

Hitachi Automation Director

インストールガイド

4010-1J-011-80

対象製品

Hitachi Automation Director 10.6.1

輸出管理に関する注意

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ます、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。

Active Directory は、米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。

AIX は、世界の多くの国で登録された International Business Machines Corporation の商標です。

Cisco は、Cisco Systems, Inc. またはその関連会社の米国およびその他の一定の国における登録商標または商標です。

Internet Explorer は、米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。

Linux は、Linus Torvalds 氏の日本およびその他の国における登録商標または商標です。

Microsoft は、米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。

Oracle と Java は、Oracle Corporation 及びその子会社、関連会社の米国及びその他の国における登録商標です。

Red Hat is a registered trademark of Red Hat, Inc. in the United States and other countries.

Red Hat は、米国およびその他の国における Red Hat, Inc. の登録商標です。

Red Hat Enterprise Linux is a registered trademark of Red Hat, Inc. in the United States and other countries.

Red Hat Enterprise Linux は、米国およびその他の国における Red Hat, Inc. の登録商標です。

RSA および BSAFE は、米国 EMC コーポレーションの米国およびその他の国における商標または登録商標です。

UNIX は、The Open Group の商標です。

Windows は、米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。

Windows Server は、米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。

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。

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

This product includes software developed by Ben Laurie for use in the Apache-SSL HTTP server project.

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/>

This product includes software developed by Ralf S. Engelschall <rse@engelschall.com> for use in the mod_ssl project (<http://www.modssl.org/>).

This product includes software developed by IAIK of Graz University of Technology.

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 Daisuke Okajima and Kohsuke Kawaguchi (<http://relaxngcc.sf.net/>).

This product includes software developed by Andy Clark.



本製品は、米国 EMC コーポレーションの RSA BSAFE®ソフトウェアを搭載しています。
Java is a registered trademark of Oracle and/or its affiliates.

HITACHI
Inspire the Next

株式会社 日立製作所



発行

2021年7月 4010-1J-011-80

著作権

All Rights Reserved. Copyright© 2019, 2021, Hitachi, Ltd.

目次

はじめに.....	9
対象読者.....	10
マニュアルの構成.....	10
マイクロソフト製品の表記について.....	10
関連マニュアル.....	11
このマニュアルで使用している記号.....	11
KB（キロバイト）などの単位表記について.....	12
1.概要.....	13
1.1 製品の概要.....	14
1.2 関連する Hitachi Command Suite 製品について.....	14
1.3 Automation Director システム構成.....	14
1.4 Automation Director のインストールと構成のワークフロー.....	16
1.5 Automation Director での認証方法.....	17
2.Automation Director をインストールする.....	19
2.1 インストールの前提条件.....	20
2.1.1 サーバ時刻を変更する.....	20
2.1.2 名前解決設定を変更する.....	21
2.1.3 ポートの衝突を回避する.....	22
2.2 Automation Director をインストールする（Windows）.....	22
2.3 クラスタ環境で Automation Director をインストールする（Windows）.....	23
2.3.1 クラスタ環境での Automation Director の使用について.....	23
2.3.2 クラスタインストールワークフロー.....	24
2.3.3 クラスタ管理ソフトウェアを使用してクラスタ構成を確認する.....	25
2.3.4 アクティブノードで Automation Director クラスタ化をセットアップする.....	25
2.3.5 スタンバイノードで Automation Director クラスタ化をセットアップする.....	26
2.3.6 サービスを登録しクラスタインストールの初期設定を行う.....	27
2.4 Automation Director をインストールする（Linux）.....	28
2.5 データベースフォルダのウイルススキャンを抑止する.....	29
2.6 インストール後のタスク.....	29
2.6.1 登録済み URL を確認する（Windows）.....	29
2.6.2 登録済み URL を確認する（Linux）.....	30
2.6.3 インストールを確認する.....	30

2.6.4 ライセンスを登録する.....	30
2.6.5 System アカウントのパスワードを変更する.....	31
2.6.6 System アカウントのメールアドレスを設定する.....	31
2.6.7 共通コンポーネントを使用する製品および Automation Director のサービスを停止および開始する...31	
(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開始する (Windows)	31
(2) 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開始する (Linux)	32
(3) コマンドプロンプトから Automation Director サービスのみ停止および開始する (Windows) ..	32
(4) コマンドプロンプトから Automation Director サービスのみ停止および開始する (Linux)	32
3.Automation Director を構成する.....	33
3.1 管理サーバのシステム設定を変更する.....	34
3.1.1 管理サーバ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.....	34
3.1.2 ポート番号を変更した場合の共通コンポーネントのプロパティ更新.....	35
3.1.3 ユーザーアカウントを管理するサーバの情報を変更する.....	36
3.1.4 管理サーバのホスト名または IP アドレスを変更する.....	37
3.1.5 管理サーバの URL を変更する.....	37
3.1.6 管理サーバの JDK を変更する.....	38
3.2 セキュア通信を構成する.....	38
3.2.1 Automation Director のセキュリティ設定について.....	38
3.2.2 管理クライアントのセキュリティを構成する.....	39
(1) 管理クライアントのセキュア通信について.....	39
(2) VMware vCenter を使用する場合にサーバ上で SSL をセットアップする.....	39
(3) セキュアなクライアント通信のためにサーバ上で SSL をセットアップする (Windows)	39
(4) セキュアなクライアント通信のためにサーバ上で SSL をセットアップする (Linux)	44
(5) Web ベースの管理クライアントで SSL をセットアップする.....	48
3.2.3 外部認証サーバのセキュア通信を設定する.....	49
(1) 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.....	49
(2) プライマリサーバへの認証接続のポート番号を変更する (Windows)	50
(3) プライマリサーバへの認証接続のポート番号を変更する (Linux)	50
3.2.4 Web サービス接続の証明書をインポートする.....	51
3.2.5 ESX クラスタサービスの VMware サーバ証明書をインストールする (Windows)	52
3.2.6 ESX クラスタサービスの VMware サーバ証明書をインストールする (Linux)	53
3.2.7 Device Manager サーバ証明書をインポートする.....	53
(1) Device Manager サーバの証明書をインポートする.....	54
(2) 共通コンポーネントのトラストストアに各 Device Manager のサーバ証明書をインポートする	
.....	54
3.2.8 Automation Director サーバと REST API サーバの間で SSL 通信を使用するための設定を指定する (認	
証局によるサーバ証明書を使っている場合)	55
3.2.9 サーバ証明書の有効期限を確認する.....	56
3.3 監査ログ.....	56
3.3.1 監査ログを設定する.....	56
3.3.2 監査ログを有効にする.....	57
3.3.3 auditlog.conf ファイルの設定.....	58
3.3.4 auditlog.conf ファイルのサンプル.....	60
3.3.5 監査ログに出力されるデータのフォーマット.....	60
3.4 別のホストへ Automation Director を移動する.....	62
3.5 システム構成を変更する.....	63
3.6 メール通知を構成する.....	70
3.7 パスワードポリシーを変更する	72
3.8 アカウントロックについて.....	74

3.8.1 アカウントロックポリシーについて.....	74
3.8.2 アカウントロックポリシーを設定する.....	74
3.8.3 System アカウントを自動的にロックする.....	75
3.8.4 アカウントのロックを解除する.....	75
3.9 操作対象機器との接続に使用される情報を構成する	76
3.10 エージェントレス接続の Windows 前提条件.....	80
3.11 エージェントレス接続の SSH 前提条件.....	81
3.11.1 パスワード認証.....	82
3.11.2 公開鍵認証.....	82
3.11.3 キーボードインタラクティブ認証.....	84
3.12 1 つの Automation Director サーバから複数の Device Manager インスタンスを使用する.....	85
4.外部認証サーバでのユーザー管理.....	87
4.1 外部認証サーバでのユーザー管理.....	88
4.2 外部認可サーバとの連携とは.....	88
4.3 LDAP ディレクトリサーバでユーザー認証するための操作フロー.....	88
4.4 RADIUS サーバでユーザー認証するための操作フロー.....	89
4.5 Kerberos サーバでユーザー認証するための操作フロー.....	90
4.6 ユーザーエントリーのデータ構造とは.....	91
4.6.1 BaseDN とは.....	91
4.6.2 階層構造モデルとは.....	92
4.6.3 フラットモデルとは.....	92
4.7 複数の外部認証サーバと連携している場合の構成.....	93
4.8 外部認証サーバと外部認可サーバの登録.....	95
4.8.1 LDAP ディレクトリサーバで認証する場合の exauth.properties ファイルの設定項目.....	96
4.8.2 LDAP ディレクトリサーバで認証する場合の exauth.properties ファイルの設定例.....	101
4.8.3 RADIUS サーバで認証する場合の exauth.properties ファイルの設定項目.....	103
4.8.4 RADIUS サーバで認証する場合の exauth.properties ファイルの設定例.....	108
4.8.5 Kerberos サーバで認証する場合の exauth.properties ファイルの設定項目.....	109
4.8.6 Kerberos サーバで認証する場合の exauth.properties ファイルの設定例.....	113
4.9 情報検索用のユーザーアカウントとは.....	115
4.9.1 情報検索用のユーザーアカウントの条件.....	115
4.9.2 情報検索用のユーザーアカウントの登録.....	116
4.9.3 情報検索用のユーザーアカウントの削除.....	117
4.9.4 情報検索用ユーザーアカウントを登録済みの LDAP ディレクトリサーバの確認.....	118
4.10 共有秘密鍵の登録.....	118
4.10.1 共有秘密鍵の削除.....	119
4.10.2 共有秘密鍵が登録されている RADIUS サーバの確認.....	119
4.11 外部認証サーバおよび外部認可サーバとの接続確認.....	119
4.12 外部認証サーバとの連携設定に使用するコマンドに関する注意事項.....	121
4.13 Kerberos 認証に使用できる暗号タイプ.....	122
5.Automation Director を削除する.....	123
5.1 Automation Director を削除する (Windows)	124
5.2 クラスタ環境で Automation Director を削除する.....	124
5.3 認証データを削除する (Windows)	126
5.4 Automation Director を削除する (Linux)	127

5.5 認証データを削除する (Linux)	127
付録 A Automation Director のファイルの場所とポート	129
A.1 Automation Director のファイルの場所	130
A.2 ポート設定	131
付録 B hcnds64keytool ユーティリティを使用して証明書を管理する	135
付録 C トラブルシューティング	137
C.1 保守情報を収集する	138
C.2 ログファイルを収集する	138
索引	139



はじめに

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

- 対象読者
- マニュアルの構成
- マイクロソフト製品の表記について
- 関連マニュアル
- このマニュアルで使用している記号
- KB (キロバイト) などの単位表記について

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

Automation Director の概要について説明しています。

第2章 Automation Director をインストールする

クラスタと非クラスタ両方の環境における Microsoft® Windows®、または非クラスタ環境における Red Hat Enterprise Linux(RHEL)/CentOS/Oracle Linux での、Automation Director のインストール方法について説明しています。

第3章 Automation Director を構成する

Automation Director を構成する方法について説明しています。

第4章 外部認証サーバでのユーザー管理

外部認証サーバ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 Automation Director を削除する

Automation Director を削除する方法について説明しています。

付録A Automation Director のファイルの場所とポート

Automation Director 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 hcnds64keytool ユーティリティを使用して証明書を管理する

hcnds64keytool ユーティリティの使用方法について説明しています。

付録C トラブルシューティング

Automation Director サーバ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
Internet Explorer	Internet Explorer®
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® 2008 R2 • Microsoft® Windows Server® 2012

表記	製品名
	<ul style="list-style-type: none"> • Microsoft® Windows Server® 2012 R2 • Microsoft® Windows Server® 2016 • Microsoft® Windows Server® 2019
Windows Server 2008	Microsoft® Windows Server® 2008 R2
Windows Server 2012	次の製品を区別する必要がない場合の表記です。 <ul style="list-style-type: none"> • Microsoft® Windows Server® 2012 • Microsoft® Windows Server® 2012 R2
Windows Server 2016	Microsoft® Windows Server® 2016
Windows Server 2019	Microsoft® Windows Server® 2019

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 Automation Director ユーザーズガイド*, 4010-1J-010
- *Hitachi Automation Director Service Builder ユーザーズガイド*, 4010-1J-013
- *Hitachi Automation Director メッセージ*, 4010-1J-014
- Hitachi Command Suite ドキュメント
- Hitachi Tuning Manager ドキュメント

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。
[]	ウィンドウのタイトル、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、ウィンドウ内のテキストを示します。 例：[OK] をクリックします。
斜体	<ul style="list-style-type: none"> • マニュアルのタイトルまたはテキスト内で強調する語を示します。 • 変数を示します。これは、ユーザーが入力する実際のテキストのプレースホルダ、またはシステムから出力されるプレースホルダです。例： <pre>pairdisplay -g group</pre> (この変数の規則の例外については、山括弧の説明を参照してください。)
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： <pre>pairdisplay -g oradb</pre>
<> (山括弧)	次のような場合に、変数を示します。 <ul style="list-style-type: none"> • 変数は、周囲のテキストや他の変数から明確には区切られません。例： <pre>Status-<report-name><file-version>.csv</pre> • 見出しに変数が含まれる場合。
[] (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。

規則	説明
{ } (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。

概要

この章では、以下について説明します。

- 1.1 製品の概要
- 1.2 関連する Hitachi Command Suite 製品について
- 1.3 Automation Director システム構成
- 1.4 Automation Director のインストールと構成のワークフロー
- 1.5 Automation Director での認証方法

1.1 製品の概要

Hitachi Automation Director 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、Automation Director 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管理タスクを自動化します。

Automation Director 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 Command Suite 製品について

Hitachi Automation Director は、以下のコンポーネントを含む Hitachi Command Suite の一部です。

- Hitachi Device Manager
- Hitachi Tiered Storage Manager
- Hitachi Dynamic Link Manager
- Hitachi Replication Manager
- Hitachi Tuning Manager
- Hitachi Global Link Manager
- Hitachi Compute Systems Manager

Automation Director を他の Hitachi Command Suite 製品と同じサーバにインストールすると、共通の設定でユーザーとセキュリティを管理できます。また、Automation Director を Device Manager が稼働しているサーバにインストールすると、2つの製品によって管理されるホスト情報が自動的に同期されるため、ホスト管理の作業効率が向上します。



メモ Automation Director と Device Manager の両方を使用した場合に同期されるのはホスト情報のみで、他の種類のリソースの情報は同期されません。

1.3 Automation Director システム構成

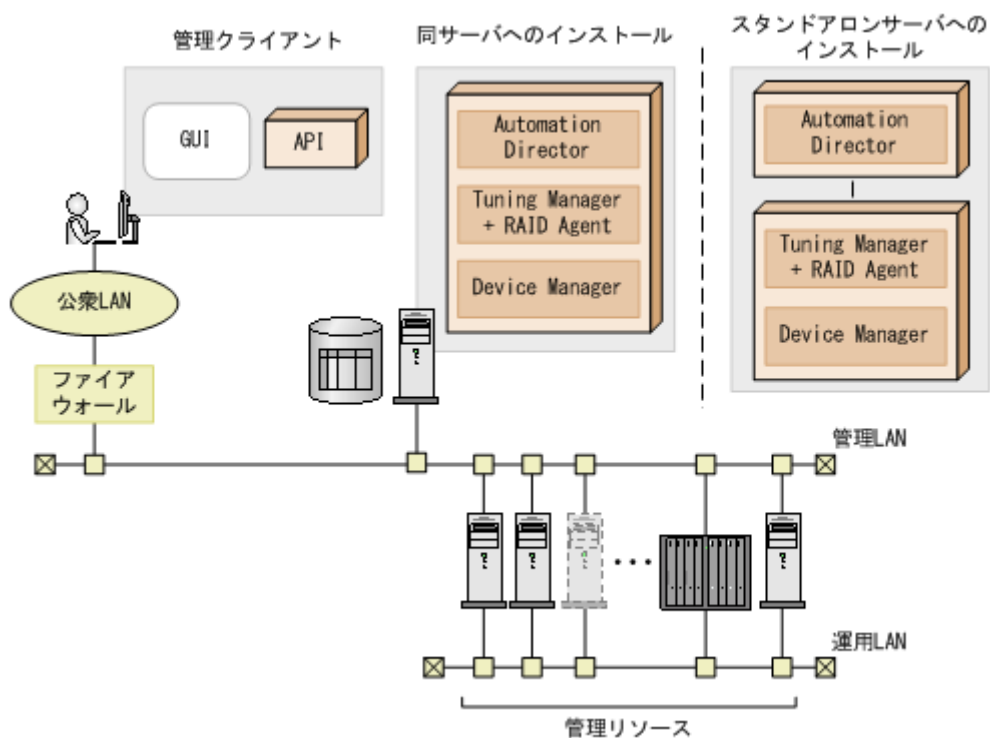
Automation Director 環境をセットアップするときのシステム構成について説明します。

Hitachi Device Manager を前提製品とする場合

Device Manager を前提製品とする場合の基本的なシステム構成は、次のいずれかがあります。

- Automation Director と Device Manager を同じサーバにインストールします。
- Automation Director はスタンドアロンサーバへインストールし、その他の Hitachi Command Suite 製品は別のサーバへインストールします。

Device Manager を前提製品とする場合の基本的なシステム構成を次の図に示します。



メモ

`hcnds64prmset` コマンドを使用して、同一サーバ構成をスタンドアロンセットアップに変更することもできます。



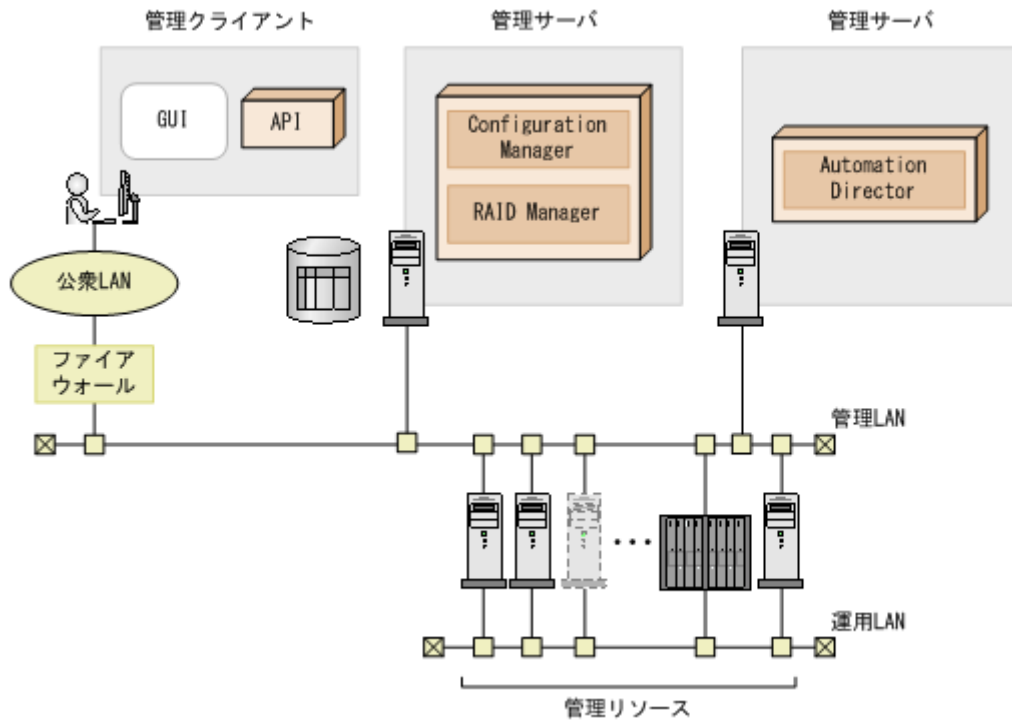
メモ

Automation Director がサポートできる Device Manager サーバの最大数は 50 です。追加情報については、Automation Director のリリースノートを参照してください。

Configuration Manager を前提製品とする場合

Configuration Manager を前提製品とする場合は、Automation Director を管理サーバにインストールし、Configuration Manager を別の管理サーバへインストールするか、Automation Director と Configuration Manager を同じ管理サーバにインストールすることもできます。

Configuration Manager を前提製品とする場合の基本的なシステム構成を次の図に示します。



1.4 Automation Director のインストールと構成のワークフロー

次の図は、Automation Director 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 Automation Director ユーザーズガイド』を参照してください。

1.5 Automation Director での認証方法

Automation Director 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：

外部認証 (LDAP 認証、RADIUS 認証、または Kerberos 認証) を使用したい場合に選択します。

ローカルユーザー認証：

Automation Director 固有でユーザー認証を使用したい場合に選択します。

Automation Director をインストールする

この章では、クラスタと非クラスタ両方の環境における Microsoft® Windows®、および非クラスタ環境における Red Hat Enterprise Linux(RHEL)/CentOS/Oracle Linux での、Automation Director のインストール方法について説明します。

- 2.1 インストールの前提条件
- 2.2 Automation Director をインストールする (Windows)
- 2.3 クラスタ環境で Automation Director をインストールする (Windows)
- 2.4 Automation Director をインストールする (Linux)
- 2.5 データベースフォルダのウイルススキャンを抑制する
- 2.6 インストール後のタスク

2.1 インストールの前提条件

Automation Director 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、Automation Director のリリースノートを参照してください。
- Automation Director 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。
- 関連マシンの名前を解決します。
- 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、Windows 管理者権限が取得されてい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、Linux の root 権限が取得されていることを確認します。
- サーバ上のセキュリティ監視、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。
- 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。
- サーバのシステム時刻が正しいことを確認します。共通コンポーネントを使用する製品が別のサーバにインストールされている場合は、Automation Director サーバの時刻を当該サーバと同期させます。
- RHEL/CentOS/Oracle Linux の場合、必要に応じて Automation Director のファイアウォール例外を、手動で再追加します。これらの例外は、インストール時に自動的に再構成されません。
- RHEL/CentOS/Oracle Linux の場合、/tmp ディレクトリが noexec オプションを使用せずにマウントされていることを確認します。

関連参照

- [2.1.2 名前解決設定を変更する](#)
- [2.1.1 サーバ時刻を変更する](#)
- [付録 A.2 ポート設定](#)

2.1.1 サーバ時刻を変更する



重要 Automation Director サーバの OS の時刻設定が、共通コンポーネントを使用する製品の管理サーバと同期している必要があります。

Automation Director のタスクおよびアラート発生時刻は、管理サーバの時刻設定に基づきます。したがって、サーバの 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、Automation Director をインストールする前にリセットしてください。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のサービスが実行しているときに Automation Director サーバの時刻を変更した場合、Automation Director が正しく動作しないことがあります。

NTP など、サーバ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 Automation Director 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の OS を構成する必要があります。サーバがサポートを提供しないかぎり、Automation Director は新しい DST ルールをサポートできません。

サーバ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。
 - マシンの時刻を戻した場合 (サーバの時刻が進んでいた場合) は、サーバのクロックが記録した時刻 (変更を加えたときのサーバの時刻) を示すまで待つってから、マシンを再起動します。
 - マシンの時刻を進めた場合は、すぐにマシンを再起動します。

Automation Director 管理サーバ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

Automation Director と、共通コンポーネントを使用する製品を 2 台の異なるマシンにインストールした場合は、クライアントに接続する Automation Director サーバの名前を解決する必要があります。

Automation Director がインストールされているマシンの名前も解決する必要があります。

Automation Director を、共通コンポーネントを使用する製品と同じマシンにインストールした場合は、Automation Director にアクセスするためにブラウザを実行するマシン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、IP アドレスがホスト名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

Automation Director を新しくインストールする前に、管理サーバ上で Automation Director 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** 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するためです。

関連タスク

- [3.1.1 管理サーバ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](#)

関連参照

- [付録 A.2 ポート設定](#)

2.2 Automation Director をインストールする (Windows)

このマニュアルでは、単体インストールメディアから製品インストーラを使用して Automation Director をインストール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。このコマンドの実行方法については、『*Hitachi Automation Director ユーザーズガイド*』を参照してください。



メモ Automation Director を、共通コンポーネントを使用するほかの製品ととも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てください。

操作手順

1. システムがインストール前のチェックリストに記載されているすべての管理サーバ前提条件を満たしていることを確認します。
2. サーバ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
3. インストールメディアを DVD ドライブに挿入します。
 4. 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
 5. 画面の指示に従って、必要な情報を指定します。
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] ウィンドウが開きます。
 6. [完了] をクリックします。



メモ

SSL 通信が有効な環境、または共通コンポーネントのポート番号が変更された環境に Automation Director をインストールする場合、[インストール完了] ウィンドウで [インストール完了時に Hitachi Command Suite GUI を起動する] チェックボックスを選択してもグラフィカルユーザーインターフェースが起動しないことがあります。
この問題が発生した場合は、変更された管理サーバ情報をチェックしてから、Web ブラウザのアドレスバーに Automation Director の URL を入力して、インターフェースを起動します。

操作結果

これで、Automation Director がインストールされます。

関連参照

- [2.6 インストール後のタスク](#)

2.3 クラスタ環境で Automation Director をインストールする (Windows)

Windows クラスタ環境に Automation Director をインストールします。



メモ Automation Director は、Windows クラスタ環境だけをサポートします。Automation Director は、Linux 環境でのクラスタリングをサポートしていません。

2.3.1 クラスタ環境での Automation Director の使用について

Automation Director 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 Automation Director は、マルチサブネット構成のクラスタへのインストールはサポートしていません。

クラスタ環境で Automation Director を使用するときには、次のように、1 台の Automation Director サーバ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。

