl/bin/openssl s_client -
     connect host-name-or-ip-address-of-product-URL:port-number-of-product-
     URL [-sigalgs Signature-Algorithm-list] < /dev/null 2> path-of-the-
     standard-error-output-file | sed -ne '/-BEGIN CERTIFICATE-/,/-END
     CERTIFICATE-/p' > path-of-download-destination-of-server-certificate
     ```

     For products that use both RSA and ECDSA server certificates, you must specify the command for RSA and again for ECDSA. For the `-sigalgs` option, specify the following signature algorithm list:

     For RSA: `RSA+SHA256:RSA+SHA384:RSA+SHA512:RSA-PSS+SHA256:RSA-PSS+SHA384:RSA-PSS+SHA512`

     For ECDSA: `ECDSA+SHA256:ECDSA+SHA384:ECDSA+SHA512`

   - Command syntax for querying the OCSP responder:

     ```
     installation-directory-of-Common-Services/openssl/bin/openssl ocsp -
     no_nonce -issuer issuer-certificate -cert path-of-server-certificate -
     url OCSP-Responder-URI [ -proxy [http[s]://][userinfo-of-proxy@]host-
     name-or-IP-address-of-proxy[:port-number-of-proxy] [/path-of-proxy] ] [-
     CAfile root-certificate-of-the-OCSP-responder-server] -text -out path-
     of-the-file-to-which-the-results-are-output 2>> path-of-the-standard-
     error-output-file
     ```

If you check by referencing the certificate file set for the Hitachi Ops Center product:

Specify the execution time and the command to query the OCSP responder in the following format.

```
* * * * * command-to-query-the-OCSP-responder
```

- Command syntax for querying the OCSP responder:

```
installation-directory-of-Common-Services/openssl/bin/openssl ocsp -
no_nonce -issuer issuer-certificate -cert path-of-server-certificate -
url OCSP-Responder-URI [ -proxy [http[s]://][userinfo-of-proxy@]host-
name-or-IP-address-of-proxy[:port-number-of-proxy] [/path-of-proxy] ] [-
CAfile root-certificate-of-the-OCSP-responder-server] -text -out path-
of-the-file-to-which-the-results-are-output 2> path-of-the-standard-
error-output-file
```

Note:

- Specify the time to run each command. Specify a value for "* * * * *". If you want to run the command every day at 4:00 a.m., specify "0 4 * * *". For details, see the crontab documentation.
- Specify different paths for *path-of-the-file-to-which-the-results-are-output* and *path-of-the-standard-error-output-file* for each command.
- For the *issuer-certificate* for the command that queries the OCSP responder, either specify the root certificate or, if there is an intermediate certificate, specify the PEM-format certificate that combines the root and intermediate certificates.
- To use a proxy for the command that queries the OCSP responder, specify the `-proxy` option.
- If the `Response Verify Failure` error is output to *standard-error-output-file*, specify the `-CAfile` option.
- For details on the **`openssl`** command, see the openssl documentation.

4. Add a command for each product, specifying each command as described in step 3.

   Example settings:

```
10 4 * * * command-for-product-1
20 4 * * * command-for-product-2
30 4 * * * command-for-product-3
…
```

5. After you finish specifying the commands, save the crontab file.
6. Run the following command to enable crond.service.

```
systemctl enable crond.service
```

7. Restart the service to apply the crond settings. Run the following command.

```
systemctl restart crond
```

Result

- At the specified time, a file is output to the directory specified in *path-of-the-file-to-which-the-results-are-output*. Check the value of `Cert Status` in the output file.
  - If the value is `good`: The server certificate is valid.
  - If the value is `revoked`: The server certificate has been revoked.
  - If the value is `unknown`: The status is unknown.
- If the output file does not include the `Cert Status` line, an error might have occurred. For details about the error, check the file output to the directory specified in *path-of-the-standard-error-output-file*.

Outputting the revocation status check results to syslog

Output the revocation status of the server certificate to `syslog` as follows.

Procedure

1. Register a command in cron for each product whose revocation status you want to check.

   For details on how to specify the command, see Sending the revocation status check results to a file (on page 155). To output the results to `syslog`, you do not need to specify the `-out` option.
2. Change the crond settings. Open crond in a text editor such as vi editor and add `-s` to the `CRONDARGS` value.

   If you use the default value, the check results will be output to `/var/log/cron`.

```
CRONDARGS=-s
```

3. Restart the service to apply the crond settings. Run the following command.

```
systemctl restart crond
```

Result

At the specified time, the results are output to `syslog`. Search the `syslog` file for `Cert Status`. The result will be `good`, `revoked`, or `unknown`.

Changing the management server host name, IP address, or port number

If you change the management server host name or IP address or the port number used by Common Services, run the **`cschgconnect`** command to change the URL for accessing the Hitachi Ops Center Portal.

In order to change IP address of the server where Administrator is installed, setting Administrator is necessary before changing the IP address. Refer to "Modifying the Ops Center Administrator server's IP address" in *Hitachi Ops Center Administrator Getting Started Guide* to change Administrator configuration and then change the IP address.

Procedure

1. Log in to the management server as the root user.

   If you log in as an ordinary user, use the **`sudo`** command to complete the following procedure as the root user.

2. Run the **`cschgconnect`** command.

   Command location

   `installation-directory-of-Common-Services``/utility/bin/cschgconnect.sh`

   Format

   ```
   cschgconnect.sh [-h host-name-or-IP-address] [-p port-number] | -enableip
   {true|false} | -list
   ```

   Options

   `-h` ***`host-name-or-IP-address`***

   Specify the host name (or FQDN) or IP address used to access the Hitachi Ops Center Portal. If you specify a host name (or FQDN), specify a value using no more than 128 characters. For the host name (or FQDN), you cannot specify uppercase characters. If you do, they are converted to lowercase characters and then registered.

   The management server on which Common Services and other relevant products are installed and the web browser used to access the Hitachi Ops Center Portal must be able to resolve and reach the host name (or FQDN) and IP address.

   `-p` ***`port-number`***

   Specify the port number used by Common Services.

   > **Note:** If you change the port number, you must also change the firewall setting.

`-enableip {true|false}`

Specify whether an IP address can be used when the host name or FQDN is used in the URL for the Hitachi Ops Center Portal. To specify that the portal can be accessed by using an IP address, specify `true`. To specify that the portal cannot be accessed by using an IP address, specify `false`. The IP address for accessing the portal is automatically acquired from the system.

This option and other options cannot be specified at the same time.

`-list`

Displays the current settings. This option and other options cannot be specified at the same time.

If you change the settings by using the `-h`, `-p`, or `-enableip` option, the settings displayed when you specify the `-list` option are not applied to the system until the Common Services service is restarted.

> **Note:** If you use this command to change the host name or IP address to one that differs from the value set for `CN` or `subjectAltName` when the SSL server certificate was created, you must issue a new server certificate.

3. Restart the Common Services service.
4. Run the following command to check the result of the change.

```
cschgconnect.sh -list
```

5. Make sure that you can use a web browser to access the login window at the following URL:

   https://*host-name-or-IP-address-of-Portal*:*port-number*/portal

6. For each product registered in Common Services, run the **`setupcommonservice`** command for registering the product in Common Services again.

   For details, see the documentation for each product.

Changing the port number used for internal communications

You can change the port number that Common Services uses for internal communications.

Procedure

1. Log in to the management server as the root user.

   If you log in as an ordinary user, use the **`sudo`** command to complete the following procedure as the root user.
2. Change the port number.

   The procedure differs depending on the port number.

Port number	Change procedure
20951	**a.** In the following property file, specify the port number after the change, and then save the file. **Property file location*** /var/*installation-directory-of-Common-Services*/userconf/config_user.properties **Settings** CS_PORTAL_PORT=*port-number-after-change* CS_GW_PORTAL_PORT=*port-number-after-change* **b.** Restart the Common Services service.
20952	**a.** In the following property file, specify the port number after the change, and then save the file. **Property file location*** /var/*installation-directory-of-Common-Services*/userconf/config_user.properties **Settings** CS_PORTAL_IDP_PORT=*port-number-after-change* CS_IDP_OP_HTTP_PORT=*port-number-after-change* CS_GW_IDP_PORT=*port-number-after-change* **b.** Restart the Common Services service.
20954	**a.** In the following property file, specify the port number after the change, and then save the file. **Property file location*** /var/*installation-directory-of-Common-Services*/userconf/config_user.properties **Setting** CS_PORTAL_IDP_POSTGRESQL_PORT=*port-number-after-change* **b.** In the following configuration definitions file, specify the port number after the change, and then save the file. **Definitions file location*** /var/*installation-directory-of-Common-Services*/pgdata/csidp/data/postgresql.conf

Port number	Change procedure
	Setting `port = port-number-after-change # (change requires restart)` **c.** Stop the Common Services service. **d.** Run the **`systemctl`** command to restart `postgresql-15@csidp`. **e.** Start the Common Services service.

20955	**a.** In the following property file, specify the port number after the change, and then save the file.
	Property file location*
	`/var/`*`installation-directory-of-Common-Services`*`/userconf/config_user.properties`
	Setting
	`CS_PORTAL_POSTGRESQL_PORT=port-number-after-change`
	b. In the following configuration definitions file, specify the port number after the change, and then save the file.
	Definitions file location*
	`/var/`*`installation-directory-of-Common-Services`*`/pgdata/csportal/data/postgresql.conf`
	Setting
	`port = port-number-after-change # (change requires restart)`
	c. Stop the Common Services service.
	d. Run the **`systemctl`** command to restart `postgresql-15@csportal`.
	e. Start the Common Services service.

20956	**a.** In the following property file, specify the port number after the change, and then save the file. **Property file location*** `/var/`*`installation-directory-of-Common-Services`*`/userconf/config_user.properties`

Port number	Change procedure
	Setting `CS_PORTAL_MANAGEMENT_PORT=`*`port-number-after-change`* **b.** Restart the Common Services service.
* If you performed installation by using an OVA, the file is located in the following directory: `/var/opt/hitachi/CommonService/userconf/`	

Backing up and recovering Hitachi Ops Center applications

This sections provides information on backing up and recovering your Hitachi Ops Center applications. You can backup and recover automatically using Protector or manually as described in the following sections:

- Backing up and restoring Hitachi Ops Center applications using Protector (on page 163)
- Backing up and restoring Ops Center applications manually (on page 175)

Backing up and restoring Hitachi Ops Center applications using Protector

You can schedule automatic backups for Hitachi Ops Center applications by using Protector. You can then restore your backups to recover each application.

