Hitachi Ops Center Automator

11.0.4

Installation and Configuration Guide

Ops Center Automator is a software solution that provides the necessary tools to automate and simplify end-to-end processes, such as storage provisioning, for storage and data center administrators. This manual describes how to install and configure Ops Center Automator.

MK-99AUT000-23
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 document describes how to install and configure Hitachi Ops Center Automator.

Product version

This document revision applies to Hitachi Ops Center Automator v11.0.4-00 or later.

Release notes

Read the release notes before installing and using this product. They may contain requirements or restrictions that are not fully described in this document or updates or corrections to this document. Release notes are available on the Hitachi Vantara documentation website: https://docs.hitachivantara.com.

Conventions for storage capacity values

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

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

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

Logical capacity unit	Value
1 block	512 bytes
1 cylinder	Mainframe: 870 KB Open-systems: ▪ OPEN-V: 960 KB ▪ Others: 720 KB
1 KB	1,024 (2^{10}) bytes
1 MB	1,024 KB or $1{,}024^2$ bytes
1 GB	1,024 MB or $1{,}024^3$ bytes
1 TB	1,024 GB or $1{,}024^4$ bytes
1 PB	1,024 TB or $1{,}024^5$ bytes
1 EB	1,024 PB or $1{,}024^6$ bytes

Accessing product documentation

Product user documentation is available on: 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

This module gives an overview of the Ops Center Automator software.

Product overview

Hitachi Ops Center Automator is a software solution that gives 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. These preconfigured templates are customized to your specific environment and processes for creating services that automate complex tasks such as resource provisioning. When configured, Ops Center Automator integrates with existing applications to automate common infrastructure management tasks by utilizing your existing infrastructure services.

Ops Center Automator includes the following features:

- Preconfigured service templates that help in creating automation services
- Automation services for intelligent provisioning of volumes from different storage classes
- Role-based access to defined services
- Performance-based pool selection that chooses the best performing pools from infrastructure groups and gives pool information to each task for specifying the volume usage details
- Common service management attributes that can be assigned and shared across all automation services

About related Hitachi Ops Center products

Ops Center Automator is a part of Hitachi Ops Center, which includes the following components:

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

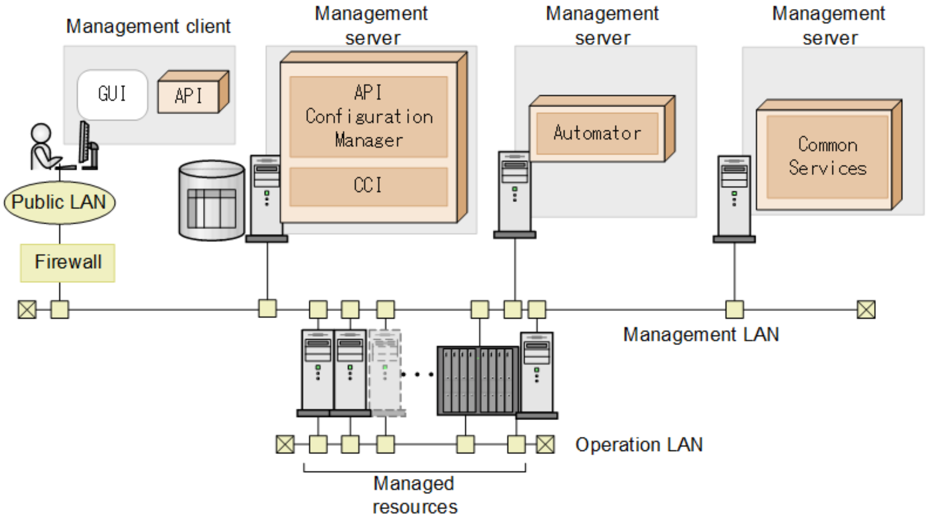
If you install Ops Center Automator along with other Hitachi Ops Center products, you can use common settings to manage users and security.

Ops Center Automator system configuration

The following gives information on the basic Ops Center Automator system configuration.

Configuration when using Ops Center API Configuration Manager

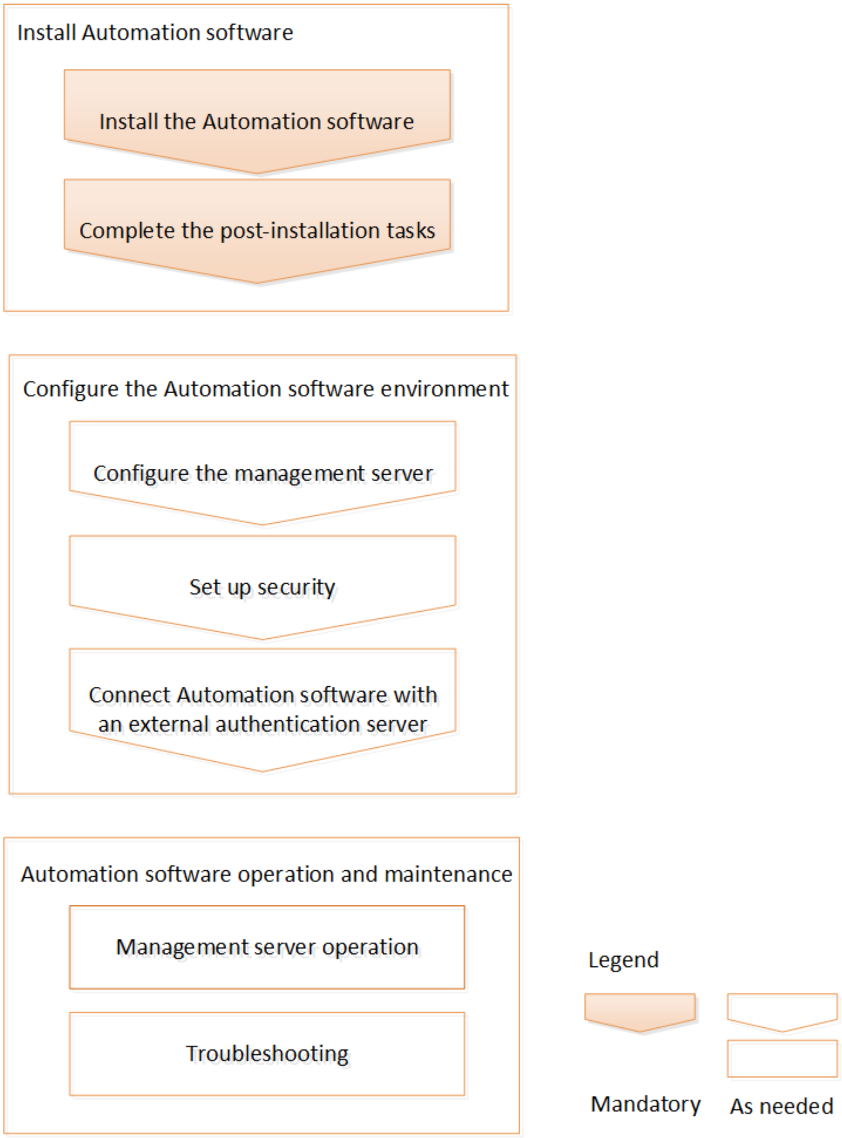
When using Ops Center Automator with Ops Center API Configuration Manager, you can install Ops Center Automator on one server and install Ops Center API Configuration Manager on another server, or you can install Ops Center Automator and Ops Center API Configuration Manager on the same server. The following figure shows the basic system configuration when using Ops Center API Configuration Manager.



Ops Center Automator supports version 10.0.0 or later of Hitachi Ops Center Common Services.

Ops Center Automator installation and configuration workflow

The following figure shows an overview workflow, which includes installing and configuring Ops Center Automator.


Install Automation software
Install the Automation software
Complete the post-installation tasks
Configure the Automation software environment
Configure the management server
Set up security
Connect Automation software with an external authentication server
Automation software operation and maintenance
Management server operation
Troubleshooting
Legend
Mandatory
As needed

This guide includes system installation, setup, management, and maintenance information. For details about using the management UI to create, manage, and automate services, see the *Hitachi Ops Center Automator User Guide*.

Authentication methods in Ops Center Automator

When using Ops Center Automator, you can use the following authentication methods.

Ops Center Common Services

Select this method to use other Ops Center products.

External authentication

Select this method to use external authentication (LDAP authentication, RADIUS authentication, or Kerberos authentication).

Local user authentication

Select this method to use Automator's own user authentication.

Chapter 2: System requirements

This module gives the system requirements for installation.

If you are installing by using the Hitachi Ops Center OVA, see the *Hitachi Ops Center Installation and Configuration Guide*.

System requirements for installing on Windows

The following lists the server requirements for installing on Windows.

Supported operating systems

Note: No functional differences due to differing operating systems exist. Windows supports installations via Remote Desktop/Terminal Client with Console connection session.

OS name	Edition	SP	Architecture
▪ Windows Server 2016 ▪ Windows Server 2019 ▪ Windows Server 2022 **Note:** Server core and Nano Server are not supported.	▪ Standard ▪ Datacenter	No SP	x64

Prerequisite software

Microsoft Visual C++ 2015-2022 Redistributable (x64) is automatically installed during Ops Center Automator installation.

Note: Microsoft Visual C++ 2015-2022 Redistributable (x64) is not automatically removed when you remove Ops Center Automator. Make sure that other programs are not dependent on it, and remove it manually.

IPv6 support

All installations on Windows servers support IPv6.

Note: You must evaluate the Windows version before using it on a cluster or virtualization environment.

System requirements for installing on Linux

The following lists the server requirements for installing on Linux.

Supported operating systems

Note: No functional differences due to differing operating systems exist. Installation via web console is not supported.

Each supported OS includes a list of RPM packages that are required for installing Ops Center Automator. When you install the software, the installation script notifies you if any of the packages are missing. If no RPM packages are missing, the installation proceeds.

Red Hat Enterprise Linux 8.8, 8.10, Oracle Linux 8.8, 8.10

After installing the default OS, the following packages are required:

- alsa-lib (x86_64)
- bash (x86_64)
- bzip2-libs (x86_64)
- chkconfig (x86_64)
- coreutils (x86_64)
- cpio (x86_64)
- cups-libs (x86_64)
- findutils (x86_64)
- fontconfig (x86_64)
- freetype (x86_64)
- gawk (x86_64)
- GConf2 (x86_64)
- gdb (x86_64)
- glib2 (x86_64)
- glibc (i686)
- glibc (x86_64)
- glibc-common (x86_64)
- glibc-devel (i686)
- glibc-devel (x86_64)
- glibc-headers (x86_64)

- glibc-utils (x86_64)
- grep (x86_64)
- gtk2 (x86_64)
- gtk3 (x86_64)
- gzip (x86_64)
- krb5-libs (x86_64)
- ksh (x86_64)
- libgcc (i686)
- libgcc (x86_64)
- libpng (x86_64)
- libstdc++ (i686)
- libstdc++ (x86_64)
- libX11 (x86_64)
- libXau (x86_64)
- libxcb (x86_64)
- libxcrypt (x86_64)
- libXext (x86_64)
- libXi (x86_64)
- libXrender (x86_64)
- libXtst (x86_64)
- lksctp-tools (x86_64)
- ncompress (x86_64)
- ncurses (x86_64)
- net-tools (x86_64)
- nscd (x86_64)
- nss (x86_64)
- pcsc-lite-libs (x86_64)
- procps-ng (x86_64)
- rpm (x86_64)
- sed (x86_64)
- sysstat (x86_64)
- tar (x86_64)
- tcsh (x86_64)
- which (x86_64)
- zlib (x86_64)

- iproute (x86_64)
- libnsl (x86_64)
- libselinux-utils (x86_64)
- policycoreutils-python-utils (noarch)
- policycoreutils (x86_64)
- glibc-langpack-en (x86_64)
- hostname (x86_64)
- perl (x86_64)

Red Hat Enterprise Linux 9.2, 9.4, Oracle Linux 9.2, 9.4

After installing the default OS, the following packages are required:

- alsa-lib (x86_64)
- bash (x86_64)
- bzip2-libs (x86_64)
- chkconfig (x86_64)
- coreutils (x86_64)
- cpio (x86_64)
- cups-libs (x86_64)
- findutils (x86_64)
- fontconfig (x86_64)
- freetype (x86_64)
- gawk (x86_64)
- gdb (x86_64)
- glib2 (x86_64)
- glibc (i686)
- glibc (x86_64)
- glibc-common (x86_64)
- glibc-devel (i686)
- glibc-devel (x86_64)
- glibc-headers (x86_64)
- glibc-utils (x86_64)
- graphite2 (x86_64)
- grep (x86_64)
- gtk2 (x86_64)
- gtk3 (x86_64)

- gzip (x86_64)
- harfbuzz (x86_64)
- krb5-libs (x86_64)
- ksh (x86_64)
- libbrotli (x86_64)
- libgcc (i686)
- libgcc (x86_64)
- libpng (x86_64)
- libstdc++ (i686)
- libstdc++ (x86_64)
- libX11 (x86_64)
- libXau (x86_64)
- libxcb (x86_64)
- libxcrypt (x86_64)
- libXext (x86_64)
- libXi (x86_64)
- libXrender (x86_64)
- libXtst (x86_64)
- lksctp-tools (x86_64)
- ncurses (x86_64)
- net-tools (x86_64)
- nscd (x86_64)
- nss (x86_64)
- pcre (x86_64)
- pcsc-lite-libs (x86_64)
- procps-ng (x86_64)
- rpm (x86_64)
- sed (x86_64)
- sysstat (x86_64)
- tar (x86_64)
- tcsh (x86_64)
- which (x86_64)
- zlib (x86_64)
- iproute (x86_64)
- libnsl (x86_64)

- libselinux-utils (x86_64)
- policycoreutils-python-utils (noarch)
- policycoreutils (x86_64)
- glibc-langpack-en (x86_64)
- hostname (x86_64)
- perl (x86_64)

Prerequisite software

None.

Kernel parameters and shell restrictions

In Linux, you must set the following kernel parameter and shell restriction values:

File*	Parameter	Value to be set

`/etc/sysctl.conf`	`fs.file-max`
	`kernel.threads-max`
	`kernel.msgmni`
	`kernel.sem` (4th and 2nd parameter)
	`kernel.shmmax`
	`kernel.shmmni`
	`kernel.shmall`
		See "Kernel parameter and shell restriction details" below.

`/etc/security/limits.conf`	`soft nofile`
	`hard nofile`
		See "Kernel parameter and shell restriction details" below.

`/etc/security/limits.d/20-nproc.conf`	`soft noproc`
	`hard noproc`
		See "Kernel parameter and shell restriction details" below.

`/etc/systemd/system.conf`	`DefaultLimitNOFILE`	Specify the same value as `nofile` in `limits.conf`.
`/etc/systemd/system.conf`	`DefaultLimitNPROC`	Specify the same value as `nproc` in `20-nproc.conf`.
* The file path differs according to the environment. In addition, note that kernel parameters and shell restrictions can also be set for files that are not listed here.		

Kernel parameter and shell restriction details

Table 1 Red Hat Enterprise Linux and Oracle Linux version 8.x and 9.x

Parameters		Value for Ops Center Automator
kernel parameters (`/etc/sysctl.conf`)	fs.file-max	175,660
	kernel.threads-max	757
	kernel.msgmni	97
	4th parameter of kernel.sem	1,244
	2nd parameter of kernel.sem	8,726
	kernel.shmmax	262,620,570
	kernel.shmmni	2,400
	kernel.shmall	224,129,511
shell restrictions (`/etc/security/limits.conf`)	nofile (soft / hard)	2,450
shell restrictions (`/etc/security/limits.d/20-nproc.conf`)	nproc (soft /hard)	1,596

Values for /etc/sysctl.conf

For kernel.shmmax:

```
kernel-parameter-value-to-be-set =
Max{
    Max{
        value-that-is-enabled-in-the-system
        ,
        initial-value-of-the-OS
    }
    ,
    value-for-Automator
}
```

Other kernel parameters

```
kernel-parameter-value-to-be-set =
Max{
    value-that-is-enabled-in-the-system
    ,
    initial-value-of-the-OS
}
```

```
+ value-for-Automator
```

Note: Max{x, y, z} indicates the maximum value among x, y, and z.

Values for /etc/security/limits.conf

The following formula is for calculating the values for the shell restriction:

```
shell-restrictions-value-to-be-set =
Max{
    Max{
        value-that-is-enabled-in-the-system
        ,
        initial-value-of-the-OS
    }
    + value-for-Automator
    ,
    8192
}
```

Note: Max{x, y, z} indicates the maximum value among x, y, and z.

Values for /etc/security/limits.d/20-nproc.conf

The following formula is for calculating the values for the shell restriction:

```
shell-restrictions-value-to-be-set =
Max{
    value-that-is-enabled-in-the-system
    ,
    initial-value-of-the-OS
}
+ value-for-Automator
```

Note: Max{x, y, z} indicates the maximum value among x, y, and z.

IPv6 support

All installations on Linux servers support IPv6.

Note: You must evaluate the Linux version before using it in a virtualization environment.

Hardware and disk space requirements

The hardware and disk space requirements for the management server are as follows:

Hardware

Note: Resource shortages might occur if the system scale changes during operation and hardware resources become inconsistent with the system scale. It is recommended that the number of resources be checked periodically so that any inconsistency can be detected.

		Ops Center Automator	
Item		Standard mode	High performance mode
CPU		(Minimum) Dual-core processor (Suggested) Quad-core processor or better	8-core processor or better
Physical memory		(Minimum) 4 GB (Suggested) 10 GB or higher	16 GB or higher
Disk	Free space required for use	(Minimum) 3000 MB*	
		(Suggested) 30 GB or higher	
	Ops Center Automator installation folder	4100 MB	
	Database space required for use	3000 MB	
*: ▪ Average size of service template: 2 MB ▪ The number of service templates: 500 ▪ Average size of task log: 1 MB ▪ The number of tasks: 2000 ▪ Total size: 3 GB (2 MB * 500 + 1 MB * 2000)			

Hitachi Ops Center products cannot be installed on a disk that has a logical sector size of 4,096 bytes (4K native). If a disk that has a logical sector size of 4,096 bytes is used, change the logical sector size to 512 bytes, and then install.

Table 2 Disk space required for installation (Windows)

Component folder	Default installation folder	Ops Center Automator
Ops Center Automator installation folder	*Program-Files-folder*\hitachi	4100 MB
Ops Center Automator database storage folder	*Program-Files-folder*\hitachi \database\Automation	3000 MB

Table 3 Disk space required for installation (Linux)

Component directory	Default installation directory	Ops Center Automator
Ops Center Automator installation directory	/opt/hitachi	2440 MB
	/var/opt/hitachi	1660 MB
Ops Center Automator database storage directory	/var/opt/hitachi/database/x64/ Automation	3000 MB

Virtual memory requirements

For management server stability, you must allocate virtual memory capacity for products and for the operating system and other programs. If insufficient virtual memory is allocated on the management server, Common Component products and other installed programs can become unstable or might not start. For the management server, allocate the total virtual memory capacity of Common Component plus the sum of the virtual memory capacities of all the installed Common Component products.

The following are the suggested amounts of virtual memories for each component:

- Common Component: 2501 MB
- Ops Center Automator: 11 GB

Port requirements

Before you install the Ops Center Automator server, review the port and firewall requirements.

Table 4 Common Component reception ports

Port number	Description	Register firewall exception	Originator	
22015/tcp	Used for accessing the HBase 64 Storage Mgmt Web Service when communicating with management clients (GUI). This port number can be changed. This port is also used when SSL is enabled. To interrupt non-SSL communication from outside the network to the management server, edit the `user_httpsd.conf` file.	Yes	Client	Ops Center Automator server
22016/tcp	Used for accessing the HBase 64 Storage Mgmt Web Service when performing SSL communication with management clients (GUI). This port number can be changed.	Yes	Client	Ops Center Automator server
22017/tcp to 22030/tcp 22033/tcp 22034/tcp	Reserved for Common Component.	No	-	-
22032/tcp	Used internally for Common Component communication (HiRDB). This port number can be changed.	No	-	-
22035/tcp	Used internally for Common Component communication (communication with the Web server).	No	-	-

Port number	Description	Register firewall exception	Originator	
22036/tcp	Used internally for Common Component communication (HiRDB). This port number can be changed.	No	-	-
22037/tcp	Used internally for Common Component communication (communication with the Web server). This port number can be changed.	No	-	-
22038/tcp	Used internally for Common Component communication (communication with the Web server). This port number can be changed.	No	-	-
22121/tcp	Used internally for Common Component communication (communication with the Web server). This port number can be changed.	No	-	-
22122/tcp	Used internally for Common Component communication (naming service). This port number can be changed.	No		
22123/tcp 22124/tcp 22125/tcp	Used internally for Common Component communication (communication with the Web server). This port number can be changed.	No	-	-
22126/tcp	Used internally for Common Component communication (naming service). This port number can be changed.	No	-	-

Port number	Description	Register firewall exception	Originator	
22127/tcp 22128/tcp	Used internally for Common Component communication (communication with the Web server). This port number can be changed.	No	-	-

Table 5 Ops Center Automator ports

Port number	Description	Register firewall exception	Originator	
22170/tcp	Used internally for Common Component communication (communication with the Web server).	No	-	-
22171/tcp	Used internally for Common Component communication (naming service). This port number can be changed.	No	-	-
22172/tcp	Used internally for Common Component communication (communication with the Web server). This port number can be changed.	No	-	-
22173/tcp	Used internally for Common Component communication (communication with the Web server). This port number can be changed.	No	-	-

Table 6 Reception ports of virtualization server

Type	Port number	Description	Register firewall exception	Originator	
VMware ESXi	443/tcp	This setting is required when a virtual WWN is assigned to a virtual machine by using NPIV.	Yes	Management server	Ops Center Automator
VMware vCenter Server that manages VMware ESXi	443/tcp	This setting is required when a virtual WWN is assigned to a virtual machine by using NPIV.	Yes	Management server	Ops Center Automator

Table 7 Reception ports of operation targets (servers)

Port number	Description	Register firewall exception	Originator	
22/tcp	Used for SSH. cjstartsv uses this port.	Yes	Management server	Ops Center Automator
23/tcp	Used for Telnet. cjstartsv uses this port.	Yes	Management server	Ops Center Automator
445/tcp or udp	Used for Windows administrative shares. cjstartsv uses this port.	Yes	Management server	Ops Center Automator
135/tcp and 139/tcp	Used for Windows administrative shares. cjstartsv uses this port.	Yes	Management server	Ops Center Automator

Table 8 Reception ports of mail servers

Port number	Description	Register firewall exception	Originator	
25/tcp	Used for mail transmission. This port number can be changed. cjstartsv uses this port.	Yes	Management server	Ops Center Automator

Table 9 Reception ports of external authentication servers

Port number	Description	Register firewall exception	Originator	
88/tcp	Used for communication with the management server and Kerberos server. This port number is generally used. However, a different port number might be used for an external authentication server.	Yes	Management server	Ops Center Automator
88/udp	Used for communication with the management server and Kerberos server. This port number is generally used. However, a different port number might be used for an external authentication server.	Yes	Management server	Ops Center Automator

Port number	Description	Register firewall exception	Originator	
389/tcp	Used for communication with the management server and LDAP directory server. This port number is generally used. However, a different port number might be used for an external authentication server.	Yes	Management server	Ops Center Automator
1812/udp	Used for communication with the management server and RADIUS server. This port number is generally used. However, a different port number might be used for an external authentication server.	Yes	Management server	Ops Center Automator

Maximum resource support

Maximum resource support

This section lists the maximum number of resources that Ops Center Automator can manage. Best practice is not to exceed these limits.

- Number of the controllable tasks: 5,000
- Number of service templates: 1,000
- Number of controllable Agentless Remote Connections: 10,000

Web client requirements

The following browsers are supported:

Table 10 Supported browsers

Web browser/other	Version
Firefox	ESR 128
Microsoft Edge	Latest version of stable channel
Chrome Browser for enterprise	Latest version of stable channel

Table 11 IPv6

OS	OS Name	Ops Center Automator
Windows	▪ Windows Server 2016 ▪ Windows Server 2019 ▪ Windows Server 2022	Supported *
Linux	▪ Red Hat Enterprise Linux ▪ Oracle Linux	Supported *
* Evaluation is needed before using this version in a cluster environment or in a virtualization environment.		

Virtualization and cluster support

Virtualization software

All Windows and Linux server installations support the following versions of VMware ESXi:

- 7.0, 7.0u1, 7.0u2, 7.0u3
- 8.0, 8.0u1, 8.0u2, 8.0u3

The following Windows and Linux installations support the following versions of Hyper-V:

OS Name	OS Version	Virtualization Version
Windows Server 2016	▪ Standard Edition ▪ Datacenter Edition	Windows Server 2016 Hyper-V
		Windows Server 2019 Hyper-V
Windows Server 2019	▪ Standard Edition ▪ Datacenter Edition	Windows Server 2016 Hyper-V
		Windows Server 2019 Hyper-V
Windows Server 2022	▪ Standard Edition ▪ Datacenter Edition	Windows Server 2016 Hyper-V
		Windows Server 2019 Hyper-V

OS Name	OS Version	Virtualization Version
Red Hat Enterprise Linux	9.4	Windows Server 2022 Hyper-V
Oracle Linux	9.4	Windows Server 2022 Hyper-V

Cluster software

All Windows server installations support WSFC cluster (Bundle version).

Management target requirements

Storage System	Interface (Interface between the host and storage subsystem)	Ops Center Automator
VSP One B24, B26, B28	Fibre Channel	All versions are supported
	iSCSI	
VSP 5200, 5600, 5200H, 5600H	Fibre Channel	All versions are supported
	iSCSI	
VSP 5100, 5500, 5100H, 5500H	Fibre Channel	90-01-42-00/xx or later
	iSCSI	90-01-42-00/xx or later
VSP G1000	Fibre Channel	80-01-21-00/00 or later
	iSCSI	80-02-01-XX/XX or later
VSP G1500	Fibre Channel	80-05-0X-XX/XX or later
	iSCSI	80-05-0X-XX/XX or later
VSP G200, G400, G600, G800	Fibre Channel	All versions are supported
	iSCSI	All versions are supported
VSP G350, G370, G700, G900	Fibre Channel	All versions are supported
	iSCSI	All versions are supported
VSP F1500	Fibre Channel	All versions are supported
	iSCSI	All versions are supported
VSP F400, F600, F800	Fibre Channel	All versions are supported

Storage System	Interface (Interface between the host and storage subsystem)	Ops Center Automator
	iSCSI	All versions are supported
VSP F350, F370, F700, F900	Fibre Channel	All versions are supported
	iSCSI	All versions are supported
VSP N400, N600, N800	Fibre Channel	All versions are supported
	iSCSI	All versions are supported
VSP E1090, E1090H	Fibre Channel	All versions are supported
	iSCSI	All versions are supported
VSP E590, E790, E990, E590H, E790H	Fibre Channel	All versions are supported
	iSCSI	All versions are supported

Chapter 3: Installing and upgrading Ops Center Automator

This module describes how to install and upgrade Ops Center Automator for Microsoft® Windows® OS in both cluster and non-cluster environments and Red Hat Enterprise Linux (RHEL)/Oracle Linux OS in a non-cluster environment.

You can also install the Automator using the Hitachi Ops Center consolidated OVA or the Express installers. For details, see the backupsystem command (on page 217).

Note: The following elements cannot be carrried over or have been changed for Ops Center Automator v10.8.0 or later:

- The SSLProtocol and SSLCipherSuite parameters in `user_httpsd.conf` cannot be carried over.
- The **`hcmds64chgjdk`** command to switch to Oracle JDK is no longer supported when you upgrade, the existing JDK will be replaced with the Hitachi JDK.
- The internal port number of `webserver.connector.ajp13.port` will not be carried over if it has been changed.

Note: If you are upgrading, you can skip the steps in Post-installation tasks (on page 45) and Configuring single sign-on in Common Services (on page 49) because the previous settings are preserved.

Installation prerequisites

Before installing Ops Center Automator complete the following tasks:

- Verify that the environment and the management server meet all hardware and software requirements. For details on the system requirements, see Chapter 2: System requirements (on page 15).
- Ensure the ports used by Ops Center Automator are available. Verify that the ports on the management server are not in use by other products and no conflicts exist. If a port is in use by another product, neither product may operate correctly.
- Resolve the IP addresses and host names of the related machines.
- Disable any security monitoring, virus detection, or process monitoring software on the server.
- If the server is running any other Common Component products, stop the services for those products.

- Make sure the server system time is correct. If the Common Component products and Ops Center products are installed on a different server, synchronize the management servers running the Common Component products and Ops Center products.
- Verify that the management server host name is 128 characters or less.

When installing Ops Center Automator on a Windows server, also complete the following tasks:

- Ensure Windows Administrator permissions are obtained to complete the installation and configuration tasks included in this guide.
- Close any Windows Services or open command prompts.

When installing Ops Center Automator on a Linux server, also complete the following tasks:

- Ensure Linux root permissions are obtained to complete the installation and configuration tasks included in this guide.
- Manually re-add firewall exceptions as needed for Ops Center Automator. These exceptions do not automatically get configured during installation.

Changing the server time

The Ops Center Automator task and alert occurrence times are based on the management server time setting. Therefore, it is important that you verify the accuracy of the server OS time setting and reset it if necessary before installing Ops Center Automator. If you change the Ops Center Automator server time while the Common Component and Common Component product services are running, Ops Center Automator might not operate correctly.

Important: The Ops Center Automator server OS time setting must synchronized with the management servers running Common Component products and Ops Center products.

Note: When Common Services and Automator are running on different hosts, launching Automator from the Ops Center portal fails if there is a time lag of more than three minutes between the host where Common Services is installed and the host where Automator is installed. You must synchronize the time on the Common Services host with the time on the Automator host. Use NTP to keep the time synchronized between the hosts.

If you plan to use a service such as NTP, which automatically adjusts the server time, you must configure the service as follows:

- Configure the settings so that the time is adjusted when the service discovers a time discrepancy.
- The service adjusts the time setting only as long as the time difference remains within a specific range. Based on the maximum range value, set the frequency so that the time difference never exceeds the fixed range.

An example of a service that can adjust the time as long as the time difference does not exceed a fixed range is the Windows Time service.

Note: When running Ops Center Automator in a U.S. or Canadian time zone, you must configure the management server OS so that it supports the new Daylight Savings Time (DST) rules. Ops Center Automator cannot support the new DST rules unless the server gives support.

If you cannot use the functionality that adjusts the server time automatically, or to manually change the system time, perform these steps:

1. Stop the Common Component and all Common Component product services, for example:
   - HBase 64 Storage Mgmt Web Service
   - HBase 64 Storage Mgmt Web SSO Service
   - HBase 64 Storage Mgmt SSO Service
   - HBase 64 Storage Mgmt Common Service
   - HCS Device Manager Web Service
   - HiCommand Suite Tuning Manager
   - HiCommand Performance Reporter
   - HCS Tuning Manager REST Application Service
   - HAutomation Engine Web Service
   - HiCommand Server
   - HiCommand Tiered Storage Manager
2. Record the current time of the management server, and then reset the time.
3. Determine when to restart the services.
   - If you set the time of the machine back (meaning that the server time was ahead), wait until the server clock shows the time you recorded (the time on the server when you made the change) and then restart the machine.
   - If you set the machine time forward, restart the machine now.

Verify that the Ops Center Automator management server reflects the correct time.

Changing the name resolution setting

If you install Ops Center Automator and the Common Component product on two different machines, you must resolve the name of the Ops Center Automator server that connects to the client.

You must also resolve the name of the machine where Ops Center Automator is installed.

If you install Ops Center Automator on the same machine as the Common Component product, you must resolve the names of the machine on which you want to run the browser to access Ops Center Automator.

Update your configuration settings so that the system can resolve the IP address from the management server host name that is set as the `ServerName` property on the first line of the `user_httpsd.conf` file. To verify that the IP address resolves to the host name, run the following command:

```
ping management-server-host-name
```

Avoiding port conflicts

Before a new installation of Ops Center Automator, verify that the ports that Ops Center Automator will use on the management server are not in use by other products. If a port is being used by another product, neither product might operate correctly.

To ensure that the necessary ports are not in use, use the **netstat** or **ss** command.

You must verify that port numbers 22170 - 22173 are not used by other products because this causes a new or upgrade installation to fail.

Installing and upgrading Ops Center Automator (Windows OS)

You use the product installer to install or upgrade the Ops Center Automator software.

If you are upgrading your software, ensure that you back up the existing system configuration and data using the **backupsystem** command. For details, see the backupsystem command (on page 217).

Procedure

1. Ensure that your system meets all management server prerequisites as listed in the pre-installation checklist.
2. If the server is running any products that use the Common Component, stop the following services:
   - HBase 64 Storage Mgmt Web Service
   - HBase 64 Storage Mgmt Web SSO Service
   - HBase 64 Storage Mgmt SSO Service
   - HBase 64 Storage Mgmt Common Service
   - HCS Device Manager Web Service
   - HiCommand Suite Tuning Manager
   - HiCommand Performance Reporter
   - HCS Tuning Manager REST Application Service
   - HAutomation Engine Web Service
   - HiCommand Server
   - HiCommand Tiered Storage Manager
3. Access the installation media.
4. Start the installation wizard by running the following command:

   ```
   Installation-media:\Windows\HAD_SERVER\setup.exe
   ```

5. Follow the prompts and specify the required information.

   In most cases, accept the default installation selections.

   Note: You cannot specify a folder mounted on a drive or network file system as the installation folder of Ops Center Automator for Windows.

   Note: If the following message is displayed, check the release notes:

   ```
   An Analyzer server prior to 10.7.0, Hitachi Ops Center Automator
   prior to 10.8.0, or Hitachi Command Suite prior to 8.8.3 is already
   installed on this server. Make sure to upgrade the relevant products
   by referring to the Release Notes. Abort the installation?
   ```

   The **Install Complete** window opens.

6. Click **Finish**.

Result

Ops Center Automator is now installed.

Note: If you are upgrading, you can skip the steps in Post-installation tasks (on page 45) and Configuring single sign-on in Common Services (on page 49) because the previous settings are preserved.

Installing and upgrading Ops Center Automator in a cluster environment (Windows OS)

You can install or upgrade Ops Center Automator in a Windows cluster environment.

Note: Ops Center Automator supports Windows cluster environments only. Ops Center Automator does not support clustering in a Linux OS environment.

Note: If you are upgrading, you can skip the steps in Post-installation tasks (on page 45) and Configuring single sign-on in Common Services (on page 49) because the previous settings are preserved.

About using Ops Center Automator in a cluster environment

When using Ops Center Automator, you can increase reliability by setting up a failover management server using Microsoft Windows Server Failover Clustering.

Note: Ops Center Automator does not support installing in a cluster that spans multiple subnets.

When you use Ops Center Automator in a cluster environment, you designate one Ops Center Automator server as the active node and another as the standby node as follows:

- Active node

  The active node is the host that is running services in a system that uses a cluster.

  If a failure occurs, the cluster services implements a failover, and the standby node takes over running the system resources so that there is no interruption of services.

- Standby node

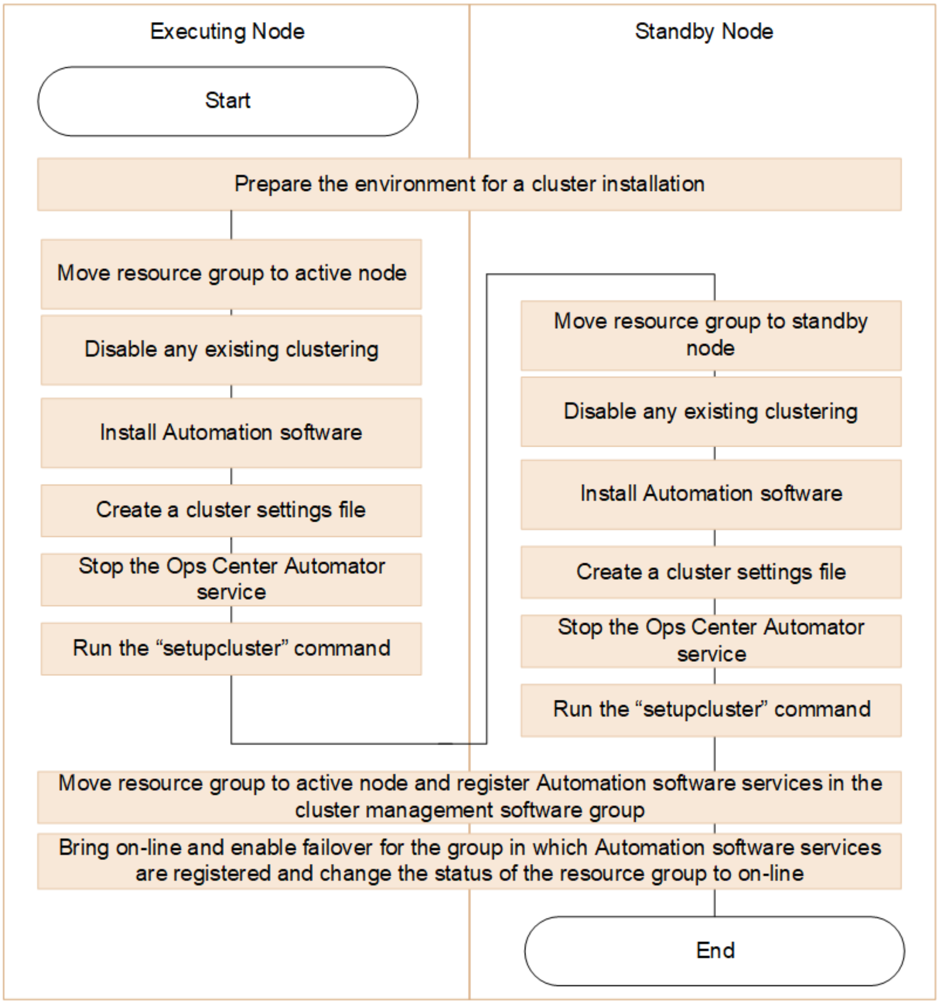
  The standby node is the host that takes over running system resources from the active node if a failure occurs.

Note: If an active node fails over to the standby node, any tasks that are running fail and you must run the tasks again on the standby node.

Cluster installation workflow

When installing Ops Center Automator in a cluster configuration, you must follow a series of steps to prepare both the active node and the standby nodes.

The following shows the general workflow for setting a up cluster environment:


Executing Node
Standby Node
Start
Prepare the environment for a cluster installation
Move resource group to active node
Disable any existing clustering
Install Automation software
Create a cluster settings file
Stop the Ops Center Automator service
Run the "setupcluster" command
Move resource group to standby node
Disable any existing clustering
Install Automation software
Create a cluster settings file
Stop the Ops Center Automator service
Run the "setupcluster" command
Move resource group to active node and register Automation software services in the cluster management software group
Bring on-line and enable failover for the group in which Automation software services are registered and change the status of the resource group to on-line
End

When installing Ops Center Automator to a cluster environment for the first time, make sure that every node in the cluster has the same disk configuration, and all Common Component products are installed in the same location (including drive letter, path, and so on) on each node.

If you are upgrading your software, ensure that you back up the existing system configuration and data using the `backupsystem` command (on page 217).

Note: When upgrading Ops Center Automator that is already installed in a cluster configuration, you must disable the resource script before running the upgrade installation.

Verifying the cluster configuration using the cluster management software

When setting up Ops Center Automator in a cluster environment, you must use the cluster management software to verify the current environment settings and to configure additional settings.

Use the cluster management software to verify the following items before setting up Ops Center Automator in a cluster environment:

- Verify whether a group exists in which other Common Component product services are registered.

  If a group in which Common Component services are registered already exists, use that group. Verify that the group consists only of resources related to Common Component products.

  If no group in which Common Component services are registered exists, use the cluster management software to create a group to register the Ops Center Automator service.

  Note: Group names cannot contain the following characters: ! " % &) * ^ | ; = , < >

- Verify that the group in which you plan to register services includes the shared disk and client access point that can be inherited between the active and standby nodes. The client access point is the cluster management IP address and the logical host name.
- Verify that you can allocate, delete, and monitor resources by using the cluster management software without any problems.

Services that are used in a cluster environment can be failed over together by registering them as a group in the cluster management software. These groups might be referred to by different names, such as "resource groups" or "roles," depending on the versions of the cluster management software and the OS.

Setting up Ops Center Automator clustering on an active node

You can complete a new installation of Ops Center Automator on the management server on an active node in a cluster configuration.

Procedure

1. Bring online the cluster management IP address and shared disk. Make sure that the resource group for the cluster installation is moved to the active node.
2. If you created the cluster environment using another Common Component product, use the following command to take offline and disable failover for the cluster group in which Common Component product services are registered:

   ```
   Common-Component-installation-directory\ClusterSetup
   \hcmds64clustersrvstate /soff /r cluster-group-name
   ```

   where

   `r` - specifies the name of the group in which the Common Component product services are registered. If the group name contains spaces, you must enclose the group name in quotation marks ("). For example, if the group name is Automator cluster, specify "Automator cluster".

3. Complete a new installation of Ops Center Automator on the active node.

   If other Common Component products already exist and are active in the cluster environment, specify the logical host name (the virtual host name allocated to the cluster management IP address) as the **IP Address or Host Name** of the management server. If there are no other Common Component products in the cluster environment, specify the IP address or the host name of the active node as the **IP Address or Host Name** of the management server.

4. Register the licenses for the products you plan to use.
5. If you already have a Common Component product configured in the cluster, skip to the next step. If Ops Center Automator is the first Common Component product in the cluster, do the following:
   a. Add the following information to a blank text file:

   ```
   mode=online
   virtualhost=logical-host-name
   onlinehost=active-node-host-name
   standbyhost=standby-node-host-name
   ```

   > **Note:** On an active node, you must specify `online` for `mode`.

   Save the file as `cluster.conf` in *`Common-Component-installation-folder`*`\conf`.

6. Use the following command to ensure that the Ops Center Automator service is stopped:

   ```
   Common-Component-installation-folder\bin\hcmds64srv /stop /server
   AutomationWebService
   ```

7. Run the **`setupcluster /exportpath`** command where the `exportpath` specifies the absolute or relative path of the folder on a shared disk. For the `exportpath`, the folder directly under the shared disk (`root` folder) cannot be specified.

Setting up Ops Center Automator clustering on a standby node

After setting up the clustering installation on an active node, you can complete installation of Ops Center Automator on the management server on a standby node in a cluster configuration.

Procedure

1. In the cluster management software, move the group containing the Ops Center Automator resources to the standby node by right-clicking the group, selecting **Move**, and then selecting either **Select Node** or **Move this service or application to another node**.
2. If you created the cluster environment using another Common Component product, use the following command to take offline and disable failover for the cluster group in which Common Component product services are registered:

   ```
   Common-Component-installation-directory\ClusterSetup
   \hcmds64clustersrvstate /soff /r cluster-group-name
   ```

   where

   `r` - specifies the name of the group in which the Common Component product services are registered. If the group name contains spaces, you must enclose the group name in quotation marks ("). For example, if the group name is Automator cluster, specify "Automator cluster".
3. Complete a new installation of Ops Center Automator on the standby node.