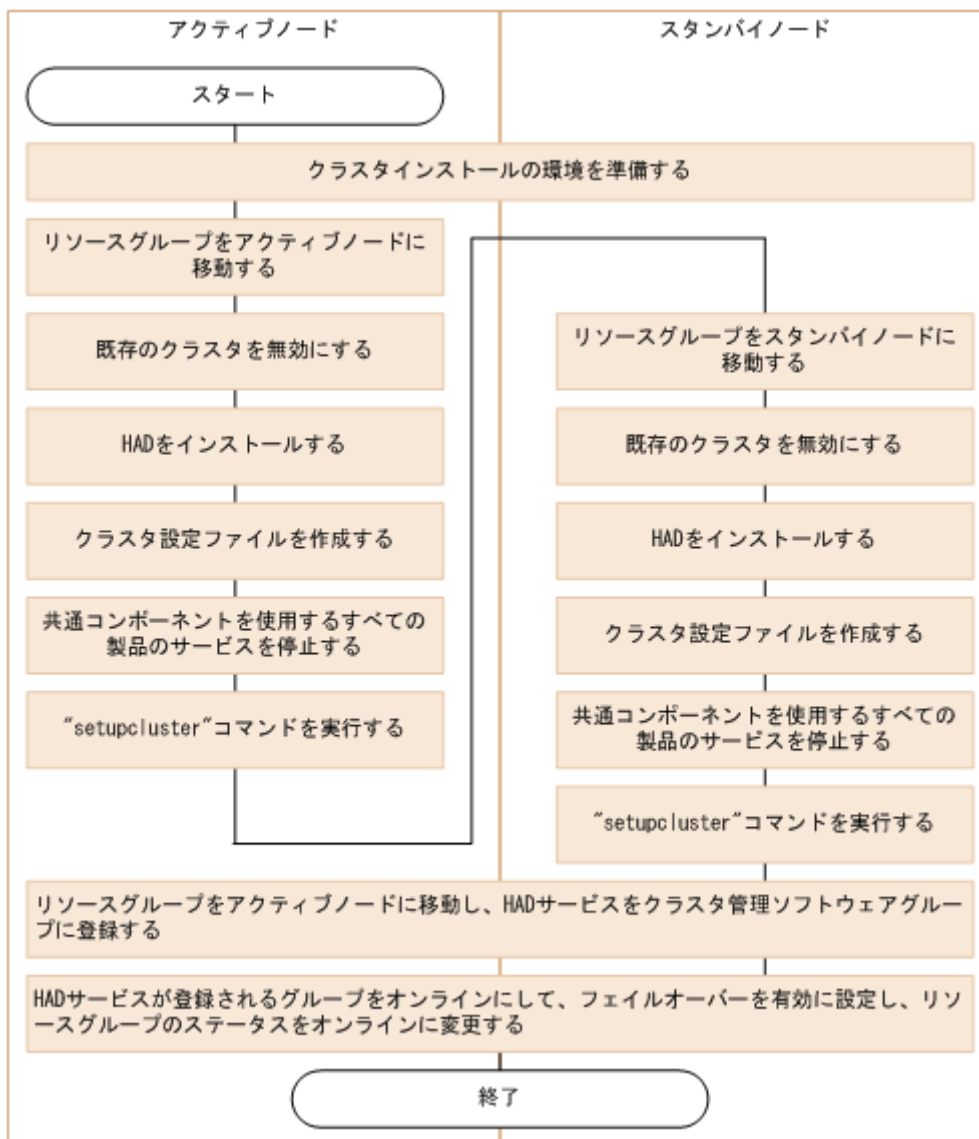


メモ アクティブノードがスタンバイノードにフェイルオーバーした場合、実行中のタスクは失敗するので、スタンバイノード上でタスクを再び実行する必要があります。

2.3.2 クラスタインストールワークフロー

Automation Director をクラスタ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 Automation Director をクラスタ環境にインストールするとき、または非クラスタ環境からクラスタ環境に移行するときには、クラスタ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。このコマンドの実行方法については、『*Hitachi Automation Director ユーザーズガイド*』を参照してください。



メモ 既にクラスタ構成でインストールされている Automation Director 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。

関連タスク

- [2.3.4 アクティブノードで Automation Director クラスタ化をセットアップする](#)
- [2.3.5 スタンバイノードで Automation Director クラスタ化をセットアップする](#)

2.3.3 クラスタ管理ソフトウェアを使用してクラスタ構成を確認する

クラスタ環境で Automation Director をセットアップするときには、クラスタ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。

クラスタ環境で Automation Director をセットアップする前に、クラスタ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、クラスタ管理ソフトウェアを使用して、Automation Director 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、クラスタ管理 IP アドレスと論理ホスト名です。
- クラスタ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。

クラスタ環境で使用されるサービスは、クラスタ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「ロール」など異なる名前と呼ばれることがあります。

2.3.4 アクティブノードで Automation Director クラスタ化をセットアップする

クラスタ構成のアクティブノード上の管理サーバで、Automation Director の新規インストールを完了することができます。

操作手順

1. クラスタ管理 IP アドレスと共有ディスクをオンラインにします。クラスタインストールのリソース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>%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。たとえば、グループ名が Automation Director cluster の場合は、"Automation Director cluster" と指定します。

3. アクティブノード上の Automation Director の新規インストールを完了します。
共通コンポーネントを使用するほかの製品がクラスタ環境に既に存在する場合は、Automation Director をインストールする前に、以下のことを確認してください。管理サーバの IP アドレスとして、論理ホストの IP アドレスを指定します。
共通コンポーネントを使用するほかの製品がクラスタ環境に存在しない場合は、Automation Director をインストールする前に、以下のことを確認してください。管理サーバの IP アドレスとして、アクティブノードの IP アドレスを指定します。
4. 使用する製品のライセンスを登録します。アクティブノードの IP アドレスにアクセスします。
5. クラスタ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。Automation Director 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内に構築される製品である場合は、以下を実行します。
 - a. 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 という名前でも共通コンポーネントのインストールフォルダ>%conf に保存します。

6. 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>%bin%hcmds64srv /stop/server
AutomationWebService
7. **setupcluster /exportpath** コマンドを実行します。exportpath には、絶対または相対フォルダパスを指定します。

関連タスク

- [2.3.5 スタンバイノードで Automation Director クラスタ化をセットアップする](#)

2.3.5 スタンバイノードで Automation Director クラスタ化をセットアップする

アクティブノードでクラスタ化インストールを設定した後、クラスタ構成のスタンバイノード上の管理サーバで Automation Director のインストールを完了できます。

操作手順

1. クラスタ管理ソフトウェアで、Automation Director 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 [Move] を選択してから、[Select Node] または [Move this service or application to another node] 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>%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。たとえば、グループ名が Automation Director cluster の場合は、"Automation Director cluster" と指定します。

3. スタンバイノード上の Automation Director の新規インストールを完了します。
スタンバイノードに Automation Director をインストールする前に、以下の要件に注意してください。
 - ・ アクティブノードと同じ場所に Automation Director 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既に存在し、クラスタ環境でアクティブな場合、管理サーバの IP アドレスとして論理ホスト名 (クラスタ管理 IP アドレスに割り当てられる仮想ホスト名) を指定します。クラスタ環境に、共通コンポーネントを使用するほかの製品がない場合、スタンバイノードの IP アドレスまたはホスト名を指定します。
4. 使用する製品のライセンスを登録します。
5. クラスタ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。もし Automation Director 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>
```

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>%conf に保存します。



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。

6. 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を確実に停止します。
hcmds64srv /stop /server AutomationWebService
7. **setupcluster /exportpath** コマンドを実行します。exportpath には、絶対または相対フォルダパスを指定します。

2.3.6 サービスを登録しクラスタインストールの初期設定を行う

Automation Director をクラスタ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、クラスタ化をオンラインにできます。

操作手順

1. クラスタ管理ソフトウェアで、Automation Director 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 [Move] を選択してから、[Select Node] または [Move this service or application to another node] を選択します。
2. 次のコマンドを使用して、クラスタ管理ソフトウェアグループで Automation Director 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>%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（Automation Director 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。たとえば、グループ名が Automation Director cluster の場合は、"Automation Director cluster"と指定します。
 - /sd
クラスタ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（Automation Director 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>%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（Automation Director 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。たとえば、グループ名が Automation Director cluster の場合は、"Automation Director cluster"と指定します。
4. クラスタソフトウェアで、リソースグループのステータスを [online] に変更します。

## 2.4 Automation Director をインストールする（Linux）

このマニュアルでは、単体インストールメディアから製品インストーラを使用して Automation Director をインストール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。このコマンドの実行方法については、『Hitachi Automation Director ユーザーズガイド』を参照してください。



**メモ** Automation Director を、共通コンポーネントを使用するほかの製品ととも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てください。

### 操作手順

1. `install.sh` を実行して、Automation Director をインストールします。

Linux での Automation Director のインストール先ディレクトリは、デフォルトでは `/opt/hitachi/Automation` です。

### 関連参照

- [2.6 インストール後のタスク](#)

## 2.5 データベースフォルダのウイルススキャンを抑止する

インストール時にウイルス検出プログラムが起動してデータベースフォルダをスキャンすると、インストールに時間が掛かる、または、失敗することがあります。

### 操作手順

1. インストール時のデータベースフォルダのウイルススキャンを抑止するために、以下のフォルダまたはディレクトリを、ウイルススキャンの対象外としてウイルススキャンプログラムに登録します。



**メモ** 以下のフォルダやディレクトリ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せん。

- Windows の場合：  
`system-drive¥Program Files¥hitachi¥Automation`  
`system-drive¥Program Files¥hitachi¥database`  
`system-drive¥Program Files¥hitachi¥Base64¥HDB`
- Linux の場合：  
`/opt/hitachi/Automation`  
`/var/opt/hitachi/Automation`  
`/var/opt/hitachi/Base64/HDB`  
`/var/opt/hitachi/database`

### 操作結果

登録されたフォルダやディレクトリは、インストール時のウイルススキャンの対象になりません。

## 2.6 インストール後のタスク

Automation Director 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. ユーザーアカウントを管理するサーバが SSL 通信を使用する場合、**hcnds64prmset** コマンドを実行して、サーバのポート番号を設定します（必要に応じて）。
2. 登録済み URL を確認します。
3. Automation Director 管理サーバへのアクセスを確認します。
4. ライセンスを登録します。
5. System アカウントのパスワードを変更します。
6. System アカウントのメールアドレスを設定します。
7. 共通コンポーネントおよび Automation Director のサービスを停止し、再開します（必要に応じて）。

System アカウントのパスワードは、必ず変更してください。

### 2.6.1 登録済み URL を確認する (Windows)

Automation Director のインストール後に、登録済み URL を確認します。

### 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>%bin%hcnds64chgurl /list`
2. URL 内のホスト名を確認します。非クラスタ環境では、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。登録済み URL が正しくなかった場合には、次のコマンドを使用して 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>%bin%hcnds64chgurl /change http://<変更前の IP アドレスまたはホスト名>:<ポート番号> http://<変更後の IP アドレスまたはホスト名>:<ポート番号>`

## 2.6.2 登録済み URL を確認する (Linux)

Automation Director のインストール後に、登録済み URL を確認します。

### 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ディレクトリ>/bin/hcmds64chgurl -list`
2. URL 内のホスト名を確認します。非クラスタ環境では、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。登録済み URL が正しくなかった場合には、次のコマンドを使用して URL を変更します。  
`<共通コンポーネントのインストールディレクトリ>/bin/hcmds64chgurl -change http://<変更前の IP アドレスまたはホスト名>:<ポート番号> http://<変更後の IP アドレスまたはホスト名>:<ポート番号>`

## 2.6.3 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 ブラウザから確認してください。

### 操作手順

1. Automation Director によってサポートされている Web ブラウザを開きます。
2. アドレスバーに、Automation Director の URL を次の形式で指定します。  
`http://<Automation Director 管理サーバの IP アドレスまたはホスト名>:22015/Automation/`

### 操作結果

管理サーバにアクセスできることを確認するログインウィンドウが開きます。

## 2.6.4 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 Automation Director 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. ログインウィンドウの [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。

## 2.6.5 System アカウントのパスワードを変更する

System アカウントは、Automation Director のユーザー管理および実行権限を持つデフォルトのアカウントです。Automation Director を初めてインストールするときには、System アカウントのパスワードを必ず変更してください。

### 操作手順

1. 管理クライアントから、次の認証情報を使用してログインします。  
ユーザー ID : system  
パスワード (デフォルト) : manager
2. [管理] タブで、[プロファイル] をクリックします。
3. [パスワード変更] をクリックし、必要なパスワードを入力して [OK] をクリックします。

## 2.6.6 System アカウントのメールアドレスを設定する

Automation Director のシステム操作に関するメール通知を Automation Director からシステムへ送信できるようにするには、System アカウントのメールアドレスを設定する必要があります。

### 操作手順

1. [管理] タブで [プロファイル] をクリックします。
2. [プロファイル] 画面で [プロファイル編集] をクリックし、フルネームとメールアドレスを入力して、[OK] をクリックします。

### 操作結果

System アカウントのメールアドレスが設定されます。

メール通知を受信するには、システム設定を実施してメールの SMTP サーバ接続情報を設定し (IP アドレスまたはホスト名、ユーザー ID、パスワードおよびポートはすべて必須です)、システム・パラメータ設定でメール通知を有効にする必要があります。詳細については、『Hitachi Automation Director ユーザーズガイド』を参照してください。

## 2.6.7 共通コンポーネントを使用する製品および Automation Director のサービスを停止および開始する

共通コンポーネントを使用する製品および Automation Director 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開始する (Windows)

次の手順により、共通コンポーネントを使用するすべての製品 (Automation Director を含む) のサービスを停止および開始します。

### 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>%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.exe /stop  
サービスを開始するには、次のコマンドを入力します。  
hcmds64srv.exe /start



## (2) 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開始する (Linux)

次の手順により、共通コンポーネントを使用するすべての製品 (Automation Director を含む) のサービスを停止および開始します。

### 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ディレクトリ>/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。  
`hcnds64srv -stop`  
サービスを開始するには、次のコマンドを入力します。  
`hcnds64srv -start`

## (3) コマンドプロンプトから Automation Director サービスのみ停止および開始する (Windows)

### 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>%bin に移動します。
2. サービスを停止または開始します。
  - サービスを停止するには、次のコマンドを入力します。  
`hcnds64srv.exe /stop /server AutomationWebService`
  - サービスを開始するには、次のコマンドを入力します。  
`hcnds64srv.exe /start /server AutomationWebService`

## (4) コマンドプロンプトから Automation Director サービスのみ停止および開始する (Linux)

### 操作手順

1. <共通コンポーネントのインストールディレクトリ>/bin に移動します。
2. サービスを停止または開始します。
  - サービスを停止するには、次のコマンドを入力します。  
`hcnds64srv -stop -server AutomationWebService`
  - サービスを開始するには、次のコマンドを入力します。  
`hcnds64srv -start -server AutomationWebService`



## Automation Director を構成する

この章では、Automation Director を構成する方法について説明します。

- 3.1 管理サーバのシステム設定を変更する
- 3.2 セキュア通信を構成する
- 3.3 監査ログ
- 3.4 別のホストへ Automation Director を移動する
- 3.5 システム構成を変更する
- 3.6 メール通知を構成する
- 3.7 パスワードポリシーを変更する
- 3.8 アカウントロックについて
- 3.9 操作対象機器との接続に使用される情報を構成する
- 3.10 エージェントレス接続の Windows 前提条件
- 3.11 エージェントレス接続の SSH 前提条件
- 3.12 1 つの Automation Director サーバから複数の Device Manager インスタンスを使用する

## 3.1 管理サーバのシステム設定を変更する

ここでは、Automation Director 管理サーバ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

Automation Director 管理サーバと管理クライアント (Web ブラウザ) 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。クラスタシステムの場合、実行系サーバと待機系サーバで同じ手順を実施してください。



**メモ** Automation Director 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。

Automation Director 管理サーバと管理クライアント間のポート番号を変更するには：

#### 操作手順

1. Automation Director 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。

Windows の場合：

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

Linux の場合：

```
<共通コンポーネントのインストールディレクトリ>/uCPsB/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
```

- b. command\_user.properties ファイルの command.http.port の行を変更します。  
クラスタシステムの場合、この定義ファイルは別のフォルダに含まれています。

Windows (非クラスタ環境) の場合：

```
<Automation Director のインストールフォルダ>%conf
```

Windows (クラスタ環境) の場合：

```
<共有フォルダ名>%Automation%conf
```

Linux の場合：

```
/opt/hitachi/Automation/conf
```

- c. config\_user.properties ファイルの server.http.port の行を変更します。  
クラスタシステムの場合、この定義ファイルは別のフォルダに含まれています。

Windows (非クラスタ環境) の場合：

```
<Automation Director のインストールフォルダ>%conf
```

Windows (クラスタ環境) の場合：

```
<共有フォルダ名>%Automation%conf
```

Linux の場合：

```
/opt/hitachi/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。
- user\_httpsd.conf ファイルを開きます。  
Windows の場合：  
<共通コンポーネントのインストールフォルダ>%uCPsB%httpsd%conf%user\_httpsd.conf  
Linux の場合：  
<共通コンポーネントのインストールディレクトリ>/uCPsB/httpsd/conf/user\_httpsd.conf
  - 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。
- OS が Windows の場合は、**hcnds64fwcancel** 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。
  - OS が Linux の場合は、OS の仕様に従って例外登録をします。手順については、OS のマニュアルを参照してください。
5. Automation Director を開始します。
6. **hcnds64chgurl** コマンドを実行して、Automation Director にアクセスするための URL を更新します。

#### 関連概念

- [2.6.7 共通コンポーネントを使用する製品および Automation Director のサービスを停止および開始する](#)

#### 関連参照

- [3.1.2 ポート番号を変更した場合の共通コンポーネントのプロパティ更新](#)
- [付録 A.2 ポート設定](#)

### 3.1.2 ポート番号を変更した場合の共通コンポーネントのプロパティ更新

Automation Director のポート番号を変更する場合は、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を更新する必要があります。

| 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インストール先フォルダ)     | 更新場所                                         |
|---------------|-----------------------------------------|----------------------------------------------|
| 22015/TCP     | %uCPsB%httpsd%conf%user_httpsd.conf     | Listen                                       |
|               |                                         | Listen [::]:                                 |
|               |                                         | #Listen 127.0.0.1:                           |
| 22016/TCP     | %uCPsB%httpsd%conf%user_httpsd.conf     | VirtualHost タグの <i>host-name:port-number</i> |
|               |                                         | Listen                                       |
|               |                                         | Listen [::]:                                 |
| 22031/TCP     | %uCPsB%httpsd%conf%user_hso_httpsd.conf | Listen                                       |
| 22032/TCP     | %HDB%CONF%emb%HiRDB.ini                 | PDNAMEPORT                                   |

| 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インストール先フォルダ)                                              | 更新場所                                 |
|---------------|----------------------------------------------------------------------------------|--------------------------------------|
|               | ¥HDB¥CONF¥pdsys                                                                  | pd_name_port                         |
|               | ¥database¥work¥def_pdsys                                                         | pd_name_port                         |
| 22035/TCP     | ¥uCPSB¥CC¥web¥redirector<br>¥workers.properties                                  | worker.HBase64StgMgmtSSOService.port |
|               | ¥uCPSB¥CC¥server¥usrconf¥ejb<br>¥HBase64StgMgmtSSOService<br>¥usrconf.properties | webserver.connector.ajp13.port       |
| 22036/TCP     | ¥uCPSB¥CC¥server¥usrconf¥ejb<br>¥HBase64StgMgmtSSOService<br>¥usrconf.properties | ejbserver.rmi.naming.port            |
| 22037/TCP     | ¥uCPSB¥CC¥server¥usrconf¥ejb<br>¥HBase64StgMgmtSSOService<br>¥usrconf.properties | ejbserver.http.port                  |
| 22038/TCP     | ¥uCPSB¥CC¥server¥usrconf¥ejb<br>¥HBase64StgMgmtSSOService<br>¥usrconf.properties | ejbserver.rmi.remote.listener.port   |
| 22170/TCP     | ¥uCPSB¥CC¥server¥userconf¥ejb<br>¥AutomationWebService<br>¥usrconf.properties    | webserver.connector.ajp13.port       |
| 22170/TCP     | ¥uCPSB¥CC¥web¥redirector<br>¥workers.properties                                  | worker.Automation.port               |
| 22171/TCP     | ¥uCPSB¥CC¥server¥userconf¥ejb<br>¥AutomationWebService<br>¥usrconf.properties    | ejbserver.rmi.naming.port            |
| 22172/TCP     | ¥uCPSB¥CC¥server¥userconf¥ejb<br>¥AutomationWebService<br>¥usrconf.properties    | ejbserver.http.port                  |
| 22173/TCP     | ¥uCPSB¥CC¥server¥userconf¥ejb<br>¥AutomationWebService<br>¥usrconf.properties    | ejbserver.rmi.remote.listener.port   |

### 3.1.3 ユーザーアカウントを管理するサーバの情報を変更する

必要に応じて、ユーザーアカウントを管理するサーバの情報を変更できます。



**メモ** ユーザーアカウントは、接続先の Device Manager がインストールされているホスト上の共通コンポーネントによって管理されます。

#### 操作手順

1. Device Manager の HBase 64 Storage Mgmt Web Service に対して SSL が設定されていない場合は、このコマンドを実行します。

Windows :

<共通コンポーネントのインストールフォルダ>%bin%hcmds64prmset /host <Device Manager サーバの IP アドレスまたはホスト名> /port <Device Manager の HBase 64 Storage Mgmt Web Service のポート番号 (非 SSL) >

Linux:

<共通コンポーネントのインストールディレクトリ>/bin/hcmds64prmset -host <Device Manager サーバの IP アドレスまたはホスト名> -port <Device Manager の HBase 64 Storage Mgmt Web Service のポート番号 (非 SSL) >

2. Device Manager の HBase 64 Storage Mgmt Web Service に対して SSL が設定されている場合は、このコマンドを実行します。

Windows :

<共通コンポーネントのインストールフォルダ>%bin%hcmds64prmset /host <Device Manager の IP アドレスまたはホスト名> /sslport <Device Manager の HBase 64 Storage Mgmt Web Service のポート番号 (SSL) >

Linux:

<共通コンポーネントのインストールディレクトリ>/bin/hcmds64prmset -host <Device Manager の IP アドレスまたはホスト名> -sslport <Device Manager の HBase 64 Storage Mgmt Web Service のポート番号 (SSL) >

### 3.1.4 管理サーバのホスト名または IP アドレスを変更する

管理サーバのホスト名は、Automation Director のインストール後に変更できます。

管理サーバのホスト名は最大 128 文字で、大文字と小文字が区別されます。

#### 操作手順

1. 新しい管理サーバのホスト名と IP アドレスをメモしておいてください。  
Windows マシンで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、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. 共通コンポーネントのプロパティを編集します。
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. 管理サーバのホスト名または IP アドレスを変更します。変更後、サーバを再起動します。
6. 元のホスト名または IP アドレスを使用してブラウザから管理サーバにアクセスする場合は、共通コンポーネントを使用する製品の URL を更新します。

### 3.1.5 管理サーバの URL を変更する

管理サーバのホスト名または IP アドレス、Automation Director のポート、または SSL 設定を変更した場合は、Automation Director 管理サーバの URL を変更する必要があります。Automation Director 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 (たとえば、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>%bin%hcmds64chgurl /list
2. Automation Director がスタンドアロンのサーバにインストールされている場合は、次のコマンドで Automation Director 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>%bin%hcmds64chgurl /change <変更後の URL > /type Automation

- Automation Director 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>%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。
- <管理サーバの IP アドレスまたはホスト名>は、Automation Director がインストールされている管理サーバの 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>%uCP%httpsd%conf にあります。

- 新しい URL を使用して Automation Director にアクセスできることを確認します。

### 3.1.6 管理サーバの JDK を変更する

運用開始後に、hcmds64chgjdk コマンドを実行すると、Automation Director が使用する Java Development Kit (JDK) を変更できます。詳細については、『Hitachi Automation Director ユーザーズガイド』の「hcmds64chgjdk コマンド」を参照してください。

## 3.2 セキュア通信を構成する

ここでは、Automation Director 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 Automation Director のセキュリティ設定について

Automation Director に対してセキュア通信を使用することによって、セキュリティを高めることができます。セキュア通信では、Automation Director は Automation Director ネットワーク通信に Secure Sockets Layer (SSL) または Transport Layer Security (TLS) を使用することによって、セキュリティを高めることができます。SSL または TLS により、Automation Director 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。

Automation Director は、以下のタイプの通信について、SSL または TLS を使用したセキュア通信を使用できます。

- 管理サーバと管理クライアント間の通信
- 管理サーバと外部認証サーバ (LDAP ディレクトリサーバ) 間の通信
- 管理サーバ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** セキュリティを有効にして Automation Director を使用するときには、サーバ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。サーバ証明書の有効期限が切れている場合は、有効な証明書を Automation Director に登録しないとサーバに接続できません。

## 3.2.2 管理クライアントのセキュリティを構成する

ここでは、管理サーバ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 Automation Director 管理サーバ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) VMware vCenter を使用する場合にサーバ上で SSL をセットアップする

「Allocate Volumes and Create Datastore on VMware vSphere」サービステンプレートを使用しようとする場合で、VMware vCenter Server のバージョンが v5.5u3 未満の場合は、共通コンポーネントの設定を次のように更新することで、SSL 経由で TLSv1.0 を検証する必要があります。

#### 操作手順

1. 編集のため、次のファイルを開きます。

Windows の場合：

<共通コンポーネントのインストールフォルダ>%conf%init.conf

Linux の場合：

<共通コンポーネントのインストールディレクトリ>/conf/init.conf

2. SSL プロパティを更新します。
  - a. ssl.protocol プロパティに移動して TLSv1 を追加します。
  - b. ssl.ClientCipherSuites プロパティに移動して TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA および TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA を追加します。
  - c. ファイルを保存して閉じます。
3. 共通コンポーネントを使用する製品のサービスを再起動します。

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

管理サーバ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 hcnds64ssltool 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。

詳細については、『Hitachi Command Suite システム構成ガイド』の「SSL サーバの構築 (Hitachi Command Suite 共通コンポーネント)」を参照してください。

hcnds64ssltool 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 ブラウザのバージョン  
Web ブラウザは、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 (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以外のフォルダに出力するか、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>%bin%hcmcmd64ssltool [/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 暗号用のサーバ証明書の署名アルゴリズム>] [/eccsigalg <ECC 用のサーバ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。Automation Director 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>%uCPsB%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。

- サーバ名 (管理サーバのホスト名) - 例: Automation\_Director\_SC1
- 組織単位 (セクション) - 例: Automation Director
- 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] 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証明書を必ず保存してください。

4. Automation Director を停止します。
5. 秘密鍵 (httpsdkey.pem) とサーバ証明書または自己署名証明書 (httpsd.pem) を、次のフォルダにコピーします。

<共通コンポーネントのインストールフォルダ>%uCPsB%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>%uCPSB%httpsd%conf  
%user\_httpsd.conf

7. user\_httpsd.conf ファイル内で、以下のようにします。

- a. ハッシュ[#]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
#<VirtualHost *:22016>
から
#</VirtualHost>
```

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。

以下に、user\_httpsd.conf ファイルの編集例を示します。SSL ECC を使用している場合は、以下の行も非コメント化します。

```
#SSLECCCertificateKeyFile
#SSLECCCertificateFile
```

```
ServerName <管理サーバのホスト名>
Listen 22015
Listen [::]:22015
#Listen 127.0.0.1:22015
SSLDisable
Listen 22016
#Listen [::]:22016
<VirtualHost *:22016>
ServerName <管理サーバのホスト名>
SSLEnable
SSLProtocol TLSv12
SSLRequiredCiphers 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
SSLRequiredCiphers ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-
GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256
SSLRequireSSL
SSLCertificateKeyFile
"<共通コンポーネントのインストールフォルダ>/uCPSB/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>/uCPSB/httpsd/conf/ssl/server/
httpsd.pem"
#SSLECCCertificateKeyFile
"<共通コンポーネントのインストールフォルダ>/uCPSB/httpsd/conf/ssl/server/
ecc-httpsdkey.pem"
#SSLECCCertificateFile
"<共通コンポーネントのインストールフォルダ>/uCPSB/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>/uCPSB/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
SSLECCCertificateKeyFile (ECC を使用する場合)
SSLECCCertificateFile (ECC を使用する場合)
#SSLCACertificateFile
```

認証局から発行されたチェーンサーバ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

外部サーバから管理サーバへの非 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。IPv6 環境の場合、#Listen [::]:22016 行の先頭の番号記号 (#) を削除します。

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。
- ディレクティブの途中で改行を入れないでください。
- 以下に示すディレクティブで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。
- 以下に示すディレクティブで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 hssso\_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 <管理サーバのホスト名>
Listen 22015
Listen [::]:22015
#Listen 127.0.0.1:22015
SSLDisable
Listen 22016
#Listen [::]:22016
<VirtualHost *:22016>
ServerName <管理サーバのホスト名>
SSLEnable
SSLProtocol TLSv12
SSLRequiredCiphers 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
SSLRequiredCiphers ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-
GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256
SSLRequireSSL
SSLCertificateKeyFile
"<共通コンポーネントのインストールフォルダ>/uCPSB/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>/uCPSB/httpsd/conf/ssl/server/
server-certificate-or-self-signed-certificate-file"
#SSLECCertificateKeyFile
"<共通コンポーネントのインストールフォルダ>/uCPSB/httpsd/conf/ssl/server/
ecc-httpsdkey.pem"
#SSLECCertificateFile
"<共通コンポーネントのインストールフォルダ>/uCPSB/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>/uCPSB/httpsd/conf/ssl/cacert/
certificate-file-from-certificate-authority"
Header set Strict-Transport-Security max-age=31536000
```

```
</VirtualHost>
#HWSLogSSLVerbose On
```

