-F7EB-4FA0-88AD-

***Hitachi Ops Center Common Services***

**Troubleshooting Guide**

**©2024, Hitachi Vantara, Ltd. All rights reserved.**

This guide must not be used for any purposes other than those referred to in this guide. No part of the contents of this guide may be reproduced or transmitted in any form or by any means without the written permission of Hitachi Vantara, Ltd.

- Preface -

The purpose of this document is to let on-site personnel and support staff know how to identify issues and isolate the cause when troubleshooting Hitachi Ops Center Common services. We hope that this document helps ease the burden on personnel and allows them to respond to and resolve issues in a timely manner.

- Revision History -

|  |  |  |  |
| --- | --- | --- | --- |
| No. | Version | Description | Date |
| 1 | 10.0.1 | Hitachi Ops Center Common services Troubleshooting Guide created | December 5, 2019 |
| 2 | 10.1.0 | Followings are added:  A-4 Downgrading Amazon Corretto 8 | February 17, 2020 |
| 3 | 10.2.0 | Followings has been fixed:  Figure 3-2 Confirmation method for group synchronization | April 21, 2020 |
| 4 | 10.3.0 | Followings are added:  3.2.8 Items to check when you cannot access AD | June 1, 2020 |
| 5 | 10.3.1 | None | July 22, 2020 |
| 6 | 10.5.0 | Followings are added:  3.2.9 AD FS registration fails  3.2.10 Configuration fails in AD FS  3.2.11 Failed to log in with registered AD FS  Followings has been fixed:  3.2.8 Items to check when you cannot access AD | September 23, 2020 |
| 7 | 10.5.1 | Followings are added:  A-5 Operation to disable the service | November 9, 2020 |
| 8 | 10.6.0 | Followings are added:  3.1.2(3) Check if the server certificate and private key are the correct key pair | January 12, 2021 |
| 9 | 10.6.1 | Followings has been fixed:  A-4 Downgrading Amazon Corretto 11 | March 2, 2021 |
| 10 | 10.7.0 | None | Jun 30, 2021 |
| 11 | 10.8.0 | Corrected an error in the manual name.  Table 1-1, Table 1-2 | September 17, 2021 |
| 12 | 10.8.1 | Followings are added:  3.2.1(6) Check if access to the https port is blocked  3.2.12 User directory service (Other) registration fails  3.2.13 The screen goes blank when you log in | January 5, 2022 |
| 13 | 10.8.2 | None | April 21, 2022 |
| 14 | 10.8.3 | Followings are added:  3.2.14 Unable to register each Ops Center product in Common Services, or upgrade installation does not proceed with Express installer | June 30, 2022 |
| 15 | 10.9.0 | Corrected default port numbers in the following section.  3.1.2 Items to check when Common Services cannot be started  Corrected commands in the following sections.  1.5.3 Failure during uninstallation  3.1.2 Items to check when Common Services cannot be started  3.2.1 Items to check when you cannot access Hitachi Ops Center  3.2.2 Initializing the sysadmin user password  Replaced the procedure for changing the user password in the following section.  3.2.2 Initializing the sysadmin user password  Corrected figures in the following sections.  3.2.1 Items to check when you cannot access Hitachi Ops Center  3.2.3 Synchronization with Active Directory group fails | September 26, 2022 |
| 16 | 10.9.1 | Followings are added:  3.1.3 Items to check when Common Services cannot be started in OVA  3.2.15 Out of memory occurs  3.2.16 [Hitachi Edition] RemoteOps log Download API is Time Out  3.2.17 [Hitachi Edition] If an error occurs in the Common Services RemoteOps, what log should check? 3.2.18 Initializing the truststore password | January 23, 2023 |
| 17 | 10.9.2 | Folllwings are added 3.2.19 When a failure occurs during backup of Common Services by the Protector backup integration function 3.3 Construction failures  3.3.1 Failed to install Analyzer with Server Express installer | March 28, 2023 |
| 18 | 10.9.3 | Followings are added  1.5.1.2 Error in database backup during repair installation.  1.5.3 Failure during repair installation  3.1.2Items to check when Common Services cannot be started  Corrected postgresql version in the following section.  1.5.4 Failure during uninstallation3.1.2 Items to check when Common Services cannot be started  Appendices  Corrected Java version in the following section.  1.5.4 Failure during uninstallation3.1.2 Items to check when Common Services cannot be started  Corrected Deleting set up information of operating system in the following section.  1.5.4.1.1 Forcibly uninstalling Common Services  Add files to be deleted during a forcibly uninstall.  1.5.4.1.1 Forcibly uninstalling Common Services | August 9, 2023 |
| 19 | 11.0.0 | Followings are added  1.5.2.2 When Vup installing with viewpoint OVF, the CS service fails to start. | December 25, 2023 |
| 4.2.73.2.7 | 11.0.1 | Followings are added  3.2.20 Unable to create a local user due to a user name or email address conflict with an Active Directory server user  3.2.21 Unable to create a local user due to a user name or email address conflict with an LDAP server user  3.2.22 Problem occurs when multiple Active Directory servers are linked  3.2.23 Problem occurs when multiple LDAP servers are linked  3.2.24 User groups button for users imported from LDAP server is not displayed | March 11, 2024 |
| 21 | 11.0.2 | Followings are added  3.2.2 Steps to follow if the sysadmin account is locked.  Following are changed  3.2.13 The screen goes blank when you log in | May 17, 2024 |
| 22 | 11.0.3 | Following is removed:  A-3 DB restore method from a dump file collected with the csgetras command  Following is changed:  A-3 Downgrading Amazon Corretto 21 (The Amazon Corretto version has changed from 17 to 21.)  3.2.13 The screen goes blank when you log in (The protocol of the URL specified in the curl command was changed from http to https.) | October 24, 2024 |
| 23 | 11.0.4 | Following are changed  4.1.13.1.1 Common Services cannot startCommon Services cannot start (1) Check if Common Services is running. has been added.  4.2.73.2.7 Issues (unexpected errors, etc.) that might occur when there is a problem in the user directory serviceIssues (unexpected errors, etc.) that might occur when there is a problem in the user directory service  Following is removed 1.1.13.2.13 The screen goes blank when you log in | January 22, 2025 |
| 24 | 11.0.4 | Revise the flowchart and added annotations  1.5.6 Failure during operation  Followings are added  3.2.24 Lost the password for the idpadmin user | February 26, 2025 | |
| 25 | 11.0.4 | Followings are added  3.2.25 Failed to log in with the registered ID provider using the Embedded Keycloak. | February 26, 2025 | |
| 26 | 11.0.4 | Followings are added  3.2.26 TLS connection fails when executing the API.  Change the indentation of 3.2.25.   1. to (a). | March 13, 2025 | |

**Contents**

1 Overview 7

1.1 Scope of this document 7

1.2 Glossary 7

1.3 Required knowledge 7

1.4 Related documents 7

1.5 Troubleshooting procedures 10

1.5.1 Installation failure 10

1.5.1.1 Failure during Common Services installation 10

1.5.2 Failure during upgrade installation 11

1.5.2.1 Error in database backup during upgrade installation. 11

1.5.2.2 When Vup installing with viewpoint OVF, the CS service fails to start. 11

1.5.3 Failure during overwrite installation 12

1.5.3.1 Error in database backup during overwrite installation. 12

1.5.4 Failure during uninstallation 13

1.5.4.1 Failure during Common Services uninstallation 13

1.5.4.1.1 Forcibly uninstalling Common Services 14

1.5.5 Failure during startup 16

1.5.6 Failure during operation 17

2 Collecting Troubleshooting Information 18

2.1 Information required for troubleshooting 18

2.2 Information collection method 19

2.2.1 The method for collecting log files (csgetras) 19

2.2.1.1 Overview 19

2.2.1.2 Objectives 19

2.2.1.3 Prerequisites 19

2.2.1.4 Usage 19

2.2.1.5 Information output after executing the csgetras command 21

2.2.2 Collecting OS system information 21

2.2.2.1 Collecting system and disk information in Linux 21

2.2.2.2 Collecting system information in Windows 21

3 Common Services Failure Examples 22

3.1 Startup failures 22

3.1.1 Common Services cannot start 22

3.1.2 Items to check when Common Services cannot be started 22

3.1.3 Items to check when Common Services cannot be started in OVA 25

3.2 Operation failures 26

3.2.1 Items to check when you cannot access Hitachi Ops Center 26

3.2.2 Initializing the sysadmin user password/Unlocking the lock 31

3.2.3 Synchronization with Active Directory group fails 34

3.2.4 Registering product instances to the Products screen fails 35

3.2.5 Single-sign on for each product fails 35

3.2.5.1 Checking the SSL certificate 35

3.2.5.2 Checking settings for the registered product 36

3.2.6 Registering HDID product instances in the OVA environment after deployment fails 37

3.2.7 Issues (unexpected errors, etc.) that might occur when there is a problem in the user directory service 37

3.2.8 Items to check when you cannot access user directory service or ID provider service 38

3.2.9 AD FS registration fails 38

3.2.10 Configuration fails in AD FS 38

3.2.11 Failed to log in with registered AD FS 38

3.2.12 User directory service (Other) registration fails 42

3.2.13 The screen goes blank when you log in 43

3.2.14 Unable to register each Ops Center product in Common Services, or upgrade installation does not proceed with Express installer 46