   Before installing Ops Center Automator on the standby node, be aware of the following requirements:

   - You must install Ops Center Automator in the same location as on the active node.
   - If other Common Component products already exist and are active in the cluster environment, specify the logical host name (the virtual host name allocated to the cluster management IP address) as the **IP Address or Host Name** of the management server. If there are no other Common Component products in the cluster environment, specify the IP address or the host name of the standby node as the **IP Address or Host Name** of the management server.
4. Register the licenses for the products you plan to use.
5. If you already have a Common Component product configured within the cluster, skip to the next step. If Ops Center Automator is the first Common Component product in the cluster, add the following information to a blank text file:

   ```
   mode=standby
   virtualhost=logical-host-name
   onlinehost=active-node-host-name
   standbyhost=standby-node-host-name
   ```

   Save the file as `cluster.conf` in *`Common-Component-installation-folder`*`\conf`.

   > **Note:** On a standby node, you must specify `standby` for `mode`.

6. Use the following command to ensure that the Ops Center Automator service is stopped:

   ```
   hcmds64srv /stop /server AutomationWebService
   ```

7. Run the **`setupcluster /exportpath`** command where the `exportpath` is the same path specified in step 7 of Setting up Ops Center Automator clustering on an active node (on page 40).

Registering the services and initializing the cluster installation

After installing Ops Center Automator on the active and standby nodes in a cluster configuration, you can register the services and scripts and then bring the clustering online as described in the following steps:

Procedure

1. In the cluster management software, move the group containing the Ops Center Automator resources to the active node by right-clicking the group, selecting **Move**, and then selecting either **Select Node** or **Move this service or application to another node**.
2. Register the Ops Center Automator service in the cluster management software group by using the following command:

   ```
   Common-Component-installation-directory\ClusterSetup
   \hcmds64clustersrvupdate /sreg /r cluster-group-name /sd drive-
   letter-of-shared-disk /ap resource-name-for-client-access-point
   ```

   where

   `r` - specifies the name of the group in which the Common Component product services including Ops Center Automator will be registered. If the group name contains spaces, you must enclose the group name in quotation marks ("). For example, if the group name is Automator cluster, specify "Automator cluster".

   `sd` - specifies the drive letter of the shared disk that is registered to the cluster management software. You cannot specify multiple drive letters for this option. If the database of Common Component products is divided into multiple shared disks, run the `hcmds64clustersrvupdate` command for each shared disk.

   `ap` - specifies the name of the resource for the client access point that is registered to the cluster management software.

3. On the active node, bring online and enable failover for the group in which Common Component services including Ops Center Automator are registered using the following command:

   ```
   Common-Component-installation-folder\ClusterSetup
   \hcmds64clustersrvstate /son /r cluster-group-name
   ```

   where

   `r` - specifies the name of the group in which the Common Component product services including Ops Center Automator are registered. If the group name contains spaces, you must enclose the group name in quotation marks ("). For example, if the group name is Automator cluster, specify "Automator cluster".

4. Change the status of the resource group to **online** in the cluster software.

Installing and upgrading Ops Center Automator (Linux OS)

You use the product installer to install or upgrade the Ops Center Automator software.

If you are upgrading your software, ensure that you back up the existing system configuration and data using the **`backupsystem`** command (on page 217).

Note: To install Ops Center Automator with other Common Component products, ensure that your system meets the installation requirements for all the products.

Install Ops Center Automator by running `install.sh`.

Note: If the following message is displayed, check the release notes:

```
An Analyzer server prior to 10.7.0, Hitachi Ops Center Automator prior to
10.8.0, or Hitachi Command Suite prior to 8.8.3 is already installed on
this server. Make sure to upgrade the relevant products by referring to
the Release Notes. Abort the installation?
```

The default Ops Center Automator installation directory for Linux OS is: `/opt/hitachi/Automation`

Note: If you are upgrading, you can skip the steps in Post-installation tasks (on page 45) and Configuring single sign-on in Common Services (on page 49) because the previous settings are preserved.

Required settings when using a virus detection program or process monitoring program

If a virus detection program accesses the files used by Ops Center Automator, operations such as I/O delays or file locks can cause errors. Also, if a process monitoring program kills any Ops Center Automator process, Ops Center Automator cannot work properly. To prevent these problems, exclude the following directories (including subdirectories) from the targets scanned by the virus detection program and the targets monitored by the process monitoring program while installing and running Ops Center Automator.

Note: The following directories are default paths that can be changed during installation.

Directories to be excluded during installation

- Windows:

  Mounted folder of the installation media

  `system-drive\Program Files\hitachi\Automation`

  `system-drive\Program Files\hitachi\database`

  `system-drive\Program Files\hitachi\Base64`

- Linux:

  Mounted directory of the installation media

  `/opt/HAD_Instdir`

  `/opt/hitachi/Automation`

  `/var/opt/hitachi/Automation`

  `/var/opt/hitachi/Base64`

  `/var/opt/hitachi/database`

Directories to be excluded during operation

- Windows:

  `system-drive\Program Files\hitachi\Automation`

  `system-drive\Program Files\hitachi\database`

  `system-drive\Program Files\hitachi\Base64\HDB`

- Linux:

  `/opt/hitachi/Automation`

  `/var/opt/hitachi/Automation`

  `/var/opt/hitachi/Base64/HDB`

  `/var/opt/hitachi/database`

Post-installation tasks

After installing Ops Center Automator, complete the following post-installation tasks:

1. If the server that manages the user account uses SSL communication, run the **`hcmds64prmset`** command to set the port number of the server (as needed).
2. Confirm the registered URL.
3. Verify access to the Ops Center Automator management server.
4. Run the **`setupcommonservice`** command to set up Common Services.

   For details about the **`setupcommonservice`** command, see setupcommonservice command (on page 237).

> **Note:** In a cluster configuration, **`setupcommonservice`** must only be run on the active node.

5. Register the license.
6. Change the System account password.
7. Set an email address for the System account.
8. Stop and restart Common Component and Ops Center Automator services (as needed).

You must change the System account password.

Confirming the registered URL (Windows OS)

Confirm the registered URL after installing Ops Center Automator.

Procedure

1. Confirm the registered URL by using the following command:

   ```
   Common-Component-installation-folder\bin\hcmds64chgurl /list
   ```

2. Verify the host name in the URL. In a noncluster environment, the host name must be a physical host name. In a cluster environment, the host name must be a logical host name. If the registered URL is incorrect, change the URL by using the following command:

   ```
   Common-Component-installation-folder\bin\hcmds64chgurl /change
   http://incorrect-IP-address-or-host-name:port-number http://
   correct-IP-address-or-host-name:port-number
   ```

   > **Note:** If you want to link with Common Services, change the registered URL by using the following command:
   >
   > ```
   > Common-Component-installation-folder\bin\hcmds64chgurl /change
   > https://IP-address-or-host-name:22016 /type Automation
   > ```

Confirming the registered URL (Linux OS)

Confirm the registered URL after installing Ops Center Automator.

Procedure

1. Confirm the registered URL by using the following command:

   ```
   Common-Component-installation-directory/bin/hcmds64chgurl -list
   ```

2. Verify the host name in the URL. If the registered URL is incorrect, change the URL by using the following command:

   ```
   Common-Component-installation-directory/bin/hcmds64chgurl -change
   http://incorrect-IP-address-or-host-name:port-number http://
   correct-IP-address-or-host-name:port-number
   ```

Note: If you want to link with Common Services, change the registered URL by using the following command:

```
Common-Component-installation-folder/bin/hcmds64chgurl -change
https://IP-address-or-host-name:22016 -type Automation
```

Verifying the installation

When installation is complete, verify that the installation was successful using a web browser.

Procedure

1. Open a web browser that is supported by Ops Center Automator.
2. In the address bar, specify the URL for Ops Center Automator in the following format:

   `http://automation_software-server-address:22015/Automation/`

Result

The logon window opens, verifying that you can access the management server.

Registering a license

When you log on initially, you must specify a valid license key.

Note: You must obtain the Ops Center Automator server license from your Hitachi Vantara representative.

Procedure

1. From the logon window, click **Licenses**.
2. Enter the license key, or click **Choose File** to browse to the license file.
3. Click **Save**.

Changing the system account password

The System account is a default account that has user management and execute permission for Ops Center Automator. When you install Ops Center Automator for the first time, you must change the System account password.

Note: This procedure only changes the local system account password. To change the Hitachi Ops Center system password, see the *Hitachi Ops Center Online Help*.

Procedure

1. From a management client, log on using the following credentials:

   User ID: system

   Password (default): manager

2. On the **Administration** tab, click **User Profile**.
3. Click **Change Password**, type the required passwords, then click **OK**.

Setting an e-mail address for the System account

Before Ops Center Automator can send e-mail notifications about Ops Center Automator system operations to the System, you must set up a System account e-mail account.

Procedure

1. On the Administration tab, click **User Profile**.
2. In the **User Profile** window, click **Edit Profile**, type the full name and the e-mail address, then click **OK**.

Result

The System account e-mail address is set up.

To receive email notifications, you must set up the System Settings to specify the Email SMTP server connection information (host name or IP address, user ID, password, and port are all required) and turn Email Notifications ON in the system parameter settings. For more detailed information, see the *Hitachi Ops Center Automator User Guide*.

Stopping and starting Common Component and Ops Center Automator services

You can start and stop Ops Center Automator services from the command prompt.

Stopping and starting all services from a command prompt (Windows OS)

The following procedure stops and starts all Common Component and Ops Center Automator services:

Procedure

1. At the command prompt, navigate to `Common-Component-installation-folder\bin`.
2. To stop the services, enter the following command:

   ```
   hcmds64srv /stop
   ```

   To start services, enter the following command:

   ```
   hcmds64srv /start
   ```

Stopping and starting all services from a command prompt (Linux OS)

The following procedure stops and starts all Common Component and Ops Center Automator services:

Procedure

1. At the command prompt, navigate to `Common-Component-installation-directory/bin`.
2. To stop the services, enter the following command:

   ```
   hcmds64srv -stop
   ```

   To start services, enter the following command:

   ```
   hcmds64srv -start
   ```

Stopping and starting only the Ops Center Automator service from the command prompt (Windows OS)

Procedure

1. Navigate to `Common-Component-installation-folder\bin`.
2. Start or stop the service:
   - To stop the service, enter the following command:

     ```
     hcmds64srv /stop /server AutomationWebService
     ```

   - To start the service, enter the following command:

     ```
     hcmds64srv /start /server AutomationWebService
     ```

Stopping and starting only the Ops Center Automator service from the command prompt (Linux OS)

Procedure

1. Navigate to `Common-Component-installation-directory/bin`.
2. Start or stop the service:
   - To stop the service, enter the following command:

     ```
     hcmds64srv -stop -server AutomationWebService
     ```

   - To start the service, enter the following command:

     ```
     hcmds64srv -start -server AutomationWebService
     ```

Configuring single sign-on in Common Services

To use the Ops Center portal single sign-on (SSO) functionality, you must register Automator with Common Services. If you deployed the Ops Center OVA, Automator is already registered in Common Services.

Registering Ops Center Automator with Ops Center Common Services

To use Common Services that is installed on a different host, or to use Common Services that was installed by using the installer, you must register Ops Center Automator with Common Services by running a command on the Ops Center Automator server.

Procedure

1. Run the **`setupcommonservice`** command with the **`auto`** option specified to register Ops Center Automator in Common Services.

   For details about the **`setupcommonservice`** command, see setupcommonservice command (on page 237).

Chapter 4: Configuring Ops Center Automator

This module gives information on how to configure Ops Center Automator.

Changing management server system settings

This module gives information about changing Ops Center Automator management server system settings.

Changing the port number used for management server communication with management clients

To change the port number used for communication between the Ops Center Automator management server and management clients (Web browsers), you must edit the definition file and configure exceptions in the firewall. For a cluster system, complete the same procedure on both the active server and standby server.

> **Note:** For information on other ports used with Ops Center Automator, see the Port settings reference topic.

To change the port number between the Ops Center Automator management server and management clients:

Procedure

1. Stop Ops Center Automator.
2. Change the port number settings by editing the keys in the definition files.
   - For HTTPS, go to Step 3.
   - For HTTP, change the port number settings by editing the keys in the definition files as follows:

     a. Modify the `Listen` key lines in the `user_httpsd.conf` file:

        Windows-based OS

        `Common-Component-installation-folder``\uCPSB11\httpsd\conf\user_httpsd.conf`

        Linux OS

        `Common-Component-installation-directory``/uCPSB11/httpsd/conf/user_httpsd.conf`

> **Note:** When you use Ops Center Automator in a cluster environment, you must edit the `user_httpsd.conf` file on both the active and standby nodes.

Specify the new port number in place of 22015 in the following lines:

```
Listen 22015
```

```
Listen [::]:22015
```

```
#Listen 127.0.0.1:22015
```

b. Modify the `command.http.port` lines in the `command_user.properties` file.

The folder that contains this definition file is different for cluster systems.

Windows-based OS (non-cluster)

`Automation_software-installation-folder\conf`

Windows-based OS (cluster)

`shared-folder-name\Automation\conf`

Linux OS

`Automation_software-installation-directory/conf`

c. Modify the `server.http.port` lines in the `config_user.properties` file.

The folder that contains this definition file is different for cluster systems.

Windows-based OS (non-cluster)

`Automation_software-installation-folder\conf`

Windows-based OS (cluster)

`shared-folder-name\Automation\conf`

Linux OS

`Automation_software-installation-directory/conf`

d. Go to Step 4.

3. For HTTPS, change the port number settings by editing the keys in the definition file as follows:

a. Open the `user_httpsd.conf` file.

Windows-based OS

`Common-Component-installation-folder\uCPSB11\httpsd\conf\user_httpsd.conf`

Linux OS

`Common-Component-installation-directory/uCPSB11/httpsd/conf/user_httpsd.conf`

> **Note:** When you use Ops Center Automator in a cluster environment, you must edit the `user_httpsd.conf` file on both the active and standby nodes.

b. Modify the `Listen` key lines by specifying the new port number in place of 22016 in the following lines:

```
Listen 22016
```

```
Listen [::]:22016
```

```
VirtualHost *22016
```

4. Configure firewall exceptions:
   - If the OS is Windows, run the **`hcmds64fwcancel`** command to configure exceptions in the firewall.
   - If the OS is Linux, configure exceptions according to the OS specifications. For details about the procedure, see the OS documentation.
5. Start Ops Center Automator.
6. Run the **`hcmds64chgurl`** command to update the URL for accessing Ops Center Automator.
7. If you use Common Services, run the **`setupcommonservice`** command to apply the change.

   See setupcommonservice command (on page 237) for more information.

Common Component property updates for port number changes

To change Common Component port numbers, you must update the Common Component properties that are listed in the following table.

Update the property files and then restart all Common Component and Ops Center Automator services.

Note: When you use Ops Center Automator in a cluster environment, you must edit the `user_httpsd.conf` file on both the active and standby nodes.

Port number (default)	Properties file path: Common Component installation folder	Location
22015/TCP	`\uCPSB11\httpsd\conf\user_httpsd.conf`	`Listen`
		`Listen [::]:`
		`#Listen 127.0.0.1:`
22016/TCP	`\uCPSB11\httpsd\conf\user_httpsd.conf`	*`host-name`*`:`*`port-number`* in the `VirtualHost` tag
		`Listen`
		`Listen [::]:`
22031/TCP	`\uCPSB11\httpsd\conf\user_hsso_httpsd.conf`	`Listen`

Port number (default)	Properties file path: Common Component installation folder	Location
22032/TCP	\HDB\CONF\emb\HiRDB.ini	PDNAMEPORT
	\HDB\CONF\pdsys	pd_name_port
	\database\work\def_pdsys	pd_name_port
22035/TCP	\uCPSB11\CC\server\usrconf\ejb \HBase64StgMgmtSSOService \usrconf.properties*	webserver.connector.nio_http.port
22036/TCP	\uCPSB11\CC\server\usrconf\ejb \HBase64StgMgmtSSOService \usrconf.properties	ejbserver.rmi.naming.port
22037/TCP	\uCPSB11\CC\server\usrconf\ejb \HBase64StgMgmtSSOService \usrconf.properties	ejbserver.http.port
22038/TCP	\uCPSB11\CC\server\usrconf\ejb \HBase64StgMgmtSSOService \usrconf.properties	ejbserver.rmi.remote.listener.port
22170/TCP	\uCPSB11\CC\server\userconf\ejb \AutomationWebService \usrconf.properties*	webserver.connector.nio_http.port
22171/TCP	\uCPSB11\CC\server\userconf\ejb \AutomationWebService \usrconf.properties	ejbserver.rmi.naming.port
22172/TCP	\uCPSB11\CC\server\userconf\ejb \AutomationWebService \usrconf.properties	ejbserver.http.port
22173/TCP	\uCPSB11\CC\server\userconf\ejb \AutomationWebService \usrconf.properties	ejbserver.rmi.remote.listener.port

*: When changing webserver.connector.nio_http.port, you must modify the following configuration files in addition to the corresponding line in usrconf.properties.

- reverse_proxy.conf
- reverse_proxy_before.conf
- reverse_proxy_after.conf
- hsso_reverse_proxy.conf

If the target port number is not described in the property file, no modification is required.

Changing the information of the server managing the user account

You can change the information of the server managing the user account, if necessary.

> **Note:** The user accounts are managed by the Common Component on the host you specified during the installation.

Procedure

1. If SSL is not set for HBase 64 Storage Mgmt Web Service on the server managing the user account, run this command:

   Windows OS:

   ```
   Common-Component-installation_folder\bin\hcmds64prmset /host
   Server-Managing-User-Account-IP-address-or-host-name /port
   HBase-64-Storage_Mgmt-Web-Service-of-Server-Managing-User-
   Account-non-SSL-portnumber
   ```

   Linux OS:

   ```
   Common-Component-installation-directory/bin/hcmds64prmset -host
   Server-Managing-User-Account-IP-address-or-host-name -port
   HBase-64-Storage-Mgmt-Web-Service-of-Server-Managing-User-
   Account-non-SSL-portnumber
   ```

2. If SSL is set for HBase 64 Storage Mgmt Web Service on the server managing the user account, run this command:

   Windows OS:

   ```
   Common-Component-installation-folder\bin\hcmds64prmset /host
   Server-Managing-User-Account-host-name /sslport HBase-64-Storage-
   Mgmt-Web-Service-of-Server-Managing-User-Account-SSL-portnumber
   ```

   Linux OS:

   ```
   Common-Component-installation-directory/bin/hcmds64prmset -host
   Server-Managing-User-Account-host-name -sslport HBase-64-Storage-
   Mgmt-Web-Service-of-Server-Managing-User-Account-SSL-portnumber
   ```

Changing the management server host name

You can change the host name of the management server after installing Ops Center Automator.

The management server host name cannot exceed 128 characters and is case-sensitive.

Procedure

1. Make a note of the new management server host name.

   If you must verify the host name on a Windows machine, use the `ipconfig /all` command to display the host name.
2. Run the `hcmds64srv /stop` command to stop all Common Component services.
3. Edit the `user_httpsd.conf` file to change the value of the ServerName parameter to the new host name.

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

- Windows OS

```
Common-Component-installation-folder\uCPSB11\httpsd\conf
```

- Linux OS

```
Common-Component-installation-directory/uCPSB11/httpsd/conf
```

If SSL settings are enabled, re-obtain the SSL server certificate and change the value of the ServerName parameter in the VirtualHost parameter to the new host name.

> **Note:** When you use Ops Center Automator in a cluster environment, you must edit the `user_httpsd.conf` file on both the active and standby nodes.

4. If you are running other Common Component products, revise the settings for those products as needed.
5. Change the host name of the management server. After making the change, restart the server.
6. If you use the host name to access the management server from a browser, run the **`hcmds64chgurl`** command to update the Common Component URL.
7. If you use Common Services, run the **`setupcommonservice`** command to apply the change.

Changing the management server IP address

You can change the IP address of the management server after installing Ops Center Automator.

Procedure

1. In the **Tasks** window, check the tasks. If any tasks are running, (In Progress, Waiting for Input, Long Running, In Progress (with Error), or In Progress (Terminating)), stop the tasks or wait until the task ends (Completed, Failed, or Canceled).
2. Run the `hcmds64srv /stop` command to stop all Common Component services.
3. Change the IP address of the management server.
4. Run the `hcmds64srv /start` command to start all Common Component services.
5. If you use the IP address to access the management server from a browser, run the **`hcmds64chgurl`** command to update the URL.
6. If you use Common Services, run the **`setupcommonservice`** command to apply the change.

Changing the Ops Center Automator management server URL

You must change the Ops Center Automator management server URL if you change the management server host name or IP address, the Ops Center Automator ports, or any SSL settings. If Ops Center Automator runs on the same management server as other Common Component products, you can change all of the Common Component URLs with one command.

Note: You must use a complete URL, which includes a protocol and a port number, for example, `http://HostA:22015`.

Procedure

1. Verify the current URL using the following command:

   ```
   Common-Component-installation-folder\bin\hcmds64chgurl /list
   ```

2. If Ops Center Automator is installed on a standalone server, change only the Ops Center Automator URL using the following command:

   ```
   Common-Component-installation-folder\bin\hcmds64chgurl /change
   new-URL /type Automation
   ```

3. If Ops Center Automator is installed on the same server, change all Common Component URLs that are running on this management server using the following command:

   ```
   Common-Component-installation-folder\bin\hcmds64chgurl /change
   old-URL new-URL
   ```

   Use the following format for the URL:

   ```
   Protocol://Management-server-IP-address-or-host-name:port-number
   ```

   Where:

   - *Protocol* is `http` for non-SSL communication and `https` for SSL communication.
   - *Management-server-IP-address-or-host-name* is the IP address or host name of the management server on which Ops Center Automator is installed.
   - *port-number* is the port number that is set for `Listen` line in the `user_httpsd.conf` file.

     For non-SSL communication, specify the port number for non-SSL communication (default: 22015).

     For SSL communication, specify the port number for SSL communication (default: 22016).

     The `user_httpsd.conf` file is in the *Common-Component-installation-folder*`\uCPSB11\httpsd\conf\` folder.

4. Verify that you can access Ops Center Automator using the new URL.
5. If you use Common Services, run the **`setupcommonservice`** command to apply the change.

Configuring secure communications

This module describes how to configure secure communications for Ops Center Automator.

About Ops Center Automator security settings

You can increase security by using secure communication for Ops Center Automator. Secure communication enables Ops Center Automator to increase security by using Transport Layer Security (TLS) for Ops Center Automator network communication. TLS enables Ops Center Automator to verify communication partners, enhance authentication for identifying partners, and detect falsified data within sent and received information. In addition, communication channels are encrypted so that data is protected from eavesdropping.

Ops Center Automator can use secure communications using TLS for the following types of communication:

- Communication between the management server and management clients
- Communication between the management server and an external authentication server (LDAP directory server)
- Communication between the management server and management targets

In addition, you can restrict access so that only specific management clients can access the management server.

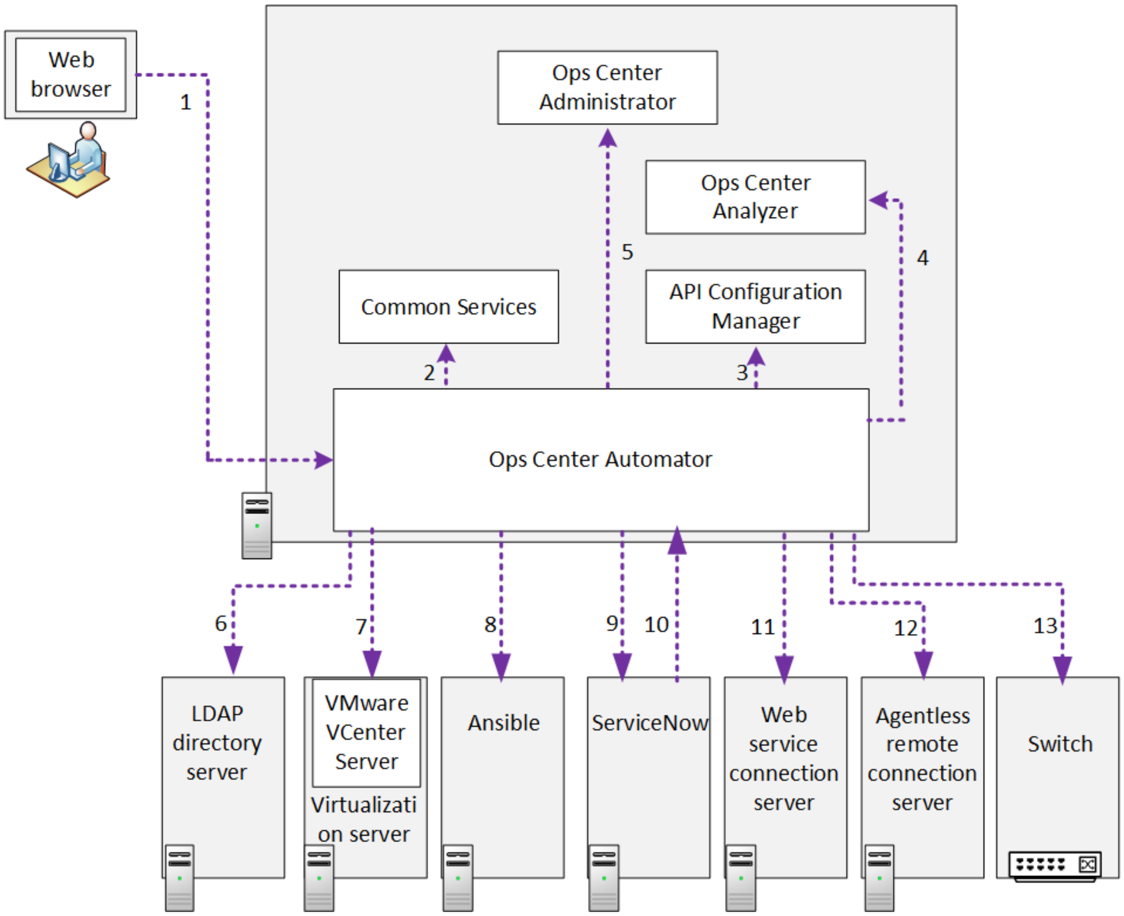
Note: When you use Ops Center Automator with security enabled, make sure that the server certificate is not expired. If the server certificate is expired, you must register a valid certificate to Ops Center Automator because users might not be able to connect to the server.

Note: For secure communication between the management server and management target, import the certificates issued by the Certificate authority, Intermediate certificate authority, or Root certificate authority into the Common Component trust store. If you want to re-register the certificates, you must delete the certificates by referring to Deleting Common Component truststore certificates (on page 85) and then import the certificates again.

Note: When you use Ops Center Automator in a cluster environment, you must import server certificates into the truststore on the active and standby nodes respectively.

Secure communication routes for Ops Center Automator

The following shows the secure communication routes for Ops Center Automator.



The following shows the secure communication routes that can be used in Ops Center Automator and the supported protocols for each route that is used. Note that the number in the table corresponds with the number in the figure.

Route	Server (program)	Client	Protocol
1	Ops Center Automator[1]	Management client (Web browser)	HTTPS[2]
2	Ops Center Common Services[1]	Ops Center Automator[1]	HTTPS
3	Ops Center API Configuration Manager[1]	Ops Center Automator[1]	HTTPS[2]
4	Ops Center Analyzer[1]	Ops Center Automator[1]	HTTPS[2]
5	Ops Center Administrator[1]	Ops Center Automator[1]	HTTPS
6	LDAP directory server	Ops Center Automator[1]	StartTLS[3]
7	VMware vCenter Server	Ops Center Automator[1]	HTTPS
8	Ops Center Automator[1]	Ansible[5]	HTTPS

Route	Server (program)	Client	Protocol
9	ServiceNow	Ops Center Automator[1]	HTTPS
10	Ops Center Automator[1]	ServiceNow[6]	HTTPS
11	Web service connection server (for example, DCNM)	Ops Center Automator[1]	HTTPS[2]
12	Agentless remote connection server	Ops Center Automator[1]	SSH[4]
13	Brocade Fabric OS	Ops Center Automator[1]	HTTPS[2]

1. You can configure this component by using the `cssslsetup` command if the products are installed on the same management server as Common Services.
2. HTTP can also be used in addition to HTTPS.
3. LDAP can also be used in addition to StartTLS.
4. Telnet or SMB and RPC can also be used in addition to SSH.
5. If you use a Common Services user to access Ops Center Automator, the SSL setting between Ansible and Common Services is also required.
6. If you use a Common Services user to access Ops Center Automator, the SSL setting between ServiceNow and Common Services is also required.

- If the protocol used for communication with Ops Center Automator is HTTPS, TLS 1.2 and TLS 1.3 are supported. Note that if you have changed the server managing the Common Component user account to a remote host, only TLS 1.2 is supported for communication from Ops Center Automator to the server. For cipher suites supported by Ops Center Automator as a server, see Cipher suites supported as a server (on page 256).
- For security settings for communication route 9 with Ansible, see the *Hitachi Ops Center Automator User Guide*.
- For security settings for communication route 10 and 11 with ServiceNow, see the *Hitachi Ops Center Automator User Guide*.

Configuring security for management clients

This module gives information about setting up secure communication between the management server and management clients.

About secure communications for management clients

Implement secure communication between the Ops Center Automator management server and management clients using SSL. To implement SSL, first set up SSL on the management server and then on the management clients. The process for setting up SSL on web-based clients is different from CLI clients.

Setting up SSL on the server for secure client communication (Windows OS)

To implement secure communication between the management server and management clients, you must set up SSL on the management server.

> **Note:** After a new installation, SSL settings are enabled. The same certificate is used as when the **`hcmds64ssltool`** command is run without any options. In the case of an upgrade installation, keep the current SSL settings.

The `hcmds64ssltool` command creates two types of private keys: certificate signing requests, and self-signed certificates supporting RSA ciphers and elliptic curve ciphers (ECC). The certificate signing request is created in PEM format. Although you can use this command to create a self-signed certificate, you should use a self-signed certificate for testing purposed only.

Before you begin

Log on as a user with Administrator permissions.

Collect the following information:

- Requirements for the certificate signing request specified by the certificate authority.
- Web browser version running on the management client.

  The Web browser must use X.509 PEM format and support the signature algorithm of the server certificates used on the management client (GUI).
- Existing storage directories for private keys, certificate signing requests, and self-signed certificates, if you are recreating them.

  If a file with the same name already exists in the output location, the command does not overwrite the file. Therefore, when you recreate a private key, certificate signing request, or self-signed certificate, you must output it to a folder other than existing storage folders or delete the existing files.

Procedure

1. To create a private key (`httpsdkey.pem`), a certificate signing request (`httpsd.csr`), and a self-signed certificate (`httpsd.pem`) for the Common Component, use the following command:

   ```
   Common-Component-installation-folder\bin\hcmds64ssltool [/key
   private-key-file] [/csr certificate-signed-request-file] [/cert
   self-signed-certificate-file] [/certtext self-signed-certificate-
   content-file] [/validity expiration-date] [/sigalg RSA-server-
   certificate-signature-algorithm] [/eccsigalg ECC-server-
   certificate-signature-algorithm] [/ecckeysize ECC-private-key-
   size] [/ext extension-information-for-the-X.509-certificate]
   ```

where

- `key` specifies the absolute path of the private key file that is created. If you omit this option, the files are output to the default output destination path# with the file name httpsdkey.pem (for RSA) and ecc-httpsdkey.pem (for ECC).
- `csr` specifies the absolute path of the certificate signing request file that is created. If you omit this option, the files are output to the default output destination path# with the file name httpsd.csr (for RSA) and ecc-httpsd.csr (for ECC).
- `cert` specifies the absolute path of the self-signed certificate file that is created. If you omit this option, the files are output to the default output destination path# with the file name httpsd.pem (for RSA) and ecc-httpsd.pem (for ECC).
- `certtext` specifies the absolute path of the self-signed certificate content file that is created. If you omit this option, the files are output to the default output destination path# with the file name httpsd.txt (for RSA) and ecc-httpsd.txt (for ECC).
- `validity` specifies the expiration date of the self-signed certificate by using the number of days. If you omit this option, the default of 3,650 days is used.
- `sigalg` specifies the signature algorithm of the RSA certificate as SHA256withRSA, or SHA1withRSA. If you omit this option, the default of SHA256withRSA is used.
- `eccsigalg` specifies the signature algorithm of the ECC certificate as SHA512withECDSA, SHA384withECDSA, SHA256withECDSA, or SHA1withECDSA. If you omit this option, the default of SHA384withECDSA is used.
- `ecckeysize` specifies the key size of the private key for the ECC server certificates in bits as 256 or 384. If you omit this option, the default of 384 is used.
- `ext` specifies the extension information for the X.509 certificate. To set SAN (Subject Alternative Name) on the self-signed certificate and certificate signing request, specify this option. The specification method is based on the `ext` option of the **`keytool`** command in Java. Note, however, that the only extension that can be specified in Ops Center Automator is SAN. If you specify the `ext` option multiple times, the first specification takes effect.

  The following is an example of specifying the extension information.

  - To specify www.example.com as the host name:

    ```
    hccmds64ssltool /ext san=dns:www.example.com
    ```

  - To specify www.example.com and www.example.net as multiple host names:

    ```
    hccmds64ssltool /ext san=dns:www.example.com,
    dns:www.example.net
    ```

This command outputs the RSA and ECC files to the specified output destination path. RSA files are output with the specified file name, and ECC files output with a prefix of "ecc-".

#The default output destination when you omit the key, csr, cert, or certtext options is as follows:

```
Common-Component-installation-folder\uCPSB11\httpsd\conf\ssl
\server
```

2. When prompted, enter the following information after the colon(:).

   - Server Name (management server host name) - for example, Automator-SC1.
   - Organizational Unit (section) - for example, Ops Center Automator.
   - Organization Name (company) - for example, Hitachi.
   - City or Locality Name - for example, Santa Clara.
   - State or Province Name (full name) - for example, California.
   - Country Name (2 letter code) - for example, US.

   To leave a field blank, type a period (.). To select a default value visible within the brackets ([]), press the **Enter** key.

3. Send the certificate signing request (`httpsd.csr`) to the certificate authority to apply for a server certificate.

   > **Note:** This step is not required if you plan to use a self-signed certificate, but you should use a signed server certificate in a production environment.

   The server certificate issued by the certificate authority is usually sent by email. Ensure that you save the email and the server certificate sent by the certificate authority.

4. Stop Ops Center Automator.
5. Copy the private key (`httpsdkey.pem`) and the server certificate or the self-signed certificate (`httpsd.pem`) to the following folder:

   ```
   Common-Component-installation-folder\uCPSB11\httpsd\conf\ssl\server
   ```

6. Open the `user_httpsd.conf` file from the following location:

   ```
   Common-Component-installation-folder\uCPSB11\httpsd\conf\user_httpsd.conf
   ```

7. Within the `user_httpsd.conf` file, do the following:

   > **Note:** When you use Ops Center Automator in a cluster environment, you must edit the `user_httpsd.conf` file on both the active and standby nodes.

   a. Uncomment the following lines by removing the hash [#] signs:

      ```
      #Listen 22016
      ```

      ```
      #<VirtualHost *:22016>
      ```

      through

      ```
      #</VirtualHost>
      ```

      with the exception of `#SSLCACertificateFile` and `#Header set Strict-Transport-Security max-age=31536000`, which must remain commented out.

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

The following is an example of how to edit the `user_httpsd.conf` file.

```
ServerName host-name
Listen [::]:22015
Listen 22015
#Listen 127.0.0.1:22015
SSLEngine Off
Listen [::]:22016
Listen 22016
<VirtualHost *:22016>
ServerName host-name
SSLEngine On
SSLProtocol +TLSv1.2 +TLSv1.3
SSLCipherSuite TLSv1.3
TLS_AES_128_GCM_SHA256:TLS_AES_256_GCM_SHA384:TLS_CHACHA20_POLY1305_SHA256
#  SSLCipherSuite ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-GCM-
SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:AES256-GCM-
SHA384:AES128-GCM-SHA256
SSLCipherSuite ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-GCM-
SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256
SSLCertificateKeyFile
"Common-Component-installation-directory/uCPSB11/httpsd/conf/ssl/server/
httpsdkey.pem"
SSLCertificateFile
"Common-Component-installation-directory/uCPSB11/httpsd/conf/ssl/server/
httpsd.pem"
SSLCertificateKeyFile
"Common-Component-installation-directory/uCPSB11/httpsd/conf/ssl/server/ecc-
httpsdkey.pem"
SSLCertificateFile
"Common-Component-installation-directory/uCPSB11/httpsd/conf/ssl/server/ecc-
httpsd.pem"
# SSLCACertificateFile
"Common-Component-installation-directory/uCPSB11/httpsd/conf/ssl/cacert/
anycert.pem"
# Header set Strict-Transport-Security max-age=31536000
</VirtualHost>
#HWSLogSSLVerbose On
```

b. Edit the following lines as required:

ServerName in the first line

ServerName in the <VirtualHost> tag

SSLCertificateKeyFile

SSLCertificateFile

#SSLCACertificateFile

When using a chained server certificate issued from a certificate authority, delete the hash sign (#) from the line "# SSLCACertificateFile", and specify the chained certificate file (created by certificate authority) by using an absolute path.

> **Note:** To block non-SSL communication from external servers to the management server, comment out the lines `Listen 22015` and `Listen [::]:22015` by adding a hash mark (#) to the beginning of each line. After you comment out these lines, remove the hash mark (#) from the line `#Listen 127.0.0.1:22015`.
>
> In addition, for a Windows cluster environment, add or edit the following line in the `command_user.properties` file:
>
> ```
> command.hostname = localhost
> ```
>
> The `command_user.properties` file is stored in the following location:
>
> ```
> shared-folder-name\Automation\conf
> ```

When editing directives, be aware of the following:

- Do not specify the same directive twice.
- Do not enter a line break in the middle of a directive.
- When specifying paths in the following directives, do not specify symbolic links or junction points. Paths must be specified as absolute paths.
- When specifying certificates and private key files in the following directives, specify PEM-format files.
- Do not edit `httpsd.conf` or `hsso_httpsd.conf`.
- Do not remove the hash mark (#) from the beginning of the following line.

```
# Header set Strict-Transport-Security max-age=31536000
```

The following is an example of how to edit the `user_httpsd.conf` file. The numbers represent the default ports.

```
ServerName host-name
Listen [::]:22015
Listen 22015
#Listen 127.0.0.1:22015
SSLEngine Off
Listen [::]:22016
Listen 22016
<VirtualHost *:22016>
ServerName host-name
SSLEngine On
SSLProtocol +TLSv1.2 +TLSv1.3
SSLCipherSuite TLSv1.3
TLS_AES_128_GCM_SHA256:TLS_AES_256_GCM_SHA384:TLS_CHACHA20_POLY1305_SHA256
#  SSLCipherSuite ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-GCM-
SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:AES256-GCM-
SHA384:AES128-GCM-SHA256
SSLCipherSuite ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-
```

```
RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256
SSLCertificateKeyFile
"Common-Component-installation-directory/uCPSB11/httpsd/conf/ssl/server/
httpsdkey.pem"
SSLCertificateFile
"Common-Component-installation-directory/uCPSB11/httpsd/conf/ssl/server/server-
certificate-or-self-signed-certificate-file"
SSLCertificateKeyFile
"Common-Component-installation-directory/uCPSB11/httpsd/conf/ssl/server/ecc-
httpsdkey.pem"
SSLCertificateFile
"Common-Component-installation-directory/uCPSB11/httpsd/conf/ssl/server/ecc-
httpsd.pem"
SSLCACertificateFile
"Common-Component-installation-directory/uCPSB11/httpsd/conf/ssl/cacert/
certificate-file-from-certificate-authority"
# Header set Strict-Transport-Security max-age=31536000
</VirtualHost>
#HWSLogSSLVerbose On
```

8. Start Ops Center Automator.
9. Update the Ops Center Automator URL by using the `hcmds64chgurl` to do the following:
   - Change the protocol from http: to https:
   - Change the port number used for secure communication.
10. If you use Common Services, run the **`setupcommonservice`** command to apply the change.

Result

SSL is now implemented on the Ops Center Automator server.

Setting up SSL on the server for secure client communication (Linux OS)

To implement secure communication between the management server and management clients, you must set up SSL on the management server.

Note: After a new installation, SSL settings are enabled. The same certificate is used as when the **`hcmds64ssltool`** command is run without any options. In the case of an upgrade installation, keep the current SSL settings.

The `hcmds64ssltool` command creates two types of private keys: certificate signing requests, and self-signed certificates supporting RSA ciphers and elliptic curve ciphers (ECC). The certificate signing request is created in PEM format. Although you can use this command to create a self-signed certificate, best practice is to use a self-signed certificate for testing purposed only.

Before you begin

Log on as a root user.

Collect the following information:

- Requirements for the certificate signing request specified by the certificate authority.
- Web browser version running on the management client.

  The Web browser must use X.509 PEM format and support the signature algorithm of the server certificates used on the management client (GUI).
- Existing storage directories for private keys, certificate signing requests, and self-signed certificates, if you are recreating them.

  If a file with the same name already exists in the output location, the command does not overwrite the file. Therefore, when you recreate a private key, certificate signing request, or self-signed certificate, you must output it to a directory other than existing storage directory or delete the existing files.

Procedure

1. To create a private key (`httpsdkey.pem`), a certificate signing request (`httpsd.csr`), and a self-signed certificate (`httpsd.pem`) for the Common Component, use the following command:

   ```
   Common-Component-installation-directory/bin/hcmds64ssltool [-key
   private-key-file] [-csr certificate-signed-request-file] [-cert
   self-signed-certificate-file] [-certtext self-signed-certificate-
   content-file] [-validity expiration-date] [-sigalg RSA-server-
   certificate-signature-algorithm] [-eccsigalg ECC-server-
   certificate-signature-algorithm] [-ecckeysize ECC-private-key-
   size] [-ext extension-information-for-the-X.509-certificate]
   ```

   where

   - `key` specifies the absolute path of the private key file that is created. If you omit this option, the files are output to the default output destination path# with the file name httpsdkey.pem (for RSA) and ecc-httpsdkey.pem (for ECC).
   - `csr` specifies the absolute path of the certificate signing request file that is created. If you omit this option, the files are output to the default output destination path# with the file name httpsd.csr (for RSA) and ecc-httpsd.csr (for ECC).
   - `cert` specifies the absolute path of the self-signed certificate file that is created. If you omit this option, the files are output to the default output destination path# with the file name httpsd.pem (for RSA) and ecc-httpsd.pem (for ECC).
   - `certtext` specifies the absolute path of the self-signed certificate content file that is created. If you omit this option, the files are output to the default output destination path# with the file name httpsd.txt (for RSA) and ecc-httpsd.txt (for ECC).
   - `validity` specifies the expiration date of the self-signed certificate by using the number of days. If you omit this option, the default of 3,650 days is used.
   - `sigalg` specifies the signature algorithm of the RSA certificate as SHA256withRSA, or SHA1withRSA. If you omit this option, the default of SHA256withRSA is used.

