HITACHI
Inspire the Next

Hitachi Ops Center Automator
インストールガイド

4010-1J-619-10

前書き

■ 対象製品

Hitachi Ops Center Automator 11.0.2

■ 輸出時の注意

本マニュアル固有の技術データおよび技術は、米国輸出管理法、および関連の規制を含む米国の輸出管理法の対象となる場合があり、その他の国の輸出または輸入規制の対象となる場合もあります。読者は、かかるすべての規制を厳守することに同意し、マニュアルおよび該当製品の輸出、再輸出、または輸入許可を取得する責任があることを了解するものとします。

■ 商標類

HITACHI は，株式会社 日立製作所の商標または登録商標です。

This product includes software developed by the Apache Software Foundation (http://www.apache.org/).

Portions of this software were developed at the National Center for Supercomputing Applications (NCSA) at the University of Illinois at Urbana-Champaign.

This product includes software developed by the University of California, Berkeley and its contributors.

This software contains code derived from the RSA Data Security Inc. MD5 Message-Digest Algorithm, including various modifications by Spyglass Inc., Carnegie Mellon University, and Bell Communications Research, Inc (Bellcore).

Regular expression support is provided by the PCRE library package, which is open source software, written by Philip Hazel, and copyright by the University of Cambridge, England. The original software is available from ftp://ftp.csx.cam.ac.uk/pub/software/programming/pcre/

1. This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)

2. This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)

3. This product includes software written by Tim Hudson (tjh@cryptsoft.com)

4. This product includes the OpenSSL Toolkit software used under OpenSSL License and Original SSLeay License. OpenSSL License and Original SSLeay License are as follow:

LICENSE ISSUES

==========

The OpenSSL toolkit stays under a double license, i.e. both the conditions of

the OpenSSL License and the original SSLeay license apply to the toolkit.

See below for the actual license texts.

OpenSSL License

/*

==========

* Copyright (c) 1998-2019 The OpenSSL Project. All rights reserved.

*

* Redistribution and use in source and binary forms, with or without

* modification, are permitted provided that the following conditions

* are met:

*

* 1. Redistributions of source code must retain the above copyright

* notice, this list of conditions and the following disclaimer.

*

* 2. Redistributions in binary form must reproduce the above copyright

* notice, this list of conditions and the following disclaimer in

* the documentation and/or other materials provided with the

* distribution.

*

* 3. All advertising materials mentioning features or use of this

* software must display the following acknowledgment:

* "This product includes software developed by the OpenSSL Project

* for use in the OpenSSL Toolkit. (http://www.openssl.org/)"

*

* 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to

* endorse or promote products derived from this software without

* prior written permission. For written permission, please contact

* openssl-core@openssl.org.

*

* 5. Products derived from this software may not be called "OpenSSL"

* nor may "OpenSSL" appear in their names without prior written

* permission of the OpenSSL Project.

*

* 6. Redistributions of any form whatsoever must retain the following

* acknowledgment:
* "This product includes software developed by the OpenSSL Project
* for use in the OpenSSL Toolkit (http://www.openssl.org/)"
*
* THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY
* EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
* PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR
* ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
* SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
* NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
* LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
* STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
* ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
* OF THE POSSIBILITY OF SUCH DAMAGE.
*
==========
*
* This product includes cryptographic software written by Eric Young
* (eay@cryptsoft.com). This product includes software written by Tim
* Hudson (tjh@cryptsoft.com).
*
*/

Original SSLeay License

/* Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)
* All rights reserved.
*
* This package is an SSL implementation written
* by Eric Young (eay@cryptsoft.com).
* The implementation was written so as to conform with Netscapes SSL.
*
* This library is free for commercial and non-commercial use as long as

* the following conditions are aheared to. The following conditions
* apply to all code found in this distribution, be it the RC4, RSA,
* lhash, DES, etc., code; not just the SSL code. The SSL documentation
* included with this distribution is covered by the same copyright terms
* except that the holder is Tim Hudson (tjh@cryptsoft.com).
*
* Copyright remains Eric Young's, and as such any Copyright notices in
* the code are not to be removed.
* If this package is used in a product, Eric Young should be given attribution
* as the author of the parts of the library used.
* This can be in the form of a textual message at program startup or
* in documentation (online or textual) provided with the package.
*
* 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.]
*/

Oracle および Java は，オラクルおよびその関連会社の登録商標です。

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.

その他記載の会社名，製品名などは，それぞれの会社の商標もしくは登録商標です。

■ 発行

2024 年 6 月 4010-1J-619-10

はじめに

このマニュアルでは、Hitachi Ops Center Automator のインストールと構成の方法を説明します。

■ 対象読者

このマニュアルは、ストレージ環境内のストレージ、サービス、およびアプリケーションを担当するストレージ管理者を対象としています。

■ マニュアルの構成

このマニュアルは、次に示す章と付録から構成されています。

第 1 章　概要

Ops Center Automator の概要について説明しています。

第 2 章　Ops Center Automator をインストールまたはアップグレードする

クラスターおよび非クラスター環境での、Ops Center Automator のインストールまたはアップグレード方法について説明しています。

第 3 章　Ops Center Automator を構成する

Ops Center Automator を構成する方法について説明しています。

第 4 章　外部認証サーバーでのユーザー管理

外部認証サーバーでユーザー認証を設定する方法について説明しています。

第 5 章　Ops Center Automator をバックアップおよびリストアする

Ops Center Automator をバックアップおよびリストアする方法について説明しています。

第 6 章　Ops Center Automator をアンインストールする

Ops Center Automator をアンインストールする方法について説明しています。

第 7 章　コマンド

Ops Center Automator および共通コンポーネントのコマンドは、コマンドラインインターフェイス（CLI）で実行できます。

付録 A　Ops Center Automator のファイルの場所とポート

Ops Center Automator のインストール時に作成されるファイルの場所およびポートについて説明しています。

付録 B　Configuration Manager を前提とするサービスで VSP One B20 を管理する場合の Configuration Manager のポート設定

Configuration Manager を前提とするサービスで VSP One B20 を管理する場合のポートの設定について説明しています。

付録 C　Ops Center Automator のプロセス

Ops Center Automator のプロセスについて説明しています。

付録 D　SSL 通信で使用する Cipher Suites

SSL 通信で使用する Cipher Suites について説明しています。

付録 E　SSH 接続で使用する暗号アルゴリズム

SSH 接続で使用する暗号アルゴリズムについて説明しています。

付録 F　トラブルシューティング

Ops Center Automator サーバーでエラーが発生した場合の対処方法について説明しています。

■ マイクロソフト製品の表記について

このマニュアルでは、マイクロソフト製品の名称を次のように表記しています。

表記	製品名
Windows	次の製品を区別する必要がない場合の表記です。 • Microsoft ® Windows Server ® 2016 • Microsoft ® Windows Server ® 2019 • Microsoft ® Windows Server ® 2022
Windows Server 2016	Microsoft ® Windows Server ® 2016
Windows Server 2019	Microsoft ® Windows Server ® 2019
Windows Server 2022	Microsoft ® Windows Server ® 2022

■ 関連マニュアル

このマニュアルの関連マニュアルを次に示します。必要に応じてお読みください。

- Hitachi Ops Center Automator ユーザーズガイド, 4010-1J-618

- Hitachi Ops Center Automator Service Builder ユーザーズガイド, 4010-1J-621
- Hitachi Ops Center Automator メッセージ, 4010-1J-622
- Hitachi Ops Center インストールガイド, 4010-1J-601
- Hitachi Ops Center API Configuration Manager REST API リファレンスガイド, 4010-1J-605

■ このマニュアルで使用している記号

このマニュアルでは、次のような表記規則を使用しています。

規則	説明
太字	リスト項目の中で強調する語を示します。
[]	画面のタイトル、メニュー、メニューオプション、ボタン、フィールド、ラベルなど、画面内のテキストを示します。 例：[OK] をクリックします。
＜ ＞ （山括弧）	可変値を示します。
斜体	
`Monospace`	画面に表示されるテキスト、またはユーザーが入力するテキストを示します。例：`pairdisplay -g oradb`
[ ]（角括弧）	オプションの値を示します。例：[a | b]は、a または b を選択できる、あるいはどちらも省略できることを示します。
{ }（波括弧）	必須の値または予期される値を示します。例：{ a | b }は、a または b のどちらかを選択する必要があることを示します。
|（縦線）	2 つ以上のオプションまたは引数から選択できることを示します。例： [a | b]は、a または b を選択できる、あるいはどちらも省略できることを示します。 { a | b }は、a または b のいずれかを選択する必要があることを示します。

■ KB（キロバイト）などの単位表記について

1KB（キロバイト）、1MB（メガバイト）、1GB（ギガバイト）、1TB（テラバイト）は、それぞれ 1KiB（キビバイト）、1MiB（メビバイト）、1GiB（ギビバイト）、1TiB（テビバイト）と読み替えてください。

1KiB、1MiB、1GiB、1TiB は、それぞれ 1,024 バイト、1,024KiB、1,024MiB、1,024GiB です。

■ このマニュアルでの表記

このマニュアルでは、製品の名称を省略して表記しています。このマニュアルでの表記と、製品の正式名称または意味を次に示します。

表記	製品名
Common Services	Hitachi Ops Center Common Services
Configuration Manager	Hitachi Ops Center API Configuration Manager
Fabric OS（FOS）	Fabric OS®
HUS VM	Hitachi Unified Storage VM
Linux	Red Hat Enterprise Linux®および Oracle Linux®の総称です。
Ops Center Automator（Automator）	Hitachi Ops Center Automator
Ops Center Portal	Hitachi Ops Center Portal
Ops Center Viewpoint	Hitachi Ops Center Viewpoint
Oracle Linux	Oracle Linux®
Red Hat Enterprise Linux（RHEL）	Red Hat Enterprise Linux®
Service Builder	Ops Center Automator Service Builder
SSL	Secure Sockets Layer
TLS	Transport Layer Security
Virtual Storage Platform	Hitachi Virtual Storage Platform
	Hitachi Virtual Storage Platform VP9500
VMware	VMware®
VMware ESX	VMware vSphere® ESXi™
VMware vCenter Server	VMware vCenter Server™
VMware vSphere	VMware vSphere®
VSP One Block	VSP One B20
VSP One B20	Hitachi Virtual Storage Platform One Block 23
	Hitachi Virtual Storage Platform One Block 26
	Hitachi Virtual Storage Platform One Block 28
VSP E シリーズ	Hitachi Virtual Storage Platform E390
	Hitachi Virtual Storage Platform E590
	Hitachi Virtual Storage Platform E790
	Hitachi Virtual Storage Platform E990
	Hitachi Virtual Storage Platform E1090
	Hitachi Virtual Storage Platform E390H

表記	製品名
VSP E シリーズ	Hitachi Virtual Storage Platform E590H
	Hitachi Virtual Storage Platform E790H
	Hitachi Virtual Storage Platform E1090H
VSP Fx00 モデル	Hitachi Virtual Storage Platform F350
	Hitachi Virtual Storage Platform F370
	Hitachi Virtual Storage Platform F400
	Hitachi Virtual Storage Platform F600
	Hitachi Virtual Storage Platform F700
	Hitachi Virtual Storage Platform F800
	Hitachi Virtual Storage Platform F900
VSP F1500	Hitachi Virtual Storage Platform F1500
VSP F シリーズ	VSP Fx00 モデル
	VSP F1500
VSP Gx00 モデル	Hitachi Virtual Storage Platform G100
	Hitachi Virtual Storage Platform G130
	Hitachi Virtual Storage Platform G150
	Hitachi Virtual Storage Platform G200
	Hitachi Virtual Storage Platform G350
	Hitachi Virtual Storage Platform G370
	Hitachi Virtual Storage Platform G400
	Hitachi Virtual Storage Platform G600
	Hitachi Virtual Storage Platform G700
	Hitachi Virtual Storage Platform G800
	Hitachi Virtual Storage Platform G900
VSP G1000	Hitachi Virtual Storage Platform G1000
VSP G1500	Hitachi Virtual Storage Platform G1500
VSP G シリーズ	VSP Gx00 モデル
	VSP G1000
	VSP G1500

表記	製品名
VSP 5000 シリーズ	Hitachi Virtual Storage Platform 5100
	Hitachi Virtual Storage Platform 5200
	Hitachi Virtual Storage Platform 5500
	Hitachi Virtual Storage Platform 5600
	Hitachi Virtual Storage Platform 5100H
	Hitachi Virtual Storage Platform 5200H
	Hitachi Virtual Storage Platform 5500H
	Hitachi Virtual Storage Platform 5600H
VSP ファミリー	VSP E シリーズ
	VSP F シリーズ
	VSP G シリーズ
	VSP 5000 シリーズ
	Virtual Storage Platform

目次

1 概要

ここでは、Ops Center Automator の概要について説明します。

1.1 製品の概要

Ops Center Automator は、ストレージおよびデータセンター管理者向けの、エンドツーエンドのストレージプロビジョニングプロセスを自動化および単純化するためのツールとなるソフトウェアソリューションです。この製品の基本要素は、サービステンプレートと呼ばれる、事前にパッケージ化されたオートメーションテンプレートです。これらの事前構成テンプレートは特定の環境とプロセスに合わせてカスタマイズされ、リソースプロビジョニングなどの複雑なタスクを自動化するサービスを作成します。構成が済むと、Ops Center Automator は既存のアプリケーションと連携して、既存のインフラストラクチャーサービスを利用することによって、共通のインフラストラクチャー管理タスクを自動化します。

Ops Center Automator は、次のような機能を備えています。

- オートメーションサービスの作成を容易にする、事前構成されたサービステンプレート
- さまざまなストレージクラスのボリュームのインテリジェントなプロビジョニングのためのオートメーションサービス
- 定義されたサービスへのロールベースのアクセス
- インフラストラクチャーグループから最も性能の高いプールを選択し、プール情報を各タスクに提供してボリューム使用量の詳細を指定する、性能ベースのプール選択
- すべてのオートメーションサービスに割り当てて共有できる共通のサービス管理属性

1.2 関連する Hitachi Ops Center 製品について

Hitachi Ops Center 製品は、下記製品で構成されます。

- Hitachi Ops Center Automator
- Hitachi Ops Center Viewpoint

Hitachi Ops Center 製品は以下のコンポーネントを内包しています。

- Hitachi Ops Center Common Services
- Hitachi Ops Center API Configuration Manager

Hitachi Ops Center 製品は共通の設定でユーザーとセキュリティーを管理できます。

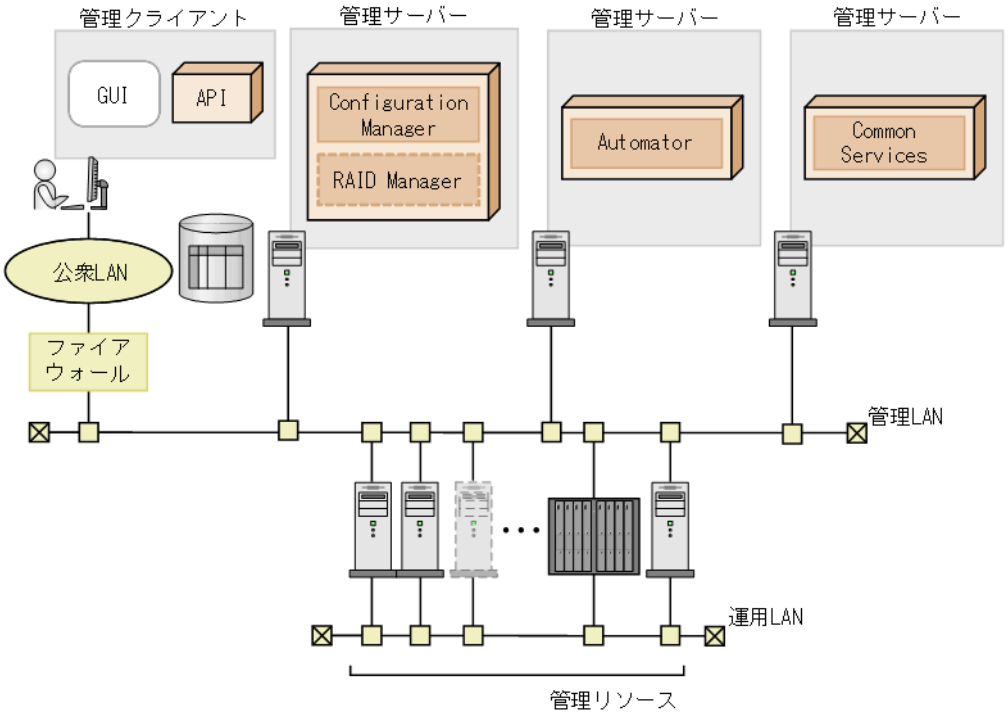
1.3 Ops Center Automator システム構成

Ops Center Automator は、Common Services および Configuration Manager を使用します。

Common Services は、ユーザー情報を一元管理して Ops Center Automator へリンク＆ラウンチするための Ops Center Portal を提供します。Configuration Manager は、ストレージシステムの情報取得や構成変更を行うための、REST の原則に従った Web API を提供します。

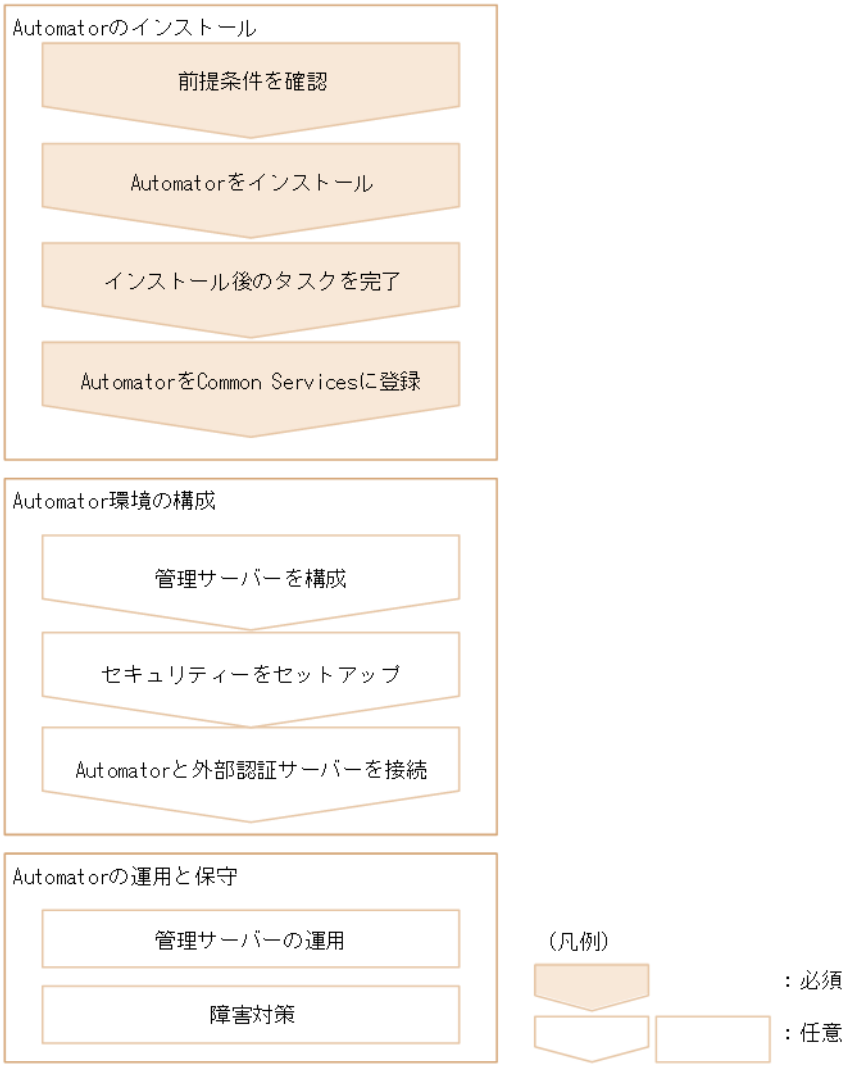
Ops Center Automator、Configuration Manager および Common Services は同じ管理サーバーにインストールするか、または、別の管理サーバーにインストールすることもできます。

Ops Center Automator システム構成を次の図に示します。



1.4 Ops Center Automator のインストールと構成のワークフロー

次の図は、Ops Center Automator のインストールと構成を含む、ワークフローの概要を示しています。



このマニュアルには、システムのインストール、セットアップ、管理、および保守に関する情報が含まれています。管理 GUI を使用したサービスの作成、管理、および自動化の詳細については、『Hitachi Ops Center Automator ユーザーズガイド』を参照してください。

1.5 Ops Center Automator での認証方法

Ops Center Automator を運用するために、次の認証方法を使用できます。

- 外部認証
- ローカルユーザー認証

これらの認証方法は Common Services で管理され、Ops Center 製品間でのシングルサインオンを可能にします。

メモ

Common Services では、外部の認証サーバーと連携することで、ユーザー認証を ID プロバイダーで一元的に行うこともできます。

2 Ops Center Automator をインストールまたはアップグレードする

ここでは、クラスターおよび非クラスター環境での、Ops Center Automator のインストールまたはアップグレード方法について説明します。

2.1　インストールの前提条件

Ops Center Automator をインストールする前に、以下のタスクを完了してください。

- 環境と管理サーバーがすべてのハードウェアおよびソフトウェア要件を満たしていることを確認します。システム要件の詳細については、Ops Center Automator のリリースノートを参照してください。
- Ops Center Automator によって使用されるポートが使用可能であることを確認します。管理サーバーのポートが他の製品によって使用されておらず、競合していないことを確認します。ポートが別の製品によって使用されていた場合、どちらの製品も正しく動作しないことがあります。
- 関連マシンの IP アドレスとホスト名の名前を解決します。
- サーバー上のセキュリティー監視、ウイルス検出、プロセス監視ソフトウェアを無効にします。
- Ops Center Automator と、共通コンポーネントを使用するほかの製品（バージョン 8.8.3 以降の Hitachi Command Suite 製品など）を同一の管理サーバーにインストールする場合は、システムがすべての製品のインストール要件を満たしていることを確認します。
  Ops Center Automator と、バージョン 8.8.3 より前の Hitachi Command Suite 製品は、同一の管理サーバーにインストールできません。
- サーバー上で、共通コンポーネントを使用するほかの製品を実行している場合は、それらの製品のサービスを停止します。
- サーバーのシステム時刻が正しいことを確認します。Ops Center 製品が別のサーバーにインストールされている場合は、Ops Center Automator サーバーと当該サーバーの時刻を同期させます。
- 管理サーバーのホスト名が 128 文字以下であることを確認します。
- このマニュアルに含まれているインストールおよび構成タスクを完了するために、Administrator 権限が取得されていることを確認します。
- Windows のサービスまたは開いているコマンドプロンプトを閉じます。

関連項目

- 2.1.1　サーバー時刻を変更する
- 2.1.2　名前解決設定を変更する
- 付録 A.2　ポート設定

2.1.1　サーバー時刻を変更する

Ops Center Automator のタスクおよびアラート発生時刻は、管理サーバーの時刻設定に基づきます。したがって、サーバーの OS の時刻設定が正確かどうかを確認することが重要です。必要に応じて、Ops Center Automator をインストールする前に時刻を変更してください。共通コンポーネントおよび共通コンポーネントを使用する製品（Ops Center Automator を含む）のサービスが実行しているときに管理サーバーの時刻を変更した場合、Ops Center Automator が正しく動作しないことがあります。

重要

Ops Center Automator の管理サーバーの OS の時刻設定が、Ops Center 製品の管理サーバーと同期している必要があります。

メモ

Common Services と Ops Center Automator が異なる管理サーバー上で稼働している場合、Common Services がインストールされているサーバーと、Ops Center Automator がインストールされているサーバーの時刻に 3 分を超えるずれがあると、Ops Center Portal から Ops Center Automator を起動できません。NTP を使用して両方のサーバーの時刻を同期させてください。

NTP など、サーバーの時刻を自動的に調整するサービスを使用する場合は、次のようにサービスを構成する必要があります。

- サービスにより時刻の不一致が検出されたときに調整されるよう、設定を構成します。
- 特定の時刻差を超えない範囲内で時刻設定の調整が行われるようにします。最大範囲値に基づいて、時刻差が固定範囲を超えないように頻度を設定してください。

特定の時刻差の範囲内で時刻を調整できるサービスの例としては、Windows Time サービスがあります。

メモ

米国またはカナダのタイムゾーンで Ops Center Automator を実行するときには、新しい夏時間（DST）ルールをサポートするように管理サーバーの OS を構成する必要があります。サーバーがサポートを提供しないかぎり、Ops Center Automator は新しい DST ルールをサポートできません。

サーバーの時刻を自動的に調整する機能を使用できない場合や、システム時刻を手動で変更する場合は、以下のステップを実行します。

1. 共通コンポーネントと、共通コンポーネントを使用するすべての製品のサービスを停止します。停止するサービスの例を次に示します。
   - 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. 管理サーバーの現在時刻を記録してから、時刻をリセットします。
3. サービスを再起動する時間を決めます。
   - サーバーの時刻を戻した場合（サーバーの時刻が進んでいた場合）は、サーバーのクロックが記録した時刻（変更を加えたときのサーバーの時刻）を示すまで待ってから、サーバーを再起動します。
   - サーバーの時刻を進めた場合は、すぐにサーバーを再起動します。

管理サーバーが正しい時刻を反映していることを確認します。

2.1.2 名前解決設定を変更する

Ops Center Automator にアクセスするためにブラウザーを実行するマシンで、Ops Center Automator サーバーの名前を解決する必要があります。

user_httpsd.conf ファイルの最初の行でServerName プロパティとして設定されている管理サーバーのホスト名からシステムが IP アドレスを解決できるように、構成設定を更新します。次のコマンドを実行して、ホスト名が IP アドレスに解決されることを確認します。

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

2.1.3 ポートの衝突を回避する

Ops Center Automator を新しくインストールする前に、管理サーバー上で Ops Center Automator が使用するポートが他の製品によって使用されていないことを確認してください。ポートが別の製品によって使用されていた場合、どちらの製品も正しく動作しないことがあります。

必要なポートが使用中でないことを確認するには、netstat またはss コマンドを使用します。

ポート番号 22170～22173 が他の製品によって使用されていないことを確認する必要があります。使用されている場合、新規インストールまたはアップグレードインストールが失敗します。

関連項目

- 3.1.1 管理サーバーと管理クライアントとの通信に使用されるポート番号を変更する
- 付録 A.2 ポート設定

2.2　Ops Center Automator をインストールまたはアップグレードする

単体インストールメディアから製品インストーラーを使用して Ops Center Automator をインストールまたはアップグレードする方法を説明します。

ソフトウェアをアップグレードする場合は、backupsystem コマンドを使用して、既存のシステム構成とデータを必ずバックアップしてください。このコマンドの詳細は、「7.2.1　backupsystem コマンド」を参照してください。

前提条件

「2.1　インストールの前提条件」を満たしていることを確認します。

操作手順

1. サーバーが共通コンポーネントを使用する製品を実行している場合は、以下のサービスを停止します。
   - 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. インストールメディアを DVD ドライブに挿入します。
3. 以下のコマンドを実行して、インストールウィザードを起動します。

   ```
   <DVDドライブ>:¥HAD_SERVER¥setup.exe
   ```

4. 画面の指示に従って、必要な情報を指定します。

   次のメッセージが表示された場合、Ops Center Automator のリリースノートを参照してください。

   ```
   このサーバには，既にDevice Manager，Tiered Storage Manager，Tuning Manager，Replication Manager，Compute Systems Manager，Global Link Manager 8.8.3より前，またはHitachi Automation Director 10.6.1以前がインストールされています。ソフトウェア添付資料を参照して，必ず関係製品のバージョンアップをしてください。一旦，インストールを中止しますか?
   ```

ほとんどの場合、デフォルトのインストール選択項目を受け入れてください。

［インストール完了］画面が開きます。

5. [完了] をクリックします。

操作結果

これで、Ops Center Automator がインストールされます。

> **メモ**
>
> アップグレードする場合は、以前の設定が保存されているため、「2.6 インストール後のタスク」および「2.7 Common Services にシングルサインオンを構成する」を省略できます。

関連項目

- 2.5　インストール後のタスク

2.3 クラスター環境で Ops Center Automator をインストールまたはアップグレードする

クラスター環境に Ops Center Automator をインストールまたはアップグレードします。

> **メモ**
>
> アップグレードする場合は、以前の設定が保存されているため、「2.6 インストール後のタスク」および「2.7 Common Services にシングルサインオンを構成する」を省略できます。

2.3.1 クラスター環境での Ops Center Automator の使用について

Ops Center Automator を使用するときには、Microsoft Windows Server Failover Clustering を使用してフェイルオーバー管理サーバーをセットアップすることで信頼性を高めることができます。

> **メモ**
>
> Ops Center Automator は、マルチサブネット構成のクラスターへのインストールはサポートしていません。

クラスター環境で Ops Center Automator を使用するときには、次のように、1 台の Ops Center Automator サーバーをアクティブノードに、もう 1 台をスタンバイノードに指定します。