3.2.15 Out of memory occurs 47

3.2.16 [Hitachi Edition] RemoteOps log Download API is Time Out 47

3.2.17 [Hitachi Edition] If an error occurs in the Common Services RemoteOps, what log should check? 47

3.2.18 Initializing the truststore password 47

3.2.19 When a failure occurs during backup of Common Services by the Protector backup integration function 49

3.2.20 Unable to create a local user due to a user name or email address conflict with an Active Directory server user 49

3.2.21 Unable to create a local user due to a user name or email address conflict with an LDAP server user 49

3.2.22 Problem occurs when multiple Active Directory servers are linked 49

3.2.23 Problem occurs when multiple LDAP servers are linked 50

3.2.24 User groups button for users imported from LDAP server is not displayed 50

3.3 Construction failures 50

3.3.1 Failed to install Analyzer with Server Express installer 50

Appendices 51

A-1 Operations that require restarting services 51

A-2 Checking the host name or IP address and port number for the Portal access URL 51

A-3 Downgrading Amazon Corretto 21 54

A-4 Operation to disable the service 55

A-5 How to distinguish Command Control Interface installed with Express installer 56

# Overview

## Scope of this document

ITPD, HSSC, CTSC/ESC/APSC, Hitachi Vantara, HPE

## Glossary

For details about the terminology, see the following manual:

* [ Hitachi Edition]Hitachi Ops Center Installation and Configuration Guide
* [HPE Edition]HPE XP Intelligent Management Suite Installation and Configuration Guide

Acronyms and abbreviations used in this manual are shown below.

|  |  |
| --- | --- |
| Acronym or abbreviation | Full name or meaning |
| AD | Active Directory |
| CLI | Command Line Interface |
| Common Services | [ Hitachi Edition]Hitachi Ops Center Common Services  [HPE Edition]HPE XP Common Services |
| CPU | Central Processing Unit |
| DN | Distinguished Name |
| HDID | [ Hitachi Edition]Hitachi Data Instance Director  [HPE Edition]HPE XP Data Protection Manager |
| IDP | Identity Provider |
| KDC | Key Distribution Center |
| OS | Operating System |
| OVA | Open Virtual Appliance |
| RAS | Reliability Availability Serviceability |
| rpm | RedHat Package Manager |
| SSL | Secure Socket Layer |
| URL | Uniform Resource Locator |
| VM | Virtual Machine |
| <install-directory> | Installation directory of Common Services |
| <log-directory> | [ Hitachi Edition] /var/log/hitachi/CommonService  [HPE Edition] /var/log/CVXPAE/CommonService |
| <user-data-directory> | [ Hitachi / HPE Edition] /var/<install-directory> |
| Product instance registration | In order for Common Services and each product to perform SSO or L&L, each product executes the setupcommonservice command and set up for Common Services. In this document, this operation is referred to as "product instance registration." |

Check the installation directory with the following command:

cat etc/.hitachi/COMSERV/pkgInfo | grep install.path

<*installation-directory*> is the value of the install.path value.

## Required knowledge

We expect that readers have knowledge for settings of Common Services product, OS , Network (including SSL communication), and authentication server such as Active Directory or Kerberos server.

## Related documents

Related manuals (latest version) necessary for Common Services are shown below.

When analyzing failures, please make sure you are using the latest version of the manual.

Table 2-1 Hitachi Ops Center manuals (overseas editions)

|  |  |
| --- | --- |
| Document title | Note |
| * Hitachi Ops Center Installation and Configuration Guide * Hitachi Ops Center Common Services REST API Reference Guide * Hitachi Ops Center System Requirements |  |

Table 2-2 HPE XP Intelligent Management Suite manuals (overseas editions)

|  |  |
| --- | --- |
| Document title | Note |
| * HPE XP Intelligent Management Suite Installation and Configuration Guide * HPE XP Common Services REST API Reference Guide for XP Intelligent Management Suite * HPE XP Intelligent Management Suite System Requirements |  |

Table 2-3 Other related documents

|  |  |
| --- | --- |
| Document title | Note |
| Hitachi Ops Center Common Services Log Analysis Guide |  |
| ENGINEERING CHANGE NOTICE | Overseas edition only |

## Troubleshooting procedures

### Installation failure

#### Failure during Common Services installation

Acquire log data.

- Acquire installation logs.#3

No

Yes

END

Reinstall Common Services.#1, #2

Start installation.#1, #2

No

Does an on-screen message describe how to resolve the issue?

Yes

Perform the action described in the message.

#1: Notes on installation

* Make sure that none of the following programs are running:

- Programs that monitor security

- Antivirus programs

- Process-monitoring programs

#2: Notes on reinstallation

* If an error occurs after starting the following pre-installation process, uninstall the product before re-installation. The pre-installation start message is as follows:

Now setting up database...

* If the uninstallation process fails, forcibly uninstall Common Services by following the procedure in 1.5.3.1.1 Forcibly uninstalling Common Services. Then, perform a new installation of Common Services.

Does the error occur after reinstallation?

#3: About installation logs

If you are able to execute the log file collection command, use the command to gather data.

(For details, see 2.2.1 Using the Common Services log file collection command (csgetras)).

If you are unable to execute the command, collect the following data manually:

* All files in *<log-dir>*

In addition, collect the following file if it exists in your system (this file might not exist in some installations).

/tmp/comserv\_inst\_*yyyymmdd-HHMMSS*.log

Analyze log data.

- Analyze the installation log data as described in the *Common Services Log Analysis Guide*.

Ask the support department to investigate.

Figure 1-1 Flow of response to an installation error

### Failure during upgrade installation

Refer to the procedure in 1.5.1 Installation .

#### Error in database backup during upgrade installation.

If postgresql15, postgresql15-libs, postgresql15-server do not exist when performing a upgrade installation of Common Services, the following message will be displayed on the screen and the upgrade installation fails.

"KAOP70007-E The database backup failed. The installation will now end."

Please follow the steps below:

1. Execute the following command and check if postgresql15, postgresql15-libs, postgresql15-server exist.

Check with the following command.

rpm -qa | grep postgresql15

Note: Check postgresql11 packages if your Common Services is 10.9.2 or ealier, check postgresql15 if your Common Services is 10.9.3 or later.

1. Store postgresql packages on the management server where Common Services is installed.

For details on the versions of postgresql packages that are supported by Common Services, see the Release Notes for Common Services.

Use the following rpm file included in the installation media when downgrading to postgresql packages.

*root-directory-of-installation-media*/Common/COMSERV/rpm/*postgresql-rpm-file*

1. If postgresql15, postgresql15-libs, postgresql15-server do not exist, execute the following command and install postgresql15, postgresql15-libs, postgresql15-server.

rpm -iv --nodeps --replacepkgs postgresql15-libs*-rpm-file*

rpm -iv --nodeps --replacepkgs postgresql15*-rpm-file*

rpm -iv --nodeps --replacepkgs postgresql15-server*-rpm-file*

Note: There are dependencies between packages. Please refer to the above order when installing.

1. Execute the upgrade installation of Common Services.

#### When Vup installing with viewpoint OVF, the CS service fails to start.

In the viewpointOVF environment, if you try to install Vup by transferring a disk from CS10.9.2 or earlier to CS11.0.0, the DB migration process fails, and the CS service startup also fails. The DB migration process requires that both PostgreSQL 11/15 be installed.

Since viewpointOVF 11.0.0, the PostgreSQL 11 to PostgreSQL 15 migration process fails because PostgreSQL 11 is not pre-installed.

The manual describes how to upgrade CS to 10.9.3 or later using the installer before replacing the disk. If you did not upgrade CS before moving the disk, perform the following steps:

(1) Install PostgreSQL11 packages(\*) manually

(2) Restart the Common Services service

\*PostgreSQL11 packages can be obtained from the Internet.

The packages consist of the following three.

- postgresql11-11.20-2PGDG.rhel8.x86\_64

- postgresql11-server-11.20-2PGDG.rhel8.x86\_64

- postgresql11-libs-11.20-2PGDG.rhel8.x86\_64

### Failure during overwrite installation

Refer to the procedure in 1.5.1 Installation .

#### Error in database backup during overwrite installation.

If postgresql15, postgresql15-libs, postgresql15-server do not exist when performing a overwrite installation of Common Services, the following message will be displayed on the screen and the overwrite installation fails.

"KAOP70007-E The database backup failed. The installation will now end."

Please follow the steps below:

1. Execute the following command and check if postgresql15, postgresql15-libs, postgresql15-server exist.

Check with the following command.

rpm -qa | grep postgresql15

1. Store postgresql packages on the management server where Common Services is installed.

For details on the versions of postgresql packages that are supported by Common Services, see the Release Notes for Common Services.Use the following rpm file included in the installation media when downgrading to postgresql packages.