You create backups by running Protector and selecting one or more Ops Center product components. (on page 166)

The restoration process consists of two stages, *restore* and *recovery*:

1. Restoring backup archives to the proper node using Protector (on page 167).
2. Recovering each application by manually extracting the archive and running the required commands to bring it back online. (on page 168)

Note: Analyzer detail view and Analyzer probe server are automatically recovered as part of the restore process, so no manual recovery is necessary. All other applications require the two-stage restore and recovery.

Caution:

Before starting a backup or recovery, review the following:

- Prerequisites and cautions for backing up Hitachi Ops Center applications (on page 164)
- Prerequisites and cautions for recovering Hitachi Ops Center applications (on page 165)

Prerequisites and cautions for backing up Hitachi Ops Center applications

There are specific and prerequisites for creating backups as described in the following table.

Application	Precautions
All	▪ Each server (or VM) to be backed up must have a Protector client installed and configured. (If a Hitachi Ops Center application is installed on the same server as the Protector master, no client is necessary.) **Note:** The Analyzer probe OVA includes the Protector client. ▪ Protector stores backup files in a repository. Prepare a Protector repository that includes the total size of backup files for each product.
Administrator	Before backing up Administrator, verify the following: ▪ Administrator service is running. ▪ No backup or restore jobs are running. ▪ The Virtual Appliance Manager log level is set to INFO (DEBUG or TRACE might cause the backup to fail).
Analyzer	During a backup, the Analyzer server stops Common Component, so other products that are using Common Component also stop.
Analyzer RAID Agent	RAID Agent backups only include settings information. If you also want to back up the performance data used by the API requests that access RAID Agent, see the section explaining RAID Agent backups in the *Hitachi Ops Center Analyzer Installation and Configuration Guide*, and run the **`htmhsbackup`** command.
Analyzer probe	Instances of the Windows probes are not backed up when using Protector.

Application	Precautions
Analyzer On-demand real time monitoring module	The on-demand real time monitoring module installed on a Windows host is not backed up when using Protector.
Automator	▪ Automator running on Windows is not backed up when using Protector. Only Linux is supported. ▪ During a backup, the Automator server stops Common Component, so other products that are using Common Component also stop. ▪ Make sure that no tasks are currently being processed in the Automator "Status" column of the Tasks tab with a status of "In Progress", "Waiting for Input", "In Progress (with Error)", "Long Running", or "In Progress (Terminating)".
API Configuration Manager	▪ When API Configuration Manager is installed by a non-root Linux user, you cannot back up by using Protector. ▪ When backing up, API Configuration Manager cannot be used because necessary services are temporarily stopped.
Common Services	If the server certificate and private key are stored in a location other than the following default, manually back up the server certificate and private key: `/var/`*`Common-Services-installation-directory`*`/tls/`

Prerequisites and cautions for recovering Hitachi Ops Center applications

Depending on the Hitachi Ops Center application, there are restrictions on how you can recover an application. For example, you cannot recover all applications when using a different IP address, host name, or Hitachi Ops Center version. For details, see the following table.

Application	Move data to different host name	Move data to different IP address	Move data to different Hitachi Ops Center version
Administrator	Supported[1]	Supported[1]	Supported
Automator	Not supported	Not supported	Not supported

Application	Move data to different host name	Move data to different IP address	Move data to different Hitachi Ops Center version
Common Services	Supported[2]	Supported[2]	Not supported
Analyzer	Supported	Supported	Not supported
Analyzer viewpoint	Not supported	Not supported	Not supported
API Configuration Manager	Not supported	Not supported	Not supported
Protector	Supported[3]	Supported	Not supported

Notes:

1. Each individual OVA has a separate OS setting, so the host information will be the same as the original.
2. The Installation path must be the same as the original.
3. The original Master Node name appears in the GUI and cannot be changed.

Note: By default, the recovery process uses `/tmp` for temporary storage. You can change this location by using the system environment variable (UBI_BACKUP_TMP_DIR). The location must be an absolute path (no symbolic links). You can set UBI_BACKUP_TMP_DIR as follows:

1. Open the `/etc/systemd/system.conf` file and add the following:

   ```
   DefaultEnvironment="UBI_BACKUP_TMP_DIR=directory"
   ```

2. Restart the OS.

Backing up Ops Center applications using Protector

You can create scheduled or immediate backups of Ops Center applications using Protector. This procedure applies to all Ops Center product components.

Before you begin

- If you are not planning to use an existing repository node, you must configure a new one before proceeding.
- You can only restore one application at a time.

Procedure

1. Log in to the Protector UI.
2. In the **Policies** window, click the plus (+) icon near the top of the screen, enter a name (example: MasterBackup), and click **Next**.
3. Click **Next** to skip **Allocate Policy to Access Control Resource Group**.

4. In the **Add one or more Classifications** window, click on the plus (+) icon, click **Application**, select **Ops Center**, and click **Next**.
5. In the **Specify Ops Center Applications** window, choose the master node as a source, and then choose whether you want to **Include all Ops Center Applications**, or select individual products by clicking **Add**. (You can also exclude products.) Click **Apply**.
6. In the **Add one or more Operations** window, click the plus (+) icon, select **Backup**, and click **Next**.
7. In the **Specify Backup operation attributes** window, you can set the schedule and retention for your backups. Click **Apply** to return to the **Add one or more Operations** window and click **Finish**.
8. Select **Data Flows**, click the plus (+) icon, enter a name (example: MasterBackup) and click **Next**.
9. Click **Next** to skip **Allocate Policy to Access Control Resource Group**.
10. In the **Create Data Flows** window, drag the master node from the **Nodes** tab into the workspace, then drag the repository you want to use to store the backup.
11. Click the master node and select **MasterBackup** from the **Policies** list.
12. Click the repository and select **MasterBackup** from the **Policies** list.
13. Click **Finish**.
14. In **Data Flows**, select **MasterBackup** from the list, and click the play icon in the toolbar.
15. In **Activate Data Flows**, click **Activate**.
16. In the **Monitor** window, you can start the backup immediately by selecting **MasterBackup** and clicking the trigger (lightning) icon. (Otherwise, the backup occurs according to the schedule.)
17. Select the operation and click **Run Now**. You can check the overall progress in the Jobs window or the details in the **Log** window.

Next steps

To recover an Ops Center application, you must first restore the backup archive as described in Restoring Ops Center application archives using Protector (on page 167).

Restoring Ops Center application archives using Protector

You can use Ops Center Protector to restore a backup archive to the server or VM where you plan to perform the recovery of the application.

Before you begin

- Analyzer detail view and Analyzer probe server are automatically recovered as part of the restore process described here, so no manual recovery is necessary. You must manually recover all other applications after the backup archive is restored using this procedure.
- If you used an OVA to install an application, the log message for the restore might state that it "succeeded with warnings." This can be safely ignored.

Procedure

1. In the **Restore** window, select the backup from the list and click the restore icon.

2. In **Select restore** options, choose the **Destination Node** to which you want the backup archive exported.
3. Click **Finish**.
4. You can check the overall progress in the **Jobs** window or the details in the **Log** window.

Recovering Hitachi Ops Center applications from a backup archive

After the backup archive has been restored (copied to the proper node or VM), you can recover your Hitachi Ops Center application. You must follow the recovery procedure for each product and any related agents by extracting each archive and supplying the path to the backup file required by the command line for each product and agent.

The recovery process for each product is described in the sections that follow:

- Administrator (on page 168)
- Analyzer (on page 169)
- Analyzer RAID Agent (on page 169)
- Analyzer detail view (on page 172)
- Analyzer probe (on page 172)
- Analyzer viewpoint (on page 172)
- Analyzer Virtual Storage Software Agent (on page 173)
- Analyzer On-demand real time monitoring module (on page 173)
- Automator (on page 174)
- API Configuration Manager (on page 174)
- Common Services (on page 175)
- Protector (on page 175)

Recovering Administrator

To recover Administrator from a backup archive, complete the following steps:

1. Access the Virtual Appliance Manager by opening a browser and entering the following URL.

   ```
   https://ip-address:port/vam
   ```

   where:

   - *ip-address* is the IP address of the Administrator server.
   - *port* is the port number of the Administrator server. The default port number is 443 or 20961. The default login credentials are `sysadmin`/`sysadmin`.

2. Click Restore and either drag and drop the backup file or click the plus sign (+) to browse.

3. Click Submit. The restore procedure can take up to an hour, after which Administrator restarts.
4. Remove and reregister Administrator in Common Services.
   a. Remove Administrator from Common Services by going to the Hitachi Ops Center Portal and deleting it.
   b. Run the **`setupcommonservice`** command to register with Common Services.
   c. If necessary, change permissions for user groups.

Recovering Analyzer

To recover Analyzer from a backup archive, complete the following steps:

1. Run the **`tar`** command to extract the backup archive file.

   ```
   tar xf backup-archive-file -C destination-directory
   ```

2. Run the following **`restoresystem`** command.

   ```
   Analyzer-installation-directory/Analytics/bin/restoresystem -dir
   destination-directory -type all
   ```

For details, see the description of the **`restoresystem`** command in the *Hitachi Ops Center Analyzer Installation and Configuration Guide*.

> **Note:** Private key files and server certificate files created or obtained by the user are not backed up. Depending on the location, the files might be included in the backup data; however, as a general rule, manually relocate the files when you recover.

Recovering Analyzer RAID Agent

<For Linux>

Before you begin

Before recovering Analyzer RAID Agent, verify the following:

- If instances with the same names as those on the backup source do not exist in the restore destination, manually create RAID Agent instances using the same instance names as those on the backup source.
- Verify that the following items are the same between the backup source host and the restore destination host:
  - OS (Linux)
  - Version number of the RAID Agent
  - Instance name
  - Hybrid Store storage destination
- 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.

To recover Analyzer RAID Agent from a backup archive, complete the following steps:

1. Confirm that the same name instance exists as when the backup was taken, and if it does not exist, create it.
2. Copy the backup archive file to a working directory and extract it:

   ```
   tar xf backup-archive-file
   ```

3. Run the following command to restore the performance data and configuration information files:

   ```
   /opt/jp1pc/htnm/bin/htmhsrestore -dir extracted-data-directory
   ```

4. Run the **`jpctdchkinst`** command to check whether the instance is monitoring the targets correctly. If it is not, run the **`jpcinssetup`** command to change the settings, and then run the **`jpctdchkinst`** command again to check the monitoring status.