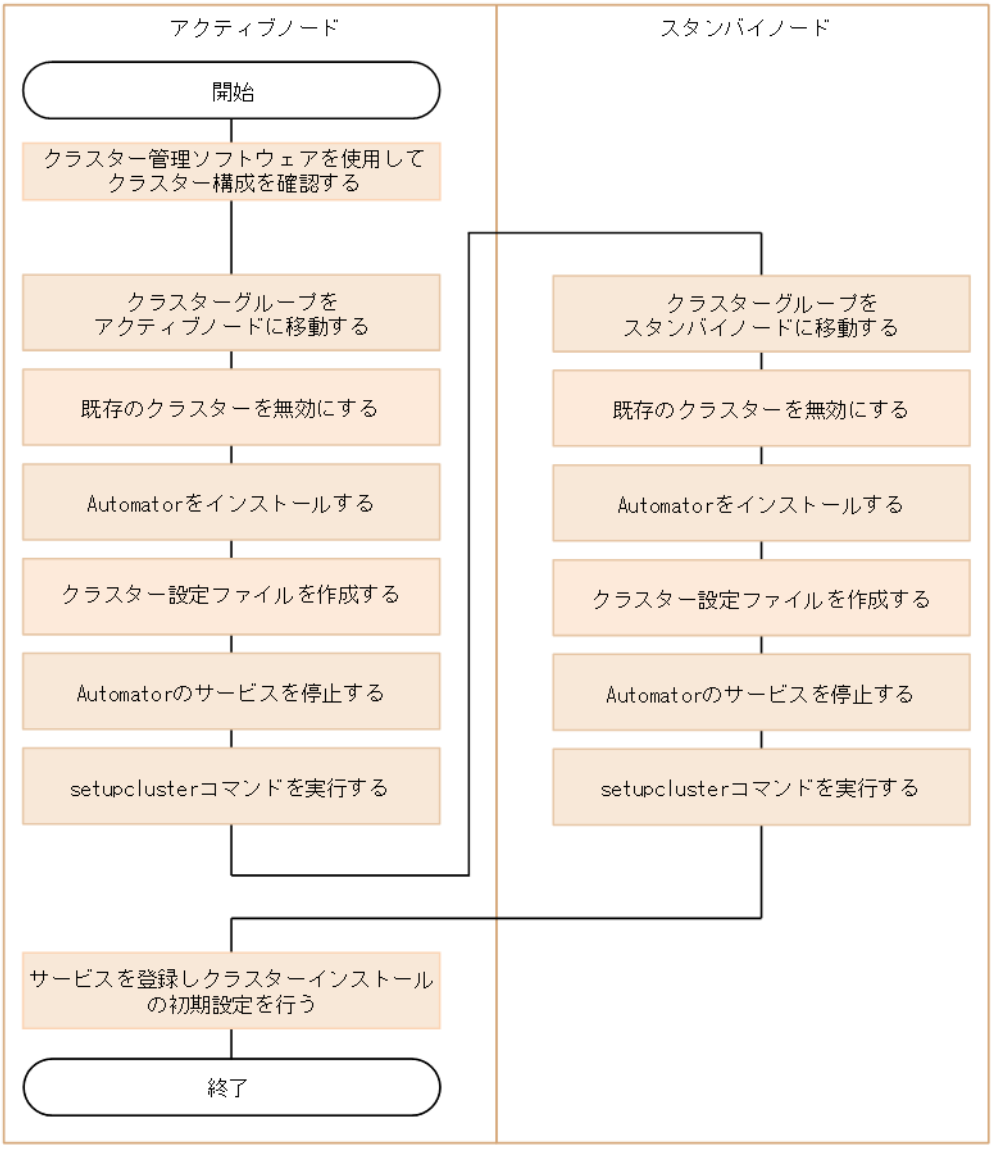
- アクティブノード
  アクティブノードは、クラスターを使用するシステムでサービスを実行しているホストです。
  障害が発生した場合、クラスターサービスがフェイルオーバーを実行し、スタンバイノードがシステムリソースの操作を引き継ぐため、サービスは中断されません。
- スタンバイノード
  スタンバイノードは、障害発生時にアクティブノードからシステムリソースの操作を引き継ぐホストです。

> **メモ**
>
> アクティブノードがスタンバイノードにフェイルオーバーした場合、実行中のタスクは失敗するので、スタンバイノード上でタスクを再び実行する必要があります。

2.3.2　クラスターインストールワークフロー

Ops Center Automator をクラスター構成でインストールするときには、一連のステップに従って、アクティブノードとスタンバイノードの両方を準備する必要があります。

以下に、クラスター環境をセットアップするための一般的なワークフローを示します。



初めて Ops Center Automator をクラスター環境にインストールするときには、クラスター内のすべてのノードが同じディスク構成を持つことと、共通コンポーネントを使用するすべての製品が各ノードの同じ場所（ドライブ名、パスなどを含む）にインストールされていることを確認してください。

ソフトウェアをアップグレードする場合は、backupsystem コマンドを使用して、既存のシステム構成とデータを必ずバックアップしてください。このコマンドの詳細は、「7.2.1　backupsystem コマンド」を参照してください。

メモ

既にクラスター構成でインストールされている Ops Center Automator のアップグレードを行うときには、アップグレードインストールを実行する前に、リソーススクリプトを無効にする必要があります。

関連項目

- 2.3.4　アクティブノードで Ops Center Automator クラスター化をセットアップする
- 2.3.5　スタンバイノードで Ops Center Automator クラスター化をセットアップする

2.3.3　クラスター管理ソフトウェアを使用してクラスター構成を確認する

クラスター環境で Ops Center Automator をセットアップするときには、クラスター管理ソフトウェアを使用して現在の環境設定を確認し、追加の設定を構成する必要があります。

クラスター環境で Ops Center Automator をセットアップする前に、クラスター環境ソフトウェアを使用して、以下の項目を確認します。

- 共通コンポーネントを使用するほかの製品のサービスが登録されているグループが存在するかどうかを確認します。
  共通コンポーネントを使用する製品のサービスが登録されているグループが既に存在する場合は、そのグループを使用します。グループが、共通コンポーネントを使用する製品に関するリソースのみで構成されていることを確認します。
  共通コンポーネントを使用する製品のサービスが登録されているグループが存在しない場合は、クラスター管理ソフトウェアを使用して、Ops Center Automator のサービスを登録するグループを作成します。

  メモ

  グループ名に次の文字を使用することはできません：!" % &) * ^ | ; = , < >
- サービスを登録するグループに、アクティブノードとスタンバイノード間で継承できる共有ディスクとクライアントアクセスポイントが含まれていることを確認します。クライアントアクセスポイントは、クラスター管理 IP アドレスと論理ホスト名です。
- クラスター管理ソフトウェアを使用してリソースの割り当て、削除、および監視が問題なくできることを確認します。

クラスター環境で使用されるサービスは、クラスター管理ソフトウェアでグループとして登録することによってフェイルオーバーできます。これらのグループは、クラスター管理ソフトウェアと OS のバージョンによって、「リソースグループ」や「役割」など異なる名前で呼ばれることがあります。

2.3.4 アクティブノードで Ops Center Automator クラスター化をセットアップする

クラスター構成のアクティブノード上の管理サーバーで、Ops Center Automator のインストールを完了することができます。

前提条件

「2.1 インストールの前提条件」を満たしていることを確認します。

操作手順

1. クラスター管理 IP アドレスと共有ディスクをオンラインにします。クラスターインストールのクラスターグループがアクティブノードに移動されることを確認します。

2. 共通コンポーネントを使用するほかの製品でクラスター環境が構築されている場合は、次のコマンドを使用して、共通コンポーネントを使用する製品のサービスが登録されるクラスターグループをオフラインにして、フェイルオーバーを無効にします。

   ```
   <共通コンポーネントのインストールフォルダー>¥ClusterSetup¥hcmds64clustersrvstate /soff
   /r <グループ名>
   ```

   r オプションには、共通コンポーネントを使用する製品のサービスが登録されるグループの名前を指定します。グループ名にスペースが含まれる場合は、グループ名を引用符（"）で囲む必要があります。例えば、グループ名が Automator cluster の場合は、"Automator cluster"と指定します。

3. アクティブノード上で Ops Center Automator をインストールします。

   インストールの前に、次の要件を確認してください。

   - 共通コンポーネントを使用するほかの製品がすでに存在し、クラスター環境でアクティブな場合、管理サーバーの［IP アドレスまたはホスト名］に論理ホスト名（クラスター管理 IP アドレスに割り当てられた仮想ホスト名）を指定する必要があります。
   - 共通コンポーネントを使用するほかの製品がクラスター環境に存在しない場合、管理サーバーの［IP アドレスまたはホスト名］にアクティブノードの IP アドレスまたはホスト名を指定する必要があります。

   インストール時に次のメッセージが表示された場合、Ops Center Automator のリリースノートを参照してください。

   ```
   このサーバには，既にDevice Manager，Tiered Storage Manager，Tuning Manager，Replication M
   anager，Compute Systems Manager，Global Link Manager 8.8.3より前，またはHitachi Automatio
   n Director 10.6.1以前がインストールされています。ソフトウェア添付資料を参照して，必ず関係
   製品のバージョンアップをしてください。一旦，インストールを中止しますか?
   ```

4. 使用する製品のライセンスを登録します。

5. クラスター内で共通コンポーネントを使用する製品を既に構成している場合、次のステップへスキップします。Ops Center Automator が、共通コンポーネントを使用する製品のうち初めてクラスター内に構築される製品である場合は、空白のテキストファイルに以下の情報を追加します。

```
mode=online
virtualhost=<論理ホスト名>
onlinehost=<アクティブノードのホスト名>
standbyhost=<スタンバイノードのホスト名>
```

> **メモ**
>
> アクティブノードで、mode としてonline を指定する必要があります。

ファイルをcluster.conf という名前で<*共通コンポーネントのインストールフォルダー*>¥conf に保存します。

6. 次のコマンドを使用して、Ops Center Automator のサービスを確実に停止します。

```
<共通コンポーネントのインストールフォルダー>¥bin¥hcmds64srv /stop /server AutomationWeb
Service
```

7. setupcluster /exportpath コマンドを実行します。exportpath には、共有ディスク上のフォルダーを絶対または相対パスで指定します。exportpath には、共有ディスク直下（ルートフォルダー）は指定できません。

関連項目

- 2.3.5　スタンバイノードで Ops Center Automator クラスター化をセットアップする

2.3.5　スタンバイノードで Ops Center Automator クラスター化をセットアップする

アクティブノードでクラスター化インストールを設定した後、クラスター構成のスタンバイノード上の管理サーバーで Ops Center Automator のインストールを完了できます。

前提条件

「2.1　インストールの前提条件」を満たしていることを確認します。

操作手順

1. クラスター管理ソフトウェアで、Ops Center Automator のリソースを含んでいるグループをスタンバイノードに移動します。グループを右クリックして［移動］を選択してから、［ノードを選択］または［このサービスまたはアプリケーションを別のノードに移動］を選択します。

2. 共通コンポーネントを使用するほかの製品でクラスター環境が構築されている場合は、次のコマンドを使用して、共通コンポーネントを使用する製品のサービスが登録されるクラスターグループをオフラインにして、フェイルオーバーを無効にします。

```
<共通コンポーネントのインストールフォルダー>¥ClusterSetup¥hcmds64clustersrvstate /soff
/r <グループ名>
```

r オプションには、共通コンポーネントを使用する製品のサービスが登録されるグループの名前を指定します。グループ名にスペースが含まれる場合は、グループ名を引用符（"）で囲む必要があります。例えば、グループ名が Automator cluster の場合は、"Automator cluster"と指定します。

3. スタンバイノード上で Ops Center Automator をインストールします。

インストールの前に、以下の要件を確認してください。

- アクティブノードと同じ場所に Ops Center Automator をインストールする必要があります。
- 共通コンポーネントを使用するほかの製品がすでに存在し、クラスター環境でアクティブな場合、管理サーバーの［IP アドレスまたはホスト名］に論理ホスト名（クラスター管理 IP アドレスに割り当てられた仮想ホスト名）を指定する必要があります。
- 共通コンポーネントを使用するほかの製品がクラスター環境に存在しない場合、管理サーバーの［IP アドレスまたはホスト名］にスタンバイノードの IP アドレスまたはホスト名を指定する必要があります。

インストール時に次のメッセージが表示された場合、Ops Center Automator のリリースノートを参照してください。

```
このサーバには，既にDevice Manager，Tiered Storage Manager，Tuning Manager，Replication M
anager，Compute Systems Manager，Global Link Manager 8.8.3より前，またはHitachi Automatio
n Director 10.6.1以前がインストールされています。ソフトウェア添付資料を参照して，必ず関係
製品のバージョンアップをしてください。一旦，インストールを中止しますか?
```

4. 使用する製品のライセンスを登録します。

5. クラスター内で共通コンポーネントを使用する製品を既に構成している場合、次のステップへスキップします。Ops Center Automator が、共通コンポーネントを使用する製品のうち初めてクラスター内に構築される製品である場合は、空白のテキストファイルに以下の情報を追加します。

```
mode=standby
virtualhost=<論理ホスト名>
onlinehost=<アクティブノードのホスト名>
standbyhost=<スタンバイノードのホスト名>
```

メモ

スタンバイノードで、mode としてstandby を指定する必要があります。

ファイルをcluster.conf という名前で*<共通コンポーネントのインストールフォルダー>*¥conf に保存します。

6. 次のコマンドを使用して、Ops Center Automator のサービスを確実に停止します。

```
<共通コンポーネントのインストールフォルダー>¥bin¥hcmds64srv /stop /server AutomationWeb
Service
```

7. setupcluster /exportpath コマンドを実行します。exportpath には、「2.3.4　アクティブノードで Ops Center Automator クラスター化をセットアップする」の setupcluster コマンド実行で指定したパスと同一のパスを指定してください。

2.3.6　サービスを登録しクラスターインストールの初期設定を行う

Ops Center Automator をクラスター構成のアクティブノードおよびスタンバイノードにインストールした後、以下のステップの説明に従ってサービスとスクリプトを登録し、クラスター化をオンラインにできます。

操作手順

1. クラスター管理ソフトウェアで、Ops Center Automator のリソースを含んでいるグループをアクティブノードに移動します。グループを右クリックして［移動］を選択してから、［ノードを選択］または［このサービスまたはアプリケーションを別のノードに移動］を選択します。

2. 次のコマンドを使用して、クラスター管理ソフトウェアグループで Ops Center Automator サービスを登録します。

```
<共通コンポーネントのインストールフォルダー>¥ClusterSetup¥hcmds64clustersrvupdate /sreg
 /r <グループ名> /sd <共有ディスクのドライブレター名> /ap <クライアントアクセスポイ
ント用リソース名>
```

   - /r
     共通コンポーネントを使用する製品（Ops Center Automator を含む）のサービスが登録されるグループの名前を指定します。グループ名にスペースが含まれる場合は、グループ名を引用符（"）で囲む必要があります。例えば、グループ名が Automator cluster の場合は、"Automator cluster" と指定します。
   - /sd
     クラスター管理ソフトウェアに登録される共有ディスクのドライブ名を指定します。このオプションに対して複数のドライブ名を指定することはできません。共通コンポーネントを使用する製品（Ops Center Automator を含む）のデータベースが複数の共有ディスクに分割されている場合は、各共有ディスクについてhcmds64clustersrvupdate コマンドを実行します。
   - /ap
     クラスター管理ソフトウェアに登録されるクライアントアクセスポイント用リソースの名前を指定します。

3. アクティブノードで、次のコマンドを使用して、共通コンポーネントを使用する製品（Ops Center Automator を含む）のサービスが登録されるグループをオンラインにして、フェイルオーバーを有効にします。

```
＜共通コンポーネントのインストールフォルダー＞¥ClusterSetup¥hcmds64clustersrvstate /son /r ＜グループ名＞
```

r オプションには、共通コンポーネントを使用する製品（Ops Center Automator を含む）のサービスが登録されるグループの名前を指定します。グループ名にスペースが含まれる場合は、グループ名を引用符（"）で囲む必要があります。例えば、グループ名が Automator cluster の場合は、"Automator cluster"と指定します。

4. クラスターソフトウェアで、クラスターグループのステータスを［online］に変更します。

2.4 ウイルス検出プログラムおよびプロセス監視ソフトウェアを使用する場合に必要な設定

ウイルス検出プログラムで Ops Center Automator が使用するファイルにアクセスすると、I/O 遅延やファイル排他などによって障害が発生することがあります。また、プロセス監視ソフトウェアが Ops Center Automator プロセスを強制終了した場合、Ops Center Automator は正常に動作しません。これらを防止するため、Ops Center Automator のインストール時、および運用中は、ウイルス検出プログラムのスキャン対象およびプロセス監視ソフトウェアの監視対象から、次のディレクトリー配下を除外してください。

メモ

以下のフォルダーはデフォルトのパスであり、インストール時に変更できます。

インストール時の除外対象フォルダー

インストール媒体を格納したフォルダー

system-drive¥Program Files¥hitachi¥Automation

system-drive¥Program Files¥hitachi¥database

system-drive¥Program Files¥hitachi¥Base64

運用中の除外対象フォルダー

system-drive¥Program Files¥hitachi¥Automation

system-drive¥Program Files¥hitachi¥database

system-drive¥Program Files¥hitachi¥Base64¥HDB

2.5　インストール後のタスク

Ops Center Automator のインストール後は、以下のインストール後のタスクを完了してください。

1. 登録済み URL を変更します。詳細は、「2.5.1　登録済み URL を変更する」を参照してください。
2. Ops Center Automator の管理サーバーへのアクセスを確認します。
3. setupcommonservice コマンドを実行して、Common Services をセットアップします。このタスクは必ず実施してください。
   setupcommonservice コマンドの詳細は、「7.2.13　setupcommonservice コマンド」を参照してください。

   メモ

   クラスター構成では、アクティブノードでのみsetupcommonservice を実行できます。
4. ライセンスを登録します。

2.5.1　登録済み URL を変更する

Ops Center Automator のインストール後に、登録済み URL を変更します。

操作手順

1. 次のコマンドを使用して、登録済み URL を確認します。

   ```
   <共通コンポーネントのインストールフォルダー>¥bin¥hcmds64chgurl /list
   ```

2. URL 内のホスト名を確認します。非クラスター環境では、ホスト名は物理ホスト名でなければなりません。クラスター環境では、ホスト名は論理ホスト名でなければなりません。
3. 次のコマンドを使用して、Ops Center Automator の登録済み URL を変更します。

   ```
   <共通コンポーネントのインストールフォルダー>¥bin¥hcmds64chgurl /change https://<Ops Center AutomatorのIPアドレスまたはホスト名>:22016 /type Automation
   ```

2.5.2　インストールを確認する

インストールが完了したら、インストールが成功したことを Web ブラウザーから確認してください。

操作手順

1. Ops Center Automator によってサポートされている Web ブラウザーを開きます。

2. アドレスバーに、Ops Center Automator の URL を次の形式で指定します。

   https://<*Ops Center AutomatorのIPアドレスまたはホスト名*>:22016/Automation/

操作結果

管理サーバーにアクセスできることを確認するログイン画面が開きます。

2.5.3 ライセンスを登録する

最初にログインするときには、有効なライセンスキーを指定する必要があります。

> **メモ**
>
> Ops Center Automator のライセンスについては、サポートサービスにお問い合わせください。

操作手順

1. ログイン画面の［ライセンス］をクリックします。
2. ライセンスキーを入力するか、［ファイルを選択］をクリックして、ライセンスファイルを参照します。
3. ［保存］をクリックします。

2.5.4 Ops Center Automator および共通コンポーネントを使用する製品のサービスを停止および起動する

Ops Center Automator および共通コンポーネントを使用する製品はコマンドプロンプトからサービスを実行できます。

(1) コマンドプロンプトからすべてのサービスを停止および起動する

次の手順により、Ops Center Automator および共通コンポーネントを使用するすべての製品のサービスを停止および起動します。

操作手順

1. コマンドプロンプトで、<*共通コンポーネントのインストールフォルダー*>¥bin に移動します。
2. サービスを停止するには、次のコマンドを入力します。

   ```
   hcmds64srv /stop
   ```

   サービスを起動するには、次のコマンドを入力します。

```
hcmds64srv /start
```

(2) コマンドプロンプトから Ops Center Automator サービスのみ停止および起動する

操作手順

1. *<共通コンポーネントのインストールフォルダー>*¥bin に移動します。
2. サービスを停止または起動します。
   - サービスを停止するには、次のコマンドを入力します。
     ```
     hcmds64srv /stop /server AutomationWebService
     ```
   - サービスを起動するには、次のコマンドを入力します。
     ```
     hcmds64srv /start /server AutomationWebService
     ```

2.6　Common Services にシングルサインオンを構成する

Ops Center Portal のシングルサインオン機能を利用するには、Ops Center Automator を Common Services に登録する必要があります。

2.6.1　Ops Center Automator を Common Services に登録する

Ops Center Automator サーバー上でコマンドを実行して、Ops Center Automator を Common Services に登録する必要があります。

操作手順

1. auto オプションを指定してsetupcommonservice コマンドを実行し、Ops Center Automator を Common Services に登録します。

   setupcommonservice コマンドの詳細については、「7.2.13　setupcommonservice コマンド」を参照してください。

3 Ops Center Automator を構成する

ここでは、Ops Center Automator を構成する方法について説明します。

3.1　管理サーバーのシステム設定を変更する

ここでは、Ops Center Automator の管理サーバーのシステム設定の変更に関して説明します。

3.1.1　管理サーバーと管理クライアントとの通信に使用されるポート番号を変更する

管理サーバーと管理クライアント（Web ブラウザー）間の通信に使用されるポート番号を変更するには、定義ファイルの編集と、ファイアウォールの例外登録が必要になります。クラスターシステムの場合、アクティブノードとスタンバイノードで同じ手順を実施してください。

> **メモ**
>
> Ops Center Automator に使用される他のポートの情報については、ポート設定の参考トピックを参照してください。

操作手順

1. Ops Center Automator のサービスを停止します。
2. 定義ファイルのキーを編集してポート番号の設定を変更します。
   - HTTPS の場合、手順 3 に進みます。
   - HTTP の場合、次のように定義ファイルのキーを編集してポート番号の設定を変更します。

   a. user_httpsd.conf ファイルのListen キーの行を変更します。

   <共通コンポーネントのインストールフォルダー>¥uCPSB11¥httpsd¥conf¥user_httpsd.conf
   次の行で、22015 に替わる新しいポート番号を指定します。

   ```
   Listen [::]:22015
   Listen 22015
   #Listen 127.0.0.1:22015
   ```

   > **メモ**
   >
   > Ops Center Automator をクラスター構成で運用している場合は、アクティブノードとスタンバイノードそれぞれでuser_httpsd.conf ファイルを編集してください。

   b. command_user.properties ファイルのcommand.http.port の行を変更します。

   クラスターシステムの場合、この定義ファイルは別のフォルダーに含まれています。
   非クラスター環境の場合：
   <Ops Center Automatorのインストールフォルダー>¥conf
   クラスター環境の場合：

<共有フォルダー名>¥Automation¥conf

c. config_user.properties ファイルのserver.http.port の行を変更します。

クラスターシステムの場合、この定義ファイルは別のフォルダーに含まれています。

非クラスター環境の場合：

<Ops Center Automatorのインストールフォルダー>¥conf

クラスター環境の場合：

<共有フォルダー名>¥Automation¥conf

d. 手順 4 に進みます。

3. HTTPS の場合、次のように定義ファイルのキーを編集してポート番号の設定を変更します。

a. user_httpsd.conf ファイルを開きます。

<共通コンポーネントのインストールフォルダー>¥uCPSB11¥httpsd¥conf¥user_httpsd.conf

> **メモ**
>
> Ops Center Automator をクラスター構成で運用している場合は、アクティブノードとスタンバイノードそれぞれでuser_httpsd.conf ファイルを編集してください。

b. 次の行で 22016 に替わる新しいポート番号を指定して、Listen キーの行を変更します。

```
Listen [::]:22016
Listen 22016
<VirtualHost *:22016>
```

4. ファイアウォールの例外登録をします。

hcmds64fwcancel コマンドを実行してファイアウォールの例外登録をします。

5. Ops Center Automator のサービスを起動します。

6. hcmds64chgurl コマンドを実行して、Ops Center Automator の URL を更新します。

7. setupcommonservice コマンドを実行して、Common Services に変更を適用します。

関連項目

- 2.5.4　Ops Center Automator および共通コンポーネントを使用する製品のサービスを停止および起動する
- 3.1.2　ポート番号を変更した場合に共通コンポーネントのプロパティを更新する
- 7.2.13　setupcommonservice コマンド
- 付録 A.2　ポート設定

3.1.2 ポート番号を変更した場合に共通コンポーネントのプロパティを更新する

Ops Center Automator のポート番号を変更する場合は、共通コンポーネントのプロパティを更新する必要があります。プロパティの更新後には、Ops Center Automator および共通コンポーネントを使用するすべての製品のサービスを再起動してください。

メモ

Ops Center Automator をクラスター構成で運用している場合は、アクティブノードとスタンバイノードそれぞれでプロパティファイルを編集してください。

操作手順

1. 次の表に示されている共通コンポーネントのプロパティに指定されているポート番号を更新します。

ポート番号（デフォルト）	プロパティファイルのパス（*<共通コンポーネントのインストールフォルダー>*配下）	更新場所
22015/TCP	¥uCPSB11¥httpsd¥conf¥user_httpsd.conf	• Listen [::]: • Listen • #Listen 127.0.0.1:
22016/TCP	¥uCPSB11¥httpsd¥conf¥user_httpsd.conf	• Listen [::]: • Listen • VirtualHost *:
22031/TCP	¥uCPSB11¥httpsd¥conf¥user_hsso_httpsd.conf	Listen
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
	¥uCPSB11¥httpsd¥conf フォルダー配下の次のファイル • reverse_proxy.conf • reverse_proxy_before.conf • reverse_proxy_after.conf • hsso_reverse_proxy.conf プロパティファイルに対象のポート番号が指定されていない場合、更新は不要です。	• ProxyPass /HiCommand/ • ProxyPassReverse /HiCommand/ • ProxyPass /StgMgmt/ • ProxyPassReverse /StgMgmt/
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

ポート番号（デフォルト）	プロパティファイルのパス（*<共通コンポーネントのインストールフォルダー>*配下）	更新場所
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
	¥uCPSB11¥httpsd¥conf フォルダー配下の次のファイル • reverse_proxy.conf • reverse_proxy_before.conf • reverse_proxy_after.conf • hsso_reverse_proxy.conf プロパティファイルに対象のポート番号が指定されていない場合、更新は不要です。	• ProxyPass /Automation/ • ProxyPassReverse /Automation/
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

2. Ops Center Automator および共通コンポーネントを使用するすべての製品のサービスを再起動します。

関連項目

- 2.5.4　Ops Center Automator および共通コンポーネントを使用する製品のサービスを停止および起動する

3.1.3　管理サーバーのホスト名を変更する

管理サーバーのホスト名は、Ops Center Automator のインストール後に変更できます。

管理サーバーのホスト名は最大 128 文字で、大文字と小文字が区別されます。

操作手順

1. 新しい管理サーバーのホスト名をメモしておいてください。
   ホスト名を確認する必要がある場合は、ipconfig /all コマンドを使用してホスト名を表示します。
2. hcmds64srv /stop コマンドを実行して、Ops Center Automator および共通コンポーネントを使用するすべての製品のサービスを停止します。

3. user_httpsd.conf ファイルを編集します。

   user_httpsd.conf ファイルは、次の場所に格納されています。

   ＜共通コンポーネントのインストールフォルダー＞¥uCPSB11¥httpsd¥conf

   ServerName 行の値を新しいホスト名に変更します。

```
ServerName ＜管理サーバーのホスト名＞
```

   SSL 設定が有効の場合、サーバー証明書を再取得し、VirtualHost ディレクティブのServerName 行の値を新しいホスト名に変更します。

```
<VirtualHost *:22016>
ServerName ＜管理サーバーのホスト名＞
```

> **メモ**
>
> Ops Center Automator をクラスター構成で運用している場合は、アクティブノードとスタンバイノードそれぞれでuser_httpsd.conf ファイルを編集してください。

4. 共通コンポーネントを使用するほかの製品を実行している場合は、必要に応じてそれらの設定を変更します。

5. 管理サーバーのホスト名を変更します。変更後、サーバーを再起動します。

6. Ops Center Automator の URL にホスト名を使用している場合、hcmds64chgurl コマンドを実行して、URL を更新します。

7. Ops Center Automator の URL にホスト名を使用している場合、setupcommonservice コマンドを実行して、Common Services に変更を適用します。

3.1.4 管理サーバーの IP アドレスを変更する

管理サーバーの IP アドレスは、Ops Center Automator のインストール後に変更できます。

操作手順

1. [タスク] タブで、タスクの状態を確認します。

   稼働中のタスク（実行中、応答待ち中、長期実行中、異常検出、または停止中）がある場合、タスクを停止する、またはタスクの状態が実行完了（完了、失敗、またはキャンセル）に変わるまで待機します。

2. hcmds64srv /stop コマンドを実行して、Ops Center Automator および共通コンポーネントを使用するすべての製品のサービスを停止します。

3. 管理サーバーの IP アドレスを変更します。

4. hcmds64srv /start コマンドを実行して、Ops Center Automator および共通コンポーネントを使用するすべての製品のサービスを起動します。

5. Ops Center Automator の URL に IP アドレスを使用している場合、hcmds64chgurl コマンドを実行して、URL を更新します。

6. Ops Center Automator の URL に IP アドレスを使用している場合、setupcommonservice コマンドを実行して、Common Services に変更を適用します。

3.1.5 管理サーバーの URL を変更する

管理サーバーのホスト名または IP アドレス、Ops Center Automator のポート、または SSL 設定を変更した場合は、管理サーバーの URL を変更する必要があります。Ops Center Automator が、共通コンポーネントを使用するほかの製品と同じ管理サーバーで実行している場合は、共通コンポーネントを使用する各製品のすべての URL を 1 つのコマンドで変更できます。

> **メモ**
>
> プロトコルとポート番号を含んだ完全な URL を使用する必要があります（例えば、http://HostA:22015）。

操作手順

1. 次のコマンドを使用して、現在の URL を確認します。

```
＜共通コンポーネントのインストールフォルダー＞¥bin¥hcmds64chgurl /list
```

2. Ops Center Automator がスタンドアロンのサーバーにインストールされている場合は、次のコマンドで Ops Center Automator の URL だけを変更します。

```
＜共通コンポーネントのインストールフォルダー＞¥bin¥hcmds64chgurl /change ＜変更後のURL＞
/type Automation
```

3. Ops Center Automator と、共通コンポーネントを使用するほかの製品が同じサーバーにインストールされている場合は、次のコマンドを使用して、この管理サーバー上で実行されている各製品のすべての URL を変更します。

```
＜共通コンポーネントのインストールフォルダー＞¥bin¥hcmds64chgurl /change ＜変更前のURL＞
＜変更後のURL＞
```

URL には次の形式を使用します。

＜プロトコル＞://＜管理サーバーのIPアドレスまたはホスト名＞:＜ポート番号＞

- ＜プロトコル＞は、非 SSL 通信の場合はhttp、SSL 通信の場合はhttps です。

- *<管理サーバーのIPアドレスまたはホスト名>*は、Ops Center Automator がインストールされている管理サーバーの IP アドレスまたはホスト名です。
- *<ポート番号>*は、user_httpsd.conf ファイルのListen 行で設定されたポート番号です。
  SSL 以外の通信の場合は、SSL 以外の通信用のポート番号を指定します（デフォルト：22015)。
  SSL 通信の場合は、SSL 通信用のポート番号を指定します（デフォルト：22016)。
  user_httpsd.conf ファイルは、*<共通コンポーネントのインストールフォルダー>*¥uCPSB11¥httpsd¥conf にあります。

4. 新しい URL を使用して Ops Center Automator にアクセスできることを確認します。

5. setupcommonservice コマンドを実行して、Common Services に変更を適用します。

3.2　セキュア通信を構成する

ここでは、Ops Center Automator のセキュア通信を構成する方法について説明します。

3.2.1　Ops Center Automator のセキュリティー設定について

Ops Center Automator に対してセキュア通信を使用することによって、セキュリティーを高めることができます。セキュア通信では、Ops Center Automator は Ops Center Automator ネットワーク通信に TLS を使用することによって、セキュリティーを高めることができます。TLS により、Ops Center Automator での通信パートナー確認、パートナー識別のための認証強化、送受信される情報内の改ざんデータ検出を実現します。また、通信チャンネルが暗号化されるため、データが盗聴から保護されます。

