Cisco Unified Communications Manager および IM and Presence サービス アップグレードおよび移行ガイド、リリース 15

最終更新：2024 年 8 月 22 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

Full Cisco Trademarks with Software License

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

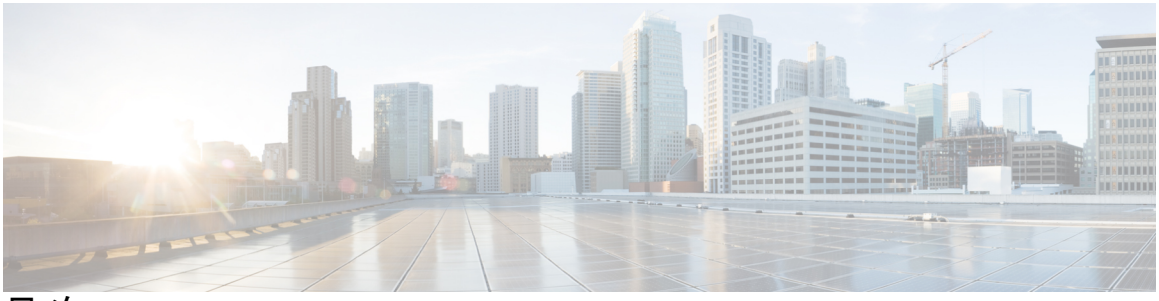
IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

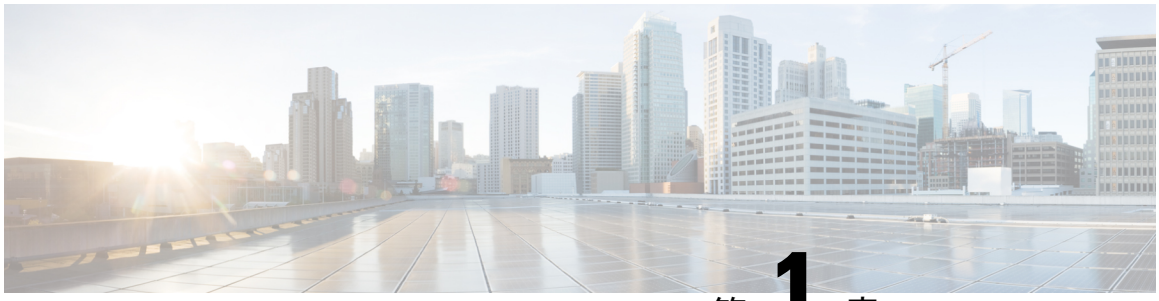
All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)



目 次



第 1 章

新規および変更情報

新規および変更情報

次の表は、この最新リリースに関するこのガイドでの機能に対する大幅な変更の概要を示したものです。ただし、このリリースに関するガイドの変更点や新機能のなかには、この表に記載されていないものもあります。

新規および変更情報

表 *1*:

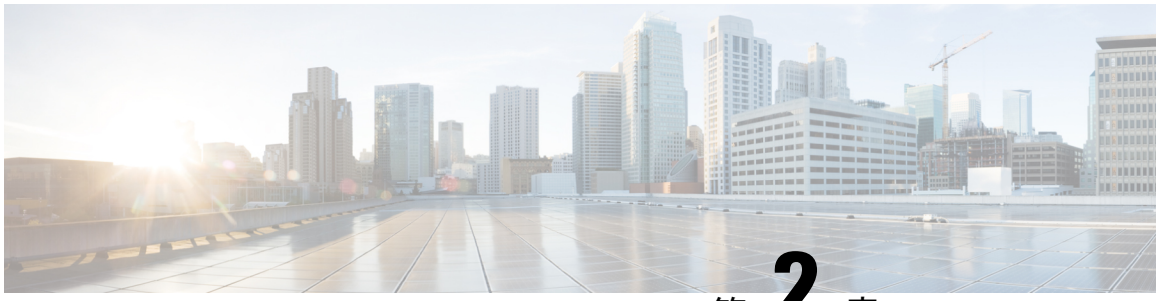
日付（**Date**）	説明	参照先
2023 年 12 月 18 日		• 要件および制約事項 （25 ページ） • 仮想マシンの設定 （26 ページ） • COP ファイルでサポートされているアップグレードおよび移行パス （10 ページ） • Upgrade Readiness COP ファイルの実行（アップグレード前） （54 ページ） • VMware Tools の更新 （136 ページ） • IPSec の要件 （40 ページ）