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

Note:

- Private key files and server certificate files created or obtained by the user are not backed up. Depending on the location, the files might be included in the backup data; however, as a general rule, manually relocate the files when you recover.
- You cannot restore the following by using the **`htmhsrestore`** command and must make any required changes manually:
  - If you changed the port numbers or SSL communication settings in the backup source environment, you must also change them in the restore destination by editing the following file.

    ```
    /opt/jp1pc/htnm/Rest/config/htnm_httpsd.conf
    ```

  - 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.

    ```
    /opt/jp1pc/htnm/Rest/config/htnm_httpsd.conf
    ```

    ```
    /opt/jp1pc/htnm/HBasePSB/CC/server/usrconf/ejb/
    AgentRESTService/usrconf.properties
    ```

<For Windows>

Before you begin

Before recovering Analyzer RAID Agent, verify the following:

- If instances with the same names as those on the backup source do not exist in the restore destination, manually create RAID Agent instances using the same instance names as those on the backup source.
- Verify that the following items are the same between the backup source host and the restore destination host:
  - OS (Windows)
  - Version number of the RAID Agent
  - Instance name
  - Hybrid Store storage destination
- 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.

To recover Analyzer RAID Agent from a backup archive, complete the following steps:

1. Confirm that same name instance exists as when the backup was taken, and if it does not exist, create it.
2. Copy the backup archive file to a working folder and extract it:

   ```
   tar xf backup-archive-file
   ```

3. Run the following command to restore the performance data and configuration information files:

   ```
   Analyzer-RAID-Agent-Installation-folder\htnm\bin\htmhsrestore -
   dir extracted-data-folder
   ```

4. Run the **jpctdchkinst** command to check whether the instance is monitoring the targets correctly. If it is not, run the **jpcinssetup** command to change the settings, and then run the **jpctdchkinst** command again to check the monitoring status.

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

Note:

- Private key files and server certificate files created or obtained by the user are not backed up. Depending on the location, the files might be included in the backup data; however, as a general rule, manually relocate the files when you recover.
- You cannot restore the following settings by using the **`htmhsrestore`** command and must make any required changes manually:
  - If you changed the port numbers or SSL communication settings in the backup source environment, you must also change them in the restore destination by editing the following file.

    ```
    Analyzer-RAID-Agent-Installation-folder\htnm\Rest
    \config\htnm_httpsd.conf
    ```

  - 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.

    ```
    Analyzer-RAID-Agent-Installation-folder\htnm\Rest
    \config\htnm_httpsd.conf
    ```

    ```
    Analyzer-RAID-Agent-Installation-folder\htnm\HBasePSB
    \CC\server\usrconf\ejb\AgentRESTService
    \usrconf.properties
    ```

Recovering Analyzer detail view

To recover Analyzer detail view from a backup archive, see the *Hitachi Ops Center Analyzer Installation and Configuration Guide*.

Note: Private key files and server certificate files created or obtained by the user are not backed up. Depending on the location, the files might be included in the backup data; however, as a general rule, manually relocate the files when you recover.

Recovering Analyzer probe

To recover Analyzer probe from a backup archive, see the *Hitachi Ops Center Analyzer Installation and Configuration Guide*.

Note: Private key files and server certificate files created or obtained by the user are not backed up. Depending on the location, the files might be included in the backup data; however, as a general rule, manually relocate the files when you recover.

Recovering Analyzer viewpoint

To recover Analyzer viewpoint from a backup archive, run the following command:

1. Run the following restore command.

   ```
   /opt/hitachi/analyzer_viewpoint/bin/restore --file {backup-archive-file-path}
   ```

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

> **Note:** Private key files and server certificate files created or obtained by the user are not backed up. Depending on the location, the files might be included in the backup data; however, as a general rule, manually relocate the files when you recover.

Recovering Analyzer Virtual Storage Software Agent

To recover Analyzer Virtual Storage Software Agent from a backup archive, complete the following steps:

1. Extract the archive file. For the specific file path, see the Protector GUI.
2. Copy the contents to the following directories:

   ```
   /var/{installation-directory}/system/access-points.yaml
   ```

   ```
   /var/{installation-directory}/config/userconfig-setting.yaml
   ```

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

> **Note:** Private key files and server certificate files created or obtained by the user are not backed up. Depending on the location, the files might be included in the backup data; however, as a general rule, manually relocate the files when you recover.

Recovering Analyzer On-demand real time monitoring module (Linux only)

To recover the Analyzer On-demand real time monitoring module for Linux from a backup archive, complete the following steps:

1. Extract the archive file. For the specific file path, see the Protector GUI.
2. Copy the contents to the following directories:

   ```
   /opt/hitachi/Analytics/granular-data-collection-api/conf/user-granular-data-collection-api.conf
   ```

   ```
   /opt/hitachi/Analytics/granular-data-collection-api/conf/system-granular-data-collection-api.conf
   ```

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

> **Note:** Private key files and server certificate files created or obtained by the user are not backed up. Depending on the location, the files might be included in the backup data; however, as a general rule, manually relocate the files when you recover.

Recovering Automator

Before you begin

- Verify the following settings are the same between the backup source host and the restore destination host:
  - Host name and IP address
  - Account of the OS user used by Automator
  - Hitachi Ops Center product environment (configuration, version, and revision)
  - Installation path of Automator
  - System locale and character set
- Verify that no tasks are currently being processed in the Automator "Status" column of the Tasks tab with a status of "In Progress", "Waiting for Input", "In Progress (with Error)", "Long Running", or "In Progress (Terminating)".

To recover Automator from a backup archive, complete the following steps:

1. Run the **`tar`** command to extract the backup archive file:

   ```
   tar xvf backup-archive-file -C destination-file-path
   ```

2. Run the **`restoresystem`** command:

   ```
   Automator-installation-directory/bin/restoresystem -dir
   destination-file-path -auto
   ```

For details about **`restoresystem`** command, see the *Hitachi Ops Center Automator Installation and Configuration Guide*.

Recovering API Configuration Manager

To recover API Configuration Manager from a backup archive, complete the following steps:

1. Run the **`jar`** command to extract the backup archive file:

   Windows:

   ```
   Configuration-Manager-installation-directory\base\jdk\bin
   \jar xf backup-archive-file ConfManager
   ```

   Linux:

   ```
   Configuration-Manager-installation-directory/
   base/jdk/bin/jar xf backup-archive-file ConfManager
   ```

2. Restore the extracted files. For details, see "Restoring the REST API database and environment settings file" in the *Hitachi Ops Center API Configuration Manager REST API Reference Guide*.

Note: Private key files and server certificate files created or obtained by the user are not backed up. Depending on the location, the files might be included in the backup data; however, as a general rule, manually relocate the files when you recover.

Recovering Common Services

Before you begin

Verify the installation path and version number of Common Services are the same between the backup source host and the restore destination host.

To recover Common Services from a backup archive, run the following **`csrestore`** command for the applicable data.

```
Common-Services-installation-directory/utility/bin/csrestore.sh -
file backup-archive-file
```

For details, see Restoring Common Services (on page 178).

Note: Data backed up by using Common Services in a viewpoint OVF environment cannot be restored to the installer version of Common Services.

Recovering Protector

To restore Protector from a backup archive, see the *Hitachi Ops Center Protector User Guide*.

Backing up and restoring Ops Center applications manually

You can back up and restore Ops Center applications manually.

You can also schedule backups using Ops Center Protector as described in Backing up and restoring Hitachi Ops Center applications using Protector (on page 163).

Product	Command	Procedure
Ops Center Common Services	**1.** Log in to the management server as the root user. **2.** Stop the Common Services service. **3.** Run the **`csbackup`** or **`csrestore`** command.	See Starting or stopping the Common Services service (on page 152). See Backing up Common Services (on page 177). See Restoring Common Services (on page 178).
Ops Center Analyzer	**1.** Stop each service in the following order and back up the setting information: ▪ Analyzer viewpoint server ▪ Analyzer server ▪ Analyzer detail view server	For details on backing up, see the *Hitachi Ops Center Analyzer Installation and Configuration Guide*.

Product	Command	Procedure
	- Analyzer probe server - RAID Agent 2. Back up and restore each of the Ops Center Analyzer components.	
Ops Center Administrator	**To back up:** Log in to Virtual Appliance Manager and click **Backup** to download a `tar.gz` file containing the system settings. **To restore:** 1. Log in to Virtual Appliance Manager and click **Restore** and either drag and drop the backup file or click the plus sign. 2. Click **Submit**.	For details, see the *Hitachi Ops Center Administrator User Guide*.
Ops Center Automator	To back up or restore the system configuration for Automator, use the **`backupsystem`** and **`restoresystem`** commands.	For details, see the *Hitachi Ops Center Automator Installation and Configuration Guide*.
Ops Center Protector	Use the **`mastersettings`** command to back up and restore the configuration settings of the master node.	For details, see the *Hitachi Ops Center Protector Installation and Configuration Guide*.
Hitachi Ops Center API Configuration Manager	You must manually back up and restore the REST API files.	For details on backing up, see the *Hitachi Ops Center API Configuration Manager Reference Guide*.

Backing up and restoring Common Services

You can back up and restore Common Services system information.

Backing up Common Services

To back up data in Common Services, run the **`csbackup`** command. You can restore the backup data to an instance of Common Services in an environment that has the same installation configuration and version.

Procedure

1. As necessary, back up each product registered in Common Services.

   For details on how to back up each product, see the documentation for each product.
2. Log in to the management server as the root user.

   If you log in as an ordinary user, use the **`sudo`** command to complete the following procedure as the root user.
3. Stop the Common Services service.
4. Run the **`csbackup`** command.

   Command location

   `installation-directory-of-Common-Services``/utility/bin/csbackup.sh`

   Format

   ```
   csbackup.sh -dir backup-destination-directory
   ```

   Option

   `-dir` ***`backup-destination-directory`***

   Specify the path to the directory that stores the backup data. A relative path can be specified. A backup file, with the following file name, is output to the specified directory.

   `csbackup_`*`YYYY-MM-DD-hh-mm-ss_VVRRSS`*`.tar.gz`

   VVRRSS indicates the version of Common Services.

   Example:

   If the version is 11.0.0-01, *VVRRSS* is 110001.