Ops Center Automator は、以下のタイプの通信について、TLS を使用したセキュア通信を使用できます。

- 管理サーバーと管理クライアント間の通信
- 管理サーバーと管理対象間の通信

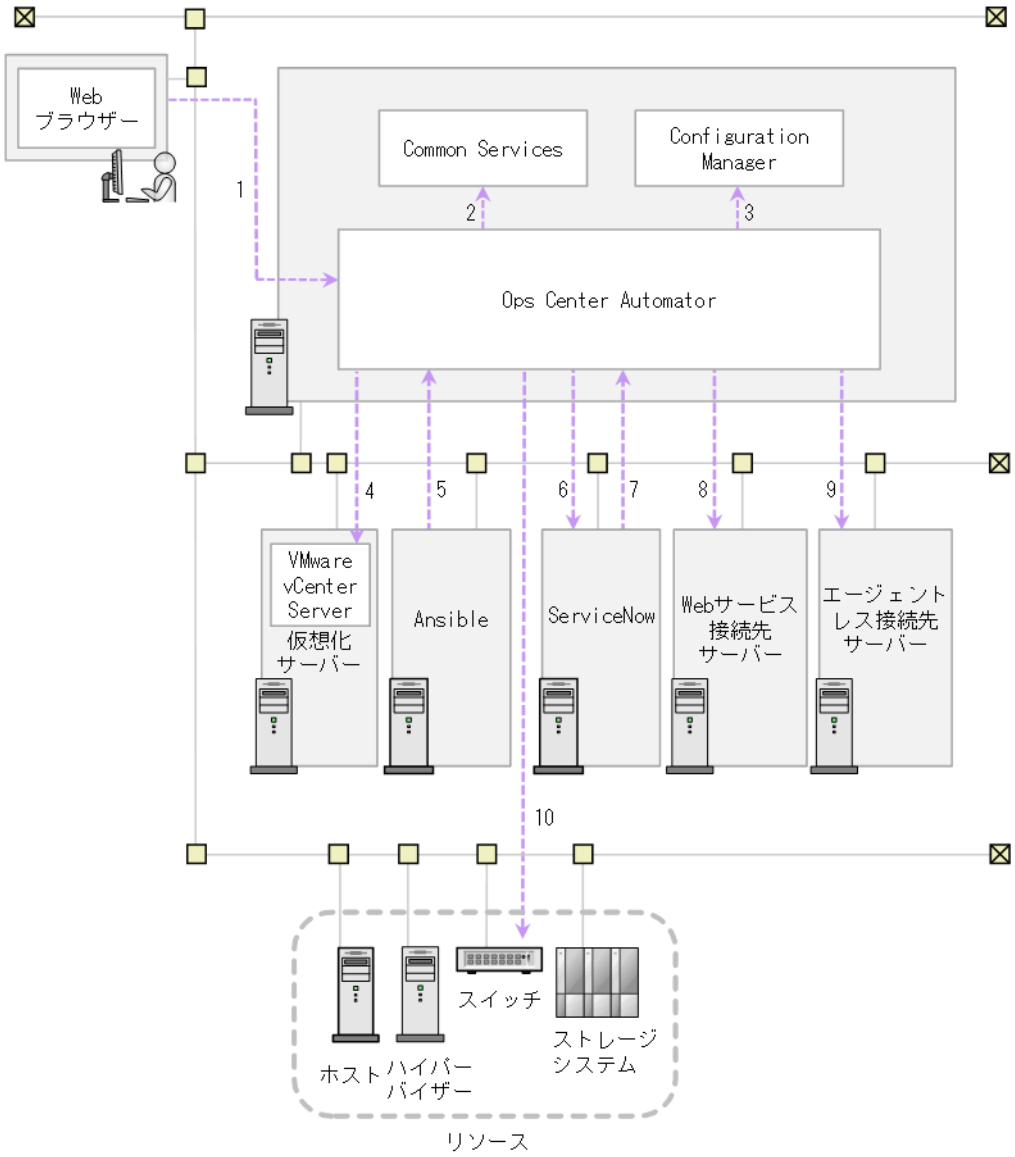
また、特定の管理クライアントだけが管理サーバーにアクセスできるように、アクセスを制限できます。

メモ

- セキュリティーを有効にして Ops Center Automator を使用するときには、サーバー証明書の有効期限が切れていないことを確認してください。サーバー証明書の有効期限が切れている場合は、有効な証明書を Ops Center Automator に登録しないとサーバーに接続できません。
- 管理サーバーと管理対象間のセキュア通信では、認証局、中間認証局、または、ルート認証局が発行した証明書を共通コンポーネントのトラストストアにインポートします。また、証明書を再登録する場合は、証明書をインポートする前に登録済みの証明書を削除する必要があります。
- Ops Center Automator をクラスター構成で運用している場合は、トラストストアへの証明書のインポートはアクティブノードとスタンバイノードそれぞれで行ってください。

3.2.2　Ops Center Automator のセキュリティー通信路

Ops Center Automator のセキュリティー通信路を次の図に示します。



Ops Center Automator で使用できるセキュリティー通信路および各通信路で使用されるプロトコルの対応を次に示します。表中の項番は、図中の番号と対応しています。

項番	サーバー（プログラム）	クライアント	プロトコル
1	Ops Center Automator※1	管理クライアント（Web ブラウザー）	HTTPS※2
2	Common Services※1	Ops Center Automator※1	HTTPS
3	Configuration Manager※1	Ops Center Automator※1	HTTPS※2
4	VMware vCenter Server	Ops Center Automator※1	HTTPS
5	Ops Center Automator※1	Ansible※4	HTTPS
6	ServiceNow※5	Ops Center Automator※1	HTTPS
7	Ops Center Automator※1	ServiceNow※5	HTTPS
8	Web サービス接続先サーバー（DCNM など）	Ops Center Automator※1	HTTPS※2

項番	サーバー（プログラム）	クライアント	プロトコル
9	エージェントレス接続先サーバー	Ops Center Automator※1	SSH※3
10	Brocade Fabric OS	Ops Center Automator※1	HTTPS※2

注※1　同一管理サーバーに Common Services がインストールされている場合、cssslsetup コマンドを利用して、この製品の SSL 通信を構成できます。

注※2　HTTPS 以外に HTTP も使用できます。

注※3　SSH 以外に Linux の場合は Telnet、Windows の場合は SMB および RPC も使用できます。

注※4　Ansible と連携するには、Ops Center Automator および Common Services との SSL 設定が必要です。

注※5　ServiceNow と連携するには、Ops Center Automator および Common Services との SSL 設定が必要です。

- Ops Center Automator との通信で使用するプロトコルが HTTPS の場合、TLS1.2 および TLS1.3 をサポートしています。Ops Center Automator がサーバーとなる HTTPS 接続においてサポートする Cipher Suites については、「付録 D.1　サーバーとしてサポートする Cipher Suites」を参照してください。
- 通信路 5 の Ansible とのセキュリティー通信の設定については、『Hitachi Ops Center Automator ユーザーズガイド』を参照してください。
- 通信路 7 の ServiceNow とのセキュリティー通信の設定については、『Hitachi Ops Center Automator ユーザーズガイド』を参照してください。

3.2.3　管理クライアントのセキュリティーを構成する

ここでは、管理サーバーと管理クライアント間のセキュア通信の設定について説明します。

(1)　管理クライアントのセキュア通信について

SSL を使用して管理サーバーと管理クライアント間のセキュア通信を実現します。SSL を実装するには、まず管理サーバーに SSL をセットアップし、次に管理クライアントに SSL をセットアップします。Web ベースのクライアントに SSL をセットアップするプロセスは、CLI クライアントの場合とは異なります。

(2)　セキュアなクライアント通信のためにサーバー上で SSL をセットアップする

管理サーバーと管理クライアント間のセキュア通信を実装するには、管理サーバーで SSL をセットアップする必要があります。

メモ

新規インストール後、SSL 設定が有効になります。 オプションなしでhcmds64ssltool コマンドを実行するときと同じ証明書が使用されます。 アップグレードインストールの場合、現在の SSL 設定を保持します。

hcmds64ssltool コマンドは、2 種類の秘密鍵、RSA 暗号と ECC（楕円曲線暗号）に対応する証明書署名要求および自己署名証明書を作成します。証明書署名要求は、PEM 形式で作成されます。このコマンドは自己署名証明書の作成にも使用できますが、自己署名証明書は、テスト目的にだけ使用する必要があります。

前提条件

Administrator 権限を持つユーザーとしてログインします。

次の情報を収集します。

- 認証局が指定する証明書署名要求の要件
- 管理クライアントで実行している Web ブラウザーのバージョン

  Web ブラウザーは、X.509 PEM 形式を使用しており、管理クライアント（GUI）で使用されているサーバー証明書の署名アルゴリズムをサポートしている必要があります。
- 既存の秘密鍵、証明書署名要求、および自己署名証明書の保存先フォルダー（再作成する場合）

  出力先パスに同じ名前のファイルが既に存在する場合、ファイルを上書きしません。したがって、秘密鍵、証明書署名要求、および自己署名証明書を再作成する場合、既存の保存先フォルダー以外のフォルダーに出力するか、既存のファイルを削除する必要があります。

操作手順

1. **共通コンポーネントの秘密鍵（httpsdkey.pem）、証明書署名要求（httpsd.csr）、および自己署名証明書（httpsd.pem）を作成するには、次のコマンドを使用します。**

   <共通コンポーネントのインストールフォルダー>¥bin¥hcmds64ssltool [/key *<秘密鍵ファイル>*] [/csr *<証明書発行要求ファイル>*] [/cert *<自己署名証明書ファイル>*] [/certtext *<自己署名証明書の内容ファイル>*] [/validity *<有効日数>*] [/sigalg *<RSA暗号用のサーバー証明書の署名アルゴリズム>*] [/eccsigalg *<ECC用のサーバー証明書の署名アルゴリズム>*] [/ecckeysize *<ECC用の秘密鍵のキーサイズ>*] [/ext *<X.509証明書の拡張情報>*]

   - /key

     作成された秘密鍵ファイルの出力先を絶対パスで指定します。このオプションを省略すると、ファイルは、RSA 暗号の場合は httpsdkey.pem、ECC の場合は ecc-httpsdkey.pem というファイル名で、デフォルトの出力先パス※に出力されます。
   - /csr

     作成された証明書発行要求ファイルの出力先を絶対パスで指定します。このオプションを省略すると、ファイルは、RSA 暗号の場合は httpsd.csr、ECC の場合は ecc-httpsd.csr というファイル名で、デフォルトの出力先パス※に出力されます。
   - /cert

     作成された自己署名証明書の出力先を絶対パスで指定します。このオプションを省略すると、ファイルは、RSA 暗号の場合は httpsd.pem、ECC の場合は ecc-httpsd.pem というファイル名で、デフォルトの出力先パス※に出力されます。
   - /certtext

作成された自己署名証明書の内容ファイルの出力先を絶対パスで指定します。このオプションを省略すると、ファイルは、RSA 暗号の場合は httpsd.txt、ECC の場合は ecc-httpsd.txt というファイル名で、デフォルトの出力先パス※に出力されます。

- /validity
  日数で自己署名証明書の有効期限を指定します。このオプションを省略すると、デフォルトの 3,650 日が使用されます。
- /sigalg
  RSA 暗号用のサーバー証明書の署名アルゴリズムを SHA256withRSA または SHA1withRSA で指定します。このオプションを省略すると、デフォルトの SHA256withRSA が使用されます。
- /eccsigalg
  ECC 用のサーバー証明書の署名アルゴリズムを SHA512withECDSA、SHA384withECDSA、SHA256withECDSA、または SHA1withECDSA で指定します。このオプションを省略すると、デフォルトの SHA384withECDSA が使用されます。
- /ecckeysize
  ECC 用のサーバー証明書の秘密鍵のサイズを 256 または 384 ビットで指定します。このオプションを省略すると、デフォルトの 384 が使用されます。
- /ext
  X.509 証明書の拡張情報を指定します。自己署名証明書および証明書署名要求に SAN（Subject Alternative Name）を設定する場合は、このオプションを指定します。指定方法は、Java の keytool コマンドの ext オプションに基づきます。Ops Center Automator で指定できる拡張情報は SAN だけであることに注意してください。ext オプションを複数回指定した場合は、最初の指定が有効になります。

  以下に、拡張情報を指定する例を示します。

  - www.example.com をホスト名として指定する場合：
    `hcmds64ssltool /ext san=dns:www.example.com`
  - www.example.com と www.example.net を複数のホスト名として指定する場合：
    `hcmds64ssltool /ext san=dns:www.example.com, dns:www.example.net`

このコマンドは、RSA ファイルおよび ECC ファイルを指定した出力先パスに出力します。RSA ファイルは、指定したファイル名で、ECC ファイルは、指定したファイル名の先頭に「ecc-」が付いて出力されます。

注※　key、csr、cert、または certtext オプションを省略した場合のデフォルトの出力先は、次のとおりです。

＜共通コンポーネントのインストールフォルダー＞¥uCPSB11¥httpsd¥conf¥ssl¥server

2. プロンプトが表示されたら、コロン（:）の後に以下の情報を入力します。
   - サーバー名（管理サーバーのホスト名） - 例：Automator_SC1
   - 組織単位（セクション） - 例：Ops Center Automator
   - 組織名（会社） - 例：Hitachi

- 都市または地区名 - 例：Yokohama
- 州または県名（フルネーム） - 例：Kanagawa
- 国名（2 文字のコード） - 例：JP

フィールドを空白のままにしておくには、ピリオド（.）を入力します。角括弧（[]）内に表示されるデフォルト値を選択するには、[Enter] キーを押します。

3. 証明書署名要求（httpsd.csr）を認証局に送信して、サーバー証明書を申請します。

> **メモ**
>
> 自己署名証明書を使用する場合、このステップは不要ですが、本番環境では署名付きサーバー証明書を使用することを推奨します。

認証局によって発行されたサーバー証明書は、通常、メールで送信されます。認証局によって送信されたメールとサーバー証明書を必ず保存してください。

4. Ops Center Automator のサービスを停止します。

5. 秘密鍵（httpsdkey.pem）とサーバー証明書または自己署名証明書（httpsd.pem）を、次のフォルダーにコピーします。

＜共通コンポーネントのインストールフォルダー＞¥uCPSB11¥httpsd¥conf¥ssl¥server

6. 次の場所からuser_httpsd.conf ファイルを開きます。

＜共通コンポーネントのインストールフォルダー＞¥uCPSB11¥httpsd¥conf¥user_httpsd.conf

7. user_httpsd.conf ファイル内で、以下のようにします。

> **メモ**
>
> Ops Center Automator をクラスター構成で運用している場合は、アクティブノードとスタンバイノードそれぞれでuser_httpsd.conf ファイルを編集してください。

a. 番号記号（#）を削除することによって、以下の行を非コメント化します。

#Listen 22016

から

#HWSLogSSLVerbose On

ただし、#SSLCACertificateFile と#Header set Strict-Transport-Security max-age=31536000 はコメントアウトしたままにしておく必要があります。

IPv6 環境の場合、#Listen [::]:22016 行の先頭の番号記号（#）を削除します。

以下に、user_httpsd.conf ファイルの編集例を示します。

```
ServerName ＜管理サーバーのホスト名＞
Listen [::]:22015
Listen 22015
#Listen 127.0.0.1:22015
```

```
SSLEngine Off
Listen [::]:22016
Listen 22016
<VirtualHost *:22016>
ServerName <管理サーバーのホスト名>
SSLEngine On
SSLProtocol +TLSv1.2 +TLSv1.3
SSLCipherSuite TLSv1.3 TLS_AES_128_GCM_SHA256:TLS_AES_256_GCM_SHA384:TLS_CHACHA20_POLY
1305_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-A
ES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256
SSLCertificateKeyFile
"<共通コンポーネントのインストールフォルダー>¥uCPSB11¥httpsd¥conf¥ssl¥server¥httpsdk
ey.pem"
SSLCertificateFile
"<共通コンポーネントのインストールフォルダー>¥uCPSB11¥httpsd¥conf¥ssl¥server¥httpsd.
pem"
SSLCertificateKeyFile
"<共通コンポーネントのインストールフォルダー>¥uCPSB11¥httpsd¥conf¥ssl¥server¥ecc-htt
psdkey.pem"
SSLCertificateFile
"<共通コンポーネントのインストールフォルダー>¥uCPSB11¥httpsd¥conf¥ssl¥server¥ecc-htt
psd.pem"
# SSLCACertificateFile
"<共通コンポーネントのインストールフォルダー>¥uCPSB11¥httpsd¥conf¥ssl¥cacert¥anycert
.pem"
# Header set Strict-Transport-Security max-age=31536000
</VirtualHost>
HWSLogSSLVerbose On
```

b. 必要に応じて、以下の行を編集します。

最初の行の ServerName

<VirtualHost>タグの ServerName

SSLCertificateKeyFile

SSLCertificateFile

#SSLCACertificateFile

認証局から発行されたチェーンサーバー証明書を使用するときには、"# SSLCACertificateFile"行から番号記号（#）を削除し、（認証局によって作成された）チェーン証明書ファイルを絶対パスで指定します。

メモ

外部サーバーから管理サーバーへの非 SSL 通信をブロックするには、Listen 22015 行と Listen [::]:22015 行の先頭に番号記号（#）を追加してコメントアウトします。これらの行をコメントアウトした後、#Listen 127.0.0.1:22015 行の番号記号（#）を削除します。また、クラスター環境の場合、command_user.properties ファイルに次の行を追加または編集します。

```
command.hostname = localhost
```

command_user.properties ファイルは、次の場所に格納されています。

＜共有フォルダー名＞¥Automation¥conf

ディレクティブを編集する場合、以下について注意してください。

- 同じディレクティブを 2 回指定しないでください。ただし、SSLCertificateKeyFile および SSLCertificateFile ディレクティブは、RSA 暗号用と ECC 用で 2 回、指定できます。
- ディレクティブの途中で改行を入れないでください。
- ディレクティブにパスを指定する場合、シンボリックリンクまたはジャンクションポイントを指定しないでください。パスは絶対パスで指定してください。
- ディレクティブに証明書および秘密鍵ファイルを指定する場合、PEM 形式のファイルを指定してください。
- httpsd.conf ファイルおよびhsso_httpsd.conf ファイルを編集しないでください。
- 次の行の番号記号（#）は削除しないでください。

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

以下に、user_httpsd.conf ファイルの編集例を示します。番号は、デフォルトのポート番号を示しています。

```
ServerName ＜管理サーバーのホスト名＞
Listen [::]:22015
Listen 22015
#Listen 127.0.0.1:22015
SSLEngine Off
Listen [::]:22016
Listen 22016
<VirtualHost *:22016>
ServerName ＜管理サーバーのホスト名＞
SSLEngine On
SSLProtocol +TLSv1.2 +TLSv1.3
SSLCipherSuite TLSv1.3 TLS_AES_128_GCM_SHA256:TLS_AES_256_GCM_SHA384:TLS_CHACHA20_POLY130
5_SHA256
# SSLCipherSuite ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AE
S256-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-AES2
56-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256
SSLCertificateKeyFile
"＜共通コンポーネントのインストールフォルダー＞¥uCPSB11¥httpsd¥conf¥ssl¥server¥httpsdkey.
pem"
SSLCertificateFile
"＜共通コンポーネントのインストールフォルダー＞¥uCPSB11¥httpsd¥conf¥ssl¥server¥server-cer
tificate-or-self-signed-certificate-file"
SSLCertificateKeyFile
"＜共通コンポーネントのインストールフォルダー＞¥uCPSB11¥httpsd¥conf¥ssl¥server¥ecc-httpsd
key.pem"
SSLCertificateFile
```

```
”<共通コンポーネントのインストールフォルダー>¥uCPSB11¥httpsd¥conf¥ssl¥server¥ecc-httpsd
.pem”
SSLCACertificateFile
”<共通コンポーネントのインストールフォルダー>¥uCPSB11¥httpsd¥conf¥ssl¥cacert¥certificat
e-file-from-certificate-authority”
# Header set Strict-Transport-Security max-age=31536000
</VirtualHost>
HWSLogSSLVerbose On
```

8. Ops Center Automator のサービスを起動します。
9. hcmds64chgurl コマンドを実行して、次のように Ops Center Automator の URL を更新します。
   - プロトコルを http:から https:に変更します。
   - セキュア通信に使用されるポート番号を変更します。
10. setupcommonservice コマンドを実行して、Common Services に変更を適用します。

操作結果

これで、Ops Center Automator サーバー上で SSL が実装されます。

(3) Web ベースの管理クライアントで SSL をセットアップする

管理サーバーと管理クライアント間のセキュア通信を実装するには、Ops Center Automator の Web ベースのユーザーインターフェイスにアクセスするすべての管理クライアント上で SSL をセットアップする必要があります。まず、管理サーバーに SSL をセットアップし、次に管理クライアントに SSL をセットアップします。このクライアントから管理サーバーに最初にアクセスするときのみ、この手順に従う必要があります。

前提条件

使用される署名アルゴリズムが SHA256 と RSA の場合、使用される Web ブラウザーは SHA256 と RSA 署名を持つサーバー証明書をサポートする必要があります。

操作手順

1. 管理クライアントから、次の URL を使用して、SSL 接続で管理サーバーにアクセスします。
   https://*<Ops Center AutomatorのIPアドレスまたはホスト名>*:*<ポート番号（SSL）>*/Automation/
2. SSL 証明書をインストールします。

操作結果

SSL 証明書が管理クライアントに登録され、SSL を使用して管理サーバーと通信できるようになります。

3.2.4 Common Services とのセキュア通信を設定する

Ops Center Automator および Common Services は、SSL 通信を行います。証明書の検証を有効にする場合は、共通コンポーネントのトラストストアに証明書をインポートする必要があります。また、使用する Cipher Suites を変更することもできます。

> **ヒント**
>
> 同一管理サーバーに Common Services がインストールされている場合、cssslsetup コマンドを利用できます。cssslsetup コマンドを利用すると、共通の秘密鍵とサーバー証明書を使用して、同一管理サーバーにインストールされている Ops Center 製品の SSL 通信を構成できます。cssslsetup コマンドの利用方法と対応範囲については、『Hitachi Ops Center インストールガイド』を参照してください。

前提条件

- Ops Center Automator の管理サーバーと管理クライアント間の SSL 設定が完了している必要があります。
- Common Services との SSL 通信を設定するためには、Common Services で SSL の設定が完了している必要があります。詳細については、『Hitachi Ops Center インストールガイド』を参照してください。

操作手順

1. 証明書の検証を有効にする場合、次の手順を実行します。
   a. 次のコマンドを実行して、共通コンポーネントのトラストストアに証明書をインポートします。

   ```
   <共通コンポーネントのインストールフォルダー>¥bin¥hcmds64keytool -import -alias <エイリアス名> -keystore <共通コンポーネントのインストールフォルダー>¥uCPSB11¥hjdk¥jdk¥lib¥security¥jssecacerts -storepass <トラストストアへのアクセスパスワード> -file <証明書ファイル名> -storetype JKS
   ```

   Java で証明書をインポートするには、トラストストアのパスワードが 6 文字以上であることを確認してください。また、新しいエイリアス名が既存のエイリアス名と衝突しないことを確認してください。

   使用する証明書は環境および構成によって異なるため、Common Services で利用可能な証明書に基づいて、RSA 証明書と ECDSA 証明書のいずれか、または両方を共通コンポーネントのトラストストアにインポートしてください。

   b. 次の場所からconfig_user.properties ファイルを開き、sso.https.certification を「true」に変更します。
   非クラスター環境の場合：

   <Ops Center Automatorのインストールフォルダー>¥conf

   クラスター環境の場合：

<共有フォルダー名>¥Automation¥conf

2. （任意）Common Services との通信で使用する Cipher Suites を変更する場合、次の手順を実行します。

   a. 次の場所からconfig_user.properties ファイルを開きます。
   非クラスター環境の場合：
   <Ops Center Automatorのインストールフォルダー>¥conf
   クラスター環境の場合：
   <共有フォルダー名>¥Automation¥conf

   b. tls.client.cipherSuites の行を編集します。
   tls.client.cipherSuites の行が存在しない場合は、追加してください。
   通信では、tls.client.cipherSuites の行に設定された Cipher Suites のいずれかを使用します。使用したい Cipher Suites をtls.client.cipherSuites の行に設定してください。使用したい Cipher Suites が複数ある場合は、Cipher Suites をカンマ区切りで設定します。
   使用できる Cipher Suites は「付録 D.2　クライアントとしてサポートする Cipher Suites」を参照してください。
   tls.client.cipherSuites プロパティの詳細は、「3.4　システム構成を変更する」を参照してください。

3. hcmds64srv コマンドを実行して、Ops Center Automator および共通コンポーネントを使用するすべての製品のサービスを再起動します。

3.2.5　Configuration Manager REST API サーバーとのセキュア通信を設定する

Ops Center Automator サーバーと Configuration Manager REST API サーバーで SSL 通信をするには、共通コンポーネントのトラストストアに証明書をインポートする必要があります。また、使用する Cipher Suites を変更することもできます。

前提条件

Configuration Manager REST API サーバーとの SSL 通信を設定するためには、Configuration Manager で SSL の設定が完了している必要があります。詳細については、『Hitachi Ops Center API Configuration Manager REST API リファレンスガイド』の REST API クライアントと REST API サーバー間での SSL 通信の設定について説明している箇所を参照してください。

操作手順

1. 次のコマンドを実行して、共通コンポーネントのトラストストアに証明書をインポートします。

```
<共通コンポーネントのインストールフォルダー>¥bin¥hcmds64keytool -import -alias <エイリアス名> -keystore <共通コンポーネントのインストールフォルダー>¥uCPSB11¥hjdk¥jdk¥lib¥security¥jssecacerts -storepass <トラストストアへのアクセスパスワード> -file <証明書ファイル名> -storetype JKS
```

Java で証明書をインポートするには、トラストストアのパスワードが 6 文字以上であることを確認してください。また、新しいエイリアス名が既存のエイリアス名と衝突しないことを確認してください。

使用する証明書は環境および構成によって異なるため、Configuration Manager REST API サーバーで利用可能な証明書に基づいて、RSA 証明書と ECDSA 証明書のいずれか、または両方を共通コンポーネントのトラストストアにインポートしてください。

2. (任意) Configuration Manager REST API サーバーとの通信で使用する Cipher Suites を変更する場合、次の手順を実行します。

> **メモ**
>
> ビルトインのサービステンプレートを使用して Configuration Manager REST API サーバーと通信する場合、このプロパティは影響しないため、この手順を実行する必要はありません。

   a. 次の場所から`config_user.properties` ファイルを開きます。
   非クラスター環境の場合：
   <Ops Center Automatorのインストールフォルダー>¥conf
   クラスター環境の場合：
   <共有フォルダー名>¥Automation¥conf

   b. `tls.client.cipherSuites` の行を編集します。
   `tls.client.cipherSuites` の行が存在しない場合は、追加してください。
   通信では、`tls.client.cipherSuites` の行に設定された Cipher Suites のいずれかを使用します。使用したい Cipher Suites を`tls.client.cipherSuites` の行に設定してください。使用したい Cipher Suites が複数ある場合は、Cipher Suites をカンマ区切りで設定します。
   使用できる Cipher Suites は「付録 D.2　クライアントとしてサポートする Cipher Suites」を参照してください。
   `tls.client.cipherSuites` プロパティの詳細は、「3.4　システム構成を変更する」を参照してください。

3. `hcmds64srv` コマンドを実行して、Ops Center Automator および共通コンポーネントを使用するすべての製品のサービスを再起動します。

3.2.6　VMware vCenter Server とのセキュア通信を設定する

ESX cluster サービステンプレートを使用するには、サービステンプレートで前提条件となるソフトウェアのセキュア通信を設定するため、VMware vCenter Server のルート証明書を共通コンポーネントのトラストストアと OS のトラストストアにインストールする必要があります。また、使用する Cipher Suites を変更することもできます。

操作手順

1. Web ブラウザーを使用して vCenter ユーザーインターフェイスにアクセスします。

2. 画面の右側で、[信頼されたルート CA 証明書をダウンロード] を選択します。

3. 共通コンポーネントのトラストストアが存在するサーバーに VMware vCenter Server のルート証明書をダウンロードします。

4. ダウンロードした zip ファイルを解凍します。

> **メモ**
>
> ダウンロードしたファイルの拡張子が.zip でない場合は、拡張子を.zip に変更します。

2 種類の証明書ファイルが含まれる.certs フォルダーが解凍されます。

5. 次のコマンドを実行して、共通コンポーネントのトラストストアに VMware vCenter Server のルート証明書をインポートします。

```
<共通コンポーネントのインストールフォルダー>¥bin¥hcmds64keytool -import -alias <エイリアス名> -keystore <共通コンポーネントのインストールフォルダー>¥uCPSB11¥hjdk¥jdk¥lib¥security¥jssecacerts -storepass <トラストストアへのアクセスパスワード> -file <証明書ファイル名> -storetype JKS
```

Java で証明書をインポートするには、トラストストアのパスワードが 6 文字以上であることを確認してください。また、新しいエイリアス名が既存のエイリアス名と衝突しないことを確認してください。

使用する証明書は環境および構成によって異なるため、VMware vCenter Server で利用可能な証明書に基づいて、RSA 証明書と ECDSA 証明書のいずれか、または両方を共通コンポーネントのトラストストアにインポートしてください。

6. OS のトラストストアに VMware vCenter Server のルート証明書をインストールします。

   1. 拡張子.crt のファイルの上で右クリックし、[証明書のインストール] を選択します。
      証明書のインポートウィザードが開きます。
   2. [ローカル コンピューター] を選択し、[次へ] をクリックします。
   3. [証明書をすべて次のストアに配置する] を選択します。
   4. [参照] をクリックし、[信頼されたルート証明機関] を選択して、[完了] をクリックします。
   5. 拡張子.crl のファイルについても手順 1 から 4 を実施します。

7. (任意) VMware vCenter Server との通信で使用する Cipher Suites を変更する場合、次の手順を実行します。

> **メモ**
>
> 次のサービステンプレートを使用して VMware vCenter Server 通信する場合、このプロパティは影響しないため、この手順を実行する必要はありません。
>
> - 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. 次の場所からconfig_user.properties ファイルを開きます。

非クラスター環境の場合：

<Ops Center Automatorのインストールフォルダー>¥conf

クラスター環境の場合：

<共有フォルダー名>¥Automation¥conf

b. tls.client.cipherSuites の行を編集します。

tls.client.cipherSuites の行が存在しない場合は、追加してください。

通信では、tls.client.cipherSuites の行に設定された Cipher Suites のいずれかを使用します。使用したい Cipher Suites をtls.client.cipherSuites の行に設定してください。使用したい Cipher Suites が複数ある場合は、Cipher Suites をカンマ区切りで設定します。