*root-directory-of-installation-media*/Common/COMSERV/rpm/*postgresql-rpm-file*

1. If postgresql15, postgresql15-libs, postgresql15-server do not exist, execute the following command and install postgresql15, postgresql15-libs, postgresql15-server.

rpm -iv --nodeps --replacepkgs postgresql15-libs*-rpm-file*

rpm -iv --nodeps --replacepkgs postgresql15*-rpm-file*

rpm -iv --nodeps --replacepkgs postgresql15-server*-rpm-file*

Note: There are dependencies between packages. Please refer to the above order when installing.

1. Execute the overwrite installation of Common Services.

### Failure during uninstallation

#### Failure during Common Services uninstallation

Start uninstallation

No

Yes

Did an uninstallation error occur?

END

1.5.3.1.1 Forcibly uninstalling Common Services

Figure 1-2 Flow of response to an uninstallation error

##### Forcibly uninstalling Common Services

If the results of the investigation by the support department indicates that a forced uninstallation is required, remove Common Services by following the procedure below.

Note 1: If necessary, uninstall the following rpm packages that are installed in the user directory when installing Common Services.

- java-17-amazon-corretto-devel

- postgresql15

- postgresql15-server

- postgresql15-libs

Stop Common Services.#1

Delete files (or directories).#2

Deleting set up information of operating system.#3

Restart the daemon#4

END

Figure 1‑3 Flow of forced uninstallation (Linux)

(1) Linux procedures

#1: Stop Common Services

Stop related processes by systemctl command.

systemctl stop csportal.service

systemctl --no-reload disable csportal.service

systemctl stop postgresql-15@csportal.service postgresql-15@csidp.service

systemctl --no-reload disable postgresql-15@csportal.service postgresql-15@csidp.service

#2: Delete files or directories

Delete files or directories by rm command.

1. HV/ HPE Edition

rm -rf /etc/systemd/system/postgresql-15@csidp.service.d

rm -rf /etc/systemd/system/postgresql-15@csportal.service.d

rm -f /etc/systemd/system/csidpdbmigration.service

rm -f /etc/systemd/system/csportaldbmigration.service

rm -f /etc/systemd/system/postgresql-15@csidp.withdbmigration.service

rm -f /etc/systemd/system/postgresql-15@csportal.withdbmigration.service

rm -rf /etc/.hitachi/COMSERV

rm -rf <install-directory>

rm -rf <user-data-directory>

rm -rf <log-directory>

#3 Deleting set up information of operating system

Delete set up information of operating system by rm command.

rm -rf /etc/systemd/system/csportal.service

rm -rf /etc/logrotate.d/csportal

rm -rf /etc/logrotate.d/csgateway

rm -rf /etc/logrotate.d/csidpaccess

rm -rf /etc/logrotate.d/csidpserver

rm -rf /etc/cron.hourly/logrotate\_cshourly

#4 Restart the daemon

Reflect information about the deletion of Common Services startup scripts on the OS by systemctl command.

systemctl daemon-reload

### Failure during startup

Common Services fails to start

Yes

Is there an applicable scenario in 3.1 Startup failures?

Follow the prescribed procedure in 3.1 Startup failures.

No

No

Is the problem resolved?

Yes

END

Collect troubleshooting information.

(For details, see 2. Collecting Troubleshooting Information.)

Analyze log data.

- Analyze the log files by referring to the Common Services Log Analysis Guide.

Ask the support department to investigate.

Figure 1‑4 Flow of response to an Common Services startup error

### Failure during operation

An error occurs.

Does an on-screen message describe how to resolve the issue?

No

END

Yes

Perform the action described in the message.

Yes

Is the problem resolved?

No

Yes

Follow the procedure in the example in 3.2 Operation failures.

Is the problem resolved?

Is there an applicable scenario in 3.2 Operation failures?

No

No

Yes

END

Is it an issue related to the ID provider?

No

Yes

No

Is the ID provider supported?#1

Yes

Not supported

Collect troubleshooting information.

(For details, see 2. Collecting Troubleshooting Information.)

Analyze log data.

- Analyze the log files by referring to the Common Services Log Analysis Guide.

Ask the support department to investigate.

Figure 1‑5 Flow of response to an error during Common Services operation

#1 Support will only be available if all of the following conditions are met in the event of a failure with the ID provider. In other cases, support will not be available, so please refer to the documentation for Keycloak or the ID provider to resolve the issue.

* It is the ID provider supported by Common Services.

As of April 2025, only AD FS is supported.

For details, see the manual "*Supported identity providers (AD FS)*" in the *Hitachi Ops Center Installation and Configuration Guide*.

* The ID provider is registered from the Hitachi Ops Center Portal.

It is not registered from the embedded Keycloak, and the ID provider is displayed on the ID provider window of the Hitachi Ops Center Portal.

# Collecting Troubleshooting Information

## Information required for troubleshooting

This section describes the information you need to collect when an error occurs. For details about the various log files, see *4. Detailed log file information* in the *Common Services Log Analysis Guide*.

To ensure that the support division has all of the information it needs to accurately diagnose the problem, submit all of the mandatory notification items listed in 1) below. In addition, copy and attach screenshots of the Common Services interface showing the operations you performed.

For an example of error reporting, see *Figure 2-1 Example of error reporting*.

1. Mandatory Notification Items

* Event that occurred
* Time of occurrence
* System configuration drawing (server OS, network configuration, etc.)
* Details of operations performed (window transitions, buttons clicked, etc.)
* Hitachi Ops Center (HPE XP Intelligent Management Suite) information
* OS (including service pack)
* Hitachi Ops Center (HPE XP Intelligent Management Suite) version
* Java version
* Data collected by the log file collection command (csgetras)
* Web Client information
* OS (including service pack)
* Web browser type and version (including service pack)

The following information is mandatory if the fault occurs during CLI execution:

* Commands entered in the command line
* Executed batch files, if any

|  |
| --- |
| - Event: A product registered in Ops Center is not displayed on the Inventory tab.  Time of occurrence: Around 15:55, May 20, 2020  [Common Services server]  OS: Red Hat Enterprise Linux 7.6  Hitachi Ops Center Common Services: 10.0.0-01  JAVA version: 1.8.0\_222  [Web client]  OS: Windows Server 2019 noSP  Browser: IE11  - Operations  (1) Register the product to Ops Center with the setupcommonservice command.  (2) Login to Ops Center with administrator privilege.  (3) Display the Products tab. |

Figure 2-1 Example of error reporting

## Information collection method

### The method for collecting log files (csgetras)

#### Overview

In the directory specified in the dir option of this command, create an archive file (Common\_csgetras.jar) that collects and compresses error information.

If the directory specified in the dir option does not exist, create it.

#### Objectives

To collect the log files, databases, and other information required to analyze Common Services errors from the operating environment in a single operation, to ensure smooth customer support.

#### Prerequisites

* The logged-in user must have the root permission or an equivalent permission.
* Common Services must be installed on the machine where the command is used.
* Java must be available in the environment where the command is used.

#### Usage

(1) Example

* In Linux:

|  |
| --- |
| *<install-directory>*/utility/bin/csgetras.sh -dir<*output-directory*> |

(2) Option

- dir

Specify an absolute path to the directory on the local disk where the collected maintenance information is to be saved.

ASCII printable character code excluding some special characters can be specified for the path.

Special characters that cannot be specified are as follows: \ / : , ; \* ? " < > | $ % & ' `

For Linux, a slash (/) can be used as a path separator, but a space cannot be used in the path.

If it is specified so that the output destination cannot be specified in the backup directory, an error message is displayed and the process ends.

(3) Return value

Table 2-1 Return value for the csgetras command

|  |  |
| --- | --- |
| Retrun value | Result |
| 0 | Successful completion |
| 1 | Argument error |
| 2 | Collection target definition file not existing |
| 255 | Abnormal completion other than the above |

(4) Message ID

Table 2-2 Message ID output by the csgetras command

|  |  |  |
| --- | --- | --- |
| Message ID | Description | Workaround |
| KAOP60001-I | Collection of RAS data for Common Service will now start. | Unnecessary |
| KAOP60002-I | Collection of RAS data for Common Service was successful. | Unnecessary |
| KAOP60311-W | Cannot delete the temporary directory (directory name: *{0}*). | Delete the directory indicated by the message. (0: *directory-name*) |
| KAOP60312-W | Cannot archive the directory (directory name: *{0}*). | Compress the directory indicated by the message. (0: *directory-name*) |
| KAOP60621-E | An option is invalid.usage: csgetras.sh -dir DirectoryName | An option is invalid. Check the option specified for the command. |
| KAOP60622-E | Collection of RAS log data Common Service failed (maintenance information: *{0}*). | Solve the problem according to the return value {0} of the csgetras command. |
| KAOP60623-E | Cannot make the directory (directory name: *{0}*). | The directory specified in the dir option could not be created. Check if there is a file with the same name and try again. (0: *value-specified-for-dir-option*) |
| KAOP60624-E | Output directory is included in the RAS source directory. (directory name: *{0}*) | The directory specified in the dir option already exists in the directory for saving. Specify a different directory and re-execute the command. |

#### Information output after executing the csgetras command

After executing the csgetras command, the following files are output to the directory specified for the dir option.