   > **Note:** Each time data is backed up, the number of backup files increases. For this reason, if data is backed up regularly over a long period of time, the backup files might take up a large amount of disk space. Delete backup files that are no longer necessary.
5. If the server certificate and secret key are stored in a location other than the following default, manually back up the server certificate and secret key.

   `/var/`*`installation-directory-of-Common-Services`*`/tls/`

   For example, for an OVA install uses the following directory:

   `/var/opt/hitachi/CommonService/tls/`

> **Note:** If SSL communication was set up by using the **`cssslsetup`** command, the secret key of the server certificate is stored in the location specified when the command was run.

6. Start the Common Services service.

Restoring Common Services

To restore the Common Services backup data, run the **`csrestore`** command.

Before you begin

Make sure that the installation configuration and version of Common Services on the restoration-destination system are the same as those on the system where the backup was taken. You cannot restore backup data to a system that has a different installation configuration and version.

Procedure

1. Log in to the management server as the root user.

   If you log in as an ordinary user, use the **`sudo`** command to complete the following procedure as the root user.
2. Stop the Common Services service.
3. Run the **`csrestore`** command.

   Command location

   `installation-directory-of-Common-Services``/utility/bin/csrestore.sh`

   Format

   ```
   csrestore.sh -file path-to-backup-file
   ```

   Option

   `-file path-to-backup-file`

   Specify the path to the backup file to be restored. A relative path can be specified.

4. If the server certificate and secret key were stored in a location other than `/var/`*`installation-directory-of-Common-Services`*`/tls/`* and backed up manually, store the server certificate and secret key in the same location that was used for backup.

   * For example, for an OVA install uses the following directory:

   `/var/opt/hitachi/CommonService/tls/`

   > **Note:** If you set up SSL communication by using the **`cssslsetup`** command prior to performing backup, store the server certificate and the secret key in the location you specified.

5. If the host name, IP address, or port number of Common Services at the restoration destination is changed, run the **`cschgconnect`** command to change the settings.

   For details on the **`cschgconnect`** command, see Changing the management server host name, IP address, or port number (on page 159).

   > **Note:** If the backup data of Common Services deployed by using the Analyzer viewpoint OVF is restored to Common Services installed by using the individual installer, you must manually run the following command:
   >
   > ```
   > cschgconnect.sh -p port-number
   > ```

6. Start the Common Services service.
7. As necessary, restore the backup data for each product registered in Common Services.

   For details on the restoration method and the prerequisites for restoring backup data, see the documentation for each product.
8. If any products are registered in Common Services, delete each product in the Hitachi Ops Center Portal, and then register the products in Common Services again.

   To re-register the products in Common Services, run the **`setupcommonservice`** command for each product. For details on the **`setupcommonservice`** command, see the documentation for each product.

Stopping unnecessary product services

After deploying the Ops Center OVA, you can stop the services of products that you do not use, and specify not to start the services when the OS starts.

After the OVA is deployed, as a best practice, we recommend that you remove any products that are not being used. If you decide not to remove them, you can use the **`opsvmservicectl`** command to stop multiple product services at the same time. You can also use the command to change the setting so that the services do not start when the OS starts.

> **Note:** The **`opsvmservicectl`** command is installed with version 10.1.0 or a later of the Ops Center OVA. If the individual installer or a version of the OVA earlier than 10.1.0 was used, uninstall any unnecessary products.

Before you begin

After you deploy the OVA and finish the configuration using the setup tool (**`opsvmsetup`**).

Procedure

1. From a VMware vSphere client, log in to the guest OS as the root user.
2. Run the **`opsvmservicectl`** command to stop the services for the products that are not needed.

   Format

   ```
   opsvmservicectl {disable|enable} product-name [product-name ...]
   ```

Options

`disable`

Stops the services for the specified products and prevents them from starting automatically when the OS starts. After you stop the services, the products remain registered in Common Services.

`enable`

Starts the services for the specified products and changes the setting so that the services automatically start when the OS starts.

`product-name`

Specify the target products by specifying the following values. To specify multiple products, use spaces to separate the products.

Product name	Value to specify
Automator	`Automator`
Analyzer	`Analyzer`
Analyzer detail view	`AnalyzerDetailView`
API Configuration Manager	`APIConfigurationManager`
Protector	`Protector`
Administrator	`Administrator`
Common Services	`CommonServices`

> **Note:** Do not perform an upgrade installation of a product that is disabled by using the **`opsvmservicectl`** command, because the product might not operate correctly.

3. Check the results by running the following command:

```
opsvmservicectl status
```

4. To delete the products, log in to the Hitachi Ops Center Portal and remove them.

Resetting the trust relationship with each product

If unauthorized access to Common Services occurs or unauthorized operations are performed on the Common Services settings, information such as tokens exchanged between Common Services and each product might be leaked. In this case, reset and disable the information that might have been compromised.

Procedure

1. Log in to the management server as the root user.

   If you log in as an ordinary user, use the **`sudo`** command to complete the following procedure as the root user.

2. Run the **`csresettrustrelationship`** command.

   Command location

   `installation-directory-of-Common-Services``/utility/bin/csresettrustrelationship.sh`

   Format

   ```
   csresettrustrelationship.sh -f
   ```

   Option

   `-f`

   Specify this option if you run this command. If you omit this option, the command usage is displayed.

   Output file

   The results of running the command are output to the following file:

   `/var/log/hitachi/CommonService/utility/result_reset_secert.json`

   Note:

   - If you run this command, logged-in users might be forcibly logged out.
   - This command runs for a period from several minutes to several tens of minutes, depending on the system configuration.
   - When the command finishes running, Common Services restarts.

3. Check the content of the output file.

   Make sure that the value of the `status` key is `SUCCESS` for both the `resetSecretResult` object and the `resetKeyResult` object.

   If the value is `ERROR`, restart Common Services, and then rerun the command. If this does not resolve the problem, collect the failure information, and contact customer support.

4. If you are linking with the identity provider by using the SAML protocol, update the metadata for Common Services in identity provider.

   This step is required because when you reset the trust relationship, the authentication key of Common Services is forcibly updated.

For details of the procedure, see one of the following topics, based on the linked identity provider:

- If a link is established with AD FS: Updating the Common Services metadata by using AD FS (on page 134)
- If a link is established with an identity provider other than AD FS: Updating the Common Services certificates (on page 147)

5. Run the **`csreregisterapp`** command or run the **`setupcommonservice`** command to re-register each product registered in Common Services.

   You can use the **`csreregisterapp`** command to re-register multiple products at once. For details, see Re-registering each product in Common Services (on page 182).
6. Restart the service of each product registered in Common Services.

Re-registering each product in Common Services

If you reset the trust relationships with each product, you must re-register each product registered in Common Services. If you use the **`csreregisterapp`** command, you can re-register each of the products in Common Services at once.

Before you begin

- Run the **`csreregisterapp`** command on the management server where the product you want to re-register is installed. To run the command on a management server and Analyzer probe server where Common Services is not installed, obtain the **`csreregisterapp`** command in advance. You can obtain the **`csreregisterapp`** command by getting `utility.tar` from the following installation media and extracting the files:
  - *`root-directory-of-the-Common-Services-installation-media`*`/utility.tar`
  - *`root-directory-of-the-Server-Express-installer-media`*`/COMMONSERVICES/utility.tar`
  - *`root-directory-of-the-Client-Express-installer-media`*`/COMMONSERVICES/utility.tar`
- The **`csreregisterapp`** command is stored in the following directory after the files are extracted from `utility.tar`:

  `directory-where-utility.tar-is-extracted``/utility/bin`
- To run the **`csreregisterapp`** command, the expect package needs to be installed. The expect package is installed on management servers where Common Services version 11.0.4 or later is installed.

Procedure

1. Log in to the management server as the root user.

   If you log in as an ordinary user, use the **`sudo`** command to complete the following procedure as the root user.

2. Run the **`csreregisterapp`** command.

   Command location

   If Common Services is installed on the management server:

   `installation-directory-of-Common-Services``/utility/bin`

   If Common Services is not installed on the management server:

   `directory-where-utility.tar-is-extracted``/utility/bin`

   Format

   ```
   csreregisterapp.sh [-cshost host-name-or-IP-address-of-Common-Services] [-
   csport port-number-of-Common-Services] [-apphost host-name-or-IP-address-
   of-Product]
   ```

   Options

   `-cshost` ***`host-name-or-IP-address-of-Common-Services`***

   Specify the host name (FQDN) or IP address for the URL to access Common Services. If you omit this option, the host name of the server on which the command was run will be specified. Specify this option if either of the following applies:

   - If you are specifying the host name in FQDN format or IP address for the URL to access Common Services
   - If the products to be re-registered and Common Services are installed on separate management servers

   `-csport` ***`port-number-of-Common-Services`***

   Specify the port number for the URL to access Common Services. If you omit this option, 443 will be specified.

   `-apphost` ***`host-name-or-IP-address-of-Product`***

   Specify the host name (FQDN) or IP address for the URL to access the product to be re-registered in Common Services. If you omit this option, the host name of the server on which the command was run will be specified. Specify this option if you specified a host name in FQDN format or IP address for the URL to access the product you want to re-register.

3. Specify the user and password for Common Services.

   Specify a user who belongs to the opscenter-administrators group.

4. When re-registering Administrator, specify whether to verify the SSL certificate for communications with Common Services. To perform verification, specify **y**, and then specify the root certificate of the certificate authority that signed the Common Services server certificate by using the absolute path.

5. When you have finished running the command, the results will be displayed. Products for which **failed** is displayed could not be re-registered. Check the cause by referring to the log files in the following storage locations, and then rerun the command.

If Common Services is installed on the management server:

`/var/log/hitachi/CommonService/utility/csreregisterapp_`*`YYYY-MM-DD-hh-mm-ss`*`.log`

If Common Services is not installed on the management server:

`/tmp/csreregisterapp_`*`YYYY-MM-DD-hh-mm-ss`*`.log`

> **Note:** Products with **warning** displayed in the command execution results are successfully re-registered. However, the product names or product descriptions displayed on the Hitachi Ops Center Portal could not be carried over. In this case, the following information will be displayed in the Products window for items that are not carried over for the re-registered product:
>
> - Product name: The host name or IP address of the management server on which the re-registered product is installed will be displayed.
> - Product description: The content before re-registration will be deleted, leaving it in a not configured state.
>
> To reset the product name and product description, in the Products window on the Hitachi Ops Center Portal, click the **Edit** icon for the relevant product, and then manually specify the settings. For details about items that were set before re-registration, see the log file of the **`csreregisterapp`** command.