- Automation Director を開始します。
- 次のように hcmds64chgurl コマンドを使用して、Automation Director 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。

#### 操作結果

これで、Automation Director サーバ上で SSL が実装されます。

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

管理サーバ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ことをお勧めします。

#### 前提条件

root 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 ブラウザのバージョン  
Web ブラウザは、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ディレクトリ (再作成する場合)  
出力先パスに同じ名前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、既存の保存先ディレクトリ以外のディレクトリに出力するか、既存のファイルを削除する必要があります。

#### 操作手順

- 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ディレクトリ>/bin/hcmd64ssltool [-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 暗号用のサーバ証明書の署名アルゴリズム>] [-eccsigalg <ECC 用のサ
```

サーバ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。Automation Director 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ディレクトリ>/uCP SB/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。

- サーバ名 (管理サーバのホスト名) - 例: Automation-Director-SC1
- 組織単位 (セクション) - 例: Automation Director
- 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] 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証明書を必ず保存してください。

4. Automation Director を停止します。

5. 秘密鍵 (httpsdkey.pem) とサーバ証明書または自己署名証明書 (httpsd.pem) を、次のディレクトリにコピーします。

<共通コンポーネントのインストールディレクトリ>/uCP SB/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ディレクトリ>/uCP SB/httpsd/conf/  
user\_httpsd.conf

7. user\_httpsd.conf ファイル内で、以下のようになります。

a. ハッシュ [#]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
#<VirtualHost *:22016>
から
#</VirtualHost>
```

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。

以下に、user\_httpsd.conf ファイルの編集例を示します。SSL ECC を使用している場合は、以下の行も非コメント化します。

```
#SSLECCCertificateKeyFile
#SSLECCCertificateFile
```

```
ServerName <管理サーバのホスト名>
Listen 22015
Listen [::]:22015
#Listen 127.0.0.1:22015
SSLDisable
Listen 22016
#Listen [::]:22016
<VirtualHost *:22016>
ServerName <管理サーバのホスト名>
SSLEnable
```

```

SSLProtocol TLSv12
SSLRequiredCiphers 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
SSLRequiredCiphers ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-
GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256
SSLRequireSSL
SSLCertificateKeyFile
"<共通コンポーネントのインストールディレクトリ>/uCPSB/httpsd/conf/ssl/
server/httpsdkey.pem"
SSLCertificateFile
"<共通コンポーネントのインストールディレクトリ>/uCPSB/httpsd/conf/ssl/
server/httpsd.pem"
#SSLECCCertificateKeyFile
"<共通コンポーネントのインストールディレクトリ>/uCPSB/httpsd/conf/ssl/
server/ecc-httpsdkey.pem"
#SSLECCCertificateFile
"<共通コンポーネントのインストールディレクトリ>/uCPSB/httpsd/conf/ssl/
server/ecc-httpsd.pem"
SSLCACertificateFile
"<共通コンポーネントのインストールディレクトリ>/uCPSB/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`

`SSLECCCertificateKeyFile` (ECC を使用する場合)

`SSLECCCertificateFile` (ECC を使用する場合)

`#SSLCACertificateFile`

認証局から発行されたチェーンサーバ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

外部サーバから管理サーバへの非 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。IPv6 環境の場合、`#Listen [::]:22016` 行の先頭の番号記号 (`#`) を削除します。

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。
- ディレクティブの途中で改行を入れないでください。
- 以下に示すディレクティブで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。
- 以下に示すディレクティブで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 `hssso_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 <管理サーバのホスト名>
Listen 22015
Listen [::]:22015
#Listen 127.0.0.1:22015
SSLDisable
Listen 22016
#Listen [::]:22016
<VirtualHost *:22016>
ServerName <管理サーバのホスト名>
SSLEnable
SSLProtocol TLSv12
SSLRequiredCiphers ECDHE-ECDSA-AES256-GCM-SHA384:ECDSA-AES128-
GCM-SHA256:ECDSA-AES256-GCM-SHA384:ECDSA-AES128-GCM-
SHA256:AES256-GCM-SHA384:AES128-GCM-SHA256
SSLRequiredCiphers ECDHE-ECDSA-AES256-GCM-SHA384:ECDSA-AES128-
GCM-SHA256:ECDSA-AES256-GCM-SHA384:ECDSA-AES128-GCM-SHA256
SSLRequireSSL
SSLCertificateKeyFile
"<共通コンポーネントのインストールディレクトリ>/uCPSB/httpsd/conf/ssl/
server/httpsdkey.pem"
SSLCertificateFile
"<共通コンポーネントのインストールディレクトリ>/uCPSB/httpsd/conf/ssl/
server/server-certificate-or-self-signed-certificate-file"
#SSLECCCertificateKeyFile
"<共通コンポーネントのインストールディレクトリ>/uCPSB/httpsd/conf/ssl/
server/ecc-httpsdkey.pem"
#SSLECCCertificateFile
"<共通コンポーネントのインストールディレクトリ>/uCPSB/httpsd/conf/ssl/
server/ecc-httpsd.pem"
SSLCACertificateFile
"<共通コンポーネントのインストールディレクトリ>/uCPSB/httpsd/conf/ssl/
cacert/certificate-file-from-certificate-authority"
Header set Strict-Transport-Security max-age=31536000
</VirtualHost>
#HWSLogSSLVerbose On
```

- Automation Director を開始します。
- 次のように hcmds64chgurl コマンドを使用して、Automation Director 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。

### 操作結果

これで、Automation Director サーバ上で SSL が実装されます。

## (5) Web ベースの管理クライアントで SSL をセットアップする

管理サーバと管理クライアント間のセキュア通信を実装するには、Automation Director の Web ベースのユーザーインターフェースにアクセスするすべての Automation Director 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 ブラウザは SHA256 と RSA 署名を持つサーバ証明書をサポートする必要があります。



## 操作手順

1. 管理 Web クライアントから、次の URL を使用して、SSL 接続で管理サーバにアクセスします。  
`https://<Automation Director 管理サーバの 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と通信できるようになります。

### 3.2.3 外部認証サーバのセキュア通信を設定する

Windows 環境で Automation Director 管理サーバと LDAP ディレクトリサーバ間のセキュア通信を実装するには、StartTLS プロトコルを使用します。StartTLS を実装するには、`exauth.properties` ファイルでプロパティを更新し、LDAP ディレクトリサーバ証明書を管理サーバにインポートする必要があります。

詳細については、「[\(1\) 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](#)」を参照してください。



メモ Linux 環境で IPV6 アドレスを指定する場合は、アドレスを角括弧[]で囲む必要があります。

#### (1) 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

証明書をトラストストア (`ldapcacerts` または `jssecacerts`) にインポートするには、`hcmads64keytool` ユーティリティ (Windows の場合) または `keytool` ユーティリティ (Linux の場合) を使用します。

#### 前提条件

- 証明書を準備します。  
証明書を安全に取得します。
  - LDAP ディレクトリサーバとの通信用：  
LDAP ディレクトリサーバのサーバ証明書を発行した認証局からルート認証局までのすべての認証局が発行した証明書が、証明書チェーンを形成している必要があります。証明書は、共通コンポーネントの製品要件を満たしている必要があります。
  - 認証局を使用する場合：  
共通コンポーネントのサーバ証明書を発行した認証局からルート認証局までのすべての認証局が発行した証明書が、証明書チェーンを形成している必要があります。
  - 自己署名証明書を使用する場合：  
共通コンポーネントの自己署名証明書を取得します。
- 次の情報を確認します。
  - トラストストアファイルのパス
  - トラストストアが既に存在する場合、トラストストアにアクセスするためのパスワード

#### 操作手順

1. 次のコマンドを実行します。  
Windows の場合：

```
<共通コンポーネントのインストールフォルダ>%bin%hcmds64keytool -import -alias
<エイリアス名> -file <証明書ファイル名> -keystore <トラストストアファイル名>
> -storepass <トラストストアのパスワード>
```

Linux の場合 :

```
<共通コンポーネントのインストールディレクトリ>/uCP5B/jdk/bin/keytool -import
-alias <エイリアス名> -file <証明書ファイル名> -keystore <トラストストアフ
ァイル名> -storepass <トラストストアのパスワード>
```

説明 :

- **alias**: トラストストア内で証明書を識別するための名前を指定します。サーバ証明書が複数ある場合は、トラストストア内で使用されていない任意のエイリアス名を指定します。
- **keystore**: インポート先のトラストストアファイルのパスを指定します。トラストストアファイルが存在しない場合は、自動的に作成されます。  
LDAP ディレクトリサーバのサーバ証明書は、**ldapcacerts** にインポートする必要があります。ほかのプログラムと証明書を共有する場合は、**jssecacerts** にインポートします。
- トラストストアにアクセスするためのパスワードを指定します。



**メモ** **hcmds64keytool** ユーティリティまたは **keytool** ユーティリティで、トラストストア内のユニーク名、トラストストアのファイル名、およびパスワードを指定するときには、次の点に注意してください。

- ファイル名には次の記号を使用しないでください。  
: ; \* ? " < > |
- ファイル名は 255 バイト以内の文字列を指定してください。
- トラストストア内のユニーク名、およびパスワードには二重引用符 (") を含めないでください。

2. 共通コンポーネントのサービスを再起動します。

## (2) プライマリサーバへの認証接続のポート番号を変更する (Windows)

外部認証サーバとのセキュア通信を設定後、認証接続のポート番号を変更する必要があります。

認証接続のポート番号を変更するには、次のように **hcmds64prmset** 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>%bin%hcmds64prmset /host <プライマリサ
ーバのホスト名> /sslport <ポート番号 (SSL)>
```

方法 :

- **host** オプションには、サーバ証明書の Common Name (CN) と同じ名前を指定します。
- **sslport** オプションには、共通コンポーネントの SSL ポート番号を指定します。デフォルトは 22016 です。

## (3) プライマリサーバへの認証接続のポート番号を変更する (Linux)

外部認証サーバとのセキュア通信を設定後、認証接続のポート番号を変更する必要があります。

認証接続のポート番号を変更するには、次のように **hcmds64prmset** 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ディレクトリ>/bin/hcmds64prmset -host <プライマ
リサーバのホスト名> -sslport <ポート番号 (SSL)>
```

方法：

- host オプションには、サーバ証明書の Common Name (CN) と同じ名前を指定します。
- sslport オプションには、共通コンポーネントの SSL ポート番号を指定します。デフォルトは 22016 です。

### 3.2.4 Web サービス接続の証明書をインポートする

共通コンポーネントのトラストストアに Web サービス接続の証明書をインポートする必要があります。

次のような Web サービス接続にサーバ証明書を使用するときに、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。

- Device Manager  
Device Manager を使用する場合、共通コンポーネントで使用されるポート (22016) の証明書をインポートします。
- Configuration Manager
- VMware vCenter
- BNA
- DCNM
- その他の Web サービス接続

次の証明書もインポートする必要があります。

- 認証局
- 中間認証局
- ルート認証局

場合によっては、認証局の証明書が既にインポートされている可能性があります。この場合、この手順は不要です。

Windows の場合、**hcnds64keytool** コマンドを使用します。Unix の場合、標準 **keytool** を使用します。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。

Windows の場合：

```
<共通コンポーネントのインストールフォルダ>%bin%hcnds64keytool -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>%uCPSEB%jdk%jre%lib%security%jssecacerts -storepass <トラストストアへのアクセスパスワード> -file <サーバ証明書のパス>
```

**hcnds64srv** コマンドを実行して、サービスを再開します。

Unix の場合：

```
<共通コンポーネントのインストールディレクトリ>/uCPSEB/jre/jdk/bin/keytool -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ディレクトリ>/uCPSEB/jdk/jre/lib/security/jssecacerts -storepass <トラストストアへのアクセスパスワード> -file <サーバ証明書のパス>
```

**hcnds64srv** コマンドを実行して、サービスを再開します。

## 追加のガイドライン

- サードパーティ接続のセキュリティ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。たとえば、VMware vCenter の場合は、VMware のマニュアルを参照してください。
- サードパーティのサーバ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。

### 3.2.5 ESX クラスタサービスの VMware サーバ証明書をインストールする (Windows)

セキュア通信を使用するすべての Web サービス接続と同様に、Automation Director が参照する Automation Director 共通コンポーネントのトラストストアに、VMware サーバ証明書をインポートする必要があります。ただし、ESX クラスタサービステンプレートを使用する場合、VMware は一部の機能に独自（自己署名）のルート証明書を使用するため、VMware ルート証明書もインストールする必要があります。



**メモ** ESX クラスタサービステンプレートを使用しない場合は、この手順を完了する必要はありません。

Windows サーバに VMware サーバ証明書をインストールするには、次の手順に従う必要があります。

#### 操作手順

1. VMware サーバ証明書を次のようにダウンロードします。
  - a. Web ブラウザを使用して vCenter ユーザーインターフェースにアクセスします。
  - b. 右側の画面で、[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。
  - c. Automation Director 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上でダウンロードする場所を選択し、ダウンロードを確認します。
2. 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で、zip ファイルをダウンロードした場所に移動し、その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。

両方の証明書ファイルが含まれる、.certs フォルダが解凍されます。

3. 証明書をインストールします。
  - a. 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。
  - b. [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。
  - c. [証明書をすべて次のストアに配置する] を選択します。
  - d. [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。
  - e. 拡張子 .crl のファイルについても手順 a から d を実施します。証明書がトラストストアにインストールされます。



メモ ESX クラスタサービステンプレートを使用する場合は、『Hitachi Automation Director ユーザーズガイド』に説明されているように、Python もインストールする必要があります。

### 3.2.6 ESX クラスタサービスの VMware サーバ証明書をインストールする (Linux)

セキュア通信を使用するすべての Web サービス接続と同様に、Automation Director が参照する Automation Director 共通コンポーネントのトラストストアに、VMware サーバ証明書をインポートする必要があります。ただし、ESX クラスタサービステンプレートを使用する場合、VMware は一部の機能に独自（自己署名）のルート証明書を使用するため、VMware ルート証明書もインストールする必要があります。



メモ ESX クラスタサービステンプレートを使用しない場合は、この手順を完了する必要はありません。

Linux サーバに VMware サーバ証明書をインストールするには、次の手順に従う必要があります。

#### 操作手順

1. VMware サーバ証明書を次のようにダウンロードします。
  - a. Web ブラウザを使用して vCenter ユーザーインターフェースにアクセスします。
  - b. 右側の画面で、[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。
  - c. Automation Director 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上でダウンロードする場所を選択し、ダウンロードを確認します。
2. 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で、zip ファイルをダウンロードした場所に移動し、その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。

拡張子が .0 (xxx.0) のファイルが含まれる「lin」という名前のフォルダが解凍されます。

3. 「xxx.0」ファイルを次のディレクトリにコピーします。

```
/etc/pki/tls/certs
```

証明書がトラストストアにインストールされます。



メモ ESX クラスタサービステンプレートを使用する場合は、『Hitachi Automation Director ユーザーズガイド』に説明されているように、Python もインストールする必要があります。

### 3.2.7 Device Manager サーバ証明書をインポートする

セキュア通信を使用する 1 つまたは複数の Device Manager サーバを接続する場合、Device Manager の証明書をインポートする必要があります。使用を計画している Device Manager サーバおよびサービスの数によって、複数の証明書のインストールが必要になる場合があります。

- 複数の Device Manager サーバに接続する場合は、各サーバに証明書をインストールする必要があります。

## (1) Device Manager サーバの証明書をインポートする

Add Host 機能が有効になっている場合、各 Device Manager のサーバ証明書を取得し、自己署名証明書または認証局の証明書を Automation Director が参照する共通コンポーネントのトラストストアにインポートする必要があります。

Device Manager 証明書をインポートするには、次の手順に従う必要があります。

1. Device Manager のサーバ証明書を取得します。  
詳細については、『Hitachi Command Suite システム構成ガイド』の「SSL サーバの構築 (Device Manager サーバ)」を参照してください。
2. 自己署名証明書または認証局の証明書をインポートします。  
認証局の証明書を使用するときには、中間認証局およびルート認証局の証明書もインポートする必要があります。場合によっては、認証局の証明書が既にインポートされている可能性があります。この場合、この手順は不要です。



メモ Automation Director サーバ上の共通コンポーネントのトラストストアは、jssecacerts です。

Device Manager 証明書をインポートするときには、次のガイドラインに従ってください。

- 複数の Device Manager 構成を実行している場合は、各 Device Manager 用のサーバ証明書を取得する必要があります。
- 自己署名証明書を使用するときには、各 Device Manager サーバ用の自己署名証明書をトラストストアにインポートします。
- 認証局の証明書を使用するときには、サーバ証明書を発行する各認証局の証明書をトラストストアにインポートします。

## (2) 共通コンポーネントのトラストストアに各 Device Manager のサーバ証明書をインポートする

サーバ証明書は、各 Device Manager サーバから入手した後、Automation Director が参照する共通コンポーネントのトラストストアにインポートする必要があります。

1. Device Manager のトラストストアファイルをダウンロードします。



メモ Device Manager サーバが認証局の証明書を既に使用している場合、このステップは不要です。

Device Manager サーバが自己署名証明書を使用している場合は、Web ブラウザからトラストストアをダウンロードします。

次の URL のどちらかを使用してトラストストアをダウンロードします。SSL の場合はポート番号を 2443 に、非 SSL の場合は 2001 (デフォルト) に設定します。

SSL の場合 :

```
https://<Device Manager サーバの IP アドレスまたはホスト名>:<Device Manager サーバのポート番号 (SSL) >/service/HiCommandCerts
```

非 SSL の場合 :

```
http://<Device Manager サーバの IP アドレスまたはホスト名>:<Device Manager サーバのポート番号 (非 SSL) >/service/HiCommandCerts
```

2. 各 Device Manager の証明書をエクスポートします。



メモ Device Manager サーバが認証局の証明書を既に使用している場合、このステップは不要です。

Device Manager が自己署名証明書を使用している場合は、**hcms64keytool** を使用して、Device Manager サーバ証明書を、ダウンロードしたトラストストアからエクスポートします。ダウンロードしたトラストストアをトラストストアファイルとして指定します。

Windows の場合 :

```
<共通コンポーネントのインストールフォルダ>%bin%hcms64keytool -export -keystore <トラストストアファイル名> -alias <エイリアス名> -file <サーバ証明書のパス>
```

Linux の場合 :

```
<共通コンポーネントのインストールディレクトリ>/uCPSB/jdk/bin/keytool -export -keystore <トラストストアファイル名> -alias <エイリアス名> -file <サーバ証明書のパス>
```

3. 各 Device Manager の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。エクスポートした自己署名証明書のサーバ証明書、または認証局の証明書をトラストストアにインポートします。

Windows の場合、**hcms64keytool** を使用します。Unix の場合、Java の標準 **keytool** を使用して、証明書をインポートします。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。

Device Manager が認証局の証明書、中間認証局および (他の認証局もルートする) ルート認証局の証明書を使用している場合、認証局をインポートする必要があります。場合によっては、認証局の証明書が既にインポートされている可能性があります。この場合、この手順は不要です。

Windows の場合 :

```
<共通コンポーネントのインストールフォルダ>%bin%hcms64keytool -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>%uCPSB%jdk%jre%lib%security%jssecacerts -storepass <トラストストアへのアクセスパスワード> -file <サーバ証明書のパス>
```

Unix の場合 :

```
<共通コンポーネントのインストールディレクトリ>/uCPSB/jdk/bin/keytool -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ディレクトリ>/uCPSB/jdk/jre/lib/security/jssecacerts -storepass <トラストストアへのアクセスパスワード> -file <サーバ証明書のパス>
```

4. **hcms64srv** コマンドを実行して、サービスを再開します。

### 3.2.8 Automation Director サーバと REST API サーバの間で SSL 通信を使用するための設定を指定する (認証局によるサーバ証明書を使っている場合)

自己署名証明書または認証局の証明書を使用することで、Automation Director サーバと REST API サーバの間で使用する SSL 通信を設定することが可能です。

詳細については、『*Hitachi Command Suite 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 サーバ間で SSL 通信するよう設定する (自己署名証明書を使用する場合)」または「REST API クライアントと REST API サーバ間で SSL 通信するよう設定する (認証局が発行したサーバ証明書を使用する場合)」を参照してください。



## 3.2.9 サーバ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。管理サーバ証明書の有効期限が切れておらず、管理対象サーバ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。

共通コンポーネントのサーバ証明書の有効期限を確認するには、次のコマンドを実行します。

Windows の場合：

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

Linux の場合：

```
<共通コンポーネントのインストールディレクトリ>/uCPSB/jdk/bin/keytool -printcert -v -file <サーバ証明書のパス>
```



**メモ** 自己署名証明書の有効期限は、サーバ間の接続時には検証されません。Automation Director サーバと Web サーバ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。

## 3.3 監査ログ

監査ログには、Automation Director サーバ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、サービスの開始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、Automation Director サーバ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、サービスの開始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。

Windows の場合、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。Linux の場合、データは syslog 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	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 <ul style="list-style-type: none"><li>OS の起動またはシャットダウン</li><li>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</li><li>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</li></ul>
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 <ul style="list-style-type: none"><li>ハードウェア障害</li></ul>



カテゴリ	説明
	<ul style="list-style-type: none"> <li>ソフトウェア障害（メモリエラーなど）</li> </ul>
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 <ul style="list-style-type: none"> <li>NTP や DNS などの外部サーバとの通信</li> <li>管理サーバ（SNMP）との通信</li> </ul>
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 <ul style="list-style-type: none"> <li>ファイバーチャネルログイン</li> <li>デバイス認証（ファイバーチャネル・セキュリティプロトコル認証、iSCSI ログイン認証、SSL サーバ/クライアント認証）</li> <li>管理者またはエンドユーザー認証</li> </ul>
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 <ul style="list-style-type: none"> <li>デバイスのアクセスコントロール</li> <li>管理者またはエンドユーザーのアクセスコントロール</li> </ul>
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 <ul style="list-style-type: none"> <li>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</li> <li>監査ログファイルへのアクセス</li> </ul>
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 <ul style="list-style-type: none"> <li>設定情報の参照または更新</li> <li>アカウントの追加や削除を含むアカウント設定の更新</li> <li>セキュリティ設定</li> <li>監査ログ設定の参照または更新</li> </ul>
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 <ul style="list-style-type: none"> <li>ハードウェアコンポーネントの追加または削除</li> <li>ソフトウェアコンポーネントの追加または削除</li> </ul>
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 <ul style="list-style-type: none"> <li>ネットワークトラフィックしきい値の超過</li> <li>CPU 負荷しきい値の超過</li> <li>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</li> </ul> 異常な通信が発生したことを示すイベント <ul style="list-style-type: none"> <li>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</li> <li>未使用ポートに対するアクセス（ポートスキャンなど）</li> </ul>

### 3.3.2 監査ログを有効にする

Automation Director サーバ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、Automation Director サーバを再起動する必要があります。



#### メモ

- Automation Director サーバがインストーラーを使用してインストールされている場合は、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. 管理者権限 (Windows) または root 権限 (Linux) のユーザーとして、Automation Director にログインします。
2. 以下のどちらかにある、auditlog.conf ファイルを開きます。

#### Windows の場合

共通コンポーネントのインストール先フォルダ¥conf¥sec¥auditlog.conf

#### Linux の場合：

共通コンポーネントのインストール先ディレクトリ/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、Automation Director サーバ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。

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をすべて削除します。
5. Automation Director 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.Facility (Linux でのみ有効)

Linux で、syslog ファイルに監査ログデータを出力するファシリティ (ログタイプ) の数値を指定します。(デフォルト値：1)

Windows では、Log.Facility が指定されても無視されます。無効な値や数値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.Facility に指定できる値と syslog.conf ファイルで定義されているファシリティの対応を示します。

Log.Facility に指定できる値	syslog.conf ファイルで定義されているファシリティ
1	user
2	mail*
3	daemon
4	auth*
6	lpr*
16	local0
17	local1
18	local2

Log.Facilityに 指定できる値	syslog.conf ファイルで定義されているファシリティ
19	local3
20	local4
21	local5
22	local6
23	local7

注※ この値を指定することはできますが、推奨していません。

syslog ファイルに出力される監査ログをフィルタリングするには、Log.Facility に指定されたファシリティと各監査イベントの重要度を組み合わせます。

以下の表に、監査イベントの重要度と syslog.conf ファイルで定義されている重要度の対応を示します。

監査イベントの重要度	syslog.conf ファイルで定義されている重要度
0	emerg
1	alert
2	crit
3	err
4	warning
5	notice
6	info
7	debug

#### Log.Event.Category

出力される監査イベントカテゴリを指定します。(デフォルト値：なし)

複数のカテゴリを指定する場合は、カテゴリとカテゴリをカンマ (,) で区切ります。この場合、カテゴリ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 は大文字小文字を区別しません。無効なカテゴリ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：StartStop、Failure、LinkStatus、ExternalService、Authentication、AccessControl、ContentAccess、ConfigurationAccess、Maintenance、AnomalyEvent

#### Log.Level (Windows でのみ有効)

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。

Log.Level は、Windows でのみ有効です。Linux では、Log.Level が指定されても無視されます。また、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
1	
2	
3	
4	警告
5	情報
6	
7	
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 an integer for Facility. (specifiable range: 1-23)
Log.Facility 1

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

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。

Windows の場合には、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。Linux の場合には、Log.Facility 1 が、syslog.conf ファイルに user ファシリティとして定義されている syslog ファイルに監査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 Windows のイベントログファイルまたは Linux の syslog 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。

#### Windows の場合

プログラム名 [プロセス ID]: メッセージ部

#### Linux の場合

syslog ヘッダー部 メッセージ部

syslog ヘッダー部の形式は、OS の環境設定によって異なります。必要な場合は設定を変更してください。

例えば、rsyslog を使用し、/etc/rsyslog.conf で以下を指定する場合は、RFC5424 に従った形式でメッセージが出力されます。

```
$ActionFileDefaultTemplate RSYSLOG_SyslogProtocol23Format
```

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 syslog 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, 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-ddThh: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	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。