- `eccsigalg` specifies the signature algorithm of the ECC certificate as SHA512withECDSA, SHA384withECDSA, SHA256withECDSA, or SHA1withECDSA. If you omit this option, the default of SHA384withECDSA is used.
- `ecckeysize` specifies the key size of the private key for the ECC server certificates in bits as 256 or 384. If you omit this option, the default of 384 is used.
- `ext` specifies the extension information for the X.509 certificate. To set SAN (Subject Alternative Name) on the self-signed certificate and certificate signing request, specify this option. The specification method is based on the `ext` option of the **`keytool`** command in Java. Note, however, that the only extension that can be specified in Ops Center Automator is SAN. If you specify the `ext` option multiple times, the first specification takes effect.

  The following is an example of specifying the extension information.

  - To specify www.example.com as the host name:

    ```
    hccmds64ssltool -ext san=dns:www.example.com
    ```

  - To specify www.example.com and www.example.net as multiple host names:

    ```
    hccmds64ssltool -ext san=dns:www.example.com,
    dns:www.example.net
    ```

This command outputs the RSA and ECC files to the specified output destination path. RSA files are output with the specified file name, and ECC files output with a prefix of "ecc-".

#The default output destination when you omit the key, csr, cert, or certtext options is as follows:

`Common-Component-installation-directory``/uCPSB11/httpsd/conf/ssl/server`

2. When prompted, enter the following information after the colon(:).

   - Server Name (management server host name) - for example, Automator-SC1.
   - Organizational Unit (section) - for example, Ops Center Automator.
   - Organization Name (company) - for example, Hitachi.
   - City or Locality Name - for example, Santa Clara.
   - State or Province Name (full name) - for example, California.
   - Country Name (2 letter code) - for example, US.

   To leave a field blank, type a period (.). To select a default value visible within the brackets ([]), press the **Enter** key.

3. Send the certificate signing request (`httpsd.csr`) to the certificate authority to apply for a server certificate.

   Note: This step is not needed if you plan to use a self-signed certificate, but best practice is to use a signed server certificate in a production environment.

The server certificate issued by the certificate authority is usually sent by email. Ensure that you save the email and the server certificate sent by the certificate authority.

4. Stop Ops Center Automator.
5. Copy the private key (`httpsdkey.pem`) and the server certificate or the self-signed certificate (`httpsd.pem`) to the following directory:

   `Common-Component-installation-directory``/uCPSB11/httpsd/conf/ssl/server`

6. Open the `user_httpsd.conf` file from the following location:

   `Common-Component-installation-directory``/uCPSB11/httpsd/conf/user_httpsd.conf`

7. Within the `user_httpsd.conf` file, do the following:

   > **Note:** When you use Ops Center Automator in a cluster environment, you must edit the `user_httpsd.conf` file on both the active and standby nodes.

   a. Uncomment the following lines by removing the hash [#] signs:

      `#Listen 22016`

      `#<VirtualHost *:22016>`

      through

      `#</VirtualHost>`

      with the exception of `#SSLCACertificateFile` and `#Header set Strict-Transport-Security max-age=31536000`, which must remain commented out.

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

      The following is an example of how to edit the `user_httpsd.conf` file.

```
ServerName host-name
Listen [::]:22015
Listen 22015
#Listen 127.0.0.1:22015
SSLEngine Off
Listen [::]:22016
Listen 22016
<VirtualHost *:22016>
ServerName host-name
SSLEngine On
SSLProtocol +TLSv1.2 +TLSv1.3
SSLCipherSuite TLSv1.3
TLS_AES_128_GCM_SHA256:TLS_AES_256_GCM_SHA384:TLS_CHACHA20_POLY1305_SHA256
# SSLCipherSuite ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-
GCMSHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:AES256-
GCMSHA384:AES128-GCM-SHA256
SSLCipherSuite ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-
GCMSHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256
SSLCertificateKeyFile
```

```
"Common-Component-installation-directory/uCPSB11/httpsd/conf/ssl/server/
httpsdkey.pem"
SSLCertificateFile
"Common-Component-installation-directory/uCPSB11/httpsd/conf/ssl/server/
httpsd.pem"
SSLCertificateKeyFile
"Common-Component-installation-directory/uCPSB11/httpsd/conf/ssl/server/ecc-
httpsdkey.pem"
SSLCertificateFile
"Common-Component-installation-directory/uCPSB11/httpsd/conf/ssl/server/ecc-
httpsd.pem"
# SSLCACertificateFile
"Common-Component-installation-directory/uCPSB11/httpsd/conf/ssl/cacert/
anycert.pem"
# Header set Strict-Transport-Security max-age=31536000
</VirtualHost>
#HWSLogSSLVerbose On
```

b. Edit the following lines as required:

   ServerName in the first line

   ServerName in the <VirtualHost> tag

   SSLCertificateKeyFile

   SSLCertificateFile

   #SSLCACertificateFile

   When using a chained server certificate issued from a certificate authority, delete the hash sign (#) from the line "# SSLCACertificateFile", and specify the chained certificate file (created by certificate authority) by using an absolute path.

   Note:

   To block non-SSL communication from external servers to the management server, comment out the lines `Listen 22015` and `Listen [::]:22015` by adding a hash mark (#) to the beginning of each line. After you comment out these lines, remove the hash mark (#) from the line `#Listen 127.0.0.1:22015`.

When editing directives, be aware of the following:

- Do not specify the same directive twice.
- Do not enter a line break in the middle of a directive.
- When specifying paths in the following directives, do not specify symbolic links or junction points. Paths must be specified as absolute paths.
- When specifying certificates and private key files in the following directives, specify PEM-format files.

- Do not edit `httpsd.conf` or `hsso_httpsd.conf`.
- Do not remove the hash mark (#) from the beginning of the following line.

```
# Header set Strict-Transport-Security max-age=31536000
```

The following is an example of how to edit the `user_httpsd.conf` file. The numbers represent the default ports.

```
ServerName host-name
Listen [::]:22015
Listen 22015
#Listen 127.0.0.1:22015
SSLEngine Off
Listen [::]:22016
Listen 22016
<VirtualHost *:22016>
ServerName host-name
SSLEngine On
SSLProtocol +TLSv1.2 +TLSv1.3
SSLCipherSuite TLSv1.3
TLS_AES_128_GCM_SHA256:TLS_AES_256_GCM_SHA384:TLS_CHACHA20_POLY1305_SHA256
# SSLCipherSuite ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-
GCMSHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:AES256-
GCMSHA384:AES128-GCM-SHA256
SSLCipherSuite ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-GCM-
SHA256:ECDHERSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256
SSLCertificateKeyFile
"Common-Component-installation-directory/uCPSB11/httpsd/conf/ssl/server/
httpsdkey.pem"
SSLCertificateFile
"Common-Component-installation-directory/uCPSB11/httpsd/conf/ssl/server/server-
certificate-or-self-signed-certificate-file"
SSLCertificateKeyFile
"Common-Component-installation-directory/uCPSB11/httpsd/conf/ssl/server/ecc-
httpsdkey.pem"
SSLCertificateFile
"Common-Component-installation-directory/uCPSB11/httpsd/conf/ssl/server/ecc-
httpsd.pem"
SSLCACertificateFile
"Common-Component-installation-directory/uCPSB11/httpsd/conf/ssl/cacert/
certificate-file-from-certificate-authority"
# Header set Strict-Transport-Security max-age=31536000
</VirtualHost>
#HWSLogSSLVerbose On
```

8. Start Ops Center Automator.

9. Update the Ops Center Automator URL by using the `hcmds64chgurl` command to do the following:
   - Change the protocol from http: to https:
   - Change the port number used for secure communication.
10. If you use Common Services, run the **`setupcommonservice`** command to apply the change.

Result

SSL is now implemented on the Ops Center Automator server.

Setting up SSL on web-based management clients

To implement secure communications between the management server and management clients, you must set up SSL on all Ops Center Automator management clients that access the Ops Center Automator web-based user interface. You must first set up SSL on the management server before setting up the management clients. You are only required to follow this procedure the first time you access the management server from this client.

Before you begin

If the signature algorithm used is SHA256 with RSA, the Web browser in use must support a server certificate that has an SHA256 with RSA signature.

Procedure

1. From the management web client, access the management server using an SSL connection by using the following URL:

   `https://`*`automation-software-management-server-name`*`:`*`port-number-for-SSL-communication`*`/Automation/`
2. Install the SSL certificate.

Result

The SSL certificate is registered on the management client so it can communicate with the management server using SSL.

Setting up secure communication for an external authentication server

In a Windows environment, use the StartTLS protocol to implement secure communication between the Ops Center Automator management server and the LDAP directory server. To implement StartTLS, you must update the properties in the `exauth.properties` file and import the LDAP directory server certificate into the management server.

See Importing a certificate into the truststore for Common Component (on page 73) for details.

> **Note:** If you specify an IPV6 address in a Linux OS environment, you are required to enclose the address with square brackets [ ].

Importing a certificate into the truststore for Common Component

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

Before you begin

- Prepare a certificate

  Securely obtain the certificate.

  - For communication with an LDAP directory server:

    The certificates issued by all the authorities from the authority that issued an LDAP directory server certificate to the root certificate authority must form a certificate chain. The certificate must satisfy the product requirements for Common Component.

  - When using a certificate authority:

    The certificates issued by all the authorities from the authority which issued the Common Component server certificate to the root certificate authority must form a certificate chain.

  - When using a self-signed certificate:

    Obtain a Common Component self-signed certificate.

- Verify that you have the password to access the truststore, if the truststore already exists.

Procedure

1. Run the following command:

   In Windows:

   ```
   Common-Component-installation-folder\bin\hcmds64keytool -import -
   alias alias-name -file certificate-file-name -keystore
   truststore-file-name -storetype JKS
   ```

   In Linux:

   ```
   Common-Component-installation-directory/uCPSB11/jdk/bin/keytool -
   import -alias alias-name -file certificate-file-name -keystore
   truststore-file-name -storetype JKS
   ```

   Where:

   - alias: Specify the name used to identify the certificate in the truststore. If there are two or more server certificates, specify an alias name which is not used in the truststore.

   - keystore: Specify the truststore file path of the import destination. If no truststore file exists, one will be automatically created.

     You should import LDAP directory server certificates into ldapcacerts. To share a certificate with other programs, you can import the certificate into jssecacerts.

   The truststore (`ldapcacerts` or `jssecacerts`) file paths are as follows.

`jssecacerts`

- For Windows:

  Common-Component-installation-folder`\uCPSB11\hjdk\jdk\lib\security\jssecacerts`

- For Linux:

  Common-Component-installation-directory`/uCPSB11/hjdk/jdk/lib/security/jssecacerts`

`ldapcacerts`

- For Windows:

  Common-Component-installation-folder`\conf\sec\ldapcacerts`

- For Linux:

  Common-Component-installation-directory`/conf/sec/ldapcacerts`

> **Note:** You are prompted to enter the truststore password in interactive mode. When prompted, specify a password of your choice used to access the truststore (minimum of 6 characters). If the truststore already exists, specify the current truststore password.

2. Restart the Common Component services.

Changing the authenticator connection port number for the primary Common Component server

After you set up secure communication with an external authentication server, you must change the authenticator connection port number.

To change the authenticator connection port number, run the **`hcmds64prmset`** command as follows:

- Windows:

```
Common-Component-installation-folder\bin\hcmds64prmset /host
primary_server_hostname /sslport SSL_port_number
```

- Linux:

```
Common-Component-installation-directory/bin/hcmds64prmset -host
primary_server_hostname -sslport SSL_port_number
```

where:

- *primary_server_hostname* is the same name as the Common Name (CN) for the credentials.
- *ssl_port_number* is the same as the SSL Common Component port number. The default is 22016.

Setting up secure communications with Ops Center Common Services

Ops Center Automator and Ops Center Common Services must communicate over an SSL connection. If you want to enable the certificate verification, you must import the certificates into the Common Component truststore. You can also change the cipher suites to be used.

> **Tip:** If Common Services is on the same server as Ops Center Automator, the **`cssslsetup`** command is available. By using the **`cssslsetup`** command, you can configure SSL communication for Hitachi Ops Center products installed on the same management server using a common private key and server certificate. For more information on the usage and support scope of the **`cssslsetup`** command, refer to "Configuring SSL communications by using the cssslsetup command" in the *Hitachi Ops Center Installation and Configuration Guide*.

Before you begin

- Set up SSL on the Ops Center Automator server between the management server and management client. For details, see "Setting up SSL on the server for secure client communication (Windows OS)" (on page 61) or Setting up SSL on the server for secure client communication (Linux OS) (on page 66).
- Set up SSL on the Common Services server. For details, see “Configuring SSL for a multi-server configuration" in the *Hitachi Ops Center Installation and Configuration Guide*.

Procedure

1. If you want to enable the certificate verification, do the following:
   a. Import the certificates into the Common Component truststore by running the following command:

      For Windows:

      ```
      Common-Component-installation-folder\bin\hcmds64keytool -import -alias
      alias-name -keystore Common-Component-installation-folder\uCPSB11
      \hjdk\jdk\lib\security\jssecacerts -file certificate-file -storetype JKS
      ```

      For Linux:

      ```
      Common-Component-installation-directory/uCPSB11/jdk/bin/keytool -import -
      alias alias-name -keystore Common-Component-installation-directory/uCPSB11/
      hjdk/jdk/lib/security/jssecacerts -file certificate-file -storetype JKS
      ```

      To import the certificates in Java, ensure that the truststore password includes six or more characters. In addition, ensure that the new alias name does not conflict with an existing alias name. Since the certificates used vary depending on the environment and configuration, import either or both RSA and ECDSA certificates into the Common Component truststore based on the certificates available in the Ops Center Common Services server.

   b. Edit the `sso.https.certification` parameter to true in the `config_user.properties` file in the following location:

      In Windows (non-cluster): `Automation-software-installation-folder\conf`

      In Windows (cluster): `shared-folder_name\Automation\conf`

      In Linux: `Automation-software-installation-directory/conf`

2. (Optional) If you want to change the cipher suites to be used for communication with the Ops Center Common Services server, do the following:

   a. Open the `config_user.properties` file from the following location.

      In Windows (non-cluster): *`Automation-software-installation-folder`*`\conf`

      In Windows (cluster): *`shared-folder_name`*`\Automation\conf`

      In Linux: *`Automation-software-installation-directory`*`/conf`

   b. Edit the `tls.client.cipherSuites` line. If the `tls.client.cipherSuites` line does not exist, add it.

      One of the cipher suites in the `tls.client.cipherSuites` line is used in the communication. Specify the cipher suites you want to use in the `tls.client.cipherSuites` line. If there are multiple cipher suites you want to use, specify the cipher suites separated by commas.

      For available cipher suites, see Cipher suites supported as a client (on page 256).

      For details about the `tls.Client.cipherSuites` property, see Changing the system configuration (on page 94).

3. Restart the services by running the **`hcmds64srv`** command.

Setting up secure communication with an Ops Center API Configuration Manager REST API server

You can set up SSL communication to be used between the Ops Center Automator server and the Ops Center API Configuration Manager REST API server by using a self-signed certificate or a certificate issued by a certificate authority. You can also change the cipher suites to be used.

Before you begin

If you already set up SSL on the Ops Center API Configuration Manager server, including creating the certificates, go to step 2. Otherwise, start at step 1.

Procedure

1. Set up SSL on the Ops Center API Configuration Manager REST API server. For details, see “Specifying settings for using SSL communication between REST API clients and the REST API server (when using a self-signed certificate)” or “Specifying settings for using SSL communication between REST API clients and the REST API server (when using a server certificate issued by a certificate authority)" in the *Hitachi Ops Center API Configuration Manager REST API Reference Guide*.

2. Import the certificates into the Common Component truststore by running the following command:

   For Windows:

   ```
   Common-Component-installation-folder\bin\hcmds64keytool -import -alias
   alias-name -keystore Common-Component-installation-folder\uCPSB11
   \hjdk\jdk\lib\security\jssecacerts -file certificate-file -storetype JKS
   ```

   For Linux:

   ```
   Common-Component-installation-directory/uCPSB11/jdk/bin/keytool -import -alias
   alias-name -keystore Common-Component-installation-directory/uCPSB11/
   hjdk/jdk/lib/security/jssecacerts -file certificate-file -storetype JKS
   ```

   To import the certificates in Java, ensure that the truststore password includes six or more characters. In addition, ensure that the new alias name does not conflict with an existing alias name. Since the certificates used vary depending on the environment and configuration, import either or both RSA and ECDSA certificates into the Common Component truststore based on the certificates available in the Ops Center API Configuration Manager REST API server.

3. (Optional) If you want to change the cipher suites to be used for communication with the Ops Center API Configuration Manager REST API server, do the following:

   Note: When you use built-in service templates to communicate with the Ops Center API Configuration Manager REST API server, the property in this step has no effect and you do not need to perform this step.

   a. Open the `config_user.properties` file from the following location.

      In Windows (non-cluster): `Automation-software-installation-folder\conf`

      In Windows (cluster): `shared-folder_name\Automation\conf`

      In Linux: `Automation-software-installation-directory/conf`

   b. Edit the `tls.client.cipherSuites` line. If the `tls.client.cipherSuites` line does not exist, add it.

      One of the cipher suites in the `tls.client.cipherSuites` line is used in the communication. Specify the cipher suites you want to use in the `tls.client.cipherSuites` line. If there are multiple cipher suites you want to use, specify the cipher suites separated by commas.

      For available cipher suites, see Cipher suites supported as a client (on page 256).

      For details about the `tls.client.cipherSuites` property, see Changing the system configuration (on page 94).

4. Restart the services by running the **`hcmds64srv`** command.

Setting up secure communication with an Ops Center Administrator server

You can set up SSL communication to be used between the Ops Center Automator server and the Ops Center Administrator server by using a self-signed certificate or a certificate issued by a certificate authority. You can also change the cipher suites to be used.

Before you begin

If you already set up SSL on the Ops Center Administrator server, including creating the certificates, go to step 2. Otherwise, start at step 1.

Procedure

1. Set up SSL on the Ops Center Administrator server. For details, see “Setting up SSL” in the *Hitachi Ops Center Administrator Getting Started Guide*.
2. Import the certificates into the Common Component truststore by running the following command:

   For Windows:

   ```
   Common-Component-installation-folder\bin\hcmds64keytool -import -alias
   alias-name -keystore Common-Component-installation-folder\uCPSB11
   \hjdk\jdk\lib\security\jssecacerts -file certificate-file -storetype JKS
   ```

   For Linux:

   ```
   Common-Component-installation-directory/uCPSB11/jdk/bin/keytool -import -alias
   alias-name -keystore Common-Component-installation-directory/uCPSB11/
   hjdk/jdk/lib/security/jssecacerts -file certificate-file -storetype JKS
   ```

   To import the certificates in Java, ensure that the truststore password includes six or more characters. In addition, ensure that the new alias name does not conflict with an existing alias name. Since the certificates used vary depending on the environment and configuration, import either or both RSA and ECDSA certificates into the Common Component truststore based on the certificates available in the Ops Center Administrator server.
3. (Optional) If you want to change the cipher suites to be used for communication with the Ops Center Administrator server, do the following:
   a. Open the `config_user.properties` file from the following location.

      In Windows (non-cluster): `Automation-software-installation-folder\conf`

      In Windows (cluster): `shared-folder_name\Automation\conf`

      In Linux: `Automation-software-installation-directory/conf`

b. Edit the `tls.client.cipherSuites` line. If the `tls.client.cipherSuites` line does not exist, add it.

   One of the cipher suites in the `tls.client.cipherSuites` line is used in the communication. Specify the cipher suites you want to use in the `tls.client.cipherSuites` line. If there are multiple cipher suites you want to use, specify the cipher suites separated by commas.

   For available cipher suites, see Cipher suites supported as a client (on page 256).

   For details about the `tls.client.cipherSuites` property, see Changing the system configuration (on page 94).

4. Restart the services by running the **`hcmds64srv`** command.

Setting up secure communication with an Ops Center Analyzer server

You can set up SSL communication to be used between the Ops Center Automator server and the Ops Center Analyzer server by using a self-signed certificate or a certificate issued by a certificate authority. You can also change the cipher suites to be used.

Before you begin

If you already set up SSL on the Ops Center Analyzer server, including creating the certificates, go to step 2. Otherwise, start at step 1.

Procedure

1. Set up SSL on the Ops Center Analyzer server. For details, see “Configuring an SSL certificate (Analyzer server)” in the *Hitachi Ops Center Analyzer Installation and Configuration Guide*.
2. Import the certificates into the Common Component truststore by running the following command:

   For Windows:

   ```
   Common-Component-installation-folder\bin\hcmds64keytool -import -alias
   alias-name -keystore Common-Component-installation-folder\uCPSB11
   \hjdk\jdk\lib\security\jssecacerts -file certificate-file -storetype JKS
   ```

   For Linux:

   ```
   Common-Component-installation-directory/uCPSB11/jdk/bin/keytool -import -alias
   alias-name -keystore Common-Component-installation-directory/uCPSB11/
   hjdk/jdk/lib/security/jssecacerts -file certificate-file -storetype JKS
   ```

   To import the certificates in Java, ensure that the truststore password includes six or more characters. In addition, ensure that the new alias name does not conflict with an existing alias name. Since the certificates used vary depending on the environment and configuration, import either or both RSA and ECDSA certificates into the Common Component truststore based on the certificates available in the Ops Center Analyzer server.

3. (Optional) If you want to change the cipher suites to be used for communication with the Ops Center Analyzer server, do the following:

   a. Open the `config_user.properties` file from the following location.

      In Windows (non-cluster): `*Automation-software-installation-folder*\conf`

      In Windows (cluster): `*shared-folder_name*\Automation\conf`

      In Linux: `*Automation-software-installation-directory*/conf`

   b. Edit the `tls.client.cipherSuites` line. If the `tls.client.cipherSuites` line does not exist, add it.

      One of the cipher suites in the `tls.client.cipherSuites` line is used in the communication. Specify the cipher suites you want to use in the `tls.client.cipherSuites` line. If there are multiple cipher suites you want to use, specify the cipher suites separated by commas.

      For available cipher suites, see Cipher suites supported as a client (on page 256).

      For details about the tls.`client.cipherSuites` property, see Changing the system configuration (on page 94).

4. Restart the services by running the **`hcmds64srv`** command.

Setting up secure communication with a VMware vCenter server

As with all web service connections that use secure communication, you must import the VMware vCenter Server root certificates to the Ops Center Automator Common Component truststore that Ops Center Automator references. However, if you plan to use the ESX cluster service templates, you must also install the VMware vCenter Server root certificates into the OS truststore in order to configure secure communication for the prerequisite software in the service templates. You can also change the cipher suites to be used.

> **Note:** If you do not plan to use the ESX cluster service templates, you do not need to complete this procedure.

Procedure

1. Download the VMware vCenter Server root certificates as follows:

   a. Using a web browser, access the vCenter user interface.

   b. In the right-side window, select **Download trusted root CA certificates**.

   c. Select a download location on the server where the Ops Center Automator Common Component truststore resides and confirm the download.

2. On the server with the Common Component truststore, go to the location in which you downloaded the zip file and unzip the file.

> **Note:** If the downloaded file does not have a .zip extension, change the extension to .zip.

- In Windows, the result is a `.certs` folder that contains both certificate files.
- In Linux, the includes a directory named `lin` that contains a file with a .0 extension (xxx.0).

3. Import the VMware vCenter Server root certificates into the Common Component truststore by running the following command:

   For Windows:

   ```
   Common-Component-installation-folder\bin\hcmds64keytool -import -alias
   alias-name -keystore Common-Component-installation-folder\uCPSB11
   \hjdk\jdk\lib\security\jssecacerts -file certificate-file -storetype JKS
   ```

   For Linux:

   ```
   Common-Component-installation-directory/uCPSB11/jdk/bin/keytool -import -alias
   alias-name -keystore Common-Component-installation-directory/uCPSB11/
   hjdk/jdk/lib/security/jssecacerts -file certificate-file -storetype JKS
   ```

   To import the certificates in Java, ensure that the truststore password includes six or more characters. In addition, ensure that the new alias name does not conflict with an existing alias name. Since the certificates used vary depending on the environment and configuration, import either or both RSA and ECDSA certificates into the Common Component truststore based on the certificates available in VMware vCenter Server.

4. Install the certificates into the OS truststore.

   In Windows:

   a. Right-click the file with the `.crt` extension and select **Install Certificate**.
      The Import Certificate Wizard opens.
   b. Select **Local Machine**, then click **Next**.
   c. Select **Place all certificates in the following store**.
   d. Click **Browse**, select **Trusted Root Certification Authorities**, then click **Finish**.
   e. Repeat steps a through d on the file with the `.crl` extension.

   In Linux:

   a. Copy the "xxx.0" file to the following directory:
      `/etc/pki/tls/certs`

5. (Optional) If you want to change the cipher suites to be used for communication with the VMware vCenter server, do the following:

Note: When you use the following service templates to communicate with VMware vCenter Server, the property in this step has no effect and you do not need to perform this step.

- Allocate Volumes, Fabric, and Datastore for ESXi Host
- Allocate Fabric Aware Volumes and Create Datastore for ESX Cluster
- Add Host to Cluster in vCenter
- Remove Host from Cluster in vCenter

a. Open the `config_user.properties` file from the following location.

   In Windows (non-cluster): `*Automation-software-installation-folder*\conf`

   In Windows (cluster): `*shared-folder_name*\Automation\conf`

   In Linux: `*Automation-software-installation-directory*/conf`

b. Edit the `tls.client.cipherSuites` line. If the `tls.client.cipherSuites` line does not exist, add it.

   One of the cipher suites in the `tls.client.cipherSuites` line is used in the communication. Specify the cipher suites you want to use in the `tls.client.cipherSuites` line. If there are multiple cipher suites you want to use, specify the cipher suites separated by commas.

   For available cipher suites, see Cipher suites supported as a client (on page 256).

   For details about the `tls.client.cipherSuites` property, see Changing the system configuration (on page 94).

6. Restart the services by running the **`hcmds64srv`** command.

Note: If you plan to use the ESX cluster service templates, you must also install Python as described in the *Hitachi Ops Center Automator User Guide*.

Setting up secure communication with external web servers

You must import the certificates into the Common Component truststore to enable SSL communication between the external web server and Ops Center Automator over the following web service connections. You can also change the cipher suites to be used.

- BNA
- Brocade FC switch
- DCNM
- ServiceNow
- Other web service connections

Procedure

1. Import the certificates into the Common Component truststore by running the following command:

For Windows:

```
Common-Component-installation-folder\bin\hcmds64keytool -import -alias alias-
name -keystore Common-Component-installation-folder\uCPSB11
\hjdk\jdk\lib\security\jssecacerts -file certificate-file  -storetype JKS
```

For Linux:

```
Common-Component-installation-directory/uCPSB11/jdk/bin/keytool  -import -alias
alias-name -keystore Common-Component-installation-directory/uCPSB11/
hjdk/jdk/lib/security/jssecacerts -file certificate-file  -storetype JKS
```

To import the certificates in Java, ensure that the truststore password includes six or more characters. In addition, ensure that the new alias name does not conflict with an existing alias name. Since the certificates used vary depending on the environment and configuration, import either or both RSA and ECDSA certificates into the Common Component truststore based on the certificates available in the external web server. Since the certificates used vary depending on the environment and configuration, import either or both RSA and ECDSA certificates into the Common Component truststore based on the certificates available in the external web server.

2. (Optional) If you want to change the cipher suites to be used for communication with the external web servers, do the following:

   Note: For web service connections to Brocade FC switch with a category of FOS_PrimarySwitch, add the following cipher suites to use for communication with FOS.

   - TLS_RSA_WITH_AES_256_CBC_SHA256
   - TLS_RSA_WITH_AES_128_CBC_SHA256

   a. Open the `config_user.properties` file from the following location.

      In Windows (non-cluster): `Automation-software-installation-folder\conf`

      In Windows (cluster): `shared-folder_name\Automation\conf`

      In Linux: `Automation-software-installation-directory/conf`

   b. Edit the `tls.client.cipherSuites` line. If the `tls.client.cipherSuites` line does not exist, add it.

      One of the cipher suites in the `tls.client.cipherSuites` line is used in the communication. Specify the cipher suites you want to use in the `tls.client.cipherSuites` line. If there are multiple cipher suites you want to use, specify the cipher suites separated by commas.

      For available cipher suites, see Cipher suites supported as a client (on page 256).

      For details about the `tls.client.cipherSuites` property, see Changing the system configuration (on page 94).

3. Restart the services by running the **`hcmds64srv`** command.

Next steps

- For additional information on the security settings for another product, see the associated product documentation.
- To obtain server certificates, see the associated product documentation for information on accessing server certificates.
- After upgrading DCNM, the server certificate is initialized. You must do the steps described in "Restoring the certificates after an upgrade" in the *Cisco DCNM Installation and Upgrade Guide for SAN Deployment*.
- If you use DCNM 11.5, create a certificate by specifying an appropriate hostname to Common Name by following the steps described in "Certificates" in the *Cisco DCNM Installation and Upgrade Guide for SAN Deployment*.
- If you use a Brocade FC switch, complete the SSL settings by following the steps described in "Managing the Security Certificates Using the secCertMgmt Command" in the *Brocade Fabric OS Administration Guide*.

Verifying the server certificate expiration date

You can verify the expiration date for an SSL certificate to ensure that your certificate has not expired. You must ensure that the management server certificate does not expire to maintain secure communication with managed servers.

To verify the expiration of the Common Component server certificate, run the following command:

For Windows OS:

```
Common-Component-installation-folder\bin\hcmds64keytool -printcert -
v -file certificate-file
```

For Linux OS:

```
Common-Component-installation-directory/uCPSB11/jdk/bin/keytool -
printcert -v -file certificate-file
```

Note: The expiration date of a self-signed server certificate is not verified at the connection between servers. If you must verify the expiration date of a certificate at the connection of the Ops Center Automator server and web servers, use the certificate issued by the certificate authority. Then, import the certificates not only for the server, but also for the certificate authority, and intermediate certificate authority.

Changing the Common Component truststore password

To change the Common Component truststore (`ldapcacerts` or `jssecacerts`) password, use the **`hcmds64keytool`** utility (for Windows) or the **`keytool`** utility (for Linux).

Before you begin

Make sure you have the truststore password.

Procedure

1. Run the following command.

   For Windows:

   ```
   Common-Component-installation-folder\bin\hcmds64keytool  -keystore truststore-file-name -storepasswd
   ```

   For Linux:

   ```
   Common-Component-installation-directory/uCPSB11/jdk/bin/keytool -keystore truststore-file-name -storepasswd
   ```

   Where `keystore` is the truststore file path where the certificate is stored.

   The truststore (`ldapcacerts` or `jssecacerts`) file paths are as follows.

   `jssecacerts`

   - For Windows:

     `Common-Component-installation-folder``\uCPSB11\hjdk\jdk\lib\security\jssecacerts`

   - For Linux:

     `Common-Component-installation-directory``/uCPSB11/hjdk/jdk/lib/security/jssecacerts`

   `ldapcacerts`

   - For Windows:

     `Common-Component-installation-folder``\conf\sec\ldapcacerts`

   - For Linux:

     `Common-Component-installation-directory``/conf/sec/ldapcacerts`

2. Specify the current truststore password.
3. Specify a new truststore password (minimum of 6 characters).
4. Specify the new truststore password again.

Deleting Common Component truststore certificates

To delete the certificates imported into the Common Component truststore (ldapcacerts or jssecacerts), use the **`hcmds64keytool`** utility (for Windows) or the **`keytool`** utility (for Linux).

Before you begin

Check the following information:

- Alias name of the certificate to be deleted
- Truststore password

Procedure

1. Run the following command.

   In Windows

   ```
   Common-component-installation-folder\bin\hcmds64keytool -delete -alias alias-name -keystore truststore-file-name
   ```

   In Linux

   ```
   Common-component-installation-directory/uCPSB11/jdk/bin/keytool -delete -alias alias-name -keystore truststore-file-name
   ```

   `alias`
   Specify the certificate alias name.

   `keystore`
   Specify the truststore file path where the certificate is stored.

   The truststore (`ldapcacerts` or `jssecacerts`) file paths are as follows.

   `jssecacerts`

   - For Windows:

     `Common-Component-installation-folder\uCPSB11\hjdk\jdk\lib\security\jssecacerts`

   - For Linux:

     `Common-Component-installation-directory/uCPSB11/hjdk/jdk/lib/security/jssecacerts`

   `ldapcacerts`

   - For Windows:

     `Common-Component-installation-folder\conf\sec\ldapcacerts`

   - For Linux:

     `Common-Component-installation-directory/conf/sec/ldapcacerts`

   Note: You are prompted to enter the truststore password in interactive mode.

Audit logging

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

Configuring the audit log

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

For Windows, the audit log data is output to the event log files (application log files). For Linux, the data is output to the `syslog` file.

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

Categories	Description
StartStop	Events indicating starting or stopping of hardware or software: ▪ Starting or shutting down an OS ▪ Starting or stopping a hardware component (including micro components) ▪ Starting or stopping software on a storage system or SVP, and products that use the Common component
Failure	Events indicating hardware or software failures: ▪ Hardware failures ▪ Software failures (memory error, etc.)
LinkStatus	Events indicating link status among devices: Whether a link is up or down
ExternalService	Events indicating the results of communication with external services: ▪ Communication with an external server, such as NTP or DNS ▪ Communication with a management server (SNMP)
Authentication	Events indicating that a device, administrator, or end user succeeded or failed in connection or authentication: ▪ Fibre Channel login ▪ Device authentication (Fibre Channel - Security Protocol authentication, iSCSI login authentication, SSL server/ client authentication) ▪ Administrator or end user authentication

Categories	Description
AccessControl	Events indicating that a device, administrator, or end user succeeded or failed in gaining access to resources: ▪ Access control for devices ▪ Access control for the administrator or end users
ContentAccess	Events indicating that attempts to access important data succeeded or failed: ▪ Access to important files on NAS or to contents when HTTP is supported ▪ Access to audit log files
ConfigurationAccess	Events indicating that the administrator succeeded or failed in performing an allowed operation: ▪ Reference or update of the configuration information ▪ Update of account settings including addition or deletion of accounts ▪ Security configuration ▪ Reference or update of audit log settings
Maintenance	Events indicating that a performed maintenance operation succeeded or failed: ▪ Addition or deletion of hardware components ▪ Addition or deletion of software components
AnomalyEvent	Events indicating that an anomaly, such as a threshold being exceeded, occurred: ▪ A network traffic threshold was exceeded ▪ A CPU load threshold was exceeded ▪ Pre-notification that a limit is being reached or a wraparound occurred for audit log data temporarily saved internally
	Events indicating that abnormal communication occurred: ▪ SYN flood attacks to a regularly used port, or protocol violations ▪ Access to an unused port (port scanning, etc.)

Enabling audit logging

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

Note:

- If the Ops Center Automator server is installed by using a virtual appliance, the audit log is enabled by default.

  If the Ops Center Automator server is installed by using the installer, the audit log is disabled by default. Enable the settings as required.

- A large volume of audit log data might be output. Change the log file size and back up or archive the generated log files accordingly.

Procedure

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

   In Windows:

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

   In Linux:

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

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

   Note: When you use Ops Center Automator in a cluster environment, you must edit the `auditlog.conf` file on both the active and standby nodes.

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

Settings in the auditlog.conf file

You can set the following values in the `auditlog.conf` file.

`Log.Facility` (Linux only)

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

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

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

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

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

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

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

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

`Log.Event.Category`

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

When specifying multiple categories, use commas (`,`) to separate them. In this case, do not insert spaces between categories and commas. If `Log.Event.Category` is not specified, audit log data is not output. `Log.Event.Category` is not case-sensitive. If an invalid category name is specified, the specified file name is ignored.

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

`Log.Level` (Effective in Windows only)

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

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

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

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

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

Specifiable value for `Log.Level`	Levels displayed in the event log
`0`	Error
`1`	
`2`	

Specifiable value for `Log.Level`	Levels displayed in the event log
3	
4	Warning
5	Information
6	
7	

Sample auditlog.conf file

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

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

# Specify the event category.
# You can specify any of the following:
# StartStop, Failure, LinkStatus, ExternalService,
# Authentication, AccessControl, ContentAccess,
# ConfigurationAccess, Maintenance, or AnomalyEvent.
Log.Event.Category StartStop,Failure,LinkStatus,ExternalService,Authentication,
AccessControl,ContentAccess,ConfigurationAccess,Maintenance,AnomalyEvent
# Specify an integer for Severity. (specifiable range: 0-7)
Log.Level 6
```

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

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

Format of data output to the audit log

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

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

In Windows:

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

In Linux:

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

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

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

```
$ActionFileDefaultTemplate RSYSLOG_SyslogProtocol23Format
```

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

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

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

Item*	Description
location-identification-information	Location identification information.
FQDN	Fully qualified domain name.
redundancy-identification-information	Redundancy identification information.
agent-information	Agent information.
request-source-host	Host name of the request sender.
request-source-port-number	Port number of the request sender.
request-destination-host	Host name of the request destination.
request-destination-port-number	Port number of the request destination.
batch-operation-identifier	Serial number of operations through the program.
log-data-type-information	Fixed to `BasicLog` or `DetailLog`.
application-identification-information	Program identification information.
reserved-area	Not output. This is a reserved space.
message-text	The contents vary according to the audit events. Characters that cannot be displayed are output as asterisks (`*`).
*: Some items are not output for some audit events.	

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