Configuring the settings for session idle timeouts

After you log in to the Hitachi Ops Center Portal by using the single sign-on functionality of Common Services, if a specific amount of time elapses with no activity in the window, the session times out.

For the idle timeout settings, you can configure the following two settings:

- Idle timeout

  Specify the amount of time that can elapse with no activity in the window before a timeout occurs. The default is 20 minutes.

- Auto refresh

  Specify whether a timeout occurs if the idle timeout time elapses with no operation performed, for a window that automatically refreshes. By default, a timeout does not occur.

  These settings apply to the following products: Automator, Analyzer, and Analyzer viewpoint.

You can configure the idle timeout settings by using the Hitachi Ops Center Portal. The settings will apply to each Hitachi Ops Center product within a few minutes.

Note:

- The idle timeout settings apply to Common Services and each Hitachi Ops Center product whose version is 10.9.0 or later (7.6.0 or later in the case of Protector). For Hitachi Ops Center products of a version earlier than 10.9.0 (earlier than 7.6.0 in the case of Protector), timeouts might not occur.
- Actual session timeouts might differ by a few minutes from the configured idle timeout time.

Changing the scale of the resources managed by an individual product

On the management server where Common Services is installed, you can change the memory size to match the scale of the resources managed by a Hitachi Ops Center product. The target products are as follows:

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

Procedure

1. Log in to the management server as the root user.

   If you log in as an ordinary user, use the `sudo` command to complete the following procedure as the root user.
2. Run the `cschgscale` command.

   Run this command on the management server where the product that changes the scale of the resources is installed. For a management server where Common Services is not installed or the Analyzer probe server, obtain the command from the installation media. The storage locations of the command are as follows:

Command location

- If Common Services is installed on the management server:

  `*installation-directory-of-Common-Services*/utility/bin/cschgscale.sh`

- If Common Services is not installed on the management server:

  Expand `utility.tar` from the installation media.

  Storage locations of `utility.tar`:

  - *root-directory-of-the-Common-Services-installation-media*/utility.tar
  - *root-directory-of-the-Server-Express-installer-media*/COMMONSERVICES/utility.tar
  - *root-directory-of-the-Client-Express-installer-media*/COMMONSERVICES/utility.tar

  The **`cschgscale`** command is stored in the following directory after the files are extracted from `utility.tar`:

  directory-where-utility.tar-is-extracted/utility/bin

Format

```
cschgscale.sh {-scale scale-of-resources [-target Product-name] [-restart]
| -h}
```

Options

-scale scale-of-resources

Specify the scale of the resources. The memory size are changed according to the specified value. Specify one of the following values. The values are not case sensitive.

- `S`: Small-scale configuration
- `M`: Medium-scale configuration
- `L`: Large-scale configuration

Note:

- You can check a detailed descriptions of the scales by using the `-h` option.
- For details on the system requirements for each product according to the scale, see *Hitachi Ops Center System Requirements*.

`-target` ***`Product-name`***

If you omit the `-target` option, all products targeted by the **`cschgscale`** command installed on the management server are changed. If you want to run the command for an individual product, specify the value as follows:

- `analyzer`: Analyzer
- `detailview`: Analyzer detail view
- `viewpoint`: Analyzer viewpoint
- `probe`: Analyzer probe server

> **Note:** The versions on which you can use the **`cschgscale`** command differ depending on the product. You can use this command on the following versions:
>
> - Analyzer, Analyzer viewpoint: 10.9.1 or later
> - Analyzer detail view, Analyzer probe server: 11.0.4 or later

`-restart`

Specify this option when you are changing the product settings and want to apply the changes immediately. If you specify this option, the product service is restarted after the command is run, and the changes are applied. For Analyzer viewpoint, the changes are applied immediately, so you do not need to specify `-restart`.

`-h`

Displays usage information. This option displays a description of the options, the names of installed products for which the command can be used, and details of the `-scale` option.

Settings required when using a virus detection program

If a virus detection program accesses database-related files used by Common Services, an error might occur for reasons such as I/O delays or file locks. To prevent such errors while Common Services is running, exclude the following directories from the targets scanned by the virus detection program:

- `/usr/pgsql-15/bin`
- *`installation-directory-of-Common-Services`*`/nginx/temp`
- `/var/`*`installation-directory-of-Common-Services`*

For details on the directories of other Hitachi Ops Center products to exclude from the scanning targets, see the manual for each product.

Upgrading Amazon Corretto 21

If a vulnerability is found in Amazon Corretto 21, upgrade Amazon Corretto 21.

Procedure

1. Log in to the management server as the root user.

   If you log in as an ordinary user, use the **`sudo`** command to complete the following procedure as the root user.
2. Download Amazon Corretto 21, and store it on the management server where Common Services is installed.

   For details on the versions of Amazon Corretto 21 that are supported by Common Services, see the Hitachi Ops Center Release Notes.
3. Stop the Common Services service.

   > **Note:** If products that use Amazon Corretto 21 are installed on the management server, stop the services of those products as needed.
4. Run the **`rpm`** command with the `--nopost` option specified to upgrade Amazon Corretto 21.
5. Start the Common Services service.

   > **Note:** If products that use Amazon Corretto 21 are installed on the management server, start the services of those products as needed.

Upgrading PostgreSQL 15

If a vulnerability is found in PostgreSQL 15, upgrade PostgreSQL 15.

Procedure

1. Log in to the management server as the root user.

   If you log in as an ordinary user, use the **`sudo`** command to complete the following procedure as the root user.
2. Download PostgreSQL 15, and store it on the management server where Common Services is installed.

   For details on the versions of PostgreSQL 15 that are supported by Common Services, see the Hitachi Ops Center Release Notes.
3. Stop the Common Services service.
4. Run the following command to stop the Common Services database:

   ```
   systemctl stop postgresql-15@csportal.service postgresql-15@csidp.service
   ```
5. Run the **`rpm`** command to upgrade the RPM package for PostgreSQL 15.

   ```
   rpm -Uv PostgreSQL-15-package-name postgresql15-libs-package-name postgresql15-
   server-package-name
   ```

6. Run the following command to start the Common Services database:

```
systemctl start postgresql-15@csportal.service postgresql-15@csidp.service
```

7. Start the Common Services service.

Applying Linux security updates using yum

You can collectively (or selectively) apply OS security updates using the **yum** command. The **yum** command requires access to a repository from which packages can be obtained. If your management server has internet access, you can use the distribution website as described in this topic. If your management server does not have internet access, you need to download the Linux ISO on a server with Internet access and create a local **yum** repository on the management server. For more information, see Creating a local yum repository (on page 190).

> **Note:** The Express installer automatically invokes **yum** if any required Linux packages are not installed. If the **yum** repository is not configured or cannot be reached, the installation fails with a message that packages could not be installed.

Accessing the RPM packages using the distribution website

1. Specify the repository to which the **yum** command will 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
   ```

Using the yum command

To update all packages for which security-related errata are available (including packages with bug fixes or new features without security errata):

```
yum --security --exclude kernel* --exclude *podman* --exclude *containers-common*
upgrade
```

To update all packages for which security-related errata are available (ignoring any newer packages without security errata):

```
yum --security --exclude kernel* --exclude *podman* --exclude *containers-common*
upgrade-minimal
```

To update all kernel and podman packages to the latest supported versions that contain security errata, follow these examples.

For Red Hat kernel (must specify supported kernel version):

```
yum --security upgrade-minimal kernel-4.18.0-305.*
```

For Unbreakable Enterprise kernel (must specify supported uek kernel version):

```
yum --security upgrade-minimal kernel-uek-5.4.17-2102.*
```

For podman (must specify supported podman version):

```
yum --security upgrade-minimal podman-3.3.*
```

You can also update only those packages that correspond to a CVE or erratum, as in the following examples:

```
yum --cve CVE-2021-37576 upgrade-minimal
```

For Red Hat Enterprise Linux:

```
yum --advisory RHSA-2021:4056 upgrade-minimal
```

For Oracle Linux:

```
yum --advisory ELSA-2021-9474 upgrade-minimal
```

Creating a local yum repository

If you cannot use **`yum`** to install updates because your management server is not connected to the internet, you must create a local repository using the required Linux ISO distribution image. Follow this procedure to set up a local **`yum`** repository on your management server:

Procedure

1. Download the applicable Linux ISO image (for example, `rhel-8.5-x86_64-dvd.iso`) on a server with internet access and copy the file to the management server.
2. Create a directory and mount the ISO image using the following commands:

   ```
   mkdir /media/OSImage
   mount -o loop filename.iso /media/OSImage
   ```

3. If the `/etc/yum.repos.d` directory contains an existing repo file, rename the file extension or delete it.
4. Use a file editor to create the new repository file, as in this example using **`vim`**:

   ```
   vim /etc/yum.repos.d/local.repo
   ```

5. Configure the **`yum`** repository by copying and pasting the following text into the file:

   ```

   [dvd-baseos]
   name=dvd-baseos
   baseurl=file:///media/OSImage/BaseOS/
   gpgcheck=0
   enabled=1