使用できる Cipher Suites は「付録 D.2　クライアントとしてサポートする Cipher Suites」を参照してください。

tls.client.cipherSuites プロパティの詳細は、「3.4　システム構成を変更する」を参照してください。

8. hcmds64srv コマンドを実行して、Ops Center Automator および共通コンポーネントを使用するすべての製品のサービスを再起動します。

次の作業

ESX cluster サービステンプレートを使用するには、Python をインストールする必要があります。詳細については、『Hitachi Ops Center Automator ユーザーズガイド』を参照してください。

3.2.7　外部 Web サーバーとのセキュア通信を設定する

外部 Web サーバーと Ops Center Automator で SSL 通信をするには、共通コンポーネントのトラストストアに証明書をインポートする必要があります。また、使用する Cipher Suites を変更することもできます。

次の外部 Web サーバーと Web サービス接続をします。

- BNA
- Brocade FC スイッチ
- DCNM
- ServiceNow
- その他の Web サービス接続

操作手順

1. 次のコマンドを実行して、共通コンポーネントのトラストストアに証明書をインポートします。

   ```
   <共通コンポーネントのインストールフォルダー>¥bin¥hcmds64keytool -import -alias <エイリアス名> -keystore <共通コンポーネントのインストールフォルダー>¥uCPSB11¥hjdk¥jdk¥lib¥security¥jssecacerts -storepass <トラストストアへのアクセスパスワード> -file <証明書ファイル名> -storetype JKS
   ```

   Java で証明書をインポートするには、トラストストアのパスワードが 6 文字以上であることを確認してください。また、新しいエイリアス名が既存のエイリアス名と衝突しないことを確認してください。

   使用する証明書は環境および構成によって異なるため、外部 Web サーバーで利用可能な証明書に基づいて、RSA 証明書と ECDSA 証明書のいずれか、または両方を共通コンポーネントのトラストストアにインポートしてください。

2. （任意）外部 Web サーバーとの通信で使用する Cipher Suites を変更する場合、次の手順を実行します。

   メモ

   カテゴリーに FOS_PrimarySwitch を設定する Brocade FC スイッチとの Web サービス接続の場合、FOS との通信で使用する下記の Cipher Suites を追加してください。

   - TLS_RSA_WITH_AES_256_CBC_SHA256
   - TLS_RSA_WITH_AES_128_CBC_SHA256

   a. 次の場所から`config_user.properties` ファイルを開きます。
   非クラスター環境の場合：

   <Ops Center Automatorのインストールフォルダー>¥conf

   クラスター環境の場合：

   <共有フォルダー名>¥Automation¥conf

   b. `tls.client.cipherSuites` の行を編集します。
   `tls.client.cipherSuites` の行が存在しない場合は、追加してください。

   通信では、`tls.client.cipherSuites` の行に設定された Cipher Suites のいずれかを使用します。使用したい Cipher Suites を`tls.client.cipherSuites` の行に設定してください。使用したい Cipher Suites が複数ある場合は、Cipher Suites をカンマ区切りで設定します。

   使用できる Cipher Suites は「付録 D.2　クライアントとしてサポートする Cipher Suites」を参照してください。

   `tls.client.cipherSuites` プロパティの詳細は、「3.4　システム構成を変更する」を参照してください。

3. `hcmds64srv` コマンドを実行して、Ops Center Automator および共通コンポーネントを使用するすべての製品のサービスを再起動します。

追加のガイドライン

- 外部 Web サーバーのセキュリティー設定の方法については、各製品のマニュアルを参照してください。

- 外部 Web サーバーのサーバー証明書を取得するには、関連する製品のマニュアルでサーバー証明書へのアクセスについて参照してください。
- DCNM をアップグレードすると、サーバー証明書が初期化されます。『Cisco DCNM Installation and Upgrade Guide for SAN Deployment』の「Restoring the certificates after an upgrade」に記載されている手順を実施する必要があります。
- DCNM 11.5 を使用する場合は、『Cisco DCNM Installation and Upgrade Guide for SAN Deployment』の「Certificates」に記載されている手順に従って、Common Name に適切なホスト名を指定して証明書を作成します。
- Brocade FC スイッチを使用する場合は、『Brocade Fabric OS Administration Guide』の「Managing the Security Certificates Using the secCertMgmt Command」に記載されている手順に従って、SSL 設定が完了している必要があります。

3.2.8 サーバー証明書の有効期限を確認する

SSL 証明書の有効期限を確認することで、証明書の有効期限が切れていないかどうかを確認できます。管理サーバー証明書の有効期限が切れておらず、管理対象サーバーとのセキュア通信を維持できることを確認する必要があります。

操作手順

共通コンポーネントのサーバー証明書の有効期限を確認するには、hcmds64keytool コマンドを使用します。

1. 次のコマンドを実行します。

```
<共通コンポーネントのインストールフォルダー>¥bin¥hcmds64keytool -printcert -v -file <サーバー証明書のパス>
```

メモ

自己署名証明書の有効期限は、サーバー間の接続時には検証されません。Ops Center Automator サーバーと Web サーバーの接続時に証明書の有効期限を確認する必要がある場合は、認証局によって発行された証明書を使用してください。その場合、サーバーの証明書だけでなく、認証局と中間認証局の証明書もインポートします。

3.2.9 共通コンポーネントのトラストストアにインポートされた証明書を削除する

共通コンポーネントのトラストストア（ldapcacerts または jssecacerts）にインポートされた証明書を削除するには、hcmds64keytool コマンドを使用します。

前提条件

次の情報を確認します。

- 削除する証明書のエイリアス名
- 証明書が格納されているトラストストアファイルのパス
- トラストストアへのアクセスパスワード

操作手順

1. 次のコマンドを実行します。

```
＜共通コンポーネントのインストールフォルダー＞¥bin¥hcmds64keytool -delete -alias ＜エイリアス名＞ -keystore ＜トラストストアファイル名＞ -storepass ＜トラストストアへのアクセスパスワード＞
```

3.3 監査ログ

監査ログには、Ops Center Automator サーバー上でのすべてのユーザーアクションが記録されます。監査ログには、外部サービス、認証、設定へのアクセス、サービスの起動や停止などのイベントが記録されます。監査ログを調べることで、システムの利用状況の確認や不正アクセスの監査ができます。

3.3.1 監査ログを設定する

監査ログには、Ops Center Automator サーバー上でのすべてのユーザーアクションが記録されます。監査ログには、外部サービス、認証、設定へのアクセス、サービスの起動や停止などのイベントが記録されます。監査ログを調べることで、システムの利用状況の確認や不正アクセスの監査ができます。

監査ログデータは、イベントログファイル（アプリケーションログファイル）に出力されます。

以下の表に、共通コンポーネントを使用する製品によって生成される、監査ログデータのカテゴリーを示します。異なる製品によってさまざまなタイプの監査ログデータが生成されます。

カテゴリー	説明
StartStop	ハードウェアやソフトウェアの起動または停止を示すイベント • OS の起動またはシャットダウン • ハードウェアコンポーネント（マイクロコンポーネントを含む）の起動または停止 • ストレージシステムまたは SVP 上のソフトウェア、および共通コンポーネントを使用する製品の起動または停止
Failure	ハードウェアまたはソフトウェアの障害を示すイベント • ハードウェア障害 • ソフトウェア障害（メモリーエラーなど）
LinkStatus	デバイス間のリンク状態を示すイベント リンクが接続しているか、または接続が切れているか
ExternalService	外部サービスとの通信結果を示すイベント • NTP や DNS などの外部サーバーとの通信 • 管理サーバー（SNMP）との通信
Authentication	デバイス、管理者、またはエンドユーザーが、接続や認証に成功または失敗したことを示すイベント • ファイバーチャネルログイン • デバイス認証（ファイバーチャネル - セキュリティープロトコル認証、iSCSI ログイン認証、SSL サーバー／クライアント認証） • 管理者またはエンドユーザー認証
AccessControl	デバイス、管理者、またはエンドユーザーが、リソースへのアクセスに成功または失敗したことを示すイベント • デバイスのアクセスコントロール • 管理者またはエンドユーザーのアクセスコントロール

カテゴリー	説明
ContentAccess	重要データへのアクセスの試みが成功または失敗したことを示すイベント • NAS 上の重要ファイルまたは HTTP がサポートされている場合のコンテンツへのアクセス • 監査ログファイルへのアクセス
ConfigurationAccess	管理者が許可されている操作に成功または失敗したことを示すイベント • 設定情報の参照または更新 • アカウントの追加や削除を含むアカウント設定の更新 • セキュリティー設定 • 監査ログ設定の参照または更新
Maintenance	実施したメンテナンス操作が成功または失敗したことを示すイベント • ハードウェアコンポーネントの追加または削除 • ソフトウェアコンポーネントの追加または削除
AnomalyEvent	しきい値超過などの異常が発生したことを示すイベント • ネットワークトラフィックしきい値の超過 • CPU 負荷しきい値の超過 • 内部に一時的に保存された監査ログデータが制限に達するか、ラップアラウンドが発生したことの事前通知
	異常な通信が発生したことを示すイベント • 通常使用しているポートに対する SYN フラッド攻撃またはプロトコル違反 • 未使用ポートに対するアクセス（ポートスキャンなど）

3.3.2 監査ログを有効にする

Ops Center Automator サーバーの監査ログを有効にし、監査イベントを監査ログに出力するよう変更するには、まず、共通コンポーネント用の環境設定ファイル（auditlog.conf）を設定します。その後で、Ops Center Automator および共通コンポーネントを使用するすべての製品のサービスを再起動してください。

メモ

- 監査ログはデフォルトで無効になっています。必要に応じて設定を有効にしてください。
- 大量の監査ログデータが出力される場合があります。ログファイルのサイズを変更し、生成されたログファイルを必要に応じてバックアップまたはアーカイブしてください。

操作手順

1. Administrator 権限のユーザーとして、管理サーバーにログインします。

2. auditlog.conf ファイルを開きます。

<共通コンポーネントのインストールフォルダー>¥conf¥sec¥auditlog.conf

> **メモ**
>
> - auditlog.conf ファイルは、共通コンポーネント用の環境設定ファイルです。したがって、共通コンポーネントを利用する別の製品が、Ops Center Automator サーバーと同じホストにインストールされている場合は、監査ログの設定が両方の製品で共有されます。
> - Ops Center Automator をクラスター構成で運用している場合は、アクティブノードとスタンバイノードそれぞれでauditlog.conf ファイルを編集してください。

3. 監査ログを有効にするには、auditlog.conf ファイルのLog.Event.Category プロパティに監査イベントカテゴリーを指定します。

4. 監査ログを無効にするには、auditlog.conf ファイルのLog.Event.Category プロパティに指定されている監査イベントカテゴリーをすべて削除します。

5. Ops Center Automator および共通コンポーネントを使用するすべての製品のサービスを再起動します。

3.3.3 auditlog.conf ファイルの設定

以下の値をauditlog.conf ファイルに設定できます。

Log.Event.Category

出力される監査イベントカテゴリーを指定します。(デフォルト値：なし)

複数のカテゴリーを指定する場合は、カテゴリーとカテゴリーをコンマ（,）で区切ります。この場合、カテゴリーとコンマの間にスペースを挿入しないでください。Log.Event.Category が指定されていないと、監査ログデータは出力されません。Log.Event.Category は大文字と小文字を区別しません。無効なカテゴリー名が指定された場合、指定したファイル名は無視されます。

有効なカテゴリー：StartStop、Failure、LinkStatus、ExternalService、Authentication、AccessControl、ContentAccess、ConfigurationAccess、Maintenance、AnomalyEvent

Log.Level

出力される監査イベントの重要度を指定します。(デフォルト値：6)

指定した重要度レベル以下のイベントがイベントログファイルに出力されます。

各監査イベントの重要度については、監査ログに出力される監査イベントのリストを参照してください。

無効な値や数字以外の文字が指定された場合は、デフォルト値が使用されます。

以下の表に、Log.Level に指定できる値とイベントログに表示されるレベルの対応を示します。

Log.Level に指定できる値	イベントログに表示されるレベル
0	エラー

Log.Level に指定できる値	イベントログに表示されるレベル
1	エラー
2	
3	
4	警告
5	情報
6	
7	

3.3.4 auditlog.conf ファイルのサンプル

以下に、auditlog.conf ファイルの例を示します。

```
# 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
```

上記の例では、監査イベントのすべてのタイプが出力されています。

Log.Level 6 がエラー、警告、情報のレベルに対応するログデータを出力します。

3.3.5 監査ログに出力されるデータのフォーマット

監査ログデータはイベントログファイルに出力されます。

監査ログに出力されるデータの形式を次に示します。

プログラム名 [*プロセスID*]: *メッセージ部*

*メッセージ部*の形式と内容は次のとおりです。*メッセージ部*のうち、最大 953 シングルバイト文字がイベントログファイルに表示できます。

統一識別子,統一仕様リビジョン番号,通番,メッセージID,日付・時刻,検出エンティティー,検出場所,監査事象の種別,監査事象の結果,監査事象の結果サブジェクト識別情報,ハードウェア識別情報,発生場所情報,ロケーション識別情報,FQDN,冗長化識別情報,エージェント情報,リクエスト送信元ホスト,リク

エスト送信元ポート番号,リクエスト送信先ホスト,リクエスト送信先ポート番号,一括操作識別子,ログ種別情報,アプリケーション識別情報,予約領域,メッセージテキスト

項目※	説明
統一識別子	CELFSS に固定
統一仕様リビジョン番号	1.1 に固定
通番	監査ログメッセージのシリアル番号
メッセージID	メッセージ ID
日付・時刻	メッセージが出力された日時。この項目は、*yyyy*-*mm*-*dd*T*hh*:*mm*:*ss*.*s**タイムゾーン*の形式で出力されます。
検出エンティティー	コンポーネント名またはプロセス名
検出場所	ホスト名
監査事象の種別	イベントタイプ
監査事象の結果	イベント結果
監査事象の結果サブジェクト識別情報	イベントに対応するアカウント ID、プロセス ID、または IP アドレス
ハードウェア識別情報	ハードウェアモデルまたはシリアル番号
発生場所情報	ハードウェアコンポーネントの識別情報
ロケーション識別情報	場所の識別情報
FQDN	完全修飾ドメイン名
冗長化識別情報	冗長性識別情報
エージェント情報	エージェント情報
リクエスト送信元ホスト	リクエスト送信元のホスト名
リクエスト送信元ポート番号	リクエスト送信元のポート番号
リクエスト送信先ホスト	リクエスト送信先のホスト名
リクエスト送信先ポート番号	リクエスト送信先のポート番号
一括操作識別子	プログラムによる操作の通番
ログ種別情報	BasicLog またはDetailLog に固定
アプリケーション識別情報	プログラム識別情報
予約領域	出力なし。予約領域です。
メッセージテキスト	コンテンツは監査イベントによって変わります。 表示できない文字は、アスタリスク（*）として出力されます。
注※　一部の監査イベントに出力されない項目もあります。	

監査ログのログインイベントのメッセージ部の例を次に示します。

```
CELFSS,1.1,3,KNAE20002-I,2021-09-03T21:31:56.8+09:00,HAD,management-host,Authentication,Success,subj:uid=sysadmin,autoAuth,Login,BasicLog,HAD,”ログインに成功しました。”
```

3.4 システム構成を変更する

config_user.properties ファイルを編集すると、ログやタスクなど、Ops Center Automator のさまざまな設定を構成できます。ファイルを変更して保存した後で、Ops Center Automator エンジン Web サービスは再起動する必要があることに注意してください。

このファイルを編集することで、以下の設定を変更できます。

- ログファイル構成（保存するログの数を指定します）
- タスクおよび履歴構成（保存するタスクとタスク履歴の数を指定します）
- リモートコマンド実行に関する構成（SSH/telnet ポート番号）
- メール通知の構成情報
- Service Builder に関する構成情報
- 接続タイムアウト値の設定
- 同時実行するプラグインの最大数

ファイルは、次の場所に格納されています。

＜Ops Center Automatorのインストールフォルダー＞¥conf
ファイルは、次の形式を使用します。

specification-key-name=setting

プロパティファイルを編集するときには、次のことに注意してください。

- #で始まる行は、コメントとして扱われます。
- 空白行は無視されます。
- エンコードは ISO 8859-1 です。
- 内容は大文字と小文字が区別されます。
- 文字列の中で¥を指定するには、¥¥と入力する必要があります。
- 設定として無効な値を入力した場合はデフォルト値に設定され、メッセージKNAE02022-W が統合トレースログとパブリックログに送信されます。
- 1 つのファイル内で同じ指定キーが複数回入力された場合は、最後に指定したキーが有効になります。

表 3-1 config_user.properties ファイルの設定

カテゴリー	キー名	設定	値	デフォルト値
HTTP 接続ポート番号	server.http.port	Ops Center Automator サーバーと共通コンポーネント間の HTTP 通信に使用されるポート番号を指定します。	0～65535	22015

カテゴリー	キー名	設定	値	デフォルト値
ログ※1	logger.message.server.MaxBackupIndex	サーバーのログバックアップファイルの最大数を指定します。	1～16	7
	logger.message.server.MaxFileSize	サーバーの最大ログファイルサイズ（KB 単位）を指定します。	4～2097151	1024
	logger.message.command.MaxBackupIndex	コマンドのログバックアップファイルの最大数を指定します。	1～16	7
	logger.message.command.MaxFileSize	コマンドの最大ログファイルサイズ（KB 単位）を指定します。	4～2097151	1024
	logger.TA.MaxFileSize	タスクの最大ログファイルサイズ（KB 単位）を指定します。	4～2097151	10240
タスク管理	tasklist.autoarchive.taskRemainingPeriod	終了したタスクをタスクリストに残しておく期間（日数）を指定します。	1～90	7
	tasklist.autoarchive.executeTime	自動アーカイブタスクを実行する時刻を指定します。	00:00:00～23:59:59	04:00:00
	tasklist.autoarchive.maxTasks	タスクリストに表示するタスクの最大数を指定します。	100～5000	5000
	tasklist.autodelete.maxHistories	保持する履歴エントリーの最大数を指定します。	100～30000	30000
繰り返し	foreach.max_value	繰り返し実行部品によって実行できる同時タスクの最大数を指定します。	1～99	3
リモート接続ポート番号	ssh.port.number	対象機器の SSH ポート番号を指定します。	0～65535	22
	telnet.port.number	対象機器の Telnet ポート番号を指定します。	0～65535	23
SSH 暗号アルゴリズム	ssh.disable.kexAlgorithms	エージェントレス接続（SSH）で無効化する鍵交換アルゴリズムをカンマ区切りで指定します。カンマの前後の空白文字（半角スペース）は無視されます。	文字列	diffie-hellman-group14-sha1
	ssh.disable.ciphers	エージェントレス接続（SSH）で無効化する Cipher をカンマ区切りで指定します。カンマの前後の空白文字（半角スペース）は無視されます。	文字列	3des-cbc,aes128-cbc,aes192-cbc,aes256-cbc
	ssh.disable.macs	エージェントレス接続（SSH）で無効化する MAC をカンマ区切りで指定します。カンマの前後の空白文字（半角スペース）は無視されます。	文字列	hmac-sha1,hmac-sha1-96,hmac-sha1-etm@openssh.com

カテゴリー	キー名	設定	値	デフォルト値
SSH 暗号アルゴリズム	ssh.disable.publicKeyAlgorithms	エージェントレス接続（SSH）で無効化するホスト鍵の公開鍵アルゴリズムをカンマ区切りで指定します。カンマの前後の空白文字（半角スペース）は無視されます。	文字列	""（null 文字）
TLS	tls.client.cipherSuites	Common Services および Web サービス接続先に接続する際に使用する Cipher Suites をカンマ区切りで指定します。TLS1.2 および TLS1.3 の Cipher Suites を指定できます。カンマの前後の空白文字（半角スペース）は無視されます。	文字列	なし※2
汎用コマンド リモートコマンド ファイル転送 ターミナル接続	plugin.stdoutSize.wmi	標準出力および標準エラーの合計サイズがプロパティ値を超えると、部品エラーが発生します。 注：プロパティ値の単位はキロバイト（KB）です。 次の条件が当てはまる場合、部品操作時にこのプロパティが適用されます。 - 接続先のホストが Windows - 実行対象の部品が汎用コマンド実行部品またはカスタム部品 Windows では、改行数が 65535 以上でも、部品は実行を続けることができます。この機能の特徴を生かすには、プロパティ値を適切に設定する必要があります。例えば、このプロパティが 100 KB に設定（デフォルト値）されている場合は、部品は改行の最大数 65535 以上を処理できません。部品は、最大 100 KB に達すると実行を停止します。	1～1024	100
	plugin.stdoutSize.ssh	標準出力および標準エラーの合計サイズがプロパティ値を超えると、部品エラーが発生します。 注：プロパティ値の単位はキロバイト（KB）です。 次の 2 つの主要な条件が当てはまる場合、部品操作時にこのプロパティが適用されます。 [条件（1）（注：次の対象の条件を満たす必要があります。）] - 接続先のホストが Linux。	1～1024	100

カテゴリー	キー名	設定	値	デフォルト値
汎用コマンド リモートコマンド ファイル転送 ターミナル接続	plugin.stdoutSize.ssh	- 実行対象の部品が汎用コマンド実行部品またはカスタム部品。 [条件（2）（注：次のプロトコル条件と部品の条件を満たす必要があります。)] - 接続プロトコルが SSH。 - 実行対象の部品がターミナル接続部品またはターミナルコマンド実行部品。	1～1024	100
	plugin.stdoutSize.telnet	標準出力および標準エラーの合計サイズがプロパティ値を超えると、部品エラーが発生します。 注：プロパティ値の単位はキロバイト（KB）です。 次の条件が当てはまる場合、部品操作時にこのプロパティが適用されます。 - 接続プロトコルが SSH。 - 対象の部品がターミナル接続部品またはターミナルコマンド実行部品。	1～1024	100
	plugin.remoteFileAccess.retry.times	カスタム部品またはファイル転送部品によって内部実行されるファイル操作コマンドの再試行回数を指定します。再試行間隔は 100ms に固定されています。 一時的なファイルアクセスエラーが発生した場合、コマンドを再試行すると操作が成功することがあります。ただし、ファイルアクセスエラーが回復しなかった場合、部品が終了するまで、再試行に余分な時間がかかります。ディスクに問題がない場合でもファイルアクセスエラーが発生する環境では、このプロパティを指定してください。	0～100	0
	ssh.privateKeyFile	SSH 接続に公開鍵認証が使用される場合、秘密鍵ファイルの絶対パスを指定します。	0～255 文字	""（null 文字）
	plugin.localMode	ローカル実行モードを有効にするか無効にするかを指定します。 true：有効 false：無効	true/false	true

カテゴリー	キー名	設定	値	デフォルト値
ターミナル接続	plugin.terminal.prompt.account	ユーザー ID 待機状態の検出に使用される正規表現を指定します。(1～1,024 文字) 標準出力および標準エラー出力が指定された正規表現に一致した場合、ターミナル接続部品（プロトコルとして Telnet が指定される）は、ユーザー ID が入力されなければならないと判断して、ユーザー ID を入力します。	正規表現パターンで使用できる文字列。	login|Login Name|Username|UserName
	plugin.terminal.prompt.password	パスワード待機状態の検出に使用される正規表現を指定します。(1～1,024 文字) 標準出力および標準エラー出力が指定された正規表現に一致した場合、ターミナル接続部品（プロトコルとして Telnet が指定される）は、パスワードが入力されなければならないと判断して、パスワードを入力します。	正規表現パターンで使用できる文字列。	password|Password|PassWord
	telnet.connect.wait	対象機器との Telnet 接続が確立された後、標準出力が戻るまでの待ち時間（秒数）を指定します。	1～600	60
リモートコマンド	plugin.remoteCommand.executionDirectory.wmi	対象ホストの OS が Windows の場合に実行するカスタム部品を含む、実行フォルダーのパスを指定します。実行フォルダーは、事前に作成しておく必要があります。 カスタム部品の［実行モード］が［スクリプト］の場合、指定された値とスクリプトファイル名の合計文字列長は最大 140 文字です。長さが 140 文字を超えた場合、スクリプトの転送は失敗します。さらに、スクリプトファイル名は 90 文字以内で指定しなければならないため、この指定値は 50 文字以内でなければなりません。	0～128 文字の文字列	""（null 文字）
	plugin.remoteCommand.executionDirectory.ssh	対象ホストの OS が Linux の場合にカスタム部品を実行する実行ディレクトリーのパスを指定します。実行ディレクトリーは、事前に作成しておく必要があります。	0～128 文字の文字列	""（null 文字）

カテゴリー	キー名	設定	値	デフォルト値
リモートコマンド	plugin.remoteCommand.workDirectory.ssh	対象ホストの OS が Linux の場合、ファイル転送部品またはカスタム部品の実行時に使用される作業ディレクトリーを指定します。ディレクトリーまたはシンボリックリンクを絶対パスとして入力します（1～128 文字）。さらに、シンボリックリンクはパスのレイヤーとして含めることができます。	1～128	/tmp/Hitachi_AO
リモートホスト接続の再試行	ssh.connect.retry.times	対象機器への SSH 接続が失敗した場合の再試行回数を指定します。	0～100	3
	ssh.connect.retry.interval	対象機器への SSH 接続が失敗した場合の再試行間隔（秒数）を指定します。	1～600	10
	wmi.connect.retry.times	対象機器への WMI 接続が失敗した場合の再試行回数を指定します。	0～100	3
	wmi.connect.retry.interval	対象機器への WMI 接続が失敗した場合の再試行間隔（秒数）を指定します。	1～600	10
	telnet.connect.retry.times	対象機器への Telnet 接続が失敗した場合の再試行回数を指定します。	0～100	3
	telnet.connect.retry.interval	対象機器への Telnet 接続が失敗した場合の再試行間隔（秒数）を指定します。	1～600	10
メール通知の再試行	mail.notify.retry.times	メールを送信する通知機能が失敗した場合の再試行回数を指定します。	0～100	3
	mail.notify.retry.interval	メールを送信する通知機能が失敗した場合の再試行間隔（秒数）を指定します。	1～600	10
	mail.plugin.retry.times	メール通知部品でのメール送信が失敗した場合の再試行回数を指定します。	0～100	3
	mail.plugin.retry.interval	メール通知部品でのメール送信が失敗した場合の再試行間隔（秒数）を指定します。	1～600	10
監査ログ	logger.Audit.command.useLoginUserID	コマンドが実行されるときの監査ログのサブジェクト識別情報に、ユーザー ID として Ops Center	true/false	false

カテゴリー	キー名	設定	値	デフォルト値
監査ログ	logger.Audit.command.useLoginUserID	Automator のログインユーザー ID を出力するかどうかを指定します。	true/false	false
画面の更新	client.events.refreshinterval	イベントの更新間隔（秒数）を指定します。	0～65535	5
Service Builder	client.editor.upload.maxfilesize	[Service Builder Edit] 画面で、Ops Center Automator の操作に使用される端末からサーバーにアップロードできる最大ファイルサイズ（MB 単位）を指定します。	1～10	3
	client.editor.canvas.maxwidth	[フロー] ビューの幅の最大サイズ（px 単位）を指定します。	3600～10000	3600
	client.editor.canvas.maxhigh	[フロー] ビューの高さの最大サイズ（px 単位）を指定します。	2400～30000	2400
	client.editor.sso.timeout.disable	Common Services での [自動更新] の設定に関わらず、[フロー参照] 画面を除く Service Builder、[外部リソースプロバイダ作成] 画面、および [外部リソースプロバイダ編集] 画面でのアイドルタイムアウトを無効にするかを指定します。 true：アイドルタイムアウトしない false：アイドルタイムアウトする	true/false	false
	server.editor.step.perTemplate.maxnum	サービステンプレートあたりの最大ステップ数を指定します。	320～40000	320
	server.editor.step.perLayer.maxnum	レイヤーあたりの最大ステップ数を指定します。	80～10000	80
	server.editor.publicProperty.perTemplate.maxnum	サービステンプレートあたりのサービスプロパティの最大数を指定します。	100～2000	1000
	server.editor.propertyGroup.perTemplate.maxnum	サービステンプレートあたりのプロパティグループの最大数を指定します。	5～1000	500
デバッガー	tasklist.debugger.autodelete.taskRemainingPeriod	サービステンプレートあたりのプロパティグループの最大数を指定します。	1～90	7
	client.debugger.tasklog.maxfilesize	[タスクログ] タブに表示されるタスクログのサイズ（KB）を指定します。	4～10240	1024

カテゴリー	キー名	設定	値	デフォルト値
デバッガー	logger.debugger.TA.MaxFileSize	デバッグタスクの最大ログファイルサイズ（KB）を指定します。	4～2097151	10240
長期実行中のタスクのチェック間隔しきい値	server.longRunning.check.interval	長期実行中のタスクのチェック間隔しきい値（分数）	0～20160	2880
長期実行中の監視間隔	server.longRunning.monitor.interval	長期実行中の監視間隔（秒数）	1～3600	60
Web クライアント	plugin.http.connect.timeout	HTTP/HTTPS 接続が確立されるときのタイムアウト値（秒数）を指定します。0 を指定した場合、タイムアウトは発生しません。	0～3600	60
	plugin.http.read.timeout	HTTP/HTTPS 接続の確立後、データが読み込まれるときのタイムアウト値（秒数）を指定します。0 を指定した場合、タイムアウトは発生しません。	0～86400	600
部品実行	plugin.threadPoolSize	部品の最大同時実行数を指定します。 製品同梱のサービステンプレートのみを使用する場合、本プロパティ値を 100 に設定して運用が可能です。カスタムサービステンプレートを使用する場合は、デフォルト値から変更後、必ず評価を行い、問題が発生しないことを確認してから、本番運用に移行してください。	1～100	10
SSO	sso.https.certification	Common Services との SSL 通信において、証明書の有効性を検証するかどうかを指定します。	true/false	false
SSH ファイル転送プロトコル	plugin.sftp.enable	ファイル転送部品およびカスタム部品で、SSH を用いてファイルを送受信する際に、SFTP を使用するかどうかを指定します。 true：SFTP を使用 false：SCP を使用	true/false	false

注※1　タスクのログ出力しきい値は、サービス共有プロパティで設定します。

例：

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

mail.plugin.retry.interval = 10

client.events.refreshinterval = 5

注※2　`tls.client.cipherSuites` はデフォルトでは行の記載がありません。

Ops Center Automator は次の Cipher Suites が設定されているものとして動作します。

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

`tls.client.cipherSuites` の行が存在しない場合は行を追加して、使用したい Cipher Suites を設定してください。使用できる Cipher Suites については、「付録 D.2　クライアントとしてサポートする Cipher Suites」を参照してください。