```
CELFSS,1.1,3,KNAE20002-I,2021-09-03T21:31:56.8+09:00,HAD,managementhost,
Authentication,Success,subj:uid=sysadmin,autoAuth,Login,BasicLog,HAD,"Login was
successful."
```

Changing the system configuration

You can configure various Ops Center Automator settings such as logs and tasks by editing the `config_user.properties` file. Note that after you change and save the file, you must restart the Ops Center Automator engine web service.

You can change the following settings by editing this file:

- Log file configuration (specify the number of logs to store).
- Task and history configuration (specify the number of tasks and task histories to store).
- Configuration regarding remote command execution (SSH/telnet port number)
- Configuration information for email notification.
- Configuration information regarding Service Builder.
- Connection timeout value setting.
- Maximum number of concurrent plug-in runs.

The file is located in the following folder: *`Automation-software-installation-folder`*`\conf`

The file uses the following format:

`specification-key-name=setting`

When editing the properties file, take note of the following:

- Lines that begin with `#` are treated as comments
- Blank lines are ignored
- The encoding is ISO 8859-1
- The contents are case sensitive
- To specify `\` in a character string, it must be written `\\`.
- If value that is not valid is entered for a setting, it is set to the default value and message KNAE02022-W is sent to the integrated trace log and public log
- If the same specification key is entered multiple times in a file, the last one that is specified takes effect

Table 12 Settings in the `config_user.properties` file

Category	Key name	Setting	Values	Default value
HTTP connection port number	`server.http.port`	Specifies the port number to be used for HTTP communication between the Ops Center Automator server and the Common Component.	0-65535	22015
Logs[1]	`logger.message.server.MaxBackupIndex`	Specifies the maximum number of log backup files for a server.	1 - 16	7

Category	Key name	Setting	Values	Default value
	`logger.message.server.MaxFileSize`	Specifies the maximum log file size (in KB) for a server.	4 - 2097151	1024
	`logger.message.command.MaxBackupIndex`	Specifies the maximum number of log backup files for a command.	1 - 16	7
	`logger.message.command.MaxFileSize`	Specifies the maximum log file size (in KB) for a command.	4 - 2097151	1024
	`logger.TA.MaxFileSize`	Specifies the maximum log file size (in KB) for a task.	4 - 2097151	10240
Task management	`tasklist.autoarchive.taskRemainingPeriod`	Specifies the period (in days) for tasks that have ended to remain in the task list.	1 - 90	7
	`tasklist.autoarchive.executeTime`	Specifies the time to run the automatic archiving task.	00:00:00 - 23:59:59	04:00:00
	`tasklist.autoarchive.maxTasks`	Specifies the maximum number of tasks to keep in the task list.	100 - 5000	5000
	`tasklist.autodelete.maxHistories`	Specifies the maximum number of history entries to retain.	100 - 30000	30000
Repeats	`foreach.max_value`	Specifies the maximum number of concurrent tasks that can be run by the Repeated Execution Plug-in.	1 - 99	3
Remote connection port number	`ssh.port.number`	Specifies the SSH port number of the target device.	0 - 65535	22
	`telnet.port.number`	Specifies the Telnet port number of the target device	0 - 65535	23

Category	Key name	Setting	Values	Default value
SSH cryptographic algorithms	`ssh.disable.kexAlgorithms`	Specifies comma-separated values of key exchange algorithms to disable for agentless connections (SSH). It is case-sensitive. Whitespace characters (half-width space) before and after the comma are ignored.	Character string	diffie-hellmangroup14-sha1
	`ssh.disable.ciphers`	Specifies comma-separated values of Ciphers to disable for agent-less connections (SSH). It is case-sensitive. Whitespace characters (half-width space) before and after the comma are ignored.	Character string	3des-cbc,aes128-cbc,aes192-cbc,aes256-cbc
	`ssh.disable.macs`	Specifies comma-separated values of MACs to disable for agentless connections (SSH). It is case-sensitive. Whitespace characters (half-width space) before and after the comma are ignored.	Character string	hmac-sha1,hmac-sha1-96,hmac-sha1-etm@openssh.com
	`ssh.disable.publicKeyAlgorithms`	Specifies comma-separated values of public key algorithms for the host key to disable for agent-less connections (SSH). It is case-sensitive. Whitespace characters (half-width space) before and after the comma are ignored.	Character string	"" (null character)

Category	Key name	Setting	Values	Default value
TLS	`tls.client.cipherSuites`	Specifies comma-separated values of cipher suites to be used when connecting to Common Services and web service connection servers. You can specify cipher suites for TLS 1.2 and TLS 1.3. It is case-sensitive. Whitespace characters (half-width space) before and after the comma are ignored.	String	None[2]
General command Remote command File-transfer Terminal connection	`plugin.stdoutSize.wmi`	If the total size of the standard output and the standard error exceeds the property value, a plug-in error occurs. Note: The property value unit is in kilobytes (KB). This property is applied during the plug-in procedure, when the following conditions are met. - Connection target host is Windows - Execution target plug-in is either a General Command Plug-in or the Custom Plug-in	1 - 1024	100

Category	Key name	Setting	Values	Default value
		In Windows OS, the plug-in can continue to run, even if the number of linefeeds exceeds 65535 or more. To take advantage of this feature, you must to set the property value accordingly. For example, if this property is set to 100 KB (default value), the plug-in cannot process the maximum number of linefeeds of 65535 or more. The plug-in stops running after it reaches the 100 KB limit.		
	`plugin.stdoutSize.ssh`	If the total size of the standard output and the standard error exceeds the property value, a plug-in error occurs. Note: The property value unit is in kilobytes (KB). This property is applied during the plug-in procedure when the following two major conditions are met. [Condition (1) (Note: The following target-based conditions must be met).] - Connection target host is Linux OS. - Execution target plug-in is a General Command Plug-in or the custom plug-in.	1 - 1024	100

Category	Key name	Setting	Values	Default value
		[Condition (2) (Note: The following protocol and plug-in conditions must be met.)] - Connection protocol is SSH. - Execution target plug-in is Terminal Connect Plug-in or Terminal Command Plug-in.		
	`plugin.stdoutSize.telnet`	If the total size of the standard output and the standard error exceeds the property value, a plug-in error occurs. Note: The property value unit is in kilobytes (KB). This property is applied during the plug-in procedure when the following conditions are met. - Connection protocol is Telnet. - The target plug-in is either Terminal Connect Plug-in or Terminal Command Plug-in.	1 - 1024	100

Category	Key name	Setting	Values	Default value
	`plugin.remoteFileAccess.retry.times`	Specifies the number of tries for a file manipulation command run internally by a content plug-in or file-transfer plug-in. The time between tries is fixed at 100 ms. If a temporary file access error occurs, trying the command again might result in a successful procedure. However, if the file access error is not recovered, extra time is needed for further tries until the plug-in stops. Specify this property in an environment in which file access errors occur even if there are no problems with disks.	0 - 100	0
	`ssh.privateKeyFile`	Specifies the absolute path of the private key file if public key authentication is used for SSH connections.	0 - 255 characters	"" (null character)
	`plugin.localMode`	Specifies whether to enable or disable local execution mode. true: enabled false: disabled	true/false	true

Category	Key name	Setting	Values	Default value
Terminal connection	`plugin.terminal.prompt.account`	Specifies the regular expression used to detect the user ID waiting state (1-1,024 characters). If the standard output and standard error output match the specified regular expression, the Terminal Connect Plug-in (Telnet is specified for the protocol) determines that a user ID must be entered, and then it enters a user ID.	Character string that can be used in regular expression patterns	logon|Logon Name|Username|UserName
	`plugin.terminal.prompt.password`	Specifies the regular expression used to detect the password waiting state (1-1,024 characters). If the standard output and standard error output match the specified regular expression, the Terminal Connect Plug-in (Telnet is specified for the protocol) determines that a password must be entered, and then it enters a password.	Character string that can be used in regular expression patterns	password|Password|PassWord
	`telnet.connect.wait`	Specifies the waiting time (in seconds) until the standard output is returned after an Telnet connection is established with the target device.	1 - 600	60

Category	Key name	Setting	Values	Default value
Remote command	`plugin.remoteCommand.executionDirectory.wmi`	Specifies the path of the execution folder that contains the custom plug-in to run if the target host is running Windows. The execution folder must be created in advance. If the "Execution Mode" of the custom plug-in is "Script", the total string length of the specified value and the script file name do not exceed 140 characters. If the length exceeds 140 characters, transferring the script might fail. In addition, because the script file name must be specified in 90 characters or less, this value specified must be within 50 characters.	Character string of 0-128 characters	"" (null character)
	`plugin.remoteCommand.executionDirectory.ssh`	Specifies the path of the execution folder to run the custom plug-in if the OS of the target host is Linux OS. The execution folder must be created in advance.	Character string of 0-128 characters	"" (null character)

Category	Key name	Setting	Values	Default value
	`plugin.remoteCommand.workDirectory.ssh`	Specifies the working folder used when the file transfer plug-in or the custom plug-in is run if the OS of the target host is Linux OS. Enter a folder or a symbolic link as an absolute path (1 - 128 characters). In addition, the symbolic link can be included as the layer of the path.	1 - 128	/tmp/Hitachi_AO
Retry remote host connection	`ssh.connect.retry.times`	Specifies the number of tries in the event of a failed SSH connection to the target device.	0 - 100	3
	`ssh.connect.retry.interval`	Specifies the time (in seconds) between tries in the event of a failed SSH connection to the target device.	1 - 600	10
	`wmi.connect.retry.times`	Specifies the number of tries in the event of a failed WMI connection to the target device.	0 - 100	3
	`wmi.connect.retry.interval`	Specifies the time (in seconds) between tries in the event of a failed WMI connection to the target device.	1 - 600	10
	`telnet.connect.retry.times`	Specifies the number of tries in the event of a failed Telnet connection to the target device.	0 - 100	3
	`telnet.connect.retry.interval`	Specifies the time (in seconds) between tries in the event of a failed Telnet connection to the target device.	1 - 600	10

Category	Key name	Setting	Values	Default value
Retry email notification	`mail.notify.retry.times`	Specifies the number of tries in the event of a failure of the notification function to send an email.	0 - 100	3
	`mail.notify.retry.interval`	Specifies the time (in seconds) between tries in the event of a failure of the notification function to send an email.	1 - 600	10
	`mail.plugin.retry.times`	Specifies the number of tries, if a failure occurs, to send email in the Email Notification Plug-in.	0 - 100	3
	`mail.plugin.retry.interval`	Specifies the time (in seconds) between tries in the event of a failure of the Email Notification Plug-in to send an email.	1 - 600	10
Audit Log	`logger.Audit.command.useLoginUserID`	Specifies whether to output the Ops Center Automator logon user ID, in place of the user ID, to the subject identification information for the audit log when a command is run.	true/false	false
Window update	`client.events.refreshinterval`	Specifies the update time (in seconds) for events.	0 - 65535	5

Category	Key name	Setting	Values	Default value
Service Builder	`client.editor.sso.timeout.disable`	Specifies whether to always disable timeout on the Service Builder windows except for the View Flow window and the Create/Edit External Resource Provider window, regardless of the Auto-refresh setting in Ops Center Common Services.	true/false	false
	`client.editor.upload.maxfilesize`	Specifies the maximum file size (in MB) that can be uploaded to the server from the terminal used for operating Ops Center Automator by using the Service Builder **Edit** window.	1 - 10	3
	`client.editor.canvas.maxwidth`	Specifies the maximum size (in px) of the width of Flow view.	3600 - 10000	3600
	`client.editor.canvas.maxhigh`	Specifies the maximum size (in px) of the height of Flow view.	2400 - 30000	2400
	`server.editor.step.perTemplate.maxnum`	Specifies the maximum number of steps per 1 service template.	320 - 40000	320
	`server.editor.step.perLayer.maxnum`	Specifies the maximum number of steps per 1 layer.	80 - 10000	80
	`server.editor.publicProperty.perTemplate.maxnum`	Specifies the maximum number of service properties per service template.	100 - 2000	1000

Category	Key name	Setting	Values	Default value
	`server.editor.propertyGroup.perTemplate.maxnum`	Specifies the maximum number of property groups per service template.	5 - 1000	500
Debugger	`tasklist.debugger.autodelete.taskRemainingPeriod`	Specifies the maximum number of property groups per service template.	1 - 90	7
	`client.debugger.tasklog.maxfilesize`	Specifies the size of task logs (KB) visible in the Task Log tab.	4 - 10240	1024
	`logger.debugger.TA.MaxFileSize`	Specifies the maximum log file size (KB) for a debug task.	4 - 2097151	10240
LongRunningTask verify interval threshold	`server.longRunning.check.interval`	LongRunningTask verify the threshold between times (in minutes)	0 - 20160	2880
LongRunning Monitor interval	`server.longRunning.monitor.interval`	LongRunning monitor interval (in seconds)	1 - 3600	60
Web Client	`plugin.http.connect.timeout`	Specifies the timeout value (in seconds) when the HTTP/HTTPS connection is established. If 0 is specified, timeout does not occur.	0 - 3600	60
	`plugin.http.read.timeout`	Specifies the timeout value (in seconds) when reading the data after the HTTP/HTTPS connection is established. If 0 is specified, timeout does not occur.	0 - 86400	600

Category	Key name	Setting	Values	Default value
Plug-in run	plugin.threadPoolSize	Specify the maximum number of concurrent plug-in runs. When using only the built-in service templates, you can set this property value to 100. To also use a custom service template, make sure to evaluate the behavior after changing the default value and make sure that no problem occurs before you move to the production process.	1-100	10
SSO	sso.https.certification	Specifies whether to verify the certificates in SSL communication with Common Services.	true/false	false
SSH file transfer protocol	plugin.sftp.enable	Specifies whether to use SFTP when sending/receiving files using SSH in the File Transfer Plug-in and Custom plug-in. If true, SFTP is used, and if false, SCP is used.	true/false	false

1. You set log output thresholds for tasks in Service Share Properties.

   Example

   ```
   logger.message.server.MaxBackupIndex = 7
   logger.message.server.MaxFileSize = 1024
   logger.message.command.MaxBackupIndex = 7
   logger.message.command.MaxFileSize = 1024
   logger.TA.MaxFileSize = 1024
   tasklist.autoarchive.taskRemainingPeriod = 7
   tasklist.autoarchive.executeTime = 04:00:00
   tasklist.autoarchive.maxTasks = 5000
   tasklist.autodelete.maxHistories = 30000
   mail.notify.retry.times = 3
   mail.notify.retry.interval = 10
   mail.plugin.retry.times = 3
   ```

Category	Key name	Setting	Values	Default value

```
mail.plugin.retry.interval = 10
client.events.refreshinterval = 5
```

2. By default, there is no `tls.client.cipherSuites` line, and Ops Center Automator works as if the following value was set:

   ```
   TLS_AES_256_GCM_SHA384,TLS_AES_128_GCM_SHA256,TLS_CHACHA20_POLY1305_SHA256,
   TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,
   TLS_RSA_WITH_AES_256_GCM_SHA384,TLS_RSA_WITH_AES_128_GCM_SHA256
   ```

   If you want to change cipher suites from the default, add the `tls.client.cipherSuites` line if it does not exist, and specify the comma-separated values of cipher suites you want to use in the `tls.client.cipherSuites` line. For available cipher suites, see Cipher suites supported as a client (on page 256).

Configuring the performance mode

Ops Center Automator has two modes of operation: Standard mode and High performance mode. High performance mode is suitable for multiple task runs and uses more resources than Standard mode.

To switch between Standard mode and High performance mode, use the **`changemode`** command (on page 217).

Note: When you run multiple Online migration with Configuration Manager tasks, you must operate in high performance mode. For details, see “Online migration with Configuration Manager service templates” in the *Hitachi Ops Center Automator User Guide*.

Configuring email notifications

You configure email notification settings so that when a task fails ("Failed" status) or a task detects an error ("In Progress (with Error)" status), you receive email notification. You can configure the email address, title, and type of information you receive about the failure or problem.

Note: To ensure that email notifications are enabled for the system, you must configure the system parameters in the Administration tab. For more detailed information, see the *Hitachi Ops Center Automator User Guide*.

The email definition file, `mailDefinition`, is in XML format and is located in the following folder:

Automation-software-installation-folder`\conf`

The definition file uses the following format:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes" ?>
<mail xmlns="http://www.example.com/products/it/software/xml/automation/conf/
mailDefinition">
<title>email-title</title>
<body>email-body</body> </mail>
```

When editing the file, take note of the following:

- A read error occurs if the definition file for email notification is missing, or is not well-formed XML. In this case, the email is sent with the default title and body.
- If you specify tags outside of <mail>, <title>, and <body>, even if the tags are well-formed XML, the tags and their content are ignored.
- An empty string is specified if the value of a <title> or <body> tag is omitted.
- The <mail> tag cannot be omitted. If it is omitted, the format is not valid and a read error occurs.
- All entries are case sensitive.

To modify the settings, edit the email-title and email-body sections in the `mailDefinition` file.

Table 13 Email notification settings

Setting	XML element	Character string length	Default value
Title of email to use for email notifications	<title>	Character string of 0-9,999 bytes	[Ops Center Automator] $TASK_NAME$ has changed to $TASK_STATUS$
Body of email to use for email notifications	<body>	Character string of 0-9,999 bytes	Service Group Name:$SERVICE_GROUP_NAME$ Task Name: $TASK_NAME$ User Name: $USER_NAME$ Task Detail: $TASK_DETAIL_URL$

Table 14 XML entity references

Character you want in the email	Character string to enter
&	&amp;
<	&lt;
>	&gt;
"	&quot;
'	&apos;

Table 15 Embedded characters for email notification

Embedded characters	Item	Remarks
$SERVICE_GROUP_NAME$	Service group name	Set to the character string representing the service group name.
$TASK_NAME$	Task name	Set the task name according to the format in the task properties.
$TASK_ID$	Task ID	
$TASK_KIND$	Task type	
$SERVICE_NAME$	Service name	
$TASK_TAGS$	Tag of the task	
$TASK_STATUS$	Task status	
$EXECUTION_DATE$	Date and time the process was run	
$PLANNED_START_DATE$	Planned date and time of start	
$START_DATE$	Actual date and time of start	
$END_DATE$	Date and time of end	
$USER_NAME$	User who runs the process	
$SCHEDULE_PERIOD$	Scheduled execution period	
$SCHEDULE_TIME$	Scheduled execution time	
$SCHEDULE_TIME$	Date execution was scheduled to start	
$TASK_DETAIL_URL$	URL of the Task Detail window	Set to a URL starting with http.

Changing the password policy

You configure various Ops Center Automator settings related to user password conditions and locks by editing the `security.conf` file. This enables you to customize your security settings to match your specific password policy.

The file is located in the following folder:

Common-Component-installation-folder\conf\sec

The file uses the following format:

specification-key-name=setting

Note: When you use Ops Center Automator in a cluster environment, you must edit the `security.conf` file on both the active and standby nodes.

When editing the file, you specify one specification key and setting per line. The following shows the default state of the security definition file:

```
# This is the minimum length of the password
# (minimum: 1 -256 characters)
password.min.length=4

# This is the minimum number of uppercase characters included in the
password
# (minimum: 0-256 characters, character type: A-Z)
password.min.uppercase=0

# This is the minimum number of lowercase characters included in the
password
# (minimum: 0-256 characters, character type: a-z)
password.min.lowercase=0

# This is the minimum number of numeric characters included in the
password
# (minimum: 0-256 characters, character type: 0-9)
password.min.numeric=0

# This is the minimum number of symbolic characters included in the
password
# (minimum: 0-256 characters, character type: ! # $ % & ' ( ) * +
- . = @ \ ^ _ |)
password.min.symbol=0

# This specifies whether the user ID can be used for the password
# (true = cannot use the user ID, false = can use the user ID)
password.check.userID=false

# This is the minimum number of login failures before an account is
locked
# (minimum: 0-10 times)
account.lock.num=0
```

Table 16 Settings in the `security.conf` file

Key name	Setting	Settable values	Default value
`password.min.length`	Specifies the minimum number of characters in a password.	1 - 256	4

Key name	Setting	Settable values	Default value
`password.min.uppercase`	Specifies the minimum number of uppercase letters that must be included in the password. If 0 is specified, there are no constraints on the number of uppercase letters.	0 - 256	0
`password.min.lowercase`	Specifies the minimum number of lowercase letters that must be included in the password. If 0 is specified, there are no constraints on the number of lowercase letters.	0 - 256	0
`password.min.numeric`	Specifies the minimum number of numeric characters that must be included in the password. If 0 is specified, there are no constraints on the number of numeric characters.	0 - 256	0
`password.min.symbol`	Specifies the minimum number of symbols that must be included in the password. If 0 is specified, there are no constraints on the number of symbols.	0 - 256	0
`password.check.userID`	Specifies whether to prevent the password from being the same as the user ID.	▪ true: prevent this ▪ false: allow this	false

Key name	Setting	Settable values	Default value
`account.lock.num`	Specifies the number of consecutive failed logons before the account is automatically locked. If 0 is specified, the account is not automatically locked after failed logon tries.	0 - 10	0

About account locking

Account locking is the locking (temporary disabling) of a user account. By enabling account locking, you can reduce the risk of unauthorized access from third parties. If you are managing user accounts by using a management server, we recommend that you enable account locking.

In Common Component products, you can automatically lock user accounts that fail to log on to the GUI many times in a row. To enable account locking, you must set the account locking policy (the number of consecutive, unsuccessful login attempts before accounts are locked).

Tip: As a way to lock an account, you can change the lock status of a user account from the GUI.

Only users with the `Admin` (user management) permission can change the lock status.

Caution:

- Account locking cannot be performed on `System` accounts when initially installing Common Component products. `System` accounts are set with `Admin` permissions for all Common Component products. If you want to set account locking for `System` accounts to improve security, you must change the settings.
- If an external authentication server is used to authenticate users, the settings on the external authentication server are used to control automatic locking.

About account locking policies

An account locking policy is the number of consecutive, unsuccessful login attempts before automatically locking (temporarily disabling) user accounts that fail to log in to the GUI many times in a row.

When you set an account locking policy, it is immediately applied to all Common Component products that use Single Sign-On functionality. For example, if you set the number of consecutive failed login attempts to 3 and a user fails to log in to Ops Center Automator three times, the user account is automatically locked.

Setting account locking policies

You can set an account locking policy for Common Component products in the `security.conf` file.

Procedure

1. Edit the `security.conf` file.

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

   In Windows:

   Common-Component-installation-folder`\conf\sec\security.conf`

   In Linux:

   Common-Component-installation-directory`/conf/sec/security.conf`

2. Set the `account.lock.num` parameter.

   Note: When you use Ops Center Automator in a cluster environment, you must edit the `security.conf` file on both the active and standby nodes.

   Specify the number of consecutive failed login attempts required to trigger automatic account locking. Specify a value from 0 to 10. If a user makes the specified number of unsuccessful login attempts, the account will be locked. If you specify 0, any number of unsuccessful login attempts is allowed.

   Default: 0

   Caution:

   - If you change the number of consecutive failed login attempts, the new value takes effect from the first failed login after the change. If a user is currently logged in and you attempt to login using his or her account, but you fail the specified number of times, his or her user account will be locked. However, the user can continue to perform operations while still logged in.

   - You can also set an account locking policy from the GUI. However, if the system is in a cluster configuration, the settings from the GUI are applied only to the executing node. To apply the settings to the standby node, switch the nodes, and then specify the same settings.

Result

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

Automatically locking the System account

To automatically lock the `System` accounts, change the settings in the `user.conf` file.

Procedure

1. Stop the Common Component product services.
2. Open the `user.conf` file.

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

   - In Windows:

     Common-Component-installation-folder\conf\user.conf

   - In Linux:

     Common-Component-installation-directory/conf/user.conf

   If the `user.conf` file does not exist, create it.

   > **Note:** When you use Ops Center Automator in a cluster environment, you must edit the `user.conf` file on both the active and standby nodes.

3. Use the following format to specify the `account.lock.system` property:

   ```
   account.lock.system=true
   ```

4. Start the Common Component product services.

Result

Account locking is applied to `System` accounts for all Ops Center products.

Unlocking accounts

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

Before you begin

- Log in as a user with Administrator permissions (for Windows) or as a root user (for Linux).
- Confirm that the locked user account has `Admin` permissions

  If the user account does not have `Admin` permissions, another user whose account has User Management Admin permissions must unlock the account.
- Check the user ID and password of the locked user account.

Procedure

1. Use the `hcmds64unlockaccount` command to unlock the account.

In Windows:

```
Common-Component-installation-folder\bin
\hcmds64unlockaccount [/useruser-ID /pass password]
```

In Linux:

```
Common-Component-installation-directory/bin/
hcmds64unlockaccount [-user user-ID -pass password]
```

If the command is executed without specifying the `user` option or the `pass` option, you will be prompted to enter a user ID and password.

Caution: If any symbols are used in the user ID or password, you must escape these symbols on the command line.

- In Windows:

  If the user ID or password ends with a backslash (`\`), use another backslash (`\`) to escape that backslash (`\`).

  Also, if the user ID or password includes an ampersand (`&`), vertical bar (`|`), or caret (`^`), enclose each character with a double quotation mark (`"`), or use a caret (`^`) to escape the symbols.

- In Linux:

  Use a backslash (`\`) to escape each character.

Operating systems supporting remote connections

The following OS or versions are supported as a target of remote connections. If the OS of the target is Windows, SMB and RPC are used to connect to the target. Otherwise, SSH is used to connect to the target. When using Terminal Connect Plug-in to connect to the target, Telnet or SSH is used. SSH protocol version 2 is supported.

- Windows
  - Windows Server 2016 Standard
  - Windows Server 2016 Datacenter
  - Windows Server 2019 Standard
  - Windows Server 2019 Datacenter
  - Windows Server 2022 Standard
  - Windows Server 2022 Datacenter
- The following SMB versions are used for connections from Ops Center Automator to a Windows connection target host.

Ops Center Automator OS	Connection target host OS	SMB version	Encrypted communication
Windows	Windows	v1, v2, v3	Supported[1]
Linux	Windows	v1, v2	Not supported[2]

1. If SMB version v2 or v3 is enabled and the "Encrypt data access" setting is enabled on the Ops Center Automator and connection target host, the communication is encrypted. The available cryptographic algorithms depend on the Ops Center Automator and connection target host to use.
2. The "Encrypt data access" setting must be disabled on the connection target host. If you test the connection in the Add/Edit Agentless Remote Connection window with the setting enabled on the connection target host, the KNAE02137-E message appears.

- Linux
  - Red Hat Enterprise Linux versions 8.8, 8.10, 9.2, 9.4
  - Oracle Linux versions 8.8, 8.10, 9.2, 9.4

The commands (other than the commands specified in the OS of the operation-target device) run by custom plug-ins, General Command Plug-in, and File-Transfer Plug-in when the OS is Linux are shown below. Before you use these plug-ins, make sure that these commands have already been installed.

- Custom plug-in

  /bin/bash, /usr/bin/id, /bin/echo, /usr/bin/find, /usr/bin/test, /bin/mkdir, /bin/chmod, /bin/gunzip, /bin/tar, /bin/rm, /bin/cp, /bin/uname, /bin/su

- General Command Plug-in

  /bin/bash, /usr/bin/id, /bin/echo, /usr/bin/test, /bin/uname, /bin/su

- File-Transfer Plug-in (Send: If the value of the plug-in property transferMode is "send")

  /bin/bash, /usr/bin/id, /usr/bin/test, /bin/mkdir, /bin/chmod, /bin/gunzip, /bin/tar, /bin/rm, /bin/cp, /bin/uname, /bin/su

- File-Transfer Plug-in (Receive: If the value of the plug-in property transferMode is "receive")

  /bin/bash, /usr/bin/id, /usr/bin/test, /bin/mkdir, /bin/chmod, /usr/bin/zip, /bin/rm, /bin/uname, /bin/su

The custom plug-in and File-Transfer Plug-in transfer files to the operation-target device using SCP or SFTP. Make sure that the operation-target device has an environment in which files can be transferred using SCP or SFTP. Note that if the operation-target device is Linux and a character string is output from `.bashrc` of the connecting user, transferring files using SCP might fail. Also, when connecting to the remote machine using SSH or telnet, do not include commands such as **`stty`**, **`tty`**, **`tset`**, and scripts that require an interactive environment in the login script of the connecting user. If so, change the login script or create a new user who uses the login script that does not run these commands.

Configuring remote machine connection information for plug-ins and services

Before Ops Center Automator plug-ins and services can communicate with remote machines on which the plug-ins run tasks and perform actions, you must configure remote machine connection information.

Before you begin, verify the following:

- All the files located in the following path are regarded as destination properties files.

  `*Automation-software-installation-folder*\Automation\conf\plugin\destinations`

- The file name uses the following format:

  `*Host-name*.properties, *IPv4-address*.properties, *IPv6-address*.properties`

> **Note:** Because you cannot use the colon ":" within an IPv6 address within the file name, replace it with a dash (-); for example: change "2001::234:abcd" to "2001--234-abcd.properties".

You can view a sample file in the following location:

Automation-software-installation-folder\Automation\conf\plugin\destinations\#sample.properties

When editing the properties file, take note of the following:

- Lines that begin with # are treated as comments.
- Blank lines are ignored.
- Encoding is ISO 8859-1.
- Contents are case sensitive
- To specify a forward slash (\) in a character string, you must use a double forward slash (\\).
- If you specify an value in the destination properties file that is not valid, an execution error occurs in the plug-in that references the destination properties file.
- If you enter the same specification key multiple times in a file, the last one you specify takes effect.
- If you edited the destination properties file, the new definitions are applied when the plug-in that references the file is run.

Use the following configuration information to connect with the target machine.

Guidelines when the target machine is part of a cluster environment

When entering information for a cluster target machine:

- If the OS of the target machine is a Windows Server cluster environment, the working folders (`wmi.workDirectory.sharedName` and `wmi.workDirectory.sharedPath`) must be set. Otherwise, the plug-in causes a connection error.
- If you run the script with the Custom Plug-in, you must specify the execution folder (`common.executionDirectory`). Otherwise, the script is not forwarded.

Key name	Setting	Valid values
terminal.charset	Specifies the character set used for communication.	EUC-JP eucjp ibm-943C ISO-8859-1 MS932 PCK Shift_JIS UTF-8 windows-31j

Key name	Setting	Valid values
telnet.port	Specifies the port number used for a Telnet connection by using the Terminal Connect Plug-in. This setting has priority over the "telnet.port.number setting" in the properties file (`config_user.properties`).	0-65535
ssh.port	Specifies the port number used for an SSH connection by using one of the following plug-ins: ▪ General Command Plug-in ▪ File-Transfer Plug-in ▪ Terminal Connect Plug-in ▪ Custom Plug-in This setting has priority over the "ssh.port.number" setting in the properties file (`config_user.properties`).	0-65535
telnet.prompt.account	Specifies a regular expression pattern used to detect the character string that is output for prompting the user to enter a user ID to establish a connection with the target device by using the Terminal Connect Plug-in. For example, specify Username:.	Character string from 1 to 1,024 characters for use in regular expression patterns.
telnet.prompt.password	Specifies a regular expression pattern used to detect the character string that is output for prompting the user to enter a password to establish a connection with the target device by using the Terminal Connect Plug-in. For example, specify Password:.	Character string from 1 to 1,024 characters for use in regular expression patterns.
telnet.noStdout.port.list	Specifies the port number of the service that does not return the standard output after a connection is established by using the Terminal Connect Plug-in. To specify multiple port numbers, use a comma as a separator.	0-65535, and commas (,) from 1 to 1,024 characters

Key name	Setting	Valid values
wmi.workDirectory.sharedName	This is a property for Windows target machines. Specifies the shared folder name of the shared folder to which the file transmitted when running a command on the target . The folder must be the same as wmi.workDirectory.sharedPath. If using this property, the administrative shared setting of a target is unnecessary.	Single-byte alphanumeric characters, "-", "_", and ".". Specify a character string from 0 to 80 characters.
wmi.workDirectory.sharedPath	This is a property for Windows target machines. Specifies the absolute path of the shared folder to which the file transmitted when running a command on the target. If using the General Command Plug-in, the execution folder becomes "\Hitachi\CMALib\HAD\home" under the path listed for this property. The folder must be the same as wmi.workDirectory.sharedName. If using this property, the administrative shared setting of a target is unnecessary.	Single-byte alphanumeric characters, ":", "\", "-", "_", and ".". Specify a character string from 0 to 80 characters.

Key name	Setting	Valid values
ssh.workDirectory	This is a property for Linux OS target machines. Specifies the absolute path of the directory to which the file for a transmission is placed for the File-Transfer or the Custom Plug-in. Neither the path specified in this property nor the path of the parent directory can be specified as the destination and the receiver of File-Transfer Plug-in. For the working directory, the read, write, and execute privilege for the connected user are required. If the path specified in this property does not exist when the plug-in is used, it is created when the plug-in is run. If the directory cannot be created, the plug-in execution ends abnormally. You must ensure that the access permission for the new directory is 777. Priority is given over the value of "plugin.remoteCommand.workDirectory.ssh" defined in the `config_user.properties` file.	Single-byte alphanumeric characters, "/", "-", "_", and ".". Specify a character string from 0 to 128 characters.
common.executionDirectory	Specifies the execution folder at the time of running the Custom Plug-in on the target. If the value of the execution folder defined in the plug-in definition is not set, the value of this property is applied. Priority is given over the value of "plugin.remoteCommand.executionDirectory.wmi" and "plugin.remoteCommand.executionDirectory.ssh" defined in the `config_user.properties` file.	Any characters Specify a character string from 0 to 128 characters.
sftp.enable	Specifies whether to use SFTP when sending/receiving files using SSH in the File Transfer Plug-in and Custom plug-in. If true, SFTP is used, and if false, SCP is used. This setting has priority over the "plugin.sftp.enable" setting in the properties file (`config_user.properties`).	true/false

Windows OS prerequisites for agentless connections

The Windows prerequisites listed in the following sections are required for using agentless connections.

Supported users

You can use the following users in an agentless connection:

- Built-in Administrator
- Built-in Administrator of Active Directory
- A user belonging to the Administrators group
- A user belonging to the Domain Admin group of Active Directory

When using a user that belongs to the Administrators group, be aware that UAC (User Access Control) elevation does not apply at the time of command execution.

You also must edit the registry. Using a registry editor, set an entry under the key of the following registry.

Note: You are not required to restart the OS.

Item	Value
Registry key	`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System`
Registry entry	`LocalAccountTokenFilterPolicy`
The value set as a registry entry	1 (DWORD)

Optionally, you can enter the following command at a command prompt:

```
reg add HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion
\Policies\System /v LocalAccountTokenFilterPolicy /t REG_DWORD /d
0x1 /f
```

Administrative share setting

Using an administrative share, set an entry under the key of the following registry using a registry editor and then restart the operating system.

Item	Value
Registry key	`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Lanmanserver\parameters`

Item	Value
Registry entry	`AutoShareServer`
The value set as a registry entry	1 (DWORD)

Enter the following command at a command prompt:

```
reg add HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services
\Lanmanserver\parameters /v AutoShareServer /t REG_DWORD /d 1
```

SSH prerequisites for agentless connections

The SSH protocol prerequisites listed in the following sections are required for using agentless connections.

The SSH prerequisites are required for the following plug-ins:

- Custom Plug-in
- General Command Plug-in
- File-Transfer Plug-in
- Terminal Connect Plug-in
- Terminal Command Plug-in
- Terminal Disconnect Plug-in

Note: SSH must support version 2.

Password authentication

You must set up password authentication to an SSH server as follows:

1. Log on to a remote process target host as root.
2. Open the `/etc/ssh/sshd_config` file.
3. Set the value of `PasswordAuthentication` to "yes". If the `PasswordAuthentication` line is commented out, remove the comment out hash sign (#).
4. Run the following command and restart `sshd` service.

   ```
   systemctl restart sshd
   ```

   Note: These commands can change with different versions of the OS. See the OS documentation for additional information.

Public key authentication

This module describes how to authenticate a public key that connects to an SSH server.

Setting up an SSH server

To use a public key authentication, it is necessary to set a public key authentication to a SSH server.

1. Log on to a remote target host as root.
2. Open the `/etc/ssh/sshd_config` file.
3. Set the value of `PubkeyAuthentication` to "yes". If the `PubkeyAuthentication` line is commented out, remove the comment out hash sign (#).
4. Run the following command and restart the `sshd` service.

   ```
   systemctl restart sshd
   ```

   Note: These commands can change with different versions of the OS. See the OS documentation for additional information.

Creating a key (for the first time)

Create a public key and a private key. Best practice is to create the keys on an OS where Ops Center Automator is installed.

The following key types and key lengths are supported for public key authentication. Note that PEM format and OpenSSH format are supported for private key format.

Key type	Key length (bits)
RSA	1024 to 16384
DSA	1024
ECDSA	256, 384, 521
ED25519	256

Note: For RSA keys where multiple cryptographic algorithms correspond to a single key type, the most secure cryptographic algorithm available on the connected Linux host within three public key algorithms (ssh-rsa, rsa-sha2-256, rsa-sha2-512) is automatically used.

As a reference, the following procedure creates a key.

1. Run the **`ssh-keygen`** command. For example,
   - If creating an RSA key: **`ssh-keygen -t rsa`**
   - If creating a DSA key: **`ssh-keygen -t dsa`**
   - If creating an ECDSA key: **`ssh-keygen -t ECDSA`**
   - If creating an ED25519 key: **`ssh-keygen -t ed25519`**

   Note: These commands can change with different versions of the OS. See the OS documentation for additional information.

2. Decide the location and name of a private key.

   Specify a path and filename that does not contain multibyte characters. As for a default, `~/.ssh/id_rsa` is set (if creating RSA key). A private key is set as the filename specified to a selected path. A public key is set to the same directory as a private key with the file extension ".pub" attached to the name of the private key.

3. Enter a pass phrase.

   You will be asked to enter the pass phrase and to press the **Enter** key. You will be then asked to enter the pass phrase again. If you choose not to set a pass phrase to a private key, press only the **Enter** key to bypass the pass phrase.

Arrange a private key to Ops Center Automator

1. Arrange a private key at an arbitrary place on the OS where Ops Center Automator is installed.
2. Specify the absolute path of the private key to `ssh.privateKeyFile` in the properties file (`config_user.properties`). When specifying the path, do not specify symbolic links or junction points.
3. Restart the services by running the **`hcmds64srv`** command.

Arranging a public key to a remote target host

1. Redirect the output of the **`cat`** command and add the contents of the generated public key file to the public key file (authorized_keys) used for an authentication. (Example: `cat id_rsa.pub >> authorized_keys`)
2. Run the **`chmod`** command and change the attribute of `authorized_keys` to 600 (give write and read privilege only to the owner). If the attribute is not 600, an authentication might fail at the time of plug-in execution.

   The arrangement place of authorized_keys is directly under `~/.ssh` by default. With regard to `~/.ssh`, change the attribute to 700 (give write, read, and execute privilege only to the owner).

Configuring a shared property

1. Log on to the Ops Center Automator application.
2. Select [Administration] > [Shared Properties Settings].
3. Open the Pass phrase of the private key (for SSH public key authentication).
4. Enter the pass phrase as a value.

   The value is the pass phrase of the private key (for SSH public key authentication).

Keyboard interactive authentication

To use keyboard interactive authentication, it is necessary to setup authentication to a SSH server.

1. Log on to a remote target host as root.
2. Open the `/etc/ssh/sshd_config` file.

3. Setup keyboard interactive authentication as follows:
   - Set yes to the value of `ChallengeResponseAuthentication`. (If the line of `ChallengeResponseAuthentication` is commented out, remove the comment out hash sign (#).)
   - Set yes to the value of `UsePAM`. (If the `UsePAM` line is commented out, remove the comment out hash sign (#).)
4. Run the following command and restart the `sshd` service. An example command for each supported OS is shown.

   ```
   systemctl restart sshd
   ```

> **Note:** These commands can change depending on the OS version. For details, see the applicable OS manual.

Disabling cryptographic algorithms

Ops Center Automator allows you to disable the encryption algorithms used for SSH connections changing settings in `config_user.properties`. For more information, refer to Changing the system configuration (on page 94).

See Supported cryptographic algorithms (on page 258) for a list of cryptographic algorithms supported by Ops Center Automator.

> **Note:** If the SSH connection fails to negotiate the cryptographic algorithm, the following message will be displayed and the connection test will fail:
>
> ```
> KNAE02137-E Connection test failed. (detail information:
> failed to negotiate algorithms)
> ```
>
> In addition, if the public key algorithm determined from the private key specified when using public key authentication is not available at the connected Linux host, the following message will be displayed and the connection test will fail:
>
> ```
> KNAE02137-E Connection test failed. (detail information:
> authentication error)
> ```
>
> Check if there is a valid cryptographic algorithm available between the Ops Center Automator server and the connected Linux host.

Setting the java heap memory size on the Ops Center API Configuration Manager server

When you run multiple Online Migration with Configuration Manager tasks, you must change the size of the Java heap used by the Ops Center API Configuration Manager server to 6,144 MB.

Before you begin

Log on to the Ops Center API Configuration Manager server as a user with Administrator permissions (in Windows).

Tip: You can check the value that is currently set by checking the value of the `rest.java.heapMemory.size` property in the `StartupV.properties` file,which is stored in the following location.

```
Configuration-Manager-installation-folder\data\properties
\StartupV.properties
```

If the file does not exist or the file does not contain the `rest.java.heapMemory.size` property, this indicates that the default value is set.

Procedure

1. Run the following command:

   ```
   Configuration-Manager-installation-folder\bin\setProperty
   rest.java.heapMemory.size 6144
   ```

   After the command is run, the Ops Center API Configuration Manager server restarts. If you specify `-noRestart` at the end of the command line, the command will run without restarting the server.

   When you run the **`setProperty`** command, the value of the `rest.java.heapMemory.size` property in the `StartupV.properties` file will be changed to 6144. If the file does not exist, it will be created.

   Each time the command is run, the current `StartupV.properties` file is backed up. The backup file is created in the same directory and the name of the backup file will include the date and time of creation (for example, `StartupV_20200220-093320.properties`).

Chapter 5: User management on an external authentication server

This module explains how to set up user authentication on the external authentication server.

About linking to an external authentication server

Note: When you use Ops Center Automator in a cluster environment, you must perform user authentication on both the active and standby nodes.

Note: To use external authentication servers with Common Services, see *Hitachi Ops Center Installation and Configuration Guide*.

If you are using external authentication servers with Common Services to login to this product, note that User IDs and passwords for external authentication servers must meet the following criteria:

- Number of characters: 1-255.
- Characters allowed: A-Z, a-z, 0-9 ! # $ % & ' ( ) * + - . = @ \ ^ _ | .

Ops Center Automator allows you to log in by using user accounts registered on an external authentication server. When you link to an external authentication server, you do not need to perform login password management and account control for Ops Center Automator. You can link Ops Center Automator to the following external authentication servers:

- LDAP directory server
- RADIUS server
- Kerberos server

About linking to an external authorization server

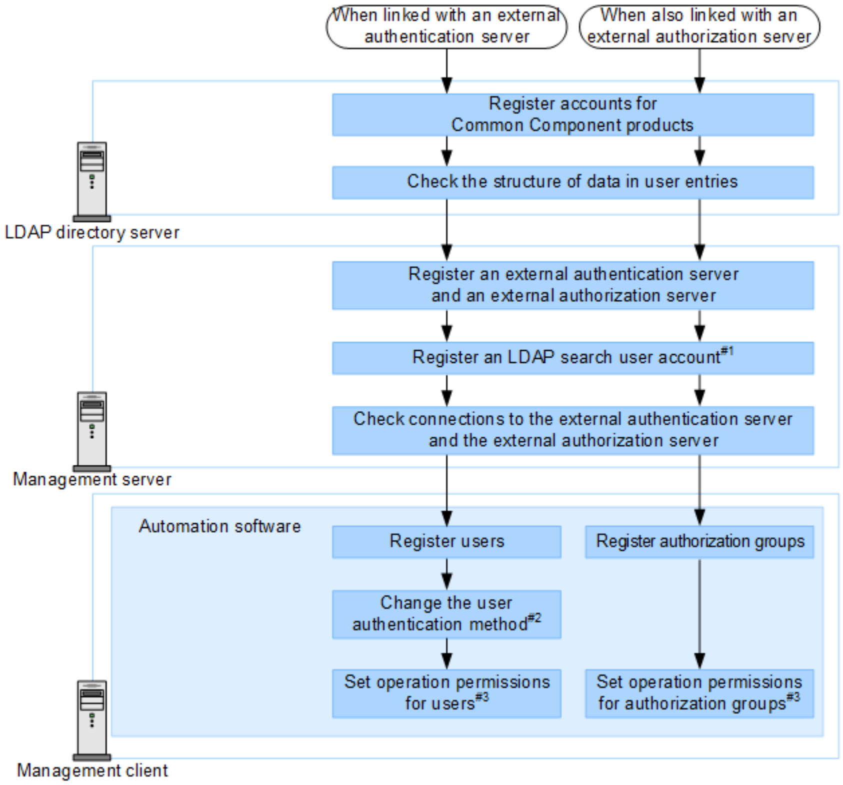
In addition to an external authentication server, if you also use an external authorization server to perform user authentication, access permissions for the management server (Common Component product) can be controlled on the external authorization server.

When an external authorization server is also linked to, you do not need to manage accounts and set permissions for individual users because Common Component products manage users by using the *authorization groups* on the external authorization server.

Common Component products can be linked to an LDAP directory server (Active Directory).

Workflow for user authentication on an LDAP directory server

To perform user authentication on an LDAP directory server, you must register the external authentication server and the accounts to be authenticated on the management server for Common Component products.


When linked with an external authentication server
When also linked with an external authorization server
Register accounts for Common Component products
Check the structure of data in user entries
LDAP directory server
Register an external authentication server and an external authorization server
Register an LDAP search user account#1
Check connections to the external authentication server and the external authorization server
Management server
Automation software
Register users
Register authorization groups
Change the user authentication method#2
Set operation permissions for users#3
Set operation permissions for authorization groups#3
Management client

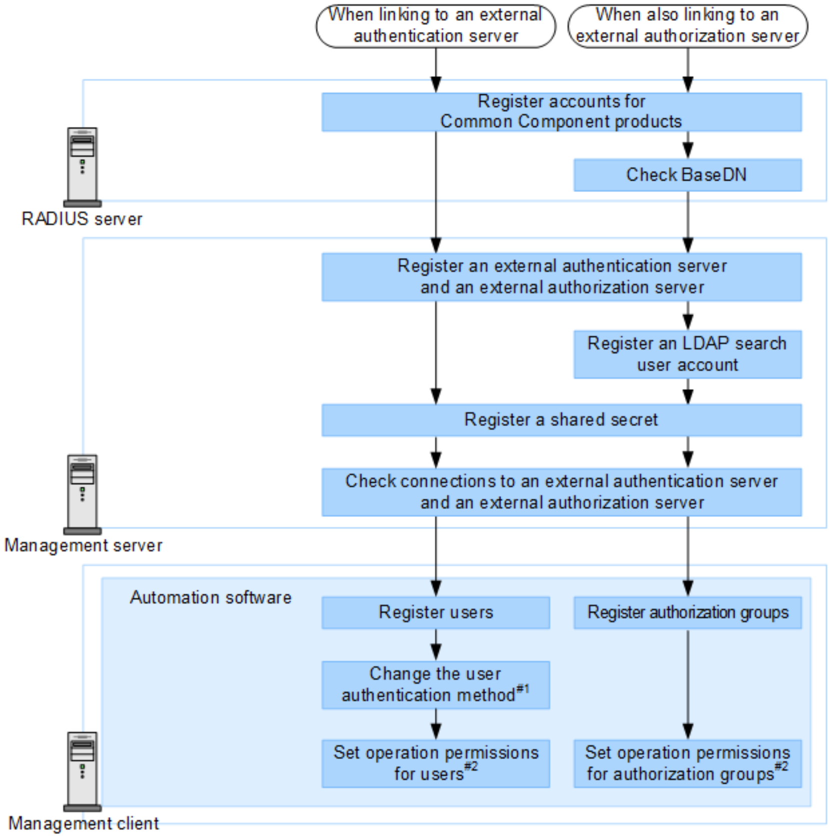
#1: This step is not required if you want to link only to an external authentication server and the structure of the data of the user entries is a flat model.
#2: This step is required if you want to change the current user authentication method.
#3: Set permissions according to the user's job description.

- User management
- Common Component products

Note: To use StartTLS to communicate between the LDAP directory server and the management server, you must set up an environment specifically for this purpose to ensure secure communications.

Workflow for user authentication on a RADIUS server

To do user authentication on a RADIUS server, you must register the external authentication server and the accounts to be authenticated on the management server for Common Component products.