   [dvd-appstream]
   name=dvd-appstream
   baseurl=file:///media/OSImage/AppStream/
   gpgcheck=0
   enabled=1
   ```

6. Save the file.

Result

You can now invoke the **`yum`** command as needed to install packages.

Replacing Command Control Interface

You can replace an individually installed instance of Command Control Interface with an instance of Command Control Interface installed by the Express installer, or replace an instance of Command Control Interface installed by the Express installer with an individually installed instance of Command Control Interface.

- To replace an individually installed instance of Command Control Interface with an instance of Command Control Interface installed by the Express installer, perform the procedure described in Switching to an instance of Command Control Interface installed by the Express installer (on page 191).
- To replace an instance of Command Control Interface installed by the Express installer with an individually installed instance of Command Control Interface, perform the procedure described in Switching to an individually installed instance of Command Control Interface (on page 192).

Switching to an instance of Command Control Interface installed by the Express installer

You can replace an individually installed instance of Command Control Interface with that installed by the Express installer.

Procedure

1. If API Configuration Manager or Protector is installed, stop the service.

   For details on how to stop the service, see the manual for the relevant product.

2. Run the **`ps`** command to check for Command Control Interface processes that are running.

   ```
   ps aux
   ```

   From the list that appears, look for items in the format `horcmd_`*`number`*. (There might be more than one such item.)

3. If any processes are running, run the following command to stop the Command Control Interface service:

   In the following, *number* consists of the fixed value 0 and *instance-number*. If there are multiple items in the format `horcmd_`*`number`*, specify each of *instance-number* separated by a space.

   ```
   horcmshutdown.sh instance-number
   ```

4. Run the following command to uninstall Command Control Interface:

   ```
   /HORCM/horcmuninstall.sh
   ```

5. Run the following command to delete the Command Control Interface installation directory:

   ```
   rm -rf $(readlink /HORCM)
   ```

6. Run the following command to delete the Command Control Interface symbolic link:

   ```
   rm /HORCM
   ```

7. Use the Express installer to install Command Control Interface. Select API Configuration Manager or Protector as the product to be installed and then perform the installation.

Switching to an individually installed instance of Command Control Interface

You can replace an instance of Command Control Interface installed by the Express installer with an individually installed instance.

Procedure

1. If API Configuration Manager or Protector is installed, stop the service.

   For details on how to stop the service, see the manual for the relevant product.

2. Run the **`ps`** command to check for Command Control Interface processes that are running.

   ```
   ps aux
   ```

From the list that appears, look for items in the format `horcmd_`*`number`*. (There might be more than one such item.)

3. If any processes are running, run the following command to stop the Command Control Interface service:

   In the following, *number* consists of the fixed value 0 and *instance-number*. If there are multiple items in the format `horcmd_`*`number`*, specify each of *instance-number* separated by a space.

   ```
   horcmshutdown.sh instance-number
   ```

4. Run the following command to uninstall Command Control Interface:

   ```
   /HORCM/horcmuninstall.sh
   ```

5. Run the following command to delete the Command Control Interface installation directory:

   ```
   rm -rf $(readlink /HORCM)
   ```

6. Run the following command to delete the Command Control Interface symbolic link:

   ```
   rm /HORCM
   ```

7. Install Command Control Interface.

   For details on the installation method, see the Command Control Interface manual.

8. Start the service of API Configuration Manager or Protector.

   For details on how to start the service, see the manual for the relevant product.

Chapter 11: Removing a Hitachi Ops Center product

To remove a Hitachi Ops Center environment or remove an unnecessary product after the OVA is deployed, use the product uninstaller. For details on how to remove products other than Common Services, see the documentation for the relevant product.

Removing Common Services

Remove Common Services by performing the following procedure.

> **Note:** If you remove Common Services, Amazon Corretto 21 and PostgreSQL 15 are not removed. If Common Services was upgraded from an earlier version, Amazon Corretto 8 (version 10.6.0 and earlier), Amazon Corretto 11 (versions 10.6.1 to 10.9.1), Amazon Corretto 17 (versions 10.9.2 to 11.0.2), and PostgreSQL 11 (version 10.9.2 and earlier) might be installed on the management server. If you do not need these programs, remove them by using the **`rpm`** command. If you cannot remove the programs by using this command, use the **`rpm`** command with the `--nopreun` option specified.
>
> The package name of each program is as follows:
>
> - Amazon Corretto 21: `java-21-amazon-corretto-devel`
> - Amazon Corretto 17: `java-17-amazon-corretto-devel`
> - Amazon Corretto 11: `java-11-amazon-corretto-devel`
> - Amazon Corretto 8: `java-1.8.0-amazon-corretto-devel`
> - PostgreSQL 15: `postgresql15, postgresql15-server, postgresql15-libs`
> - PostgreSQL 11: `postgresql11, postgresql11-server, postgresql11-libs`

Before you begin

Before removing Common Services, complete the following:

- If necessary, back up the data.
- If any products are registered in Common Services, log in to the Hitachi Ops Center Portal, and delete all products.

Procedure

1. Log in to the management server as the root user.

   If you log in as an ordinary user, use the **`sudo`** command to complete the following procedure as the root user.
2. Move to the root directory.
3. Run the following command:

   ```
   installation-directory-of-Common-Services/inst/uninstall.sh
   ```

Appendix A: Troubleshooting

Check the messages or log files to determine the cause of the error and take action. If you cannot determine the cause or resolve the error, collect the maintenance information about the management server and Common Services, and then contact support personnel.

Collecting failure information

If a failure occurs while using Hitachi Ops Center, collect the failure information required to analyze the cause.

Procedure

1. Log in to the management server as the root user.

   If you log in as an ordinary user, use the **`sudo`** command to complete the following procedure as the root user.

2. To collect the failure information of Common Services, run the **`csgetras`** command.

   Command location

   `installation-directory-of-Common-Services``/utility/bin/csgetras.sh`

   Format

   ```
   csgetras.sh -dir path-to-output-destination-directory
   ```

   Option

   `-dir` ***`path-to-output-destination-directory`***

   Specify the path to the directory to which the collected failure information is output. A relative path can be specified.

   If you run the command, a file that compresses and archives the collected information is created.

3. As necessary, collect the failure information of each product registered in Common Services and the Server Express installer.

   For details on how to collect failure information, see the documentation for each product.

   For failure information for the Server Express installer, manually save the following log files.

Log file	Location	Description
`ExpressInstaller_`*`version`*`.hv_`*`yyyymmdd-hhmmss`*`.log`	`/tmp`	The log file of the Server Express installer.
`ExpressInstaller_`*`version`*`.`*`product-name_yyyymmdd-hhmmss`*`.log`	`/tmp`	The log files for the standard output displayed during the installation of products selected in the Server Express installer. For *product-name*, one of the following strings is output: ▪ `commonservices`: Common Services ▪ `administrator`: Administrator ▪ `ConfManager`: API Configuration Manager ▪ `protector`: Protector ▪ `automator`: Automator ▪ `analyzer`: Analyzer ▪ `detailview`: Analyzer detail view ▪ `viewpoint`: Analyzer viewpoint ▪ `CCI`: Command Control Interface
`ExpressInstaller_`*`version`*`.`*`command-name_yyyymmdd-hhmmss`*`.log`	`/tmp`	The log file output when a command is run by the Server Express installer. For *command-name*, the following string is output: ▪ **`cschgscale`**: Output when a product is newly installed and resources have been configured.
`COMSERV_Report.txt`	`/var/log/hitachi/CommonService/inst`	Installation report file that is output if Common Services is installed.

4. To collect the following failure information for work performed on a server where Common Services is not installed, log in to the server:
   - Client Express installer
   - SSL Setup tool (Use the **`cssslsetup`** command in `utility.tar`.)

- **csreregisterapp** command (Use the command in `utility.tar`.)
- **cschgscale** command (Use the command in `utility.tar`.)

Manually save the following log files.

Log file	Location	Description
`ClientExpressInstaller_`*`version`*`.hv_`*`yyyymmdd-hhmmss`*`.log`	`/tmp`	The log file of the Client Express installer.
`ClientExpressInstaller_`*`version`*`.`*`product-name_yyyymmdd-hhmmss`*`.log`	`/tmp`	The log files for the standard output displayed during the installation of products selected in the Client Express installer. For *product-name*, one of the following strings is output: - `probe`: Analyzer probe server - `ConfManager`: API Configuration Manager - `protector`: Protector Client - `CCI`: Command Control Interface
`ClientExpressInstaller_`*`version`*`.`*`command-name_yyyymmdd-hhmmss`*`.log`	`/tmp`	The log file output when a command is run by the Client Express installer. For *command-name*, the following string is output: - **cschgscale**: Output when a product is newly installed and resources have been configured.
`command-name_YYYY-MM-DD-hh-mm-ss``.log`	`/tmp`	This is the log file that is output when a command is run. For *command-name*, the following string is output: - **cssslsetup** - **csreregisterapp** - **cschgscale**

Collecting Ops Center log files

The following table provides the commands for collecting log files from Ops Center component products.

Product	Command
Ops Center Common Services	*installation-directory-of-Common-Services*`/utility/bin/csgetras.sh -dir` *output-directory-path*
Ops Center Analyzer	*Common-component-installation-destination-directory*`/bin/hcmds64getlogs -dir` *output-directory-path*
Ops Center Analyzer viewpoint	`/opt/hitachi/analyzer_viewpoint/bin/diag`
Ops Center Analyzer detail view Analyzer probe server	Obtain the log files from the UI.
Ops Center Analyzer RAID Agent	`/opt/jp1pc/tools/jpcras` *output-directory-path-all* `all`
Ops Center Administrator	`/opt/rainier/bin/rainier-getlogs -dir [`*output-directory*`]` Check the location of collected log file (`rainier-logs.tar.gz`).
Ops Center Automator	**Windows:** *Common-component-installation-destination-directory*`\bin\hcmds64getlogs /dir` *output-directory-path* **Linux:** *Common-component-installation-destination-directory*`/bin/hcmds64getlogs -dir` *output-directory-path*

Ops Center Protector	Collect a mini diagnostic log from a node:
	`diagdata --mini`
	Collect a full diagnostic log from a node:
	`diagdata --full`

Product	Command

Ops Center API Configuration Manager	**Windows:**
	`*REST-API-installation-destination*\SupportTools\CollectTool\RestTI.bat -dir *omaintenance-information-storage-destination*`
	Linux:
	`*REST-API-installation-destination*/SupportTools/CollectTool/RestTI.sh -dir *omaintenance-information-storage-destination*`

Common Services logs

In Common Services, log files are output and can be used to analyze the causes of failures that occur.

Three types of log files are output for Common Services.

Output-destination directory