(1) Common\_csgetras.jar

Archive file that stores error information

If the csgetras command succeeds, send it to the help desk.

(2)csgetras.log

csgetras command execution log

If the csgetras command fails, send it to the help desk.

### Collecting OS system information

#### Collecting system and disk information in Linux

Execute the csgetras command.

For details, refer to 2.2.1The method for collecting log files (csgetras).

#### Collecting system information in Windows

No information is required.

# Common Services Failure Examples

## Startup failures

If you cannot start Common Services, take action according to the following procedures.

### Common Services cannot start

1. Check if Common Services is running.

systemctl status csportal

* The value of Active is “active (running)”.
* The following processes exist in the Cgroup hierarchy:
  + A process starting with “nginx: master process”
  + Two java processes

1. If not, start Common Services.

systemctl start csportal

### Items to check when Common Services cannot be started

1. Check if Amazon Corretto or PostgreSQL has been uninstalled or if their versions are not supported.

Use the following command to check the package information of Amazon Corretto and PostgreSQL:

rpm -qa | grep amazon-corretto

rpm -qa | grep postgresql

# Use the following command to check the package information from the failure information collected by the csgetras command.

grep amazon-corretto <*decompression-directory-for-csgetras-result*>/Common\_csgetras/rpm\_qa.txt

grep postgresql <*decompression-directory-for-csgetras-result*>/Common\_csgetras/rpm\_qa.txt

# Target package names are as follows:

- java-17-amazon-corretto-devel

- postgresql15

- postgresql15-server

- postgresql15-libs

If the target package has been uninstalled, reinstall the Common Services. (The above packages are installed by re-installing Common Services.)

If the installed package is not supported, uninstall the package and reinstall Common Services.

1. Check that port numbers do not conflict.

Use the following command to check for port number conflicts:

ss -an | grep ":<*Portal-startup-port*> [^0-9]"

# Use the following command to check for port number conflicts from the failure information collected by the csgetras command.

grep ":443[^0-9]" <*decompression-directory-for-csgetras-result>*/Common\_csgetras/ss\_aenpo.txt

The following is an output example where port numbers conflict. If port numbers do not conflict, nothing is output. (If the status is LISTEN, the port is being used.)

tcp LISTEN 0 128 \*:<*Portal-startup-port*> \*:\*

# The default port number is 443,20951,20952 and 20954 to 20956.

If a port number is displayed by the above command, change the port number for Common Services or the conflicting one.

1. Check if the server certificate and private key are the correct key pair

If the server certificate and private key are not the correct key pair, the Common Services service will fail to start. If the key pairs do not match, the following error will be output to the GW error log (<log-directory>/nginx/error.log).

|  |
| --- |
| *YYYY/MM/DD hh:mm:ss* [emerg] 14660#14660: SSL\_CTX\_use\_PrivateKey("*<Absolute path of private key>*") failed (SSL: error:0B080074:x509 certificate routines:X509\_check\_private\_key:key values mismatch) |

If the server certificate and private key are the correct key pair, the Modulus values will match.

Common Services can be configured with server certificates and private keys for RSA and ECDSA cryptography. Check the properties in <user-data-directory> /userconf/config\_user.properties for the storage location of the server certificate and private key.

Table 4‑1 Properties in config\_user.properties

|  |  |  |
| --- | --- | --- |
| # | Property name | Contents |
| 1 | CS\_GW\_SSL\_CERTIFICATE | Absolute path of server certificate for RSA |
| 2 | CS\_GW\_SSL\_CERTIFICATE\_KEY | Absolute path of private key for RSA |
| 3 | CS\_GW\_SSL\_CERTIFICATE\_ECDSA | Absolute path of server certificate for ECDSA |
| 4 | CS\_GW\_SSL\_CERTIFICATE\_KEY\_ECDSA | Absolute path of private key for ECDSA |

Modulus must match in CS\_GW\_SSL\_CERTIFICATE and CS\_GW\_SSL\_CERTIFICATE\_KEY, CS\_GW\_SSL\_CERTIFICATE\_ECDSA and CS\_GW\_SSL\_CERTIFICATE\_KEY\_ECDSA.

Follow the steps below to check if the server certificate and the Modulus value of the private key match.

(a) Execute the following command to check the Modulus of the server certificate.

openssl x509 -in <Server certificate path> -modulus -noout | openssl md5

Example)

# openssl x509 -in /var/opt/hitachi/CommonService/tls/tmpserver\_chained.crt -modulus -noout | openssl md5

(stdin)= 53393b656e90ad3f1c4d56d061eb78dc

\* In the above case, "53393b656e90ad3f1c4d56d061eb78dc" is the value of Modulus.

(b) Execute the following command to check the Modulus of the private key.

openssl rsa -in <Path of private key> -modulus -noout | openssl md5

Example)

# openssl rsa -in /var/opt/hitachi/CommonService/tls/tmpserver.key -modulus -noout | openssl md5

(stdin)= 53393b656e90ad3f1c4d56d061eb78dc

\* In the above case, "53393b656e90ad3f1c4d56d061eb78dc" is the value of Modulus.

(c) Check if the Modulus value of the server certificate collected in (a) matches the Modulus value of the private key collected in (b). If they do not match, recreate the server certificate or both the server certificate and private key, and set SSL again.

1. Check the status of database.

If you performed an upgrade installation from 10.9.2 or earlier to 10.9.3 or later, the database will be migrated.

Follow the steps below to check the status of the database.

(a) Check if database is running.

|  |
| --- |
| systemctl status postgresql-15@csidp  systemctl status postgresql-15@csportal |

(b) Check if database migration was successful.

If the database is not started, check whether the following message is output to csdbmigration log (<log-directory>/utility/csdbmigration\_\*\_yyyy-mm-dd-HH-MM-SS.log).

|  |
| --- |
| yyyy/mm/dd HH:MM:SS.SSS [INF] csdbmigration completed successfully. |

if the database migration was failed, Contact Support Center, who may ask you to collect troubleshooting information.

### Items to check when Common Services cannot be started in OVA

1. Check the cschgconnect command log.

When deploying OVA, if you do not check "Connect at power on" in the VM network adapter 1 settings before executing the opsvmsetup command, the cschgconnect command log (<log-directory>/utility/cschgconnect\_\*.log), the following error is output.

|  |
| --- |
| *YYYY/MM/DD hh:mm:ss* [WRN] KAOP64017-W The IP address information cannot be obtained. Therefore, accessing the URL by IP address is not possible. Check the connection and try again later. |

If the above error is output, you need to check "Connect at power on" in the VM's network adapter 1 settings, and then restart the VM (shutdown -r now).

## Operation failures

### Items to check when you cannot access Hitachi Ops Center

1. If you cannot log in to Hitachi Ops Center, check the following settings

- Your user ID and password are correct.

- You are registered as a user with Hitachi Ops Center.

- Your user account is enabled.

- If you are an Active Directory linkage user, see Figure 3-1 Confirmation method for Active Directory access.

Use the following procedure to check whether the external authentication server (Active Directory) is properly authenticated.

Unable to log in as an Active Directory linkage user?

Use kerberos authentication?

No

Contact a user administrator with administrative privilege.

Yes

Check if the KDC address can be resolved?

Log in to Common Services as a local user with administrative privilege.

Yes

Problem solved?

Display the User directories screen from Manage users.

No

Check if a user who has the same sAMAccountName for the username as the user that cannot log in is included in the DN subtree specified in the Base DN of Common Services.#1

Click the **Edit user directory service** button for the entry that you want to update.

Reset the password of the user on the Active Directory side.

Contact users that could not log in.

Yes

Can they log in?

No

Change the value of the Base DN.

Included?

No

Yes

Click the **Test connection** button to check the connection.

After entering the Bind user password, press the **Test authentication** button and confirm the authentication.

No

Yes

Check the following#1:

- Is the setting for BIND UESR DN correct?

- Is the setting for BIND USER PASSWORD correct?

Resolve the problem.

Yes

Check the following:

- Is the setting of [CONNECTION URL] correct?

- Is there any network failure?

- Has a failure occurred in the Active Directory server?

Resolve the problem.

No

Successful connection?

Analyze log data.

- Analyze the installation log data as described in the Common Services Log Analysis Guide.

Authentication successful?

Contact the help desk.

END

**Figure 3-1 Confirmation method for Active Directory access**

#1 The values entered when registering or updating Active Directory linkage can be checked by using the following method:

Search for the next message output last in <*log-directory*>/debug.log.

- Output log when registering

"KAOP00000-I Method start. (Class:InnerApiController, Method:innerCreateUserFederation, Argument:"

- Output log when updating

"KAOP00000-I Method start. (Class:InnerApiController, Method:innerUpdateUserFederation, Argument: "

Check the value output to "Argument:" in the searched message.

\* For details on debug\_log, see the *Common Services Log Analysis Guide*.

1. Check if the firewall settings are correct.

Execute the following command and confirm that the Common Services access ports above the REJECT line are ACCEPT in the target column. (In the following example, dpt:https is output because it is the default port 443.)