3.5　パフォーマンスモードを設定する

Ops Center Automator には、スタンダードモードとハイパフォーマンスモードの 2 つの動作モードがあります。ハイパフォーマンスモードは、複数のタスクの実行に適しており、スタンダードモードよりも多くのリソースを使用します。

スタンダードモードとハイパフォーマンスモードを切り替えるには、changemode コマンドを使用します。このコマンドの詳細は、「7.2.2　changemode コマンド」を参照してください。

メモ

複数の Online Migration with Configuration Manager タスクを実行する場合は、ハイパフォーマンスモードで操作する必要があります。詳細については、『Hitachi Ops Center Automator ユーザーズガイド』を参照してください。

3.6 メール通知を構成する

メール通知設定を構成し、タスクの実行が失敗または異常検出した場合に、メール通知を受信するようにします。メールアドレス、件名、障害や問題について受信する情報のタイプを構成できます。

> **メモ**
>
> システムのメール通知を有効にするには、[管理] タブでシステム・パラメーターを設定する必要があります。詳細については、『Hitachi Ops Center Automator ユーザーズガイド』を参照してください。

メール定義ファイル、mailDefinition は XML 形式です。次の場所に格納されています。

<Ops Center Automatorのインストールフォルダー>¥conf
定義ファイルは、次の形式を使用します。

```
<?xml version="1.0" encoding="UTF-8" standalone="yes" ?>
<mail xmlns="http://www.example.com/products/it/software/xml/automation/">
<title><メールタイトル></title>
<body><メール本文></body> </mail>
```

ファイルを編集するときには、次のことに注意してください。

- メール通知の定義ファイルがない場合や整形式 XML でない場合、読み取りエラーが発生します。この場合、メールはデフォルトの件名と本文で送信されます。
- <mail>、<title>、および<body>の外部でタグを指定した場合、タグが整形式 XML であっても、タグとその内容は無視されます。
- <title>または<body>タグの値が省略された場合には、空の文字列が指定されます。
- <mail>タグを省略することはできません。省略した場合、形式は無効であり、読み取りエラーが発生します。
- すべてのエントリーで大文字と小文字が区別されます。

設定を変更するには、mailDefinition ファイルのメールの件名およびメール本文のセクションを編集します。

表 3-2 メール通知設定

設定	XML 要素	文字列長	デフォルト値
メール通知に使用されるメールの件名	<title>	0～9,999 バイトの文字列	[Ops Center Automator] $TASK_NAME$が $TASK_STATUS$に変更されました。
メール通知に使用されるメールの本文	<body>	0～9,999 バイトの文字列	サービスグループ名：$SERVICE_GROUP_NAM

設定	XML 要素	文字列長	デフォルト値
メール通知に使用されるメールの本文	<body>	0～9,999 バイトの文字列	E$ タスク名：$TASK_NAME$ 実行者：$USER_NAME$ タスク詳細：$TASK_DETAIL_ URL$

表 3-3　XML エンティティー参照

メールに表示する文字	入力する文字
&	&amp;
<	<
>	>
"	"
'	'

表 3-4　メール通知に埋め込まれる文字

埋め込まれる文字	項目	備考
$SERVICE_GROUP_NAME$	サービスグループ名	サービスグループ名を表す文字列が設定されます。
$TASK_NAME$	タスク名	タスクのプロパティの形式に従ってタスク名が設定されます。
$TASK_ID$	タスク ID	なし
$TASK_KIND$	タスク種別	
$SERVICE_NAME$	サービス名	
$TASK_TAGS$	タスクのタグ	
$TASK_STATUS$	タスクの状態	
$EXECUTION_DATE$	実行操作日時	
$PLANNED_START_DATE$	開始予定日時	
$START_DATE$	開始日時	
END_DATE	終了日時	
$SCHEDULE_PERIOD$	定期実行周期	
$SCHEDULE_TIME$	定期実行時刻	
$SCHEDULE_ START_DATE$	定期実行適用開始日	
$USER_NAME$	実行者	
$TASK_DETAIL_URL$	［タスク詳細］画面の URL	http で始まる URL が設定されます。

3.7　エージェントレス接続の対応 OS

次の OS およびバージョンを、エージェントレス接続の操作対象機器として利用できます。

操作対象機器の OS が Windows の場合は SMB および RPC、Linux の場合は SSH を使用して機器に接続します。ターミナル接続部品を使用して操作対象機器に接続する場合は、Telnet または SSH を使用します。

- Windows の場合：
  - Windows Server 2016 Standard (x64)
  - Windows Server 2016 Datacenter (x64)
  - Windows Server 2019 Standard (x64)
  - Windows Server 2019 Datacenter (x64)
  - Windows Server 2022 Standard (x64)
  - Windows Server 2022 Datacenter (x64)

  Ops Center Automator から Windows ホストの操作対象機器への接続には次の SMB バージョンを使用します。

操作対象機器	SMB バージョン	暗号化通信
Windows	v1、v2、v3	できる※

  注※　Ops Center Automator および操作対象機器で SMB バージョン v2 または v3 が有効かつデータアクセスの暗号化の設定が有効な場合、通信は暗号化されます。使用可能な暗号アルゴリズムは使用する Ops Center Automator および操作対象機器によって異なります。
- Linux の場合：
  - Red Hat Enterprise Linux 8.6、8.8 (x64)
  - Red Hat Enterprise Linux 9.2 (x64)
  - Oracle Linux 8.6、8.8 (x64)
  - Oracle Linux 9.2 (x64)

  カスタム部品、汎用コマンド実行部品、ファイル転送部品が操作対象機器の OS で指定されたコマンド以外で、各部品が実行するコマンドを次に示します。部品を使用する場合、各コマンドがインストール済みである必要があります。
  - カスタム部品
    `/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`
  - 汎用コマンド実行部品
    `/bin/bash`、`/usr/bin/id`、`/bin/echo`、`/usr/bin/test`、`/bin/uname`、`/bin/su`
  - ファイル転送部品（送信：部品プロパティ transferMode の値が send の場合）

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

- ファイル転送部品（受信：部品プロパティ transferMode の値が receive の場合）
  /bin/bash、/usr/bin/id、/usr/bin/test、/bin/mkdir、/bin/chmod、/usr/bin/zip、/bin/rm、/bin/uname、/bin/su

カスタム部品とファイル転送部品では、SCP または SFTP にて操作対象機器にファイルを転送します。操作対象の機器は、SCP または SFTP でファイル転送可能な環境にしてください。なお、操作対象の機器が Linux で、接続するユーザーの.bashrc で文字列を出力している場合は、SCP でのファイル転送が失敗するおそれがあります。また、エージェントレス接続先に Telnet または SSH で接続する場合、接続ユーザーのログインスクリプトに対話環境が前提である stty、tty、tset、script コマンドなどを記載しないでください。記載されている場合は、ログインスクリプトを変更する、または、これらのコマンドを実行しないログインスクリプトを使用するユーザーを新たに作成してください。

3.8 操作対象機器との接続に使用される情報を構成する

Ops Center Automator の部品およびサービスが、部品によるタスクが実行され、アクションが実施されるリモートマシンと通信できるようになる前に、リモートマシン接続情報を構成する必要があります。

開始する前に、以下のことを確認してください。

- 次のパスにあるすべてのファイルは、接続先プロパティファイルとみなされます。
  ＜Ops Center Automatorのインストールフォルダー＞¥conf¥plugin¥destinations
- ファイル名は、次の形式を使用します。
  ＜ホスト名＞.properties, *＜IPv4アドレス＞*.properties, *＜IPv6アドレス＞*.properties

> **メモ**
>
> IPv6 アドレス内のコロン「:」はファイル名には使用できないため、ダッシュ（-）に置き換えます。例：2001::234:abcd -> 2001--234-abcd.properties.

サンプルファイルは、次の場所にあります。

＜Ops Center Automatorのインストールフォルダー＞¥conf¥plugin¥destinations¥#sample.properties
プロパティファイルを編集するときには、次のことに注意してください。

- #で始まる行は、コメントとして扱われます。
- 空白行は無視されます。
- エンコードは ISO 8859-1 です。
- 内容は大文字と小文字が区別されます。
- 文字列の中で¥を指定するには、¥¥と入力する必要があります。
- 接続先プロパティファイルで無効な値を指定した場合、接続先プロパティファイルを参照する部品で実行エラーが発生します。
- 1 つのファイル内で同じ指定キーを複数回入力した場合は、最後に指定したキーが有効になります。
- 接続先プロパティファイルを編集した場合、そのファイルを参照する部品が実行されると、新しい定義が適用されます。

対象機器に接続するには、以下の構成情報を使用してください。

対象機器がクラスター環境の一部である場合のガイドライン

クラスターの対象機器に情報を入力する場合：

- 対象機器が Windows のクラスター環境である場合は、作業フォルダー（wmi.workDirectory.sharedName および wmi.workDirectory.sharedPath）を設定する必要があります。設定しないと、部品が接続エラーの原因となります。

- カスタム部品でスクリプトを実行する場合は、実行フォルダー（common.executionDirectory）を指定する必要があります。指定しないと、スクリプトは転送されません。

キー名	設定	有効値	最小値	最大値
terminal.charset	通信に使用される文字セットを指定します。	EUC-JP eucjp ibm-943C ISO-8859-1 MS932 PCK Shift_JIS UTF-8 windows-31j	-	-
telnet.port	ターミナル接続部品での Telnet 接続に使用されるポート番号を指定します。この設定は、プロパティファイル（config_user.properties）の telnet.port.number 設定に優先します。	0～65535	0	65535
ssh.port	次のどれかの部品を使用して、SSH 接続に使用されるポート番号を指定します： • 汎用コマンド実行部品 • ファイル転送部品 • ターミナル接続部品 • カスタム部品 この設定は、プロパティファイル（config_user.properties）の ssh.port.number 設定に優先します。	0～65535	0	65535
telnet.prompt.account	ターミナル接続部品を使用して対象機器との接続を確立する際に出力されるユーザー ID の入力を求める文字列の検出に使用する、正規表現パターンを指定します。1～1,024 文字を使用できます。例えば、「Username:」と指定します。	正規表現パターンで使用される文字列	1 文字	1024 文字
telnet.prompt.password	ターミナル接続部品を使用して対象機器との接続を確立する際に出力されるパスワードの入力を求める文字列の検出に使用する、正規表現パターンを指定します。1～1,024 文	正規表現パターンで使用される文字列	1 文字	1024 文字

キー名	設定	有効値	最小値	最大値
telnet.prompt.password	字を使用できます。例えば、「Password:」と指定します。	正規表現パターンで使用される文字列	1 文字	1024 文字
telnet.noStdout.port.list	ターミナル接続部品を使用して接続が確立された後に標準出力を返さないサービスのポート番号を指定します。1～1,024 文字を使用できます。複数のポート番号を指定するには、区切り文字としてコンマを使用します。	0～65535 とコンマ（,）	1 文字	1024 文字
wmi.workDirectory.sharedName	Windows 対象機器のプロパティです。対象でのコマンド実行時にファイルが送信される共有フォルダーの共有フォルダー名を指定します。フォルダーは wmi.workDirectory.sharedPath と同じである必要があります。このプロパティを使用する場合、対象の管理共有設定は不要です。0～80 文字の文字列を指定します。	1 バイトの英数字、「-」、「_」、および「.」。	0 文字	80 文字
wmi.workDirectory.sharedPath	Windows 対象機器のプロパティです。対象でのコマンド実行時にファイルが送信される共有フォルダーの絶対パスを指定します。汎用コマンド実行部品を使用している場合、実行フォルダーは、このプロパティにリストされるパスの下の¥Hitachi¥CMALib¥HAD¥home になります。フォルダーは wmi.workDirectory.sharedName と同じである必要があります。このプロパティを使用する場合、対象の管理共有設定は不要です。0～80 文字の文字列を指定します。	1 バイトの英数字、「:」、「¥」、「-」、「_」、および「.」。	0 文字	80 文字
ssh.workDirectory	Linux 対象機器のプロパティです。ファイル転送部品またはカスタム部品で転送用ファイルが置かれるディレクトリーの絶対パスを指定します。このプロパティで指定されたパスも、親ディレクトリーのパスも、ファイル転送部品の接	1 バイトの英数字、「/」、「-」、「_」、および「.」。	0 文字	128 文字

キー名	設定	有効値	最小値	最大値
ssh.workDirectory	続先および受信先として指定することはできません。作業フォルダーには、接続するユーザーの読み取り権限、書き込み権限、および実行権限が必要です。ファイル転送部品またはカスタム部品が使用されるときに、このプロパティで指定されたパスが存在しなかった場合、部品の実行時に作成されます。ディレクトリーを作成できない場合、部品の実行は異常終了します。新しいディレクトリーのアクセス権限は、必ず 777 であることを確認してください。優先されるのは、プロパティファイル（config_user.properties）で定義された plugin.remoteCommand.workDirectory.ssh の値です。0～128 文字の文字列を指定します。	1 バイトの英数字、「/」、「-」、「_」、および「.」。	0 文字	128 文字
common.executionDirectory	対象に対してカスタム部品を実行するときの実行フォルダーを指定します。部品定義で定義された実行フォルダーの値が設定されていなかった場合、このプロパティの値が適用されます。優先されるのは、プロパティファイル（config_user.properties）で定義された plugin.remoteCommand.executionDirectory.wmi と plugin.remoteCommand.executionDirectory.ssh の値です。0～128 文字の文字列を指定します。	任意の文字列	0 文字	128 文字
sftp.enable	ファイル転送部品およびカスタム部品で、SSH を用いてファイルを送受信する際に、SFTP を使用するかどうかを指定します。この設定は、プロパティファイル（config_user.properties）の plugin.sftp.enable よりも優先されます。	true/false	-	-

キー名	設定	有効値	最小値	最大値
sftp.enable	true：SFTP を使用 false：SCP を使用	true/false	-	-

3.9 エージェントレス接続の Windows 前提条件

エージェントレス接続を使用するには、以下に記載されている Windows の前提条件が必要です。

サポートされるユーザー

エージェントレス接続では、次のユーザーを使用できます。

- ビルトイン Administrator
- Active Directory のビルトイン Administrator
- Administrators グループに属するユーザー
- Active Directory の Domain Admin グループに属するユーザー

Administrators グループに属するユーザーを使用する場合は、コマンド実行時に UAC（ユーザーアクセス制御）昇格が適用されないことに注意してください。

レジストリーを編集する必要があります。レジストリーエディターを使用して、次のレジストリーのキーのエントリーを設定します。

メモ

OS を再起動する必要はありません。

項目	値
レジストリーキー	HKEY_LOCAL_MACHINE¥SOFTWARE¥Microsoft¥Windows¥CurrentVersion¥Policies¥System
レジストリーエントリー	LocalAccountTokenFilterPolicy
レジストリーエントリーとして設定される値	1 (DWORD)

必要に応じて、コマンドプロンプトで次のコマンドを入力できます。

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

管理共有設定

管理共有を使用するために、レジストリーエディターで次のレジストリーのキーの下にエントリーを設定し、OS を再起動します。

項目	値
レジストリーキー	HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Services¥Lanmanserver¥parameters

項目	値
レジストリーエントリー	AutoShareServer
レジストリーエントリーとして設定される値	1 (DWORD)

コマンドプロンプトで次のコマンドを入力します。

```
reg add HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Services¥Lanmanserver¥parameters /v Auto
ShareServer /t REG_DWORD /d 1
```

3.10　エージェントレス接続の SSH 前提条件

エージェントレス接続を使用するには、以下に記載されている SSH プロトコル前提条件が必要です。

SSH 前提条件は次の部品で必要です。

- カスタム部品
- 汎用コマンド実行部品
- ファイル転送部品
- ターミナル接続部品
- ターミナルコマンド実行部品
- ターミナル切断部品

> **メモ**
>
> SSH はバージョン 2 をサポートする必要があります。

3.10.1　パスワード認証

SSH サーバーに対するパスワード認証を、次のように設定する必要があります。

1. リモート操作対象ホストに root としてログインします。
2. sshd_config ファイルを開きます。
   /etc/ssh/sshd_config
3. PasswordAuthentication の値を yes に設定します。PasswordAuthentication の行がコメントアウトされている場合は、コメントアウトの番号記号（#）を削除します。
4. 次のコマンドを実行して、sshd サービスを再起動します。

```
systemctl restart sshd
```

> **メモ**
>
> このコマンドは、OS のバージョンによって変わることがあります。追加情報については、該当する OS のマニュアルを参照してください。

3.10.2　公開鍵認証

ここでは、SSH サーバーに接続する公開鍵を認証する方法について説明します。

SSH サーバーのセットアップ

公開鍵認証を使用するには、SSH サーバーに対する公開鍵認証を設定する必要があります。

1. リモート操作対象ホストに root としてログインします。
2. sshd_config を開きます。
   /etc/ssh/sshd_config
3. PubkeyAuthentication の値を yes に設定します。PubkeyAuthentication の行がコメントアウトされている場合は、コメントアウトの番号記号（#）を削除します。
4. 次のコマンドを実行して、sshd サービスを再起動します。

```
systemctl restart sshd
```

> **メモ**
>
> このコマンドは、OS のバージョンによって変わることがあります。追加情報については、該当する OS のマニュアルを参照してください。

鍵の作成（初回）

公開鍵と秘密鍵を作成します。鍵は、Ops Center Automator がインストールされる OS 上で作成することを推奨します。

公開鍵認証でサポートする鍵種別と鍵長は下記の通りです。なお、秘密鍵の形式は OpenSSH 形式と PEM 形式をサポートしています。

鍵種別	鍵長（bits）
DSA	1,024
ECDSA	256、384、521
ED25519	256
RSA	1,024～16,384

> **メモ**
>
> 複数の暗号アルゴリズムが 1 つの鍵種別に対応する RSA 鍵の場合、3 つの公開鍵アルゴリズム（rsa-sha2-256、rsa-sha2-512、ssh-rsa）のうち、接続する Linux ホストで使用できる最も安全な暗号アルゴリズムが自動的に使用されます。

参考として、以下に鍵を作成する手順を示します。

1. ssh-keygen コマンドを実行します。
   実行例を次に示します。
   DSA 鍵を作成する場合：ssh-keygen -t dsa
   ECDSA 鍵を作成する場合：ssh-keygen -t ECDSA
   ED25519 鍵を作成する場合：ssh-keygen -t ed25519
   RSA 鍵を作成する場合：ssh-keygen -t rsa

   > **メモ**
   >
   > このコマンドは、OS のバージョンによって変わることがあります。追加情報については、該当する OS のマニュアルを参照してください。

2. 秘密鍵の場所と名前を決めます。
   マルチバイト文字を含まないパスとファイル名を指定します。デフォルトでは、~/.ssh/id_rsa が設定されます（RSA 鍵を作成する場合）。秘密鍵は、選択されたパスに対して指定されたファイル名として設定されます。公開鍵は、秘密鍵と同じディレクトリーに、秘密鍵の名前に「.pub」ファイル拡張子を付けたファイルとして設定されます。
3. パスフレーズを入力します。
   パスフレーズを入力して、[Enter] キーを押すように求められます。次に、パスフレーズの再入力を求められます。秘密鍵のパスフレーズを設定しない場合は、パスフレーズを入力せずに [Enter] キーを押します。

Ops Center Automator への秘密鍵の配置

1. Ops Center Automator がインストールされた OS 上の任意の場所に秘密鍵を配置します。
2. プロパティファイル（config_user.properties）のssh.privateKeyFile に秘密鍵のパスを設定します。パスを指定する際、シンボリックリンクまたはジャンクションポイントを指定しないでください。パスは絶対パスで指定してください。
3. hcmds64srv コマンドを実行して、Ops Center Automator および共通コンポーネントを使用するすべての製品のサービスを再起動します。

リモート対象ホストへの公開鍵の配置

1. cat コマンドの出力をリダイレクトし、生成された公開鍵ファイルの内容を、認証に使用される公開鍵ファイル（authorized_keys）に追加します。(例：cat id_rsa.pub >> authorized_keys)
2. chmod コマンドを実行して、authorized_keys の属性を 600 に変更します（書き込みおよび読み取り権限を所有者にのみ与えます)。属性が 600 でない場合、部品実行時に認証が失敗することがあります。デフォルトでは、authorized_keys の配置場所は、~/.ssh の直下になっています。~/.ssh に関しては、属性を 700 に変更します（書き込み、読み取り、および実行権限を所有者にのみ与えます)。

shared property の構成

1. Ops Center Automator アプリケーションにログインします。
2. [管理] － [サービス共有プロパティ] を選択します。

3. 秘密鍵のパスフレーズを開きます（SSH 公開鍵認証の場合）。
4. 値としてパスフレーズを入力します。
   値は、秘密鍵のパスフレーズです（SSH 公開鍵認証の場合）。

3.10.3　キーボードインタラクティブ認証

キーボードインタラクティブ認証を使用するには、認証を SSH サーバーに設定する必要があります。

1. リモート対象ホストに root としてログインします。
2. sshd_config を開きます。
   /etc/ssh/sshd_config
3. 次のようにキーボードインタラクティブ認証を設定します。
   - ChallengeResponseAuthentication の値を yes に設定します。（ChallengeResponseAuthentication の行がコメントアウトされている場合は、コメントアウトの番号記号（#）を削除します。）
   - UsePAM の値を yes に設定します。（UsePAM の行がコメントアウトされている場合は、コメントアウトの番号記号（#）を削除します。）
4. 次のコマンドを実行して、sshd サービスを再起動します。

```
systemctl restart sshd
```

メモ

このコマンドは、OS のバージョンによって変わる場合があります。詳細については、該当する OS のマニュアルを参照してください。

3.10.4　暗号アルゴリズムを無効化する

Ops Center Automator ではconfig_user.properties ファイルの設定を行うことで SSH 接続に使用する暗号アルゴリズムを無効にすることができます。詳細は、「3.4　システム構成を変更する」を参照してください。

Ops Center Automator がサポートする暗号アルゴリズムは、「付録 E.1　サポートする暗号アルゴリズム一覧」を参照してください。

メモ

SSH 接続で暗号アルゴリズムのネゴシエーションに失敗した場合、メッセージKNAE02137-E で詳細情報に暗号アルゴリズムのネゴシエーションに失敗したことが表示され、接続テストに失

敗します。また、公開鍵認証使用時に指定された秘密鍵から決まる公開鍵アルゴリズムが接続先で無効な場合は、メッセージKNAE02137-E で詳細情報に認証エラーが表示され、接続テストに失敗します。Ops Center Automator サーバーと接続先 Linux ホスト間で使用できる有効な暗号アルゴリズムが存在するか確認してください。

3.11 Configuration Manager で Java ヒープメモリーサイズを設定する

複数の Online Migration with Configuration Manager タスクを実行する場合、Configuration Manager が使用する Java ヒープのサイズを 6,144MB に変更する必要があります。

前提条件

Administrator 権限のユーザーとして、Configuration Manager がインストールされているサーバーにログインします。

ヒント

次の場所に格納されているStartupV.properties ファイルのrest.java.heapMemory.size プロパティの値を確認することで、現在設定されている値を確認できます。

```
＜Configuration Managerのインストールフォルダー＞¥data¥properties¥StartupV.properties
```

このファイルが存在しない場合、またはファイルにrest.java.heapMemory.size プロパティが含まれていない場合は、デフォルト値が設定されていることを示しています。

操作手順

1. 次のコマンドを実行します。

```
＜Configuration Managerのインストールフォルダー＞¥bin¥setProperty rest.java.heapMemory.size 6144
```

このコマンドを実行すると、Configuration Manager が再起動します。コマンドラインの最後に-noRestart を指定すると、サーバーを再起動せずにコマンドが実行されます。

setProperty コマンドを実行すると、StartupV.properties ファイルのrest.java.heapMemory.size プロパティの値が 6144 に変更されます。ファイルが存在しない場合は作成されます。

このコマンドを実行するたびに、現在のStartupV.properties ファイルがバックアップされます。バックアップファイルは同じディレクトリーに作成され、バックアップファイルの名前には作成日時が含まれます（例：StartupV_20200220-093320.properties）。

4 外部認証サーバーでのユーザー管理

ここでは、外部認証サーバーでユーザー認証を設定する方法について説明します。

4.1　外部認証サーバーでのユーザー管理

外部認証サーバー（LDAP または Kerberos）に登録したユーザーアカウントを使用して Ops Center Automator にログインできます。外部認証サーバーと連携するための設定は Common Services で行います。詳細は、『Hitachi Ops Center インストールガイド』の Active Directory との連携について説明している箇所を参照してください。

5 Ops Center Automator をバックアップおよびリストアする

ここでは、Ops Center Automator をバックアップ、リストアする方法について説明します。

5.1 Ops Center Automator のバックアップとリストアの概要

Ops Center Automator では、障害が発生してシステムが壊れた場合などに備えてシステムのバックアップ、およびリストアができます。

ユースケース

- 定期バックアップ：通常の運用の中で障害に備えて定期的にバックアップします。障害が発生した場合にはバックアップデータをリストアすることで、障害から回復できます。
- 同一管理サーバー内での OS の再インストール：システム構成およびデータベース情報を引き継げます。
- 別ホストへの移動：バックアップ・リストアの機能を使用して、Ops Center Automator を別のホストに移動できます。システム構成およびデータベース情報も引き継げます。

Ops Center Automator は定期自動バックアップをサポートしていません。要件に合ったバックアップスケジュールを計画して、手動でバックアップを実施してください。

5.2 Ops Center Automator をバックアップする

Ops Center Automator のシステム構成およびデータベース情報をバックアップします。

前提条件

［タスク］タブで、実行中、応答待ち中、異常検出、長期実行中、または停止中を示す処理中のタスクがないことを確認します。

操作手順

1. Administrator 権限のユーザーとして、管理サーバーにログインします。
2. サービスを停止、またはフェイルオーバーを無効にします。

   非クラスター環境の場合：

   hcmds64srv /stop コマンドを実行して、Ops Center Automator および共通コンポーネントを使用するすべての製品のサービスを停止します。

   クラスター環境の場合：

   次のコマンドを使用して Ops Center Automator および共通コンポーネントを使用する製品のサービスが登録されるクラスターグループをオフラインにして、フェイルオーバーを無効にします。

   ```
   <共通コンポーネントのインストールフォルダー>¥ClusterSetup¥hcmds64clustersrvstate /soff /r <グループ名>
   ```

3. backupsystem コマンドを実行して、バックアップします。
4. サービスを起動、またはフェイルオーバーを有効にします。

   非クラスター環境の場合：

   hcmds64srv /start コマンドを実行して、Ops Center Automator および共通コンポーネントを使用するすべての製品のサービスを起動します。

   クラスター環境の場合：

   次のコマンドを使用して Ops Center Automator および共通コンポーネントを使用する製品のサービスが登録されるクラスターグループをオンラインにして、フェイルオーバーを有効にします。

   ```
   <共通コンポーネントのインストールフォルダー>¥ClusterSetup¥hcmds64clustersrvstate /son /r <グループ名>
   ```

5.3 Ops Center Automator をリストアする

バックアップされた Ops Center Automator のシステム構成およびデータベース情報をリストアします。

前提条件

- バックアップ元のホストとリストア先のホストで、次の項目が同じであることを確認してください。
  - ホスト名と IP アドレス
  - Ops Center Automator によって使用される OS ユーザーのアカウント
  - インストールされている Ops Center 製品の種類、バージョン、およびリビジョン
  - Ops Center Automator のインストールパス
  - システムロケールおよび文字コード
- ［タスク］タブで、実行中、応答待ち中、異常検出、長期実行中、または停止中を示す処理中のタスクがないことを確認してください。

操作手順

1. Administrator 権限のユーザーとして、管理サーバーにログインします。
2. サービスを停止、またはフェイルオーバーを無効にします。

   非クラスター環境の場合：

   `hcmds64srv /stop` コマンドを実行して、Ops Center Automator および共通コンポーネントを使用するすべての製品のサービスを停止します。

   クラスター環境の場合：

   次のコマンドを使用して Ops Center Automator および共通コンポーネントを使用する製品のサービスが登録されるクラスターグループをオフラインにして、フェイルオーバーを無効にします。

   ```
   <共通コンポーネントのインストールフォルダー>¥ClusterSetup¥hcmds64clustersrvstate /soff /r <グループ名>
   ```
3. `restoresystem` コマンドを実行して、リストアします。
4. バックアップ元で変更していた内容に合わせて、次の項目を設定します。

   メモ

   Ops Center Automator クラスター構成で運用している場合は、アクティブノードとスタンバイノードそれぞれでプロパティファイルを編集してください。

項目名	設定内容
監査ログ（`auditlog.conf`※1）	3.3.2　監査ログを有効にする

項目名	設定内容
ポート番号※2（user_httpsd.conf※3）	3.1.1　管理サーバーと管理クライアントとの通信に使用されるポート番号を変更するおよび 3.1.2　ポート番号を変更した場合に共通コンポーネントのプロパティを更新する
セキュア通信	3.2　セキュア通信を構成する
エージェントレス接続で使用する秘密鍵	3.10.2　公開鍵認証
パフォーマンスモード	3.5　パフォーマンスモードを設定する
警告バナー	7.1.1　hcmds64banner コマンド

注※1　バックアップ元のauditlog.conf ファイルは、次の場所に格納されています。

＜バックアップ先のフォルダー＞¥HBase¥base¥conf¥sec

注※2　デフォルトの設定から変更している場合に設定が必要です。

注※3　バックアップ元のuser_httpsd.conf ファイルは、次の場所に格納されています。

＜バックアップ先のフォルダー＞¥HBase¥base¥httpsd.conf

5. サービスを起動、またはフェイルオーバーを有効にします。

非クラスター環境の場合：

hcmds64srv /start コマンドを実行して、Ops Center Automator および共通コンポーネントを使用するすべての製品のサービスを起動します。

クラスター環境の場合：

次のコマンドを使用して Ops Center Automator および共通コンポーネントを使用する製品のサービスが登録されるクラスターグループをオンラインにして、フェイルオーバーを有効にします。

＜共通コンポーネントのインストールフォルダー＞¥ClusterSetup¥hcmds64clustersrvstate /son /r *＜グループ名＞*

5.4 Ops Center Automator を別のホストへ移動する

必要に応じて、Ops Center Automator を別のホストに移動できます。

> **メモ**
>
> 移動元のホスト名または IP アドレスと移動先のホスト名または IP アドレスが異なる場合は、管理サーバーのホスト名を変更する必要があります。

前提条件

「5.3 Ops Center Automator をリストアする」の前提条件を参照してください。

操作手順

1. Administrator 権限のユーザーとして、管理サーバーにログインします。
2. 移動元ホストで Ops Center Automator のバックアップを完了します。
   a. `hcmds64srv /stop` コマンドを実行して、現在のサービスを停止します。