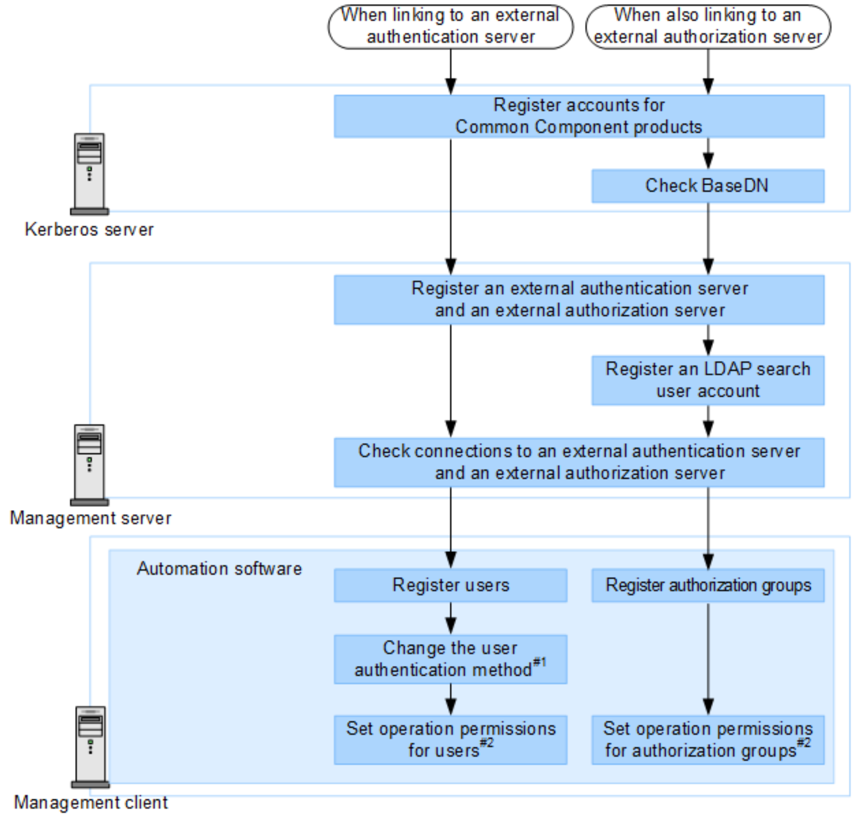

When linking to an external authentication server
When also linking to an external authorization server
Register accounts for Common Component products
Check BaseDN
RADIUS server
Register an external authentication server and an external authorization server
Register an LDAP search user account
Register a shared secret
Check connections to an external authentication server and an external authorization server
Management server
Automation software
Register users
Register authorization groups
Change the user authentication method#1
Set operation permissions for users#2
Set operation permissions for authorization groups#2
Management client

#1: This step is required if you want to change the current user authentication method.
#2: Set permissions according to the user's job description.

- User management
- Common Component products

Workflow for user authentication on a Kerberos server

To perform user authentication on a Kerberos server, you must register the external authentication server and the accounts to be authenticated on the management server for Common Component products.


When linking to an external authentication server
When also linking to an external authorization server
Register accounts for Common Component products
Check BaseDN
Kerberos server
Register an external authentication server and an external authorization server
Register an LDAP search user account
Check connections to an external authentication server and an external authorization server
Management server
Automation software
Register users
Register authorization groups
Change the user authentication method#1
Set operation permissions for users#2
Set operation permissions for authorization groups#2
Management client

#1: This step is required if you want to change the current user authentication method.
#2: Set permissions according to user's job description.

- User management
- Common Component products

About the data structures of user entries

Two data structures of user entries for an LDAP directory server exist: the hierarchical structure model and the flat model.

When performing user authentication on an LDAP directory server, verify which data structure is being used, because information about the LDAP directory server registered on the management server and the procedures you need to perform on the management server depend on the data structure.

In addition, when performing user authentication or authorization on an LDAP directory server, also verify BaseDN, which is the start point for searching for users.

About the BaseDN

BaseDN is the starting point for searching for users during authentication or authorization.

Only user entries in the following hierarchies BaseDN are subject to authentication or authorization. In Common Component products, user entries must contain all of the users to be authenticated or authorized. BaseDN is required when registering information about the LDAP directory server on the management server.

About the hierarchical structure model

A data structure in which the following hierarchies BaseDN branch off and in which user entries are registered in another hierarchy.

If the hierarchical structure model is used, the entries in the following hierarchy BaseDN are searched for an entry that has the same login ID and user attribute value. The following figure shows an example of the hierarchical structure model.

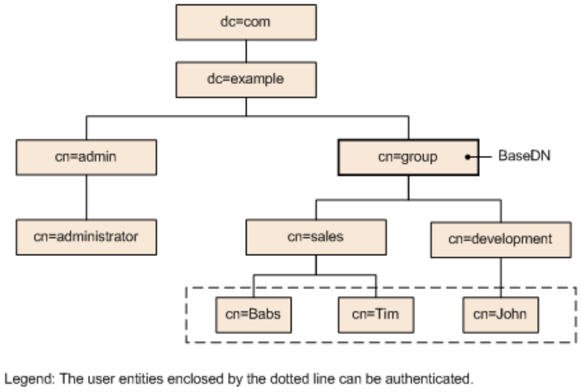


Figure 1 Example of the hierarchical structure model

About the flat model

A flat model is a data structure in which there are no branches in the hierarchy after BaseDN and in which user entries are registered in the hierarchy located just after BaseDN.

If the flat model is used, the entries in the hierarchy after BaseDN are searched for an entry that has the DN that consists of a combination of the login ID and BaseDN. If such a value is found, the user is authenticated. The following figure shows an example of the flat model.

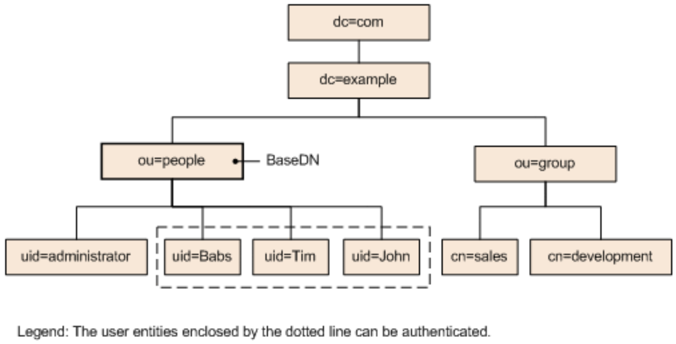


Figure 2 Example of the flat model

Configurations when multiple external authentication servers are linked

When multiple external authentication servers are linked, user authentication is performed in a redundant configuration or a multi-domain configuration.

A redundant configuration is used when each external authentication server manages the same user information. If a failure occurs on one external authentication server, user authentication can be performed by using another external authentication server.

A multi-domain configuration is used to manage different user information for each external authentication server. If a user logs in with a user ID that includes a domain name, the user will be authenticated by an external authentication server in the domain whose name is included in the user ID. When a Kerberos server is used as an external authentication server, you can create a configuration similar to a multi-domain configuration by managing different user information for each realm.

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

Table 17 Support status for redundant configurations and multi-domain configurations

External authentication server	Redundant configuration	Multi-domain configuration
LDAP directory server	Y[#1]	Y[#1]
RADIUS server	Y	N
Kerberos server	Y	Y[#2]

Legend:

Y: Supported

N: Not supported

#1

You can use either a redundant configuration or a multi-domain configuration.

#2

By managing different user information for each realm, you can create a configuration that is similar to a multi-domain configuration.

When an LDAP directory server is used for user authentication in a multi-domain configuration, the user authentication process varies depending on whether you log in by entering a user ID that includes a domain name.

If you log in with a user ID that includes a domain name, as in the following figure, user authentication will be performed by using the LDAP directory server of the specified domain.

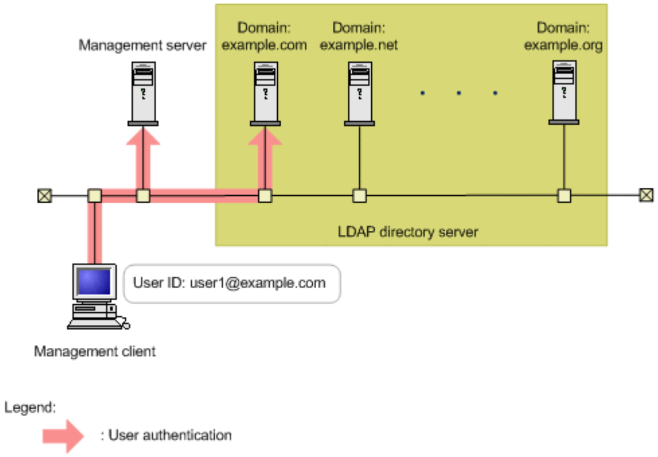


Figure 3 User authentication in a multi-domain configuration (when using a user ID that includes a domain name)

If you log in with a user ID that does not include a domain name, user authentication will be performed sequentially on all LDAP directory servers that are linked until the user is authorized, as shown in the following figure. If a large number of LDAP directory servers are linked, user authentication will take a long time. For this reason, you should log in with a user ID that includes a domain name.

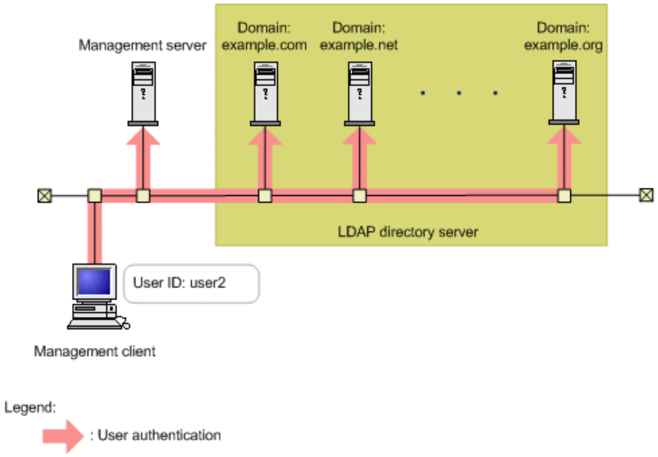


Figure 4 User authentication in a multi-domain configuration (when using a user ID that does not include a domain name)

Registering an external authentication server and an external authorization server

In the `exauth.properties` file, set the type of the external authentication server to be used, the server identification name, and the machine information about the external authentication server and external authorization server.

Before you begin

- Log in as a user with Administrator permissions (for Windows) or as a root user (for Linux).
- Copy the template of the `exauth.properties` file.

  In Windows:

  ```
  Common-Component-installation-folder\sample\conf
  \exauth.properties
  ```

  In Linux:

  ```
  Common-Component-installation-directory/sample/conf/
  exauth.properties
  ```

- Verify the data structure of user entries (for LDAP authentication).
- Set up the environment for the DNS server on the OS of the LDAP directory server.*
- Register information about the LDAP directory server to the SRV record of the DNS server.*

Verify the following information:

- Common information:
  - Type of the external authentication server
- For LDAP authentication:
  - Machine information about the external authentication server and the external authorization server (Host name or IP address, Port number)
  - BaseDN
  - Domain name for external authentication servers managed by the LDAP directory server (when linking to an external authorization server)
  - Domain name for multi-domain configurations managed by the LDAP directory server (for a multi-domain configuration)

- For RADIUS authentication
  - Machine information about the external authentication server and the external authorization server (Host name or IP address, Port number)
  - Authentication protocol
  - Host name or IP address of the management server
  - Domain name managed by the LDAP directory server (when linking to an external authorization server)
  - BaseDN (when linking to an external authorization server)
- For Kerberos authentication
  - Machine information about the external authentication server and the external authorization server (Host name or IP address, Port number)
  - Realm name
  - Domain name managed by the LDAP directory server (when linking to an external authorization server)
  - BaseDN (when linking to an external authorization server)

*: This process is required to look up the information about the LDAP directory server by using the DNS server.

Procedure

1. Specify required items in the `exauth.properties` file being copied.
2. Save the `exauth.properties` file in the following location:

   In Windows:

   `Common-Component-installation-folder``\conf\exauth.properties`

   In Linux:

   `Common-Component-installation-directory``/conf/`
   `exauth.properties`

3. If the setting value of the `auth.ocsp.enable` or `auth.ocsp.responderURL` property is changed, the Common Component product services must be restarted.

   If the setting value of any other property or attribute is changed, the change takes effect immediately.

Setup items in the exauth.properties file for LDAP authentication

In the `exauth.properties` file, set the type of the external authentication server to be used, the server identification name, and the machine information about the external authentication server.

- Common properties

  See "Setup items in the exauth.properties file for LDAP authentication (common items)"

- Properties for an external authentication server and an external authorization server

  Setup items in the `exauth.properties` file vary depending on whether information about the LDAP direx server being connected to is directly specified or looked up by using the DNS server.

  - When directly specifying information about the LDAP direx server:

    See "Setup items in the exauth.properties file for LDAP authentication (when directly specifying information about the external authentication server)" or "Setup items in the exauth.properties file for LDAP authentication (when an external authentication server and StartTLS are used for communication)"

  - When using the DNS server to look up information about the LDAP direx server:

    See "Setup items in the exauth.properties file for LDAP authentication (when using the DNS server to look up information about the external authentication server)"

Note:

- Make sure to distinguish between uppercase and lowercase letters for property settings.
- To use StartTLS for communication between the management server and the LDAP direx server, you must directly specify information about the LDAP direx server to connect to in the `exauth.properties` file.
- If you use the DNS server to look up the LDAP direx server to connect to, it might take longer for users to log in.
- If the LDAP direx server to which you want to connect is in a multidomain configuration, you will not be able to look up the LDAP direx server by using the DNS server.

Table 18 Setup items in the exauth.properties file for LDAP authentication (common items)

Property	Details
`auth.server.type`	Specify an external authentication server type. Specify `ldap`. Default value: `internal` (used when not linking to an external authentication server)
`auth.server.name`	Specify the server identification names of LDAP direx servers. You can specify any name for this property to

Property	Details

	identify which LDAP direx servers the settings such as the port number and the protocol for connecting to the LDAP direx server to which they are applied. (see "Setup items in the exauth.properties file for LDAP authentication (when directly specifying information about the external authentication server)" or "Setup items in the exauth.properties file for LDAP authentication (when using the DNS server to look up information about the external authentication server)".
	`ServerName` has been set as the initial value. You must specify at least one name. To specify multiple server identification names, delimit the server identification names by using commas (,). Do not register the same server identification name more than once.
	Specifiable values: No more than 64 bytes of the following characters:
	`A` to `Z`
	a to z
	`0` to `9`
	`! # ( ) + - . = @ [ ] ^ _ { } ~`
	Default value: none

`auth.ldap.multi_domain`	When specifying multiple server identification names for LDAP direx servers, specify, for each server, the configuration to be used. Specify `true` to use a multi-domain configuration. Specify `false` to use a redundant configuration. Default value: `false`
`auth.group.mapping`	Specify whether to also link to an external authorization server. Specify `true` to link to an external authorization server. Specify `false` to not to link to an external authorization server. Default value: `false`

Table 19 Setup items in the exauth.properties file for LDAP authentication (when directly specifying information about the external authentication server)

Attributes	Details
`protocol`	Specify the protocol for connecting to the LDAP direx server. This attribute is required. When communicating in plain text format, specify `ldap`. When using StartTLS communication, specify `tls`. For StartTLS, TLS 1.2 and TLS 1.3 are supported. Before specifying `tls`, make sure that one of the following encryption methods can be used on the LDAP direx server: ▪ TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ▪ TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ▪ TLS_RSA_WITH_AES_128_GCM_SHA256 ▪ TLS_RSA_WITH_AES_256_GCM_SHA384 ▪ TLS_AES_256_GCM_SHA384 ▪ TLS_AES_128_GCM_SHA256 ▪ TLS_CHACHA20_POLY1305_SHA256 You can specify `ldap` or `tls`. Default value: none When communicating by using StartTLS as the protocol for connecting to the LDAP direx server, you must specify the security settings of Common Component.
`host`	Specify the host name or IP address of the LDAP direx server. If you specify the host name, make sure that the host name can be resolved to an IP address. If you specify the IP address, you can use either an IPv4 or IPv6 address. When specifying an IPv6 address, enclose it in square brackets ([]). This attribute is required. Default value: none When using StartTLS as the protocol for connecting to the LDAP direx server, in the `host` attribute specify the same host name as the value of CN in the LDAP direx server certificate. You cannot use an IP address.
`port`	Specify the port number of the LDAP direx server. Make sure that the port you specify is set as the listen port number on the LDAP direx server. Specifiable values: 1 to 65535 Default value: 389

Attributes	Details
`timeout`	Specify the amount of time to wait before timing out when connecting to the LDAP direx server. If you specify `0`, the system waits until a communication error occurs without timing out. Specifiable values: 0 to 120 (seconds) Default value: 15
`attr`	Specify the attribute (Attribute Type) to use as the user ID during authentication. ▪ For the hierarchical structure model Specify the name of the attribute containing the unique value to be used for identifying the user. The value stored in this attribute will be used as the user ID for Common Component products. The specified attribute must not include characters that cannot be used in a user ID of the Common Component product. For example, if you are using Active Directory and you want to use the Windows logon ID for the user ID of a Common Component product, specify the attribute name `sAMAccountName` in which the Windows logon ID has been defined. ▪ For the flat model Specify the RDN attribute name of the user entry. For example, if the user's DN is `uid=John,ou=People,dc=example,dc=com`, specify the `uid` that is the attribute name of the `uid=John`. `sAMAccountName` has been set as the initial value. This attribute is required. Default value: none
`basedn`	Specify the BaseDN, which is the DN of the entry that will be used as the start point when searching for LDAP user information on the LDAP direx server. The user entries that are located in the hierarchy after this DN will be verified during authentication. If characters that must be escaped are included in the specified BaseDN, escape all of those characters correctly because the specified value will be passed to the LDAP direx server without change. ▪ For the hierarchical structure model Specify the DN of the hierarchy that includes all of the user entries to be searched. ▪ For the flat model Specify the DN of the hierarchy just before the user entries to be searched.

Attributes	Details
	This attribute is required. Specify the DN by following the rules defined in RFC4514. For example, if any of the following characters are included in a DN, you must use a backslash (\\) to escape each character. Spaces # + ; , < = > \\ Default value: none
`retry.interval`	Specify the interval (in seconds) a failed connection to the LDAP direx server and the next try. Specifiable values: 1 to 60 (seconds) Default value: 1
`retry.time`	Specify the number of times to try to connect to the LDAP direx server. If you specify 0, no further tries occur. Specifiable values: 0 to 50 Default value: 20
`domain.name`	Specify the name of a domain for external authentication servers managed by the LDAP direx server. This item is required when an external authorization server is also linked to. Default value: none
`domain`	Specify the name of a domain for multi-domain configurations managed by the LDAP direx server. If you log in by using a user ID that includes the domain name specified in this attribute, the LDAP direx server that belongs to the specified domain will be used as the authentication server. When specifying a domain name for the server identification name of each LDAP direx server, do not specify the same domain name more than once. This value is not case sensitive. This item is required when a multi-domain configuration is used. Default value: none
`dns_lookup`	Specify `false`. Default value: `false`
Note: To specify the attributes, use the following syntax: `auth.ldap.auth.server.name-property-value.attribute=value`	

Table 20 Setup items in the exauth.properties file for LDAP authentication (when an external authentication server and StartTLS are used for communication)

Property	Details
`auth.ocsp.enable`	Specify whether to verify the validity of an LDAP direx server's electronic signature certificate by using an OCSP responder when the LDAP direx server and StartTLS are used for communication. To verify the validity of certificates, specify `true`. To not verify the validity of certificates, specify `false`. Default value: `false`
`auth.ocsp.responderURL`	Specify the URL of an OCSP responder to use an OCSP responder that is not the one written in the AIA field of the electronic signature certificate to verify the validity of the electronic signature certificate. If this value is omitted, the OCSP responder written in the AIA field is used. Default value: none

Table 21 Setup items in the exauth.properties file for LDAP authentication (when using the DNS server to look up information about the external authentication server)

Attributes	Details
`protocol`	Specify the protocol for connecting to the LDAP direx server. This attribute is required. Specifiable values: `ldap` Default value: `none`
`port`	Specify the port number of the LDAP direx server. Make sure that the port you specify is set as the listen port number on the LDAP direx server. Specifiable values: 1 to 65535 Default value: 389
`timeout`	Specify the amount of time to wait before timing out when connecting to the LDAP direx server. If you specify `0`, the system waits until a communication error occurs without timing out. Specifiable values: 0 to 120 (seconds) Default value: 15

Attributes	Details
`attr`	Specify the attribute (Attribute Type) to use as the user ID during authentication. ▪ For the hierarchical structure model Specify the name of the attribute containing the unique value to be used for identifying the user. The value stored in this attribute will be used as the user ID for Common Component products. The specified attribute must not include characters that cannot be used in a user ID of the Common Component product. For example, if you are using Active Directory and you want to use the Windows logon ID for the user ID of a Common Component product, specify the attribute name `sAMAccountName` in which the Windows logon ID has been defined. ▪ For the flat model Specify the RDN attribute name of the user entry. For example, if the user's DN is `uid=John,ou=People,dc=example,dc=com`, specify the `uid` that is the attribute name of the `uid=John`. `sAMAccountName` has been set as the initial value. This attribute is required. Default value: none
`basedn`	Specify the BaseDN, which is the DN of the entry that will be used as the start point when searching for LDAP user information on the LDAP direx server. The user entries that are located in the hierarchy after this DN will be verified during authentication. If characters that must be escaped are included in the specified BaseDN, escape all of those characters correctly because the specified value will be passed to the LDAP direx server without change. ▪ For the hierarchical structure model Specify the DN of the hierarchy that includes all of the user entries to be searched. ▪ For the flat model Specify the DN of the hierarchy just before the user entries to be searched. This attribute is required. Specify the DN by following the rules defined in RFC4514. For example, if any of the following characters are included in a DN, you must use a backslash (\) to escape each character. Spaces # + ; , < = > \

Attributes	Details
	Default value: none
`retry.interval`	Specify the interval (in seconds) between tries to connect to the LDAP direx server. Specifiable values: 1 to 60 (seconds) Default value: 1
`retry.time`	Specify the number of tries to connect to the LDAP direx server. If you specify 0, no further tries occur. Specifiable values: 0 to 50 Default value: 20
`domain.name`	Specify the name of a domain for external authentication servers managed by the LDAP direx server. Default value: none
`dns_lookup`	Specify `true`. However, if the following attribute values are already set, the LDAP direx server will be connected to by using the user specified values instead of by using the DNS server to look up the information. ▪ `auth.ldap.auth.server.name-property-value.host` ▪ `auth.ldap.auth.server.name-property-value.port` Default value: `false`

Note: To specify the attributes, use the following syntax:

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

Examples of setting the exauth.properties file for LDAP authentication

This section gives examples of how to set the exauth.properties file when using an LDAP directory server to perform authentication.

- When directly specifying information about an LDAP directory server (when linking to only an external authentication server)

```
auth.server.type=ldap
auth.server.name=ServerName
auth.group.mapping=false
auth.ocsp.enable=false
auth.ocsp.responderURL=
auth.ldap.ServerName.protocol=ldap
auth.ldap.ServerName.host=ldap.example.com
auth.ldap.ServerName.port=389
auth.ldap.ServerName.timeout=15
auth.ldap.ServerName.attr=sAMAccountName
auth.ldap.ServerName.basedn=dc=Example,dc=com
auth.ldap.ServerName.retry.interval=1
auth.ldap.ServerName.retry.times=20
auth.ldap.ServerName.dns_lookup=false
```

- When using the DNS server to look up an LDAP directory server (when linking to only an external authentication server)

```
auth.server.type=ldap
auth.server.name=ServerName
auth.group.mapping=false
auth.ldap.ServerName.protocol=ldap
auth.ldap.ServerName.timeout=15
auth.ldap.ServerName.attr=sAMAccountName
auth.ldap.ServerName.basedn=dc=Example,dc=com
auth.ldap.ServerName.retry.interval=1
auth.ldap.ServerName.retry.times=20
auth.ldap.ServerName.domain.name=EXAMPLE.COM
auth.ldap.ServerName.dns_lookup=true
```

- When directly specifying information about the LDAP directory server (when also linking to an authorization server)

```
auth.server.type=ldap
auth.server.name=ServerName
auth.group.mapping=true
auth.ocsp.enable=false
auth.ocsp.responderURL=
auth.ldap.ServerName.protocol=ldap
auth.ldap.ServerName.host=ldap.example.com
auth.ldap.ServerName.port=389
auth.ldap.ServerName.timeout=15
auth.ldap.ServerName.attr=sAMAccountName
auth.ldap.ServerName.basedn=dc=Example,dc=com
auth.ldap.ServerName.retry.interval=1
auth.ldap.ServerName.retry.times=20
auth.ldap.ServerName.domain.name=EXAMPLE.COM
auth.ldap.ServerName.dns_lookup=false
```

- When using the DNS server to look up the LDAP directory server (when also linking to an authorization server)

```
auth.server.type=ldap
auth.server.name=ServerName
auth.group.mapping=true
auth.ldap.ServerName.protocol=ldap
auth.ldap.ServerName.timeout=15
auth.ldap.ServerName.attr=sAMAccountName
auth.ldap.ServerName.basedn=dc=Example,dc=com
auth.ldap.ServerName.retry.interval=1
auth.ldap.ServerName.retry.times=20
auth.ldap.ServerName.domain.name=EXAMPLE.COM
auth.ldap.ServerName.dns_lookup=true
```

- When using a redundant configuration

```
auth.server.type=ldap
auth.server.name=ServerName1,ServerName2
auth.ldap.multi_domain=false
auth.group.mapping=false
auth.ldap.ServerName1.protocol=ldap
auth.ldap.ServerName1.host=ldap1.example.com
auth.ldap.ServerName1.port=389
auth.ldap.ServerName1.timeout=15
auth.ldap.ServerName1.attr=sAMAccountName
auth.ldap.ServerName1.basedn=dc=Example,dc=com
auth.ldap.ServerName1.retry.interval=1
auth.ldap.ServerName1.retry.times=20
auth.ldap.ServerName2.protocol=ldap
auth.ldap.ServerName2.host=ldap2.example.com
auth.ldap.ServerName2.port=389
auth.ldap.ServerName2.timeout=15
auth.ldap.ServerName2.attr=sAMAccountName
auth.ldap.ServerName2.basedn=dc=Example,dc=net
auth.ldap.ServerName2.retry.interval=1
auth.ldap.ServerName2.retry.times=20
```

- When using a multi-domain configuration

```
auth.server.type=ldap
auth.server.name=ServerName1,ServerName2
auth.ldap.multi_domain=true
auth.group.mapping=false
auth.ldap.ServerName1.protocol=ldap
auth.ldap.ServerName1.host=ldap1.example.com
auth.ldap.ServerName1.port=389
auth.ldap.ServerName1.timeout=15
auth.ldap.ServerName1.attr=sAMAccountName
auth.ldap.ServerName1.basedn=dc=Example,dc=com
auth.ldap.ServerName1.retry.interval=1
auth.ldap.ServerName1.retry.times=20
auth.ldap.ServerName1.domain=example.com
auth.ldap.ServerName2.protocol=ldap
auth.ldap.ServerName2.host=ldap2.example.com
auth.ldap.ServerName2.port=389
auth.ldap.ServerName2.timeout=15
auth.ldap.ServerName2.attr=sAMAccountName
auth.ldap.ServerName2.basedn=dc=Example,dc=net
auth.ldap.ServerName2.retry.interval=1
auth.ldap.ServerName2.retry.times=20
auth.ldap.ServerName2.domain=example.net
```

Setup items in the exauth.properties file for RADIUS authentication

In the `exauth.properties` file, set the type of the external authentication server to be used, the server identification name, and the machine information about the external authentication server.

- Common properties

  See "Setup items in the exauth.properties file for RADIUS authentication (common items)"

- Properties for an external authentication server

  Specify these property values for each RADIUS server.

  See "Setup items in the exauth.properties file for RADIUS authentication (settings for the external authentication server)

- Properties for an external authorization server

  These properties must be set when an external authorization server is also linked to. Specify information about the LDAP directory server for each domain.

  Setup items in the `exauth.properties` file vary depending on whether information about the LDAP directory server being connected to is directly specified or looked up by using the DNS server.

  - When directly specifying information about the LDAP directory server

    See "Setup items in the exauth.properties file for RADIUS authentication (common settings for the external authorization server)", "Setup items in the exauth.properties file for RADIUS authentication (when directly specifying information about the external authorization server)", and "Setup items in the exauth.properties file for RADIUS authentication (when an external authorization server and Start TLS are used for communication)"

  - When using the DNS server to look up the information about the LDAP directory server

    See "Setup items in the exauth.properties file for RADIUS authentication (common settings for the external authorization server)" and "Setup items in the exauth.properties file for RADIUS authentication (when using the DNS server to look up information about the external authorization server)"

Note:

- Make sure to distinguish between uppercase and lowercase letters for property settings.
- To use StartTLS for communication between the management server and the LDAP directory server, you must directly specify information about the LDAP directory server to connect to in the `exauth.properties` file.
- If you use the DNS server to look up the LDAP directory server to connect to, it might take longer for users to log in.

Table 22 Setup items in the exauth.properties file for RADIUS authentication (common items)

Property names	Details
`auth.server.type`	Specify an external authentication server type. Specify `radius`. Default value: `internal` (used when not linking to an external authentication server)

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

`auth.group.mapping`	Specify whether to also link to an external authorization server. Specify `true` to link to an external authorization server. Specify `false` to not to link to an external authorization server. Default value: `false`

Table 23 Setup items in the exauth.properties file for RADIUS authentication (settings for the external authentication server)

Attributes	Details
`protocol`	Specify the protocol for RADIUS server authentication. This attribute is required. Specifiable values: `PAP` or `CHAP` Default value: none

Attributes	Details
host[1]	Specify the host name or IP address of the RADIUS server. If you specify the host name, make sure beforehand that the host name can be resolved to an IP address. If you specify the IP address, you can use either an IPv4 or IPv6 address. When specifying an IPv6 address, enclose it in square brackets ([]). This attribute is required. Default value: none
port	Specify the port number for RADIUS server authentication. Make sure beforehand that the port you specify is set as the listen port number on the RADIUS server. Specifiable values: 1 to 65535 Default value: 1812
timeout	Specify the amount of time to wait before timing out when connecting to the RADIUS server. Specifiable values: 1 to 65535 (seconds) Default value: 1
retry.times	Specify the number of times to try to connect to the RADIUS. If you specify 0, no further tries occur. Specifiable values: 0 to 50 Default value: 3
attr.NAS-Identifier[2]	Specify the host name of the Ops Center Automator management server. The RADIUS server uses this attribute value to identify the management server. The host name of the management server has been set as the initial value. Specifiable values: Specify no more than 253 bytes of the following characters: A to Z a to z 0 to 9 ! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ ` { | } ~ Default value: none

Attributes	Details
`attr.NAS-IP-Address`[2]	Specify the IPv4 address of the Ops Center Automator management server. The RADIUS server uses this attribute value to identify the management server. If the format of the address is not valid, this property is disabled. Default value: none
`attr.NAS-IPv6-Address`[2]	Specify the IPv6 address of the Ops Center Automator management server. The RADIUS server uses this attribute value to identify the management server. Enclose the IPv6 address in square brackets (`[]`). If the format of the address is not valid, this property is disabled. Default value: none

1. When linking to an external authorization server that is running on the same computer and using StartTLS as the protocol for connecting to the LDAP directory server, in the `host` attribute specify the same host name as the value of CN in the LDAP directory server certificate. You cannot use an IP address.
2. You must specify exactly one of the following: `attr.NAS-Identifier`, `attr.NAS-IP-Address`, or `attr.NAS-IPv6-Address`.

Note: To specify the attributes, use the following syntax:

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

Table 24 Setup items in the exauth.properties file for RADIUS authentication (common settings for the external authorization server)

Attributes	Details
`domain.name`	Specify the name of a domain managed by the LDAP directory server. This item is required when an external authorization server is also linked to. Default value: none
`dns_lookup`	Specify whether to use the DNS server to look up the information about the LDAP directory server. To directly specify information about the LDAP directory server in the `exauth.properties` file, specify `false`. To use the DNS server to look up the information, specify `true`.

Attributes	Details
	However, if the following attribute values are already set, the LDAP directory server will be connected to by using the user-specified values instead of by using the DNS server to look up the information. ▪ `auth.group.`*`domain-name`*`.host` ▪ `auth.group.`*`domain-name`*`.port` Default value: `false`
Note: To specify the attributes, use the following syntax: `auth.radius.`*`auth.server.name-property-value.attribute`*`=`*`value`*	

Table 25 Setup items in the exauth.properties file for RADIUS authentication (when directly specifying information about the external authorization server)

Attributes	Details
`protocol`	Specify the protocol for connecting to the LDAP directory server. When communicating in plain text format, specify `ldap`. When using StartTLS communication, specify `tls`. Before specifying `tls`, make sure that one of the following encryption methods can be used on the LDAP directory server. For StartTLS, TLS 1.2 and TLS 1.3 are supported. ▪ TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ▪ TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ▪ TLS_RSA_WITH_AES_128_GCM_SHA256 ▪ TLS_RSA_WITH_AES_256_GCM_SHA384 ▪ TLS_AES_256_GCM_SHA384 ▪ TLS_AES_128_GCM_SHA256 ▪ TLS_CHACHA20_POLY1305_SHA256 Specifiable values: `ldap` or `tls` Default value: `ldap` **Note:** When communicating by using StartTLS as the protocol for connecting to the LDAP directory server, you must specify the security settings of Common Component.

Attributes	Details
`host`	If the external authentication server and the external authorization server are running on different computers, specify the host name or IP address of the LDAP directory server. If you specify the host name, make sure beforehand that the host name can be resolved to an IP address. If you specify the IP address, you can use either an IPv4 or IPv6 address. When specifying an IPv6 address, enclose it in square brackets (`[]`). If you omit this attribute, the external authentication server and the external authorization server are assumed to be running on the same computer. Default value: none **Note:** When the external authentication server and the external authorization server are running on different computers and when using StartTLS as the protocol for connecting to the LDAP directory server, in the `host` attribute specify the same host name as the value of CN in the LDAP directory server certificate. You cannot use an IP address.
`port`	Specify the port number of the LDAP directory server. Make sure beforehand that the port you specify is set as the listen port number on the LDAP directory server. Specifiable values: 1 to 65535 Default value: 389
`basedn`	Specify the BaseDN, which is the DN of the entry that will be used as the start point when searching for LDAP user information on the LDAP directory server. The user entries that are located in the hierarchy after this DN will be verified during authorization. Specify the DN of the hierarchy that includes all of the user entries to be searched. Specify the DN by following the rules defined in RFC4514. For example, if any of the following characters are included in a DN, you must use a backslash (\) to escape each character. Spaces `# + ; , < = > \` If characters that must be escaped are included in the specified BaseDN, escape all of those characters correctly because the specified value will be passed to the LDAP directory server without change. If you omit this attribute, the value specified in the `defaultNamingContext` property of Active Directory is assumed as the BaseDN. Default value: none

Attributes	Details
`timeout`	Specify the amount of time to wait before timing out when connecting to the LDAP directory server. If you specify `0`, the system waits until a communication error occurs without timing out. Specifiable values: 0 to 120 (seconds) Default value: 15
`retry.interval`	Specify the interval (in seconds) between tries to connect to the LDAP directory server. Specifiable values: 1 to 60 (seconds) Default value: 1
`retry.times`	Specify the number of tries to connect to the LDAP directory server. If you specify 0, no further tries occur. Specifiable values: 0 to 50 Default value: 20

Note: To specify the attributes, use the following syntax:

```
auth.group.domain-name.attribute=value
```

For *domain-name*, specify the value specified for `auth.radius.`*`auth.server.name-property-value`*`.domain.name`.

Table 26 Setup items in the exauth.properties file for RADIUS authentication (when an external authorization server and StartTLS are used for communication)

Property	Details
`auth.ocsp.enable`	Specify whether to verify the validity of an LDAP directory server's electronic signature certificate by using an OCSP responder when the LDAP directory server and StartTLS are used for communication. To verify the validity of certificates, specify `true`. To not verify the validity of certificates, specify `false`. Default value: `false`
`auth.ocsp.responderURL`	Specify the URL of an OCSP responder to use an OCSP responder that is not the one written in the AIA field of the electronic signature certificate to verify the validity of the electronic signature certificate. If this value is omitted, the OCSP responder written in the AIA field is used. Default value: None

Table 27 Setup items in the exauth.properties file for RADIUS authentication (when using the DNS server to look up information about the external authorization server)

Attributes	Details
`protocol`	Specify the protocol for connecting to the LDAP directory server. Specifiable values: `ldap` Default value: `ldap`
`port`	Specify the port number of the LDAP directory server. Make sure beforehand that the port you specify is set as the listen port number on the LDAP directory server. Specifiable values: 1 to 65535 Default value: 389
`basedn`	Specify the BaseDN, which is the DN of the entry that will be used as the start point when searching for LDAP user information on the LDAP directory server. The user entries that are located in the hierarchy after this DN will be verified during authorization. Specify the DN of the hierarchy that includes all of the user entries to be searched. Specify the DN by following the rules defined in RFC4514. For example, if any of the following characters are included in a DN, you must use a backslash (`\`) to escape each character. Spaces `# + ; , < = > \` If characters that must be escaped are included in the specified BaseDN, escape all of those characters correctly because the specified value will be passed to the LDAP directory server without change. If you omit this attribute, the value specified in the `defaultNamingContext` property of Active Directory is assumed as the BaseDN. Default value: none
`timeout`	Specify the amount of time to wait before timing out when connecting to the LDAP directory server. If you specify `0`, the system waits until a communication error occurs without timing out. Specifiable values: 0 to 120 (seconds) Default value: 15
`retry.interval`	Specify the interval (in seconds) between tries to connect to the LDAP directory server. Specifiable values: 1 to 60 (seconds) Default value: 1

Attributes	Details
`retry.times`	Specify the number of times to try to connect to the LDAP directory server. If you specify 0, no further tries occur. Specifiable values: 0 to 50 Default value: 20
Note: To specify the attributes, use the following syntax: `auth.group.`*`domain-name`*`.`*`attribute`*`=`*`value`* For *domain-name*, specify the value specified for `auth.radius.`*`auth.server.name-property-value`*`.domain.name`.	

Examples of setting the exauth.properties file for RADIUS authentication

The following are examples of how to set the `exauth.properties` file when using a RADIUS server to perform authentication:

- When linking to only an external authentication server

```
auth.server.type=radius
auth.server.name=ServerName
auth.group.mapping=false
auth.radius.ServerName.protocol=PAP
auth.radius.ServerName.host=radius.example.com
auth.radius.ServerName.port=1812
auth.radius.ServerName.timeout=1
auth.radius.ServerName.retry.times=3
auth.radius.ServerName.attr.NAS-Identifier=host_A
```

- When directly specifying information about an external authorization server

```
auth.server.type=radius
auth.server.name=ServerName
auth.group.mapping=true
auth.ocsp.enable=false
auth.ocsp.responderURL=
auth.radius.ServerName.protocol=PAP
auth.radius.ServerName.host=radius.example.com
auth.radius.ServerName.port=1812
auth.radius.ServerName.timeout=1
auth.radius.ServerName.retry.times=3
auth.radius.ServerName.attr.NAS-Identifier=host_A
auth.radius.ServerName.domain.name=EXAMPLE.COM
auth.radius.ServerName.dns_lookup=false
auth.group.EXAMPLE.COM.protocol=ldap
auth.group.EXAMPLE.COM.host=ldap.example.com
auth.group.EXAMPLE.COM.port=389
auth.group.EXAMPLE.COM.basedn=dc=Example,dc=com
auth.group.EXAMPLE.COM.timeout=15
auth.group.EXAMPLE.COM.retry.interval=1
auth.group.EXAMPLE.COM.retry.times=20
```

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

```
auth.server.type=radius
auth.server.name=ServerName
auth.group.mapping=true
auth.radius.ServerName.protocol=PAP
auth.radius.ServerName.host=radius.example.com
auth.radius.ServerName.port=1812
auth.radius.ServerName.timeout=1
auth.radius.ServerName.retry.times=3
auth.radius.ServerName.attr.NAS-Identifier=host_A
auth.radius.ServerName.domain.name=EXAMPLE.COM
auth.radius.ServerName.dns_lookup=true
auth.group.EXAMPLE.COM.protocol=ldap
auth.group.EXAMPLE.COM.basedn=dc=Example,dc=com
auth.group.EXAMPLE.COM.timeout=15
auth.group.EXAMPLE.COM.retry.interval=1
auth.group.EXAMPLE.COM.retry.times=20
```

- When using a redundant configuration

```
auth.server.type=radius
auth.server.name=ServerName1,ServerName2
auth.group.mapping=false
auth.radius.ServerName1.protocol=PAP
auth.radius.ServerName1.host=radius1.example.com
auth.radius.ServerName1.port=1812
auth.radius.ServerName1.timeout=1
auth.radius.ServerName1.retry.times=3
auth.radius.ServerName1.attr.NAS-IP-Address=127.0.0.1
auth.radius.ServerName2.protocol=PAP
auth.radius.ServerName2.host=radius2.example.com
auth.radius.ServerName2.port=1812
auth.radius.ServerName2.timeout=1
auth.radius.ServerName2.retry.times=3
auth.radius.ServerName2.attr.NAS-IP-Address=127.0.0.1
```

Setup items in the exauth.properties file for Kerberos authentication

In the `exauth.properties` file, specify the type of the external authentication server, the server identification name, and the information about the external authentication server.

- Common properties

  See "Setup items in the exauth.properties file for Kerberos authentication (common items)"

- Properties for an external authentication server

  Specify these property values for each Kerberos server.

  Setup items in the `exauth.properties` file vary depending on whether information about the Kerberos server being connected to is directly specified or looked up by using the DNS server.

  - When directly specifying information about the Kerberos server:

    See "Setup items in the exauth.properties file for Kerberos authentication (when directly specifying information about the external authentication server)"

  - When using the DNS server to look up information about the Kerberos server:

    See "Setup items in the exauth.properties file for Kerberos authentication (when using the DNS server to look up information about the external authentication server)"

- Properties for an external authorization server

  These properties must be set if you directly specify information about the Kerberos server and an external authorization server is also linked. Specify the properties for each realm.

  See "Setup items in the exauth.properties file for Kerberos authentication (settings for the external authorization server)" or "Setup items in the exauth.properties file for Kerberos authentication (when an external authorization server and StartTLS are used for communication)

Note:

- Make sure to distinguish between uppercase and lowercase letters for property settings.

- To use StartTLS for communication between the management server and the LDAP directory server, you must directly specify information about the LDAP directory server to connect to in the `exauth.properties` file.

- If you use the DNS server to look up the LDAP directory server to connect to, it might take longer for users to log in.