項目*	説明
	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,1.1,0,KAPM01124-I,2017-05-15T14:08:23.1+09:00,HBase-SSO,management-host,Authentication,Success,uid=system,,,,,,,,,,,,BasicLog,,, "The login was successful. (session ID = session ID)"
```

## 3.4 別のホストへ Automation Director を移動する

必要に応じて、Automation Director 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、管理サーバのホスト名を変更する必要があります。

### 前提条件

以下の設定が移動元のホストと移動先のホストで同じであることを確認します。

- ホスト名と IP アドレス。
- Automation Director によって使用される OS ユーザーのアカウント。
- 共通コンポーネントを使用する製品の環境（構成、バージョン、およびリビジョン）。
- Automation Director のインストールパス。

Automation Director の [タスク] タブの「状態」列が実行中、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も確認する必要があります。

### 操作手順

1. Administrator 権限を使用して管理サーバにログインします。
2. 移動元ホストで Automation Director のバックアップを完了します。
  - a. `hcnds64srv /stop` コマンドを実行して、現在のサービスを停止します。
  - 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にログインします。
5. 移動先のホストで、Automation Director のリストアを実行します。
  - a. `hcnds64srv /stop` コマンドを実行して、サービスを停止します。
  - 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. リストア先の環境に合わせて、以下の構成ファイルの設定を変更します。
    - 外部認証サーバ連携構成ファイル (`exauth.properties`)
    - セキュリティ定義ファイル (`security.conf`)
    - 監査ログ定義ファイル (`auditlog.conf`)
    - ポート番号変更設定 (`user_httpsd.conf`)
    - SSL 環境構築手順 (`user_httpsd.conf`)

これらの構成ファイルは、次のディレクトリにあります。

- ・ <バックアップ先のディレクトリ>%HBase%base%conf
- ・ <バックアップ先のディレクトリ>%HBase%base%httpsd.conf

6. ポート番号が変更された場合、新しいポート番号を反映するように、必要な設定を変更します。
7. `hcmds64srv /start` コマンドを実行して、サービスを再開します。

## 3.5 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、Automation Director 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、Automation Director 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、次のフォルダにあります。

<Automation Director のインストールフォルダ>%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 1 `config_user.properties` ファイルの設定

カテゴリ	キー名	設定	値	デフォルト値
HTTP 接続ポート番号	<code>server.http.port</code>	Automation Director サーバ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	キー名	設定	値	デフォルト値
ログ <sup>1</sup>	logger.message.server.MaxBackupIndex	サーバ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
一般的なコマンド 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コンテンツ部品 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	1~1024	100



カテゴリ	キー名	設定	値	デフォルト値
		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。たとえば、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。		
	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 または UNIX。 - 実行対象の部品が汎用コマンド実行部品またはコンテンツ部品。 [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	コンテンツ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	0~100	0

カテゴリ	キー名	設定	値	デフォルト値
		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。		
	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
リモートファイル操作の再試行	plugin.remoteFileAccess.retry.times	コンテンツ部品およびファイル転送部品によって内部実行されるファイルを操作する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でも、再試行によって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。ディスクなど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、このプロパティを設定してください。	0~100	0
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	正規表現パターンで使用できる文字列。	password   Password   PassWord

カテゴリ	キー名	設定	値	デフォルト値
		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。		
	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	対象ホストが Windows を実行している場合に実行するコンテンツ部品を含む、実行フォルダのパスを指定します。実行フォルダは、事前に作成しておく必要があります。コンテンツ部品の [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 UNIX の場合にコンテンツ部品を実行する実行ディレクトリのパスを指定します。実行ディレクトリは、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)
	plugin.remoteCommand.workDirectory.ssh	対象ホストの OS が UNIX の場合、ファイル転送部品またはコンテンツ部品の実行時に使用される作業ディレクトリを指定します。ディレクトリ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

カテゴリ	キー名	設定	値	デフォルト値
	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 Automation Director 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
ウィンドウの更新	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] ウィンドウで、Automation Director の操作に使用される端末からサーバ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
	server.editor.steps.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

カテゴリ	キー名	設定	値	デフォルト値
	server.editor.step.perLayer.maxnum	レイヤ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	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
	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 接続が確立されるまでのタイムアウト値 (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までのタイムアウト値 (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

<sup>1</sup> 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
```

## 3.6 メール通知を構成する

メール通知設定を構成し、障害発生時またはタスクに問題が発生した場合に、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・パラメータを設定する必要があります。詳細については、『Hitachi Automation Director 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。次のディレクトリにあります。

```
<Automation Director のインストールフォルダ>\%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 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	[Automation Director] \$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_NAME\$ タスク名： \$TASK_NAME\$ 実行 者:\$USER_NAME\$ タスク 詳細： \$TASK_DETAIL_URL\$

**表 3 XML エンティティ参照**

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

**表 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	
\$TASK_KIND\$	タスク種別	
\$SERVICE_NAME\$	サービス名	
\$TASK_TAGS\$	タスクのタグ	

埋め込まれる文字	項目	備考
\$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] ウィンドウの URL	http で始まる URL が設定されます。

### 3.7 パスワードポリシーを変更する

security.conf ファイルを編集すると、ユーザーパスワードの条件とロックに関連する Automation Director のさまざまな設定を構成できます。これにより、ユーザーの特定のパスワードポリシーに適したセキュリティ設定にカスタマイズできます。

ファイルは、次のフォルダにあります。

<共通コンポーネントのインストールフォルダ>%conf%sec

ファイルは、次の形式を使用します。

*specification-key-name=setting*

ファイルを編集する場合は、1行に1つの指定キーと設定を指定します。以下に、セキュリティ定義ファイルのデフォルトの状態を示します。

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

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

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

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



```

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

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

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

```

**表 5 security.conf ファイルの設定**

キー名	設定	設定可能な値	デフォルト値
password.min.length	パスワードの最小文字数を指定します。	1~256	4
password.min.uppercase	パスワードに含むべき大文字の最小数を指定します。0を指定した場合、大文字の数に関する制約はありません。	0~256	0
password.min.lowercase	パスワードに含むべき小文字の最小数を指定します。0を指定した場合、小文字の数に関する制約はありません。	0~256	0
password.min.numeric	パスワードに含むべき数字の最小数を指定します。0を指定した場合、文字の数に関する制約はありません。	0~256	0
password.min.symbol	パスワードに含むべき記号の最小数を指定します。0を指定した場合、記号の数に関する制約はありません。	0~256	0
password.check.userID	ユーザー ID と同じパスワードの設定を禁止するかどうかを指定します。	<ul style="list-style-type: none"> <li>• true : 禁止します</li> <li>• false : 禁止しません</li> </ul>	false
account.lock.num	アカウントが自動的にロックされるまでのログインの連続失敗回数を指定します。0を指定した場合、ログインの試みが失敗	0~10	0

キー名	設定	設定可能な値	デフォルト値
	してもアカウントは自動的にロックされません。		

## 3.8 アカウントロックについて

アカウントロックとは、ユーザーアカウントをロックする（一時的に無効にする）ことです。アカウントロックを有効にすることで、第三者による不正アクセスのリスクを軽減できます。管理サーバでユーザーアカウントを管理する場合は、アカウントロックを有効にすることをお勧めします。

共通コンポーネントを使用する製品では、ユーザーが複数回連続して GUI へのログインに失敗した場合に、ユーザーアカウントを自動的にロックできます。アカウントロックを有効にするには、アカウントロックポリシー（アカウントがロックされるまでのログイン連続失敗回数）を設定する必要があります。



**ヒント** アカウントをロックする方法として、ユーザーアカウントのロック状態を GUI から変更することができます。

Admin（ユーザー管理）権限を持つユーザーだけが、ロック状態を変更できます。



**注意**

- 共通コンポーネントを使用する製品の初期インストール時には、System アカウントに対してアカウントロックを行うことはできません。System アカウントには、共通コンポーネントを使用するすべての製品の Admin 権限が設定されています。セキュリティ向上のために System アカウントにアカウントロックを設定する場合は、設定を変更する必要があります。

- ユーザー認証に外部認証サーバを使用している場合、自動ロックの制御には、外部認証サーバの設定が使用されます。

### 3.8.1 アカウントロックポリシーについて

アカウントロックポリシーとは、ユーザーが複数回連続して GUI へのログインに失敗した場合に、そのユーザーアカウントを自動的にロックする（一時的に無効にする）までのログイン連続失敗回数のことです。

アカウントロックポリシーを設定すると、共通コンポーネントを使用する製品のうち、シングルサインオン機能を利用しているすべての製品に直ちに適用されます。たとえば、ログイン連続失敗回数を 3 回に設定している場合、ユーザーが Automation Director へのログインに 3 回連続して失敗すると、ユーザーアカウントが自動的にロックされます。

### 3.8.2 アカウントロックポリシーを設定する

共通コンポーネントを使用する製品のアカウントロックポリシーは、security.conf ファイルで設定します。

#### 操作手順

1. security.conf ファイルを編集します。

security.conf ファイルは次の場所に格納されています。

Windows の場合：

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

Linux の場合 :

<共通コンポーネントのインストールディレクトリ>/conf/sec/security.conf

2. `account.lock.num` パラメータを設定します。

自動的にアカウントをロックするために必要なログイン連続失敗回数を指定します。0 から 10 までの値を指定します。ユーザーが指定された回数ログインに失敗すると、そのユーザーアカウントはロックされます。0 を指定すると、ユーザーがログインに何度失敗しても、ユーザーアカウントはロックされません。

デフォルト : 0



#### 注意

- ログイン連続失敗回数を変更した場合、新しい値は、変更後の最初のログイン失敗時から有効になります。あるユーザーが現在ログインしていて、そのユーザーのアカウントを使用してログインしようとした場合、指定された回数ログインに失敗すると、そのユーザーのアカウントはロックされます。ただし、ログインしていたユーザーはそのまま操作を続けることができます。
- アカウントロックポリシーは GUI からでも設定できます。ただし、システムがクラスタ構成の場合、GUI からの設定は実行系ノードだけに適用されます。スタンバイノードに設定を適用するときは、ノードを切り替えてから同じ設定を行います。

#### 操作結果

`security.conf` ファイルの設定値を変更すると、新しいアカウントロックポリシーがすぐに有効になります。

### 3.8.3 System アカウントを自動的にロックする

System アカウントを自動的にロックするには、`user.conf` ファイルの設定を変更します。

#### 操作手順

1. 共通コンポーネントを使用する製品のサービスを停止します。
2. `user.conf` ファイルを開きます。

`user.conf` ファイルは次の場所に格納されています。

- Windows の場合 :  
<共通コンポーネントのインストールフォルダ>%conf%user.conf
- Linux の場合 :  
<共通コンポーネントのインストールディレクトリ>/conf/user.conf

`user.conf` ファイルが存在しない場合は、作成してください。

3. 次の形式で、`account.lock.system` プロパティを指定します。

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

4. 共通コンポーネントを使用する製品のサービスを起動します。

#### 操作結果

共通コンポーネントを使用するすべての製品の System アカウントに、アカウントロックが適用されます。

### 3.8.4 アカウントのロックを解除する

ロックされたユーザーアカウントは、`hcnds64unlockaccount` コマンドで解除できます。

## 前提条件

- Administrator 権限を持つユーザー (Windows の場合) または root ユーザー (Linux の場合) としてログインします。
- ロックされたユーザーアカウントに Admin 権限があることを確認します。  
ロックされたユーザーアカウントに Admin 権限がない場合、アカウントにユーザー管理の Admin 権限がある別のユーザーがアカウントのロックを解除する必要があります。
- ロックされたユーザーアカウントのユーザー ID とパスワードを確認します。

## 操作手順

1. hcmds64unlockaccount コマンドを実行して、アカウントのロックを解除します。

Windows の場合 :

```
<共通コンポーネントのインストールフォルダ>%bin%hcmd64unlockaccount [/user ユーザー ID /pass パスワード]
```

Linux の場合 :

```
<共通コンポーネントのインストールディレクトリ>/bin/hcmd64unlockaccount [-user ユーザー ID -pass パスワード]
```

user オプションや pass オプションを指定せずにコマンドを実行すると、ユーザー ID とパスワードを入力を求められます。



**注意** ユーザー ID またはパスワードに記号が使用されている場合は、コマンドラインでこれらの記号をエスケープする必要があります。

- Windows の場合 :  
ユーザー ID やパスワードの末尾に円記号 (¥) がある場合は、その円記号 (¥) を別の円記号 (¥) でエスケープしてください。  
また、ユーザー ID やパスワードにアンパサンド (&)、縦線 (|) またはキャレット (^) が含まれる場合は、それぞれの文字を引用符 (") で囲むか、キャレット (^) でエスケープしてください。
- Linux の場合 :  
それぞれの文字を円記号 (¥) でエスケープしてください。

## 3.9 操作対象機器との接続に使用される情報を構成する

Automation Director 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。  
<Automation Director のインストールフォルダ>%Automation%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。

```
<Automation Director のインストールフォルダ>\Automation\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。

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環境の一部である場合のガイドライン

クラスタの対象機器に情報を入力する場合：

- クラスタ環境で対象機器が Windows Server 2012 または Windows Server 2012 R2 を実行している場合、作業フォルダ（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。
- コンテンツ部品でスクリプトを実行する場合は、実行フォルダ（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	1	64
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	0~65535	0	65535

キー名	設定	有効値	最小値	最大値
	telnet.port.number 設定に優先します。			
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： <ul style="list-style-type: none"> <li>汎用コマンド実行部品</li> <li>ファイル転送部品</li> <li>ターミナル接続部品</li> <li>コンテンツ部品</li> </ul> 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。たとえば、「Username:」と指定します。	正規表現パターンで使用する文字列	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 文字を使用できます。たとえば、「Password:」と指定します。	正規表現パターンで使用する文字列	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の共有フォルダ名を指定します。フォルダは wmi.workDirectory.share	1 バイトの英数字、「-」、「_」、および「。」。	0 文字	80 文字

キー名	設定	有効値	最小値	最大値
	dPath 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。			
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。フォルダは wmi.workDirectory.shareName 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/Unix 対象機器のプロパティです。ファイル転送部品またはコンテンツ部品で転送用ファイルが置かれるディレクトリ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、親ディレクトリのパスも、ファイル転送部品の接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コンテンツ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、config_user.propert	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
	ies ファイルで定義された plugin.remoteCommand. workDirectory.ssh の値で す。0~128 文字の文字列 を指定します。			
common.executionDirectory	対象に対してコンテンツ 部品を実行するときの実 行フォルダを指定します。 部品定義で定義された実 行フォルダの値が設定さ 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、 config_user.properties ファイルで定義され 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。		0 文字	128 文字

### 3.10 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、次のセクションに記載されている 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

administrator 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。

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



メモ OS を再起動する必要はありません。



項目	値
レジストリキー	HKEY_LOCAL_MACHINE¥SOFTWARE¥Microsoft¥Windows¥CurrentVersion¥Policies¥System
レジストリエントリ	LocalAccountTokenFilterPolicy
レジストリエントリ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

管理共有を使用して、レジストリエディタで次のレジストリのキーの下にエンTRIESを設定し、OSを再起動します。

項目	値
レジストリキー	HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Services¥Lanmanserver¥parameters
レジストリエントリ	AutoShareServer
レジストリエントリ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 AutoShareServer /t REG_DWORD /d 1
```

## 3.11 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、次のセクションに記載されている 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。

- コンテンツ部品
- 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。

### 3.11.1 パスワード認証

SSH サーバ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。  
HP-UX の場合 : `/opt/ssh/etc/sshd_config`  
他の OS の場合 : `/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、コメントアウトのハッシュ記号 (`#`) を削除します。
4. 次のコマンドを実行して、`sshd` サービスを再開します。  
RHEL/CentOS/SUSE Linux/Oracle Linux (RHEL 6.4 など) の場合 : `/etc/rc.d/init.d/sshd restart`  
Solaris (Solaris 10 など) の場合 : `/usr/sbin/svcadm restart ssh`  
AIX (AIX 6.1 など) の場合 : `kill -HUP [Process ID of sshd]`  
HP-UX (HP-UX 11i V3 など) の場合 : `/sbin/init.d/secsh stop; /sbin/init.d/secsh start`



**メモ** これらのコマンドは、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、OS のマニュアルを参照してください。

---

### 3.11.2 公開鍵認証

ここでは、SSH サーバ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 サーバのセットアップ

公開鍵認証を使用するには、SSH サーバ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。  
HP-UX : `/opt/ssh/etc/sshd_config`  
HP-UX 以外 : `/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、コメントアウトのハッシュ記号 (`#`) を削除します。
4. 次のコマンドを実行して、`sshd` サービスを再開します。  
RHEL/CentOS/SUSE Linux/Oracle Linux (RHEL 6.4 など) の場合 : `/etc/rc.d/init.d/sshd restart`  
Solaris (Solaris 10 など) の場合 : `/usr/sbin/svcadm restart ssh`  
AIX (AIX 6.1 など) の場合 : `kill -HUP [Process ID of sshd]`  
HP-UX (HP-UX 11i V3 など) の場合 : `/sbin/init.d/secsh stop; /sbin/init.d/secsh start`



**メモ** これらのコマンドは、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、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、Automation Director 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。



**メモ** 秘密鍵を別の OS に移動すると、秘密鍵が漏えいしてセキュリティリスクを負う恐れがあります。ただし、別の OS 上で作成された鍵を使用することは可能です。

参考として、以下の手順では RHEL6.4（Linux）上で鍵を作成します。

### 1. `ssh-keygen` コマンドを実行します。

RSA 鍵を作成する場合：`ssh-keygen -t rsa`

DSA 鍵を作成する場合：`ssh-keygen -t dsa`

### 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、Return 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 Return キーを押します。

## Automation Director への秘密鍵の配置

Automation Director がインストールされる OS 上に秘密鍵を配置します。任意の場所に配置し、パスをプロパティファイル（`config_user.properties`）の `ssh.privateKeyFile` に設定します。

## 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

- Automation Director アプリケーションにログインします。
- [管理] > [サービス共有プロパティ]を選択します。
- 秘密鍵のパスフレーズを開きます（SSH 公開鍵認証の場合）。
- 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)。

### 3.11.3 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。  
HP-UX : `/opt/ssh/etc/sshd_config`  
HP-UX 以外 : `/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。  
RHEL/CentOS/SUSE、Linux/Oracle Linux、Linux/AIX/HP-UX の場合 :
  - `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、コメントアウトのハッシュ記号 (#) 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、コメントアウトのハッシュ記号 (#) を削除します。)Solaris10 の場合 :  
`PAMAuthenticationViaKBDInt` の値を `yes` に設定します。  
(`PAMAuthenticationViaKBDInt` の行がコメントアウトされている場合は、コメントアウトのハッシュ記号 (#) を削除します。)  
Solaris11 の場合 :  
`KbdInteractiveAuthentication` の値を `yes` に設定します。  
(`KbdInteractiveAuthentication` の行がコメントアウトされている場合は、コメントアウトのハッシュ記号 (#) を削除します。)
4. AIX の場合、以下の設定を行います。



メモ AIX OS 以外の場合は、設定を変更する必要はありません。

---

- `/etc/pam.conf` を開き、以下を追加します。
  - `# Authentication` ブロックの内側  
`sshd auth required /usr/lib/security/pam_aix` を追加します。
  - `# Account Management` ブロックの内側  
`sshd account required /usr/lib/security/pam_aix` を追加します。
  - `# Password Management` ブロックの内側  
`sshd auth required /usr/lib/security/pam_aix` を追加します。
  - `# Password Management` ブロックの内側  
`sshd password required /usr/lib/security/pam_aix` を追加します。
  - `# Session Management` ブロックの内側  
`sshd session required /usr/lib/security/pam_aix` を追加します。
- `/etc/ssh/sshd_config` を開いて、次の行を変更します。  
`UsePAM = no` を `UsePAM = yes` に変更します。(UsePAM の行がコメントアウトされている場合は、コメントアウトのハッシュ記号 (#) を削除します。)

- /etc/security/login.cfg を開いて、次の行を変更します。  
auth\_type = STD\_AUTH を auth\_type = PAM\_AUTH に変更します。(auth\_type の行がコメントアウトされている場合は、コメントアウトのハッシュ記号 (#) を削除します。)
5. 次のコマンドを実行して、sshd サービスを再開します。サポートされる各 OS についてコマンド例を示します。

- RHEL/CentOS/SUSE Linux/Oracle Linux (RHEL 6.4 など) の場合：