# iptables -L

Chain INPUT (policy ACCEPT)

target prot opt source destination

**ACCEPT tcp -- anywhere anywhere tcp dpt:https**

ACCEPT all -- anywhere anywhere state RELATED,ESTABLISHED

ACCEPT icmp -- anywhere anywhere

ACCEPT all -- anywhere anywhere

ACCEPT tcp -- anywhere anywhere state NEW tcp dpt:ssh

**REJECT**  all -- anywhere anywhere reject-with icmp-host-prohibited

# firewall-cmd --list-all

public (active)

target: default

icmp-block-inversion: no

interfaces: ens192

sources:

services: cockpit dhcpv6-client ssh https

ports: 24221/tcp 25445/tcp 25442/tcp 22016/tcp

protocols:

forward: no

masquerade: no

forward-ports:

source-ports:

icmp-blocks:

rich rules:

#

1. Check if the access URL specified for the browser is different from Common Services.

The access URL is specified by the host name or IP address for Common Services by either of the following:

- Specified during installation

- Changed by the cschgconnect command after installation

If the access URL specified for the browser is different from the setting, specify the access URL according to the settings of Common Services.

For details on how to check the current settings, see *A-2 Checking the host name or IP address and port number for the Portal access URL*.

1. Check if the SSL settings are correct

Check that the root certificate for the Common Services server has been imported to the trust store.

Execute the following command and confirm that the root certificate can be displayed.

keytool -v -list -keystore *<user-data-directory>*/tls/cacerts

1. Check if the services are restarted after executing the cschgconnect command

If the cschgconnect command is executed after the Common Services services start, restart the services.

- How to check the execution time of the cschgconnect command

Check the log file output by the following command. The latest creation time is the last execution time of the command.

ls -l *<log-directory>*/utility/cschgconnect\_\*.log

- How to check the startup time for the Common Services services

Execute the following command to check the time of the last output line.

grep "JVM running for" /var/log/hitachi/CommonService/csportal.log | awk '{print substr($0, index($0, $0), index($0, " ") -1 )}'

1. Check if access to the https port is blocked

If you have a network connection to the host on which Common Services is installed, but you still cannot access the Hitachi Ops Center Portal, it may be blocked by a firewall.

Run the following command on the client accessing Common Services and make sure you can access the https port.

curl -k -v https: // <hostname or IP address>: <port number> / portal

Sample output when the port is blocked

\* Trying <IP address>...

\* TCP\_NODELAY set

\* connect to <IP address> port <Port number> failed: No route to host

\* Failed to connect to <Host name> port <Port number>: No route to host

\* Closing connection 0

curl: (7) Failed to connect to <Host name> port <Port number>: No route to host

If you are unable to access it, check your firewall settings.

The confirmation method and setting method differ depending on the type of firewall such as iptables, nftables, firewalld.

### Initializing the sysadmin user password/Unlocking the lock

If you forget the password for sysadmin, the built-in user in the customer environment, you need to initialize the password. Additionally, if sysadmin gets locked, you need to unlock it. Use the following procedure to initialize the password and unlock sysadmin.

In addition, if the customer environment is reproduced from the failure information collected by the csgetras command by using the procedure described in A-3 DB restore method from a dump file collected with the csgetras command , the sysadmin password must be initialized.

1. Export the environment variables.

eval export `grep -v '^#' <install-directory>/conf/config\_system.properties`

eval export `grep -v '^#' <user-data-directory>/userconf/config\_user.properties`

1. Get the process ID of Keycloak.

KEYCLOAK=$(ps -C java -o pid,cmd | awk '/keycloak\/bin/{print $1}')

1. Get the Keycloak administrator username and password.

eval $(tr '\0' '\n' < "/proc/${KEYCLOAK}/environ" | grep '^CS\_IDP\_ADMIN\_')

1. Acquire an access token with the Keycloak administrator.

TOKEN=$(curl --noproxy 127.0.0.1 -X POST -H "Content-Type: application/x-www-form-urlencoded" -d "grant\_type=password&client\_id=admin-cli&username=${CS\_IDP\_ADMIN\_USERID}&password=${CS\_IDP\_ADMIN\_PASSWORD}&scope=openid" [http://127.0.0.1:${CS\_PORTAL\_IDP\_PORT}/auth/realms/master/protocol/openid-connect/token](http://127.0.0.1:$%7bCS_PORTAL_IDP_PORT%7d/auth/realms/master/protocol/openid-connect/token) 2>/dev/null | sed 's/.\*access\_token":"//g' | sed 's/".\*//g')

1. Display the user list.

curl --noproxy 127.0.0.1 -X GET -H "Content-Type: application/json" -H "Authorization: Bearer ${TOKEN}" "http://127.0.0.1:${CS\_PORTAL\_IDP\_PORT}/auth/admin/realms/${CS\_IDP\_OP\_BASE\_ID}/users "

Execution result example

[{"id":"efc652da-8f50-400a-a950-7fe716b8e979",

"createdTimestamp":1571896330506,

"username":"sysadmin",

"enabled":true,

"totp":false,

"emailVerified":false,

"email":"sysadmin@local",

"attributes":{"description":["Built-in user"]},

"disableableCredentialTypes":["password"],

"requiredActions":[],"notBefore":0,

"access":{"manageGroupMembership":true,"view":true,"mapRoles":true,"impersonate":true,"manage":true}}]

1. According to the execution result (5), set the environment variable CS\_TMP\_USER\_ID to the id for which the username is sysadmin.

In the following example, the id of the execution result example in (5) is used.

CS\_TMP\_USER\_ID=efc652da-8f50-400a-a950-7fe716b8e979

(7)-1 Reset the sysadmin password.

curl --noproxy 127.0.0.1 -X PUT -H "Content-Type: application/json" -H "Authorization: Bearer ${TOKEN}" -d '{"value":"sysadmin", "type":"password", "temporary":"false"}' "http://127.0.0.1:${CS\_PORTAL\_IDP\_PORT}/auth/admin/realms/${CS\_IDP\_OP\_BASE\_ID}/users/${CS\_TMP\_USER\_ID}/reset-password"

(7)-2 Unlock the sysadmin.

curl --noproxy 127.0.0.1 -X PUT -H "Content-Type: application/json" -H "Authorization: Bearer ${TOKEN}" -d '{"enabled":true}' "

http://127.0.0.1:${CS\_PORTAL\_IDP\_PORT}/auth/admin/realms/${CS\_IDP\_OP\_BASE\_ID}/users/${CS\_TMP\_USER\_ID}

1. Delete the access tokens and environment variables.

unset TOKEN CS\_TMP\_USER\_ID KEYCLOAK CS\_IDP\_ADMIN\_USERID CS\_IDP\_ADMIN\_PASSWORD

### Synchronization with Active Directory group fails

Use the following procedure to check whether Active Directory groups and groups imported to Common Services can be synchronized correctly.

Check if a group with a DistinguishedName that matches the group DN specified in Group entry list of Common Services exists in Active Directory.

Group sync fails.

Log in to Common Services as a local user with administrative privilege.

Yes

Does it exist?

No

Display the User directories screen from Manage users.

Change the value of the group DN specified in Group entry list.

Contact the help desk.

No

Change the value of the Base DN.

Yes

Included?

Yes

Analyze log data.

- Analyze the installation log data as described in the Common Services Log Analysis Guide.

Is the group synchronized

No

Click the **Edit user directory service** button for the entry that you want to update.

Is the Active Directory group included in the DN subtree specified for the Base DN of Common Services.#1

Click the **Test connection** button to check the connection.

Successful connection?

Yes

No

Check the following:

- Is setting of [CONNECTION URL] correct?

- Is there any network failure?

- Has a failure occurred in the Active Directory server?

Execute Sync Groups.

Resolve the problem.

Yes

No

After entering the Bind user password, press the **Test authentication** button and confirm the authentication.

Authentication successful?

Check for the following problems.#1

- Is the setting for BIND UESR DN correct?

- Is the setting for BIND USER PASSWORD correct?

END

Resolve the problem.

**Figure 3-**2 **Confirmation method for group synchronization**

#1 Refer to #1 in "**Figure 3-3 Confirmation method for Active Directory access**" for the confirmation method.

### Registering product instances to the Products screen fails

Check the setupcommonservice command log to see if the registered Common Services URL specified in the argument of the setupcommonservice command is correct.

Use the following procedure to check the Common Services API log.

(1) Check if the Common Service API succeeded

If the following message is output to <*log-directory*>/debug.log at the setupcommonservice command execution time, it indicates that the setupcommonservice command succeeded.

"KAOP00002-I Method end normally. (Class:AppApiController, Method:createApplicationService, Return:"

(2) Check if the setupcommonservice command has failed

If the KAOP00002-I message cannot be found in (1) and if the following message is output to <*log-directory*>/debug.log at the setupcommonservice command execution time, the setupcommonservice command has failed. Check the argument of the setupcommonservice command and re-execute the command.

"KAOP00000-I Method start. (Class:AppApiController, Method:createApplicationService, Argument:"

For the argument when the setupcommonservice command fails, search the following character string output at the command execution time in <*log-directory*>/debug.log, and check the value output to "Argument: ".

\* For details on debug\_log, see the *Common Services Log Analysis Guide*.