   > **メモ**
   >
   > クラスター環境の場合、次のコマンドを実行して Ops Center Automator のサービスが登録されるグループをオフラインにして、フェイルオーバーを無効にします。
   >
   > ```
   > <共通コンポーネントのインストールフォルダー>¥ClusterSetup¥hcmds64clustersrvstate /soff /r <グループ名>
   > ```

   b. `backupsystem` コマンドを実行して、バックアップを実行します。
3. アーカイブされたバックアップファイルを移動先のホストに移動します。
4. 移動先のホストの管理サーバーにログインします。
5. 移動先のホストで、Ops Center Automator のリストアを実行します。
   a. `hcmds64srv /stop` コマンドを実行して、サービスを停止します。

   > **メモ**
   >
   > クラスター環境の場合、次のコマンドを実行して Ops Center Automator のサービスが登録されるグループをオフラインにして、フェイルオーバーを無効にします。
   >
   > ```
   > <共通コンポーネントのインストールフォルダー>¥ClusterSetup¥hcmds64clustersrvstate /soff /r <グループ名>
   > ```

   b. `restoresystem` コマンドを実行して、バックアップをリストアします。

c. 移動先の環境に合わせて、次の項目を設定します。

項目名	設定内容
監査ログ（auditlog.conf※1）	3.3.2　監査ログを有効にする
ポート番号※2（user_httpsd.conf※3）	3.1.1　管理サーバーと管理クライアントとの通信に使用されるポート番号を変更するおよび 3.1.2　ポート番号を変更した場合に共通コンポーネントのプロパティを更新する
セキュア通信	3.2　セキュア通信を構成する
エージェントレス接続で使用する秘密鍵	3.10.2　公開鍵認証
パフォーマンスモード	3.5　パフォーマンスモードを設定する
警告バナー	7.1.1　hcmds64banner コマンド

注※1　バックアップ元のauditlog.conf ファイルは、次の場所に格納されています。

＜バックアップ先のフォルダー＞¥HBase¥base¥conf¥sec

注※2　デフォルトの設定から変更している場合に設定が必要です。

注※3　バックアップ元のuser_httpsd.conf ファイルは、次の場所に格納されています。

＜バックアップ先のフォルダー＞¥HBase¥base¥httpsd.conf

6. Common Services から Ops Center Automator の登録を解除し、再び登録します。
   a. Ops Center Portal から Ops Center Automator の登録を解除します。
   b. setupcommonservice コマンドを実行し、Common Services に変更を適用します。
   c. 必要に応じて、ユーザーグループおよびサービスグループの権限を変更します。
7. hcmds64srv /start コマンドを実行して、サービスを起動します。

メモ

クラスター環境の場合、次のコマンドを実行して Ops Center Automator のサービスが登録されるグループをオンラインにして、フェイルオーバーを有効にします。

```
＜共通コンポーネントのインストールフォルダー＞¥ClusterSetup¥hcmds64clustersrvstate /son /r ＜グループ名＞
```

6 Ops Center Automator をアンインストールする

ここでは、Ops Center Automator をアンインストールする方法について説明します。

6.1 Ops Center Automator をアンインストールする

Ops Center Automator をアンインストールするには、次の手順に従います。

前提条件

- Ops Center Automator のタスクタブを確認して、タスクの状態が待機中、応答待ち中、実行中、長期実行中、異常検出のいずれかの状態になっているタスクがある場合には、タスクが停止または終了するまで待ちます。
- すべてのサービスダイアログボックスを閉じます。
- Windows のサービスまたは開いているコマンドプロンプトを閉じます。
- サーバー上のセキュリティー監視、ウイルス検出、またはプロセス監視ソフトウェアを無効にします。

> **注意**
>
> 共通コンポーネントを使用するほかの製品が同じホストにインストールされている場合は、共有フォルダー（¥Base64）を削除しないでください。このフォルダーを削除すると、共通コンポーネントを使用するほかの製品が正しく動作しなくなります。

操作手順

1. Administrator 権限のユーザーとして、管理サーバーにログインします。
2. 次のコマンドを実行して、すべてのサービスを停止します。

   ```
   <共通コンポーネントのインストールフォルダー>¥bin¥hcmds64srv /stop
   ```

3. [コントロールパネル] を開き、[プログラムと機能] または [プログラムのアンインストール] を選択します。
4. [Hitachi Ops Center Automator] を選択して [アンインストール] をクリックするか、プログラムを選択し、右クリックして [アンインストール] を選択します。
5. 画面の指示に従って、アンインストールを進めます。

   [アンインストール前の確認] 画面で [削除] をクリックすると、ソフトウェアのアンインストールプロセスが開始されます。
   アンインストールプロセスによって、Ops Center Automator のインストールフォルダーが削除されます。
6. Ops Center Portal から Ops Center Automator の登録を解除します。

操作結果

Ops Center Automator がホストからアンインストールされます。

Microsoft Visual C++ 2015-2019 Redistributable (x64)は、自動でアンインストールされません。同じホストにインストールされているほかのソフトウェアで使用していない場合は、プログラムを手動で削除できます。

6.2 クラスター環境で Ops Center Automator をアンインストールする

Ops Center Automator を別のサーバーに移行するか、運用を中止する場合には、クラスター環境のサーバーから Ops Center Automator ソフトウェアをアンインストールします。

> **メモ**
>
> Ops Center Automator をアンインストールした場合、プロパティファイル、ログファイル、その他の製品関連のファイルも削除されます。

操作手順

1. クラスター管理ソフトウェアで、Ops Center Automator サービスが登録されているグループをスタンバイノードからアクティブノードに移動します。グループを右クリックして［移動］を選択し、［ノードを選択］または［このサービスまたはアプリケーションを別のノードに移動］を選択します。

2. 次のコマンドを使用して、共通コンポーネントを使用する製品（Ops Center Automator を含む）のサービスが登録されているグループをオフラインにして、フェイルオーバーを無効にします。

   ```
   <共通コンポーネントのインストールフォルダー>¥ClusterSetup¥hcmds64clustersrvstate /soff
   /r <グループ名>
   ```

   r オプションには、共通コンポーネントを使用する製品（Ops Center Automator を含む）のサービスが登録されるグループの名前を指定します。グループ名にスペースが含まれる場合は、グループ名を引用符（"）で囲む必要があります。例えば、グループ名が Automator cluster の場合は、"Automator cluster"と指定します。

3. 次のコマンドを使用して、共通コンポーネントを使用する製品（Ops Center Automator を含む）のサービスを削除します。

   > **メモ**
   >
   > サービスを削除する前に、クラスター管理ソフトウェアからユーザースクリプトを削除します。

   ```
   <共通コンポーネントのインストールフォルダー>¥ClusterSetup¥hcmds64clustersrvupdate /sdel
   /r <グループ名>
   ```

   r オプションには、共通コンポーネントを使用する製品（Ops Center Automator を含む）のサービスが登録されるグループの名前を指定します。グループ名にスペースが含まれる場合は、グループ名を引用符（"）で囲む必要があります。例えば、グループ名が Automator cluster の場合は、"Automator cluster"と指定します。

メモ

- r オプションで指定されたグループに登録されているすべての Ops Center Automator と、共通コンポーネントを使用するほかの製品のサービスが削除されます。
- 共通コンポーネントを使用する製品を引き続き使用する場合は、Ops Center Automator を削除した後で再登録できます。Ops Center Automator サービスを削除しても、問題はありません。
  サービスリソース名を変更していた場合、サービスが再登録されるときに、すべてのリソース名が再初期化されます。したがって、削除するサービスのリソース名を記録しておき、それらのサービスの再登録後に名前を変更する必要があります。

4. 次のコマンドを使用して、Ops Center Automator および共通コンポーネントを使用するすべての製品のサービスを停止します。

```
<共通コンポーネントのインストールフォルダー>¥bin¥hcmds64srv /stop
```

5. アクティブノードから Ops Center Automator をアンインストールします。
6. アクティブノードで、不要になったファイルとフォルダー（クラスター環境でのインストール時に作成されたファイルとフォルダーなど）を削除します。
7. クラスター管理ソフトウェアで、Ops Center Automator services group をスタンバイノードに移動します。グループを右クリックして［移動］を選択してから、［ノードを選択］または［このサービスまたはアプリケーションを別のノードに移動］を選択します。
8. スタンバイノードから Ops Center Automator をアンインストールします。
9. クラスターインストールの削除を実行した後、Ops Center Automator フォルダーを削除して、共通コンポーネントを使用するほかの製品のサービスを使用しない場合は、スタンバイノードからBase64 フォルダーも削除します。
10. 以下のリソースが他のアプリケーションによって使用されていない場合は、クラスター管理ソフトウェアを使用して、それらをオフラインにしてから削除します。
    - IP アドレス
    - 共有ディスク
11. スタンバイノードで、不要になったファイルとフォルダー（クラスター環境でのインストール時に作成されたファイルとフォルダーなど）を削除します。
12. 共通コンポーネントを使用するほかの製品を引き続き使用する場合は、次のコマンドを使用して、共通コンポーネントを使用する製品のサービスをクラスター管理ソフトウェアグループに登録します。

```
<共通コンポーネントのインストールフォルダー>¥ClusterSetup¥hcmds64clustersrvupdate /sreg
 /r <グループ名> /sd <共有ディスクのドライブレター名> /ap <クライアントアクセスポイント用リソース名>
```

- /r
  共通コンポーネントを使用する製品のサービスを登録するグループの名前を指定します。グループ名にスペースが含まれる場合は、グループ名を引用符（"）で囲む必要があります。例えば、グループ名が Automator cluster の場合は、"Automator cluster"と指定します。
- /sd
  クラスター管理ソフトウェアに登録される共有ディスクのドライブ名を指定します。このオプションに対して複数のドライブ名を指定することはできません。共通コンポーネントを使用する製品のデータベースが複数の共有ディスクに分割されている場合は、各共有ディスクについて hcmds64clustersrvupdate コマンドを実行します。
- /ap
  クラスター管理ソフトウェアに登録されるクライアントアクセスポイント用リソースの名前を指定します。

13. 共通コンポーネントを使用するほかの製品を引き続き使用する場合は、次のコマンドを使用して、共通コンポーネントを使用するほかの製品のサービスが登録されるグループをオンラインにして、フェイルオーバーを有効にします。

```
<共通コンポーネントのインストールフォルダー>¥ClusterSetup¥hcmds64clustersrvstate /son /
r <グループ名>
```

r オプションには、共通コンポーネントを使用する製品のサービスが登録されるグループの名前を指定します。グループ名にスペースが含まれる場合は、グループ名を引用符（"）で囲む必要があります。例えば、グループ名が Automator cluster の場合は、"Automator cluster"と指定します。

14. クラスター管理ソフトウェアで、共通コンポーネントを使用する製品（Ops Center Automator を含む）のリソースを含んでいるグループをアクティブノードに移動します。グループを右クリックして［移動］を選択してから、［ノードを選択］または［このサービスまたはアプリケーションを別のノードに移動］を選択します。

15. Ops Center Portal から Ops Center Automator の登録を解除します。

操作結果

Ops Center Automator がホストからアンインストールされます。
Microsoft Visual C++ 2015-2019 Redistributable (x64)は、自動でアンインストールされません。同じホストにインストールされているほかのソフトウェアで使用していない場合は、プログラムを手動で削除できます。

7 コマンド

Ops Center Automator および共通コンポーネントのコマンドは、コマンドラインインターフェイス（CLI）で実行できます。

コマンドを実行するには、Ops Center Automator の Admin、Modify、または Submit のロールおよび OS の管理者権限が必要です。

7.1 共通コンポーネントコマンド

共通コンポーネントのコマンドは CLI で使用できます。

<共通コンポーネントのインストールフォルダー>¥bin に移動します。コマンドプロンプトを開き、共通コンポーネントのコマンドを実行します。

> **メモ**
>
> hcmds64clustersrvupdate コマンドとhcmds64clustersrvstate コマンドについては、コマンドの格納先が異なります。*<共通コンポーネントのインストールフォルダー>*¥ClusterSetup に移動します。

7.1.1 hcmds64banner コマンド

hcmds64banner コマンドは、Ops Center Automator の警告バナーに表示されるメッセージを登録および削除します。

このコマンドを実行する前に、テキストエディターを使用してメッセージを作成します。

英語（bannermsg.txt）と日本語（bannermsg_ja.txt）の サンプルメッセージは、次の場所にあります。

<共通コンポーネントのインストールフォルダー>¥sample¥resource

これらのサンプルファイルはインストール時に上書きされるため、サンプルファイルを使用する場合は、コピーしてから編集します。

デフォルトのメッセージを次に示します。

```
<center><b>警告</b></center>
これは{会社名}のコンピュータシステムです。このコンピュータシステムは，承認を受けた人だけがその業務のためにのみ使用できます。承認を受けない人からのアクセスや使用があった場合，侵入者として刑事，民事，および行政上の訴訟を提起する場合があります。<br>
犯罪捜査を含む公の目的のために，このコンピュータシステムに対するすべてのアクセスの履歴は，責任者によって傍受，記録，読み取り，複写，および開示される場合があります。アクセスした人に関する私的な機密情報についても機密性とプライバシーの要件に従って暗号化され，アクセス履歴として記録されます。このシステムを使用する人は，承認を受けているかどうかに関係なく，上記の条件に同意したものとみなします。このシステムにおいてプライバシーの権利はありません。
```

構文：

```
hcmds64banner {/add /file file-name [/locale locale-name]}
 | {/delete [/locale locale-name]}
```

説明：

- /add はメッセージを登録します。すでにメッセージが登録されている場合、上書きされます。

- /delete はメッセージを削除します。
- /file は絶対パスを使用して、メッセージを格納しているファイルを指定します。
- /locale はメッセージに使用した言語のロケールを指定します（例えば、英語の場合はen、日本語の場合はja です）。この設定を省略すると、ロケールに関係なく、登録したメッセージが常に警告バナーに表示されます（メッセージはデフォルトロケールのメッセージとして登録されます）。
  GUI を複数のロケールで使用する場合、同じ内容のメッセージをロケールごとに別の言語で登録しておくと、Web ブラウザーのロケールに合わせて、メッセージを自動的に切り替えられます。
  1 つの Web ブラウザーに複数の言語が指定されている場合、警告バナーのロケールは Web ブラウザーの言語の優先順位の設定によって決定されます。

注意事項

Ops Center Automator をクラスター構成で運用している場合は、アクティブノードとスタンバイノードそれぞれでこのコマンドを実行してください。

7.1.2 hcmds64chgurl コマンド

hcmds64chgurl コマンドは、GUI に登録されている共通コンポーネントを使用する製品の URL を変更します。共通コンポーネントの運用開始後に、以下のいずれかの構成変更によって製品の URL が変更された場合、hcmds64chgurl コマンドを使用して、GUI に登録されている各製品の URL を変更する必要があります。

- HBase 64 Storage Mgmt Web Service が使用するポートの変更
- 管理サーバーのホスト名または IP アドレスの変更
- SSL 通信を有効または無効にするための設定変更

構文：

```
hcmds64chgurl {/print | /list | /change old-URL new-URL | /change new-URL /type Common-Component-product-name}
```

説明：

- /print は、現在登録されている URL とプログラムのリストを表示します。
- /list は、/print オプションと同じ情報を異なる形式で表示します。
- /change は、現在登録されている URL を変更します。
- /type は、共通コンポーネントを使用する特定の製品の URL を変更する場合に、対象の製品の名前を指定します。Ops Center Automator の URL だけを変更する場合は、Automation と指定します。

注意

指定する URL は、プロトコルとポート番号を含む完全な URL である必要があります。IPv6 アドレスは使用できません。IPv6 環境では、次の例に示すように、ホスト名を使用して URL を指定する必要があります。

```
http://hostname:22015
```

7.1.3 hcmds64clustersrvstate コマンド

hcmds64clustersrvstate コマンドは、Ops Center Automator を含む共通コンポーネントのサービスが登録されているグループをオンラインにして、フェイルオーバーを有効にします。また、Ops Center Automator を含む共通コンポーネントのサービスが登録されているグループをオフラインにして、フェイルオーバーを無効にします。

Ops Center Automator を含む共通コンポーネントのサービスが登録されているグループをオンラインにして、フェイルオーバーを有効にする場合の構文を次に示します。

```
hcmds64clustersrvstate /son /r  cluster-group-name
```

Ops Center Automator を含む共通コンポーネントのサービスが登録されているグループをオフラインにして、フェイルオーバーを無効にする場合の構文を次に示します。

```
hcmds64clustersrvstate /soff /r cluster-group-name
```

説明：/r は、Ops Center Automator を含む共通コンポーネントのサービスが登録されているグループの名前を指定します。グループ名にスペースが含まれる場合は、グループ名を二重引用符（"）で囲む必要があります。例えば、グループ名が Automator cluster の場合は、"Automator cluster"と指定します。

7.1.4 hcmds64clustersrvupdate コマンド

hcmds64clustersrvupdate コマンドは、Ops Center Automator を含む共通コンポーネントのサービスをクラスター管理ソフトウェアグループに登録します。また、Ops Center Automator を含む共通コンポーネントのサービスをクラスター管理ソフトウェアグループから削除します。

Ops Center Automator を含む共通コンポーネントのサービスを登録する場合の構文を次に示します。

```
hcmds64clustersrvupdate /sreg /r cluster-group-name /sd
shared-disk-drive-letter /ap client-access-point-resource-name
```

Ops Center Automator を含む共通コンポーネントのサービスを削除する場合の構文を次に示します。

```
hcmds64clustersrvupdate /sdel /r cluster-group-name
```

説明：

- /r は 、Ops Center Automator を含む共通コンポーネントのサービスが登録されているグループの名前を指定します。グループ名にスペースが含まれる場合は、グループ名を二重引用符（"）で囲む必要があります。例えば、グループ名が Automator cluster の場合は、"Automator cluster"と指定します。
- /sd は、クラスター管理ソフトウェアに登録する共有ディスクのドライブ文字を指定します。このオプションに対して複数のドライブ文字を指定することはできません。共通コンポーネントを使用する製品のデータベースが複数の共有ディスクに分割されている場合は、各共有ディスクについて hcmds64clustersrvupdate コマンドを実行します。
- /ap は、クラスター管理ソフトウェアに登録するクライアントアクセスポイント用リソースの名前を指定します。

7.1.5 hcmds64dbinit コマンド

hcmds64dbinit コマンドは、製品を再インストールすることなく、インストール直後の状態に復元できます。製品自体が正しくインストールおよびセットアップされていて、DB の破損やディスク障害などによって DB の障害が発生して、環境が回復不可能な状態にある場合にだけ使用できます。

構文：

```
hcmds64dbinit /databasepath database-path
```

説明：/databasepath は 、データベースを再作成する場所を絶対パスで指定します。

7.1.6 hcmds64dbrepair コマンド

hcmds64dbrepair コマンドは、すべてのデータベースを強制的に削除して再作成し、hcmds64dbtrans コマンドで取得したバックアップデータからデータベースを復元します。データベースが破損して、restoresystem コマンドおよびhcmds64dbtrans コマンドを/import オプションを指定して実行しても復元できない場合に、このコマンドを使用します。

構文：

```
hcmds64dbrepair /trans backup-data
```

説明：/trans は、hcmds64dbtrans コマンドで取得したバックアップデータを指定します。hcmds64dbtrans コマンドの/workpath オプションまたは/file オプションのパスを指定してください。

注意事項

- このコマンドを実行する前に、Ops Center Automator のサービスを停止してください。
- このコマンドの実行後は、Ops Center Automator のサービスを起動してください。
- このコマンドは、*<共通コンポーネントのインストールフォルダー>*¥tmp フォルダーを使用して、バックアップデータを展開します。バックアップデータのサイズに応じて、データを展開するのに十分なスペースを確保してください。
- クラスターシステムの場合、アクティブノードでこのコマンドを実行してください。スタンバイノードでは実行できません。

7.1.7 hcmds64dbsrv コマンド

hcmds64dbsrv コマンドは、Ops Center Automator のデータベースを起動および停止します。データベースのメンテナンスを実施するときに使用します。

構文：

```
hcmds64dbsrv {/start | /stop}
```

説明：

- /start はデータベースを起動します。
- /stop はデータベースを停止します。

注意事項

データベースのメンテナンス手順以外では使用しないでください。

7.1.8 hcmds64dbtrans コマンド

hcmds64dbtrans コマンドは、Ops Center Automator のデータベースをバックアップ（エクスポート）またはリストア（インポート）します。Ops Center Automator のデータベースを再編成する場合に使用します。

Ops Center Automator のデータベースをバックアップ（エクスポート）する場合の構文を次に示します。

```
hcmds64dbtrans /export /workpath working-folder-path /file archive-file-path [/auto]
```

Ops Center Automator のデータベースをリストア（インポート）する場合の構文を次に示します。

```
hcmds64dbtrans /import /type Automation /workpath working-folder-path
[/file archive-file-path] [/auto]
```

説明：

- /export は、データベースをエクスポートします。
- /workpath は、エクスポート時またはインポート時に一時的に使用する作業用フォルダーを絶対パスで指定します。指定できるのはローカルディスクのフォルダーだけです。エクスポート時やインポート時に/file オプションを指定する場合、作業用フォルダーには空のフォルダーを使用してください。
- /file は、データのエクスポート先またはインポート元のアーカイブファイルを絶対パスで指定します。/export オプションを指定する場合は必ず指定します。
  出力ファイルサイズが 2GB を超える場合や、アーカイブファイル作成先のディスク容量が不足している場合、アーカイブファイルは作成されません。
- /auto を指定すると、Ops Center Automator および共通コンポーネントを使用する製品のサービスとデータベースを自動的に起動・停止します。このオプションを省略すると、Ops Center Automator および共通コンポーネントを使用する製品のサービスとデータベースを自動的に起動・停止しません。
- /import を指定すると、データベースをインポートします。データがインポートされる前に、既存の認証データはすべて削除されます。
- /type Automation は、データベースをインポートする対象の製品名としてAutomation を指定します。

注意事項

- エクスポート操作でリターンコード「3」が出力された場合、/workpath オプションに指定したフォルダーにデータベースの情報が残っています。この情報をインポートするには、エクスポート操作時に/workpath オプションに指定したフォルダーを、インポート操作の/workpath オプションに指定してください。このとき、エクスポート操作時に/workpath オプションに指定したフォルダーの構成を変更しないでください。また、インポート操作を実行するとき、/file オプションには値を指定しないでください。
- 次の場合、/workpath オプションに指定したフォルダーは空になり、コマンドが完了します。
  - エクスポート操作で、リターンコード「1」、「2」、「233」、「234」、「235」、「237」、「238」、「239」、「240」または「255」が出力された場合
  - インポート操作で、リターンコード「3」が出力された場合

7.1.9 hcmds64fwcancel コマンド

hcmds64fwcancel コマンドは、Windows ファイアウォールによって Ops Center Automator サーバーと Web ブラウザーの間の通信が遮断されないように例外登録をします。Web ブラウザーが接続する Ops Center Automator サーバーのポート番号をデフォルト値から変更する場合に使用します。

構文：

```
hcmds64fwcancel
```

7.1.10　hcmds64getlogs コマンド

hcmds64getlogs コマンドは、管理サーバーの保守情報を取得します。

構文：

```
hcmds64getlogs /dir folder-name [/types Automation] [/arc archive-file-name] [/logtypes log-file-type[ log-file-type ...]]
```

説明：

- /dir は、収集した保守情報を格納するローカルディスク上のフォルダーを絶対パスで指定し ます。
  フォルダーがすでに作成されている場合は、フォルダーを空にしてください。
  指定できるパスの最大長は 100 バイトです。一部の特殊文字を除いた ASCII 印字可能文字を指定できます。次の文字は指定できません。

  ¥ / : , ; * ? " < > | $ % & ' `

  ただし、パスの区切り文字として、円記号（¥)、コロン（:)、およびスラッシュ（/）を使用できます。パスの末尾にはパスの区切り文字を指定しないでください。

  パス中に空白文字を指定するときは、パスを二重引用符（"）で囲んでください
- /types Automation には、Ops Center Automator の保守情報しか取得できない場合に、Automation を指定します。このオプションを指定する場合、/logtypes オプションにログファイルの種別log も指定してください。このオプションを省略した場合、Ops Center Automator サーバーおよび同一管理サーバーにインストールされている共通コンポーネントを使用するすべての製品の保守情報が取得されます。
- /arc は、作成するアーカイブファイルの名前を指定します。このオプションを省略した場合、ファイル名はHiCommand_log_64 になります。
  ファイル名には、一部の特殊文字を除いた ASCII 印字可能文字を指定できます。次の文字は指定できません。

  ¥ / : , ; * ? " < > | $ % & ' `
- /logtypes は、障害によって特定の種別のログファイルが収集できない場合に、取得するログファイルの種別を指定します。
  - log：.jar ファイルと.hdb.jar ファイルだけを取得する場合に指定します。
  - db：.db.jar ファイルだけを取得する場合に指定します。
  - csv：.csv.jar ファイルだけを取得する場合に指定します。

  複数の種別を指定する場合は、空白で区切ってください。

  このオプションを省略した場合、すべてのログファイルが取得されます。

ヒント

このコマンドを実行すると、メッセージ KAPM05318-I または KAPM05319-E が出力されます。また、保守情報（ログファイルとデータベースファイル）が取得され、/dir オプションで指定したフォルダーに 4 つのアーカイブファイル（.jar、.hdb.jar、.db.jar、および.csv.jar）が出力されます。

注意事項

- このコマンドは実行中に中断しないでください。
- hcmds64getlogs コマンドが中断された場合、/dir オプションに指定したフォルダーの空き容量が不足しているため、コマンドが途中で終了しています。この場合、フォルダーに十分な空き容量があることを確認してから、再度このコマンドを実行してください。
- hcmds64getlogs コマンドは同時に複数実行しないでください。
- Ops Center Automator をクラスター構成で運用している場合は、アクティブノードとスタンバイノードそれぞれでこのコマンドを実行してください。このコマンドは、Ops Center Automator サーバーが停止していても実行できます。そのため、クラスター構成でエラーが発生しても、系を切り替えることなくログ情報を収集できます。ただし、データベースが停止している場合、データベースの情報は取得できません。
- 同じオプションを 2 回以上指定した場合、最初に指定したオプションが有効となります。

7.1.11 hcmds64keytool コマンド

hcmds64keytool コマンドでは次のことができます。

- JDK の keytool ユーティリティーを使用して、JDK のトラストストアに証明書を登録する。
- JDK の keytool ユーティリティーを使用して、キーストアまたはトラストストアに登録されている証明書を確認する。
- JDK の keytool ユーティリティーを使用して、JDK のトラストストアから証明書を削除する。
- JDK の keytool ユーティリティーを使用して、JDK のトラストストアから証明書をエクスポートする。

JDK のトラストストアに証明書を登録する場合の構文を次に示します。

```
hcmds64keytool -import -alias alias-name -file file-name -keystore file-name -storepass pass
word -storetype JKS
```

キーストアまたはトラストストアに登録されている証明書を確認する場合の構文を次に示します。

```
hcmds64keytool -list -v -keystore file-name -storepass password
```

JDK のトラストストアに登録されている証明書を削除する場合の構文を次に示します。

```
hcmds64keytool -delete -alias alias-name -keystore file-name -storepass password
```

JDK のトラストストアから証明書をエクスポートする場合の構文を次に示します。

```
hcmds64keytool -export -keystore file-name -alias alias-name -file file-name -storepass pass
word -storetype JKS
```

説明：

- -alias は、トラストストア内の証明書を識別するための名前（エイリアス名）を指定します。すでに存在するエイリアス名は指定できないため、前もって別の名前に変更するか、削除しておいてください。
- -file は、入力証明書（PEM 形式または DER 形式）を指定します。エクスポートする場合は、証明書の出力先パスを指定します。
- -keystore は、登録、確認、削除、またはエクスポートするトラストストアファイルを指定します。
- -storepass は、登録済みの証明書にアクセスするためのパスワードを指定します。
- -storetype は、ストアタイプのトラストストアとしてJKS を指定します。

7.1.12 hcmds64srv コマンド

hcmds64srv コマンドは、Ops Center Automator のサービスやデータベースを起動および停止します。また、Ops Center Automator のサービスの状態を表示したり、サービスの起動方法を変更したりできます。このコマンドの/server オプションにAutomationWebService を指定して実行すると、以下に示すサービスを起動、停止、または状態を表示できます。

- 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
- データベースのプロセス※1, 2

注※1　共通コンポーネントを使用する製品のサービスが実行されている間は停止されません。

注※2　Ops Center Automator の内部プロセスです。hcmds64srv コマンドは、データベースのサービスを示すHiRDB/EmbeddedEdition _HD1 を起動および停止しません。

構文：

特定のサービスだけを起動、停止、または状態を表示する場合：

```
hcmds64srv {/start /stop /check | /status} [/server service-name]
```

Ops Center Automator および共通コンポーネントを使用する製品のサービスの状態を確認する場合：

```
hcmds64srv /statusall
```

サービスの起動方法を変更する場合：

```
hcmds64srv /starttype {auto | manual} {/server service-name | /all}
```

説明：

- /start は、/server オプションで指定したサービスとデータベースを起動します。
- /stop は、/server オプションで指定したサービスとデータベースを停止します。
- /check は、/server オプションで指定したサービスとデータベースの状態を表示します。
- /status は、/server オプションで指定したサービスとデータベースの状態を表示します。
- /server は、サービスの停止、起動、および状態を表示します。
  Ops Center Automator のサービスだけを対象とする場合、service-name にAutomationWebService を指定します。このオプションを省略した場合、Ops Center Automator および共通コンポーネントを使用するすべての製品のサービスが対象となります。
- /statusall は、サービスとデータベースの状態、および共通コンポーネントを使用する製品のサービスの状態を表示します。
- /starttype は、/server オプションで指定したサービスの起動種別を指定します。サービスを自動的に起動する場合は、auto を使用します。手動で起動する場合は、manual を使用します。
- /all を指定した場合は、Ops Center Automator および共通コンポーネントを使用するすべての製品のサービスが対象となります。

注意事項

- 日常運用で Ops Center Automator のサービスを起動および停止する場合は、/server オプションを指定せずに、すべてのサービスを起動および停止してください。 /server オプションを指定して Ops Center Automator のサービスだけを起動する場合は、事前に共通コンポーネントのサービスを起動しておく必要があるため、/server オプションにHBase を指定して共通コンポーネントのサービスを起動してください。
- タスクの処理中に/stop オプションを指定してコマンドを実行すると、接続先で実行中の処理はすべて終了します。そのため、実行状態（実行中、応答待ち中、異常検出、または停止中）のタスクがある場合は、停止状態（正常終了、失敗、またはキャンセル）に遷移するまで待つかすべてのタスクを停止してから、/stop オプションを指定してコマンドを使用してください。