```
/var/log/hitachi/CommonService
```

Log files

Log file	Description
`error.log`	The Common Services error log is output to this file. Check the contents of this file as needed.
`debug.log`	This log file is necessary for customer support to analyze the cause of a failure when, for example, you cannot identify the cause or cannot perform recovery.
`server.log`	This log file is necessary for customer support to analyze the cause of a failure when, for example, you cannot identify the cause or cannot perform recovery.

The following items are output to `error.log`.

Item	Description
Date and time	The date and time when the log was output
Level	The log level
Thread name	The name of the internal processing of Common Services
Message ID	The message ID in the following format. KAOP*nnnnn*-*Z* In the above, *nnnnn* is the message number. *Z* is the message type. ▪ E: Error message ▪ W: Warning message ▪ I: Information
Message	The message corresponding to the message ID
Exception	Information about the exception that occurred

Changing the properties of logs

You can change the properties of Common Services logs to change how the logs are output.

Procedure

1. Log in to the management server as the root user.

   If you log in as an ordinary user, use the **sudo** command to complete the following procedure as the root user.
2. Edit the following properties file.

   ```
   /var/installation-directory-of-Common-Services/userconf/
   config_user.properties
   ```

   For example, for an OVA install uses the following file:

   ```
   /var/opt/hitachi/CommonService/userconf/config_user.properties
   ```

   The properties of logs are as follows:

Property	Description
CS_PORTAL_LOG_LEVEL_DEBUG	Specify the level for which the debug log is to be output. You can specify one of the following values (listed in descending order of detail level): TRACE, DEBUG, and INFO.

Property	Description
	Default value: DEBUG
CS_PORTAL_LOG_MAX_FILESIZE	Specify the maximum size of each log file. When the size of a log file exceeds the specified size, a new log file is created. The value of this property must be specified in the form of an integer and a unit. You can specify KB, MB, or GB for the unit. KB, MB, and GB correspond to KiB, MiB, and GiB, respectively. If you do not specify a unit, the unit is assumed to be bytes. Default value: 20MB
CS_PORTAL_LOG_MAX_INDEX_ERROR	Specify the maximum number of error log backups to keep. When the error log file reaches the maximum size specified for the CS_PORTAL_LOG_MAX_FILESIZE property, a backup of the file is created, where the name of the backup file is the original file name with a number appended to the end. Each time the log file reaches the maximum size, a new backup file is created until the number of backup files reaches the number specified for this property. After this number of backup files is reached, each time a new backup file is created, the oldest backup file is deleted. You can specify a value in the range from 1 to 21. Default value: 10
CS_PORTAL_LOG_MAX_INDEX_DEBUG	Specify the maximum number of debug log backups to keep.

Property	Description
	When the debug log file reaches the maximum size specified for the `CS_PORTAL_LOG_MAX_FILESIZE` property, a backup of the file is created, where the name of the backup file is the original file name with a number appended to the end. Each time the log file reaches the maximum size, a new backup file is created until the number of backup files reaches the number specified for this property. After this number of backup files is reached, each time a new backup file is created, the oldest backup file is deleted. You can specify a value in the range from `1` to `21`. Default value: `20`
`CS_PORTAL_LOG_MAX_INDEX_APPLOG`	Specify the maximum number of server log backups to keep. When the server log file reaches the maximum size specified for the `CS_PORTAL_LOG_MAX_FILESIZE` property, a backup of the file is created, where the name of the backup file is the original file name with a number appended to the end. Each time the log file reaches the maximum size, a new backup file is created until the number of backup files reaches the number specified for this property. After this number of backup files is reached, each time a new backup file is created, the oldest backup file is deleted. You can specify a value in the range from `1` to `21`. Default value: `20`

3. Restart the Common Services service.

Common Services audit log

Common Services can output audit log information about who performed which operation and when. By default, the audit log output is disabled, but you can enable it and change the properties as needed.

Output destination

The audit log is output to the `syslog`.

Output items

The following items are output to the audit log.

Location	Item	Description	Example
PRI	Priority	A number that indicates the priority level. This number is converted from the facility value and the log level. The facility value is converted based on the value set for the `CS_PORTAL_AUDIT_FACILITY` property.	`<11>`
HEADER	Date and time	The date and time when the auditing event occurred	`Sep 2 13:15:04`
	Host name	The name of the host for which the auditing event occurred	`WIN-00ABCD11EFG`
MSG	Process ID	The process ID	`5828`
	Thread ID	The thread ID	`http-nio-8081-exec-2`
	Log level	The log level, such as `ERROR` or `DEBUG`	`ERROR`
	Date and time	The date and time when the audit log was output	`2019-09-02T13:15:04.362+0900`
	Message ID	The message ID	`KAOP91111-E`
	Type of auditing event	The auditing event type, such as `StartStop` or `Authentication`	`Authentication`
	Result of the auditing event	The result of the event, such as whether the event was successful or not	`Success`
	Subject-identifying information	Information such as the user ID or a URI	`User ID=system,URI=/portal`

Location	Item	Description	Example
	Message	The message	`KAOP91111-E Audit Log.`

The auditing event types that are output and their corresponding severity levels are as follows. You can change the properties of the audit log to narrow down the severity levels that are output.

Type of auditing event	Description	Corresponding severity level
`Authentication`	Indicates an auditing event that is related to login or authentication	If the event is successful: `6` If the event fails: `4`
`ConfigurationAccess`	Indicates an auditing event that is related to the creation, referencing, modification, or deletion of a user account or user group	If the event is successful: `6` If the event fails: `3`

Auditing events output to the audit log

Common Services outputs the following types of auditing events to the audit log. A message to be output consists of a message ID and message text.

The following shows the message ID format:

prefixNNNNN-x

A message ID consists of the following elements:

prefix

Indicates the component from which the message is output. The prefix of audit log messages is KAOP.

NNNNN

Indicates the serial number of the message. The serial number differs depending on the type.

- KAOP9800*N*: `Authentication` message
- KAOP90*NNN*: `ConfigurationAccess` message

x

Indicates the message type. The following shows the message types and their meanings:

- `E` (`Error`): Message that notifies users of an error that prevents processing from continuing
- `I` (`Information`): Message that notifies users of information

If the auditing event type is `Authentication`:

Detailed type	Auditing event	Message
User authentication	Successful login	KAOP98001-I,Authentication,Success,type=LOGIN
	Login error	KAOP98002-E,Authentication,Failed,type=LOGIN_ERROR
	Successful logout	KAOP98001-I,Authentication,Success,type=LOGOUT
	Logout error	KAOP98002-E,Authentication,Failed,type=LOGOUT_ERROR
Profile	Successful account editing	KAOP98001-I,Authentication,Success,type=UPDATE_PROFILE
	Account editing error	KAOP98002-E,Authentication,Failed,type=UPDATE_PROFILE_ERROR
	Successful password change	KAOP98001-I,Authentication,Success,type=UPDATE_PASSWORD
	Password change error	KAOP98002-E,Authentication,Failed,type=UPDATE_PASSWORD_ERROR

- For the audit log, message IDs other than those listed in this table are also output from the internal processing of Common Services.
- Based on the message ID and the type value, determine each event in the auditing log.

If the auditing event type is `ConfigurationAccess`:

Detailed type	Auditing event	Message
User	Successful user creation	KAOP90001-I

Detailed type	Auditing event	Message
	User creation error	KAOP90002-E
	Successful acquisition of a user list	KAOP90003-I
	Error obtaining a user list	KAOP90004-E
	Successful acquisition of information about a specific user	KAOP90005-I
	Error obtaining information about a specific user	KAOP90006-E
	Successful update of information about a specific user	KAOP90007-I
	Error updating information about a specific user	KAOP90008-E
	Successful user deletion	KAOP90009-I
	User deletion error	KAOP90010-E
	Successful acquisition of a list of user groups to which a specific user belongs	KAOP90011-I
	Error obtaining a list of user groups to which a specific user belongs	KAOP90012-E
User group	Successful addition of users to a user group	KAOP90013-I
	Error adding users to a user group	KAOP90014-E
	Successful deletion of users from a user group	KAOP90015-I
	Error deleting users from a user group	KAOP90016-E
	Successful reset of a user password	KAOP90017-I
	Error resetting a user password	KAOP90018-E
	Successful registration of a user group	KAOP90019-I
	Error registering a user group	KAOP90020-E
	Successful acquisition of a user group list	KAOP90021-I
	Error obtaining a user group list	KAOP90022-E
	Successful update of registered information of a user group	KAOP90023-I
	Error updating registered information of a user group	KAOP90024-E
	Successful acquisition of information about a specific user group	KAOP90025-I

Detailed type	Auditing event	Message
	Error obtaining information about a specific user group	KAOP90026-E
	Successful deletion of a user group	KAOP90027-I
	Error deleting a user group	KAOP90028-E
	Successful acquisition of a list of users who belong to a specific user group	KAOP90029-I
	Error obtaining a list of users who belong to a specific user group	KAOP90030-E
	Successful acquisition of a list of roles assigned to a specific user group	KAOP90031-I
	Error obtaining a list of roles assigned to a specific user group	KAOP90032-E
	Successful assignment of roles to a user group	KAOP90033-I
	Error assigning roles to a user group	KAOP90034-E
	Successful deletion of roles assigned to a user group	KAOP90035-I
	Error deleting roles assigned to a user group	KAOP90036-E
	Successful acquisition of a list of roles that can be assigned to a specific user group	KAOP90037-I
	Error obtaining a list of roles that can be assigned to a specific user group	KAOP90038-E
User directory	Successful registration of an Active Directory or LDAP server	KAOP90039-I
	Error registering an Active Directory or LDAP server	KAOP90040-E
	Successful acquisition of an Active Directory or LDAP server list	KAOP90041-I
	Error obtaining an Active Directory or LDAP server list	KAOP90042-E
	Successful acquisition of information about a specific Active Directory or LDAP server	KAOP90043-I
	Error obtaining information about a specific Active Directory or LDAP server	KAOP90044-E

Detailed type	Auditing event	Message
	Successful update of information about an Active Directory or LDAP server	KAOP90045-I
	Error updating information about an Active Directory or LDAP server	KAOP90046-E
	Successful deletion of information about an Active Directory or LDAP server	KAOP90047-I
	Error deleting information about an Active Directory or LDAP server	KAOP90048-E
	Successful synchronization of user groups	KAOP90049-I
	Error synchronizing user groups	KAOP90050-E
	Successful implementation of the connection and authentication tests of an Active Directory server	KAOP90051-I
	Error implementing the connection and authentication tests of an Active Directory server	KAOP90052-E
`setupcommonservice` command of each product	Successful registration of a product	KAOP90053-I
	Error registering a product	KAOP90054-E
Product	Successful acquisition of a list of products registered in Common Services	KAOP90055-I