```
/etc/rc.d/init.d/sshd restart
```

- Solaris (Solaris 10 など) の場合：

```
/usr/sbin/svcadm restart ssh
```

- AIX (AIX 6.1 など) の場合：

```
kill -HUP [Process ID of sshd]
```

- HP-UX (HP-UX 11i V3 など) の場合：

```
/sbin/init.d/secsh stop; /sbin/init.d/secsh start
```



**メモ** これらのコマンドは、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。

## 3.12 1 つの Automation Director サーバから複数の Device Manager インスタンスを使用する

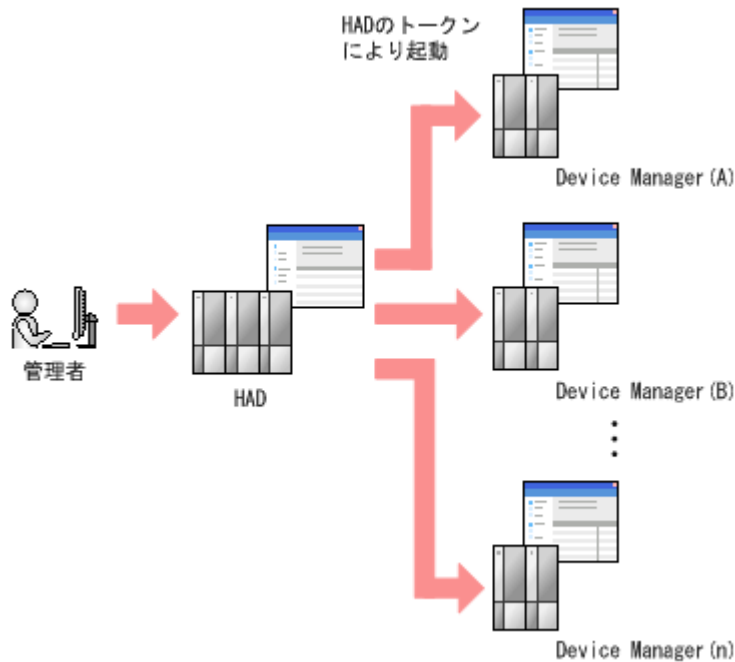
Automation Director では、1 つの Automation Director サーバから複数の Device Manager インスタンスを使用することができます。この機能は、1 つのトークンだけを（主に）使用する複数の共通コンポーネント認証サーバ間の相互認証を使用することによって可能になります。

相互認証とは、クライアント/サーバ接続経路でアプリケーショントラフィックを送信する前にクライアントがサーバに身元を証明しなければならず、サーバがクライアントに身元を証明しなければならないセキュリティ機能です。

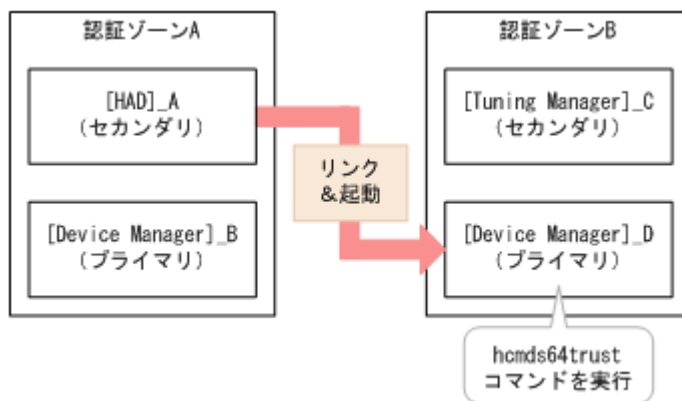


**メモ** 相互認証は、システムアカウントや共通コンポーネントの内部アカウント（セットアップやその他の内部機能に使用される）などのビルトインアカウントでは行うことができません。

次の図は、1 つの Automation Director サーバから複数の Device Manager インスタンスを使用する例を示しています。



次の図は、2つの認証ゾーンの相互認証を示しています。図のあとで、このシナリオをセットアップするプロセスについて説明しています。



### 相互認証構成プロセス

1. サーバ ID を変更するには、`hcnds64chgtsid` コマンドを使用します。サーバ ID がデフォルトのホスト名の場合、このステップは不要です。
2. [Device Manager]\_D で `hcnds64trust` コマンドを実行し、[Device Manager]\_B の接続先情報を登録します。
3. 認証ゾーン A と認証ゾーン B で相互認証を行うユーザーの設定を、次のように選択します。
  - 共通ユーザー管理に登録されたユーザーを使用する場合は、認証ゾーン A と認証ゾーン B の共通ユーザー管理に同じユーザーを登録し、権限を付与します。
  - 共通ユーザー管理に登録されていない外部認証グループのユーザーを使用する場合は、グループ DN (そのユーザーが含まれる認証サーバ上の外部ユーザーグループ) を認証ゾーン A と認証ゾーン B の共通ユーザー管理に登録し、必要な権限を付与します。

## 外部認証サーバでのユーザー管理

この章では、外部認証サーバ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 外部認証サーバでのユーザー管理
- 4.2 外部認可サーバとの連携とは
- 4.3 LDAP ディレクトリサーバでユーザー認証するための操作フロー
- 4.4 RADIUS サーバでユーザー認証するための操作フロー
- 4.5 Kerberos サーバでユーザー認証するための操作フロー
- 4.6 ユーザーエントリーのデータ構造とは
- 4.7 複数の外部認証サーバと連携している場合の構成
- 4.8 外部認証サーバと外部認可サーバの登録
- 4.9 情報検索用のユーザーアカウントとは
- 4.10 共有秘密鍵の登録
- 4.11 外部認証サーバおよび外部認可サーバとの接続確認
- 4.12 外部認証サーバとの連携設定に使用するコマンドに関する注意事項
- 4.13 Kerberos 認証に使用できる暗号タイプ

## 4.1 外部認証サーバでのユーザー管理

外部認証サーバに登録したユーザーアカウントを使用して Automation Director にログインできます。外部認証サーバと連携すると、Automation Director のためのログインパスワードの管理やアカウントの制御が不要になります。Automation Director は、次の外部認証サーバと連携させることができます。

- LDAP ディレクトリサーバ
- RADIUS サーバ
- Kerberos サーバ

## 4.2 外部認可サーバとの連携とは

外部認証サーバでユーザー認証を行う場合には、外部認可サーバも併用することで、管理サーバ（共通コンポーネントを使用する製品）に対するアクセス可否を外部認可サーバで制御できます。

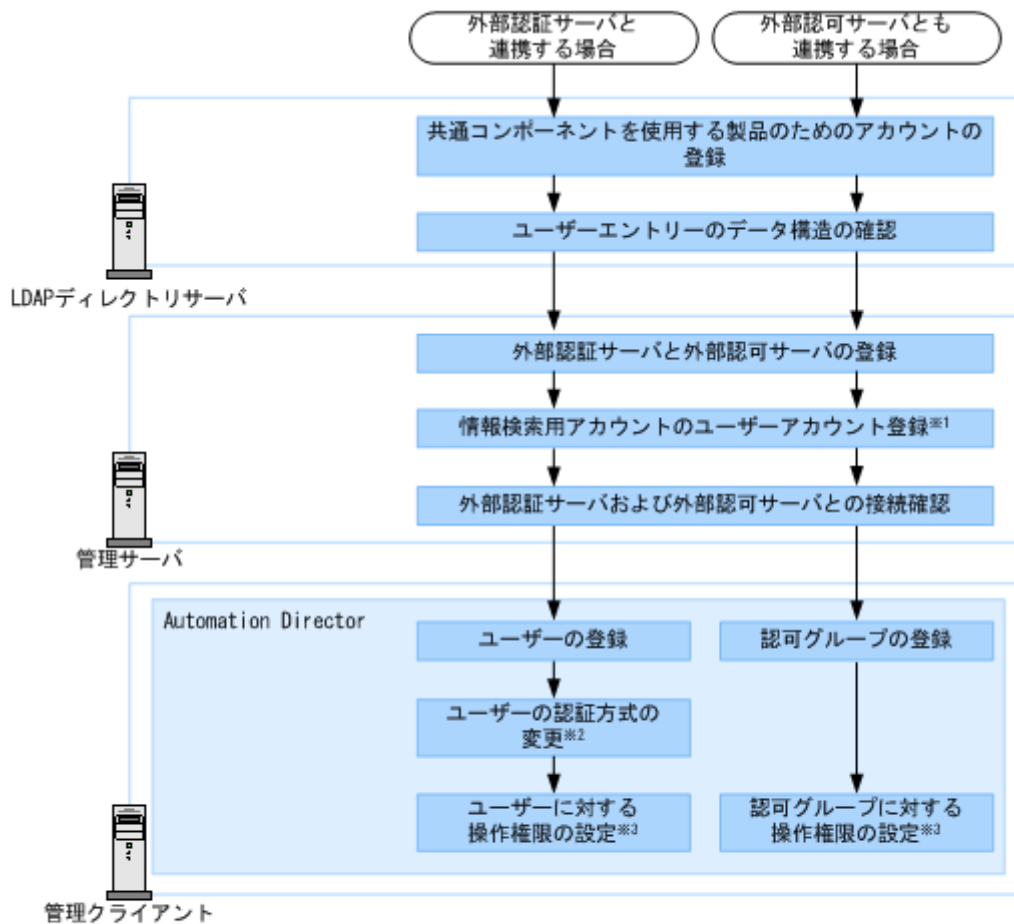
外部認可サーバとも連携する場合、共通コンポーネントを使用する製品では、ユーザーを外部認可サーバのグループ（認可グループ）ごとに管理するため、各製品での個々のユーザーのアカウント管理や権限設定が不要になります。

共通コンポーネントを使用する製品は、LDAP ディレクトリサーバ（Active Directory）との連携をサポートしています。

## 4.3 LDAP ディレクトリサーバでユーザー認証するための操作フロー

LDAP ディレクトリサーバでユーザー認証するためには、管理サーバへの外部認証サーバの登録や認証対象のアカウントの登録などが必要です。





注※1 外部認証サーバとだけ連携する場合、ユーザーエントリーのデータ構造がフラットモデルのときは、不要な操作です。

注※2 既存のユーザーの認証方式を変更する場合に必要な操作です。

注※3 ユーザーの作業範囲に応じて操作権限を設定します。

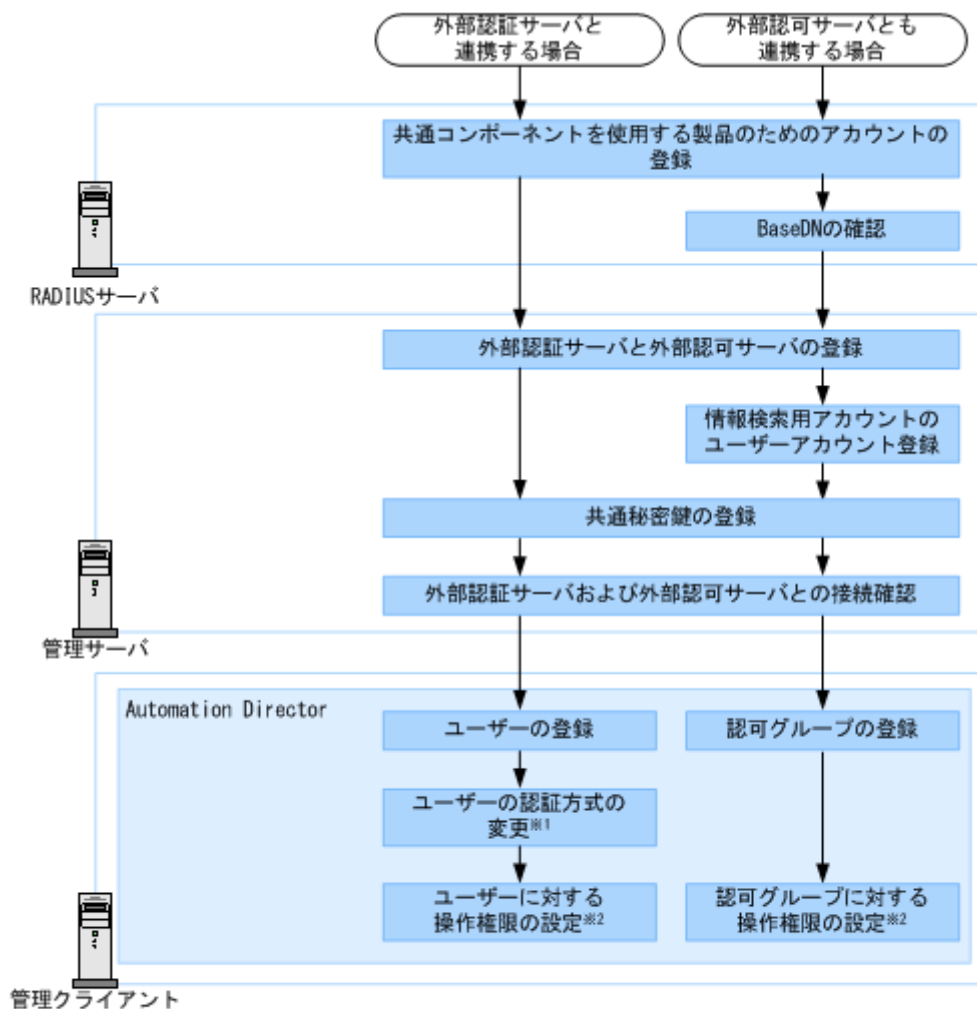
- ユーザー管理 (User Management)
- 共通コンポーネントを使用する製品



メモ LDAPディレクトリサーバと管理サーバとの通信に StartTLS を使用する場合は、セキュリティ通信のための環境設定が別途必要です。

## 4.4 RADIUS サーバでユーザー認証するための操作フロー

RADIUS サーバでユーザー認証するためには、管理サーバへの外部認証サーバの登録や認証対象のアカウントの登録などが必要です。



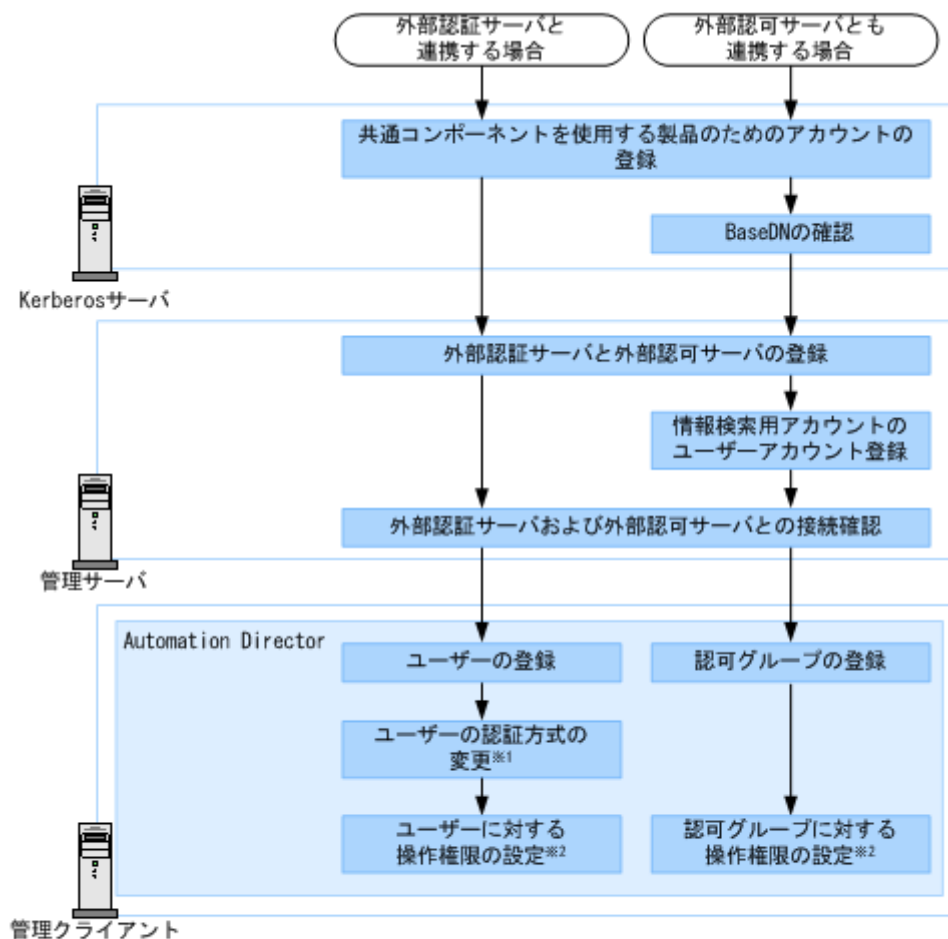
注※1 既存のユーザーの認証方式を変更する場合に必要な操作です。

注※2 ユーザーの作業範囲に応じて操作権限を設定します。

- ユーザー管理 (User Management)
- 共通コンポーネントを使用する製品

## 4.5 Kerberos サーバでユーザー認証するための操作フロー

Kerberos サーバでユーザー認証するためには、管理サーバへの外部認証サーバへの登録や認証対象のアカウントの登録などが必要です。



注※1 既存のユーザーの認証方式を変更する場合に必要な操作です。

注※2 ユーザーの作業範囲に応じて操作権限を設定します。

- ユーザー管理 (User Management)
- 共通コンポーネントを使用する製品

## 4.6 ユーザーエントリーのデータ構造とは

LDAP ディレクトリサーバのユーザーエントリーのデータ構造には階層構造モデルとフラットモデルがあります。

LDAP ディレクトリサーバでユーザー認証を行う場合、管理サーバに登録する LDAP ディレクトリサーバの情報や管理サーバで必要な作業がデータ構造によって異なるため、ユーザーエントリーがどちらに該当しているかを確認してください。

また、LDAP ディレクトリサーバでユーザー認証・認可する場合には、ユーザーを検索する起点となるエントリー (BaseDN) についても確認してください。

### 4.6.1 BaseDN とは

認証および認可の際にユーザーを検索する起点となるエントリーを BaseDN といいます。

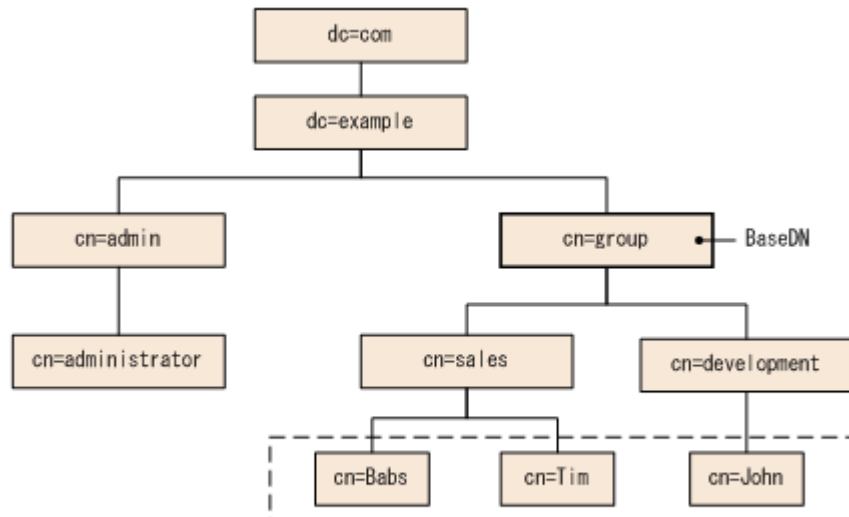
BaseDN より下の階層のユーザーエントリーが認証・認可の対象となります。共通コンポーネントを使用する製品で認証・認可したいユーザーをすべて含むエントリーであることが必要です。BaseDN は、管理サーバに LDAP ディレクトリサーバの情報を登録する際に必要になります。

## 4.6.2 階層構造モデルとは

BaseDN より下の階層が分岐していて、かつ別の階層下にユーザーエントリが登録されているデータ構造の場合は階層構造モデルになります。

階層構造モデルの場合は、BaseDN より下のエントリを対象に、ログイン ID とユーザー属性値が等しいエントリが検索されます。次の図に階層構造モデルの例を示します。

図 1 階層構造モデルの例



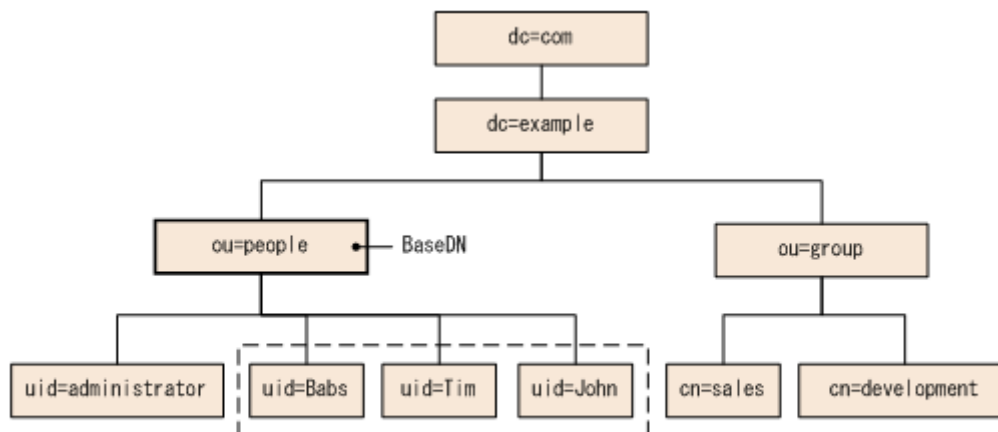
(凡例) [-----]: 認証対象のユーザーエントリ

## 4.6.3 フラットモデルとは

BaseDN より下に分岐がなく、かつ直下にユーザーエントリが登録されているデータ構造の場合はフラットモデルになります。

フラットモデルの場合は、BaseDN より下のエントリを対象に、ログイン ID と BaseDN を組み合わせた DN を持つエントリが認証されます。次の図にフラットモデルの例を示します。

図 2 フラットモデルの例



(凡例) [-----]: 認証対象のユーザーエントリ

## 4.7 複数の外部認証サーバと連携している場合の構成

複数の外部認証サーバと連携している場合、冗長構成またはマルチドメイン構成でユーザー認証します。

それぞれの外部認証サーバで同一のユーザー情報を管理する構成を、冗長構成と呼びます。ある外部認証サーバに障害が発生しても、ほかの外部認証サーバでユーザー認証できます。

外部認証サーバごとに異なるユーザー情報を管理する構成を、マルチドメイン構成と呼びます。ドメイン名を含んでいるユーザー ID でログインすると、入力したドメインの外部認証サーバでユーザー認証されます。外部認証サーバが Kerberos サーバの場合は、レルムごとに異なるユーザー情報を管理することで、マルチドメイン構成と同様の構成にできます。

冗長構成およびマルチドメイン構成に対応している外部認証サーバは次のとおりです。

**表 6 冗長構成およびマルチドメイン構成のサポート状況**

外部認証サーバ	冗長構成	マルチドメイン構成
LDAP ディレクトリサーバ	Y※1	Y※1
RADIUS サーバ	Y	N
Kerberos サーバ	Y	Y※2

(凡例)

Y : サポートしている

N : サポートしていない

注※1

冗長構成またはマルチドメイン構成のどちらか一方の構成にできます。

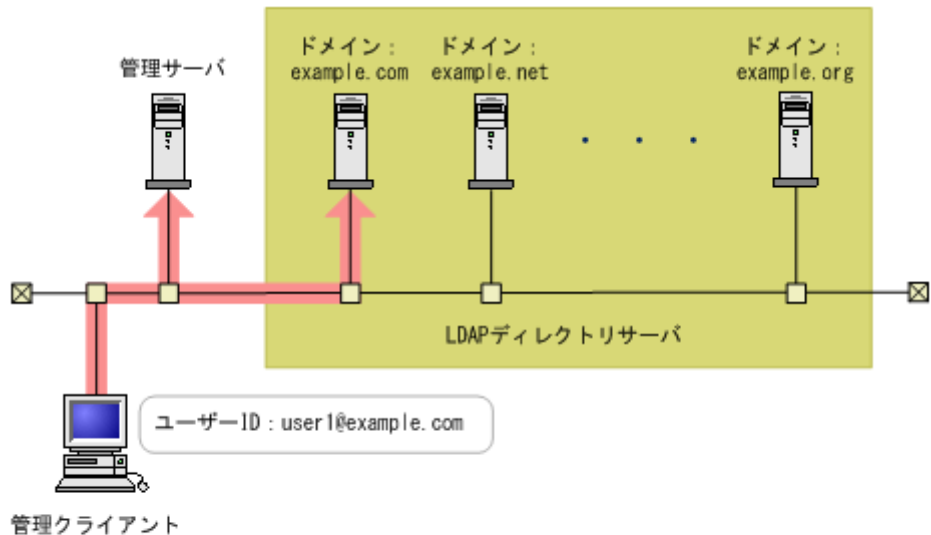
注※2


レルムごとに異なるユーザー情報を管理することで、マルチドメイン構成と同様の構成にできます。

マルチドメイン構成の LDAP ディレクトリサーバでユーザー認証する場合、ログイン時に入力したユーザー ID にドメイン名を含んでいるかどうかで、ユーザー認証の処理が異なります。

ドメイン名を含んでいるユーザー ID でログインすると、次の図に示すように、入力したドメインの LDAP ディレクトリサーバでユーザー認証されます。

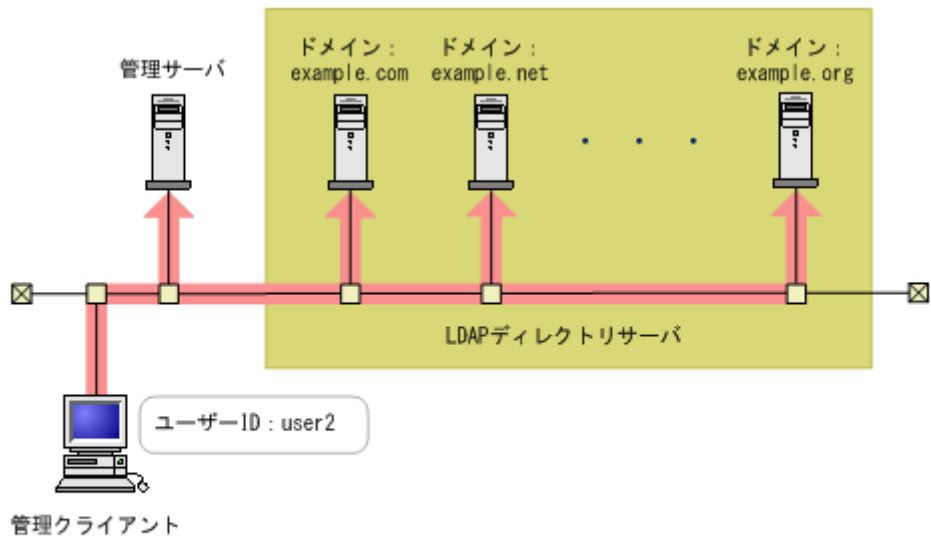
図 3 マルチドメイン構成のユーザー認証処理（ドメイン名を含んでいるユーザー ID の場合）




(凡例)  
 : ユーザー認証の処理

ドメイン名を含んでいないユーザー ID でログインすると、次の図に示すように、連携しているすべての LDAP ディレクトリサーバへ順にユーザー認証ができるまで認証処理が実行されます。このとき、多数の LDAP ディレクトリサーバと連携していると、ユーザー認証に時間が掛かるため、ドメイン名を含んでいるユーザー ID でログインする必要があります。

図 4 マルチドメイン構成のユーザー認証処理（ドメイン名を含んでいないユーザー ID の場合）



(凡例)  
 : ユーザー認証の処理

## 4.8 外部認証サーバと外部認可サーバの登録

exauth.properties ファイルに、使用する外部認証サーバの種類やサーバ識別名、外部認証サーバと外部認可サーバのマシン情報などを設定します。

### 前提条件

- Administrator 権限 (Windows の場合) または root (Linux の場合) でのログイン
- exauth.properties ファイルのひな形のコピー

Windows の場合 :

```
<共通コンポーネントのインストールフォルダ>%sample%conf%exauth.properties
```

Linux の場合 :