新規および変更情報

日付（**Date**）	説明	参照先
	Unified Communications Manager、IM and Presence サービス、およびすべてのアプリケーションが 64 ビットアーキテクチャに移動しました。 影響を受ける領域は次のとおりです。 • Unified Communications Manager および IM and Presence Service 15 では、7.0 U3 または 8.0 U1 以上の ESXi バージョンが必要です。 • リリース 15 の Unified Communications Manager は、インストール時に 110 GB 以上の仮想ディスクのみをサポートします。 インストール時の 80GB の仮想ディスクはサポートされていません。 • Pre-12.5.x ソースからリリース 15 への直接更新アップグレードはサポートされていません。 • アップグレード前の準備 COP ファイルには、Unified Communications Manager および IM and Presence サービスの新しいチェックが追加されました。 • Unified Communications Manager および IM and Presence Service 15 は Open VM Tools のみをサポートします。 • Release 15 の FIPS モードでは、3DES アルゴリズムの IPSec ポリシーはサポー	

新規および変更情報

日付（**Date**）	説明	参照先
	トされていません。	
2023 年 12 月 18 日	単一の「CiscoRTMTPlugin.zip」プラグインを使用して、Windows または Linux オペレーティングシステムの両方で実行されるワークステーションで Cisco Unified Real-Time Monitoring Tool (Unified RTMT) をアップグレードできます。	RTMT のアップグレード（141 ページ）



第 2 章

アップグレードの計画

アップグレードと移行の概要

このガイドの手順では、Cisco Unified Communications Manager (Unified Communications Manager) および Cisco Unified Communications Manager IM and Presence Service (IM and Presence Service) を以前のバージョンから現在のバージョンにアップグレードする方法について説明しています。

すべてのアップグレードと移行パスの開始点として、このガイドの手順を使用してください。このガイドで「アップグレード」という用語が使用されいる際は、アップグレードという用語の用法に注意してください。

- 「アップグレード」という用語は、すべてのクラスターノードがエンドツーエンドのプロセスに必要なステップを完了するシナリオを指します。結果として、クラスタ全体がアップグレード先のバージョンで実行されます。この場合、アップグレードは「完了」と見なされます。「アップグレード」のエンドツーエンドのプロセスは、すべてのノードがアップグレード-非アクティブバージョンを完了し、すべてのノードがバージョンの切り替え-リブートを完了し、すべてのクラスターノード間でデータベースのレプリケーションが完了すると定義されます。アップグレード状況の確認については、手動でバージョンを切り替える (クラスター全体) （61 ページ） のセクションを参照してください。
- 「非アクティブ バージョン」または「非アクティブ バージョンのアップグレード」という用語は、1 つ以上のクラスタノードで、切り替え-バージョン-再起動を実行しないまたは実行する前に、非アクティブバージョンのみをアップグレードすることを意味します。

アップグレードに関する推奨される考慮事項:

1. 「直接アップグレード」の方法を選択します。[シンプルアップグレード]を選択することを推奨しますが、従来の単一ノードのアップグレード方法を実行することもできます。アップグレード方法 （6 ページ）を参照してください。
2. 選択したアップグレード方法に関係なく、すべてのクラスタノードを完了させる必要があります。
   - 無効なバージョンをアップグレード
   - バージョンを切り替えて再起動
   - クラスターのすべてのノードでデータベースのレプリケーションが完了するのを待ちます。
3. 「順序付けの規則と時間要件」の章で説明されているように、アップグレード計画のステップ 2 に記載されているポイントがノードの順序付け規則に従うようにする必要があります。
4. ステップ 2 のすべての要件が完了しないと、アップグレードは完了しません。 Cisco Unified OS Administration ユーザーインターフェイスからアップグレードステータスを表示するか、ステータスを監視する CLI コマンドを使用できます。 すべてのクラスタでステップ 2 の条件が満たされるまで、クラスタノードへのブロックおよび追加/更新/削除の機能の可能性について警告するバナー メッセージがユーザーインターフェイスで表示されます。