(3) If you cannot confirm the success or failure of the Common Services API in (1) and (2), check with the administrator as to whether the setupcommonservice command has been executed.

If the command has been executed but success or failure cannot be confirmed on Common Services, check your product for any cause of failure in the setupcommonservice command, resolve the problem, and re-execute the command.

For the confirmation method on the product, refer to the troubleshooting guide or manual for your product.

### Single-sign on for each product fails

#### Checking the SSL certificate

If the GUI of the product is not displayed after clicking the host name (or IP address) for the registered product from the Products screen, check that there is no problem with the SSL certificate for the server certificate of the product registered in the Common Services trust store.

(1) Check if the SSL certificate has been imported to the trust store.

For the confirmation method, refer to *Check for SSL settings* in 3.1.1Common Services cannot start.

(2) Check whether the expiration date has expired.

Execute the following command:

keytool -printcert -file *<certificate>*

In the output result of Valid from:<*start-date*> until:<*expiration-date*>, check whether <*valid-date*> is in the past.

If it has expired, import the new SSL certificate into the Common Services trust store.

#### Checking settings for the registered product

If a product registered with the setupcommonservice command is not displayed on the Products screen, the scheme, host name, or port number of the product may not match the execution result of the setupcommonservice command. In this case, check the arguments specified in the setupcommonservice command.

For the arguments when executing the setupcommonservice command, search for the following character string output to the command execution time in <*log-directory*>/debug.log, and check the value output in "Argument:".

\* For details on debug\_log, see the *Common Services Log Analysis Guide*.

"KAOP00000-I Method start. (Class:AppApiController, Method:createApplicationService, Argument:"

If the scheme, host name, or port number of the product differs from the execution result of the setupcommonservice command, rectify the incorrect item and then re-execute the setupcommonservice command.

### Registering HDID product instances in the OVA environment after deployment fails

If the VM specifications do not meet the system requirements, HDID product instance registration may fail after the opsvmsetup command is executed.

Check if the VM where the OVA file is installed meets the requirements described in "*Default settings for the virtual machine and the guest operating system*" in the *Hitachi Ops Center Installation and Configuration Guide*. If not, install the OVA file on ESXi that meets the requirements.

If the requirements are met, re-execute the HDID product registration command (setcommonservice) and re-register the product instance with the Common Service.

Refer to the following manuals for how to check the VM requirements:

For HV:Hitachi Ops Center Virtual Appliance System Requirements  
For HPE:HPE XP Intelligent Management Suite Virtual Appliance System Requirements

### Issues (unexpected errors, etc.) that might occur when there is a problem in the user directory service

If there is a problem in the user directory services, issues such as the following might occur:

• When a non-existent Username is specified in the login window, an unexpected error occurs.

• When an attempt is made to register a new user, an unexpected error occurs.

• When an attempt is made to display details of a user group, an unexpected error occurs.

• When an email address is modified in the Profile window and then submitted, an internal server error occurs.

• The user of a user directory service cannot log in.

• The user of a identity provider cannot log in.

• When clicking the Pre-check the number of users (filter) button, Pre-check the number of imported users button, or Submit button on the Add user directory service or Edit user directory service screen, an unexpected error occurs.

If any of these issues occurs, perform a connection test and verification test of the user directory service, and check whether there is a problem with the user directory service. If there is a problem, resolve it. Disable the user directory service that has the problem until you resolve the problem.

For problems with the user directory service, possible issues include the following:

• Issues with the machine, OS, or services, etc., of the user directory service

• Issues with the network to the user directory service

• Incorrect information registered for the user directory service (including mismatch of user and password)

• Incorrect SSL settings

• Mismatch between the CN and SAN set in the AD server certificate and the Connection URL

• The response time from the User Directory Service is too long (It is configured with a multi-domain structure, etc)

For details on how to perform the connection test and verification test for the user directory service, and how to modify the service, see the manual.

### Items to check when you cannot access user directory service or ID provider service

1. Check if the SSL settings are correct

Check that the root certificate of the CA for the user directory service or ID provider service has been imported to the trust store.

Execute the following command and confirm that the root certificate can be displayed.

keytool -v -list -keystore *<user-data-directory>*/tls/cacerts

1. Check that the Connection URL and the CN set in the user directory service or ID provider service certificate match

Execute the following command and confirm the CN set in the user directory service or ID provider service certificate.

openssl s\_client -connect *<host-name of the user directory service or ID provider service>*:*<port-number of the user directory service or ID provider service>* -showcerts

### AD FS registration fails

You entered the Metadata URI on the Add Identity provider screen, but you cannot go to the next entry screen.  
The following message is displayed on the screen.  
"Failed to import metadata."  
"KAOP20087-E The metadata endpoint is incorrect or the certificate is not set correctly. (There is no additional information.) "  
  
Check for SSL/TLS or Metadata URI configuration issues between Common Services and AD servers.  
See the manual "*Configuring SSL communications*" or "*Checking the AD FS metadata endpoint*" in *Hitachi Ops Center Installation and Configuration Guide*.

### Configuration fails in AD FS

When you add a Relying party, the metadata import fails with the URL specified on the Select Data Source screen.

"An error occurred during an attempt to read the federation metadata. Verify that the specified URL or host name is a valid federation metadata endpoint."  
  
Check for SSL/TLS configuration issues between Common Services and AD servers.  
See the manual "*Configuring SSL communications*" in *Hitachi Ops Center Installation and Configuration Guide*.

### Failed to log in with registered AD FS

1. If the log in using external identity provider link does not appear on the Common Services login screen.  
   Change registered AD FS Enabled to True.
2. The following error appears on the AD FS sign-in screen  
   "An error occured."  
   "Error Details: MSIS7007: The requested relying party trust 'https://<*hostname*>/auth/realms/<*Vendor-specific opscenter xpims*>' is unspecified or unsupported. If a relying party trust was specified, it is possible that you do not have permission to access the relying party. Contact your administrator for details."  
     
   Or the following error is logged in the AD FS event log of the AD FS server.  
   "Microsoft.IdentityServer.Web.InvalidScopeException: MSIS7007: The requested relying party trust 'https://<*hostname*>/auth/realms/<*Vendor-specific opscenter xpims>*' is unspecified or unsupported. If a relying party trust was specified, it is possible that you do not have permission to access the trust relying party. Contact your administrator for details."  
     
   Check the AD FS event log for the following steps.
   1. Log in to the AD FS server.
   2. Select Start > Windows Administrative Tools > Event Viewer.
   3. From the tree at the left side, select Applications and Services Logs > AD FS > Admin.

Check the relying party settings in AD FS for problems.  
See the manual "*Registering Common Services in AD FS as a relying party*"and"*Setting up a claim issuance policy*" in *Hitachi Ops Center Installation and Configuration Guide*.

1. You receive the following error in the Common Services login screen.  
   "Contact your administrator. Unable to get login user attribute information."  
   1. On the AD FS side, Check the "*Mapping of LDAP Attributes to outgoing claim types*" of "*Send LDAP Attributes as Claims*" of relying party configuration issues.  
        
      See the manual "*Setting up a claim issuance policy*" in *Hitachi Ops Center Installation and Configuration Guide*.
   2. On the AD FS side, verify that the login user has a value for the attribute set to LDAP Attributes.   
        
      See the manual for how to verify the LDAP Attribute "*Setting up a claim issuance policy*" in *Hitachi Ops Center Installation and Configuration Guide*.  
        
      The attributes are checked by the following procedure.  
        
      Procedure
      1. Log in to the AD FS server.
      2. Choose Start > Windows PowerShell > Windows PowerShell.
      3. Run the following command to get the list of users.

|  |
| --- |
| dsquery user |

* + 1. Find the DN of the logged-in user from the user list.
    2. Run the following command to get the attributes of the logged-in user.

|  |
| --- |
| dsquery \* <DN of the logged-in user> -scope base -attr \* |

\*The LDAP attribute is the CN of Active Directory Schema, and the attributes obtained in the command are Ldap-Display-Name of Active Directory Schema, so please translation.

\*Token-Groups-Qualified by Domain Name is set to a valid value by default, so the verification step is omitted.

1. You receive the following error in the Common Services login screen.  
   "Your session is not valid.  
    Possible causes are: XXXX"  
     
   Users logged in with AD FS are not granted a group of Common Services.  
   Change the registered AD FS Default group mapper or Custom group mapper to grant groups to users logged in with AD FS.
2. You receive the following error in the Common Services login screen.  
   "Account already exists  
    User with XXXX already exists. How do you want to continue?"  
     
   After changing the NameID policy format of AD FS in Common Services, by logging in without deleting the user of the AD FS, because the unnecessary information remains, it becomes information mismatch.  
   Delete users of the AD FS in Common Services.  
     
   Alternatively, if you re-register an AD FS Relying Party, Application Group, or Common Services external IdP, the user imported before the re-registration will be determined to be a different user than the re-registered user, so you will already receive the same email. An error will occur if there is a user who has it. Delete the user of the AD FS in CommonServices.
3. You receive the following error in the Common Services login screen.  
   "Login timeout. Please log in again."  
     