```
<共通コンポーネントのインストールディレクトリ>/sample/conf/
exauth.properties
```

- ユーザーエントリーのデータ構造の確認 (認証方式が LDAP の場合)
- LDAP ディレクトリサーバの OS での DNS サーバの環境設定※
- DNS サーバの SRV レコードへの LDAP ディレクトリサーバ情報の登録※
- 次の情報の確認
  - 共通
    - 外部認証サーバの種類
  - 認証方式が LDAP の場合
    - 外部認証サーバおよび外部認可サーバのマシン情報 (ホスト名または IP アドレス、ポート番号)
    - BaseDN
    - LDAP ディレクトリサーバが管理する外部認可サーバ用のドメイン名 (外部認可サーバと連携する場合)
    - LDAP ディレクトリサーバが管理するマルチドメイン構成用のドメイン名 (マルチドメイン構成の場合)
  - 認証方式が RADIUS の場合
    - 外部認証サーバおよび外部認可サーバのマシン情報 (ホスト名または IP アドレス、ポート番号)
    - 認証プロトコル
    - 管理サーバのホスト名または IP アドレス
    - LDAP ディレクトリサーバが管理するドメイン名 (外部認可サーバと連携する場合)
    - BaseDN (外部認可サーバと連携する場合)
  - 認証方式が Kerberos の場合
    - 外部認証サーバおよび外部認可サーバのマシン情報 (ホスト名または IP アドレス、ポート番号)
    - レルム名
    - LDAP ディレクトリサーバが管理するドメイン名 (外部認可サーバと連携する場合)
    - BaseDN (外部認可サーバと連携する場合)

注※ LDAP ディレクトリサーバの情報を DNS サーバに照会する場合に必要な作業です。

## 操作手順

1. コピーした `exauth.properties` ファイルに必要な事項を指定します。
2. `exauth.properties` ファイルを次の場所に格納します。

Windows の場合：

<共通コンポーネントのインストールフォルダ>%conf%\exauth.properties

Linux の場合：

<共通コンポーネントのインストールディレクトリ>/conf/exauth.properties

3. `auth.ocsp.enable` プロパティと `auth.ocsp.responderURL` プロパティの設定値を変更した場合には、共通コンポーネントを使用する製品のサービスを再起動します。  
それ以外のプロパティまたは属性の設定値を変更した場合は、直ちに変更後の値が有効になります。

### 4.8.1 LDAP ディレクトリサーバで認証する場合の `exauth.properties` ファイルの設定項目

`exauth.properties` ファイルには、使用する外部認証サーバの種類やサーバ識別名、外部認証サーバのマシン情報などを設定します。

- 共通のプロパティ  
「[表 7 LDAP ディレクトリサーバで認証する場合の `exauth.properties` ファイルの設定項目 \(共通項目\)](#)」を参照してください。
- 外部認証サーバと外部認可サーバのプロパティ  
接続先の LDAP ディレクトリサーバの情報を `exauth.properties` ファイルに直接指定する場合と、DNS サーバに照会する場合とで設定する項目が異なります。
  - LDAP ディレクトリサーバの情報を直接指定する場合  
「[表 8 LDAP ディレクトリサーバで認証する場合の `exauth.properties` ファイルの設定項目 \(外部認証サーバの情報を直接指定するとき\)](#)」または「[表 9 LDAP ディレクトリサーバで認証する場合の `exauth.properties` ファイルの設定項目 \(外部認証サーバと StartTLS で通信するとき\)](#)」を参照してください。
  - LDAP ディレクトリサーバの情報を DNS サーバに照会する場合  
「[表 10 LDAP ディレクトリサーバで認証する場合の `exauth.properties` ファイルの設定項目 \(外部認証サーバの情報を DNS サーバに照会するとき\)](#)」を参照してください。



#### メモ

- プロパティの設定値は、大文字と小文字を区別してください。
- 管理サーバと LDAP ディレクトリサーバとの間の通信に StartTLS を使用する場合は、`exauth.properties` ファイルに接続先の LDAP ディレクトリサーバの情報を直接指定する必要があります。
- DNS サーバに接続先の LDAP ディレクトリサーバを照会する場合は、ユーザーがログインする際に処理に時間が掛かることがあります。
- 接続先の LDAP ディレクトリサーバがマルチドメイン構成の場合、DNS サーバに LDAP ディレクトリサーバを照会できません。



表 7 LDAP ディレクトリサーバで認証する場合の exauth.properties ファイルの設定項目（共通項目）

プロパティ名	説明
auth.server.type	外部認証サーバの種類です。ldap を指定します。 デフォルト値：internal（外部認証サーバと連携しない場合）
auth.server.name	LDAP ディレクトリサーバのサーバ識別名を指定します。接続プロトコルやポート番号などの設定（「 <a href="#">表 8 LDAP ディレクトリサーバで認証する場合の exauth.properties ファイルの設定項目（外部認証サーバの情報を直接指定するとき）</a> 」および「 <a href="#">表 10 LDAP ディレクトリサーバで認証する場合の exauth.properties ファイルの設定項目（外部認証サーバの情報を DNS サーバに照会するとき）</a> 」）を LDAP ディレクトリサーバごとに区別するために付ける任意の名称です。初期値として「ServerName」が設定されています。必ず 1 つ以上のサーバ識別名を指定してください。サーバ識別名を複数指定する場合は、サーバ識別名をコンマ（,）で区切って指定します。同じサーバ識別名は重複して登録しないでください。 指定できる値：64 バイト以内の次の文字列 A～Z a～z 0～9 ! # ( ) + - . = @ [ ] ^ _ { } ~ デフォルト値：なし
auth.ldap.multi_domain	LDAP ディレクトリサーバのサーバ識別名を複数指定する場合、各サーバがマルチドメイン構成であるか、冗長構成であるかを指定します。 マルチドメイン構成の場合は true を指定します。 冗長構成の場合は false を指定します。 デフォルト値：false
auth.group.mapping	外部認可サーバとも連携するかどうかを指定します。 連携する場合は true を指定します。 連携しない場合は false を指定します。 デフォルト値：false

表 8 LDAP ディレクトリサーバで認証する場合の exauth.properties ファイルの設定項目（外部認証サーバの情報を直接指定するとき）

属性	説明
protocol	LDAP ディレクトリサーバ接続のプロトコルです。 この項目は必須です。 平文による通信の場合は ldap、StartTLS による通信の場合は tls を指定します。 tls を指定する場合には、LDAP ディレクトリサーバで次のどれかの暗号方式を使用できることを事前に確認してください。 <ul style="list-style-type: none"> <li>• TLS_RSA_WITH_AES_256_GCM_SHA384</li> <li>• TLS_RSA_WITH_AES_256_CBC_SHA256</li> <li>• TLS_RSA_WITH_AES_256_CBC_SHA</li> <li>• TLS_RSA_WITH_AES_128_CBC_SHA256</li> <li>• TLS_RSA_WITH_AES_128_CBC_SHA</li> <li>• SSL_RSA_WITH_3DES_EDE_CBC_SHA</li> </ul> 指定できる値：ldap または tls デフォルト値：なし

属性	説明
	LDAP ディレクトリサーバの接続プロトコルに <b>StartTLS</b> を使用する場合には、共通コンポーネントのセキュリティ設定が必要です。
host	LDAP ディレクトリサーバのホスト名または IP アドレスを指定します。ホスト名を指定する場合、IP アドレスへの名前解決ができることを事前に確認してください。IP アドレスには、IPv4 アドレスと IPv6 アドレスの両方を使用できます。IPv6 アドレスは必ず角括弧 ( [ ] ) で囲んでください。 この項目は必須です。 デフォルト値：なし LDAP ディレクトリサーバの接続プロトコルに <b>StartTLS</b> を使用する場合は、host 属性には LDAP ディレクトリサーバの証明書の CN と同じホスト名を設定してください。IP アドレスは使用できません。
port	LDAP ディレクトリサーバのポート番号です。指定するポートが、LDAP ディレクトリサーバで待ち受けポート番号として設定されていることを確認してください。 指定できる値：1～65535 デフォルト値：389
timeout	LDAP ディレクトリサーバと接続するときの接続待ち時間です。この値を 0 にした場合、タイムアウトしないで、通信エラーが発生するまで待ち続けます。 指定できる値：0～120 (秒) デフォルト値：15
attr	認証で使用するユーザー ID の値が定義されている属性名 (Attribute Type) です。  <ul style="list-style-type: none"> <li>• 階層構造モデルの場合 ユーザーを一意に特定できる値が格納されている属性名を指定します。この属性に格納された値を、共通コンポーネントを使用する製品のユーザー ID として使用します。 共通コンポーネントを使用する製品のユーザー ID として使用できない文字列が値に含まれていない属性を指定してください。 例えば、Active Directory を使用している場合で、Windows のログイン ID をユーザー ID として使用したいときは、Windows のログイン ID が値として定義されている属性名の sAMAccountName を指定します。</li> <li>• フラットモデルの場合 ユーザーエントリーの RDN の属性名を指定します。 例えば、ユーザーの DN が uid=John,ou=People,dc=example,dc=com の場合、uid=John の属性名である uid を指定します。</li> </ul> 初期値として sAMAccountName が設定されています。この項目は必須です。 デフォルト値：なし
basedn	LDAP ディレクトリサーバの情報を検索する際に、起点となるエントリーの DN (BaseDN) です。この DN より下の階層のユーザーエントリーが認証の対象となります。指定した値は LDAP ディレクトリサーバにそのまま渡されるため、BaseDN にエスケープが必要な文字が含まれる場合は、正しくエスケープしてください。  <ul style="list-style-type: none"> <li>• 階層構造モデルの場合 検索対象のユーザーエントリーをすべて含む階層の DN です。</li> <li>• フラットモデルの場合 検索対象のユーザーエントリーより 1 つ上の階層の DN です。</li> </ul> この項目は必須です。DN は RFC4514 の規約に従って指定してください。例えば、次の文字が DN に含まれる場合は、1 文字ごとに円記号 ( ¥ ) でエスケープする必要があります。 空白文字 # + ; , < = > ¥ デフォルト値：なし

属性	説明
retry.interval	LDAP ディレクトリサーバとの通信に失敗した場合のリトライ間隔となる秒数です。 指定できる値：1～60（秒） デフォルト値：1
retry.times	LDAP ディレクトリサーバとの通信に失敗した場合のリトライ回数です。この値を0にした場合、リトライされません。 指定できる値：0～50 デフォルト値：20
domain.name	LDAP ディレクトリサーバが管理する外部認可サーバ用のドメインの名称です。外部認可サーバとも連携する場合、この項目は必須です。 デフォルト値：なし
domain	LDAP ディレクトリサーバが管理するマルチドメイン構成用のドメインの名称です。 ログイン時に、この属性で指定したドメイン名をユーザー ID に含めると、指定したドメインに属する LDAP ディレクトリサーバが認証先となります。 LDAP ディレクトリサーバのサーバ識別名ごとにドメイン名を指定する際に、ドメイン名を重複しないように指定してください。大文字小文字は区別されません。 マルチドメイン構成の場合、この項目は必須です。 デフォルト値：なし
dns_lookup	false を指定します。 デフォルト値：false
注：各属性は、次のように指定します。	
auth.ldap.< auth.server.name に指定した値>.<属性>=<値>	

表 9 LDAP ディレクトリサーバで認証する場合の exauth.properties ファイルの設定項目（外部認証サーバと StartTLS で通信するとき）

プロパティ名	説明
auth.ocsp.enable	LDAP ディレクトリサーバと StartTLS で通信する場合に、OCSP レスポンダーを使用して LDAP ディレクトリサーバの電子署名証明書の有効性を検証するかどうかを指定します。 検証する場合は true を、検証しない場合は false を指定します。 デフォルト値：false
auth.ocsp.responderURL	電子署名証明書の AIA フィールドに記載された OCSP レスポンダー以外の OCSP レスポンダーで電子署名証明書の有効性を検証する場合に、OCSP レスポンダーの URL を指定します。省略した場合は、AIA フィールドに記載された OCSP レスポンダーに問い合わせます。 デフォルト値：なし

表 10 LDAP ディレクトリサーバで認証する場合の exauth.properties ファイルの設定項目（外部認証サーバの情報を DNS サーバに照会するとき）

属性	説明
protocol	LDAP ディレクトリサーバ接続のプロトコルです。 この項目は必須です。 指定できる値：ldap デフォルト値：なし

属性	説明
port	LDAP ディレクトリサーバのポート番号です。指定するポートが、LDAP ディレクトリサーバで待ち受けポート番号として設定されていることを確認してください。 指定できる値：1～65535 デフォルト値：389
timeout	LDAP ディレクトリサーバと接続するときの接続待ち時間です。この値を 0 にした場合、タイムアウトしないで、通信エラーが発生するまで待ち続けます。 指定できる値：0～120 (秒) デフォルト値：15
attr	認証で使用するユーザー ID の値が定義されている属性名 (Attribute Type) です。  <ul style="list-style-type: none"> <li>階層構造モデルの場合 ユーザーを一意に特定できる値が格納されている属性名を指定します。この属性に格納された値を、共通コンポーネントを使用する製品のユーザー ID として使用します。 共通コンポーネントを使用する製品のユーザー ID として使用できない文字列が値に含まれていない属性を指定してください。 例えば、Active Directory を使用している場合で、Windows のログイン ID をユーザー ID として使用したいときは、Windows のログイン ID が値として定義されている属性名の sAMAccountName を指定します。</li> <li>フラットモデルの場合 ユーザーエントリーの RDN の属性名を指定します。 例えば、ユーザーの DN が uid=John,ou=People,dc=example,dc=com の場合、uid=John の属性名である uid を指定します。</li> </ul> 初期値として sAMAccountName が設定されています。この項目は必須です。 デフォルト値：なし
basedn	LDAP ディレクトリサーバの情報を検索する際に、起点となるエントリーの DN (BaseDN) です。この DN より下の階層のユーザーエントリーが認証の対象となります。指定した値は LDAP ディレクトリサーバにそのまま渡されるため、BaseDN にエスケープが必要な文字が含まれる場合は、正しくエスケープしてください。  <ul style="list-style-type: none"> <li>階層構造モデルの場合 検索対象のユーザーエントリーをすべて含む階層の DN です。</li> <li>フラットモデルの場合 検索対象のユーザーエントリーより 1 つ上の階層の DN です。</li> </ul> この項目は必須です。DN は RFC4514 の規約に従って指定してください。例えば、次の文字が DN に含まれる場合は、1 文字ごとに円記号 (¥) でエスケープする必要があります。 空白文字 # + ; , < = > ¥ デフォルト値：なし
retry.interval	LDAP ディレクトリサーバとの通信を削除した場合のリトライ間隔となる秒数です。 指定できる値：1～60 (秒) デフォルト値：1
retry.times	LDAP ディレクトリサーバとの通信を削除した場合のリトライ回数です。この値を 0 にした場合、リトライされません。 指定できる値：0～50 デフォルト値：20
domain.name	LDAP ディレクトリサーバが管理する外部認可サーバ用のドメインの名称です。この項目は必須です。

属性	説明
	デフォルト値：なし
dns_lookup	<p>true を指定します。</p> <p>ただし、次の属性に値が設定されている場合は、DNS サーバには照会されず、ユーザーが指定した値を使用して LDAP ディレクトリサーバに接続されます。</p> <ul style="list-style-type: none"> <li>auth.ldap.&lt; auth.server.name に指定した値 &gt;.host</li> <li>auth.ldap.&lt; auth.server.name に指定した値 &gt;.port</li> </ul> <p>デフォルト値：false</p>
注：各属性は、次のように指定します。	
auth.ldap.< auth.server.name に指定した値 >.<属性>=<値>	

## 4.8.2 LDAP ディレクトリサーバで認証する場合の exauth.properties ファイルの設定例

LDAP ディレクトリサーバで認証する場合の exauth.properties ファイルの設定例を次に示します。

- LDAP ディレクトリサーバの情報を直接指定する場合（外部認証サーバとだけ連携するとき）

```
auth.server.type=ldap
auth.server.name=ServerName
auth.group.mapping=false
auth.ocsp.enable=false
auth.ocsp.responderURL=
auth.ldap.ServerName.protocol=ldap
auth.ldap.ServerName.host=ldap.example.com
auth.ldap.ServerName.port=389
auth.ldap.ServerName.timeout=15
auth.ldap.ServerName.attr=sAMAccountName
auth.ldap.ServerName.basedn=dc=Example,dc=com
auth.ldap.ServerName.retry.interval=1
auth.ldap.ServerName.retry.times=20
auth.ldap.ServerName.dns_lookup=false
```

- LDAP ディレクトリサーバを DNS サーバに照会する場合（外部認証サーバとだけ連携するとき）

```
auth.server.type=ldap
auth.server.name=ServerName
auth.group.mapping=false
auth.ldap.ServerName.protocol=ldap
auth.ldap.ServerName.timeout=15
auth.ldap.ServerName.attr=sAMAccountName
auth.ldap.ServerName.basedn=dc=Example,dc=com
auth.ldap.ServerName.retry.interval=1
auth.ldap.ServerName.retry.times=20
auth.ldap.ServerName.domain.name=EXAMPLE.COM
auth.ldap.ServerName.dns_lookup=true
```

- LDAP ディレクトリサーバの情報を直接指定する場合（外部認可サーバとも連携するとき）

```
auth.server.type=ldap
auth.server.name=ServerName
auth.group.mapping=true
auth.ocsp.enable=false
auth.ocsp.responderURL=
auth.ldap.ServerName.protocol=ldap
auth.ldap.ServerName.host=ldap.example.com
auth.ldap.ServerName.port=389
auth.ldap.ServerName.timeout=15
```

```
auth.ldap.ServerName.attr=sAMAccountName
auth.ldap.ServerName.basedn=dc=Example,dc=com
auth.ldap.ServerName.retry.interval=1
auth.ldap.ServerName.retry.times=20
auth.ldap.ServerName.domain.name=EXAMPLE.COM
auth.ldap.ServerName.dns_lookup=false
```

- LDAP ディレクトリサーバを DNS サーバに照会する場合（外部認可サーバとも連携するとき）

```
auth.server.type=ldap
auth.server.name=ServerName
auth.group.mapping=true
auth.ldap.ServerName.protocol=ldap
auth.ldap.ServerName.timeout=15
auth.ldap.ServerName.attr=sAMAccountName
auth.ldap.ServerName.basedn=dc=Example,dc=com
auth.ldap.ServerName.retry.interval=1
auth.ldap.ServerName.retry.times=20
auth.ldap.ServerName.domain.name=EXAMPLE.COM
auth.ldap.ServerName.dns_lookup=true
```

- 冗長構成の場合

```
auth.server.type=ldap
auth.server.name=ServerName1,ServerName2
auth.ldap.multi_domain=false
auth.group.mapping=false
auth.ldap.ServerName1.protocol=ldap
auth.ldap.ServerName1.host=ldap1.example.com
auth.ldap.ServerName1.port=389
auth.ldap.ServerName1.timeout=15
auth.ldap.ServerName1.attr=sAMAccountName
auth.ldap.ServerName1.basedn=dc=Example,dc=com
auth.ldap.ServerName1.retry.interval=1
auth.ldap.ServerName1.retry.times=20
auth.ldap.ServerName2.protocol=ldap
auth.ldap.ServerName2.host=ldap2.example.com
auth.ldap.ServerName2.port=389
auth.ldap.ServerName2.timeout=15
auth.ldap.ServerName2.attr=sAMAccountName
auth.ldap.ServerName2.basedn=dc=Example,dc=net
auth.ldap.ServerName2.retry.interval=1
auth.ldap.ServerName2.retry.times=20
```

- マルチドメイン構成の場合

```
auth.server.type=ldap
auth.server.name=ServerName1,ServerName2
auth.ldap.multi_domain=true
auth.group.mapping=false
auth.ldap.ServerName1.protocol=ldap
auth.ldap.ServerName1.host=ldap1.example.com
auth.ldap.ServerName1.port=389
auth.ldap.ServerName1.timeout=15
auth.ldap.ServerName1.attr=sAMAccountName
auth.ldap.ServerName1.basedn=dc=Example,dc=com
auth.ldap.ServerName1.retry.interval=1
auth.ldap.ServerName1.retry.times=20
auth.ldap.ServerName1.domain=example.com
auth.ldap.ServerName2.protocol=ldap
auth.ldap.ServerName2.host=ldap2.example.com
auth.ldap.ServerName2.port=389
auth.ldap.ServerName2.timeout=15
auth.ldap.ServerName2.attr=sAMAccountName
auth.ldap.ServerName2.basedn=dc=Example,dc=net
auth.ldap.ServerName2.retry.interval=1
auth.ldap.ServerName2.retry.times=20
auth.ldap.ServerName2.domain=example.net
```

## 4.8.3 RADIUS サーバで認証する場合の exauth.properties ファイルの設定項目

exauth.properties ファイルには、使用する外部認証サーバの種類やサーバ識別名、外部認証サーバのマシン情報などを設定します。

- 共通のプロパティ  
「[表 11 RADIUS サーバで認証する場合の exauth.properties ファイルの設定項目 \(共通項目\)](#)」を参照してください。
- 外部認証サーバのプロパティ  
RADIUS サーバごとに設定します。  
「[表 12 RADIUS サーバで認証する場合の exauth.properties ファイルの設定項目 \(外部認証サーバの設定\)](#)」を参照してください。
- 外部認可サーバのプロパティ  
外部認可サーバとも連携する場合に必要な設定です。LDAP ディレクトリサーバの情報をドメインごとに設定します。  
接続先の LDAP ディレクトリサーバの情報を直接指定する場合と、DNS サーバに照会する場合とで exauth.properties ファイルに設定する項目が異なります。
  - LDAP ディレクトリサーバの情報を直接指定する場合  
「[表 13 RADIUS サーバで認証する場合の exauth.properties ファイルの設定項目 \(外部認可サーバの共通設定\)](#)」、「[表 14 RADIUS サーバで認証する場合の exauth.properties ファイルの設定項目 \(外部認可サーバの情報を直接指定するとき\)](#)」および「[表 15 RADIUS サーバで認証する場合の exauth.properties ファイルの設定項目 \(外部認可サーバと StartTLS で通信するとき\)](#)」を参照してください。
  - LDAP ディレクトリサーバの情報を DNS サーバに照会する場合  
「[表 13 RADIUS サーバで認証する場合の exauth.properties ファイルの設定項目 \(外部認可サーバの共通設定\)](#)」および「[表 16 RADIUS サーバで認証する場合の exauth.properties ファイルの設定項目 \(外部認可サーバの情報を DNS サーバに照会するとき\)](#)」を参照してください。



### メモ

- プロパティの設定値は、大文字と小文字を区別してください。
- 管理サーバと LDAP ディレクトリサーバとの間の通信に StartTLS を使用する場合は、exauth.properties ファイルに接続先の LDAP ディレクトリサーバの情報を直接指定する必要があります。
- DNS サーバに接続先の LDAP ディレクトリサーバを照会する場合は、ユーザーがログインする際に処理に時間が掛かることがあります。

表 11 RADIUS サーバで認証する場合の exauth.properties ファイルの設定項目 (共通項目)

プロパティ名	説明
auth.server.type	外部認証サーバの種類です。radius を指定します。 デフォルト値: internal (外部認証サーバと連携しない場合)
auth.server.name	RADIUS サーバのサーバ識別名を指定します。接続プロトコルやポート番号などの設定 ( <a href="#">表 12 RADIUS サーバで認証する場合の exauth.properties ファイルの設定項目 (外部認証サーバの設定)</a> ) を RADIUS サーバごとに区別するために付ける任意の名称です。初期値として「ServerName」が設定さ

プロパティ名	説明
	<p>れています。必ず1つ以上のサーバ識別名を指定してください。RADIUSサーバを冗長構成にする場合は、各サーバのサーバ識別名をコンマ(,)で区切って指定します。サーバ識別名は重複して登録しないでください。</p> <p>指定できる値: 64バイト以内の次の文字列</p> <p>A~Z</p> <p>a~z</p> <p>0~9</p> <p>! # ( ) + - . = @ [ ] ^ _ { } ~</p> <p>デフォルト値: なし</p>
auth.group.mapping	<p>外部認可サーバとも連携するかどうかを指定します。</p> <p>連携する場合は true を指定します。</p> <p>連携しない場合は false を指定します。</p> <p>デフォルト値: false</p>

表 12 RADIUS サーバで認証する場合の exauth.properties ファイルの設定項目 (外部認証サーバの設定)

属性	説明
protocol	<p>RADIUS サーバ認証に使用する認証プロトコルです。この項目は必須です。</p> <p>指定できる値: PAP または CHAP</p> <p>デフォルト値: なし</p>
host <sup>1</sup>	<p>RADIUS サーバのホスト名または IP アドレスを指定します。ホスト名を指定する場合、IP アドレスへの名前解決ができることを事前に確認してください。IP アドレスには、IPv4 アドレスと IPv6 アドレスの両方を使用できます。IPv6 アドレスは必ず角括弧 ([ ]) で囲ってください。この項目は必須です。</p> <p>デフォルト値: なし</p>
port	<p>RADIUS サーバの認証用ポート番号です。指定するポートが RADIUS サーバで待ち受けポート番号として設定されていることを事前に確認してください。</p> <p>指定できる値: 1~65535</p> <p>デフォルト値: 1812</p>
timeout	<p>RADIUS サーバと接続するときの接続待ち時間です。</p> <p>指定できる値: 1~65535 (秒)</p> <p>デフォルト値: 1</p>
retry.times	<p>RADIUS サーバとの通信を削除した場合のリトライ回数です。この値を 0 にした場合、リトライされません。</p> <p>指定できる値: 0~50</p> <p>デフォルト値: 3</p>
attr.NAS-Identifier <sup>2</sup>	<p>Device Manager の管理サーバのホスト名です。RADIUS サーバが管理サーバを識別するために使用します。初期値として、管理サーバのホスト名が設定されています。</p> <p>指定できる値: 253 バイト以内の次の文字列</p> <p>A~Z</p> <p>a~z</p> <p>0~9</p> <p>! " # \$ % &amp; ' ( ) * + , - . / : ; &lt; = &gt; ? @ [ ¥ ] ^ _ ` {   } ~</p> <p>デフォルト値: なし</p>



属性	説明
attr.NAS-IP-Address <sup>2</sup>	Automation Director の管理サーバの IPv4 アドレスです。RADIUS サーバが管理サーバを識別するために使用します。 IPv4 アドレスの形式が不正な場合、この属性は無効です。 デフォルト値：なし
attr.NAS-IPv6-Address <sup>2</sup>	Automation Director の管理サーバの IPv6 アドレスです。RADIUS サーバが管理サーバを識別するために使用します。IPv6 アドレスは必ず角括弧（[]）で囲んでください。 IPv6 アドレスの形式が不正な場合、この属性は無効です。 デフォルト値：なし
<p>1. 同一マシンで稼働する外部認可サーバとも連携し、かつ LDAP ディレクトリサーバの接続プロトコルに StartTLS を使用する場合は、host 属性には LDAP ディレクトリサーバの証明書の CN と同じホスト名を設定してください。IP アドレスは使用できません。</p> <p>2. attr.NAS-Identifier、attr.NAS-IP-Address、attr.NAS-IPv6-Address はどれか 1 つを必ず指定してください。</p> <p>注：各属性は、次のように指定します。 auth.radius.&lt;auth.server.name に指定した値&gt;.&lt;属性&gt;=&lt;値&gt;</p>	

表 13 RADIUS サーバで認証する場合の exauth.properties ファイルの設定項目（外部認可サーバの共通設定）

属性	説明
domain.name	LDAP ディレクトリサーバが管理するドメインの名称です。外部認可サーバとも連携する場合、この項目は必須です。 デフォルト値：なし
dns_lookup	LDAP ディレクトリサーバの情報を DNS サーバに照会するかどうかを指定します。 exauth.properties ファイルに LDAP ディレクトリサーバの情報を直接指定する場合は false を指定します。 DNS サーバに照会する場合は、true を指定します。 ただし、次の属性に値が設定されている場合は、DNS サーバには照会されず、ユーザーが指定した値を使用して LDAP ディレクトリサーバに接続されます。 <ul style="list-style-type: none"> <li>auth.group.&lt;ドメイン名&gt;.host</li> <li>auth.group.&lt;ドメイン名&gt;.port</li> </ul> デフォルト値：false
<p>注：各属性は、次のように指定します。 auth.radius.&lt;auth.server.name に指定した値&gt;.&lt;属性&gt;=&lt;値&gt;</p>	

表 14 RADIUS サーバで認証する場合の exauth.properties ファイルの設定項目（外部認可サーバの情報を直接指定するとき）

属性	説明
protocol <sup>1</sup>	LDAP ディレクトリサーバ接続のプロトコルです。 平文による通信の場合は ldap、StartTLS による通信の場合は tls を指定します。 tls を指定する場合には、LDAP ディレクトリサーバで次のどれかの暗号方式を使用できることを事前に確認してください。 <ul style="list-style-type: none"> <li>TLS_RSA_WITH_AES_256_GCM_SHA384</li> </ul>

属性	説明
	<ul style="list-style-type: none"> <li>• TLS_RSA_WITH_AES_256_CBC_SHA256</li> <li>• TLS_RSA_WITH_AES_256_CBC_SHA</li> <li>• TLS_RSA_WITH_AES_128_CBC_SHA256</li> <li>• TLS_RSA_WITH_AES_128_CBC_SHA</li> <li>• SSL_RSA_WITH_3DES_EDE_CBC_SHA</li> </ul> 指定できる値：ldap または tls デフォルト値：ldap
host <sup>2</sup>	外部認証サーバと外部認可サーバが異なるマシンで稼働している場合に、LDAP ディレクトリサーバのホスト名または IP アドレスを指定します。ホスト名を指定する場合、IP アドレスへの名前解決ができることを事前に確認してください。IP アドレスには、IPv4 アドレスと IPv6 アドレスの両方を使用できます。IPv6 アドレスは必ず角括弧 ([ ]) で囲んでください。 省略した場合は、外部認証サーバと外部認可サーバが同一マシンで稼働しているものと見なされます。 デフォルト値：なし
port	LDAP ディレクトリサーバのポート番号です。指定するポートが、LDAP ディレクトリサーバで待ち受けポート番号として設定されていることを事前に確認してください。 指定できる値：1～65535 デフォルト値：389
basedn	LDAP ディレクトリサーバの情報を検索する際に、起点となるエントリーの DN (BaseDN) です。 この DN より下の階層のユーザーエントリーが認可の対象となります。 DN は RFC4514 の規約に従って指定してください。例えば、次の文字が DN に含まれる場合は、1 文字ごとに円記号 (¥) でエスケープする必要があります。 空白文字 # + ; , < = > ¥ 指定した値は LDAP ディレクトリサーバにそのまま渡されるため、BaseDN にエスケープが必要な文字が含まれる場合は、正しくエスケープしてください。 省略した場合は、Active Directory の defaultNamingContext 属性に指定されている値が BaseDN と見なされます。 デフォルト値：なし
timeout	LDAP ディレクトリサーバと接続するときの接続待ち時間です。この値を 0 にした場合、タイムアウトしないで、通信エラーが発生するまで待ち続けます。 指定できる値：0～120 (秒) デフォルト値：15
retry.interval	LDAP ディレクトリサーバとの通信を削除した場合のリトライ間隔となる秒数です。 指定できる値：1～60 (秒) デフォルト値：1
retry.times	LDAP ディレクトリサーバとの通信を削除した場合のリトライ回数です。この値を 0 にした場合、リトライされません。 指定できる値：0～50 デフォルト値：20
<ol style="list-style-type: none"> <li>1. LDAP ディレクトリサーバの接続プロトコルに StartTLS を使用する場合には、共通コンポーネントのセキュリティ設定が必要です。</li> <li>2. 外部認証サーバと外部認可サーバが別のマシンで稼働していて、かつ LDAP ディレクトリサーバの接続プロトコルに StartTLS を使用する場合は、host 属性には LDAP ディレクトリサーバの証明書の CN と同じホスト名を設定してください。IP アドレスは使用できません。</li> </ol> 注：各属性は、次のように指定します。	

属性	説明
	auth.group.<ドメイン名>.<属性>=<値> <ドメイン名>には、auth.radius.<auth.server.name に指定した値>.domain.name の値を指定します。

表 15 RADIUS サーバで認証する場合の exauth.properties ファイルの設定項目（外部認可サーバと StartTLS で通信するとき）

プロパティ名	説明
auth.ocsp.enable	LDAP ディレクトリサーバと StartTLS で通信する場合に、OCSP レスポンダーを使用して LDAP ディレクトリサーバの電子署名証明書の有効性を検証するかどうかを指定します。 検証する場合は true を、検証しない場合は false を指定します。 デフォルト値：false
auth.ocsp.responderURL	電子署名証明書の AIA フィールドに記載された OCSP レスポンダー以外の OCSP レスポンダーで電子署名証明書の有効性を検証する場合に、OCSP レスポンダーの URL を指定します。省略した場合は、AIA フィールドに記載された OCSP レスポンダーに問い合わせます。 デフォルト値：なし

表 16 RADIUS サーバで認証する場合の exauth.properties ファイルの設定項目（外部認可サーバの情報を DNS サーバに照会するとき）

属性	説明
protocol	LDAP ディレクトリサーバ接続のプロトコルです。 指定できる値：ldap デフォルト値：ldap
port	LDAP ディレクトリサーバのポート番号です。指定するポートが、LDAP ディレクトリサーバで待ち受けポート番号として設定されていることを事前に確認してください。 指定できる値：1～65535 デフォルト値：389
basedn	LDAP ディレクトリサーバの情報を検索する際に、起点となるエントリーの DN (BaseDN) です。この DN より下の階層のユーザーエントリーが認可の対象となります。 検索対象のユーザーエントリーをすべて含む階層の DN を指定してください。 DN は RFC4514 の規約に従って指定してください。例えば、次の文字が DN に含まれる場合は、1 文字ごとに円記号 (¥) でエスケープする必要があります。 空白文字 # + ; , < = > ¥ 指定した値は LDAP ディレクトリサーバにそのまま渡されるため、BaseDN にエスケープが必要な文字が含まれる場合は、正しくエスケープしてください。 省略した場合は、Active Directory の defaultNamingContext 属性に指定されている値が BaseDN と見なされます。 デフォルト値：なし
timeout	LDAP ディレクトリサーバと接続するときの接続待ち時間です。この値を 0 にした場合、タイムアウトしないで、通信エラーが発生するまで待ち続けます。 指定できる値：0～120 (秒) デフォルト値：15
retry.interval	LDAP ディレクトリサーバとの通信を削除した場合のリトライ間隔となる秒数です。 指定できる値：1～60 (秒)

属性	説明
	デフォルト値：1
retry.times	LDAP ディレクトリサーバとの通信を削除した場合のリトライ回数です。この値を0にした場合、リトライされません。 指定できる値：0～50 デフォルト値：20
注：各属性は、次のように指定します。 auth.group.<ドメイン名>.<属性>=<値> <ドメイン名>には、auth.radius.<auth.server.name に指定した値>.domain.name の値を指定します。	

## 4.8.4 RADIUS サーバで認証する場合の exauth.properties ファイルの設定例

RADIUS サーバで認証する場合の exauth.properties ファイルの設定例を次に示します。

- 外部認証サーバとだけ連携する場合