Table 28 Setup items in the exauth.properties file for Kerberos authentication (common items)

Property names	Details
`auth.server.type`	Specify an external authentication server type. Specify `kerberos`. Default value: `internal` (used when not linking to an external authentication server)
`auth.group.mapping`	Specify whether to also link to an external authorization server. Specify `true` to link to an external authorization server. Specify `false` to not to link to an external authorization server. Default value: `false`

Table 29 Setup items in the exauth.properties file for Kerberos authentication (when directly specifying information about the external authentication server)

Attributes	Details
`default_realm`	Specify the default realm name. If you specify a user ID but not a realm name in the login window of the GUI, the user is authenticated as a user who belongs to the realm specified for this attribute. This attribute is required. Default value: none
`dns_lookup_kdc`	Specify `false`. Default value: `false`
`default_tkt_enctypes`	Specify the encryption type used for Kerberos authentication. You can use the following encryption types: ▪ AES256-SHA2 ▪ AES128-SHA2 ▪ AES256-CTS ▪ AES128-CTS ▪ RC4-HMAC ▪ DES3-CBC-SHA1 ▪ DES-CBC-MD5 ▪ DES-CBC-CRC

Attributes	Details
	To specify multiple encryption types, use a comma to separate the encryption types. Among the specified encryption types, an encryption type that is supported by both the management server OS and a Kerberos server will be used. Default value: None (AES256-SHA2, AES128-SHA2, AES256-CTS, or AES128-CTS is used for authentication.)
`clockskew`	Specify the acceptable range of difference between the management server time and Kerberos server time. If the difference exceeds this value, an authentication error occurs. Specifiable values: 0 to 300 (seconds) Default value: 300
`timeout`	Specify the amount of time to wait before timing out when connecting to the Kerberos server. If you specify 0, the system waits until a communication error occurs without timing out. Specifiable values: 0 to 120 (seconds) Default value: 3
`realm_name`	Specify the realm identification names. You can specify any name for this attribute to identify which realms the property attribute settings are applied to. You must specify at least one name. When specifying multiple realm identification names, separate the names with commas (`,`). Do not register the same realm identification name more than once. Default value: none
`value-specified-for-realm_name``.realm`	Specify the name of the realm set in the Kerberos server. This attribute is required. Default value: none
`value-specified-for-realm_name``.kdc`	Specify the information about the Kerberos server in the following format: *`host-name-or-IP-address`*`[:`*`port-number`*`]` This attribute is required.

<table>
<tr><th>Attributes</th><th>Details</th></tr>
<tr><td></td><td><b><i>host-name-or-IP-address</i></b>
If you specify the host name, make sure beforehand that the name can be resolved to an IP address. If you specify the IP address, use an IPv4 address. In an IPv6 environment, you must specify the host name. Note that you cannot specify the loopback address (<code>localhost</code> or <code>127.0.0.1</code>).
<b><i>port-number</i></b>
Make sure beforehand that the port you specify is set as the listen port number on the Kerberos server. If you do not specify a port number or the specified port number cannot be used in a Kerberos server, <code>88</code> is assumed.
When configuring the Kerberos server in redundant configuration, separate the servers with commas (<code>,</code>) as follows:
<code><i>host-name-or-IP-address</i>[:<i>port-number</i>]</code>
<code>,<i>host-name-or-IP-address</i>[:<i>port-number</i>],...</code>
<b>Note:</b> When using StartTLS as the protocol for connecting to the external authorization server, specify the same host name as the value of CN in the external authorization server certificate. You cannot use an IP address.</td></tr>
<tr><td colspan="2"><b>Note:</b> To specify the attributes, use the following syntax:
<code>auth.kerberos.<i>attribute</i>=<i>value</i></code></td></tr>
</table>

Table 30 Setup items in the exauth.properties file for Kerberos authentication (when using the DNS server to look up information about the external authentication server)

Attributes	Details
`default_realm`	Specify the default realm name. If you specify a user ID but not a realm name in the login window of the GUI, the user is authenticated as a user who belongs to the realm specified for this attribute. This attribute is required. Default value: none
`dns_lookup_kdc`	Specify `true`. This attribute is required. However, if all the following attributes values are already set, the Kerberos server will not be looked up by using the DNS server. ▪ `realm_name` ▪ *`value-specified-for-realm_name`*`.realm` ▪ *`value-specified-for-realm_name`*`.kdc`
`default_tkt_enctypes`	Specify the encryption type used for Kerberos authentication. You can use the following encryption types: ▪ AES256-SHA2 ▪ AES128-SHA2 ▪ AES256-CTS ▪ AES128-CTS ▪ RC4-HMAC ▪ DES3-CBC-SHA1 ▪ DES-CBC-MD5 ▪ DES-CBC-CRC To specify multiple encryption types, use a comma to separate the encryption types. Among the specified encryption types, an encryption type that is supported by both the management server OS and a Kerberos server will be used. Default value: None (AES256-SHA2, AES128-SHA2, AES256-CTS, or AES128-CTS is used for authentication.)

Attributes	Details
`clockskew`	Specify the acceptable range of difference between the management server time and Kerberos server time. If the difference exceeds this value, an authentication error occurs. Specifiable values: 0 to 300 (seconds) Default value: 300
`timeout`	Specify the amount of time to wait before timing out when connecting to the Kerberos server. If you specify `0`, the system waits until a communication error occurs without timing out. Specifiable values: 0 to 120 (seconds) Default value: 3
Note: To specify the attributes, use the following syntax: `auth.kerberos.attribute=value`	

Table 31 Setup items in the exauth.properties file for Kerberos authentication (settings for the external authorization server)

Attributes	Details
`protocol`	Specify the protocol for connecting to the LDAP directory server. When communicating in plain text format, specify `ldap`. When using StartTLS communication, specify `tls`. StartTLS communication can be used only when directly specifying information about the Kerberos server. Before specifying `tls`, make sure that one of the following encryption methods can be used on the LDAP directory server. For StartTLS, TLS 1.2 and TLS 1.3 are supported. ▪ TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ▪ TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ▪ TLS_RSA_WITH_AES_128_GCM_SHA256 ▪ TLS_RSA_WITH_AES_256_GCM_SHA384 ▪ TLS_AES_256_GCM_SHA384 ▪ TLS_AES_128_GCM_SHA256 ▪ TLS_CHACHA20_POLY1305_SHA256 Specifiable values: `ldap` or `tls`

Attributes	Details
	Default value: `ldap` **Note:** When communicating by using StartTLS as the protocol for connecting to the LDAP directory server, you must specify the security settings of Common Component.
`port`	Specify the port number of the LDAP directory server. Make sure beforehand that the port you specify is set as the listen port number on the LDAP directory server. Specifiable values: 1 to 65535 Default value: 389
`basedn`	Specify the BaseDN, which is the DN of the entry that will be used as the start point when searching for LDAP user information on the LDAP directory server. The user entries that are located in the hierarchy after this DN will be verified during authorization. Specify the DN of the hierarchy that includes all of the user entries to be searched. Specify the DN by following the rules defined in RFC4514. For example, if any of the following characters are included in a DN, you must use a backslash (`\`) to escape each character. Spaces `# + ; , < = > \` If characters that must be escaped are included in the specified BaseDN, escape all of those characters correctly because the specified value will be passed to the LDAP directory server without change. If you omit this attribute, the value specified in the `defaultNamingContext` property of Active Directory is assumed as the BaseDN. Default value: none
`timeout`	Specify the amount of time to wait before timing out when connecting to the LDAP directory server. If you specify `0`, the system waits until a communication error occurs without timing out. Specifiable values: 0 to 120 (seconds) Default value: 15
`retry.interval`	Specify the interval (in seconds) between tries to connect to the LDAP directory server. Specifiable values: 1 to 60 (seconds) Default value: 1

Attributes	Details
retry.times	Specify the number of tries to connect to the LDAP directory server. If you specify 0, no further tries occur. Specifiable values: 0 to 50 Default value: 20
Note: To specify the attributes, use the following syntax: `auth.group.realm-name.attribute=value` For *realm-name*, specify the value specified for `auth.kerberos.`*`realm_name-property-value`*`.realm`.	

Table 32 Setup items in the exauth.properties file for Kerberos authentication (when an external authorization server and StartTLS are used for communication)

Property	Details
auth.ocsp.enable	Specify whether to verify the validity of an LDAP directory server's electronic signature certificate by using an OCSP responder when the LDAP directory server and StartTLS are used for communication. To verify the validity of certificates, specify `true`. To not verify the validity of certificates, specify `false`. Default value: `false`
auth.ocsp.responderURL	Specify the URL of an OCSP responder to use an OCSP responder that is not the one written in the AIA field of the electronic signature certificate to verify the validity of the electronic signature certificate. If this value is omitted, the OCSP responder written in the AIA field is used. Default value: None

Examples of setting the exauth.properties file for Kerberos authentication

The following are examples of how to set the `exauth.properties` file when using a Kerberos server to perform authentication:

- When directly specifying information about a Kerberos server (when not linking to an external authorization server)

```
auth.server.type=kerberos
auth.group.mapping=false
auth.kerberos.default_realm=EXAMPLE.COM
auth.kerberos.dns_lookup_kdc=false
auth.kerberos.clockskew=300
auth.kerberos.timeout=3
auth.kerberos.realm_name=RealmName
auth.kerberos.RealmName.realm=EXAMPLE.COM
auth.kerberos.RealmName.kdc=kerberos.example.com:88
```

- When using the DNS server to look up a Kerberos server (when not linking to an external authorization server)

```
auth.server.type=kerberos
auth.group.mapping=false
auth.kerberos.default_realm=EXAMPLE.COM
auth.kerberos.dns_lookup_kdc=true
auth.kerberos.clockskew=300
auth.kerberos.timeout=3
```

- When directly specifying information about a Kerberos server (when also linking to an external authorization server)

  ```
  auth.server.type=kerberos
  auth.group.mapping=true
  auth.ocsp.enable=false
  auth.ocsp.responderURL=
  auth.kerberos.default_realm=EXAMPLE.COM
  auth.kerberos.dns_lookup_kdc=false
  auth.kerberos.clockskew=300
  auth.kerberos.timeout=3
  auth.kerberos.realm_name=RealmName
  auth.kerberos.RealmName.realm=EXAMPLE.COM
  auth.kerberos.RealmName.kdc=kerberos.example.com:88
  auth.group.EXAMPLE.COM.protocol=ldap
  auth.group.EXAMPLE.COM.port=389
  auth.group.EXAMPLE.COM.basedn=dc=Example,dc=com
  auth.group.EXAMPLE.COM.timeout=15
  auth.group.EXAMPLE.COM.retry.interval=1
  auth.group.EXAMPLE.COM.retry.times=20
  ```

- When using the DNS server to look up a Kerberos server (when also linking to an external authorization server)

  ```
  auth.server.type=kerberos
  auth.group.mapping=true
  auth.kerberos.default_realm=EXAMPLE.COM
  auth.kerberos.dns_lookup_kdc=true
  auth.kerberos.clockskew=300
  auth.kerberos.timeout=3
  ```

- When using a redundant configuration

```
auth.server.type=kerberos
auth.group.mapping=false
auth.kerberos.default_realm=EXAMPLE.COM
auth.kerberos.dns_lookup_kdc=false
auth.kerberos.clockskew=300
auth.kerberos.timeout=3
auth.kerberos.realm_name=S1
auth.kerberos.S1.realm=EXAMPLE.COM
auth.kerberos.S1.kdc=kerberos.example.com:88,kerberos.example.net:88
```

- When specifying multiple realm identifiers

```
auth.server.type=kerberos
auth.group.mapping=false
auth.kerberos.default_realm=EXAMPLE.COM
auth.kerberos.dns_lookup_kdc=false
auth.kerberos.clockskew=300
auth.kerberos.timeout=3
auth.kerberos.realm_name=S1,S2
auth.kerberos.S1.realm=EXAMPLE.COM
auth.kerberos.S1.kdc=kerberos1.example.com:88,kerberos1.example.net:88
auth.kerberos.S2.realm=EXAMPLE.NET
auth.kerberos.S2.kdc=kerberos2.example.com:88,kerberos2.example.net:88
```

About LDAP search user accounts

An LDAP search user account is used when an account needs to be authenticated or authorized, or when searching for information within an LDAP directory server.

In the following cases, you must register an LDAP search user account on the management server.

- When an LDAP directory server is used as an external authentication server and the data structure is the hierarchical structure model

- When an LDAP directory server is used as an external authorization server

  When registering an authorization group in Common Component products by using the GUI, to verify whether the distinguished name of the authorization group is registered on the external authorization server by using a user ID such as the `System` account registered in Common Component products, you must register a user account used to search for LDAP user information on the management server.

Except in the cases shown previously, this step is not necessary, because LDAP user information is not searched during authentication and authorization. If a user account used to search for LDAP user information has been already registered, delete it.

Conditions for LDAP search user account

Conditions for the LDAP search user account vary depending on the authentication method.

Prepare a user account that satisfies the following conditions on the LDAP directory server.

For LDAP authentication:

- The user account can bind to the DN specified for `auth.ldap.`*`auth.server.name-property-value`*`.basedn` in the `exauth.properties` file
- The user account can search the attributes for all entries after the DN specified for `auth.ldap.`*`auth.server.name-property-value`*`.basedn` in the `exauth.properties` file
- The user account can reference the DN specified for `auth.ldap.`*`auth.server.name-property-value`*`.basedn` in the `exauth.properties` file
- The user account can reference the authorization groups that are under the DN specified for `auth.ldap.`*`auth.server.name-property-value`*`.basedn` in the `exauth.properties` file (when an external authorization server is also linked to)
- The user account can search the attributes of the authorization groups that are under the DN specified for `auth.ldap.`*`auth.server.name-property-value`*`.basedn` in the `exauth.properties` file and search the attributes of nested groups of the authorization groups (when an external authorization server is also linked to)

For RADIUS authentication:

- The user account can bind to the DN specified for `auth.group.`*`domain-name`*`.basedn` in the `exauth.properties` file
- The user account can search the attributes for all entries after the DN specified for `auth.group.`*`domain-name`*`.basedn` in the `exauth.properties` file
- The user account can reference the DN specified for `auth.group.`*`domain-name`*`.basedn` in the `exauth.properties` file
- The user account can reference the authorization groups that are under the DN specified for `auth.group.`*`domain-name`*`.basedn` in the `exauth.properties` file.
- The user account can search the attributes of the authorization groups that are under the DN specified for `auth.group.`*`domain-name`*`.basedn` in the `exauth.properties` file and search the attributes of nested groups of the authorization groups

For Kerberos authentication:

- The user account can bind to the DN specified for `auth.group.`*`realm-name`*`.basedn` in the `exauth.properties` file

- The user account can search the attributes for all entries after the DN specified for `auth.group.`*`realm-name`*`.basedn` in the `exauth.properties` file

- The user account can reference the DN specified for `auth.group.`*`realm-name`*`.basedn` in the `exauth.properties` file

- The user account can reference the authorization groups that are under the DN specified for `auth.group.`*`realm-name`*`.basedn` in the `exauth.properties` file

- The user account can search the attributes of the authorization groups that are under the DN specified for `auth.group.`*`realm-name`*`.basedn` in the `exauth.properties` file and search the attributes of nested groups of the authorization groups

Registering an LDAP search user account

Use the `hcmds64ldapuser` command to register an LDAP search user account on the management server.

Before you begin

- Register an LDAP search user on the LDAP directory server.
- Verify the following information:
  - DN and password of the LDAP search user
  - Server identification name or the domain name for external authentication servers of the LDAP directory server (for LDAP authentication)

    Specify the server identification name that was specified for the `auth.server.name` property in the `exauth.properties` file, or specify the domain name specified for `auth.ldap.`*value-specified-for-auth.server.name*`.domain.name` property in the `exauth.properties` file.
  - Domain name of the RADIUS server (for RADIUS authentication)

    Specify the domain name specified for `auth.radius.`*`auth.server.name-property-value`*`.domain.name` in the `exauth.properties` file.
  - Realm name of the Kerberos server (for Kerberos authentication)

    If you directly specify information about a Kerberos server in the `exauth.properties` file, specify the value specified for `auth.kerberos.default_realm` or `auth.kerberos.`*`auth.kerberos.realm_name-property-value`*`.realm`.

    If you specify the settings in the `exauth.properties` file to use the DNS server to look up information about a Kerberos server, specify the realm name registered in the DNS server.

Procedure

1. Execute the `hcmds64ldapuser` command.

   In Windows:

   ```
   Common-Component-installation-folder\bin
   \hcmds64ldapuser /set /dn DN-of-user-account-used-to-search-
   for-LDAP-user-info [/pass password-of-user-account-used-to-
   search-for-LDAP-user-info] /name name
   ```

In Linux:

```
Common-Component-installation-directory/bin/hcmds64ldapuser
-set -dn DN-of-user-account-used-to-search-for-LDAP-user-
info [-pass password-of-user-account-used-to-search-for-
LDAP-user-info] -name name
```

- *DN-of-user-account-used-to-search-for-LDAP-user-info*

  Specify a DN by following the rules defined in RFC4514. For example, if the following characters are included in a DN, you must use a backslash (`\`) to escape each character.

  Spaces `# + , ; < = > \`

- *password-of-user-account-used-to-search-for-LDAP-user-info*

  This is case-sensitive and must exactly match the password registered in the LDAP directory server. If you execute the command without specifying the `pass` option, you will be prompted to enter a password.

Note:

- In the LDAP directory server, you can use double quotation marks (`"`) for the DN and password. In the management server, however, you must register a user account whose DN and password do not include double quotation marks.
- If you are using Active Directory, you can use the `dsquery` command provided by Active Directory to verify the DN of a user. The following example shows how to use the `dsquery` command to verify the DN of the user `administrator`, and also shows the execution results:

  ```
  dsquery user -name administrator
  ```

  ```
  "CN=administrator,CN=admin,DC=example,DC=com"
  ```

- If the DN includes commas such as `cn=administrator,cn=admin,dc=example,com`, specify as follows:

  In Windows:

  ```
  hcmds64ldapuser /set /dn
  "cn=administrator,cn=admin,dc=example\,com" /pass
  administrator_pass /name ServerName
  ```

  In Linux:

  ```
  hcmds64ldapuser -set -dn
  "cn=administrator,cn=admin,dc=example\\,com" -pass
  administrator_pass -name ServerName
  ```

Deleting an LDAP search user account

Before you begin

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

Verify the following information:

- Server identification name or the domain name for external authentication servers of the LDAP directory server (for LDAP authentication)
- Domain name of the RADIUS server (for RADIUS authentication)
- Realm name of the Kerberos server (for Kerberos authentication)

Procedure

1. Execute the `hcmds64ldapuser` command.

   In Windows:

   ```
   Common-Component-installation-folder\bin\hcmds64ldapuser /
   delete /name name
   ```

   In Linux:

   ```
   Common-Component-installation-directory/bin/hcmds64ldapuser
   -delete -name name
   ```

Verifying the LDAP directory server that registered the LDAP search user account

Use the **`hcmds64ldapuser`** command to verify which LDAP directory server has registered the LDAP search user account on the management server.

Procedure

1. Run the `hcmds64ldapuser` command.

   In Windows:

   ```
   Common-Component-installation-folder\bin\hcmds64ldapuser /
   list
   ```

   In Linux:

   ```
   Common-Component-installation-directory/bin/hcmds64ldapuser
   -list
   ```

Registering a shared secret

Before you begin

Use the **`hcmds64radiussecret`** command to register the RADIUS shared secret on the management server.

Verify the following information:

- Shared secret
- RADIUS server indication name

  RADIUS-server-indication-name must match a server indication name specified for the `auth.server.name` property in the `exauth.properties` file.

Procedure

1. Run the `hcmds64radiussecret` command.

   In Windows:

   ```
   Common-Component-installation-folder\bin\hcmds64radiussecret
   [/set shared-secret] /name RADIUS-server-indication-name
   ```

   In Linux:

   ```
   Common-Component-installation-directory/bin/
   hcmds64radiussecret [-set shared-secret] -name RADIUS-
   server-indication-name
   ```

   - If you execute the command without specifying the `set` option, you will be prompted to enter a shared secret.

Deleting a shared secret

Before you begin

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

Verify the RADIUS server indication name.

Procedure

1. Run the `hcmds64radiussecret` command.

   In Windows:

   ```
   Common-Component-installation-folder\bin
   \hcmds64radiussecret /delete /name RADIUS-server-indication-
   name
   ```

   In Linux:

   ```
   Common-Component-installation-directory/bin/
   hcmds64radiussecret -delete -name RADIUS-server-indication-
   name
   ```

Verifying the RADIUS server that registered a shared secret on the management server

Use the **`hcmds64radiussecret`** command to verify which RADIUS server has registered the shared secret on the management server.

Procedure

1. Run the `hcmds64radiussecret` command.

   In Windows:

   ```
   Common-Component-installation-folder\bin
   \hcmds64radiussecret /list
   ```

   In Linux:

   ```
   Common-Component-installation-directory/bin/
   hcmds64radiussecret -list
   ```

Result

The server identification name of the RADIUS server is displayed.

Verifying connections to an external authentication server and an external authorization server

Before you begin

Use the **`hcmds64checkauth`** command to verify whether the management server is correctly connected to the external authentication server and the external authorization server.

- Register an external authentication server and an external authorization server
- Verify the following information:
  - For LDAP authentication

    Verify the user accounts registered on the LDAP directory server. For user IDs, specify the value saved in the attribute specified by `auth.ldap.`*`value-specified-in-auth.server.name`*`.attr` in the `exauth.properties` file.
  - For RADIUS authentication

    Verify the user accounts registered on the RADIUS server.
  - For Kerberos authentication

    When linking only to an external authentication server:

    Verify the user accounts that are registered in Common Component products and whose authentication method is Kerberos authentication.

    When also linking to an external authorization server:

    Verify the user accounts not registered in Common Component products.

    In addition, if you specify a user who belongs to a realm other than the realm specified for `default_realm` in the `exauth.properties` file, also verify the realm that the user belongs to. If more than one realm name is specified in the `exauth.properties` file, verify all specified realm names.

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

Procedure

1. Run the **`hcmds64checkauth`** command.

   In Windows:

   ```
   Common-Component-installation-folder\bin\hcmds64checkauth [/
   user user-ID /pass password] [/summary]
   ```

In Linux:

```
Common-Component-installation-directory/bin/hcmds64checkauth
[-user user-ID -pass password] [-summary]
```

- If you run the command without specifying the `user` option or the `pass` option, you will be prompted to enter a user ID and password.
- If you run the command with the `summary` option specified, the confirmation message is displayed in summary format.

Note: When using the Kerberos authentication method, if more than one realm name is specified in the `exauth.properties` file, verify the connection for each realm name. In addition, specify user IDs according to the following:

- To specify a user belonging to a realm other than the realm set for `default_realm` in the `exauth.properties` file:

  user-ID`@`*realm-name*

- To specify a user who belongs to the realm set for `default_realm` in the `exauth.properties` file:

  You can omit the realm name.

- When using the LDAP authentication method, if the `hcmds64checkauth` command is executed, all connected external authentication servers are verified and the verification results for each external authentication server are displayed.

  For external authentication servers for which the user account specified for the `hcmds64checkauth` command is not registered, an error message indicating that the user account is not registered is displayed in phase 3 of the verification result, and confirmation at phase 3 might fail.

  When this occurs, verify the connection of each external authentication server by using a user account that is registered to that server.

Result

Settings in the `exauth.properties` file and connections to the external authentication server and external authorization server are verified, and verification results are displayed in each of four phases. The following message is displayed if the verifying in each phase finishes normally.

```
KAPM15004-I The result of the configuration check of Phase phase-number was normal.
```

Phase 1

The command verifies that common properties have been correctly specified in the `exauth.properties` file.

Phase 2

The command verifies that the properties for the external authentication server and properties for the external authorization server have been correctly specified in the `exauth.properties` file.

Phase 3

The command verifies that the external authentication server can be connected to.

Phase 4

If an external authorization server is also linked to, the command verifies that the external authorization server can be connected to and authorization groups can be searched.

Command notes for setting up a link to an external authentication server

If command line control characters are included in the arguments of commands that will be executed when specifying the settings to link to an external authentication server, escape the characters correctly according to the specifications of the command line.

Also, you must pay attention to backslashes (`\`) included in the arguments because they are treated specially in the command line.

The following explains how to escape when running the **`hcmds64ldapuser`** command, **`hcmds64radiussecret`** command, or **`hcmds64checkauth`** command.

In Windows:

If the following characters are included in an argument, enclose the argument in double quotation marks (`"`) or use a caret (`^`) to escape each character:

Spaces `& | ^ < > ( )`

A backslash might be treated as an escape character depending on the character that follows it. Therefore, if a backslash and any of the previous characters are included in an argument, use a caret to escape each character rather than enclose the argument in double quotation marks.

Also, if there is a backslash at the end of an argument, escape it by using another backslash.

In Linux:

If the following characters are included in an argument, enclose the argument in double quotation marks or use a backslash to escape each character:

Spaces `# & ' ( ) ~ \ ` < > ; |`

Note that a backslash in an argument is treated as an escape character even if the argument is enclosed in double quotation marks. If a backslash is included in an argument, escape it by using another backslash.

For example, if a shared secret to be registered by the `hcmds64radiussecret` command is `secret01\`, escape it as follows:

In Windows:

```
hcmds64radiussecret /set secret01\\ /name ServerName
```

In Linux:

Use either of the following formats:

```
hcmds64radiussecret -set secret01\\ -name ServerName
```

```
hcmds64radiussecret -set "secret01\\" -name ServerName
```

Encryption types for Kerberos authentication

Configure the Kerberos server so that the encryption types supported by Common Component products can be used.

In Common Component products, the following encryption types can be used for Kerberos authentication.

- AES256-SHA2
- AES128-SHA2
- AES256-CTS
- AES128-CTS
- RC4-HMAC
- DES3-CBC-SHA1
- DES-CBC-MD5
- DES-CBC-CRC

Chapter 6: Backing up and restoring Ops Center Automator

This module describes how to backup and restore Ops Center Automator.

Overview of backup and restore

Ops Center Automator allows you to backup and restore your system in case a failure occurs and your system go down.

Use cases

Periodic backup

Prepare for any failures by periodically backing up your data as part of your normal operations. Then, if a failure occurs, restore the backed up data to recover from the failure.

Re-installation of the OS on the same management server

System configuration and database information can be carried over.

Move to another host

You can use the backup and restore feature to move Ops Center Automator to another host. System configuration and database information can also be carried over.

Ops Center Automator does not support periodic automatic backup. Create a backup schedule that fits your requirements and perform a manual backup.

Backing up Ops Center Automator

Ops Center Automator allows you to back up your system configuration and database information.

Before you begin

On the Tasks tab, verify that there is no task in the In Progress, Waiting for Input, In Progress (with Error), Long Running, or In Progress (Terminating) status.

Procedure

1. Log on to the management server using Administrator privilege (for Windows) or root privilege (for Linux).

2. Stop the services or disable failover.

   - For a non-cluster environment:

     Stop the Ops Center Automator and Common Component services by running the **`hcmds64srv /stop`** command.

   - For a cluster environment:

     Run the following command to take the group where the Ops Center Automator and Common Component services are registered offline and disable failover.

     ```
     Common-Component-installation-folder\ClusterSetup\hcmds64clustersrvstate /
     soff /r group-name
     ```

3. Run the **`backupsystem`** command.
4. Start the services or enable failover.

   - For a non-cluster environment:

     Start the Ops Center Automator and Common Component services by running the **`hcmds64srv /start`** command.

   - For a cluster environment:

     Run the following command to take the group where the Ops Center Automator and Common Component services are registered online and enable failover.

     ```
     Common-Component-installation-folder\ClusterSetup
     \hcmds64clustersrvstate /son /r group-name
     ```

Restoring Ops Center Automator

Ops Center Automator allows you to restore your system configuration and database information.

Before you begin

Make sure following settings are the same between the backup source host and the restore destination host:

- The host name and IP address
- The account of the OS user used by Ops Center Automator
- The Hitachi Ops Center product environment (configuration, version, and revision)
- The installation path of Ops Center Automator
- The system locale and character set

You should also make sure that no tasks are currently being processed in the "Status" column of the Tasks tab of Ops Center Automator with the indication "In Progress", "Waiting for Input", "In Progress (with Error)", "Long Running", or "In Progress (Terminating)".

Procedure

1. Log on to the management server using Administrator privilege (for Windows) or root privilege (for Linux).
2. Complete a backup of Ops Center Automator on the source host.

   See Backing up Ops Center Automator (on page 184) for the steps to do this.
3. Transfer the archived backup to the destination host.
4. Stop the services or disable failover.
   - For a non-cluster environment:

     Stop the Ops Center Automator and Common Component services by running the **`hcmds64srv /stop`** command (on page 210).
   - For a cluster environment:

     Run the following command to take the group where the Ops Center Automator and Common Component services are registered offline and disable failover.

   ```
   Common-Component-installation-folder\ClusterSetup\hcmds64clustersrvstate /
   soff /r group-name
   ```
5. Run the **`restoresystem`** command (on page 230) to restore the backup.
6. Reconfigure the following settings to match the destination environment.

   > **Note:** When you use Ops Center Automator in a cluster environment, you must reconfigure the property files listed in the following table on both the active and standby nodes.

To set	See
External authentication server integration (`exauth.properties`[1])	Registering an external authentication server and an external authorization server (on page 137) and Registering an LDAP search user account (on page 174)
Password policy (`security.conf`[2])	Changing the password policy (on page 112)
Audit log (`auditlog.conf`[2])	Enabling audit logging (on page 89)
Port number[3] (`user_httpsd.conf`[4])	Changing the port number used for management server communication with management clients (on page 51) and Common Component property updates for port number changes (on page 53)
Secure communications	Configuring secure communications (on page 58)
Server managing the user account	Changing the information of the server managing the user account (on page 55)

To set	See
Agentless connection private key	Public key authentication (on page 126)
RADIUS server shared private key	Registering a shared secret (on page 178)
Performance mode	Configuring the performance mode (on page 109)
Warning banner	hcmds64banner command (on page 197)

1. The backup source file is stored in the following location:

- For Windows:

```
Backup-destination-folder\HBase\base\conf
```

- For Linux:

```
Backup-destination-directory/HBase/base/conf
```

2. The backup source file is stored in the following location:

- For Windows:

```
Backup-destination-folder\HBase\base\conf\sec
```

- For Linux:

```
Backup-destination-directory/HBase/base/conf/sec
```

3: This setting is required if it had been changed from the default.

4: The backup source file is stored in the following location:

- For Windows:

```
Backup-destination-folder\HBase\base\httpsd.conf
```

- For Linux:

```
Backup-destination-directory/HBase/base/httpsd.conf
```

7. Start the services or enable failover.
   - For a non-cluster environment:

     Start the Ops Center Automator and Common Component services by running the **`hcmds64srv /start`** command.
   - For a cluster environment:

     Run the following command to take the group where the Ops Center Automator and Common Component services are registered online and enable failover.

```
Common-Component-installation-folder\ClusterSetup
\hcmds64clustersrvstate /son /r group-name
```

Moving Ops Center Automator to another host

If necessary, you can move Ops Center Automator from one host to another.

Note: If the host name or IP address of the replacement source and host name or IP address of the replacement destination are different, you must change the management server host name.

Before you begin

Make sure following settings are the same between the source host and the replacement destination host:

- The host name and IP address
- The account of the OS user used by Ops Center Automator
- The Hitachi Ops Center product environment (configuration, version, and revision)
- The installation path of Ops Center Automator
- The system locale and character set

You should also make sure that no tasks are currently being processed in the "Status" column of the Tasks tab of Ops Center Automator with the indication "In Progress", "Waiting for Input", "In Progress (with Error)", "Long Running", or "In Progress (Terminating)".

Procedure

1. Log on to the management server using Administrator privilege.
2. Complete a backup of Ops Center Automator on the source host.
   a. Stop the current services by running the **`hcmds64srv /stop`** command.
   b. Run the **`backupsystem`** command (on page 217) to perform the backup.
3. Transfer the archived backup file to the replacement destination host.
4. Log on to the management server for the destination host.
5. Complete a restore of Ops Center Automator on the replacement destination host.
   a. Stop the services by running the **`hcmds64srv /stop`** command (on page 210).

b. Run the **`restoresystem`** command (on page 230) to restore the backup.

c. Reconfigure the following settings to match the environment of the restore destination.

To set	See
External authentication server integration (`exauth.properties`[1])	Registering an external authentication server and an external authorization server (on page 137) and Registering an LDAP search user account (on page 174)
Password policy (`security.conf`[2])	Changing the password policy (on page 112)
Audit log (`auditlog.conf`[2])	Enabling audit logging (on page 89)
Port number[3] (`user_httpsd.conf`[4])	Changing the port number used for management server communication with management clients (on page 51) and Common Component property updates for port number changes (on page 53)
Secure communications	Configuring secure communications (on page 58)
Server managing the user account	Changing the information of the server managing the user account (on page 55)
Agentless connection private key	Public key authentication (on page 126)
RADIUS server shared private key	Registering a shared secret (on page 178)
Performance mode	Configuring the performance mode (on page 109)
Warning banner	hcmds64banner command (on page 197)

1. The backup source file is stored in the following location:

For Windows:

```
backup-destination-folder\HBase\base\conf
```

For Linux:

```
backup-destination-directory/HBase/base/conf
```

To set	See

2. The backup source file is stored in the following location:

For Windows:

```
backup-destination-folder\HBase\base\conf\sec
```

For Linux:

```
backup-destination-directory/HBase/base/conf/sec
```

3. This setting is required if it has been changed from the default.

4. The backup source file is stored in the following location:

For Windows:

```
backup-destination-folder\HBase\base\httpsd.conf
```

For Linux:

```
backup-destination-directory/HBase/base/httpsd.conf
```

6. Remove and register Ops Center Automator from Common Services.
   a. Remove Ops Center Automator from Common Services. To remove Ops Center Automator, see the *Hitachi Ops Center Installation and Configuration Guide*.
   b. Run the **`setupcommonservice`** command to apply the changes to Common Services.
   c. If necessary, change permissions for user groups and service groups.
7. Restart the services by running the **`hcmds64srv /start`** command.

Backing up and recovering using Ops Center Protector

You can schedule automatic backups for your Ops Center products by using Ops Center Protector. For information about how to use Ops Center to back up and restore, go the documentation portal, and select Management Software > Ops Center > Getting Started with Ops Center > Backing up and recovering Ops Center products using Ops Center Protector.

Chapter 7: Removing Ops Center Automator

This module describes how to remove Ops Center Automator.

Removing Ops Center Automator (Windows OS)

You can remove Ops Center Automator in a Windows environment by completing the steps listed in the following sections.

Before you begin

- If tasks in the Status column of the Tasks tab of Ops Center Automator are in the Waiting, Waiting for Input, In Progress, Long Running, or In Progress (with Error) state, wait until the tasks stop or finish running.
- Close all of the service dialog boxes.
- Close any Windows Services or open command prompts.
- Disable any security monitoring, virus detection, or process monitoring software on the server.

> ⚠ **Caution:** If other Common Component products are installed in the same host, do not delete the shared folder (`\Base64`). If you delete this folder, other Common Component products will not work properly.

Procedure

1. Log on to Windows OS as a user with Administrator permissions.
2. Run the following command to stop all services:
   ```
   Common-Component-installation-folder\bin\hcmds64srv /stop
   ```
3. Open the **Control Panel**, and then choose **Programs and Features** or **Uninstall a Program**.
4. Select **Hitachi Ops Center Automator**, and then click **Uninstall**, or select the program, right-click, and select **Uninstall**.
5. In the **Automation Software** window, click **Next** > **Remove** to start the software removal process.
   The removal process deletes the Ops Center Automator installation folder.
6. If you use Common Services, delete Ops Center Automator information from Common Services.

Result

Ops Center Automator is removed from the host.

Microsoft Visual C++ 2015-2022 Redistributable (x64) is not automatically removed. Make sure that other programs are not dependent on it, and remove it manually.

Removing Ops Center Automator software in a cluster environment

You can remove the Ops Center Automator software from the server in a cluster environment to migrate to a different server or stop Ops Center Automator processes.

> **Note:** If you remove Ops Center Automator, the properties files, log files, and other product-related files are deleted.

Procedure

1. In the cluster management software, move the group in which the Common Component services are registered from the standby node to the active node by right-clicking the group, selecting **Move**, and then either **Select Node** or **Move this service or application to another node**.
2. Take offline and disable failover for the group in which Common Component services including Ops Center Automator are registered by using the following command:

   ```
   Common-Component-installation-directory\ClusterSetup
   \hcmds64clustersrvstate /soff /r cluster-group-name
   ```

   where

   `r` - specifies the name of the group in which the Common Component product services including Ops Center Automator are registered. If the group name contains spaces, you must enclose the group name in quotation marks ("). For example, if the group name is Automator cluster, specify "Automator cluster".

3. Delete the Common Component services including Ops Center Automator by using the following command:

   > **Note:** Before deleting the services, delete the "customer script" from the cluster management software.

   ```
   Common-Component-installation-directory\ClusterSetup
   \hcmds64clustersrvupdate /sdel /r cluster-group-name
   ```

   where

   `r` - specifies the name of the group in which the Common Component product services including Ops Center Automator are registered. If the group name contains spaces, you must enclose the group name in quotation marks ("). For example, if the group name is Automator cluster, specify "Automator cluster".

> **Note:**
>
> - All Ops Center Automator and Common Component product services that are registered in the group specified by the r option are deleted.
> - If you plan to continue using Common Component products, reregister them after you remove Ops Center Automator. Deleting the Ops Center Automator service does not cause a problem.
>
>   Remember that if you changed the service resource names, all resource names are reinitialized when the services are reregistered. Therefore, you must write down the resource names for the services that you are deleting, and change the names after reregistering those services.

4. Use the following command to stop the Common Component products:

   ```
   Common-Component-installation-folder\bin\hcmds64srv /stop
   ```
5. Remove Hitachi Ops Center Automator from the active node.
6. On the active node, delete any files and folders that are no longer required (such as those files and folders created during installation in the cluster environment).
7. In the cluster management software, move the Ops Center Automator service group to the standby node by right-clicking the group, selecting **Move**, and selecting either **Select Node** or **Move this service or application to another node**.
8. Remove Ops Center Automator from the standby node.
9. After performing the removal of the cluster installation, delete the Ops Center Automator folder and, if you no longer plan to use any other Common Component services, also delete the `Base64` folder from the standby node.
10. If the following resources are not in use by other applications, use the cluster management software to take them offline, and then delete them:
    - IP address
    - Shared disk
11. On the standby node, delete any files and folders that are no longer required (such as those files and folders created during installation in the cluster environment).

12. To continue using other Common Component products, use the following command to register the Common Component services in the cluster management software group:

    ```
    Common-Component-installation-folder\ClusterSetup
    \hcmds64clustersrvupdate /sreg /r cluster-group-name /sd drive-
    letter-of-shared-disk /ap resource-name-for-client-access-point
    ```

    where

    `r` - specifies the name of the group in which you to plan to register the Common Component product services. If the group name contains spaces, you must enclose the group name in quotation marks ("). For example, if the group name is Automator cluster, specify "Automator cluster".

    `sd` - specifies the drive letter of the shared disk that is registered to the cluster management software. You cannot specify multiple drive letters for this option. If the database of Common Component products is divided into multiple shared disks, run the `hcmds64clustersrvupdate` command for each shared disk.

    `ap` - specifies the name of the resource for the client access point that is registered to the cluster management software.

13. To continue using other Common Component products, use the following command to bring online and enable failover for the group in which the Common Component services are registered:

    ```
    Common-Component-installation-folder\ClusterSetup
    \hcmds64clustersrvstate /son /r cluster-group-name
    ```

    where

    `r` - specifies the name of the group in which the Common Component product services are registered. If the group name contains spaces, you must enclose the group name in quotation marks ("). For example, if the group name is Automator cluster, specify "Automator cluster".

14. In the cluster management software, move the group containing the Common Component resources to the active node by right-clicking the group, selecting **Move**, and then selecting either **Select Node** or **Move this service or application to another node**.
15. If you are using Common Services, delete the Ops Center Automator information from Common Services.

Result

Ops Center Automator is removed from both the active and standby nodes.

Microsoft Visual C++ 2015-2022 Redistributable (x64) is not automatically removed. Make sure that other programs are not dependent on it, and remove it manually.

Deleting authentication data (Windows OS)

If the `KNAE04574-E` warning dialog box appears although the removal completes successfully, the deletion of authentication data failed. Delete the data by running the **`hcmds64intg`** command on the server that administers user accounts (on the host running the product using Common Component and connected to the server)

To run the **`hcmds64intg`** command to delete the authentication data from a Windows host:

Procedure

1. Start all installed services of the products using Common Component products by running the following command:
   `Common-Component-installation-folder\bin\hcmds64srv /start`
2. Delete the authentication data by running the following command: `Common-Component-installation-folder\bin\hcmds64intg /delete /type component-name /user user-id /pass password`

   - `/type`

     Specify the name of the component that you want to delete. `Automation` can be specified.

   - `/user`

     Specify the user ID of a user who has the Admin (user management) permission. If you run the command without the user option, you are prompted to specify a user ID.

   - `/pass`

     Specify the password of a user who has the Admin (user management) permission. If you run the command without the pass option, you are prompted to specify a password.

Note: If you display a GUI window of another product using Common Component without deleting the authentication data, the following problems might occur, even after removing the Ops Center Automator server:

- User management information of the Ops Center Automator server displays.
- The button used to start the Ops Center Automator server is enabled on the dashboard. Clicking the enabled button causes a link error to appear.

Note: If you use Common Services, see the Hitachi Ops Center online help for the steps to delete a user account.

Removing Ops Center Automator (Linux OS)

You can remove Ops Center Automator in a Linux OS environment as listed in the following procedure.

Procedure

1. Run the following command: `*Directory-specified-when-installing-Automation-software*/ADUninstall/uninstall.sh`
2. If you use Common Services, delete Ops Center Automator information from Common Services.

Deleting authentication data (Linux OS)

If the `KNAE04574-E` warning dialog box appears although the removal completes successfully, the deletion of authentication data failed. Delete the data by running the **`hcmds64intg`** command on the server that administers user accounts (on the host running the product using Common Component and connected to the server)

Procedure

1. Start all installed services of the products using Common Component product by running the following command:
   `*Common-Component-installation-directory*/bin/hcmds64srv -start`
2. Delete the authentication data by running the following command: `*Common-Component-installation-directory*/bin/hcmds64intg -delete -type *component-name* -user *user-id* -pass *password*`
   - `-type`

     Specify the name of the component that you want to delete. `Automation` can be specified.
   - `-user`

     Specify the user ID of a user who has the Admin (user management) permission. If you run the command without the user option, you are prompted to specify a user ID.
   - `-pass`

     Specify the password of a user who has the Admin (user management) permission. If you run the command without the pass option, you are prompted to specify a password.

   Note: If you display a GUI window of another product using Common Component without deleting the authentication data, the following problems might occur, even after removing the Ops Center Automator server:

   - User management information of the Ops Center Automator server displays.
   - The button used to start the Ops Center Automator server is enabled on the dashboard. Clicking the enabled button causes a link error to appear.

   Note: If you use Common Services, see the Hitachi Ops Center online help for the steps to delete a user account.

Chapter 8: CLI commands

A set of Ops Center Automator and Common Component commands are available to run on the command line interface (CLI).