   The time difference between Common Services and AD FS hosts exceeds the Allowed clock skew setting.  
   Eliminate time differences between Common Services and AD FS hosts and review the Allowed clock skew settings.
4. The Common Services login screen is returned and no errors are displayed.  
   Or the following error is logged in the AD FS event log of the AD FS server.  
   "Microsoft.IdentityServer.Protocols.Saml.InvalidNameIdPolicyException: MSIS7070: The SAML request contained a NameIDPolicy that was not satisfied by the issued token. "  
     
   For details on how to check the event log in AD FS, See 2.  
     
   Check the settings below to see if there are any problems.  
     
    - NameID policy format for AD FS registered with Common Services.  
    - Transform an Incoming Claim of relying party of AD FS.  
    - Send LDAP Attributes as Claims of relying party of AD FS.  
     
   See the manual "*Setting up a claim issuance policy*" in *Hitachi Ops Center Installation and Configuration Guide*.
5. The Common Services login screen is returned and no errors are displayed.  
   The following error message is displayed in the browser:  
   Unexpected error when authenticating with identity provider  
     
   The following error message is displayed in the AD FS eventlog:  
   MSIS9371: Client credential validation failed for client  
   MSIS9372: Invalid client secret provided  
     
   The following error message is displayed in /var/log/hitachi/CommonService/idp/log/server.log:  
   Failed to make identity provider oauth callback: org.keycloak.broker.provider.IdentityBrokerException: No access\_token from server.  
     
   The Client Secret is incorrect, so correct it to the correct value.
6. The Common Services login screen is returned and no errors are displayed.  
   The following error message is displayed in the browser:  
   Unexpected error when authenticating with identity provider  
     
   The following error message is displayed in the AD FS eventlog:  
   MSIS9329: Received invalid OAuth request. The 'resource' parameter's value does not correspond to any valid registered relying party.  
     
   The following error message is displayed in /var/log/hitachi/CommonService/idp/log/server.log:  
   Failed to make identity provider oauth callback: org.keycloak.storage.ReadOnlyException: Federated storage is not writable   
     
   The Web API Identifier is incorrect, so correct it to the correct value.
7. The Common Services login screen is returned and no errors are displayed.  
   The following error message is displayed in the browser:  
   Unexpected error when authenticating with identity provider  
     
   The following error message is displayed in /var/log/hitachi/CommonService/idp/log/server.log:  
   Failed to make identity provider oauth callback: org.keycloak.storage.ReadOnlyException: Federated storage is not writable  
     
   There may be duplicate emails for local users in Common Services and emails for external IdP users. Check and eliminate any duplicates.

### User directory service (Other) registration fails

Follow the steps below to check if the LDAP server settings are correct.

1. Inventory-Open the edit screen of the LDAP server from the user directory.
2. Execute a connection test to check if the connection is correct.

If an error occurs, resolve the cause and re-execute.

The possible causes of the error are as follows.

- Network misconfiguration between CS and LDAP server, or network failure

- LDAP server machine, OS or LDAP server process failure

1. If the connection test is successful, execute the certification test.

If an error occurs, resolve the cause and re-execute.

The possible causes of the error are as follows.

-The bind DN or bind password is incorrect

-SSL / TLS is not set correctly

-The URL of the LDAP server and the CN or SAN of the LDAP server certificate do not match.

- LDAP server certificate expired

1. If the authentication test is successful, perform a pre-check on the number of users to import.

If an error occurs, resolve the cause and re-execute.

Identify the cause by the error message.

- When KAOP20089-E Invalid ldap search filter or object classes is displayed

User object class or custom user LDAP filter may be invalid

- When KAOP20090-E Invalid SSL / TLS settings. Is displayed

The SSL / TLS settings may be incorrect, or the certificate may have expired.

- When KAOP20091-E Invalid hostname, address, or port number. Is displayed

The host name, IP address, and port number may be incorrect

- When KAOP20092-E Invalid bind DN or bind password. Is displayed

The base DN and password may be incorrect

- When KAOP20093-E Invalid connection URL or user DN. Is displayed

- The base DN is likely to be incorrect

- When KAOP20094-E Invalid URI syntax. Is displayed

Connection URL is likely to be incorrect

- When KAOP20095-E One or more of the supplied parameters is incorrect. Is displayed

Most likely one of the parameters is incorrect

- KAOP10009-W When the number of imported users is 0 is displayed.

There are no users that match the specified conditions (base DN, user object class, search scope, custom user LDAP filter), so review the conditions. Also note that even if the conditions are correct, if the user entry does not have the attribute specified in the LDAP attribute assigned to the user ID, it will not be applicable.

1. If the pre-check of the number of users to import is successful, check the number of imports.

If it is 0, the following parameters may be inappropriate and should be reviewed.

Base DN, custom user LDAP filter, LDAP attributes assigned to user ID

If it is -1, the import limit is exceeded, so narrow down the target users with the custom user LDAP filter.















### Unable to register each Ops Center product in Common Services, or upgrade installation does not proceed with Express installer

If the OS environment variable http\_proxy / https\_proxy is set to a proxy that does not exclude the host name / IP address of the Ops Center Portal, the following symptoms will occur.

* Failed to execute the setupcommonservice command
* When new installation of Common Services is performed by using the Express installer, product registration of each Ops Center product fails.
* When upgrade installation / overwrite installation is performed by using the Express installer, the system requests to enter the administrator credentials indefinitely, and the installation cannot be started.

If this occurs, run the following command before registering the Ops Center products.

|  |
| --- |
| export no\_proxy="127.0.0.1,localhost,*host-name-or-IP-address-of-Portal*" |

### Out of memory occurs

If out of memory occurs, change the Java heap size of Common Services by adding the following properties to *<user-data-directory>*/userconf/config\_user.properties.

|  |
| --- |
| CS\_PORTAL\_MEMORY\_HEAP\_MAX\_SIZE=512m  CS\_IDP\_MEMORY\_HEAP\_MAX\_SIZE=256m |

The above values are the default values. Set a value greater than the above.

### [Hitachi Edition] RemoteOps log Download API is Time Out

If the log download API returns a status code 408 error, Add the following properties to the *<user-data-directory>*/userconf/config\_user.properties.

|  |
| --- |
| CS\_PORTAL\_CSGETRAS\_TIMEOUT=600 |

The above values are the default values.

Set a value greater than the download time (in seconds).

### [Hitachi Edition] If an error occurs in the Common Services RemoteOps, what log should check?

Check the log for each API below.

* <*log-directory*>/debug.log
* <*log-directory*>//error.log

The log download is done with the csgetras command.

Csgetras log is included in the downloaded Compression file.

If the download fails, see /tmp/.common-services/log/csgetras.log.

/tmp/.common-services/log/csgetras.log may not be output if the error is due to insufficient capacity of /tmp.

In this case, the following logs are output to <*log-directory*>/error. log.

|  |
| --- |
| KAOP30012-E ApiException throwing. status = 500 INTERNAL\_SERVER\_ERROR, message = KAOP20061-E An unexpected error occurred. Contact the support center., additionalInfo = csgetras exit code=255. |

### Initializing the truststore password

If you lose your truststore password, you will need to recreate the truststore with the new password, as shown below.

1. If you cannot log in to Hitachi Ops Center, check the following settings  
   Use the following keytool command to check the alias of the certificate imported to the trust store. At this time, a password is required, but the list can be displayed by skipping the input with Enter.

Command:

/opt/hitachi/CommonService/jdk/bin/keytool -list -v -keystore /var/opt/hitachi/CommonService/tls/cacerts | grep -i Alias

Execution example:

|  |
| --- |
| /opt/hitachi/CommonService/jdk/bin/keytool -list -v -keystore /var/opt/hitachi/CommonService/tls/cacerts | grep -i Alias  Enter keystore password:  \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* WARNING WARNING WARNING \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*  \* The integrity of the information stored in your keystore \*  \* has NOT been verified! In order to verify its integrity, \*  \* you must provide your keystore password. \*  \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* WARNING WARNING WARNING \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*  Alias name: opscenterca |

1. Output all alias certificates confirmed in (1) to a file using the following keytool command. At this time, a password is required, but the list can be displayed by skipping the input with Enter.

Command:

/opt/hitachi/CommonService/jdk/bin/keytool -export -alias <alias name> -rfc -keystore /var/opt/hitachi/

CommonService/tls/cacerts -file <output file path>

Execution example:

|  |
| --- |
| /opt/hitachi/CommonService/jdk/bin/keytool -export -alias opscenterca -rfc -keystore /var/opt/hitachi/CommonService/tls/cacerts -file /var/opt/hitachi/CommonService/tls/opscenterca.cer  Enter keystore password:  \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* WARNING WARNING WARNING \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*  \* The integrity of the information stored in your keystore \*  \* has NOT been verified! In order to verify its integrity, \*  \* you must provide your keystore password. \*  \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* WARNING WARNING WARNING \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*  Certificate stored in file </var/opt/hitachi/CommonService/tls/opscenterca.cer> |

1. Back up the current truststore.

|  |
| --- |
| mv /var/opt/hitachi/CommonService/tls/cacerts /var/opt/hitachi/CommonService/tls/cacerts.bk |

1. Create a new trust store by importing the certificate output in (2).

Import all certificates output in (2).When importing the second and subsequent certificates, specify the password that was specified during the initial execution.