```
auth.server.type=radius
auth.server.name=ServerName
auth.group.mapping=false
auth.radius.ServerName.protocol=PAP
auth.radius.ServerName.host=radius.example.com
auth.radius.ServerName.port=1812
auth.radius.ServerName.timeout=1
auth.radius.ServerName.retry.times=3
auth.radius.ServerName.attr.NAS-Identifier=host_A
```

- 外部認可サーバの情報を直接設定する場合

```
auth.server.type=radius
auth.server.name=ServerName
auth.group.mapping=true
auth.ocsp.enable=false
auth.ocsp.responderURL=
auth.radius.ServerName.protocol=PAP
auth.radius.ServerName.host=radius.example.com
auth.radius.ServerName.port=1812
auth.radius.ServerName.timeout=1
auth.radius.ServerName.retry.times=3
auth.radius.ServerName.attr.NAS-Identifier=host_A
auth.radius.ServerName.domain.name=EXAMPLE.COM
auth.radius.ServerName.dns_lookup=false
auth.group.EXAMPLE.COM.protocol=ldap
auth.group.EXAMPLE.COM.host=ldap.example.com
auth.group.EXAMPLE.COM.port=389
auth.group.EXAMPLE.COM.basedn=dc=Example,dc=com
auth.group.EXAMPLE.COM.timeout=15
auth.group.EXAMPLE.COM.retry.interval=1
auth.group.EXAMPLE.COM.retry.times=20
```

- 外部認可サーバを DNS サーバに照会する場合

```
auth.server.type=radius
auth.server.name=ServerName
auth.group.mapping=true
auth.radius.ServerName.protocol=PAP
auth.radius.ServerName.host=radius.example.com
auth.radius.ServerName.port=1812
auth.radius.ServerName.timeout=1
auth.radius.ServerName.retry.times=3
auth.radius.ServerName.attr.NAS-Identifier=host_A
auth.radius.ServerName.domain.name=EXAMPLE.COM
```

```
auth.radius.ServerName.dns_lookup=true
auth.group.EXAMPLE.COM.protocol=ldap
auth.group.EXAMPLE.COM.basedn=dc=Example,dc=com
auth.group.EXAMPLE.COM.timeout=15
auth.group.EXAMPLE.COM.retry.interval=1
auth.group.EXAMPLE.COM.retry.times=20
```

- 冗長構成の場合

```
auth.server.type=radius
auth.server.name=ServerName1,ServerName2
auth.group.mapping=false
auth.radius.ServerName1.protocol=PAP
auth.radius.ServerName1.host=radius1.example.com
auth.radius.ServerName1.port=1812
auth.radius.ServerName1.timeout=1
auth.radius.ServerName1.retry.times=3
auth.radius.ServerName1.attr.NAS-IP-Address=127.0.0.1
auth.radius.ServerName2.protocol=PAP
auth.radius.ServerName2.host=radius2.example.com
auth.radius.ServerName2.port=1812
auth.radius.ServerName2.timeout=1
auth.radius.ServerName2.retry.times=3
auth.radius.ServerName2.attr.NAS-IP-Address=127.0.0.1
```

## 4.8.5 Kerberos サーバで認証する場合の exauth.properties ファイルの設定項目

exauth.properties ファイルには、使用する外部認証サーバの種類やサーバ識別名、外部認証サーバのマシン情報などを設定します。

- 共通のプロパティ  
「[表 17 Kerberos サーバで認証する場合の exauth.properties ファイルの設定項目 \(共通項目\)](#)」を参照してください。
- 外部認証サーバのプロパティ  
Kerberos サーバごとに設定します。  
接続先の Kerberos サーバの情報を直接指定する場合と、DNS サーバに照会する場合とで exauth.properties ファイルに設定する項目が異なります。
  - Kerberos サーバの情報を直接指定する場合  
「[表 18 Kerberos サーバで認証する場合の exauth.properties ファイルの設定項目 \(外部認証サーバの情報を直接指定するとき\)](#)」を参照してください。
  - Kerberos サーバの情報を DNS サーバに照会する場合  
「[表 19 Kerberos サーバで認証する場合の exauth.properties ファイルの設定項目 \(外部認証サーバの情報を DNS サーバに照会するとき\)](#)」を参照してください。
- 外部認可サーバのプロパティ  
Kerberos サーバの情報を直接指定し、かつ外部認可サーバとも連携する場合にだけ必要な設定です。レルムごとに指定します。  
「[表 20 Kerberos サーバで認証する場合の exauth.properties ファイルの設定項目 \(外部認可サーバの設定\)](#)」または「[表 21 Kerberos サーバで認証する場合の exauth.properties ファイルの設定項目 \(外部認可サーバと StartTLS で通信するとき\)](#)」を参照してください。



### メモ

- プロパティの設定値は、大文字と小文字を区別してください。
- 管理サーバと LDAP ディレクトリサーバとの間の通信に StartTLS を使用する場合は、exauth.properties ファイルに接続先の LDAP ディレクトリサーバの情報を直接指定する必要があります。

- DNS サーバに接続先の LDAP ディレクトリサーバを照会する場合は、ユーザーがログインする際に処理に時間が掛かることがあります。

表 17 Kerberos サーバで認証する場合の exauth.properties ファイルの設定項目（共通項目）

プロパティ名	説明
auth.server.type	外部認証サーバの種類です。kerberos を指定します。 デフォルト値：internal（外部認証サーバと連携しない場合）
auth.group.mapping	外部認可サーバとも連携するかどうかを指定します。 連携する場合は true を指定します。 連携しない場合は false を指定します。 デフォルト値：false

表 18 Kerberos サーバで認証する場合の exauth.properties ファイルの設定項目（外部認証サーバの情報を直接指定するとき）

属性	説明
default_realm	デフォルトのレルム名を指定します。GUI のログイン画面でレルム名を省略してユーザー ID を入力した場合に、この項目で指定したレルムに所属するユーザーとして認証されます。この項目は必須です。 デフォルト値：なし
dns_lookup_kdc	false を指定します。 デフォルト値：false
default_tkt_enctypes	Kerberos 認証に使用する暗号タイプを指定します。このプロパティは、管理サーバの OS が Windows の場合にだけ有効です。 次の暗号タイプを使用できます。 <ul style="list-style-type: none"> <li>• aes128-cts</li> <li>• rc4-hmac</li> <li>• des3-cbc-sha1</li> <li>• des-cbc-md5</li> <li>• des-cbc-crc</li> </ul> 複数指定する場合は、コンマ (,) で区切ってください。 指定した暗号タイプのうち、管理サーバの OS と Kerberos サーバの両方でサポートされているものが使用されます。 デフォルト：なし（DES-CBC-MD5 での認証）
clockskew	管理サーバと Kerberos サーバ間の時刻の差の許容範囲を指定します。この値よりも時刻に差がある場合、認証エラーになります。 指定できる値：0～300（秒） デフォルト値：300
timeout	Kerberos サーバと接続するときの接続待ち時間です。この値を 0 にした場合、タイムアウトしないで、通信エラーが発生するまで待ち続けます。 指定できる値：0～120（秒） デフォルト値：3
realm_name	レルム識別名を指定します。レルムごとに Kerberos サーバの情報を区別するために付ける任意の名称です。必ず 1 つ以上のレルム識別名を指定してください。レルム識別名を複数指定する場合は、レルム識別名をコンマ (,) で区切って指定します。同じレルム識別名は重複して登録しないでください。 デフォルト値：なし

属性	説明
< realm_name に指定した値 > .realm	Kerberos サーバに設定してあるレルム名を指定します。この項目は必須です。 デフォルト値：なし
< realm_name に指定した値 > .kdc*	Kerberos サーバの情報を次の形式で指定します。 <ホスト名または IP アドレス>[:<ポート番号>] この項目は必須です。  <ホスト名または IP アドレス> ホスト名を指定する場合、IP アドレスへの名前解決ができることを事前に確認してください。IP アドレスは、IPv4 アドレスで指定してください。IPv6 環境では、ホスト名で指定してください。ただし、ループバックアドレス (localhost または 127.0.0.1) を指定しないでください。  <ポート番号> 指定するポートが Kerberos サーバで待ち受けポート番号として設定されていることを事前に確認してください。ポート番号を省略した場合、または指定したポート番号が Kerberos サーバで使用できないポート番号である場合は、88 を指定したと見なされます。  Kerberos サーバを冗長構成にする場合は、次のようにコンマ (,) で区切って指定します。 <ホスト名または IP アドレス>[:<ポート番号>], <ホスト名または IP アドレス>[:<ポート番号>], ...
<p>※ 外部認可サーバの接続プロトコルに StartTLS を使用する場合は、外部認可サーバのサーバ証明書の CN と同じホスト名を設定してください。IP アドレスは使用できません。</p> <p>注：各属性は、次のように指定します。 auth.kerberos.&lt;属性&gt;=&lt;値&gt;</p>	

表 19 Kerberos サーバで認証する場合の exauth.properties ファイルの設定項目 (外部認証サーバの情報を DNS サーバに照会するとき)

属性	説明
default_realm	デフォルトのレルム名を指定します。GUI のログイン画面でレルム名を省略してユーザー ID を入力した場合に、この項目で指定したレルムに所属するユーザーとして認証されます。この項目は必須です。 デフォルト値：なし
dns_lookup_kdc	true を指定します。この項目は必須です。 ただし、次のすべての属性に値を設定していると、Kerberos サーバは DNS サーバに照会されません。 <ul style="list-style-type: none"> <li>• realm_name</li> <li>• &lt; realm_name に指定した値 &gt; .realm</li> <li>• &lt; realm_name に指定した値 &gt; .kdc</li> </ul>
default_tkt_encypes	Kerberos 認証に使用する暗号タイプを指定します。このプロパティは、管理サーバの OS が Windows の場合にだけ有効です。 次の暗号タイプを使用できます。 <ul style="list-style-type: none"> <li>• aes128-cts</li> <li>• rc4-hmac</li> <li>• des3-cbc-sha1</li> <li>• des-cbc-md5</li> </ul>

属性	説明
	<ul style="list-style-type: none"> <li>des-cbc-crc</li> </ul> 複数指定する場合は、コンマ (,) で区切ってください。 指定した暗号タイプのうち、管理サーバの OS と Kerberos サーバの両方でサポートされているものが使用されます。 デフォルト：なし (DES-CBC-MD5 での認証)
clockskew	管理サーバと Kerberos サーバ間の時刻の差の許容範囲を指定します。この値よりも時刻に差がある場合、認証エラーになります。 指定できる値：0～300 (秒) デフォルト値：300
timeout	Kerberos サーバと接続するときの接続待ち時間です。この値を 0 にした場合、タイムアウトしないで、通信エラーが発生するまで待ち続けます。 指定できる値：0～120 (秒) デフォルト値：3
注：各属性は、次のように指定します。 auth.kerberos.<属性>=<値>	

表 20 Kerberos サーバで認証する場合の exauth.properties ファイルの設定項目 (外部認可サーバの設定)

属性	説明
protocol*	LDAP ディレクトリサーバ接続のプロトコルです。 平文による通信の場合は ldap、StartTLS による通信の場合は tls を指定します。Kerberos サーバの情報を直接指定する場合にだけ、StartTLS で通信できます。 tls を指定する場合には、LDAP ディレクトリサーバで次のどれかの暗号方式を使用できることを事前に確認してください。 <ul style="list-style-type: none"> <li>TLS_RSA_WITH_AES_256_GCM_SHA384</li> <li>TLS_RSA_WITH_AES_256_CBC_SHA256</li> <li>TLS_RSA_WITH_AES_256_CBC_SHA</li> <li>TLS_RSA_WITH_AES_128_CBC_SHA256</li> <li>TLS_RSA_WITH_AES_128_CBC_SHA</li> <li>SSL_RSA_WITH_3DES_EDE_CBC_SHA</li> </ul> 指定できる値：ldap または tls デフォルト値：ldap
port	LDAP ディレクトリサーバのポート番号です。指定するポートが、LDAP ディレクトリサーバで待ち受けポート番号として設定されていることを事前に確認してください。 指定できる値：1～65535 デフォルト値：389
basedn	LDAP ディレクトリサーバの情報を検索する際に、起点となるエントリーの DN (BaseDN) です。この DN より下の階層のユーザーエントリーが認可の対象となります。 検索対象のユーザーエントリーをすべて含む階層の DN を指定してください。 DN は RFC4514 の規約に従って指定してください。例えば、次の文字が DN に含まれる場合は、1 文字ごとに円記号 (¥) でエスケープする必要があります。 空白文字 # + ; , < = > ¥ 指定した値は LDAP ディレクトリサーバにそのまま渡されるため、BaseDN にエスケープが必要な文字が含まれる場合は、正しくエスケープしてください。



属性	説明
	省略した場合は、Active Directory の defaultNamingContext 属性に指定されている値が BaseDN と見なされます。 デフォルト値：なし
timeout	LDAP ディレクトリサーバと接続するときの接続待ち時間です。この値を 0 にした場合、タイムアウトしないで、通信エラーが発生するまで待ち続けます。 指定できる値：0~120 (秒) デフォルト値：15
retry.interval	LDAP ディレクトリサーバとの通信を削除した場合のリトライ間隔となる秒数です。 指定できる値：1~60 (秒) デフォルト値：1
retry.times	LDAP ディレクトリサーバとの通信を削除した場合のリトライ回数です。この値を 0 にした場合、リトライされません。 指定できる値：0~50 デフォルト値：20
<p>※ LDAP ディレクトリサーバの接続プロトコルに StartTLS を使用する場合には、共通コンポーネントのセキュリティ設定が必要です。</p> <p>注：各属性は、次のように指定します。</p> <p>auth.group.&lt;レルム名&gt;.&lt;属性&gt;=&lt;値&gt;</p> <p>&lt;レルム名&gt;には auth.kerberos.&lt;realm_name に指定した値&gt;.rHealm の値を指定します。</p>	

表 21 Kerberos サーバで認証する場合の exauth.properties ファイルの設定項目 (外部認可サーバと StartTLS で通信するとき)

プロパティ名	説明
auth.ocsp.enable	LDAP ディレクトリサーバと StartTLS で通信する場合に、OCSP レスポンダーを使用して LDAP ディレクトリサーバの電子署名証明書の有効性を検証するかどうかを指定します。 検証する場合は true を、検証しない場合は false を指定します。 デフォルト値：false
auth.ocsp.responderURL	電子署名証明書の AIA フィールドに記載された OCSP レスポンダー以外の OCSP レスポンダーで電子署名証明書の有効性を検証する場合に、OCSP レスポンダーの URL を指定します。省略した場合は、AIA フィールドに記載された OCSP レスポンダーに問い合わせます。 デフォルト値：なし

## 4.8.6 Kerberos サーバで認証する場合の exauth.properties ファイルの設定例

Kerberos サーバで認証する場合の exauth.properties ファイルの設定例を次に示します。

- Kerberos サーバの情報を直接指定する場合 (外部認可サーバと連携しないとき)

```
auth.server.type=kerberos
auth.group.mapping=false
auth.kerberos.default_realm=EXAMPLE.COM
auth.kerberos.dns_lookup_kdc=false
auth.kerberos.clockskew=300
auth.kerberos.timeout=3
auth.kerberos.realm_name=RealmName
auth.kerberos.RealmName.realm=EXAMPLE.COM
auth.kerberos.RealmName.kdc=kerberos.example.com:88
```

- Kerberos サーバを DNS サーバに照会する場合（外部認可サーバと連携しないとき）

```
auth.server.type=kerberos
auth.group.mapping=false
auth.kerberos.default_realm=EXAMPLE.COM
auth.kerberos.dns_lookup_kdc=true
auth.kerberos.clockskew=300
auth.kerberos.timeout=3
```

- Kerberos サーバの情報を直接指定する場合（外部認可サーバとも連携するとき）

```
auth.server.type=kerberos
auth.group.mapping=true
auth.ocsp.enable=false
auth.ocsp.responderURL=
auth.kerberos.default_realm=EXAMPLE.COM
auth.kerberos.dns_lookup_kdc=false
auth.kerberos.clockskew=300
auth.kerberos.timeout=3
auth.kerberos.realm_name=RealmName
auth.kerberos.RealmName.realm=EXAMPLE.COM
auth.kerberos.RealmName.kdc=kerberos.example.com:88
auth.group.EXAMPLE.COM.protocol=ldap
auth.group.EXAMPLE.COM.port=389
auth.group.EXAMPLE.COM.basedn=dc=Example,dc=com
auth.group.EXAMPLE.COM.timeout=15
auth.group.EXAMPLE.COM.retry.interval=1
auth.group.EXAMPLE.COM.retry.times=20
```

- Kerberos サーバを DNS サーバに照会する場合（外部認可サーバとも連携するとき）

```
auth.server.type=kerberos
auth.group.mapping=true
auth.kerberos.default_realm=EXAMPLE.COM
auth.kerberos.dns_lookup_kdc=true
auth.kerberos.clockskew=300
auth.kerberos.timeout=3
```

- 冗長構成の場合

```
auth.server.type=kerberos
auth.group.mapping=false
auth.kerberos.default_realm=EXAMPLE.COM
auth.kerberos.dns_lookup_kdc=false
auth.kerberos.clockskew=300
auth.kerberos.timeout=3
auth.kerberos.realm_name=S1
auth.kerberos.S1.realm=EXAMPLE.COM
auth.kerberos.S1.kdc=kerberos.example.com:88,kerberos.example.net:88
```

- レalm識別名を複数指定した場合

```
auth.server.type=kerberos
auth.group.mapping=false
auth.kerberos.default_realm=EXAMPLE.COM
auth.kerberos.dns_lookup_kdc=false
auth.kerberos.clockskew=300
auth.kerberos.timeout=3
auth.kerberos.realm_name=S1,S2
auth.kerberos.S1.realm=EXAMPLE.COM
auth.kerberos.S1.kdc=kerberos1.example.com:88,kerberos1.example.net:88
auth.kerberos.S2.realm=EXAMPLE.NET
auth.kerberos.S2.kdc=kerberos2.example.com:88,kerberos2.example.net:88
```

## 4.9 情報検索用のユーザーアカウントとは

情報検索用のユーザーアカウントとは、認証・認可対象のアカウントが存在するか LDAP ディレクトリサーバ内の情報を検索する際に使用されるユーザーアカウントです。

次の運用を行う場合には、管理サーバに情報検索用のユーザーアカウントを登録しておく必要があります。

- LDAP ディレクトリサーバを外部認証サーバとして利用し、データ構造が階層モデルの場合
- LDAP ディレクトリサーバを外部認可サーバとして利用する場合  
GUI で、共通コンポーネントを使用する製品に認可グループを登録する際に、認可グループの **Distinguished Name** が外部認可サーバに登録されているか確認したい場合、**System** アカウントなど共通コンポーネントを使用する製品に登録されたユーザー **ID** で操作するためには、情報検索用のユーザーアカウントを管理サーバに登録しておく必要があります。

上記以外の場合は、認証・認可時にユーザー情報の検索を行わないため、この作業は不要です。すでに登録されている場合は、削除してください。

### 4.9.1 情報検索用のユーザーアカウントの条件

情報検索用のユーザーアカウントの条件は、認証方式によって異なります。

次の条件を満たすユーザーアカウントを LDAP ディレクトリサーバに準備してください。

認証方式が LDAP の場合

- `exauth.properties` ファイルの `auth.ldap.<auth.server.name>` に指定した値 `>.basedn` で指定した DN にバインドできること
- `exauth.properties` ファイルの `auth.ldap.<auth.server.name>` に指定した値 `>.basedn` で指定した DN 以下のすべてのエントリーに対して属性を検索できること
- `exauth.properties` ファイルの `auth.ldap.<auth.server.name>` に指定した値 `>.basedn` で指定した DN を参照できること
- `exauth.properties` ファイルの `auth.ldap.<auth.server.name>` に指定した値 `>.basedn` で指定した DN 下にある認可グループを参照できること (外部認可サーバとも連携するとき)
- `exauth.properties` ファイルの `auth.ldap.<auth.server.name>` に指定した値 `>.basedn` で指定した DN 下にある認可グループの属性と、認可グループのネストグループの属性を検索できること (外部認可サーバとも連携するとき)

認証方式が RADIUS の場合

- `exauth.properties` ファイルの `auth.group.<ドメイン名>.basedn` で指定した DN にバインドできること
- `exauth.properties` ファイルの `auth.group.<ドメイン名>.basedn` で指定した DN 以下のすべてのエントリーに対して属性を検索できること
- `exauth.properties` ファイルの `auth.group.<ドメイン名>.basedn` で指定した DN を参照できること
- `exauth.properties` ファイルの `auth.group.<ドメイン名>.basedn` で指定した DN 下にある認可グループを参照できること

- `exauth.properties` ファイルの `auth.group.<ドメイン名>.basedn` で指定した DN 下にある認可グループの属性と、認可グループのネストグループの属性を検索できること

認証方式が **Kerberos** の場合

- `exauth.properties` ファイルの `auth.group.<レルム名>.basedn` で指定した DN にバインドできること
- `exauth.properties` ファイルの `auth.group.<レルム名>.basedn` で指定した DN 以下のすべてのエントリーに対して属性を検索できること
- `exauth.properties` ファイルの `auth.group.<レルム名>.basedn` で指定した DN を参照できること
- `exauth.properties` ファイルの `auth.group.<レルム名>.basedn` で指定した DN 下にある認可グループを参照できること
- `exauth.properties` ファイルの `auth.group.<レルム名>.basedn` で指定した DN 下にある認可グループの属性と、認可グループのネストグループの属性を検索できること

## 4.9.2 情報検索用のユーザーアカウントの登録

`hcmds64ldapuser` コマンドを実行して、情報検索用のユーザーアカウントを管理サーバに登録します。

### 前提条件

- LDAP ディレクトリサーバへの情報検索用のユーザーアカウントの登録
- 次の情報の確認
  - 情報検索用ユーザーの DN とパスワード
  - LDAP ディレクトリサーバのサーバ識別名または外部認可サーバ用のドメイン名（認証方式が LDAP の場合）  
`exauth.properties` ファイルの `auth.server.name` プロパティに指定したサーバ識別名または `auth.ldap.<auth.server.name に指定した値>.domain.name` プロパティに指定したドメイン名を指定します。
  - RADIUS サーバのドメイン名（認証方式が RADIUS の場合）  
`exauth.properties` ファイルの `auth.radius.<auth.server.name に指定した値>.domain.name` に指定したドメイン名を指定します。
  - Kerberos サーバのレルム名（認証方式が Kerberos の場合）  
`exauth.properties` ファイルで **Kerberos** サーバの情報を直接指定した場合は、`auth.kerberos.default_realm` の値、または `auth.kerberos.<auth.kerberos.realm_name 値>.realm` の値を指定します。  
`exauth.properties` ファイルで **Kerberos** サーバの情報を DNS サーバに照会するように設定した場合は、DNS サーバに登録されたレルム名を指定します。

### 操作手順

1. `hcmds64ldapuser` コマンドを実行します。

Windows の場合：

```
<共通コンポーネントのインストールフォルダ>%bin%\hcmds64ldapuser /set /dn
<情報検索用ユーザーの DN > [/pass <情報検索用ユーザーのパスワード>] /name
<名前>
```

Linux の場合 :

```
<共通コンポーネントのインストールディレクトリ>/bin/hcmds64ldapuser -set
-dn <情報検索用ユーザーの DN > [-pass <情報検索用ユーザーのパスワード>] -
name <名前>
```

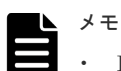
- <情報検索用ユーザーの DN >

DN は RFC4514 の規約に従って指定してください。例えば、次の文字が含まれる場合は、1文字ごとに円記号 (¥) でエスケープする必要があります。

空白文字 # + , ; < = > ¥

- <情報検索用ユーザーのパスワード>

大文字と小文字の違いも含めて、LDAP ディレクトリサーバに登録しているパスワードと完全に一致する必要があります。pass オプションを省略してコマンドを実行すると、対話形式でパスワードを入力できます。



- LDAP ディレクトリサーバでは DN やパスワードに引用符 (") を使用できますが、管理サーバには DN およびパスワードに引用符 (") が含まれていないユーザーアカウントを登録してください。

- Active Directory が提供する dsquery コマンドでユーザーの DN を確認できます。dsquery コマンドを使用して、ユーザー「administrator」の DN を確認する場合の実行例と実行結果を次に示します。

```
dsquery user -name administrator
"CN=administrator,CN=admin,DC=example,DC=com"
```

- DN が「cn=administrator,cn=admin,dc=example,com」の場合など、DN にコンマ (,) が含まれる場合は次のように指定します。

Windows の場合 :

```
hcmds64ldapuser /set /dn
"cn=administrator,cn=admin,dc=example¥,com" /pass
administrator_pass /name ServerName
```

Linux の場合 :

```
hcmds64ldapuser -set -dn
"cn=administrator,cn=admin,dc=example¥¥,com" -pass
administrator_pass -name ServerName
```

---

### 4.9.3 情報検索用のユーザーアカウントの削除

hcmds64ldapuser コマンドを実行して、情報検索用のユーザーアカウントを管理サーバから削除します。

#### 前提条件

次の情報の確認

- LDAP ディレクトリサーバのサーバ識別名または外部認可サーバ用のドメイン名 (認証方式が LDAP の場合)
- RADIUS サーバのドメイン名 (認証方式が RADIUS の場合)
- Kerberos サーバのレルム名 (認証方式が Kerberos の場合)

#### 操作手順

1. hcmds64ldapuser コマンドを実行します。

Windows の場合 :

```
<共通コンポーネントのインストールフォルダ>%bin%hcmds64ldapuser /delete /
name <名前>
```

Linux の場合 :

```
<共通コンポーネントのインストールディレクトリ>/bin/hcmds64ldapuser -
delete -name <名前>
```

## 4.9.4 情報検索用ユーザーアカウントを登録済みの LDAP ディレクトリサーバの確認

hcmds64ldapuser コマンドを実行して、情報検索用ユーザーアカウントを管理サーバに登録済みの LDAP ディレクトリサーバを確認します。

### 操作手順

1. hcmds64ldapuser コマンドを実行します。

Windows の場合 :

```
<共通コンポーネントのインストールフォルダ>%bin%hcmds64ldapuser /list
```

Linux の場合 :