To run CLI commands, the Admin, Modify, or Submit role is required for Ops Center Automator and Administrator permission is required for the OS.

Common Component CLI commands

A set of Common Component commands are available on the CLI.

For Windows-based OS servers, navigate to `<system-drive>\Program Files\hitachi\Base64\bin`. For Linux OS servers, navigate to: `/opt/hitachi/Base64/bin`. Open the command prompt to run Common Component commands.

> **Note:** Regarding the **`hcmds64clustersrvupdate`** command and the **`hcmds64clustersrvstate`** command, the location of the file is different. For Windows-based OS servers, navigate to `<system-drive>\Program Files\hitachi\Base64\ClusterSetup`. For Linux OS servers, navigate to: `/opt/hitachi/Base64/ClusterSetup`.

> **Note:** When the Ops Center Automator server is using the Linux OS, read "/" to "-" is used for each argument.

hcmds64banner command

The **`hcmds64banner`** command registers and deletes a message displayed on a warning banner for Ops Center Automator.

Before executing this command, use a text editor to create a message.

Sample messages in English (`bannermsg.txt`) and Japanese (`bannermsg_ja.txt`) are provided in the following locations:

- In Windows:

```
Common-Component-installation-folder\sample\resource
```

- In Linux:

```
Common-Component-installation-directory/sample/resource
```

These sample files are overwritten at installation, so to use a sample file, copy it and then edit it.

The following shows the default message:

```
<center><b>Warning Notice!</b></center>
This is a {Company Name Here} computer system, which may be accessed and used only
for authorized {Company Name Here} business by authorized personnel. Unauthorized
access or use of this computer system may subject violators to criminal, civil,
and/or administrative action.
<br>
All information on this computer system may be intercepted, recorded, read, copied,
and disclosed by and to authorized personnel for official purposes, including
criminal investigations. Such information includes sensitive data encrypted to comply
with confidentiality and privacy requirements. Access or use of this computer system
by any person, whether authorized or unauthorized, constitutes consent to these
terms. There is no right of privacy in this system.
```

The syntax is:

```
hcmds64banner {/add /file file-name [/locale locale-name]}
 | {/delete [/locale locale-name]}
```

where:

- `/add` registers a message. If it is already registered, it is overwritten.
- `/delete` deletes a message.
- `/file` Using an absolute path, specify the file that stores the message. In Linux, do not specify a path that includes a space.
- `/locale` specifies the locale of the language used for the message (for example, `en` for English, or `ja` for Japanese). If this setting is omitted, the registered message will always be displayed in the warning banner regardless of the locale (the message is registered as a message of the default locale).

  When the GUI is used in multiple locales, if you register a message with the same contents in a different language for each locale, the message can be automatically switched to match the locale of the web browser.

  When multiple languages are specified on one web browser, the locale of the warning banner is determined by the language priority settings of the web browser.

Remarks

When Ops Center Automator is running in a cluster configuration, run this command on both the active host and standby host.

hcmds64checkauth command

The **`hcmds64checkauth`** command verifies the settings in the configuration file for external authentication server linkage and the connection with an external authentication server when Ops Center Automator links with the external authentication server.

If you run this command, the command will perform verifications in the following four phases, and then the results will be displayed:

1. The command verifies whether the property used when connecting to the external authentication server is correctly set in the `exauth.properties` file.
2. The command verifies whether the properties for the external authentication server and the external authorization server are correctly set in the `exauth.properties` file.
3. The command verifies whether a connection to the external authentication server can be established.
4. If the settings are specified so that an external authorization server is also connected, the command verifies whether a connection to the external authorization server can be established, and whether the authorization group can be searched.

The following message is displayed if the verification in each phase finishes normally.

```
KAPM15004-I The result of the configuration check of Phase phase-number
was normal.
```

The syntax is:

```
hcmds64checkauth [/user user-name] [/summary]
```

Note: You are prompted to enter the password in interactive mode.

where:

- `/user` specifies the username which has already been registered in the external authentication server.
- `/summary` simplifies the confirmation message that appears when the command is run. If this option is specified, the messages to be displayed are limited to messages indicating whether each processing phase is successful or failed, error messages, and messages indicating the results. However, if an error message similar to the message indicating the results is to appear, the former error message is omitted and only the latter resulting message is displayed.

hcmds64chgurl command

The **`hcmds64chgurl`** command changes the URLs of the products using Common Component that are registered on the GUI. After starting a Common Component process, if a product URL is changed due to any of the following configuration changes, you must use the **`hcmds64chgurl`** command to change the URL registered in the GUI for each product.

- Changing a port used by HBase 64 Storage Mgmt Web Service
- Changing the host name or IP address of the management server
- Changing the settings for enabling or disabling SSL communication

The syntax is:

```
hcmds64chgurl {/print | /list | /change old-URL new-URL | /change new-URL /type
Common-Component-product-name}
```

where:

- `/print` displays a list of URLs and programs that are currently registered.
- `/list` displays the same information as the /print option in a different format.
- `/change` changes a currently registered URL.
- `/type` To change the URL for a specific product using Common Component, use this option to specify the name of that product. To change only the Ops Center Automator URL, specify `Automation`.

Caution: The specified URL must be a complete URL that contains protocols and a port number. You cannot use an IPv6 address. You must use a host name to specify the URL in an IPv6 environment, as shown in the following example:

```
http://hostname:22015
```

When changing the URL during migration to a cluster environment, use the following format to specify *new-URL*:

```
http://logical-host-name:port-number
```

hcmds64clustersrvstate command

The **`hcmds64clustersrvstate`** command brings online and enables failover for the group in which the Common Component services including Ops Center Automator are registered. This command also takes offline and disables failover for the group in which Common Component services including Ops Center Automator are registered.

To bring online and enable failover for the group in which the Common Component services including Ops Center Automator are registered, the syntax is:

```
hcmds64clustersrvstate /son /r  cluster-group-name
```

To take offline and disable failover for the group in which the Common Component services including Ops Center Automator are registered, the syntax is:

```
hcmds64clustersrvstate /soff /r cluster-group-name
```

where `/r` specifies the name of the group in which the Common Component services including Ops Center Automator are registered. If the group name contains spaces, you must enclose the group name in quotation marks ("). For example, if the group name is Automator cluster, specify "Automator cluster".

hcmds64clustersrvupdate command

The **`hcmds64clustersrvupdate`** command registers the Common Component services including Ops Center Automator in the cluster management software group. This command also deletes the Common Component services including Ops Center Automator from the cluster management software group.

To register the Common Component services including Ops Center Automator the syntax is:

```
hcmds64clustersrvupdate /sreg /r cluster-group-name /sd
shared-disk-drive-letter /ap client-access-point-resource-name
```

To delete the Common Component services including Ops Center Automator the syntax is:

```
hcmds64clustersrvupdate /sdel /r cluster-group-name
```

where :

- `/r` specifies the name of the group in which the Common Component services including Ops Center Automator are registered. If the group name contains spaces, you must enclose the group name in quotation marks ("). For example, if the group name is Automation cluster, specify "Automation cluster".
- `/sd` specifies the drive letter of the shared disk that is registered to the cluster management software. You cannot specify multiple drive letters for this option. If the database of the products using Common Component is divided into multiple shared disks, run the **`hcmds64clustersrvupdate`** command for each shared disk.
- `/ap` specifies the name of the resource for the client access point that is registered to the cluster management software.

hcmds64dbinit command

The **`hcmds64dbinit`** command can recover to the status immediately after installation without reinstalling the product. It can be used only when the product itself is correctly installed and set up, and a DB failure occurs due to DB corruption or disk failure, and so forth, and the environment is in an unrecoverable status. This command is not supported in the Linux environment of Ops Center Automator.

The syntax is:

```
hcmds64dbinit /databasepath database-path
```

where `/databasepath` specifies the location to recreate the databases with the absolute path.

hcmds64dbrepair command

The **`hcmds64dbrepair`** command forces all the databases to be deleted, re-creates them, and then recovers them using the backup data obtained by the **`hcmds64dbtrans`** command. Use this command if any of the databases is corrupted and using the **`restoresystem`** command and the **`hcmds64dbtrans`** command with the **`/import`** option specified cannot restore the database.

The syntax is:

```
hcmds64dbrepair /trans backup-data
```

where `/trans` specifies the backup data obtained using the **hcmds64dbtrans** command. Make sure you specify the path in the `/workpath` or `/file` options of the **hcmds64dbtrans** command.

Remarks

- Stop Ops Center Automator services before running this command.
- Start Ops Center Automator services after running this command.
- This command uses the *Common-Component-installation-folder*`\tmp` folder to extract the backup data. Secure enough space to extract the backup data according to the size of the data.
- After running the command, the password of the built-in account (System account) is initialized. Change the password.
- In a cluster system, run this command on the execution host. This command cannot be run on the standby host.

hcmds64dbsrv command

The **hcmds64dbsrv** command starts and stops the databases of Ops Center Automator. Use this command when maintaining the databases.

The syntax is:

```
hcmds64dbsrv {/start | /stop}
```

where:

- `/start` starts the databases.
- `/stop` stops the databases.

Remarks

This command is restricted for database maintenance procedures.

hcmds64dbtrans command

The **hcmds64dbtrans** command backs up (exports) or restores (imports) the databases of Ops Center Automator. Use this command when reorganizing the databases of Ops Center Automator.

To back up (export) the Ops Center Automator databases, the syntax is:

```
hcmds64dbtrans /export /workpath working-folder-path /file archive-file-path [/auto]
```

To restore (import) the Ops Center Automator databases, the syntax is:

```
hcmds64dbtrans /import /type Automation /workpath working-folder-path
[/file archive-file-path] [/auto]
```

where:

- `/export` exports the databases.
- `/workpath` specifies the absolute path to a working folder that is temporarily used for exporting or importing. A folder on the local disk drive can only be specified. Use an empty folder for the working folder when you specify the /file option for exporting or importing.
- `/file` specifies the absolute path to the archive file to which the data is exported or from which the data is imported. This option is required if the /export option is specified.

  The archive file is not created if the output file size exceeds 2 GB, or if the amount of disk space for a location in which the archive file is created is insufficient.
- `/auto` causes the command to automatically start and stop the services and databases of Ops Center Automator and the products using Common Component. If this option is omitted, the services and databases of Ops Center Automator and the products using Common Component are not automatically started and stopped.
- `/import` causes the command to import the databases. All the exiting authentication data is deleted before the data is imported.
- `/type Automation` specifies `Automation` as the name of the product whose database is to be imported.

Remarks

- If the return code 3 is output by an export procedure, the database information remains in the folder specified for the /workpath option. To import this information, set the folder that you specified for the /workpath option at the time of the export procedure for the /workpath option for the import procedure. At this time, do not change the folder structure in the folder you specified for the /workpath option at the time of the export procedure. In addition, do not specify any value for the /file option when performing the import procedure.
- In the following cases, the folder specified for the /workpath option becomes empty, and the command is completed.
  - When the return code 1, 2, 233, 234, 235, 237, 238, 239, 240, or 255 is output by an export procedure
  - When the return code 3 is output by an import procedure

hcmds64fwcancel command

The **`hcmds64fwcancel`** command adds an exception so that Windows Firewall does not block communication between the Ops Center Automator server and a Web browser. Use this command when you change the port number on the Ops Center Automator server to which the Web browser connects from the default value.

The syntax is:

```
hcmds64fwcancel
```

hcmds64getlogs command

The **`hcmds64getlogs`** command acquires maintenance information on the management server.

The syntax is:

```
hcmds64getlogs /dir folder-name [/types Automation] [/arc archive-file-name] [/
logtypes log-file-type[ log-file-type ...]]
```

where:

- `/dir` specifies the absolute path to the folder on a local disk that contains collected maintenance information. If the folder has already been created, empty the folder.

  The maximum length of a path name that can be specified is 100 bytes. You can specify any printable ASCII character excluding certain special characters. You cannot specify the following characters:

  \ / : , ; * ? " < > | $ % & ' `

  However, you can specify backslashes (\), colons (:), and forward slashes (/) in Windows, or forward slashes (/) in Linux as a path delimiter. Do not specify a path delimiter at the end of a path name.

  In Windows, to specify a space character in a path name, enclose the path name in double quotation marks ("). In Linux, you cannot specify a space character in a path name.

- `/types Automation` specify `Automation` if the maintenance information for only Ops Center Automator can be collected. When specifying this option, also specify the log file type `log` for the /logtypes option. If this option is not specified, the Ops Center Automator server and all products using Common Component installed on the same management server is collected.

- `/arc` specifies the name of the archive files to be created. If you do not specify this option, the default file name is `HiCommand_log_64`.

  For the file name, you can specify any printable ASCII character excluding certain special characters. You cannot specify the following characters:

  \ / : , ; * ? " < > | $ % & ' `

  In Linux, you cannot specify a space character in a file name.

- `/logtypes` specifies the types of log files to acquire when log files of a particular type cannot be collected due to a failure.

  - `log`: Specify this to acquire `.jar` files and `.hdb.jar` files only.
  - `db`: Specify this to acquire `.db.jar` files only.
  - `csv`: Specify this to acquire `.csv.jar` files only.

  To specify multiple types, separate them by a space.

  If you omit this option, all log files will be acquired.

Tip: When this command is run, the KAPM05318-I or KAPM05319-E message is output. In addition, maintenance information (log file and database file) is acquired and four archive files (`.jar`, `.hdb.jar`, `.db.jar`, and `.csv.jar`) are output in the folder specified in the /dir option.

Remarks

- Do not interrupt this command while it is running.
- If the **`hcmds64getlogs`** command is interrupted, this command has ended before this command completed due to insufficient free space in the folder specified in the /dir option. In this case, make sure that the folder has enough free space, and then execute this command again.
- Do not run more than one **`hcmds64getlogs`** command at the same time.
- When Ops Center Automator is running in a cluster configuration, execute this command on both the active host and standby host. You can run this command even if the Ops Center Automator server is not running. Therefore, even if an error occurs in a cluster configuration, you can collect log information without switching nodes. However, if the database is not running, you cannot obtain the database information.
- If the same option is specified more than one time, only the first option is effective.

hcmds64intg command

The **`hcmds64intg`** command deletes authentication data stored in the repository on the server that manages user accounts. This command can also display the address of the server that stores authentication data. Use this command to delete authentication data if you failed to delete those data during the removal of Ops Center Automator.

The syntax is:

```
hcmds64intg {/delete /type Automation | /print | /primary} [/user user-ID]
```

Note: You are prompted to enter the password in interactive mode.

where:

- `/delete` deletes authentication data.
- `/type Automation` specifies `Automation` as the product name of the server that stores authentication data.
- `/print` displays the name of the program with which authentication data is registered.
- `/primary` displays the host name or IP address of the server that stores authentication data.
- `/user` specifies the user ID for connecting the server that stores authentication data. Specify the user ID of the account with User Management permission.

hcmds64keytool command

The **hcmds64keytool** command can do the following:

- Register the certificate in the Common Component truststore by using the JDK **keytool** utility.
- Verify the certificate registered in the keystore or truststore by using the JDK **keytool** utility.
- Change the Common Component truststore password by using the JDK **keytool** utility.
- Deletes the certificate from the Common Component truststore by using the JDK **keytool** utility.
- Exports the certificate from the Common Component truststore by using the JDK **keytool** utility.

To register the certificate in the Common Component truststore, the syntax is:

```
hcmds64keytool -import -alias alias-name -file file-name
 -keystore file-name -storetype JKS
```

To verify the certificate registered in the keystore/truststore, the syntax is:

```
hcmds64keytool -list -v -keystore file-name
```

To change the Common Component truststore password, the syntax is:

```
hcmds64keytool -keystore truststore-file-name -storepasswd
```

To delete the certificate registered in the Common Component truststore, the syntax is:

```
hcmds64keytool -delete -alias alias-name -keystore file-name
```

To export the certificate from the Common Component truststore, the syntax is:

```
hcmds64keytool -export -keystore file-name -alias alias-name -file file-name
```

Note:

You are prompted to enter the following password in interactive mode.

- For registering the certificate:
  - If the truststore does not exist: Password of your choice
  - If the trustsotre exists: Current truststore password
- For verifying, deleting or exporting the certificate: Current truststore password
- For changing the truststore password: Enter the current truststore password, then enter a new password

where:

- `-alias` specifies the name (Alias name) for identifying the certificate in the truststore. Alias name that already exists cannot be specified, so either change it to another name or delete it in advance.
- `-keystore` specifies the truststore file to be registered, verified, deleted, or exported.

  The truststore (`ldapcacerts` or `jssecacerts`) file paths are as follows.

  `jssecacerts`

  - For Windows:

    Common-Component-installation-folder\uCPSB11\hjdk\jdk\lib\security\jssecacerts

  - For Linux:

    Common-Component-installation-directory/uCPSB11/hjdk/jdk/lib/security/jssecacerts

  `ldapcacerts`

  - For Windows:

    Common-Component-installation-folder\conf\sec\ldapcacerts

  - For Linux:

    Common-Component-installation-directory/conf/sec/ldapcacerts

- `-file` specifies the input certificate (PEM or DER format). In the case of export, specify the output path of the certificate.
- `-storetype JKS` specifies JKS as the store type of the truststore.

hcmds64ldapuser command

The **hcmds64ldapuser** command registers the user information required for Active Directory registration information search when Ops Center Automator links with Active Directory. This command can also be used to delete registered user information.

After you use this command to register the user information, run the **hcmds64checkauth** command to verify that the information can be properly authenticated.

The syntax is:

```
hcmds64ldapuser {/set /dn user-identifier | /delete} /name {server-identifier |
domain-name} | /list
```

Note: You are prompted to enter the password in interactive mode.

where:

- `/set` registers the user information.
- `/dn` specifies the user identifier of the user to be registered. Follow RFC 4514 for the possible characters. The characters &, |, ^, (,), <, and > must be enclosed by double quotation marks (") or escaped with a caret (^). To specify a value that ends with \, escape it with \.
- `/delete` deletes the registered user information. The information of the user which includes the server identifier or domain name specified by the /name option is deleted.
- `/name` specifies the server identifier or domain name to which the user is registered. When deleting the user information, specify the server identifier or domain name of the server in which the user to be deleted is registered. However, you cannot specify the domain name if group linkage with Active Directory is disabled and a user for LDAP search is registered. In that case, specify the server identifier.
- `/list` displays the list of server identifiers and domain names contained in the registered user information.

hcmds64prmset command

The **`hcmds64prmset`** command registers, changes, and cancels the registration of the host that manages the user accounts used to connect with Ops Center Automator. If you run this command, the information about the user accounts in the Common Component will be managed by the Common Component of the primary server. The host whose user accounts are managed by the primary server is called the secondary server. Run this command on the server that is set as the secondary server.

When registering the primary server or changing information about the registered primary server, the syntax is:

```
hcmds64prmset [/host host-name-or-IP-address] [/port port-number-(non-SSL-
communication) | /sslport port-number-(SSL-communication)] [/check]
```

When canceling the primary server, the syntax is:

```
hcmds64prmset /setprimary
```

When displaying the registration information, the syntax is:

```
hcmds64prmset /print
```

where:

- /host specifies the host name or IP address of the primary server. If SSL communication is enabled on the primary server, specify the same value as that of Common Name (CN) in the server certificate. If you change the host name of only the registered primary server, you can omit the /port or /sslport option.
- /port specifies the port number of HBase 64 Storage Mgmt Web Service of the primary server. Specify this option if SSL communication is disabled on the primary server. The default port number is 22015. If you change the port number of only the registered primary server, you can omit the /host option.
- /sslport specifies the port number of HBase 64 Storage Mgmt Web Service of the primary server. Specify this option if SSL communication is enabled on the primary server. The default port number is 22016. If you change the port number of only the registered primary server, you can omit the /host option.
- /check checks the connection to the primary server.
- /setprimary cancels the registered primary server. The host on which the command was run changes from the secondary server to the primary server.
- /print displays the following:
  - The role of the host on which the command was run (primary or secondary)
  - The host name (IP address) and port number of the primary server, if the role of the host is the secondary server.

Remarks

When Ops Center Automator is running in a cluster configuration, run this command on both the active host and standby host.

hcmds64radiussecret command

The **hcmds64radiussecret** command registers a shared secret for the RADIUS server in the Ops Center Automator server when connecting with an external authentication server.

If you register a shared secret by using this command, run the **hcmds64checkauth** command to verify whether the shared secret can be correctly authenticated.

To register a shared secret, the syntax is:

```
hcmds64radiussecret [/set shared-Secret] /name RADIUS-server-indication-name
```

To delete a shared secret, the syntax is:

```
hcmds64radiussecret /delete /name RADIUS-server-indication-name
```

To display a list of server indication names of the RADIUS servers for which shared secrets are registered, the syntax is:

```
hcmds64radiussecret /list
```

where:

- `/set` registers a shared secret for the RADIUS server in the Ops Center Automator server. For a `shared-Secret`, you can specify printable ASCII characters (0x21 to 0x7E) of 128 bytes or less. If you execute the command without specifying the /set option, you will be promoted to enter a shared secret.
- `/delete` deletes a shared secret registered in the Ops Center Automator server.
- `/name` specifies a RADIUS server indication name. The specified name must match a server indication name specified for the `auth.server.name` property in the `exauth.properties` file.
- `/list` displays a list of server indication names of the RADIUS servers for which shared secrets are registered.

hcmds64srv command

The **`hcmds64srv`** command starts and stops the services and databases of Ops Center Automator. This command can also display the status of the Ops Center Automator services or change how to start the services. Note that if you run this command by specifying `AutomationWebService` for the `/server` option, you can start, stop, or display the status of the following services:

- HAutomation Engine Web Service
- HBase 64 Storage Mgmt SSO Service[1]
- HBase 64 Storage Mgmt Web Service[1]
- HBase 64 Storage Mgmt Web SSO Service[1]
- Database process[1, 2]
    1. The service does not stop while a service from the products using Common Component is running.
    2. These are the internal processes of Ops Center Automator. The **`hcmds64srv`** command does not start and stop `HiRDB/EmbeddedEdition _HD1` that represents the database service.

The syntax is:

To start, stop, or display only the status of a specific service:

```
hcmds64srv {/start /stop /check | /status} [/server service-name]
```

To see the status of services of Ops Center Automator and the products using Common Component:

```
hcmds64srv /statusall
```

To change how to start a service or services:

```
hcmds64srv /starttype {auto | manual} {/server service-name | /all}
```

where:

- `/start` starts the service and database specified in the /server option.
- `/stop` stops the service and database specified in the /server option.
- `/check` displays the status of the service and database specified in the /server option.
- `/status` displays the status of the service and database specified in the /server option.
- `/server` stops and starts the service and displays status.

  To start and stop only the service, or display its status, of Ops Center Automator, specify `AutomationWebService` for `service-name`. If this option is omitted, the command has an effect on the services of Ops Center Automator and all products using Common Component.
- `/statusall` displays the status of the services and databases, and of the services of the products using Common Component.
- `/starttype` specifies the start type of the service specified in the /server option. To start the service automatically, use `auto`. To start the service manually, use `manual`.
- `/all` If this option is specified, the command has an effect on the services of Ops Center Automator and all products using Common Component.

Remarks

- When you start and stop the services for Ops Center Automator in day-to-day functions, start and stop all the services without specifying the /server option. To start only the services from Ops Center Automator with /server option, use `HBase` for the /server option to start the services of Common Component because these services must be started beforehand.
- Running the command with the /stop option while a task is being processed ends any processing running on the connection destination. For this reason, if any task is In Progress, Waiting for Input, In Progress (with Error), or In Progress (Terminating), you must wait the status transition of the task to one of the ended status (Completed, Failed, or Canceled) or stop all the tasks, and then use the command with the /stop option.
- If the service does not stop within three minutes after the command with the /stop option, the command ends abnormally with a message indicating a timeout. In this case, wait a little while and then run the command with the /stop option again.

hcmds64ssltool command

The **`hcmds64ssltool`** command creates a private key, CSR, self-signed certificate, and the self-signed certificate content file that are required for an SSL connection.

The created files are used for the following purposes:

- The CSR is submitted to CA to obtain the SSL server certificate. You can build an SSL connection environment by combining the obtained SSL server certificate with the private key.
- You can build an SSL connection environment by combining the self-signed certificate and the private key. However, you should use this environment for test purposes because the security level is low.
- You can verify the information registered in the self-signed certificate by viewing the self-signed certificate content file.

The syntax is:

```
hcmds64ssltool [/key private-key-file] [/csr certificate-signed-request-file] [/cert
self-signed-certificate-file] [/certtext self-signed-certificate-content-file] [/
validity expiration-date] [/dname distinguished-name(DN)] [/sigalg RSA-server-
certificate-signature-algorithm] [/eccsigalg ECC-server-certificate-signature-
algorithm] [/ecckeysize ECC-private-key-size] [/ext extension-information-for-the-
X.509-certificate]
```

where:

- `/key` specifies the absolute path of the private key file that is created. If you omit this option, the files are output to the default output destination path with the file name `httpsdkey.pem` (for RSA) and `ecc-httpsdkey.pem` (for ECC). The default output destination when you omit this option is as follows:

  ```
  Common-Component-installation-folder\uCPSB11\httpsd\conf\ssl\server
  ```

- `/csr` specifies the absolute path of the certificate signing request file that is created. If you omit this option, the files are output to the default output destination path with the file name `httpsd.csr` (for RSA) and `ecc-httpsd.csr` (for ECC). The default output destination when you omit this option is as follows:

  ```
  Common-Component-installation-folder\uCPSB11\httpsd\conf\ssl\server
  ```

- `/cert` specifies the absolute path of the self-signed certificate file that is created. If you omit this option, the files are output to the default output destination path with the file name `httpsd.pem` (for RSA) and `ecc-httpsd.pem` (for ECC). The default output destination when you omit this option is as follows:

  ```
  Common-Component-installation-folder\uCPSB11\httpsd\conf\ssl\server
  ```

- `/certtext` specifies the absolute path of the self-signed certificate content file that is created. If you omit this option, the files are output to the default output destination path with the file name `httpsd.txt` (for RSA) and `ecc-httpsd.txt` (for ECC). The default output destination when you omit this option is as follows:

  ```
  Common-Component-installation-folder\uCPSB11\httpsd\conf\ssl\server
  ```

- `/validity` specifies the expiry date of the self-signed certificate in the number of days. If this option is omitted, the expiry date becomes 3,650 days. A specifiable value is a number of days until December 31, 9999.
- `/sigalg` specifies the signature algorithm of the RSA certificate as SHA256withRSA, or SHA1withRSA. If you omit this option, the default of SHA256withRSA is used.
- `/eccsigalg` specifies the signature algorithm of the ECC certificate as SHA512withECDSA, SHA384withECDSA, SHA256withECDSA, or SHA1withECDSA. If you omit this option, the default of SHA384withECDSA is used.
- `/ecckeysize` specifies the key size of the private key for the ECC server certificates in bits as 256 or 384. If you omit this option, the default of 384 is used.

- `/ext` specifies the extension information for the X.509 certificate. To set the SAN (Subject Alternative Name) on the self-signed certificate and certificate signing request, specify this option. The specification method is based on the `/ext` option of the keytool command in Java. Note, however, that the only extension that can be specified in Ops Center Automator is SAN. If you specify the `/ext` option multiple times, the first specification takes effect.

  The following is an example of specifying the extension information.

  - To specify www.example.com as the host name:

    ```
    hccmds64ssltool /ext san=dns:www.example.com
    ```

  - To specify www.example.com and www.example.net as multiple host names:

    ```
    hccmds64ssltool /ext san=dns:www.example.com, dns:www.example.net
    ```

- `/dname` specifies the identification name (DN) written in the SSL server certificate in the `attribute-type=attribute-value` format. You can specify a value with multiple attribute types by separating with a comma (,). The `attribute-type` is case insensitive. The `attribute-value` cannot include a double quotation mark (") or backslash (\).

  Follow RFC 2253 for character escapes.

  Escape the following characters with a backslash (\).

  - + , ; < =>
  - A space at the beginning of the character string
  - A space at the end of the character string
  - A hash mark (#) at the beginning of the character string

  If you omit this option, you will input the attribute values by response input according to the prompt displayed when you run the command.

  The following table describes attribute types that can be specified in this option.

Table 33 List of attribute types that can be specified in the identification name (DN)

Attribute type	Description	Prompt displayed	Value
CN	Common Name	Server Name	Identification name of the Ops Center Automator server such as a host name, IP address, and domain name#
OU	Organizational Unit Name	Organizational Unit	Organization name of a small unit such as a department or division name
O	Organization Name	Organization Name	Organization name of the company or organization#
L	Locality Name	City or Locality	Name of the city or locality.
ST	State or Province Name	State or Province	Name of the state or province
C	Country Name	Two-character country code	Country code
#: Required when you use a response input.			

The following shows an example of a response input:

```
Enter  Server  Name  [default=MyHostname]:example.com
Enter Organizational Unit:Automation Administration
Enter Organization Name [default=MyHostname]:HITACHI
Enter your City or Locality:Sanfrancisco
Enter your State or Province:California
Enter your two-character country-code:US
Is CN=example.com,OU=Automation Administration,O=HITACHI,L=Sanfrancisco,
ST=California,C=US correct? (y/n) [default=n]:y
```

if you made a mistake when inputting a value, enter `n` at the confirmation to do the response input again.

Remarks

If the attribute type CN of the SSL server certificate does not match the host name, IP address or domain name specified as the connection target from the Web browser to the Ops Center Automator server, a server name mismatch warning or error occurs.

hcmds64unlockaccount command

The **`hcmds64unlockaccount`** command unlocks a user account. Use this command when all the user accounts are locked and the users cannot log in to Ops Center Automator.

The syntax is:

```
hcmds64unlockaccount [/user user-ID]
```

Note: You are prompted to enter the password in interactive mode.

where:

- `/user` specifies the user ID of the user account that you want to unlock. You must specify the user ID with User Management permission.

Remarks

- Only a user account with User Management permission can unlock user accounts by using the **`hcmds64unlockaccount`** command.
- If the user name specified in the options includes characters, &, |, or ^, enclose the character with double quotation marks (") or escape the character with a caret (^). For example, in Windows, if the user ID is ^a^b^c^, the command can be written as:

  ```
  hcmds64unlockaccount /user "^"a"^"b"^"c"^"
  ```

  or

  ```
  hcmds64unlockaccount /user ^^a^^b^^c^^
  ```

Ops Center Automator CLI commands

Ops Center Automator gives a set of CLI commands.

Note: When the Ops Center Automator server is using the Linux OS, read "/" to "-" is used for each argument.

When running Ops Center Automator in a Windows-based OS, navigate to `<system-drive>\Program Files\hitachi\Automation\bin`, (when running Linux OS, navigate to `/opt/hitachi/Automation/bin`) then open the command prompt to run the following Ops Center Automator CLI commands.

backupsystem command

The **`backupsystem`** command backs up the system configuration and database information in the specified folder.

Syntax

```
backupsystem {/dir directoryname [/auto] | /help}
```

Options

Option	Description
`/dir`	The absolute or relative folder path that contains the backup data.
`/auto`	Directs the Ops Center Automator, Common Component services, and database to start and stop automatically.

Note: Before running the **`backupsystem`** command in a cluster environment, you must run the following command to take the group where the Automator service is registered offline and disable failover.

```
Common-component-Installation-folder\ClusterSetup
\hcmds64clustersrvstate /soff /r group-name
```

changemode command

The **`changemode`** command allows you to change the performance mode for Ops Center Automator. There are two performance modes, standard and high performance.

Standard mode

This is the default mode which supports running a single Online Migration with Configuration Manager task.

High performance mode

Use high performance mode if you need to run multiple Online Migration with Configuration Manager tasks concurrently. If you select this mode, you will must change the `logger.TA.MaxFileSize` and `plugin.threadPoolSize` parameters in config_user.properties. For more information, see Changing the system configuration (on page 94).

Syntax

```
changemode {/mode {standard| highPerformance} [/auto] |  /print |  /help}
```

Options

Option	Description
/mode	Specify a performance mode, either standard (standard mode) or highPerformance* (high performance mode).
/auto	Optionally stop and start services that use Common Component and HiRDB automatically. To specify this option in a cluster environment, the services registered in the cluster software must be offline.
/print	Output the current mode.
/help	Display command help.
*: If you change the mode to highPerformance, you must change the logger.TA.MaxFileSize and plugin.threadPoolSize parameters in config_user.properties. For more information, see Changing the system configuration (on page 94).	

Permissions

Ops Center Automator users must have Administrator permissions in Window or root permissions in Linux.

Return codes

The following table lists the **changemode** command return codes and descriptions.

Return code	Description
0	The command succeeded.
1	The argument is not valid.
2	The command stopped.
3	The service status is not valid.
4	An exclusion error has occurred.

Return code	Description
101	Cannot change the mode because it failed due to a cause other than those listed above.
90	Cannot start or stop the service.
255	The command stopped because of an error not in this table.

Usage example: To change to high performance mode

```
changemode /mode highPerformance
```

Usage example: To change to standard mode and specify the auto option

```
changemode /mode standard /auto
```

Usage example: To output the current mode

```
changemode /print
```

Output example: Changing to high performance mode

```

# changemode /mode highPerformance

KNAE03000-I The changemode command will now start.
KNAE03542-I
Changed to high performance mode. Set the following values in config_user.properties:
logger.TA.MaxFileSize=100240
plugin.threadPoolSize=100
After updating config_user.properties, restart the service.
KNAE03001-I The changemode command ended normally.
```

Remarks

- When Ops Center Automator is running in a cluster configuration, run this command on both the active host and standby host.
- Before running the **`changemode`** command in a cluster environment, you must run the following command to take the group where the Ops Center Automator service is registered offline and disable failover.

  ```
  Common-component-Installation-folder\ClusterSetup\hcmds64clustersrvstate /soff /r
  group-name
  ```

deleteremoteconnection command

The **`deleteremoteconnection`** command deletes the agentless connection-destination definitions registered through Ops Center Automator based on the definition ID derived with the **`listremoteconnections`** command.

Functions

The **`deleteremoteconnection`** command performs the following function:

- Deletes a succession of agentless connection-destination definitions based on their definition IDs. To determine the definition ID of the agentless connection-destination definition, use the **`listremoteconnections`** command.

Syntax:

```
deleteremoteconnection {/id Definition ID
[/user UserName | /user UserName /passwordfile PasswordFile]
[/authmode local | external]
| /help}
```

Note: You are prompted to enter the password in interactive mode if you do not specify the `passwordfile` option.

Permission

- Ops Center Automator users must have Admin permissions.
- Only users who have OS administrator permissions (members of the Administrators group) are allowed to run the **`deleteremoteconnection`** command.
- If a user who does not have the necessary permissions runs the command, the following message is visible requesting promotion of the user's permissions:

Message: KNAE03226-W The user does not have permission to execute the command.

Options

Option	Description
`/id`	Specifies the single-byte numerical definition ID (between 1 - 64 characters) of the agentless connection-destination definition information to be deleted. If the specified ID does not exist, an error is generated.
`/user`	Specifies the name of the user (must have Admin permission) executing the command. The user name can consist of any single-byte alphanumeric characters including (! # $ % & ' ( ) * + - . = @ \ ^ _ |) from 1 - 256 characters in length. The user name is case sensitive.

Option	Description
`/passwordfile`	Specifies a password file (with absolute or relative path) that includes the encrypted user credentials for the selected user.
`/authmode local | external`	Specify the authentication type, either `local` or `external`. Specify `local` to authenticate locally with Automator. Specify `external` to authenticate with Common Services. If this option is not specified, Ops Center Automator operates in the authentication mode specified by the `command.auth.mode` of `command_user.properties`.

Storage destination

`installation-folder``\bin`

Return codes

The following table lists the **`deleteremoteconnection`** command return codes and descriptions.

Return code	Description
0	The command succeeded.
1	The argument is not valid.
2	The command stopped.
3	The service status is not valid.
4	An exclusion error has occurred.
5	Communication failed.
6	Authentication failed.
14	The user does not have permission to run the command.
17	The interactive input value is not valid.
240	Failed to delete an agentless connection-destination definition
255	The command stopped due to an error other than the ones listed in this table.

Usage example: - To delete the agentless connection-destination definition of the ID specified for the parameter

```
deleteremoteconnection /id 12345 /user xxxxx
```

Example: Output of normal deletion

```
KNAE03000-I The deleteremoteconnection command will now start.
KNAE03001-I The deleteremoteconnection command ended normally.
```

Example: Output of abnormal deletion

```
KNAE03000-I The deleteremoteconnection command will now start.
KNAE03002-E The deleteremoteconnection command ended abnormally (12345).
```

deleteservicetemplate command

The **deleteservicetemplate** command deletes a service template.

Syntax

```
deleteservicetemplate {/name service-template-key-name /vendor vendor-ID /version
XX.YY.ZZ [/user username | /user username /passwordfile passwordfile] [/authmode
local | external] | /help}
```

Note: You are prompted to enter the password in interactive mode if you do not specify the passwordfile option.

Options

Option	Description
/name	The key name of the service template.
/vendor	The vendor ID of the service template.
/version	The version of the service template.
/user	The user ID.
/passwordfile	The password file (with absolute or relative path) that includes the encrypted user credentials.
/authmode	Specifies the authentication type, either local or external. Specify local to authenticate locally with Automator. Specify external to authenticate with Common Services. If this option is not specified, Ops Center Automator operates in the authentication mode specified by the command.auth.mode of command_user.properties.

encryptpassword command

The **`encryptpassword`** command creates a file that includes an encrypted user name and password. You can specify the password file instead of the password for any Ops Center Automator command that allows the `/passwordfile` option.

Syntax

```
encryptpassword {[/user username] /passwordfile passwordfile [/authmode local |
external] | /help }
```

Note: You are prompted to enter the password in interactive mode.

Options

Option	Description
`/user`	The ID of the user who is added to the password file.
`/passwordfile`	The name of the password file (with absolute or relative path) that includes the encrypted user credentials.
`/authmode`	Specifies the authentication type, either `local` or `external`. Specify `local` to authenticate locally with Automator. Specify `external` to authenticate with Common Services. If this option is not specified, Ops Center Automator operates in the authentication mode specified by the `command.auth.mode` of `command_user.properties`.

importservicetemplate command

The **`importservicetemplate`** command imports a service template.

Syntax

```
importservicetemplate {/file service-template [/user username | /user username /
passwordfile passwordfile] [/authmode local | external] | /help}
```

Note: You are prompted to enter the password in interactive mode if you do not specify the `passwordfile` option.

Options

Option	Description
`/file`	The service template file to import.
`/user`	The user ID.
`/passwordfile`	The password file (with absolute or relative path) that includes the encrypted user credentials.
`/authmode`	Specifies the authentication type, either `local` or `external`. Specify `local` to authenticate locally with Automator. Specify `external` to authenticate with Common Services. If this option is not specified, Ops Center Automator operates in the authentication mode specified by the `command.auth.mode` of `command_user.properties`.

listremoteconnections command

The **`listremoteconnections`** command outputs a listing of the agentless connection-destination definitions registered through Ops Center Automator to a CSV formatted file.

Functions

The **`listremoteconnections`** command performs the following functions:

- output a list of agentless connection-destination definitions that include names of connection destinations and credential information.
- The CSV file that you have output can be used as an input file for the **`setremoteconnection`** command as-is.

Syntax:

```
listremoteconnections {/file OutputFile
[/user UserName | /user UserName /passwordfile PasswordFile]
[/authmode local | external] | /help}
```

Note: You are prompted to enter the password in interactive mode if you do not specify the `passwordfile` option.

Permission

- Ops Center Automator users must have Admin permissions.
- Only users who have OS administrator permissions (members of the Administrators group) are allowed to run the **`listremoteconnections`** command.
- If a user who does not have the necessary permissions runs the command, the following message appears, asking for the promotion of the user's permissions:

Message: KNAE03226-E The user does not have permission to execute the command.

Options

Option	Description
`/file`	Specifies the path of the file to which the list is output; if the specified file already exists, an error is generated. .
`/user`	Specifies the name of the user executing the command. The user name can consist of any single-byte alphanumeric characters including (! # $ % & ' ( ) * + - . = @ \ ^ _ |) from 1 - 256 characters. The user name is case-sensitive.
`/passwordfile`	Specifies a password file (with absolute or relative path) that includes the encrypted user credentials for the selected user.
`/authmode local | external`	Specify the authentication type, either `local` or `external`. Specify `local` to authenticate locally with Automator. Specify `external` to authenticate with Common Services. If this option is not specified, Ops Center Automator operates in the authentication mode specified by the `command.auth.mode` of `command_user.properties`.

Storage Destination

`installation-folder``\bin`

Return codes

The following table lists the **`listremoteconnections`** command return codes and descriptions.

Return code	Description
0	The command succeeded.
1	The argument is not valid.
2	The command stopped.

Return code	Description
3	The service status is not valid.
4	An exclusion error has occurred.
5	Communication failed.
6	Authentication failed.
7	A path is specified is not valid.
8	A file with the specified name already exists.
9	Path not found.
10	Path cannot be accessed.
13	Failed to output the specified file.
14	User does not have permission to run the command.
17	The interactive input value is not valid.
220	Failed to acquire a list of agentless connection-destination definitions.
255	The command stopped because of an error not in this table.

Data Format

Agentless connection destinations are output in CSV format with one host in one line and with the following data items in the order in which they are shown in the following table.

Property	Header Section (first line)	Data Section (second and subsequent lines)
Definition ID	Id	Agentless connection-destination definition ID
Connection destination type	Method	Connection destination can be specified as follows: ▪ IPv4: The connection destination is an IP address in the IPv4 format. ▪ IPv6: The connection destination is an IP address in the IPv6 format. ▪ HostName: The connection destination is a host name.

Property	Header Section (first line)	Data Section (second and subsequent lines)
Connection destination	IP Address/Host Name	IP address or host name of the connection-destination host.
Service resource group	Service Group	Service group name allocated to the agentless connection-destination definition.
Authentication information	Authentication	Can be either of the following: ▪ Enable: Authentication information is set ▪ Disable: Authentication information is not set
Protocol	Protocol	Can be any of the following: ▪ Windows: Connect using Windows-based OS ▪ SSH: Connect using SSH ▪ Telnet: Connect using Telnet
SSH authentication method	SSH authentication method	When the protocol is not SSH, null character ("") When the protocol is SSH, any one of the following: ▪ Password Authentication ▪ Public Key Authentication ▪ Keyboard Interactive Authentication
User ID	User ID	User ID of the user who logs on to the connection-destination host.
Password	Password	Fixed to "*******"
Super user's password	Super user's password	Fixed to "*******"
Status	Connection Status	Connection Successful, Error, Unknown, or -.
Last connection time	Connected Time	The last connection time.