	Error obtaining a list of products registered in Common Services	KAOP90056-E
	Successful acquisition of information about a specific product registered in Common Services	KAOP90057-I
	Error obtaining information about a specific product registered in Common Services	KAOP90058-E
	Successful update of registered information of a product	KAOP90059-I
	Error updating registered information of a product	KAOP90060-E
	Successful deletion of a product	KAOP90061-I
	Error deleting a product	KAOP90062-E
	Successful acquisition of configuration information of a specific product registered in Common Services	KAOP90063-I

Detailed type	Auditing event	Message
	Error obtaining configuration information of a specific product registered in Common Services	KAOP90064-E
	Successful acquisition of version information of a specific product registered in Common Services	KAOP90065-I
	Error obtaining version information of a specific product registered in Common Services	KAOP90066-E
	Successful acquisition of status information of a specific product registered in Common Services	KAOP90067-I
	Error obtaining status information of a specific product registered in Common Services	KAOP90068-E
	Successful acquisition of license information of a specific product registered in Common Services	KAOP90069-I
	Error obtaining license information of a specific product registered in Common Services	KAOP90070-E
Data Center	Successful registration of a data center	KAOP90071-I
	Error registering a data center	KAOP90072-E
	Successful acquisition of a data center list	KAOP90073-I
	Error obtaining a data center list	KAOP90074-E
	Successful acquisition of information about a specific data center	KAOP90075-I
	Error obtaining information about a specific data center	KAOP90076-E
	Successful update of registered information of a data center	KAOP90077-I
	Error updating registered information of a data center	KAOP90078-E
	Successful deletion of a data center	KAOP90079-I
	Error deleting a data center	KAOP90080-E
	Successful acquisition of a list of products registered in a specific data center	KAOP90081-I
	Error obtaining a list of products registered in a specific data center	KAOP90082-E
	Successful registration of products registered in Common Services to a data center	KAOP90083-I

Detailed type	Auditing event	Message
	Error registering products registered in Common Services to a data center	KAOP90084-E
	Successful deletion of products registered in Common Services from a data center	KAOP90085-I
	Error deleting products registered in Common Services from a data center	KAOP90086-E
Password policy	Successful acquisition of the password policy	KAOP90087-I
	Error obtaining the password policy	KAOP90088-E
	Successful update of the password policy	KAOP90089-I
	Error updating the password policy	KAOP90090-E
Warning banner	Successful acquisition of the banner	KAOP90091-I
	Error obtaining the banner	KAOP90092-E
	Successful update of the banner	KAOP90093-I
	Error updating the banner	KAOP90094-E
	Successful preview of the banner	KAOP90095-I
	Error previewing the banner	KAOP90096-E
	Successful acquisition of the banner tag	KAOP90097-I
	Error obtaining the banner tag	KAOP90098-E
Version information	Successful acquisition of version information of Common Services	KAOP90099-I
	Error obtaining version information of Common Services	KAOP90100-E
Access token	Successful acquisition of the access token	KAOP90103-I
	Error obtaining the access token	KAOP90104-E
	Successful acquisition of information about the user who obtained the access token	KAOP90105-I
	Error obtaining information about the user who obtained the access token	KAOP90106-E
Periodic running by a registered product	Successful notification of the status of a linked product	KAOP90109-I
	Error reporting the status of a linked product	KAOP90110-E

Detailed type	Auditing event	Message
Login	Successful acquisition of the logged-in user's profile	KAOP90111-I
	Error obtaining the logged-in user's profile	KAOP90112-E
Login banner	Successful acquisition of the login banner	KAOP90113-I
	Error obtaining the login banner	KAOP90114-E
Checking the session and token status during use of the GUI	Successful acquisition of the logged-in user status	KAOP90115-I
	Error obtaining the logged-in user status	KAOP90116-E
Product deletion	Error notifying a product of deletion	KAOP90125-W
Kerberos connection settings	Successful acquisition of information about the Kerberos authentication connection	KAOP90126-I
	Error obtaining information about the Kerberos authentication connection	KAOP90127-E
	Successful update of the Kerberos connection settings	KAOP90128-I
	Error updating the Kerberos connection settings	KAOP90129-E
	Successful creation of a Kerberos realm	KAOP90130-I
	Error creating a Kerberos realm	KAOP90131-E
	Successful deletion of a Kerberos realm	KAOP90132-I
	Error deleting a Kerberos realm	KAOP90133-E
	Successful acquisition of information about a specific realm for Kerberos authentication	KAOP90134-I
	Error obtaining information about a specific realm for Kerberos authentication	KAOP90135-E
	Successful acquisition of a list of information about Kerberos authentication realms	KAOP90136-I
	Error obtaining a list of information about Kerberos authentication realms	KAOP90137-E
	Successful update of Kerberos realm information	KAOP90138-I
	Error updating Kerberos realm information	KAOP90139-E
Identity provider	Successful import of metadata	KAOP90172-I

Detailed type	Auditing event	Message
	Error importing metadata	KAOP90173-E
	Successful registration of an identity provider	KAOP90174-I
	Error registering an identity provider	KAOP90175-E
	Successful export of metadata	KAOP90176-I
	Error exporting metadata	KAOP90177-E
	Successful acquisition of an identity provider list	KAOP90178-I
	Error obtaining an identity provider list	KAOP90179-E
	Successful acquisition of information about a specific identity provider	KAOP90180-I
	Error obtaining information about a specific identity provider	KAOP90181-E
	Successful update of registered information of an identity provider	KAOP90182-I
	Error updating registered information of an identity provider	KAOP90183-E
	Successful deletion of an identity provider	KAOP90184-I
	Error deleting an identity provider	KAOP90185-E
Authentication key	Successful acquisition of the authentication key settings	KAOP90186-I
	Error obtaining the authentication key settings	KAOP90187-E
	Successful update of the update interval of the authentication key	KAOP90188-I
	Error updating the update interval of the authentication key	KAOP90189-E
	Successful update of the authentication key	KAOP90190-I
	Error updating the authentication key	KAOP90191-E
User directory	Successful synchronization of all users of an external authentication server	KAOP90192-I
	Error synchronizing all users of an external authentication server	KAOP90193-E
	Successful check of the number of users obtained from an Active Directory or LDAP server	KAOP90196-I

Detailed type	Auditing event	Message
	Error checking the number of users obtained from an Active Directory or LDAP server	KAOP90197-E
Product	Successful acquisition of session information of the product	KAOP90198-I
	Error obtaining session information of the product	KAOP90199-E
Session control	Successful acquisition of information about the session settings	KAOP90200-I
	Error obtaining information about the session settings	KAOP90201-E
	Successful update of information about the session settings	KAOP90202-I
	Error updating information about the session settings	KAOP90203-E

Changing the audit log properties

You can change the Common Services audit log properties to change the output.

Procedure

1. Log in to the management server as the root user.

   If you log in as an ordinary user, use the **sudo** command to complete the following procedure as the root user.
2. Edit the following properties file.

   `/var/`*`installation-directory-of-Common-Services`*`/userconf/config_user.properties`

   For example, for an OVA install uses the following file:

   `/var/opt/hitachi/CommonService/userconf/config_user.properties`

   The properties of the audit log are as follows:

Property	Description
`CS_PORTAL_AUDIT_ENABLE`	Specify one of the following values to indicate whether to generate the audit log. ▪ `true`: Generate the audit log. ▪ `false`: Do not generate the audit log. Default value: `false`

Property	Description
CS_PORTAL_AUDIT_ SYSLOGHOST	If you want audit logs output to a server other than the management server on which Common Services is installed, specify the host name or IP address of that server. Default value: localhost
CS_PORTAL_AUDIT_ PORT	Specify the port number of the syslog server. Communication with the syslog server is over UDP. TCP is not supported. Default value: 514
CS_PORTAL_AUDIT_ FACILITY	Specify the information needed to identify the sender of a message. You can specify the following values: ▪ KERN ▪ USER ▪ MAIL ▪ DAEMON ▪ AUTH ▪ SYSLOG ▪ LPR ▪ NEWS ▪ UUCP ▪ CRON ▪ AUTHPRIV ▪ FTP ▪ NTP ▪ AUDIT ▪ ALERT ▪ CLOCK ▪ LOCAL0 ▪ LOCAL1 ▪ LOCAL2 ▪ LOCAL3 ▪ LOCAL4 ▪ LOCAL5

Property	Description
	▪ LOCAL6 ▪ LOCAL7 Default value: USER
CS_PORTAL_AUDIT_LEVEL	Specify the severity levels to include in the audit log output. You can specify the following values. ▪ DEBUG: Output the audit log for severity levels 0 to 7. ▪ INFO: Output the audit log for severity levels 0 to 6. ▪ WARN: Output the audit log for severity levels 0 to 4. ▪ ERROR: Output the audit log for severity levels 0 to 3. Default value: INFO

3. Restart the Common Services service.

Appendix B: Linking with Hitachi Remote Ops

The Hitachi Remote Ops feature, allows log files to be automatically collected and sent to support personnel when an error occurs.

To enable Hitachi Remote Ops, you need to install Hitachi Remote Ops and register information about Common Services.

Note: The following products do not support collecting and sending of log files by Hitachi Remote Ops:

- Hitachi Ops Center Automator
- Hitachi Ops Center Analyzer viewpoint
- Hitachi Ops Center Protector

Installing Hitachi Remote Ops

Download the latest version of the software from the Hitachi Support Connect portal, and then install it on a Linux or Windows host. Hitachi Ops Center products support version 9.3 or later of Hitachi Remote Ops.

For details on the installation procedure, see the *Hitachi Remote Ops Installation Guide*. If necessary, also see the *Hitachi Remote Ops Storage VSP G1000, VSP Gx00, USP V/VM, USP/NSC Installation and Reference Guide*.

Specifying settings for Hitachi Remote Ops

You must register information about Common Services in the Hitachi Remote Ops Monitor Agent so that log files can be automatically collected.

For details on Hitachi Remote Ops settings, see the *Hitachi Remote Ops Installation Guide*.

Before you begin

Using the Hitachi Ops Center Portal, create the user that Hitachi Remote Ops Monitor Agent uses to access Common Services, and assign the support-services group to the user.

For details on how to create a user, see Creating and editing Ops Center user accounts (on page 98).

For details on how to assign a group to a user, see Assigning privileges to local (non-AD) Ops Center users (on page 105).

Procedure

1. Log in to Hitachi Remote Ops and add a device that is named `Hitachi Ops Center Common Services`.
2. Create a remote user ID that Hitachi Remote Ops Monitor Agent uses to access Common Services.

   For the remote user ID created in this step, specify the login information of a user who belongs to the support-services group created on the Hitachi Ops Center Portal.

   a. From the security object list on the **Remote Ops User Management** page, select **Remote User ID**, and then click **Refresh**.

   b. Enter the alias name in **Security Name**, and then click **Refresh**.

   c. In the **Detail for Remote User Id** area at the bottom of the page, enter the user ID that belongs to the support-services group created on the Hitachi Ops Center Portal.

   d. Enter a password in **Remote Password**, and then click **Refresh**.

Hitachi Vantara

Corporate Headquarters
2535 Augustine Drive
Santa Clara, CA 95054 USA

HitachiVantara.com/contact