```
<共通コンポーネントのインストールディレクトリ>/bin/hcmds64ldapuser -list
```

## 4.10 共有秘密鍵の登録

hcmds64radiussecret コマンドを実行して、RADIUS サーバの共有秘密鍵 (shared secret) を管理サーバに登録します。

### 前提条件

次の情報の確認

- 共有秘密鍵
- RADIUS サーバのサーバ識別名  
exauth.properties ファイルの auth.server.name プロパティに指定するサーバ識別名と一致している必要があります。

### 操作手順

1. hcmds64radiussecret コマンドを実行します。

Windows の場合 :

```
<共通コンポーネントのインストールフォルダ>%bin%hcmds64radiussecret [/set
<共有秘密鍵>] /name <RADIUS サーバのサーバ識別名>
```

Linux の場合 :

```
<共通コンポーネントのインストールディレクトリ>/bin/hcmds64radiussecret
[-set <共有秘密鍵>] -name <RADIUS サーバのサーバ識別名>
```

- set オプションを省略してコマンドを実行すると、対話形式で共有秘密鍵を入力できます。

## 4.10.1 共有秘密鍵の削除

hcmds64radiussecret コマンドを実行して、共有秘密鍵 (shared secret) を削除します。

### 前提条件

RADIUS サーバのサーバ識別名を確認する

### 操作手順

1. hcmds64radiussecret コマンドを実行します。

Windows の場合 :

```
<共通コンポーネントのインストールフォルダ>%bin%hcmds64radiussecret /
delete /name <RADIUS サーバのサーバ識別名>
```

Linux の場合 :

```
<共通コンポーネントのインストールディレクトリ>/bin/hcmd64radiussecret -
delete -name <RADIUS サーバのサーバ識別名>
```

## 4.10.2 共有秘密鍵が登録されている RADIUS サーバの確認

hcmds64radiussecret コマンドを実行して、共有秘密鍵 (shared secret) を管理サーバに登録済みの RADIUS サーバを確認します。

### 操作手順

1. hcmd64radiussecret コマンドを実行します。

Windows の場合 :

```
<共通コンポーネントのインストールフォルダ>%bin%hcmd64radiussecret /list
```

Linux の場合 :

```
<共通コンポーネントのインストールディレクトリ>/bin/hcmd64radiussecret -
list
```

### 操作結果

RADIUS サーバのサーバ識別名が表示されます。

## 4.11 外部認証サーバおよび外部認可サーバとの接続確認

hcmd64checkauth コマンドを実行して、管理サーバから外部認証サーバおよび外部認可サーバに正しく接続できるか確認します。

### 前提条件

- 外部認証サーバと外部認可サーバの登録
- 次の情報の確認
  - 認証方式が LDAP の場合  
LDAP ディレクトリサーバに登録されているユーザーアカウントを確認してください。ユーザー ID は、exauth.properties ファイルの auth.ldap.<auth.server.name に指定した値>.attr で指定した属性に格納されている値を指定してください。

- 認証方式が **RADIUS** の場合  
RADIUS サーバに登録されているユーザーアカウントを確認してください。
- 認証方式が **Kerberos** の場合  
外部認証サーバとだけ連携する場合：  
共通コンポーネントを使用する製品に登録されていて、かつ認証方式が **Kerberos** のユーザーアカウントを確認してください。  
外部認可サーバとも連携する場合：  
共通コンポーネントを使用する製品に登録されていないユーザーアカウントを確認してください。  
なお、exauth.properties ファイルの default\_realm で設定したレルム名とは異なるレルムに所属するユーザーを指定する場合、ユーザーが所属するレルムも確認してください。exauth.properties ファイルでレルム名を複数指定した場合、指定したレルム名をすべて確認してください。  
なお、ユーザー **ID** またはパスワードの先頭に、**Windows** の場合はスラント (/)、**Linux** の場合はハイフン (-) が含まれるユーザーアカウントは使用できません。

## 操作手順

1. hcnds64checkauth コマンドを実行します。

Windows の場合：

```
<共通コンポーネントのインストールフォルダ>%bin%hcnds64checkauth [/user
<ユーザー ID > /pass <パスワード>] [/summary]
```

Linux の場合：

```
<共通コンポーネントのインストールディレクトリ>/bin/hcnds64checkauth [-
user <ユーザー ID > -pass <パスワード>] [-summary]
```

- user オプションおよび pass オプションを省略してコマンドを実行すると、対話形式でユーザー ID およびパスワードを入力できます。
- summary オプションを指定すると、コマンド実行時に表示される確認メッセージが簡略化されます。



**メモ** 認証方式が **Kerberos** の場合、exauth.properties ファイルでレルム名を複数指定したときは、レルムごとに接続確認してください。また、ユーザー ID は次の形式で指定してください。

- exauth.properties ファイルの default\_realm で設定したレルム名とは異なるレルムに所属するユーザーを指定する場合：  
<ユーザー ID >@<レルム名>
- exauth.properties ファイルの default\_realm で設定したレルムに所属するユーザーを指定する場合：  
レルム名を省略して入力できます。
- 認証方式が **LDAP** でマルチドメイン構成の場合、hcnds64checkauth コマンドを実行すると、連携しているすべての外部認証サーバに対して検証し外部認証サーバごとに検証結果が表示されます。  
hcnds64checkauth コマンドで指定したユーザーアカウントが登録されていない外部認証サーバでは、検証結果のフェーズ 3 でユーザーアカウントが登録されていないことを示すエラーメッセージが表示され、フェーズ 3 での確認で失敗することがあります。  
この場合、接続確認したい外部認証サーバごとに、外部認証サーバに登録されているユーザーアカウントで確認してください。



## 操作結果

exauth.properties ファイルの設定や、外部認証サーバおよび外部認可サーバとの接続状況が検証され、検証結果がフェーズごとに表示されます（全4フェーズ）。各フェーズでの確認が正常に終了した場合、次のメッセージが表示されます。

```
KAPM15004-I The result of the configuration check of Phase <phase-number> was normal.
```

### フェーズ 1

exauth.properties ファイルの共通のプロパティが正しく設定されているか検証します。

### フェーズ 2

exauth.properties ファイルの外部認証サーバと外部認可サーバのプロパティが正しく設定されているか検証します。

### フェーズ 3

外部認証サーバに接続できるか検証します。

### フェーズ 4

外部認可サーバとも連携するよう設定されている場合に、外部認可サーバに接続できるか、および認可グループを検索できるかを検証します。

## 4.12 外部認証サーバとの連携設定に使用するコマンドに関する注意事項

外部認証サーバと連携するための設定で実行するコマンドの引数に、コマンドラインの制御文字が含まれる場合には、コマンドラインの仕様に従い正しくエスケープしてください。

また、円記号 (¥) はコマンドラインでは特殊な扱いとなるため、引数に円記号 (¥) が含まれる場合には注意が必要です。

**hcnds64ldapuser** コマンド、**hcnds64radiussecret** コマンド、および **hcnds64checkauth** コマンドを実行する際のエスケープ方法は次のとおりです。

### Windows の場合 :

次の文字が含まれる場合は、引数を引用符 (") で囲むか、1文字ごとにキャレット (^) でエスケープしてください。

空白文字 & | ^ < > ( )

円記号 (¥) は、次に続く文字によってはエスケープ文字として扱われることがあります。このため、引数に円記号 (¥) と上記の文字が含まれる場合には、引用符 (") で囲まないで、上記文字を1文字ごとにキャレット (^) でエスケープしてください。

また、引数の末尾に円記号 (¥) がある場合は、円記号 (¥) でエスケープしてください。

### Linux の場合 :

次の文字が含まれる場合は、引数を引用符 (") で囲むか、1文字ごとに円記号 (¥) でエスケープしてください。

空白文字 # & ' ( ) ~ ¥ ` < > ; |

ただし、円記号 (¥) は、引用符 (") で囲われていてもエスケープ文字として扱われます。引数に円記号 (¥) が含まれる場合には、必ず円記号 (¥) でエスケープしてください。

例えば、hcnds64radiussecret コマンドで登録する共有秘密鍵が「secret01¥」の場合は、次のとおりエスケープしてください。

Windows の場合 :

```
hcnds64radiussecret /set secret01¥¥ /name ServerName
```

Linux の場合 :

次のどちらかの形式で指定してください。

```
hcnds64radiussecret -set secret01¥¥ -name ServerName
```

```
hcnds64radiussecret -set "secret01¥¥" -name ServerName
```

## 4.13 Kerberos 認証に使用できる暗号タイプ

共通コンポーネントを使用する製品でサポートされている暗号タイプを使用できるように Kerberos サーバを構築してください。

共通コンポーネントを使用する製品で、Kerberos 認証に使用できる暗号タイプ (encryption types) は次のとおりです。

- AES256-CTS-HMAC-SHA1-96
- AES128-CTS-HMAC-SHA1-96
- RC4-HMAC
- DES3-CBC-SHA1
- DES-CBC-CRC
- DES-CBC-MD5

# Automation Director を削除する

この章では、Automation Director を削除する方法について説明します。

- 5.1 Automation Director を削除する (Windows)
- 5.2 クラスタ環境で Automation Director を削除する
- 5.3 認証データを削除する (Windows)
- 5.4 Automation Director を削除する (Linux)
- 5.5 認証データを削除する (Linux)

## 5.1 Automation Director を削除する (Windows)

Windows 環境で Automation Director を削除するには、次のセクションに記載されている手順に従います。

### 前提条件

- Automation Director のタスクタブの「状態」列が待機中、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。
- サーバ上のセキュリティ監視、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 (¥Base64¥database) を削除しないでください。このフォルダを削除すると、共通コンポーネントを使用するほかの製品が停止します。

### 操作手順

- Windows に管理者としてログインします。
- 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>¥bin¥hcmds64srv /stop
- [Control Panel] を開き、[Programs and Features] または [Add or Remove Programs] を選択します。
- [Automation Director] を選択して [Remove] をクリックするか、プログラムを選択し、右クリックして [Uninstall] を選択します。
- [Setup] ウィンドウで [Uninstallation] をクリックして、ソフトウェア削除プロセスを開始します。  
削除プロセスによって、<Automation Director のインストールフォルダ>¥Automation フォルダが削除されます。

### 操作結果

Automation Director がホストから削除されます。

## 5.2 クラスタ環境で Automation Director を削除する

Automation Director を別のサーバに移行するか、運用を中止する場合には、クラスタ環境のサーバから Automation Director ソフトウェアを削除します。



**メモ** Automation Director を削除した場合、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が削除されます。

### 操作手順

- クラスタ管理ソフトウェアで、Automation Director 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 [Move] を選択し、[Select Node] または [Move this service or application to another node] 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（Automation Director 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>%ClusterSetup  
%hcms64clustersrvstate /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（Automation Director 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。たとえば、グループ名が Automation Director cluster の場合は、"Automation Director 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（Automation Director 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、クラスタ管理ソフトウェアから customer script 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>%ClusterSetup

%hcms64clustersrvupdate /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（Automation Director 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。たとえば、グループ名が Automation Director cluster の場合は、"Automation Director 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 Automation Director 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。ただし、Hitachi File Services Manager のサービスは削除されません。
- 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、Automation Director を削除した後で再登録できます。Automation Director 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、共通コンポーネントを使用する製品を停止します。  
<共通コンポーネントのインストールフォルダ>%bin%hcms64srv /stop
5. アクティブノードから Automation Director を削除します。
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（クラスタ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など）を削除します。
7. クラスタ管理ソフトウェアで、Automation Director 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 [Move] を選択してから、[Select Node] または [Move this service or application to another node] を選択します。
8. スタンバイノードから Automation Director を削除します。
9. クラスタインストールの削除を実行した後、Automation Director フォルダを削除して、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（クラスタ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>%ClusterSetup
```

```
%hcms64clustersrvupdate /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。たとえば、グループ名が Automation Director cluster の場合は、"Automation Director cluster" と指定します。

- /sd

クラスタ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 hcms64clustersrvupdate コマンドを実行します。

- /ap

クラスタ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>%ClusterSetup
```

```
%hcms64clustersrvstate /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。たとえば、グループ名が Automation Director cluster の場合は、"Automation Director cluster" と指定します。

14. クラスタ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 [Move] を選択してから、[Select Node] または [Move this service or application to another node] を選択します。

## 5.3 認証データを削除する (Windows)

Automation Director の削除が正常に完了したにもかかわらず KNAE04574-E 警告ダイアログボックスが表示された場合、認証データの削除は失敗しています。データを削除するには、ユーザーアカウントを管理するサーバ（共通コンポーネントを使用する製品がインストールされている接続先のホスト）上で **hcms64intg** コマンドを実行します。

**hcms64intg** コマンドを実行して、Windows ホストから認証データを削除するには：

### 操作手順

1. 次のコマンドを実行して、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製品のすべてのサービスを開始します。  
<共通コンポーネントのインストールフォルダ>%bin%hcms64srv /start
  2. 次のコマンドを実行して、認証データを削除します。  
<共通コンポーネントのインストールフォルダ>%bin%hcms64intg /delete /type <コンポーネント名> /user <ユーザー ID > /pass <パスワード>
- /type

削除するコンポーネントの名前を指定します。Automation を指定できます。

- /user  
Admin (ユーザー管理) 権限を持つユーザーのユーザー ID を指定します。user オプションを指定せずにコマンドを実行した場合、ユーザー ID の指定を求められます。
- /pass  
Admin (ユーザー管理) 権限を持つユーザーのパスワードを指定します。pass オプションを指定せずにコマンドを実行した場合、パスワードの指定を求められます。



**メモ** 認証データを削除せずに、共通コンポーネントを使用する別の製品の GUI ウィンドウを表示した場合、Automation Director サーバを削除した後でも、次のような問題が発生することがあります。

- Automation Director サーバのユーザー管理情報が表示される。
- ダッシュボードにある Automation Director サーバを起動するためのボタンが有効になる。ボタンをクリックすると、リンクエラーが表示される。

## 5.4 Automation Director を削除する (Linux)

Linux 環境で Automation Director を削除するには、次の手順に従います。

### 操作手順

1. root ディレクトリ (/root など) に移動します。
2. 次のコマンドを実行します。  
<Automation Director のインストールディレクトリ>/ADUninstall/uninstall.sh

## 5.5 認証データを削除する (Linux)

Automation Director の削除が正常に完了したにもかかわらず KNAE04574-E 警告ダイアログボックスが表示された場合、認証データの削除は失敗しています。データを削除するには、ユーザーアカウントを管理するサーバ (共通コンポーネントを使用する製品がインストールされている接続先のホスト) 上で、**hcmds64intg** コマンドを実行します。

### 操作手順

1. 次のコマンドを実行して、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製品のすべてのサービスを開始します。  
<共通コンポーネントのインストールディレクトリ>/bin/hcmd64srv -start
  2. 次のコマンドを実行して、認証データを削除します。  
<共通コンポーネントのインストールディレクトリ>/bin/hcmd64intg -delete -type <コンポーネント名> -user <ユーザー ID > -pass <パスワード>
- -type  
削除するコンポーネントの名前を指定します。Automation を指定できます。
  - -user  
Admin (ユーザー管理) 権限を持つユーザーのユーザー ID を指定します。user オプションを指定せずにコマンドを実行した場合、ユーザー ID の指定を求められます。
  - -pass  
Admin (ユーザー管理) 権限を持つユーザーのパスワードを指定します。pass オプションを指定せずにコマンドを実行した場合、パスワードの指定を求められます。



**メモ** 認証データを削除せずに、共通コンポーネントを使用する別の製品の GUI ウィンドウを表示した場合、Automation Director サーバを削除した後も、次のような問題が発生することがあります。

- Automation Director サーバのユーザー管理情報が表示される。
  - ダッシュボードにある Automation Director サーバを起動するためのボタンが有効になる。ボタンをクリックすると、リンクエラーが表示される。
-



# Automation Director のファイルの場所と ポート

この付録には、Automation Director のインストール時に作成されるすべてのフォルダの一覧が含まれています。またポートの一覧も含まれています。

- [A.1 Automation Director のファイルの場所](#)
- [A.2 ポート設定](#)

## A.1 Automation Director のファイルの場所

### インストール先フォルダ

次の表は、Automation Director をインストールしたときに作成されるフォルダを示しています。「Windows フォルダの場所」列、または「Linux ディレクトリの場所」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。

Windows フォルダの詳細	Windows フォルダの場所
インストール先フォルダ	<code>system-drive¥Program Files¥hitachi¥Automation</code>
コマンドファイル	<code>system-drive¥Program Files¥hitachi¥Automation¥bin</code>
構成ファイル	<code>system-drive¥Program Files¥hitachi¥Automation¥conf</code>
サービステンプレートのフォルダ	<code>system-drive¥Program Files¥hitachi¥Automation¥contents</code>
データファイル	<code>system-drive¥Program Files¥hitachi¥Automation¥data</code>
ヘルプファイル	<code>system-drive¥Program Files¥hitachi¥Automation¥docroot</code>
事前設定プロパティ定義ファイル	<code>system-drive¥Program Files¥hitachi¥Automation¥extra_presets</code>
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	<code>system-drive¥Program Files¥hitachi¥Automation¥inst</code>
ライブラリファイル	<code>system-drive¥Program Files¥hitachi¥Automation¥lib</code>
ログファイル	<code>system-drive¥Program Files¥hitachi¥Automation¥logs</code>
オープンソースソフトウェアのソースファイル	<code>system-drive¥Program Files¥hitachi¥Automation¥ossSource</code>
システムファイル	<code>system-drive¥Program Files¥hitachi¥Automation¥system</code>
内部コマンドによって使用される作業用ファイル	<code>system-drive¥Program Files¥hitachi¥Automation¥webapps</code>
作業用フォルダ	<code>system-drive¥Program Files¥hitachi¥Automation¥work</code>
共通コンポーネント	<code>system-drive¥Program Files¥hitachi¥Base64</code>

Linux ディレクトリの詳細	Linux ディレクトリの場所
インストール先ディレクトリ	<code>/opt/hitachi/Automation</code>
コマンドファイル	<code>/opt/hitachi/Automation/bin</code>
構成ファイル	<code>/opt/hitachi/Automation/conf</code>
サービステンプレートのディレクトリ	<code>/var/opt/hitachi/Automation/contents</code>
データファイル	<code>/var/opt/hitachi/Automation/data</code>
ヘルプファイル	<code>/opt/hitachi/Automation/docroot</code>
事前設定プロパティ定義ファイル	<code>/var/opt/hitachi/Automation/extra_presets</code>
インストールおよびアンインストール時の一時作業ディレクトリ	<code>/opt/hitachi/Automation/inst</code>

Linux ディレクトリの詳細	Linux ディレクトリの場所
ライブラリファイル	/opt/hitachi/Automation/lib
ログファイル	/var/opt/hitachi/Automation/logs
オープンソースソフトウェアのソースファイル	/opt/hitachi/Automation/ossSource
システムファイル	/opt/hitachi/Automation/system
内部コマンドによって使用される作業用ファイル	/var/opt/hitachi/Automation/work
共通コンポーネント	/opt/hitachi/Base64

## A.2 ポート設定

Automation Director 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	Automation Director ↔ 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	Automation Director ↔ 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。
445/tcp または udp	Automation Director ↔ 操作対象	共有管理に使用されます。 cjstartsv は、このポートを使用します。
135/tcp および 139/tcp	Automation Director ↔ 操作対象	共有管理に使用されます。 cjstartsv は、このポートを使用します。
22015/tcp	ブラウザ → Automation Director	HBase 64 Storage Mgmt Web Service へのアクセスに使用。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 → Automation Director	HBase 64 Storage Mgmt Web Service へのアクセスに使用。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	Automation Director → SMTP サーバ	メール送信に使用されます。 このポート番号は変更できます。 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
88/tcp または udp	Automation Director → Kerberos サーバ	cjstartsv は、このポートを使用します。
359/tcp	Automation Director → LDAP ディレクトリサーバ	ldap/tls に使用されます。 cjstartsv は、このポートを使用します。
636/tcp	Automation Director → LDAP ディレクトリサーバ	LDAP に使用されます。 このポート番号は変更できます。 cjstartsv は、このポートを使用します。
1812/udp	Automation Director → Radius サーバ	Radius サーバに使用されます。 cjstartsv は、このポートを使用します。
さまざまな Web サービス接続ポート/tcp	Automation Director → さまざまなサーバ	Web サービス接続に登録されているサーバに使用されます。

#### 内部接続ポート

ポート番号	ファイアウォール	説明
22017/tcp	Automation Director → Automation Director	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	Automation Director → Automation Director	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。
22025/tcp	Automation Director → Automation Director	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。
22026/tcp	Automation Director → Automation Director	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	Automation Director → Automation Director	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	Automation Director → Automation Director	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	Automation Director → Automation Director	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	Automation Director → Automation Director	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	Automation Director → Automation Director	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	Automation Director → Automation Director	共通コンポーネントへのアクセスに使用されます。

ポート番号	ファイアウォール	説明
		cjstartsv は、このポートを使用します。
22170/tcp	Automation Director → Automation Director	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	Automation Director → Automation Director	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	Automation Director → Automation Director	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	Automation Director → Automation Director	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	Automation Director → Automation Director	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。



# hcnds64keytool ユーティリティを使用して証明書を管理する

hcnds64keytool ユーティリティは、次のようにさまざまな方法で使用できます。

- 証明書をトラストストアにインポートする。
- トラストストアから証明書を削除する。
- Device Manager サーバの自己署名証明書をエクスポートする。
- トラストストアに証明書が正しくインポートされたことを確認する。



メモ 証明書が正しくインポートされたことを確認するには、この手順を実行します。

---

詳細については、『Hitachi Automation Director ユーザーズガイド』を参照してください。





## トラブルシューティング

ここでは、Automation Director サーバ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。

- C.1 保守情報を収集する
- C.2 ログファイルを収集する

## C.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。

## C.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。

### 操作手順

1. Administrator 権限を持つユーザー（Windows の場合）または root ユーザー（Linux の場合）として、管理サーバにログインします。
2. `hcmds64getlogs` コマンドを実行して、ログファイルを収集します。

Windows の場合：

```
<共通コンポーネントのインストールフォルダ>%bin%hcmds64getlogs /dir 出力フォルダのパス
```

Linux の場合：

```
<共通コンポーネントのインストールディレクトリ>/bin/hcmd64getlogs -dir 出力ディレクトリのパス
```

### 操作結果

アーカイブファイルが指定先に出力されます。

『*Hitachi Automation Director ユーザーズガイド*』の「`hcmds64getlogs` コマンド」を参照してください。

# 索引

## A

- auditlog.conf
  - サンプル 60
  - 設定 58
- Automation Director
  - インストールする 22, 28
  - 関連製品 14
  - 基本的なシステム構成 14
  - セキュリティ設定 38
  - ワークフロー 16
- Automation Director のコンポーネントの削除 124, 127
- Automation Director のファイルの場所 129
- Automation Director をインストールする 19
- Automation Director を削除する 123

## E

- exauth.properties ファイル 96, 103
  - Kerberos サーバ 109

## H

- hcmds64unlockaccount コマンド 75
- Hitachi Command Suite 製品 14

## I

- IPv6 76
- IP アドレス
  - 変更する 37

## J

- JDK
  - 変更する 38

## K

- Kerberos サーバ 90
  - exauth.properties ファイル 109

## L

- LDAP サーバ 88
- LDAP ディレクトリサーバ 96
- Linux 127

## R

- RADIUS サーバ 89, 103

## S

- security.conf ファイル 72
- SSL
  - VMware vCenter に SSL をセットアップする 39
  - Web ベースの管理クライアントでセットアップする 48
  - セキュアなクライアント通信のためにサーバ上でセットアップする 39
  - セキュアなクライアント通信のために使用 39
- System アカウント
  - 自動的にロックする 75

## U

- URL
  - 確認する (Linux) 30
  - 確認する (Windows) 29
  - 管理サーバの URL を変更する 37

## W

- Windows 23, 80, 124

## あ

アンインストールする 124, 127

## い

インストール 23  
インストール後のタスク 29  
インストールする  
Automation Director 22, 28  
ソフトウェアを別のホストに移動する 62  
別のホスト 62  
ポートの衝突を回避する 22  
インストールの前提条件 20  
インストールを確認する 30

## う

ウイルススキャン  
抑止する 29  
ウイルススキャンを抑止する  
データベースフォルダ 29

## え

エージェントレス 80

## か

外部認可サーバ 88  
接続確認 119  
登録 95  
外部認証サーバ  
接続確認 119  
登録 95  
概要 13  
関連製品 14  
基本的なシステム構成 14  
ワークフロー 16  
監査ログ 56  
監査ログ (Automation Director サーバ)  
環境設定ファイルの設定 57  
出力形式 60  
管理クライアント  
SSL をセットアップする 48  
セキュアなクライアント通信のためにサーバ上で  
SSL をセットアップする 39  
セキュアなクライアント通信のためにサーバをセ  
ットアップする 39

## き

共有秘密鍵  
確認 119

削除 119  
登録 118

## く

クラスタ 23  
インストールの前提条件 24  
クラスタ環境構成を確認する 25

## こ

構成する  
管理サーバの URL 37  
基本的なシステム 14  
サーバの IP アドレス 37  
サーバのホスト名 37

## さ

サーバ 80  
削除する 124, 127

## し

システムアカウント  
パスワードを変更する 31  
条件  
情報検索用のユーザーアカウント 115  
冗長構成 93  
情報検索用のユーザーアカウント 115  
削除 117  
条件 115  
登録 116

## せ

セキュア通信 38  
セキュリティ設定 72  
Web ベースの管理クライアントで SSL をセットア  
ップする 48  
概要 38  
管理クライアントのセキュア通信 39  
セキュアなクライアント通信のためサーバ上でセ  
ットアップする 39  
セットアップする : VMware vCenter SSL のサー  
バ 39  
セキュリティ設定を変更する 72  
セキュリティ定義 72  
接続確認  
外部認可サーバ 119  
外部認証サーバ 119  
設定 96, 103  
前提条件 80

## そ

ソフトウェアを削除する  
削除手順 124

## て

定義ファイル 70  
ディレクトリサーバ 88

## と

トラブルシューティング 137

## な

名前解決 21

## に

認可グループ 88  
認証  
メソッド 17  
ユーザー 88-90  
外部 87

## は

はじめに 9  
パスワードポリシー 72  
パスワードを変更する  
システムアカウント 31

## ふ

ファイルの場所 130  
プランニング  
ポートの衝突を回避する 22  
プロパティ 76  
プロパティファイル (config\_user.properties) 63

## ほ

ポート  
衝突を回避する 22  
ポートを変更したときに更新を必要とするプロパ  
ティ 35  
ポート設定 131  
保守  
情報 138  
ホスト 70, 80

ホスト名  
変更する 37

## ま

マシン 80  
マニュアルの構成 10  
マルチドメイン構成 93

## め

メール通知 70  
メール通知の構成 70

## ゆ

ユーザーアカウント  
アカウントのロックを解除する 75  
アカウントロック 74  
アカウントロックポリシー 74  
アカウントロックポリシーを設定する 74  
ユーザー管理 87

## ら

ライセンスを登録する 30

## り

リモート接続情報 76  
リモートマシン用接続情報 76

## ろ

ログファイル  
収集する 138  
ログファイルを収集する 138  
ロックする  
System アカウント 75  
アカウントのロックを解除する 75  
ユーザーアカウント 74

## わ

ワークフロー 88-90  
概要 16