Command:

/opt/hitachi/CommonService/jdk/bin/keytool -importcert -alias <alias name> -file <File path output in (2)> -keystore /var/opt/hitachi/CommonService/tls/cacerts -storetype jks

Execution example:

|  |
| --- |
| /opt/hitachi/CommonService/jdk/bin/keytool -importcert -alias opscenterca -file /var/opt/hitachi/Com  monService/tls/opscenterca.cer -keystore /var/opt/hitachi/CommonService/tls/cacerts -storetype jks  Enter keystore password:  Re-enter new password:  (snip)  Trust this certificate? [no]: yes  Certificate was added to keystore |

1. Change truststore permissions.

|  |
| --- |
| chmod 600 /var/opt/hitachi/CommonService/tls/cacerts |

1. Restart the Common Services service.

|  |
| --- |
| systemctl restart csportal |

### When a failure occurs during backup of Common Services by the Protector backup integration function

If a failure occurs when acquiring Common Services backup using the Protector backup integration function and the problem cannot be resolved, please obtain csbackupprescript.log (the log of the csbackupprescript command executed by the function) and contact the help desk.

The log can be collected using the csgetaras command.

### Unable to create a local user due to a user name or email address conflict with an Active Directory server user

For Active Directory server, run the following command by Windows PowerShell on Active Directory server to verify that there are no conflicting username and email address:

|  |
| --- |
| Import-Module ActiveDirectory  Get-ADUser -Filter { SamAccountName -eq "<Username>" } -SearchBase "<Base DN>"  Get-ADUser -Filter { Mail -eq "<Email>" } -SearchBase "<Base DN>" -Properties Mail |

### Unable to create a local user due to a user name or email address conflict with an LDAP server user

For LDAP server, check the following values of LDAP server user specified in user directory to ensure that there are no conflicting usernames and email addresses:

- LDAP attribute for username

- LDAP attribute for email

### Problem occurs when multiple Active Directory servers are linked

Linking between multiple Active Directory servers is not supported.

If you are still operating in conjunction with multiple Active Directory servers,

Make sure that there are no conflicts between username, email address, and user group belong on all servers.

### Problem occurs when multiple LDAP servers are linked

Linking between multiple LDAP servers is not supported.

If you are still operating in conjunction with multiple LDAP servers,

Make sure that there are no conflicts between username and email address belong on all servers.

### User groups button for users imported from LDAP server is not displayed

Occurs when you linking both Active Directory and LDAP server.

Configuring both linking Active Directory server and LDAP server is not supported.

Set only one of them.

### Lost the password for the idpadmin user

Reset the password for the idpadmin user using the following steps.

1. Change the value of the property key CS\_PORTAL\_EMBEDDED\_KEYCLOAK in the following file to "false".

*<user-data-directory>*/userconf/config\_environment.properties

CS\_PORTAL\_EMBEDDED\_KEYCLOAK=false

1. Execute the csembeddedkeycloak command as follows and follow the instructions to reset the password for the idpadmin user.

*<install-directory>*/utility/bin/csembeddedkeycloak -enable

### Failed to log in with the registered ID provider using the Embedded Keycloak.

1. You receive the following error in the Common Services login screen.

"Contact your administrator. Unable to get login user attribute information."

* 1. Log in to the Embedded Keycloak and check the user list.

If the username is empty, you cannot log in with the registered ID provider using the Embedded Keycloak.

There may be an issue with the Mapper settings of the ID provider.If the key specified in the Mapper for the username value is incorrect, the username will be empty.

### TLS connection fails when executing the API.

1. The following error is displayed during a TLS connection.

"The request was aborted: Could not create SSL/TLS secure channel."  
One possible factor is that the source of the connection is not using the signature algorithms supported by Common Services.

* 1. Please check if the Signature algorithm used for communication is included in the Signature algorithms supported by Common Services.

The Signature algorithms supported by Common Services are listed in the release notes.

* 1. If the source ClientOS is Windows Server 2019 or earlier and the source application uses the OS's Signature algorithms(\*), there may be a possibility of TLS communication failure. In such cases, please consider one of the following solutions.

- configure the ECDSA server certificate/private key in Common Services.

See the manual "*Configuring SSL communications*" in *Hitachi Ops Center Installation and Configuration Guide*.

- Use Windows Server 2022 or later as the ClientOS for the connection source.

(\*) If the source application is PowerShell, .NET application, etc., it uses the OS's signature algorithms.

Manual: "Hitachi Ops Center Installation Guide"

## Construction failures

### Failed to install Analyzer with Server Express installer

If the following conditions are met, installation of the prerequisite package may fail when installing Analyzer with Server Express installer.

- OS version is REHL8.4 or earlier.

- The configuration file of yum repository under /etc/yum.repos.d is set to a newer version of AppStream repository than the OS used.

(e.g.: The configuration is set to install podman-3.3.1, which is a prerequisite package when installing Administrator, etc.)

Perform one of the following steps and then run Analyzer installation with Server Express installer.

(A) Delete the AppStream repository settings of the version newer than the OS in use from the yum repository configuration file under /etc/yum.repos.d.

(B) Add the BaseOS repository to the yum repository configuration file under /etc/yum.repos.d. If the installation of the prerequisite package fails, manually update the rpm package for the architecture at the end of the message.

Update method: yum update <package name>.

Example: yum update libstdc++.x86\_64

# Appendices

* 1. Operations that require restarting services

If the following operations are performed for Common Services, you need to restart Common Services (systemctl restart csportal).

- Executing the cschgconnect.sh command

- Executing the csrestore.sh command

- Executing the cssslmycert.sh command

- Setting the server certificate

- Changing the description in *<user-data-directory>*/userconf/config\_user.properties.

* 1. Checking the host name or IP address and port number for the Portal access URL

Open the following file:

*<user-data-directory>*/userconf/config\_environment.properties

Check the values on the right side of the following property keys:

CS\_PORTAL\_GW\_HOSTNAME=*<host-name>*

CS\_PORTAL\_GW\_PORT=*<port number>*

The above properties are used as the access URL information as follows:

https:// <*host-name*>:*<port-number>*/portal

For <*host-name*>, the host name or IP address set during installation or with the cschgconnect command is set. You cannot access the portal screen of Common Services if you do not specify the value of <*host-name*>.

* 1. Downgrading Amazon Corretto 21

As a countermeasure against vulnerabilities, the manual has released the procedure for upgrading Amazon Corretto 21. If a failure occurs due to the upgrade, downgrade Amazon Corretto 21 according to the following procedure.

Note: A downgrading Amazon Corretto 21 to a previous version normally means security strength downgrading to a weaker JDK. It is not suggested to downgrade unless it is really necessary, and you clearly know that Common Services does not support a higher version.

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.

1. Store Amazon Corretto 21 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 Release Notes for Common Services.

Use the following rpm file included in the installation media when downgrading to Amazon Corretto 21.

*root-directory-of-installation-media*/Common/COMSERV/rpm/*amazon-corretto-rpm-file*

1. Stop the Common Services service.

systemctl stop csportal

1. Run the rpm command with the --nopost option and --oldpackage option specified to downgrade Amazon Corretto 21.

rpm -Uvh --nopost --oldpackage *amazon-corretto-rpm-file*

1. Start the Common Services service.

systemctl start csportal

* 1. Operation to disable the service

Use Hitachi Ops Center Analyzer viewpoint OVF without uninstalling Hitachi Ops Center Common Services. If you want to disable the automatic service startup of Hitachi Ops Center Common Services, please follow the steps below.

Note: The automatic service startup of Hitachi Ops Center Common Services will be enabled when upgrade is performed with Hitachi Ops Center Analyzer viewpoint OVF. In this case, perform the operation to disable it again.

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.

1. Disable automatic startup of Common Services and related services

systemctl disable csportal

systemctl disable postgresql-15@csportal

systemctl disable postgresql-15@csidp

1. Stop the Common Services service.

systemctl stop csportal

* 1. How to distinguish Command Control Interface installed with Express installer

It is an explanation of how to distinguish whether it is Command Control Interface (CCI) installed with Express installer.

It is CCI installed with Express installer if it satisfies the following.

* /etc/.hitachi/OpsRM/pkgInfo file exists.
* The value of install.path of the pkgInfo file and the symbolic link destination of /HORCM are the same.
* The value of install.version of the pkgInfo file and the version of CCI that is the symbolic link destination of /HORCM are the same

How to get the version of CCI

Run '/HORCM/usr/bin/raidqry -help' and get it from 'Ver&Rev:' line.

Model : RAID-Manager/Linux/x64

Ver&Rev: 01-68-03/01

:

(Omitted bellow)

Version display format in /etc/.hitachi/OpsRM/pkgInfo

install.version=01680301

install.path=/opt/hitachi/HORCM

The value of install.version in the pkgInfo file is in the form of 'Ver&Rev:' with symbols (- and /) removed.

And then compare if install.version and 'Ver&Rev:' are the same.