- /stop オプションを指定してコマンドを実行したあと、3 分以内にサービスが停止しない場合は、タイムアウトを示すメッセージを出力してコマンドが異常終了します。この場合は、しばらく待ってから、再度/stop オプションを指定して実行してください。

7.1.13 hcmds64ssltool コマンド

hcmds64ssltool コマンドは、SSL 接続に必要な秘密鍵、CSR、自己署名証明書および自己署名証明書の内容ファイルを作成します。

作成したファイルは、次の用途に使用されます。

- CSR を CA に提出して SSL サーバー証明書を取得します。取得した SSL サーバー証明書と秘密鍵を組み合わせて、SSL 接続環境を構築できます。
- 自己署名証明書と秘密鍵を組み合わせて、SSL 接続環境を構築できます。ただし、セキュリティーレベルが低いため、この環境はテスト目的にだけ使用してください。
- 自己署名証明書の内容ファイルを表示することで、自己署名証明書に登録されている情報を確認できます。

構文：

```
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.509certificate]
```

説明：

- /key は、作成する秘密鍵ファイルを絶対パスで指定します。このオプションを省略すると、ファイルは、RSA の場合はhttpsdkey.pem、ECC の場合はecc-httpsdkey.pem というファイル名で、デフォルトの出力先パスに出力されます。このオプションを省略した場合のデフォルトの出力先は次のとおりです。

  ＜共通コンポーネントのインストールフォルダー＞¥uCPSB11¥httpsd¥conf¥ssl¥server

- /csr は、作成する証明書署名要求ファイルを絶対パスで指定します。このオプションを省略すると、ファイルは、RSA の場合はhttpsd.csr、ECC の場合はecc-httpsd.csr というファイル名で、デフォルトの出力先パスに出力されます。このオプションを省略した場合のデフォルトの出力先は次のとおりです。

  ＜共通コンポーネントのインストールフォルダー＞¥uCPSB11¥httpsd¥conf¥ssl¥server

- /cert は、作成する自己署名証明書ファイルを絶対パスで指定します。このオプションを省略すると、ファイルは、RSA の場合はhttpsd.pem、ECC の場合はecc-httpsd.pem というファイル名で、デフォルトの出力先パスに出力されます。このオプションを省略した場合のデフォルトの出力先は次のとおりです。

```
<共通コンポーネントのインストールフォルダー>¥uCPSB11¥httpsd¥conf¥ssl¥server
```

- /certtext は、作成する自己署名証明書の内容ファイルを絶対パスで指定します。このオプションを省略すると、ファイルは、RSA の場合はhttpsd.txt、ECC の場合はecc-httpsd.txt というファイル名で、デフォルトの出力先パスに出力されます。このオプションを省略した場合のデフォルトの出力先は次のとおりです。

  ```
  <共通コンポーネントのインストールフォルダー>¥uCPSB11¥httpsd¥conf¥ssl¥server
  ```

- /validity は、自己署名証明書の有効期限を日数で指定します。このオプションを省略すると、有効期限は 3,650 日となります。指定できる値は、9999 年 12 月 31 日までの日数です。
- /sigalg は、RSA 証明書の署名アルゴリズムを SHA256withRSA または SHA1withRSA で指定します。このオプションを省略すると、デフォルトの SHA256withRSA が使用されます。
- /eccsigalg は、ECC 証明書の署名アルゴリズムを SHA512withECDSA、SHA384withECDSA、SHA256withECDSA または SHA1withECDSA で指定します。このオプションを省略すると、デフォルトの SHA384withECDSA が使用されます。
- /ecckeysize は、ECC サーバー証明書の秘密鍵のサイズを 256 または 384 ビットで指定します。このオプションを省略すると、デフォルトの 384 が使用されます。
- /ext は、X.509 証明書の拡張情報を指定します。自己署名証明書および証明書署名要求に SAN（Subject Alternative Name）を設定する場合は、このオプションを指定します。指定方法は、Java のkeytool コマンドの/ext オプションに基づきます。Ops Center Automator で指定できる拡張情報は SAN だけであることに注意してください。/ext オプションを複数回指定した場合は、最初の指定が有効になります。
  以下に、拡張情報を指定する例を示します。
  - www.example.com をホスト名として指定する場合：

    ```
    hcmds64ssltool /ext san=dns:www.example.com
    ```

  - www.example.com と www.example.net を複数のホスト名として指定する場合：

    ```
    hcmds64ssltool /ext san=dns:www.example.com, dns:www.example.net
    ```

- /dname は、SSL サーバー証明書に記述する識別名（DN）を*attribute-type=attribute-value* の形式で指定します。コンマ（,）で区切ることで、複数の属性型の値を指定できます。*attribute-type* の大文字と小文字は区別されません。*attribute-value* に二重引用符（"）や円記号（¥）を含めることはできません。
  文字のエスケープについては、RFC 2253 に従ってください。
  次の文字は円記号（¥）でエスケープしてください。
  - ＋ , ; < =>
  - 文字列の先頭の空白
  - 文字列の末尾の空白
  - 文字列の先頭のハッシュ記号（#）

このオプションを省略した場合、コマンド実行時に表示されるプロンプトに従って属性値を応答入力します。

次の表に、このオプションに指定できる属性型について示します。

表 7-1　識別名（DN）に指定できる属性型一覧

属性型	説明	表示されるプロンプト	値
CN	Common Name	Server Name	ホスト名、IP アドレス、ドメイン名など Ops Center Automator サーバーの識別名※
OU	Organizational Unit Name	Organizational Unit	部門や部署名など小さな単位の組織名
O	Organization Name	Organization Name	会社または団体の組織名※
L	Locality Name	City or Locality	都市または地区名
ST	State or Province Name	State or Province	州または都道府県名
C	Country Name	two-character country code	国コード
注※　応答入力を使用する場合に必要です。			

応答入力例を次に示します。

```
Enter  Server  Name  [default=MyHostname]:example.com
Enter Organizational Unit:Automation Administration
Enter Organization Name [default=MyHostname]:HITACHI
Enter your City or Locality:Yokohama
Enter your State or Province:Kanagawa
Enter your two-character country-code:JP
Is CN=example.com,OU=Automation Administration,O=HITACHI,L=Yokohama,ST=Kanagawa,C=JP corr
ect? (y/n) [default=n]:y
```

値の入力に誤りがあった場合は、確認時にn を入力して応答入力を再度行います。

注意事項

SSL サーバー証明書の属性型 CN と、Web ブラウザーから Ops Center Automator サーバーへの接続先として指定したホスト名、IP アドレスまたはドメイン名が一致しない場合、サーバー名の不一致の警告またはエラーが発生します。

7.2 Ops Center Automator コマンド

Ops Center Automator は、CLI で使用できるコマンドを提供しています。

<Ops Center Automatorのインストールフォルダー>¥bin に移動し、コマンドプロンプトを開いて次の Ops Center Automator コマンドを実行します。

7.2.1 backupsystem コマンド

backupsystem は、システム構成とデータベース情報を指定フォルダーにバックアップします。

構文

```
backupsystem {/dir directoryname [/auto] | /help}
```

オプション

オプション	説明
/dir	バックアップデータを含む絶対または相対フォルダーパスです。
/auto	Ops Center Automator および共通コンポーネントのサービスとデータベースの自動的な起動および停止を指示します。

メモ

クラスター環境では、backupsystem コマンドを実行する前に、次のコマンドを実行して Ops Center Automator のサービスが登録されるグループをオフラインにして、フェイルオーバーを無効にする必要があります。

```
<共通コンポーネントのインストールフォルダー>¥ClusterSetup¥hcmds64clustersrvstate /soff /r <グループ名>
```

7.2.2 changemode コマンド

changemode コマンドでは、Ops Center Automator のパフォーマンスモードを変更することができます。パフォーマンスモードには、スタンダードとハイパフォーマンスの 2 種類があります。

スタンダードモード

単一の Online Migration with Configuration Manager タスクの実行をサポートするデフォルトのモードです。

ハイパフォーマンスモード

複数の Online Migration with Configuration Manager タスクを同時に実行する必要がある場合は、ハイパフォーマンスモードを使用します。このモードを選択した場合は、config_user.properties の logger.TA.MaxFileSize および plugin.threadPoolSize パラメーターを変更する必要があります。詳細については、「3.4　システム構成を変更する」を参照してください。

構文

```
changemode {/mode {standard| highPerformance} [/auto] |  /print |  /help}
```

オプション

オプション	説明
/mode	standard（スタンダードモード）またはhighPerformance（ハイパフォーマンスモード）のいずれかのパフォーマンスモードを指定します。
/auto	必要に応じて、共通コンポーネントと HiRDB を使用するサービスを自動的に停止および起動します。クラスター環境でこのオプションを指定するには、クラスターソフトウェアに登録されているサービスがオフラインである必要があります。
/print	現在のモードを出力します。
/help	コマンドヘルプを表示します。

権限

Ops Center Automator ユーザーには、Administrator 権限が必要です。

終了コード

次の表に、changemode コマンドの終了コードと説明を示します。

終了コード	説明
0	コマンドが成功しました。
1	引数が無効です。
2	コマンドが停止しました。
3	サービスの状態が不正です。
4	排他エラーが発生しました。
101	サービスを起動または停止できません。
90	上記以外の原因で失敗したため、モードを変更できません。
255	この表にはないエラーが原因でコマンドが停止しました。

使用例：ハイパフォーマンスモードに変更する

```
changemode /mode highPerformance
```

使用例：スタンダードモードに変更し、auto オプションを指定する

```
changemode /mode standard /auto
```

使用例：現在のモードを出力する

```
changemode /print
```

出力例：ハイパフォーマンスモードへの変更

```
# 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.
```

注意事項

Ops Center Automator をクラスター構成で運用している場合は、アクティブノードとスタンバイノードそれぞれでこのコマンドを実行してください。

メモ

クラスター環境では、changemode コマンドを実行する前に、次のコマンドを実行して Ops Center Automator のサービスが登録されるグループをオフラインにして、フェイルオーバーを無効にする必要があります。

```
<共通コンポーネントのインストールフォルダー>¥ClusterSetup¥hcmds64clustersrvstate
 /soff /r <グループ名>
```

7.2.3 deleteremoteconnection コマンド

deleteremoteconnection コマンドは、listremoteconnections コマンドで取得した定義 ID に基づいて、Ops Center Automator で登録されたエージェントレス接続先定義を削除します。

機能

deleteremoteconnection コマンドは以下の機能を実行します。

- 連続するエージェントレス接続先定義をその定義 ID に基づいて削除します。エージェントレス接続先定義の定義 ID を確認するには、listremoteconnections コマンドを使用します。

構文

```
deleteremoteconnection {/id Definition ID
[/user UserName |
/user UserName /passwordfile PasswordFile]
[/authmode local | external] | /help}
```

> **メモ**
>
> passwordfile オプションを指定しない場合は、対話形成でパスワードの入力を求められます。

権限

- Ops Center Automator ユーザーには Admin 権限が必要です。
- OS の管理者権限を持つユーザー（Administrators グループのメンバー）のみが deleteremoteconnection コマンドを実行できます。
- 必要な権限を持たないユーザーがこのコマンドを実行した場合、ユーザーの権限を昇格するよう求める次のメッセージが表示されます。

```
KNAE03226-W The user does not have permission to execute the command.
```

オプション

オプション	説明
/id	削除するエージェントレス接続先定義情報を示す 1 バイト数値の定義 ID（1～64 文字長）を指定します。指定した ID が存在しない場合、エラーが生成されます。
/user	コマンドを実行するユーザー（Admin 権限を持っている必要があります）の名前を指定します。ユーザー名には、1 バイトの英数字を使用できます。これには(!# $ % & ' ( ) * + - .= @ ¥ ^ _ |)が含まれます。長さは 1～256 文字です。ユーザー名の大文字と小文字は区別されます。
/passwordfile	選択したユーザーの暗号化されたユーザー認証情報が含まれるパスワードファイル（絶対パスまたは相対パス付き）を指定します。
/authmode	認証方式としてexternal を指定します。local の指定は非サポートです。このオプションを省略すると、Ops Center Automator はexternal で動作します。

格納先

＜Ops Center Automatorのインストールフォルダー＞¥bin

終了コード

次の表にdeleteremoteconnection コマンドの終了コードと説明を示します。

終了コード	説明
0	コマンドが成功しました。
1	引数が無効です。
2	コマンドが停止しました。
3	サービスの状態が不正です。
4	排他エラーが発生しました。
5	通信が失敗しました。
6	認証が失敗しました。
14	ユーザーにコマンドの実行権限がありません。
17	対話形式の入力値が無効です。
240	エージェントレス接続先定義の削除に失敗しました。
255	この表にリストされていないエラーが原因でコマンドが停止しました。

使用例：パラメーターで指定した ID のエージェントレス接続先定義を削除する

```
deleteremoteconnection /id 12345 /user xxxxx
```

例：正常削除時の出力

```
KNAE03000-I The deleteremoteconnection command will now start.
KNAE03001-I The deleteremoteconnection command ended normally.
```

例：異常削除時の出力

```
KNAE03000-I The deleteremoteconnection command will now start.
KNAE03002-E The deleteremoteconnection command ended abnormally (12345).
```

7.2.4　deleteservicetemplate コマンド

deleteservicetemplate コマンドは、サービステンプレートを削除します。

構文

```
deleteservicetemplate {/name service-template-key-name /vendor vendor-ID /version XX.YY.ZZ [
/user username | /user username /passwordfile passwordfile] [/authmode local | external] | /
help}
```

> **メモ**
>
> passwordfile オプションを指定しない場合は、対話形成でパスワードの入力を求められます。

オプション

オプション	説明
/name	サービステンプレートのキー名です。
/vendor	サービステンプレートの Vendor ID です。
/version	サービステンプレートのバージョンです。
/user	ユーザー ID です。
/passwordfile	（絶対または相対パスの）パスワードファイルで、暗号化したユーザー認証情報が格納されています。
/authmode	認証方式としてexternal を指定します。local の指定は非サポートです。このオプションを省略すると、Ops Center Automator はexternal で動作します。

7.2.5 encryptpassword コマンド

encryptpassword コマンドは、暗号化したユーザー名とパスワードを含むファイルを作成します。/passwordfile オプションを許している Ops Center Automator コマンド用に、パスワードを使う代わりにパスワードファイルを指定できます。

構文

```
encryptpassword {[/user username] /passwordfile passwordfile [/authmode local | external] |
/help }
```

> **メモ**
>
> 対話形式でパスワードの入力を求められます。

オプション

オプション	説明
/user	ユーザーの ID で、パスワードファイルに追加されます。
/passwordfile	暗号化したユーザー認証情報が格納されている（絶対または相対パスの）パスワードファイルの名前です。
/authmode	認証方式としてexternal を指定します。local の指定は非サポートです。このオプションを省略すると、Ops Center Automator はexternal で動作します。

7.2.6 importservicetemplate コマンド

importservicetemplate コマンドは、サービステンプレートのパッケージをインポートします。

構文

```
importservicetemplate {/file service-template [/user username | /user username /passwordfile passwordfile] [/authmode local | external] | /help}
```

> **メモ**
>
> passwordfile オプションを指定しない場合は、対話形成でパスワードの入力を求められます。

オプション

オプション	説明
/file	インポートするサービステンプレートのファイルです。
/user	ユーザー ID です。
/passwordfile	（絶対または相対パスの）パスワードファイルで、暗号化したユーザー認証情報が格納されています。
/authmode	認証方式としてexternal を指定します。local の指定は非サポートです。このオプションを省略すると、Ops Center Automator はexternal で動作します。

7.2.7 listremoteconnections コマンド

listremoteconnections コマンドは、Ops Center Automator を通じて登録されたエージェントレス接続先定義のリストを CSV 形式ファイルに出力します。

機能

listremoteconnections コマンドは次の機能を実行します。

- 接続先の名前と認証情報を含むエージェントレス接続先定義のリストを出力します。
- 出力した CSV ファイルは、そのままsetremoteconnection コマンドの入力ファイルとして使用できます。

構文

```
listremoteconnections {/file OutputFile
[/user UserName |
/user UserName /passwordfile PasswordFile]
[/authmode local | external] | /help}
```

> **メモ**
>
> passwordfile オプションを指定しない場合は、対話形成でパスワードの入力を求められます。

権限

- Ops Center Automator ユーザーには Admin 権限が必要です。
- OS 管理者権限を持つユーザー（Administrators グループのメンバー）のみ、listremoteconnections コマンドを実行できます。
- 必要な権限を持たないユーザーがコマンドを実行すると、次のメッセージが表示され、ユーザーの権限を昇格するよう求められます。

  ```
  KNAE03226-E The user does not have permission to execute the command.
  ```

オプション

オプション	説明
/file	リストの出力先とするファイルのパスを指定します。指定されたファイルがすでに存在する場合は、エラーが生成されます。
/user	コマンドを実行するユーザーの名前を指定します。ユーザー名には、1 バイトの英数字を使用できます。これには(! # $ % & ' ( ) * + - . = @ ¥ ^ _ |)が含まれます。長さは 1～256 文字です。ユーザー名の大文字と小文字は区別されます。
/passwordfile	選択したユーザーの暗号化されたユーザー認証情報が含まれるパスワードファイル（絶対パスまたは相対パス付き）を指定します。
/authmode	認証方式としてexternal を指定します。local の指定は非サポートです。このオプションを省略すると、Ops Center Automator はexternal で動作します。

格納先

＜Ops Center Automatorのインストールフォルダー＞¥bin

終了コード

以下の表は、listremoteconnections コマンドの終了コードと説明のリストです。

終了コード	説明
0	コマンドが成功しました。
1	引数が無効です。
2	コマンドが停止しました。
3	サービスの状態が不正です。
4	排他エラーが発生しました。
5	通信が失敗しました。
6	認証が失敗しました。
7	不正なパスが指定されました。
8	指定された名前のファイルはすでに存在しています。
9	パスが見つかりません。
10	パスにアクセスできません。
13	指定されたファイルの出力に失敗しました。
14	ユーザーにはコマンドを実行する権限がありません。
17	対話形式の入力値が無効です。
220	エージェントレス接続先定義のリストの取得に失敗しました。
255	この表にリストされていないエラーが原因でコマンドが停止しました。

データ形式

エージェントレス接続先は、ホストごとに 1 行ずつ CSV 形式で出力されます。これには次のデータ項目が以下の表と同じ順序で含められます。

プロパティ	ヘッダー部（1 行目）	データ部（2 行目以降）
接続先定義の ID	Id	エージェントレス接続先定義 ID
接続先種別	Method	接続先を次のように指定できます。 • IPv4：接続先は IPv4 形式の IP アドレスです。 • IPv6：接続先は IPv6 形式の IP アドレスです。 • HostName：接続先はホスト名です。
接続先	IP Address/Host Name	接続先ホストの IP アドレスまたはホスト名。
Service resource group	Service Group	エージェントレス接続先定義に割り当てられたサービスグループ名。このプロパティは使用しません。
認証情報	Authentication	以下のいずれかです。

プロパティ	ヘッダー部（1 行目）	データ部（2 行目以降）
認証情報	Authentication	• Enable：認証情報が設定されています。 • Disable：認証情報が設定されていません。
プロトコル	Protocol	以下のいずれかです。 • Windows：Windows を使用して接続します。 • SSH：SSH を使用して接続します。 • Telnet：Telnet を使用して接続します。
SSH 認証方式	SSH authentication method	プロトコルが SSH ではない場合は null 文字（""）です。 プロトコルが SSH の場合は以下のいずれかです。 • Password Authentication • Public Key Authentication • Keyboard Interactive Authentication
ユーザー ID	User ID	接続先ホストにログインするユーザーのユーザー ID です。
パスワード	Password	「*******」固定です。
スーパーユーザーのパスワード	Super user's password	「*******」固定です。
状態	Connection Status	Connection Successful、Error、Unknown、または「-」
最後に接続した時間	Connected Time	最後に接続した時間。

使用例：登録されているエージェントレス接続先定義のリストをファイルに出力するには

```
listremoteconnections /file bbbbb /user xxxxx
```

例：リスト作成が成功した場合の出力メッセージ

```
KNAE03000-I The listremoteconnections command will now start.
KNAE03001-I The listremoteconnections command ended normally.
```

例：リスト作成が失敗した場合の出力メッセージ

```
KNAE03000-I The listremoteconnections command will now start.
KNAE03002-E The listremoteconnections command ended abnormally (12345).
```

例：一般的な出力ファイル

```
”Id”,”Method”,”IP Address/Host Name”,”Service Group”,”Authentication ”,”Protocol”,”SSH Authe
ntication 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”,””,””,””,””,””
```

7.2.8 listservices コマンド

listservices コマンドは、サービスの一覧またはサービステンプレートの一覧を CSV ファイルにエクスポートします。

構文

```
listservices {/output {services | servicetemplates} /file output-file [/encoding encoding] [
/user username | /user username /passwordfile passwordfile] [/authmode local | external] | /
help}
```

> **メモ**
>
> passwordfile オプションを指定しない場合は、対話形成でパスワードの入力を求められます。

オプション

オプション	説明
/output	services（サービスをエクスポート）またはservicetemplates（サービステンプレートをエクスポート）のどちらかです。
/file	出力ファイルのパスです。
/encoding	出力ファイルのエンコーディングで、UTF-8 またはShift_JIS のどちらかです。
/user	ユーザー ID です。 サービス一覧を出力するには、Submit ロールが必要です。サービステンプレート一覧を出力するには、Modify ロールが必要です。
/passwordfile	（絶対または相対パスの）パスワードファイルで、選択ユーザー用の暗号化したユーザー認証情報が格納されています。
/authmode	認証方式としてexternal を指定します。local の指定は非サポートです。このオプションを省略すると、Ops Center Automator はexternal で動作します。

7.2.9 listtasks コマンド

listtasks コマンドは、タスク一覧を CSV ファイルにエクスポートします。

構文

```
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}
```

> **メモ**
>
> passwordfile オプションを指定しない場合は、対話形成でパスワードの入力を求められます。

オプション

オプション	説明
/startrange	タスク開始日の日付範囲です。これを使って、タスク一覧の内容を特定の期間内に実行されるタスクだけに制限します。output オプションにtaskdetails を指定した場合は、このオプションを使用できません。
/output	次のいずれかの出力データ種別です。tasks（タスクをエクスポート）、histories（履歴をエクスポート）、taskdetails（プロパティを持つタスクをエクスポート）
/file	絶対または相対パスを持つ出力ファイルです。
/taskdetaildir	絶対または相対パスを持つ出力ファイルです。/output taskdetails が指定される場合には、/file の代わりに/taskdetaildir が必須となります。
/encoding	出力ファイルのエンコーディングで、UTF-8 またはShift_JIS のどちらかです。
/user	ユーザー ID です。taskdetails を出力するには、Admin ロールが必要です。
/passwordfile	パスワードファイルの絶対または相対パスです。
/authmode	認証方式としてexternal を指定します。local の指定は非サポートです。このオプションを省略すると、Ops Center Automator はexternal で動作します。

7.2.10 restoresystem コマンド

restoresystem コマンドは、データがバックアップされている指定フォルダーからシステム構成とデータベース情報をリストアします。

構文

```
restoresystem {/dir directoryname [/auto] | /help}
```

オプション

オプション	説明
/dir	backupsystem コマンドによってバックアップされているデータを含む絶対または相対のフォルダーパス。
/auto	Ops Center Automator および共通コンポーネントのサービスとデータベースの自動的な起動および停止を指示します。

メモ

クラスター環境では、restoresystem コマンドを実行する前に、次のコマンドを実行して Ops Center Automator のサービスが登録されるグループをオフラインにして、フェイルオーバーを無効にする必要があります。

```
＜共通コンポーネントのインストールフォルダー＞¥ClusterSetup¥hcmds64clustersrvstate /soff /r ＜グループ名＞
```

7.2.11 setremoteconnection コマンド

setremoteconnection コマンドは CSV ファイルを介して Ops Center Automator のエージェントレス接続先定義を追加または更新します。

機能

setremoteconnection コマンドは、Ops Center Automator のエージェントレス接続先定義を追加または更新します。エージェントレス接続先定義を追加または更新するには、CSV ファイルに情報を定義し、コマンド引数としてファイルを指定します。

メモ

CSV ファイルはlistremoteconnections コマンドの出力ファイルと同じ形式でなくてはなりません。

構文

```
setremoteconnection {/file Input File
[/user UserName |
/user UserName /passwordfile PasswordFile]
[/authmode local | external] | /help}
```

メモ

passwordfile オプションを指定しない場合は、対話形成でパスワードの入力を求められます。

権限

- Ops Center Automator ユーザーには Admin 権限が必要です。
- OS 管理者権限を持つユーザー（Administrators グループのメンバー）のみ、setremoteconnection コマンドを実行できます。
- 必要な権限を持たないユーザーがコマンドを実行すると、次のメッセージが表示され、ユーザーの権限を昇格するよう求められます。

```
KNAE03226-W The user does not have permission to execute the command.
```

オプション

オプション	説明
/file	追加または更新するエージェントレス接続先定義を含むファイルのパスを指定します。指定されたファイルが存在しない場合、エラーが生成されます。絶対パスと相対パスの両方を使用できます。
/user	コマンドを実行するユーザーの名前を指定します。ユーザー名には、1 バイトの英数字を使用できます。長さは 1～256 文字です。# $ % & ' ( ) * + - .= @ ¥ ^ _ |)を含めることができます。ユーザー名の大文字と小文字は区別されます。
/passwordfile	選択したユーザーの暗号化されたユーザー認証情報が含まれるパスワードファイル（絶対パスまたは相対パス付き）を指定します。
/authmode	認証方式としてexternal を指定します。local の指定は非サポートです。このオプションを省略すると、Ops Center Automator はexternal で動作します。

格納先

＜Ops Center Automatorのインストールフォルダー＞¥bin

終了コード

以下の表は、setremoteconnection コマンドの終了コードと説明のリストです。

終了コード	説明
0	コマンドが成功しました。
1	引数が無効です。
2	コマンドが停止しました。
3	サービスの状態が不正です。

終了コード	説明
4	排他エラーが発生しました。
5	通信が失敗しました。
6	認証が失敗しました。
7	不正なパスが指定されました。
9	パスが見つかりません。
10	パスにアクセスできません。
14	ユーザーにはコマンドを実行する権限がありません。
17	対話形式の入力値が無効です。
230	エージェントレス接続先定義のフォーマットが不正です。
231	一部のエージェントレス接続先定義の登録が失敗しました。
232	すべてのエージェントレス接続先定義の登録が失敗しました。
255	この表にはないエラーが原因でコマンドが停止しました。

ファイル形式

エージェントレス接続先定義ファイルの形式は、次のように/file オプションで指定します。形式は、基本的にはlistremoteconnections コマンドで生成される出力と同じです。

エージェントレス接続先定義ファイルの形式は、以下のように実行環境によって異なるため注意してください。

- Windows 環境：文字コード MS932 と改行コード CR+LF を使用します。
- Linux 環境：ユーザーの環境変数 LANG に指定された文字コードと改行コード LF を使用します。

データ項目	説明
接続先定義の ID (Id)	更新するエージェントレス接続先定義の ID を指定します。この項目に null 文字が指定された場合、エージェントレス接続先定義は追加として登録されます。指定された ID のエージェントレス接続先定義が存在しない場合、エラーが生成されます。
接続先種別 (Method)	以下の接続先タイプのいずれかを指定します。 • IPv4：接続先は IPv4 形式の IP アドレスです。 • IPv6：接続先は IPv6 形式の IP アドレスです。 • HostName：接続先はホスト名です。
接続先 (IP Address/Host Name)	接続先ホストの IP アドレスまたはホスト名。
Service resource group (Service Group)	この項目は設定不要です。
認証情報	以下のいずれかです。

データ項目	説明
(Authentication)	• Enable：認証情報が設定されています。 • Disable：認証情報が設定されていません。 認証情報が設定されていないことを示すメッセージが表示された場合、以降のデータは無視されます。ただし、データ項目自体は必須です。
プロトコル (Protocol)	次のいずれかのプロトコルを指定します。 • Windows：Windows を使用して接続します。 • SSH：SSH を使用して接続します。 • Telnet：Telnet を使用して接続します。

SSH 認証方式
(SSH Authentication Method)
	プロトコルが SSH ではない場合は null 文字（""）です。
	• プロトコルが SSH ではない場合は null 文字（""）です。
	• プロトコルが SSH の場合は以下のいずれかです。
	  • パスワード認証（PW）
	  • 公開鍵認証（PK）
	  • キーボードインタラクティブ認証（KI）

ユーザー ID (User ID)	接続先ホストにログインするのに使用するユーザー ID を指定します。プロトコルが Windows または SSH の場合、この項目は必須です。
パスワード (Password)	接続先ホストにログインするのに使用するユーザー ID のパスワードを指定します。定義 ID が以下のように指定されているかどうかに従って、この情報は必須の場合とそうでない場合があります。 ケース 1：定義 ID が指定されていない場合（定義の追加時） • プロトコルが Windows の場合、この項目は必須です。 • プロトコルが SSH であり、SSH 認証方式が「公開鍵認証」でない場合、この項目は必須です。 **メモ** パスワードとして「********」を指定することは できません。指定された場合、省略とみなされエラーが生成されます。 ケース 2：定義 ID が指定されている場合（定義の更新時） • プロトコルが Windows の場合、この項目は必須です。 • プロトコルが SSH であり、SSH 認証方式が「公開鍵認証」でない場合、この項目は必須です。 **メモ** パスワードに「********」を指定した場合、パスワードは変更されません。パスワードに null 文字（""）を指定した場合、パスワードは削除されます。
スーパーユーザーのパスワード (Super User's Password)	接続先ホストのスーパーユーザーのパスワードを指定します。この項目は、プロトコルが SSH または Telnet の場合に指定できます（ただし必須ではありません）。 • パスワードに「********」以外の文字列を指定した場合、指定された文字列がパスワードとして設定されます。

データ項目	説明
スーパーユーザーのパスワード (Super User's Password)	• パスワードに「********」を指定した場合、パスワードは変更されません。 • パスワードに null 文字（""）を指定した場合、パスワードは削除されます。
状態 (Connection Status)	「成功」、「エラー」、「不明」または「-」のいずれかを、状態によって指定します。
最後に接続した時間 (Connected Time)	最後に接続した時間を指定します。

setremoteconnection コマンドの動作

setremoteconnection コマンドで、/file オプションにエージェントレス接続先定義ファイルを指定した場合の動作について、詳細の一部を以下で説明します。