Usage example: To output a list of registered agentless connection-destination definitions to a file

```
listremoteconnections /file bbbbb /user xxxxx
```

Example: Output message for successful list

```
KNAE03000-I The listremoteconnections command will now start.
KNAE03001-I The listremoteconnections command ended normally.
```

Example: Output message for unsuccessful list

```
KNAE03000-I The listremoteconnections command will now start.
KNAE03002-E The listremoteconnections command ended abnormally (12345).
```

Example: Typical output file

```
"Id","Method","IP Address/Host Name","Service Group","Authentication ","Protocol",
"SSH Authentication Method","User ID","Password","Super User's Password"
"1","IPv4","10.197.158.107","All Service Groups","Enable","Windows","",
"Administrator@DOM1","********",""
"10","HostName","vmc006","All Service Groups","Enable","SSH","Password
Authentication","ao","********","********"
"100","IPv6","fd00::6172:839:2e15:f6f3:da7e"," All Service Groups ","Enable","Telnet",
"","","",""
"1000","HostName","vmc007"," All Service Groups ","Disable","","","","",""
```

listservices command

The `listservices` command exports a list of services or a list of service templates to a CSV file.

Syntax

```
listservices {/output {services | servicetemplates} /file output-file [/encoding
encoding] [/user username | /user username /passwordfile passwordfile] [/authmode
local | external] | /help}
```

Note: You are prompted to enter the password in interactive mode if you do not specify the `passwordfile` option.

Options

Option	Description
`/output`	Either `services` (export services) or `servicetemplates` (export service templates).
`/file`	The output file path.
`/encoding`	The encoding of the output file, either `UTF-8` or `Shift_JIS`.

Option	Description
`/user`	The user ID. The Submit role is required to output services list. The Modify role is required to output service templates list.
`/passwordfile`	Specifies a password file (with an absolute or relative path) that includes the encrypted user credentials for the specified user.
`/authmode`	Specifies the authentication type, either `local` or `external`. Specify `local` to authenticate locally with Automator. Specify `external` to authenticate with Common Services. If this option is not specified, Ops Center Automator operates in the authentication mode specified by the `command.auth.mode` of `command_user.properties`.

listtasks command

The **`listtasks`** command exports a list of services or a list of tasks to a CSV file.

Syntax

```
listtasks {[/startrange {yyyy-mm-dd | ,yyyy-mm-dd | yyyy-mm-dd, yyyy-mm-dd}] /output
{tasks | histories | taskdetails} {/file outputfile | /taskdetaildir directoryname} [/
encoding encoding] [/user username | /user username /passwordfile passwordfile] [/
authmode local | external] | /help}
```

Note: You are prompted to enter the password in interactive mode if you do not specify the `passwordfile` option.

Options

Option	Description
`/startrange`	The date range of the task start date. Use this to limit the contents of the list to tasks run within a specific period of time. This option cannot be specified if `taskdetails` is specified for the `output` option.
`/output`	Either of the following output data types: `tasks` (export tasks), `histories` (export histories), `taskdetails` (export task with properties)
`/file`	The output file with an absolute or relative path.

Option	Description
/taskdetaildir	The output file with an absolute or relative path. /taskdetaildir is required instead of /file when /output taskdetails is specified.
/encoding	The encoding of the output file, either UTF-8 or Shift_JIS.
/user	The user ID. The Admin role is required to output taskdetails.
/passwordfile	The absolute or relative path of the password file.
/authmode	Specifies the authentication type, either local or external. Specify local to authenticate locally with Automator. Specify external to authenticate with Common Services. If this option is not specified, Ops Center Automator operates in the authentication mode specified by the command.auth.mode of command_user.properties.

restoresystem command

The **restoresystem** command restores the system configuration and database information from the specified folder where the data was backed up.

Syntax

```
restoresystem {/dir directoryname [/auto] | /help}
```

Options

Option	Description
/dir	The absolute or relative folder path that contains data that is backed up by the **backupsystem** command.
/auto	Directs the Ops Center Automator, Common Component services and database to start and stop automatically.

Note: Before running the **restoresystem** command in a cluster environment, you must run the following command to take the group where the Automator service is registered offline and disable failover.

```
Common-component-Installation-folder\ClusterSetup
\hcmds64clustersrvstate /soff /r group-name
```

setremoteconnection command

The **setremoteconnection** command adds or updates agentless connection-destination definitions in Ops Center Automator through a CSV file.

Function

The **setremoteconnection** command adds or updates agentless connection-destination definitions in Ops Center Automator. To add or update agentless connection-destination definitions, you define the information in a CSV file and then specify the file name as a command argument.

Note: The CSV file must have the same format as the output file of the **listremoteconnections** command.

Syntax:

```
setremoteconnection {/file Input File
[/user UserName | /user UserName /passwordfile PasswordFile]
 [/authmode local | external]| /help}
```

Note: You are prompted to enter the password in interactive mode if you do not specify the `passwordfile` option.

Permission

- Ops Center Automator users must have Administrator permissions (members of the OS Administrators group) to run the **setremoteconnection** command.
- If a user without the necessary permissions runs the command, the system generates the following message:

Message: KNAE03226-W The user does not have permission to execute the command.

Options

Option	Description
`/file`	Specifies the path of the file that contains the agentless connection-destination definitions to add or update. If the specified file does not exist, the system generates an error. Both absolute and relative paths are allowed.
`/user`	Specifies the name of the user running the command. The user name must be between 1 and 256 characters in length and consist of single-byte alphanumeric characters including (! # $ % & ' ( ) * + - . = @ \ ^ _ |). The user name is case sensitive.
`/passwordfile`	Specifies a password file (with an absolute or relative path) that includes the encrypted user credentials for the specified user.

Option	Description
`/authmode local | external`	Specify the authentication type, either `local` or `external`. Specify `local` to authenticate locally with Automator. Specify `external` to authenticate with Common Services. If this option is not specified, Ops Center Automator operates in the authentication mode specified by the `command.auth.mode` of `command_user.properties`.

Storage destination

`installation-folder``\bin`

Return codes

The following table lists the **`setremoteconnection`** command return codes and descriptions:

Return code	Description
0	The command succeeded.
1	The argument is not valid.
2	The command stopped.
3	The service status is not valid.
4	An exclusion error occurred.
5	Communication failed.
6	Authentication failed.
7	A path is specified that is not valid.
9	Path not found.
10	Path cannot be accessed.
14	User does not have permission to run the command.
17	The interactive input value is not valid.
230	Format of the agentless connection-destination definition is not valid.
231	Registration of some of the agentless connection-destination definitions failed.
232	Registration of all of the agentless connection-destination definitions failed.

Return code	Description
255	The command stopped because of an error not in this table.

File format

The agentless connection-destination definition file that you specify for the `/file` option uses the same basic format that is used in the output generated by the **`listremoteconnections`** command.

The agentless connection-destination definition file differs depending on the environment as follows:

- In a Windows-based OS environment: Uses character encoding MS932 and line feed code CR+LF.
- In a Linux OS environment: Uses the character encoding that is specified for the user's LANG environment variable and uses the line feed code LF.

Data item	Description
Definition ID (Id)	Specifies the ID of the agentless connection-destination definition to update. If a null character is specified, the agentless connection-destination definitions are registered as an addition. If the agentless connection-destination definition of the specified ID does not exist, the system generates an error.
Connection destination type (Method)	Specifies any of the following connection destination types: ▪ IPv4: The connection destination is an IP address in IPv4 format. ▪ IPv6: The connection destination is an IP address in IPv6 format. ▪ HostName: The connection destination is a host name.
Connection destination (IP Address/Host Name)	Specifies the IP address or host name of the connection-destination host.
Service resource group (Service Group)	Specifies the service group to allocate to the agentless connection-destination definition. **Note:** This parameter is ignored from v8.5.1 onward because agentless connection settings are allocated to infrastructure groups.

Data item	Description
Authentication information (Authentication)	Specifies whether to set authentication information: ▪ Enable: Authentication information is set. ▪ Disable: Authentication information is not set. When the system displays the message "Authentication information is not set," any additional data is ignored. However, the data item is still required.
Protocol (Protocol)	Specifies one of the following protocols: ▪ Windows: Connect using a Windows-based OS. ▪ SSH: Connect using SSH. ▪ Telnet: Connect using Telnet.
SSH authentication method (SSH Authentication Method)	Specifies the SSH authentication method: ▪ When the protocol is not SSH, specify a null character (""). ▪ When the protocol is SSH, one of the following: • Password Authentication (PW) • Public Key Authentication (PK) • Keyboard Interactive Authentication (KI)
User ID (User ID)	Specifies the User ID used to log on to the connection-destination host when the protocol is Windows or SSH. This parameter is required.
Password (Password)	Specifies the password of the user ID used to log on to the connection-destination host. This parameter is required in some cases and not in others as follows: Case 1: When no definition ID is specified (when adding a definition). ▪ In a Windows-based OS, the parameter is required. ▪ When the protocol is SSH the SSH authentication method is not "public key authentication", this parameter is required. Note: You cannot specify "********" as a password. The system generates an error if you specify this password.

Data item	Description
	Case 2: A definition ID is specified (when updating a definition). ▪ In a Windows-based OS, the parameter is required. ▪ When the protocol is SSH the SSH authentication method is not "public key authentication", this parameter is required. Note: If you specify "********" for the password, the password is not changed. If you specify a null character (“”) for the password, the password is deleted.
Super user's password (Super User's Password)	Specifies the password of a super user of the connection-destination host. When the protocol is SSH or Telnet, this parameter is optional. ▪ If you specify a string that is not "********" for the password, the specified string is set as the password. ▪ If you specify "********" for the password, the password is not changed. ▪ If you specify a null character (“”) for the password, the password is deleted.
Status (Connection Status)	Specifies either Connection Successful, Error, Unknown, or "-" depending on the status.
Last connection time (Connected Time)	Specifies the last connection time.

Behavior of the setremoteconnections command

The following lists includes details about the behavior of the **`setremoteconnections`** command when specifying an agentless connection-destination definition file for the `/file` option:

- The first line of the file is the header section output by the **`setremoteconnections`** command and is ignored unconditionally. The second and subsequent lines are treated as agentless connection-destination definitions.
- When you specify two or more agentless connection-destination definitions in the file, a single syntax error in either definition causes the command to end with an error, and no agentless connection-destination definitions are registered.
- The values of the data items output by the **`listremoteconnections`** command in CSV format are enclosed in double quotation marks ("). However, if the values are not enclosed by double quotation marks, they are not treated as errors. (This is because when you edit a CSV file in Excel, double quotation marks are removed).

- If the value of the first data item (ID) of an agentless connection-destination definition is a null character, the specified content is added as an agentless connection-destination definition.
- If a value is specified for the first data item (ID) of an agentless connection-destination definition, the agentless connection-destination definition corresponding to the specified ID is updated with the content specified in the line. If the agentless connection destination definition corresponding to the specified ID does not exist, the system generates an error.
- When two or more agentless connection-destination definitions are specified in a file and the addition or update portion of the definitions fails, the command results are as follows:

  - A return value (warning, not error) is used to report a definition that was not successfully registered.

  - Information is output as a standard error, which enables you to identify the definition that was not successfully registered.

  - The registration processing continues for all remaining definitions, even if an error occurs.

Usage example: Register or update the agentless connection-destination definitions in Ops Center Automator with the content of a specified file

```
setremoteconnection /file bbbbb /user xxxxx
```

Example: Successful registration of agentless connection-destination definition

```
KNAE03000-I The setremoteconnection command will now start.
KNAE03002-E The remote connection definition was registered (ID:12345, line number:
12345).
```

Example: Unsuccessful registration or update

```
KNAE03000-I The setremoteconnection command will now start.
KNAE03002-E The setremoteconnection command ended abnormally (12345).
```

Example: Error encountered in parameters

```
KNAE03000-I The setremoteconnection command will now start.
KNAE03333-E A required parameter was not found (parameter name: XXXXX, line number:
12345). Specify the required parameter, and then try again.
KNAE03334-E Unnecessary parameter has been specified (parameter name: XXXXX, line
number: 12345). Delete the specified parameters, and then try again.
KNAE03002-E The setremoteconnection command ended abnormally (12345).
```

setupcluster command

The **setupcluster** command sets up an Ops Center Automator cluster environment.

Syntax

```
setupcluster {/exportpath exportpath | /help}
```

Options

Option	Description
/exportpath	The absolute or relative path of the folder on a shared disk used to store the database and server information. The folder directly under the shared disk (`root` folder) cannot be specified.

setupcommonservice command

The **`setupcommonservice`** command is a setting command for linking with Common Services. The **`setupcommonservice`** command registers Ops Center Automator as an application in Common Services and sets Ops Center Automator as an authentication server that uses Common Services.

Note: You cannot unregister Ops Center Automator using the **`setupcommonservice`**. To delete the product, use the Ops Center portal.

Functions

The **`setupcommonservice`** command registers the Ops Center Automator URL in Common Services. The URL to be registered uses the URL registered in the **`hcmds64chgurl`** command. Confirm in advance that the URL registered in **`hcmds64chgurl`** can be resolved by the browser, then run the **`setupcommonservice`** command.

This command needs a secure connection between Ops Center Common Services and Ops Center Automator. See the *Hitachi Ops Center Installation and Configuration Guide* for more information.

Syntax

Windows syntax:

```
setupcommonservice {[/csUri CommonServiceUri | /csUri CommonServiceUri /csUsername
CommonServiceUsername] [/appName ApplicationName]
[/appDescription ApplicationDescription] [ /auto ] | /help }
```

Linux syntax:

```
setupcommonservice {[-csUri CommonServiceUri | -csUri CommonServiceUri -csUsername
CommonServiceUsername] [-appName ApplicationName]
[-appDescription ApplicationDescription] [ -auto ] | -help }
```

Note: You are prompted to enter the password in interactive mode.

Options

Option	Description
`csUri`	Specify the URL of Common Services. (For example: https://common.service/portal)
`csUsername`	Specify a user with opscenter-security-administrator privileges to be managed by Common Services. The username can be 1-byte alphanumeric characters. This includes (! # $% & '() * +-. = @ ^ _ |). The length is from 1 to 255 characters. Usernames are case-sensitive. You are prompted to enter the password when you run the command with this option.
`appName`	Specify the name of the Ops Center Automator to be displayed by Common Services. The name is specified with 1 to 128 characters. If `appName` is omitted at the time of new registration, the host name or IP address of Ops Center Automator is set as the name. If `appName` is omitted when updating, the name is not changed.
`appDescription`	Specify a description of the Ops Center Automator displayed by Common Services. The description can be from 0 to 512 characters.
`auto`	Automatically start and stop the services and databases of Ops Center Automator.

Remarks

Before running the **`setupcommonservice`** command in a cluster environment, you must run the following two commands in sequence to take the group where the Ops Center Automator service is registered offline, disable failover, and start the databases.

- *`Common-component-Installation-folder`*`\ClusterSetup\hcmds64clustersrvstate /soff /r` *`group-name`*
- *`Common-component-Installation-folder`*`\bin\hcmds64dbsrv /start`

stoptask command

The **`stoptask`** command stops a running task.

Syntax

```
stoptask {/taskid task-ID [/user username | /user username /passwordfile
passwordfile] [/authmode local | external] | /help}
```

Note: You are prompted to enter the password in interactive mode if you do not specify the `passwordfile` option.

Options

Option	Description
`/taskid`	The task ID. You can confirm the task ID from the **Task Details** window, output of **`submittask`** command, output of **`listtasks`** command.
`/user`	The user ID.
`/passwordfile`	The absolute or relative path of the password file.
`/authmode`	Specifies the authentication type, either `local` or `external`. Specify `local` to authenticate locally with Automator. Specify `external` to authenticate with Common Services. If this option is not specified, Ops Center Automator operates in the authentication mode specified by the `command.auth.mode` of `command_user.properties`.

submittask command

The **`submittask`** command submits a service for execution using the specified service name, service group name, and property options, and returns the task ID as the execution output of the command.

Functions

The submittask command has four functions:

- Immediate execution of a service.
- Scheduled execution of a service.
- Recurrent execution of a service.
- Reregistration of tasks.

  If this option is specified, you can reregister tasks that were output by the **`listtasks`** command with the taskdetails option.

Syntax: Immediate execution of a service

```
submittask {/servicename ServiceName [/servicegroup ServiceGroup]
    [/taskname  TaskName]
    [/taskdescription TaskDescription]
    [{[/property Key "Value"]... | /propertyfile PropertyFile}]
    [/user UserName | /user UserName /passwordfile PasswordFile]
    [/wait]
    [/authmode local | external] | /help}
```

Syntax: Scheduled execution of a service

```
submittask {/servicename ServiceName
    [/servicegroup ServiceGroup]
    [/taskname TaskName]
    [/taskdescription TaskDescription]
    [{[/property Key "Value"]... | /propertyfile PropertyFile}]
    [/user UserName | /user UserName /passwordfile PasswordFile]
    /scheduledate yyyy-mm-dd
    /scheduletime hh:mm
    [/authmode local | external] | /help}
```

Syntax: Recurrent execution of a service

```
submittask {/servicename ServiceName
    [/servicegroup ServiceGroup]
    [/taskname TaskName]
    [/taskdescription TaskDescription]
    [{[/property Key "Value"]... | /propertyfile PropertyFile}]
    [/user UserName | /user UserName /passwordfile PasswordFile]
    /recurrencepattern {daily[:{1h|2h|3h|4h|6h|8h|12h|24h}] |
    weekly:sun,mon,...,sat | monthly:{dd,dd,...,dd
    [,endofmonth] | endofmonth}}
    /recurrencetime hh:mm /recurrencestart yyyy-mm-dd
    [/authmode local | external] | /help}
```

Syntax: Reregistration of tasks

```
submittask {/reregister
    /taskdetaildir DirectoryName
    [/setoriginalsubmitter]
    [/user UserName | /user UserName /passwordfile PasswordFile]
    [/authmode local | external] | /help}
```

Note: You are prompted to enter the password in interactive mode if you do not specify the `passwordfile` option.

Permission

- To run this command, you must have the Admin, Modify, or Submit role in Ops Center Automator and Administrator permission for the OS.
- You cannot run services that are in a service group whose role is not set.
- The service you want to run must belong to the service group with a role that is assigned by the user group. The user must belong to the user group.

Options

Option	Description
`/servicename`	Specify a service name. The name of a service you want to submit. The service name can be 1 to 128 characters long.
`/servicegroup`	Specifies a service group to which the service belongs. The name of the service group that the service belongs to. This is an optional parameter. If you omit this option, the service group that is associated with the user who is specified in the `/user` option is used. However, if more than one service group is associated with that user, an error occurs. The service group name can be 1 to 80 characters long and consists of half-width alphanumeric characters and _ (underscore).
`/taskname`	Specify a task name. The name of the task. If you omit this option, the system defaults to *service-name_YYYYMMDDhhmmss*, where *service-name* is the value of the `/servicename` option and *YYYYMMDDhhmmss* is the time when the service runs. The task name can be 1 to 128 characters long and can consists of any characters except control characters ('\u0000'~'\u001F' or \u007F'~'\u009F'). This is an optional parameter.
`/taskdescription`	Specify a task description. The description of the task. The description can be 1 to 256 characters long and can consists of any characters except control characters ('\u0000'~'\u001F' or \u007F'~'\u009F'). This is an optional parameter.
`/property`	Specify a property key and value. One or more property key-value combinations that are used by the service to be performed.

Option	Description
	If a property value is not set for a key, the default value used. If the value of a required property key is not set, then an error occurs. You cannot specify both the `/property` and the `/propertyfile` options. If you do, then an error occurs. You can specify this option more than one time, for example, `/property property-key-1 property-value-1 /property property-key-2 property-value-2`. The maximum number of combinations of property keys and values available is 1000 pairs. This value can be changed by using the `server.editor.publicProperty.perTemplate.maxnum` key in the `config_user.properties` file. ▪ *key* is the property key for the service. It can be 1 to 1024 characters long. The key consists of half-width alphanumeric characters and the following characters: / (slash), . (period), (hyphen), and _ (underscore). Specifying the same property key more than one time causes an error. ▪ *value* is the value for the *key* property. If the value includes a space or special character, the value must be enclosed in double quotation marks (").
`/propertyfile`	Specify a properties file. Use an absolute or relative path. The name of a properties file, including an absolute or relative path, that defines the property settings that the service you want to perform uses. Property keys and values that are not specified in the properties file are set to default values. If you do not specify a required property key and that key has no default value, then an error occurs. This option and the `/property` option cannot be specified at the same time. If both options are specified, then an error occurs.

Option	Description
	Additional requirements: ▪ Location: The properties file can be in any folder. However, the user who runs the command must be able to access it. ▪ File name: Any file name. ▪ Key-value combination format: *property-key*=*property-value*(linefeed code) *property-key*=*property-value*(linefeed code) If you add a suffix @FILE to the key, it is possible to specify a text file to value. For example, key@FILE=C:\properties \valuefile.txt.
`/user`	Specify a user ID. The ID for the Ops Center Automator user who has access permission to run the service. The ID can be 1 to 256 half-width alphanumeric characters. It can consist of any characters, except the following: ! # $ % & ( ) * + - . = @ \ ^ _ |. The ID is not case-sensitive.
`/passwordfile`	Specify a password file. Use an absolute or relative path. The absolute or relative path to the password file for the user who is specified in the `/user` option. You can create a password file by using the **`encryptpassword`** command.
`/wait`	Wait for a task to finish. Shows the task execution result (normal termination or failure). If the `/wait` option is not specified, the command ends without waiting for the task to end. In this case, a message reporting the task ID is provided only when the task execution has started normally.
`/scheduledate`	Specify a date for executing a service. When this option is specified, any of the following conditions will result in an error: ▪ A combination of arguments that is not valid. ▪ The form of the specified date is incorrect.

Option	Description
	▪ The time indicated by `/ scheduledate` and `/ scheduletime` is in the past. The relevant time is server time. ▪ The specified date is outside the range of January 1, 1994 to December 31, 2036 Format: Specify the date in the form of "yyyy-mm-dd." Specify the year as yyyy in four digits. Specify the month as mm in the range 1 (or 01) to 12. Specify a day as dd in the range 1 (or 01) to 31.
`/scheduletime`	Specify a time for executing a service. When this option is specified, any of the following conditions will result in an error: ▪ A combination of arguments that is not valid. ▪ The form of the specified time is incorrect. ▪ The time indicated by `/ scheduledate` and `/ scheduletime` is in the past. The relevant time is server time. Specify the time in the form of "hh:mm." Specify hours as hh in the range 0 (or 00)-23. Specify minutes as mm in the range 0 (or 00)-59.
`/recurrencepattern`	Specify a pattern for a recurring service. Use this option with the `/recurrencetime` option, and the `/recurrencestart` option. When this option is specified, the following conditions will result in an error: ▪ A combination of arguments that is not valid. ▪ The format of the specified fixed execution cycle is incorrect.

Option	Description
	Recurrence options and formats: ▪ Daily: specify "daily:1h, 2h, 3h, 4h, 6h, 8h, 12h, 24h". The default recurrence is every 24 hours. ▪ Weekly: specify "weekly:sun, mon, ..." using three letter English abbreviations for days of the week and comma-separated values following a colon. The days can be in any order. • Sunday: sun • Monday: mon • Tuesday: tue • Wednesday: wed • Thursday: thu • Friday: fri • Saturday: sat ▪ Monthly: specify two-digit comma-separated values following a colon. For the last day of the month, specify "endofmonth."
`/recurrencetime`	Specify the execution time for a recurring service. Use this option with the `/recurrencepattern` option, and the `/recurrencestart` option. When this option is specified, the following conditions will result in an error: ▪ A combination of arguments that is not valid. ▪ The form of the specified time is inaccurate. Format: Specify the time in the form of "hh:mm." Specify hours as hh in the range 0 (or 00) to 23. Specify minutes as mm in the range 0 (or 00) to 59.
`/recurrencestart`	Specify a date for a recurring service to start. Use this option with the `/recurrencepattern` option, and the `/recurrencetime` option.

Option	Description
	When this option is specified, the following conditions will result in an error: ▪ A combination of arguments that is not valid. ▪ The form of the specified date is inaccurate. ▪ The specified date is outside the range on January 1, 1994 to December 31, 2036. Format: Specify the date in the form of "yyyy-mm-dd." Specify the year as yyyy in four digits. Specify the month as mm in the range 1 (or 01) to 12. Specify a day as dd in the range 1 (or 01) to 31.
`/reregister`	Specify to reregister scheduled tasks. This option has no value.
`/taskdetaildir`	Specify a folder that was output by the **`listtasks`** command with the `/taskdetails` option. Use an absolute or relative path. The folder must be located on a local disk. The maximum path length is 180 characters.
`/setoriginalsubmitter`	Specify whether you want to reregister tasks as the user at the point in time in which task details were output. This option has no value. When this option is not specified, the user ID specified as the `/user` of the `submittask` command serves as the assigned user of the task after reregistration.
`/authmode local | external`	Specify the authentication type, either `local` or `external`. Specify `local` to authenticate locally with Automator. Specify `external` to authenticate with Common Services. If this option is not specified, Ops Center Automator operates in the authentication mode specified by the `command.auth.mode` of `command_user.properties`.
`/help`	Show command syntax and usage.

Command location

installation-folder\bin

Return codes

The following table lists the **`submittask`** command return codes and descriptions.

Return code	Description
0	The command succeeded.
1	The argument is not valid.
2	The command stopped.
3	The service status is not valid.
4	The number of commands that can be run simultaneously is exceeded.
5	Communication failed.
6	Authentication failed.
7	A path is specified that is not valid.
9	Path not found.
10	Path cannot be accessed.
14	You do not have permission to run the command.
17	The interactive input value is not valid.
130	The service did not start.
131	The properties file does not exist.
132	The properties file has a format that is not valid.
133	The command with `/wait` option failed to get the current command status.
134	The task failed.
135	The task was canceled.
136	The contents of the folder specified by the `/taskdetails` option are not valid.
137	Some part of the tasks failed to be registered by the command with the `/reregister` option.
138	All tasks failed to be registered by the command with the `/reregister` option.
139	The content of task detail folder is different from the current version or revision.
255	The command stopped due to an error other than the ones listed in this table.

Example: Immediate execution of a service

```
submittask /servicename "Execute Remote Command"
        /servicegroup "Default Service Group"
        /taskname "Submittask sample"
        /taskdescription "This is a sample."
        /property common.targetHost host01 /property common.remoteCommand ipconfig
        /user Bob
```

Example: Scheduled execution of a service

```
submittask /servicename "Execute Remote Command"
        /propertyfile "C:\temp\properties.txt"
        /scheduledate 2020-01-23 /scheduletime 12:34
        /user Bob
```

Example: Recurrent execution of a service

```
submittask /servicename "Execute Remote Command"
        /propertyfile "C:\temp\properties.txt"
        /recurrencepattern weekly:sun,mon,sat
        /recurrencetime 12:34 /recurrencestart 2020-01-23
        /user Bob
```

Example: Reregistration of tasks

```
submittask /reregister /taskdetaildir "C:\temp\taskdetails"
        /user Bob
```

Appendix A: Ops Center Automator file location and ports

This module includes a list of all the folders or directories that Ops Center Automator creates as part of the installation. It also includes a list of ports.

Ops Center Automator file location

Installation folders

The following tables list the folders or directories that are created when Ops Center Automator is installed. The Windows folder locations column and Linux OS directory locations column lists default paths that can be changed during installation.

Windows folder details	Windows folder locations
Folder specified when installing Ops Center Automator	`system-drive\Program Files\hitachi`
Ops Center Automator installation folder	`system-drive\Program Files\hitachi\Automation`
Commands files	`system-drive\Program Files\hitachi\Automation\bin`
Configuration files	`system-drive\Program Files\hitachi\Automation\conf`
Folder for service templates	`system-drive\Program Files\hitachi\Automation\contents`
Folder for service templates and plug-ins under development	`system-drive\Program Files\hitachi\Automation\develop`
Data files	`system-drive\Program Files\hitachi\Automation\data`
Help files	`system-drive\Program Files\hitachi\Automation\docroot`
Temporary working folder for installation and removal	`system-drive\Program Files\hitachi\Automation\inst`

Windows folder details	Windows folder locations
Library files	`system-drive\Program Files\hitachi \Automation\lib`
Log files	`system-drive\Program Files\hitachi \Automation\logs`
System files	`system-drive\Program Files\hitachi \Automation\system`
Working folder used by Internal command	`system-drive\Program Files\hitachi \Automation\webapps`
Working folder	`system-drive\Program Files\hitachi \Automation\work`
Common Component	`system-drive\Program Files\hitachi\Base64`

Linux OS directory details	Linux OS directory locations
Directory specified when installing Ops Center Automator	`/opt/hitachi`
Ops Center Automator installation directory	`/opt/hitachi/Automation`
Commands files	`/opt/hitachi/Automation/bin`
Configuration files	`/opt/hitachi/Automation/conf`
Directory for service templates	`/var/opt/hitachi/Automation/contents`
Directory for service templates and plug-ins under development	`/var/opt/hitachi/Automation/develop`
Data files	`/var/opt/hitachi/Automation/data`
Help files	`/opt/hitachi/Automation/docroot`
Temporary working directory for installation and removal	`/opt/hitachi/Automation/inst`
Library files	`/opt/hitachi/Automation/lib`
Log files	`/var/opt/hitachi/Automation/logs`
System files	`/opt/hitachi/Automation/system`
Working directory used by Internal command	`/opt/hitachi/Automation/webapps`

Linux OS directory details	Linux OS directory locations
Working directory	`/var/opt/hitachi/Automation/work`
Common Component	`/opt/hitachi/Base64`

Port settings

Ops Center Automator uses the following port settings:

External connection port

Port number	Firewall	Description
22/tcp	Automator --> Operation target	Used for SSH. `cjstartsv` uses this port.
23/tcp	Automator --> Operation target	Used for Telnet. `cjstartsv` uses this port.
443/tcp	Automator-->Common Services	Used to access Common Services
445/tcp or udp	Automator --> Operation target	Used for Windows administrative shares. `cjstartsv` uses this port.
135/tcp and 139/tcp	Automator --> Operation target	Used for Windows administrative shares. `cjstartsv` uses this port.
22015/tcp	Browser -> Automator	Used to access HBase 64 Storage Mgmt Web Service. In non-SSL (unsecured) communication, initial setup is a required. This port number can be changed. `httpsd` uses this port.
22016/tcp	Browser -> Automator	Use to access HBase 64 Storage Mgmt Web Service. In SSL (secured) communication, a setting is required. This port number can be changed. `httpsd` uses this port.

Port number	Firewall	Description
25/tcp	Automator -> SMTP server	Used for mail transmission. This port number can be changed. For details, see "Configuring email and log settings" in the *Hitachi Ops Center Automator User Guide*. `cjstartsv` uses this port.
88/tcp or udp	Automator -> Kerberos server	`cjstartsv` uses this port.
389/tcp	Automator -> LDAP directory server	Used for `ldap/tls`. `cjstartsv` uses this port.
1812/udp	Automator -> Radius server	Used for Radius servers. `cjstartsv` uses this port.
Various Web Service connection ports/tcp	Automator -> Various servers	Used for the servers registered to Web Service connections.

Internal connection port

Port number	Firewall	Description
22017/tcp	Automator -> Automator	Used to access the Common Component. `cjstartsv` uses this port.
22018/tcp	Automator -> Automator	Used to access the Common Component. `cjstartsv` uses this port.
22025/tcp	Automator -> Automator	Used to access the Common Component. `cjstartsv` uses this port.
22026tcp	Automator -> Automator	Used to access the Common Component. `cjstartsv` uses this port.
22031/tcp	Automator -> Automator	Used to access the Common Component. `cjstartsv` uses this port.

Port number	Firewall	Description
22032/tcp	Automator -> Automator	Used to access the Common Component. `cjstartsv` uses this port.
22035/tcp	Automator -> Automator	Used to access the Common Component. `cjstartsv` uses this port.
22036/tcp	Automator -> Automator	Used to access the Common Component. `cjstartsv` uses this port.
22037/tcp	Automator -> Automator	Used to access the Common Component. `cjstartsv` uses this port.
22038/tcp	Automator -> Automator	Used to access the Common Component. `cjstartsv` uses this port.
22170/tcp	Automator -> Automator	Used to access the Common Component. `cjstartsv` uses this port.
22171/tcp	Automator -> Automator	Used to access the Common Component. `cjstartsv` uses this port.
22172/tcp	Automator -> Automator	Used to access the Common Component. `cjstartsv` uses this port.
22173/tcp	Automator -> Automator	Used to access the Common Component. `cjstartsv` uses this port.
22220/tcp	Automator -> Automator	Used in an embedded database.

Note: These ports are "reserved" and are used only for an internal port connection.

Appendix B: Ops Center Automator processes

This module includes a list of the Ops Center Automator processes.

Ops Center Automator processes (Windows)

The following table lists the Ops Center Automator processes in Windows. This table contains the process information necessary to check Ops Center Automator status. Note that this is not a table of the Ops Center Automator process configuration.

Process name	Service name	Description
cjstartsv.exe	HAutomation Engine Web Service	Used in Common Component.
hcmdssvctl.exe		
cjstartsv.exe	HBase 64 Storage Mgmt SSO Service	Used in Common Component.
hcmdssvctl.exe		
httpsd.exe	HBase 64 Storage Mgmt Web Service	Used in Common Component.
rotatelogs.exe		
httpsd.exe	HBase 64 Storage Mgmt Web SSO Service	Used in Common Component.
rotatelogs.exe		
pdservice.exe	HiRDB/EmbeddedEdition _HD1	Used in the Common Component database.
pdprcd.exe		
pdmlgd.exe		
pdrdmd.exe		

Ops Center Automator processes (Linux)

The following table lists the Ops Center Automator processes in Linux. This table contains the process information necessary to check Ops Center Automator status. Note that this is not a table of the Ops Center Automator process configuration.

Process name	Daemon name	Description
cjstartsv	hicommand64-hcs_ao	Used in Common Component.
hcs_ao		
cjstartsv	hicommand64-hcs_hsso	Used in Common Component.
hcs_hsso		
httpsd	hicommand64-hcs_web	Used in Common Component.
rotatelogs		
httpsd	hicommand64-hcs_hweb	Used in Common Component.
rotatelogs		
pdprcd	-	Used in the Common Component database.
pdmlgd		
pdrdmd		

Appendix C: SSL cipher suites

The following is a list of cipher suites used for SSL communication.

Cipher suites supported as a server

The following table lists cipher suites supported by Ops Center Automator as a server.

TLS version	Cipher suite name
1.3	TLS_AES_128_GCM_SHA256
	TLS_AES_256_GCM_SHA384
	TLS_CHACHA20_POLY1305_SHA256
1.2	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

Cipher suites supported as a client

The following table lists cipher suites available by default in Ops Center Automator as a client.

TLS version	Cipher suite name
1.3	TLS_AES_256_GCM_SHA384
	TLS_AES_128_GCM_SHA256
	TLS_CHACHA20_POLY1305_SHA256
1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
	TLS_RSA_WITH_AES_256_GCM_SHA384

TLS version	Cipher suite name
	TLS_RSA_WITH_AES_128_GCM_SHA256

Note: In addition to the cipher suites in the table, you can add any cipher suites available by default in the bundled JDK.

Appendix D: SSH cryptographic algorithms

The following is a list of cryptographic algorithms used in SSH connections.

Supported cryptographic algorithms

The following tables list each cryptographic algorithm supported by Ops Center Automator.

Table 34 List of key exchange algorithms supported by Ops Center Automator

Cryptographic algorithm name	Default value
curve25519-sha256	Valid
curve25519-sha256@libssh.org	Valid
diffie-hellman-group14-sha1	Invalid
diffie-hellman-group14-sha256	Valid
diffie-hellman-group16-sha512	Valid
diffie-hellman-group18-sha512	Valid
diffie-hellman-group-exchange-sha256	Valid
ecdh-sha2-nistp256	Valid
ecdh-sha2-nistp384	Valid
ecdh-sha2-nistp521	Valid

Table 35 List of cipher algorithms supported by Ops Center Automator

Cryptographic algorithm name	Default value
3des-cbc	Invalid
aes128-cbc	Invalid
aes128-ctr	Valid
aes128-gcm@openssh.com	Valid
aes192-cbc	Invalid

Cryptographic algorithm name	Default value
aes192-ctr	Valid
aes256-cbc	Invalid
aes256-ctr	Valid
aes256-gcm@openssh.com	Valid
chacha20-poly1305@openssh.com	Valid

Table 36 List of MAC algorithms supported by Ops Center Automator

Cryptographic algorithm name	Default value
hmac-sha1	Invalid
hmac-sha1-96	Invalid
hmac-sha1-etm@openssh.com	Invalid
hmac-sha2-256	Valid
hmac-sha2-256-etm@openssh.com	Valid
hmac-sha2-512	Valid
hmac-sha2-512-etm@openssh.com	Valid

Table 37 List of public key algorithms for the host key supported by Ops Center Automator

Cryptographic algorithm name	Default value
ecdsa-sha2-nistp256	Valid
ecdsa-sha2-nistp384	Valid
ecdsa-sha2-nistp521	Valid
rsa-sha2-256	Valid
rsa-sha2-512	Valid
ssh-dss	Valid
ssh-ed25519	Valid
ssh-rsa	Valid

List of public key algorithms for public key authentication supported by Ops Center Automator

The following is a list of cryptographic algorithm names supported by Ops Center Automator.

- cdsa-sha2-nistp256
- ecdsa-sha2-nistp384
- ecdsa-sha2-nistp521
- rsa-sha2-256
- rsa-sha2-512
- ssh-dss
- ssh-ed25519
- ssh-rsa

Note: The cryptographic algorithm corresponding to the key type and key length is automatically used.

Appendix E: Troubleshooting

This module describes the actions to take if an error occurs on the Ops Center Automator server. Confirm the messages or log files to determine the cause of the error, and take action accordingly.

Collecting maintenance information

If no messages are output when a problem occurs, or you cannot correct the problem even after following the instructions in the message, collect maintenance information, and then contact user support.

Collecting the log files

Run the **`hcmds64getlogs`** (on page 204) (on page 204) command to collect the log files.

Procedure

1. Log on to the management server as a user with Administrator permissions (for Windows) or as a root user (for Linux).
2. Run the **`hcmds64getlogs`** (on page 204) (on page 204) command to collect the log files.

   In Windows:

   ```
   Common-Component-installation-folder\bin\hcmds64getlogs /dir output-folder-path
   ```

   In Linux:

   ```
   Common-Component-installation-directory/bin/hcmds64getlogs -dir output-directory-path
   ```

Result

An archive file is output to the specified destination.

See hcmds64getlogs command (on page 204).

Appendix F: Notices

This software product includes the following redistributable software.

Notices

This product includes software developed by the Apache Software Foundation (http://www.apache.org/).

Portions of this software were developed at the National Center for Supercomputing Applications (NCSA) at the University of Illinois at Urbana-Champaign.

This product includes software developed by the University of California, Berkeley and its contributors.

This software contains code derived from the RSA Data Security Inc. MD5 Message-Digest Algorithm, including various modifications by Spyglass Inc., Carnegie Mellon University, and Bell Communications Research, Inc (Bellcore).

Regular expression support is provided by the PCRE library package, which is open source software, written by Philip Hazel, and copyright by the University of Cambridge, England. The original software is available from ftp://ftp.csx.cam.ac.uk/pub/software/programming/pcre/

1. This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)

2. This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)

3. This product includes software written by Tim Hudson (tjh@cryptsoft.com)

4. This product includes the OpenSSL Toolkit software used under OpenSSL License and Original SSLeay License. OpenSSL License and Original SSLeay License are as follow:

LICENSE ISSUES

==============

The OpenSSL toolkit stays under a double license, i.e. both the conditions of

the OpenSSL License and the original SSLeay license apply to the toolkit.

See below for the actual license texts.

OpenSSL License

----

* "This product includes software developed by the OpenSSL Project
* for use in the OpenSSL Toolkit. (http://www.openssl.org/)"
*
* 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to
* endorse or promote products derived from this software without
* prior written permission. For written permission, please contact
* openssl-core@openssl.org.
*
* 5. Products derived from this software may not be called "OpenSSL"
* nor may "OpenSSL" appear in their names without prior written
* permission of the OpenSSL Project.
*
* 6. Redistributions of any form whatsoever must retain the following
* acknowledgment:
* "This product includes software developed by the OpenSSL Project
* for use in the OpenSSL Toolkit (http://www.openssl.org/)"
*
* THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY
* EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
* PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR
* ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
* SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
* NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
* LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
* STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
* ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
* OF THE POSSIBILITY OF SUCH DAMAGE.
* ==
*
* This product includes cryptographic software written by Eric Young
* (eay@cryptsoft.com). This product includes software written by Tim
* Hudson (tjh@cryptsoft.com).
*
*/

Original SSLeay License

/* Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)
* All rights reserved.
*
* This package is an SSL implementation written
* by Eric Young (eay@cryptsoft.com).
* The implementation was written so as to conform with Netscapes SSL.
*
* This library is free for commercial and non-commercial use as long as
* the following conditions are aheared to. The following conditions
* apply to all code found in this distribution, be it the RC4, RSA,
* lhash, DES, etc., code; not just the SSL code. The SSL documentation
* included with this distribution is covered by the same copyright terms

```
* except that the holder is Tim Hudson (tjh@cryptsoft.com).
*
* Copyright remains Eric Young's, and as such any Copyright notices in
* the code are not to be removed.
* If this package is used in a product, Eric Young should be given attribution
* as the author of the parts of the library used.
* This can be in the form of a textual message at program startup or
* in documentation (online or textual) provided with the package.
*
* Redistribution and use in source and binary forms, with or without
* modification, are permitted provided that the following conditions
* are met:
* 1. Redistributions of source code must retain the copyright
* notice, this list of conditions and the following disclaimer.
* 2. Redistributions in binary form must reproduce the above copyright
* notice, this list of conditions and the following disclaimer in the
* documentation and/or other materials provided with the distribution.
* 3. All advertising materials mentioning features or use of this software
* must display the following acknowledgement:
* "This product includes cryptographic software written by
* Eric Young (eay@cryptsoft.com)"
* The word 'cryptographic' can be left out if the rouines from the library
* being used are not cryptographic related :-).
* 4. If you include any Windows specific code (or a derivative thereof) from
* the apps directory (application code) you must include an acknowledgement:
* "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"
*
* THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND
* ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
* ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE
* FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
* DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
* OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
* LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
* OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
* SUCH DAMAGE.
*
* The licence and distribution terms for any publically available version or
* derivative of this code cannot be changed. i.e. this code cannot simply be
* copied and put under another distribution licence
* [including the GNU Public Licence.]
*/
```

This product includes the OpenSSL library.

The OpenSSL library is licensed under Apache License, Version 2.0.

https://www.apache.org/licenses/LICENSE-2.0

Oracle and Java are registered trademarks of Oracle and/or its affiliates.

This product includes software developed by IAIK of Graz University of Technology.

This product includes software developed by Daisuke Okajima and Kohsuke Kawaguchi (http://relaxngcc.sf.net/).

This product includes software developed by the Java Apache Project for use in the Apache JServ servlet engine project (http://java.apache.org/).

This product includes software developed by Andy Clark.

Java is a registered trademark of Oracle and/or its affiliates.

Java™
COMPATIBLE
ENTERPRISE
EDITION

Java™
COMPATIBLE

Other company and product names mentioned in this document may be the trademarks of their respective owners.

Hitachi Vantara

Corporate Headquarters
2535 Augustine Drive
Santa Clara, CA 95054 USA

HitachiVantara.com/contact