- ファイルの 1 行目は、setremoteconnection コマンドにより出力されるヘッダーセクションで、常に無視されます。2 行目以降がエージェントレス接続先定義として処理されます。
- ファイル内で 2 つ以上のエージェントレス接続先定義が指定されている場合、構文エラーが 1 つでも含まれていると、コマンドはエラー終了し、ファイル内のエージェントレス接続先定義はいずれも登録されません。
- listremoteconnections コマンドが CSV 形式で出力するデータ項目の値は、引用符（"）で囲まれています。ただし、値が引用符（"）で囲まれていない場合でもエラーとして処理されません（これは CSV ファイルを Excel で編集すると、引用符が取り除かれるためです）。
- エージェントレス接続先定義の 1 番目のデータ項目（ID）である値が null 文字である場合、指定された内容はエージェントレス接続先定義として追加されます。
- エージェントレス接続先定義の 1 番目のデータ項目（ID）に値が指定されている場合、指定された ID に対応するエージェントレス接続先定義が行で指定された内容で更新されます。指定された ID に対応するエージェントレス接続先定義が存在しない場合は、エラーが生成されます。
- 2 つ以上のエージェントレス接続先定義がファイル内で指定されている場合、定義の一部の追加または更新が失敗すると、次のように処理されます。
  戻り値（警告、エラーではない）を使用して、登録が失敗した定義を報告します。
  情報は標準エラー出力に出力されるため、登録に失敗した定義を特定することができます。
  エラーが発生しても、残りのすべての定義に登録処理が継続されます。

使用例：指定したファイルの内容で、Ops Center Automator のエージェントレス接続先定義を登録または更新する

```
setremoteconnection /file bbbbb /user xxxxx
```

例：エージェントレス接続先定義の登録に成功

```
KNAE03000-I The setremoteconnection command will now start.
KNAE03002-E The remote connection definition was registered (ID:12345, line number: 12345).
```

例：登録または更新に失敗

```
KNAE03000-I The setremoteconnection command will now start.
KNAE03002-E The setremoteconnection command ended abnormally (12345).
```

例：パラメーターにエラーを検出

```
KNAE03000-I The setremoteconnection command will now start.
KNAE03333-E A required parameter was not found (parameter name: XXXXX, line number: 12345).S
pecify the required parameter, and then try again.
KNAE03334-E Unnecessary parameter has been specified (parameter name: XXXXX, line number: 12
345).Delete the specified parameters, and then try again.
KNAE03002-E The setremoteconnection command ended abnormally (12345).
```

7.2.12　setupcluster コマンド

setupcluster コマンドは、Ops Center Automator のクラスター環境をセットアップします。

構文

```
setupcluster {/exportpath exportpath | /help}
```

オプション

オプション	説明
/exportpath	データベースとサーバー情報の格納に使用する共有ディスク上のフォルダーの絶対または相対パスです。共有ディスク直下（ルートフォルダー）は指定できません。

7.2.13　setupcommonservice コマンド

setupcommonservice コマンドは、Common Services と連携するための設定コマンドです。
setupcommonservice コマンドは、Ops Center Automator を Common Services にアプリケーションとして登録し、Common Services を Ops Center Automator の認証サーバーに設定します。

メモ

setupcommonservice コマンドを使用して Ops Center 製品を削除することはできません。製品の削除は、Ops Center Portal で行います。

機能

setupcommonservice コマンドは、Ops Center Automator の URL を Common Services に登録します。登録される URL は、hcmds64chgurl コマンドに登録された URL を使用します。hcmds64chgurl に登録されている URL がブラウザーで解決できることをあらかじめ確認してから、setupcommonservice コマンドを実行してください。

このコマンドには、Common Services と Ops Center Automator との間にセキュアな接続が必要です。詳細については、「3.2.4　Common Services とのセキュア通信を設定する」を参照してください。

構文

```
setupcommonservice {[/csUri CommonServiceUri | /csUri CommonServiceUri /csUsername CommonServiceUsername] [/appName ApplicationName]
[/appDescription ApplicationDescription] [ /auto ] | /help }
```

メモ

対話モードでのパスワードの入力を求められます。

オプション

オプション	説明
csUri	Common Services の URL を指定します。（例：https://common.service/portal）
csUsername	Common Services で管理される、opscenter-security-administrator ロールを持つユーザーを指定します。ユーザー名には、1 バイトの英数字を使用できます。これには、(! # $% & '() * +-. = @ ^ _ |)が含まれます。長さは 1～255 文字です。ユーザー名の大文字と小文字は区別されます。 このオプションを指定してコマンドを実行する場合は、パスワードの入力を求められます。
appName	Common Services で表示される Ops Center Automator の名前を指定します。名前は、1～128 文字で指定できます。 新規登録時にappName を省略すると、Ops Center Automator のホスト名または IP アドレスが名前として設定されます。更新時にappName を省略すると、名前は変更されません。
appDescription	Common Services で表示される、Ops Center Automator の説明を指定します。説明は、0～512 文字で指定できます。
auto	Ops Center Automator のサービスおよびデータベースを自動で起動および停止します。

メモ

クラスター環境では、setupcommonservice コマンドを実行する前に、次の 2 つのコマンドを順に実行し、Ops Center Automator のサービスが登録されるグループをオフラインにして、フェイルオーバーを無効にした上で、データベースを起動しておく必要があります。

```
<共通コンポーネントのインストールフォルダー>¥ClusterSetup¥hcmds64clustersrvstate
 /soff /r <グループ名>
```

```
<共通コンポーネントのインストールフォルダー>¥bin¥hcmds64dbsrv /start
```

関連項目

- 3.2.4 Common Services とのセキュア通信を設定する

7.2.14 stoptask コマンド

stoptask コマンドは、実行中のタスクを停止します。

構文

```
stoptask {/taskid task-ID [/user username | /user username /passwordfile passwordfile] [/aut
hmode local | external] | /help}
```

メモ

passwordfile オプションを指定しない場合は、対話形成でパスワードの入力を求められます。

オプション

オプション	説明
/taskid	タスク識別子です。タスク識別子は、[タスク詳細] 画面、submittask コマンドの出力、listtasks コマンドの出力から確認できます。
/user	ユーザー ID です。
/passwordfile	パスワードファイルの絶対または相対パスです。
/authmode	認証方式としてexternal を指定します。local の指定は非サポートです。このオプションを省略すると、Ops Center Automator はexternal で動作します。

7.2.15　submittask コマンド

submittask コマンドは、指定されたサービス名、サービスグループ名、およびプロパティオプションを使用して実行するためにサービスを実行し、コマンドの実行出力としてタスク識別子を返します。

機能

submittask コマンドには以下の 4 つの機能があります。

- サービスの即時実行。
- サービスのスケジュール実行。
- サービスの反復実行。
- タスクの再登録。
  このオプションが指定されている場合、listtasks コマンドでの taskdetails オプションで出力されたタスクを再登録できます。

構文：サービスの即時実行

```
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}
```

構文：サービスのスケジュール実行

```
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}
```

構文：サービスの反復実行

```
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}
```

構文：タスクの再登録

```
submittask {/reregister /taskdetaildir DirectoryName
        [/setoriginalsubmitter]
        [/user UserName |
        /user UserName /passwordfile PasswordFile]
        [/authmode local | external] | /help}
```

メモ

passwordfile オプションを指定しない場合は、対話形成でパスワードの入力を求められます。

権限

- このコマンドを実行するには、Ops Center Automator の Admin、Modify、または Submit ロールで、オペレーティングシステムの管理者権限を保有している必要があります。
- ロールが設定されていないサービスグループ内のサービスは実行できません。
- 実行したいサービスはユーザーグループによって割り当てられたロールを持っているサービスグループに属している必要があります。ユーザーはユーザーグループに属している必要があります。

オプション

オプション	説明
/servicename	サービス名を指定します。 実行したいサービスの名前です。サービス名は 1～128 文字で指定できます。
/servicegroup	サービスの属するサービスグループを指定します。 サービスが属するサービスグループの名前です。これは任意のパラメーターです。 このオプションを省略すると、/user オプションで指定されたユーザーに関連付けられているサービスグループが使用されます。ただし、そのユーザーに複数のサービスグループが関連付けられている場合にはエラーが発生します。 サービスグループ名は、1～80 文字の半角英数字と_（アンダースコア）で指定できます。
/taskname	タスク名を指定します。 タスクの名前です。このオプションを省略すると、デフォルト値 *service-name_YYYYMMDDhhmmss* が使用されます。ここで *service-name* は/servicename オプションの値で、 *YYYYMMDDhhmmss* はサービスが実行された時間です。 タスク名は 1～128 文字の制御文字（'¥u0000'～'¥u001F'または '¥u007F'～'¥u009F'）を除くすべての文字で指定できます。 これは任意のパラメーターです。

オプション	説明
/taskdescription	タスクの説明を指定します。 タスクの説明です。説明は 1～256 文字の制御文字（'¥u0000'～'¥u001F'または '¥u007F'～'¥u009F'）を除くすべての文字で指定できます。 これは任意のパラメーターです。
/property	プロパティのキーと値を指定します。 サービスが使用する 1 つまたは複数のプロパティのキーと値の組み合わせが実行されます。 プロパティ値がキーに設定されていない場合、デフォルト値が使用されます。必要なプロパティキーの値がセットされていない場合、エラーが発生します。 /property オプションと/propertyfile オプションの両方を指定することはできません。両方指定するとエラーが発生します。 このオプションは、/property property-key-1 property-value-1 /property property-key-2 property-value-2 のように複数回指定できます。使用できるプロパティのキーと値の組み合わせは最大で 1,000 組です。この値は、config_user.properties ファイルの server.editor.publicProperty.perTemplate.maxnum を使用することで変更できます。 • *key* はサービスのプロパティキーです。1～1,024 文字で指定できます。キーには半角英数文字および次の文字を使用できます。/（スラッシュ）、.（ピリオド）、(ハイフン)、_（アンダースコア）。同じプロパティキーを複数回指定するとエラーが発生します。 • *value* は、*key* プロパティの値です。値にスペースまたは特殊文字が含まれている場合、引用符（"）でこの値を囲む必要があります。
/propertyfile	プロパティファイルを指定します。絶対パスまたは相対パスを使用します。 実行したいサービスが使用するプロパティ設定を定義する、絶対パスまたは相対パスを含むプロパティファイルの名前です。 プロパティファイルで指定されていないプロパティのキーと値は、デフォルト値に設定されます。必要なプロパティキーが指定されておらず、そのキーにデフォルト値がない場合にはエラーが発生します。 このオプションと/property オプションは同時に指定できません。両方のオプションを指定するとエラーが発生します。 追加の要件： • **場所：** プロパティファイルは任意のフォルダーに置くことができます。ただし、コマンドを実行するユーザーがこれにアクセスできる必要があります。 • **ファイル名：** ファイル名は任意です。 • **キー値の組み合わせの形式：** *property-key=property-value*（改行コード） *property-key=property-value*（改行コード） キーに接尾辞「@FILE」を加えると、値にテキストファイルを指定できます。例えば、key@FILE=C:¥properties¥valuefile.txt のように指定します。
/user	ユーザー ID を指定します。 サービスを実行するアクセス権限を持つ Ops Center Automator ユーザーの ID です。 ID は 1～256 文字の半角英数字で指定できます。以下を除くすべての文字を使用できます。! # $ % & ( ) * + - .= @ ¥ ^ _ |。ID の大文字と小文字は区別されません。
/passwordfile	パスワードファイルを指定します。絶対パスまたは相対パスを使用します。

オプション	説明
/passwordfile	/user オプションで指定されたユーザーのパスワードファイルを指す絶対パスまたは相対パスです。 パスワードファイルは、encryptpassword コマンドを使用して作成できます。
/wait	タスクの終了を待機します。 タスクの実行結果を表示します（正常終了または失敗）。/wait オプションが指定されていない場合、コマンドはタスクが終了するのを待たずに終了します。この場合、タスク実行が正常に開始された場合のみ、タスク識別子を報告するメッセージが提供されます。
/scheduledate	サービスを実行する日付を指定します。 このオプションが指定されている場合、以下の条件のいずれかでエラーが発生します。 • 引数の組み合わせが不正。 • 指定された日付の形式が不正。 • /scheduledate と/scheduletime で指定された時間が過去である。関連する時間がサーバー時間である。 • 指定された日付が 1994 年 1 月 1 日から 2036 年 12 月 31 日の範囲外にある。 形式： 日付は「yyyy-mm-dd」形式で指定します。年は yyyy として 4 桁で指定します。月は mm として 1（または 01）~12 の範囲で指定します。日は dd として 1（または 01）~31 の範囲で指定します。
/scheduletime	サービスを実行する日付を指定します。 このオプションが指定されている場合、以下の条件のいずれかでエラーが発生します。 • 引数の組み合わせが不正。 • 指定された時間の形式が不正。 • /scheduledate と/scheduletime で指定された時間が過去である。関連する時間がサーバー時間である。 時間は「hh:mm」形式で指定します。時間は hh として 0（または 00）~23 の範囲で指定します。分は mm として 0（または 00）~59 の範囲で指定します。

/recurrencepattern	サービスを反復するパターンを指定します。
	このオプションは、/recurrencetime オプションおよび/recurrencestart オプションとあわせて使用します。
	このオプションを指定すると、以下の条件でエラーになります。
	• 引数の組み合わせが不正。
	• 指定された固定の実行サイクルの形式が不正。
	反復オプションと形式：
	• 毎日：「daily:1h, 2h, 3h, 4h, 6h, 8h, 12h, 24h」のように指定します。デフォルト値は 24 時間毎の繰り返し実行です。
	• 週 1 回：「weekly:sun, mon, ...」のように指定します。曜日には 3 文字の省略形を使用し、コロンの後にコンマ区切りで値を続けます。曜日の順は任意です。
	  • 日： sun
	  • 月： mon
	  • 火： tue
	  • 水： wed

オプション	説明
/recurrencepattern	• 木： thu • 金： fri • 土： sat • 月 1 回： コロンに続いて 2 桁のコンマ区切りの値を指定します。月の末日の場合は「endofmonth」を指定します。
/recurrencetime	反復するサービスの実行時間を指定します。 このオプションは、/recurrencepattern オプションおよび/recurrencestart オプションとあわせて使用します。 このオプションを指定すると、以下の条件でエラーになります。 • 引数の組み合わせが不正。 • 指定された時間の形式が不正。 形式： 時間は「hh:mm」形式で指定します。時間は hh として 0（または 00）~23 の範囲で指定します。分は mm として 0（または 00）~59 の範囲で指定します。
/recurrencestart	反復するサービスを開始する日付を指定します。 このオプションは、/recurrencepattern オプションおよび/recurrencetime オプションとあわせて使用します。 このオプションを指定すると、以下の条件でエラーになります。 • 引数の組み合わせが不正。 • 指定された日付の形式が不正。 • 指定された日付が 1994 年 1 月 1 日から 2036 年 12 月 31 日の範囲外にある。 形式： 日付は「yyyy-mm-dd」形式で指定します。年は yyyy として 4 桁で指定します。月は mm として 1（または 01）~12 の範囲で指定します。日は dd として 1（または 01）~31 の範囲で指定します。
/reregister	スケジュールされたタスクを再登録したい場合に指定します。 このオプションには値がありません。
/taskdetaildir	listtasks コマンドの/taskdetails オプションで出力されたフォルダーを指定します。絶対パスまたは相対パスを使用します。 フォルダーはローカルディスクになくてはなりません。 パスの長さは最大で 180 文字です。
/setoriginalsubmitter	タスク詳細が出力された時点のユーザーとしてタスクを再登録したいかどうかを指定します。 このオプションには値がありません。 このオプションが指定されていない場合、submittask コマンドの/user に指定されたユーザー ID が、再登録後のタスクに割り当てられたユーザーになります。
/authmode	認証方式としてexternal を指定します。local の指定は非サポートです。このオプションを省略すると、Ops Center Automator はexternal で動作します。
/help	コマンドの構文と使用方法を表示します。

コマンドの場所

<Ops Center Automatorのインストールフォルダー>¥bin

終了コード

以下の表は、submittask コマンドの終了コードと説明のリストです。

終了コード	説明
0	コマンドが成功しました。
1	引数が無効です。
2	コマンドが停止しました。
3	サービスの状態が不正です。
4	同時に実行できるコマンドの数を超過しました。
5	通信が失敗しました。
6	認証が失敗しました。
7	不正なパスが指定されました。
9	パスが見つかりません。
10	パスにアクセスできません。
14	コマンドを実行する権限がありません。
17	対話形式の入力値が無効です。
130	サービスが開始しませんでした。
131	プロパティファイルが存在しません。
132	プロパティファイルの形式が不正です。
133	/wait オプションが指定されたコマンドが、現在のコマンド状態の取得に失敗しました。
134	タスクが失敗しました。
135	タスクはキャンセルされました。
136	/taskdetails オプションで指定されたフォルダーの内容が不正です。
137	/reregister オプションが指定されたコマンドで、一部のタスクを登録できませんでした。
138	/reregister オプションが指定されたコマンドで、すべてのタスクを登録できませんでした。
139	タスク詳細フォルダーの内容が、現在のバージョンまたはリビジョンとは異なります。
255	この表にリストされていないエラーが原因でコマンドが停止しました。

例：サービスの即時実行

```
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
```

例：サービスのスケジュール実行

```
submittask /servicename "Execute Remote Command"
        /propertyfile "C:¥temp¥properties.txt"
        /scheduledate 2020-01-23 /scheduletime 12:34
        /user Bob
```

例：サービスの反復実行

```
submittask /servicename "Execute Remote Command"
        /propertyfile "C:¥temp¥properties.txt"
        /recurrencepattern weekly:sun,mon,sat
        /recurrencetime 12:34 /recurrencestart 2020-01-23
        /user Bob
```

例：タスクの再登録

```
submittask /reregister /taskdetaildir "C:¥temp¥taskdetails"
        /user Bob
```

付録

付録 A　Ops Center Automator のファイルの場所とポート

ここでは、Ops Center Automator のインストール時に作成されるすべてのフォルダー、および、ポートの設定を一覧で説明します。

付録 A.1　Ops Center Automator のファイルの場所

次の表は、Ops Center Automator をインストールしたときに作成されるフォルダーを示しています。「フォルダーの場所」列にはデフォルトのパスが示されていますが、インストール時に変更できます。

フォルダーの詳細	フォルダーの場所
Ops Center Automator インストール時の指定フォルダー	*system-drive*¥Program Files¥hitachi
Ops Center Automator のインストールフォルダー	*system-drive*¥Program Files¥hitachi¥Automation
コマンドファイル	*system-drive*¥Program Files¥hitachi¥Automation¥bin
構成ファイル	*system-drive*¥Program Files¥hitachi¥Automation¥conf
サービステンプレートのフォルダー	*system-drive*¥Program Files¥hitachi¥Automation¥contents
開発中のサービステンプレートおよび部品の格納フォルダー	*system-drive*¥Program Files¥hitachi¥Automation¥develop
データファイル	*system-drive*¥Program Files¥hitachi¥Automation¥data
ヘルプファイル	*system-drive*¥Program Files¥hitachi¥Automation¥docroot
インストールおよびアンインストール時の一時作業フォルダー	*system-drive*¥Program Files¥hitachi¥Automation¥inst
ライブラリーファイル	*system-drive*¥Program Files¥hitachi¥Automation¥lib
ログファイル	*system-drive*¥Program Files¥hitachi¥Automation¥logs
システムファイル	*system-drive*¥Program Files¥hitachi¥Automation¥system
内部コマンドで使用する作業フォルダー	*system-drive*¥Program Files¥hitachi¥Automation¥webapps
作業用フォルダー	*system-drive*¥Program Files¥hitachi¥Automation¥work
共通コンポーネントのインストールフォルダー	*system-drive*¥Program Files¥hitachi¥Base64

付録 A.2　ポート設定

Ops Center Automator は、以下のポートを使用します。

外部接続ポート

ポート番号	ファイアウォール	説明
22/tcp	Automator → 操作対象	SSH に使用されます。 `cjstartsv` は、このポートを使用します。
23/tcp	Automator → 操作対象	Telnet に使用されます。 `cjstartsv` は、このポートを使用します。
443/tcp	Automator → Common Services	Common Services へのアクセスに使用されます。
445/tcp または udp	Automator → 操作対象	Windows の管理共有に使用されます。 `cjstartsv` は、このポートを使用します。
135/tcp および 139/tcp	Automator → 操作対象	Windows の管理共有に使用されます。 `cjstartsv` は、このポートを使用します。
22015/tcp	ブラウザー → Automator	HBase 64 Storage Mgmt Web Service へのアクセスに使用されます。非 SSL（非セキュア）通信では、初期設定が必要です。 このポート番号は変更できます。 `httpsd` は、このポートを使用します。
22016/tcp	ブラウザー→ Automator	HBase 64 Storage Mgmt Web Service へのアクセスに使用されます。SSL（セキュア）通信では、設定が必要です。 このポート番号は変更できます。 `httpsd` は、このポートを使用します。
25/tcp	Automator → SMTP サーバー	メール送信に使用されます。 `cjstartsv` は、このポートを使用します。 このポート番号は変更できます。詳細については、『Hitachi Ops Center Automator ユーザーズガイド』の、メールとログの設定を構成する方法について説明している箇所を参照してください。
さまざまな Web サービス接続ポート/tcp	Automator → さまざまなサーバー	Web サービス接続に登録されているサーバーに使用されます。

内部接続ポート

ポート番号	ファイアウォール	説明
22017/tcp	Automator → Automator	共通コンポーネントへのアクセスに使用されます。 `cjstartsv` は、このポートを使用します。
22018/tcp	Automator → Automator	共通コンポーネントへのアクセスに使用されます。 `cjstartsv` は、このポートを使用します。

ポート番号	ファイアウォール	説明
22025/tcp	Automator → Automator	共通コンポーネントへのアクセスに使用されます。 cjstartsv は、このポートを使用します。
22026tcp	Automator → Automator	共通コンポーネントへのアクセスに使用されます。 cjstartsv は、このポートを使用します。
22031/tcp	Automator → Automator	共通コンポーネントへのアクセスに使用されます。 cjstartsv は、このポートを使用します。
22032/tcp	Automator → Automator	共通コンポーネントへのアクセスに使用されます。 cjstartsv は、このポートを使用します。
22035/tcp	Automator → Automator	共通コンポーネントへのアクセスに使用されます。 cjstartsv は、このポートを使用します。
22036/tcp	Automator → Automator	共通コンポーネントへのアクセスに使用されます。 cjstartsv は、このポートを使用します。
22037/tcp	Automator → Automator	共通コンポーネントへのアクセスに使用されます。 cjstartsv は、このポートを使用します。
22038/tcp	Automator → Automator	共通コンポーネントへのアクセスに使用されます。 cjstartsv は、このポートを使用します。
22170/tcp	Automator → Automator	共通コンポーネントへのアクセスに使用されます。 cjstartsv は、このポートを使用します。
22171/tcp	Automator → Automator	共通コンポーネントへのアクセスに使用されます。 cjstartsv は、このポートを使用します。
22172/tcp	Automator → Automator	共通コンポーネントへのアクセスに使用されます。 cjstartsv は、このポートを使用します。
22173/tcp	Automator → Automator	共通コンポーネントへのアクセスに使用されます。 cjstartsv は、このポートを使用します。
22220/tcp	Automator → Automator	組み込みデータベースで使用されます。

メモ

これらのポートは予約済みであり、内部ポート接続にのみ使用されます。

付録 B　Configuration Manager を前提とするサービスで VSP One B20 を管理する場合の Configuration Manager のポート設定

Configuration Manager を前提とするサービスで VSP One B20 を管理する場合は、『Hitachi Ops Center API Configuration Manager REST API リファレンスガイド』に記載されたポートに加え以下のポートも開放してください。

付録 B.1　REST API で使用するポート

REST API では、デフォルトで次のポート番号を使用します。

リモートコピー操作を行う場合は、次に示すポート以外に、正サイトと副サイト間の通信でもポートを使用します。正サイトと副サイト間の通信で使用するポートについては、リモートコピーで使用するポートの説明を参照してください。

通信元		通信先		説明
マシン	ポート番号	マシン	ポート番号	
管理サーバー	any/tcp	管理サーバー （通信元と同じ）	4369/tcp	次のストレージシステムの構成変更の通知を利用するとき、REST API サーバーの内部通信に使用されます。 VSP One B20
			23459/tcp	次のストレージシステムの構成変更の通知を利用するとき、REST API サーバーの内部通信に使用されます。 VSP One B20
		ストレージシステム （ESM）	443/tcp	REST API サーバーと次のストレージシステム間の通信で使用されます。 VSP One B20
ストレージシステム （ESM）	any/tcp	管理サーバー	23454/tcp	REST API サーバーが次のストレージシステムの構成変更の通知を受信するときに使用されます。 通信先のポート番号は変更できます。 VSP One B20

付録 B.2　リモートコピーで使用するポート

リモートコピー操作を行う場合の正サイトと副サイト間の通信で使用するポートを説明します。リモートコピー操作を行う場合は、REST API で使用するポートに加えて、正サイトと副サイト間の通信でもポートを使用します。

正サイトと副サイトが入れ替わった構成の場合も、通信元のポートから通信先のポートに通信できるようにしてください。

正サイトのストレージシステムが VSP One B20 の場合

正サイト		副サイト		説明
マシン	ポート番号	マシン	ポート番号	
（通信元）ストレージシステム （ESM）	any/tcp	（通信先）ストレージシステム （ESM）	443/tcp	副サイトのストレージシステムが次の場合に、REST API サーバー間の通信に使用されます。 VSP One B20
	36000～37000/udp	（通信先）ストレージシステム （ESM）	36000～37000/udp	副サイトのストレージシステムが次の場合に、RAID Manager 間の通信に使用されます。 VSP One B20

付録 C　Ops Center Automator のプロセス

ここでは、Ops Center Automator のプロセスを一覧で説明します。

付録 C.1　プロセス一覧

プロセス一覧を次の表に示します。

この表には Ops Center Automator の状態を確認する場合に必要なプロセス情報を記載しています。Ops Center Automator のプロセス構成を表にしたものではありません。

プロセス	対応サービス名	説明
cjstartsv.exe	HAutomation Engine Web Service	共通コンポーネントで使用します。
hcmdssvctl.exe		
cjstartsv.exe	HBase 64 Storage Mgmt SSO Service	共通コンポーネントで使用します。
hcmdssvctl.exe		
httpsd.exe	HBase 64 Storage Mgmt Web Service	共通コンポーネントで使用します。
rotatelogs.exe		
httpsd.exe	HBase 64 Storage Mgmt Web SSO Service	共通コンポーネントで使用します。
rotatelogs.exe		
pdservice.exe	HiRDB/EmbeddedEdition _HD1	共通コンポーネントのデータベースで使用します。
pdprcd.exe		
pdmlgd.exe		
pdrdmd.exe		

付録 D　SSL 通信で使用する Cipher Suites

ここでは、SSL 通信で使用する Cipher Suites について説明します。

付録 D.1　サーバーとしてサポートする Cipher Suites

Ops Center Automator がサーバーとしてサポートする Cipher Suites を次の表に示します。

TLS のバージョン	Cipher Suites
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

付録 D.2　クライアントとしてサポートする Cipher Suites

Ops Center Automator がクライアントとしてデフォルトで使用できる Cipher Suites を次の表に示します。

TLS のバージョン	Cipher Suites
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_RSA_WITH_AES_128_GCM_SHA256

メモ

これらのほかに Ops Center Automator に同梱されている JDK がデフォルトで使用できる Cipher Suites を追加して使用することができます。

付録 E　SSH 接続で使用する暗号アルゴリズム

ここでは、SSH 接続で使用する暗号アルゴリズムについて一覧で説明します。

付録 E.1　サポートする暗号アルゴリズム一覧

Ops Center Automator がサポートする各暗号アルゴリズム一覧を次の表に示します。

サポートする鍵交換アルゴリズム

暗号アルゴリズム名	デフォルト値
curve25519-sha256	有効
curve25519-sha256@libssh.org	有効
diffie-hellman-group14-sha1	無効
diffie-hellman-group14-sha256	有効
diffie-hellman-group16-sha512	有効
diffie-hellman-group18-sha512	有効
diffie-hellman-group-exchange-sha256	有効
ecdh-sha2-nistp256	有効
ecdh-sha2-nistp384	有効
ecdh-sha2-nistp521	有効

サポートする Cipher アルゴリズム

暗号アルゴリズム名	デフォルト値
3des-cbc	無効
aes128-cbc	無効
aes128-ctr	有効
aes128-gcm@openssh.com	有効
aes192-cbc	無効
aes192-ctr	有効
aes256-cbc	無効
aes256-ctr	有効
aes256-gcm@openssh.com	有効
chacha20-poly1305@openssh.com	有効

サポートする MAC アルゴリズム

暗号アルゴリズム名	デフォルト値
hmac-sha1	無効
hmac-sha1-96	無効
hmac-sha1-etm@openssh.com	無効
hmac-sha2-256	有効
hmac-sha2-256-etm@openssh.com	有効
hmac-sha2-512	有効
hmac-sha2-512-etm@openssh.com	有効

サポートするホスト鍵の公開鍵アルゴリズム

暗号アルゴリズム名	デフォルト値
ecdsa-sha2-nistp256	有効
ecdsa-sha2-nistp384	有効
ecdsa-sha2-nistp521	有効
rsa-sha2-256	有効
rsa-sha2-512	有効
ssh-dss	有効
ssh-ed25519	有効
ssh-rsa	有効

サポートする公開鍵認証の公開鍵アルゴリズム

暗号アルゴリズム名
ecdsa-sha2-nistp256
ecdsa-sha2-nistp384
ecdsa-sha2-nistp521
rsa-sha2-256
rsa-sha2-512
ssh-dss
ssh-ed25519
ssh-rsa

注　鍵種別および鍵長に対応する暗号アルゴリズムが自動的に使用されます。

付録 F　トラブルシューティング

ここでは、Ops Center Automator サーバーでエラーが発生した場合の対処方法について説明します。メッセージまたはログファイルを確認してエラーの原因を特定し、それに応じて対処してください。

付録 F.1　保守情報を収集する

問題が発生してもメッセージが出力されない場合、またはメッセージの指示に従っても問題を修正できない場合は、保守情報を収集してからユーザーサポートに連絡してください。

付録 F.2　ログファイルを収集する

hcmds64getlogs コマンドを実行して、ログファイルを収集します。収集できるファイルおよびこのコマンドの詳細は、「7.1.10　hcmds64getlogs コマンド」を参照してください。

操作手順

1. Administrator 権限のユーザーとして、管理サーバーにログインします。
2. hcmds64getlogs コマンドを実行して、ログファイルを収集します。

```
<共通コンポーネントのインストールフォルダー>¥bin¥hcmds64getlogs /dir 出力フォルダーのパス
```

操作結果

アーカイブファイルが指定先に出力されます。

株式会社 日立製作所
〒 100-8280　東京都千代田区丸の内一丁目 6 番 6 号