アップグレード方法

次の表では、Cisco Unified Communications Manager および IM and Presence サービスで完了できるアップグレードのタイプ、およびアップグレードを完了するために使用できるアップグレードツールについて説明します。

アップグレードの種類	説明	アップグレードツール
直接標準アップグレード	標準アップグレードは、アプリケーション ソフトウェアをアップグレードする必要があるが、基礎となるオペレーティングシステムをアップグレードする必要がない場合の直接アップグレードです。 これは通常最も簡単なアップグレードの形式で、OS が両方のリリースで同じである同じメジャーマイナーリリースカテゴリ内からのアップグレードに適用されます。 リリース 12.5 以降では、直接の標準アップグレードにより、期間が大幅に改善され、手順が簡素化され、サービスへの影響が軽減されました。 **例**: 12.5 (1) から 12.5(1)SU1 へのアップグレード。 （**注**） アップグレード前のリリースが 12.5 (1) 以降である標準アップグレードの場合、簡素化されたクラスター全体のアップグレードを使用して、クラスター全体をアップグレードできます。	標準アップグレードを完了するには、以下のツールを使用します。 • Unified OS Admin • CLI • PCD アップグレードタスク
直接のアップグレードの更新	直接のアップグレードの更新とは、アプリケーション ソフトウェアと基礎となるオペレーティングシステム ソフトウェアの両方をアップグレードする必要がある場合の、直接アップグレードです。 これは通常、1 つのメジャーマイナーリリースから、2 つのリリースで OS が異なる別のリリースにアップグレードする場合に使用されます。 **例** : Pre-12.5.x ソースからリリース 15 への更新アップグレードはサポートされていません。	更新アップグレードを完了するには、以下のツールを使用します。 • 統合 OS 管理 • CLI • PCD アップグレードタスク

アップグレードの種類	説明	アップグレードツール
直接移行	直接移行では、直接アップグレードだけでは対処できない複数の要素が存在する場合に「システムの再構築」が行われます。 直接移行は次の場合に使用されます。 • サイトの移転 • 目的のアップグレードでは、インフラストラクチャ ハードウェアとプラットフォームを変更する必要があります。 **例**: ESXi 5.5 の Unified CM 10.5(x) と Cisco UCS M3 世代ハードウェアを ESXi 7.0 の 12.5(x) と Cisco UCS M5 世代ハードウェアにアップグレード。 • ESXi のアップグレードおよび/または Unified CM 仮想マシン構成の変更 • Unified CM アドレス/ホスト名の変更 • 希望するアップグレードには、ソースリリースに存在しない直接アップグレードパスが必要です。 **例**: ESXi の Unified CM 8.5(1) を ESXi の 12.5(x) にアップグレード—直接のアップグレードパスは存在せず、移行が必須。 • 「仮想から仮想 (V2V)」への移行。直接アップグレードパスが存在する場合でも、継続時間、サービスへの影響、短い停止期間など、アップグレードパスの複雑さの要因を軽減するために直接移行が好まれます。	移行を完了するには、次のツールを使用します。 • PCD の移行 • データ インポートを伴うフレッシュ インストール

アップグレードの種類	説明	アップグレードツール
データインポートでインストール	フレッシュ インストールとデータ インポートは、リリース 10.5 以降からリリース 15 への直接アップグレードおよび直接移行の代替方法です。これには以下が含まれます。 • 10x または 11x のソースリリースに **ciscocm.DataExport_v1.0.cop.sgn** COP ファイルをインストールします。 • ソースリリースのデータを Secure FTP（SFTP）サーバーにエクスポートします。 • リリース 15 の新しい仮想マシンをインストールしてから、このデータをインポートします(通常、応答ファイルとインポート データの両方が事前にステージングされるタッチレス クラスター インストール)。 前のリリースにロールバックするには、**ciscocm.DataExport_rollback_v1.0.cop.sgn** COP ファイルをインストールします。	データインポートを含むインストールを完了するために CLI が使用されます
レガシーリリースからの移行	レガシーリリースとは、非常に古いソースリリースであるため、希望するアップグレードには直接アップグレードパスも、ターゲットリリース 15 への直接移行パスもありません。唯一のオプションは、PCD 移行をサポートする新しいリリースへの直接アップグレードか、データインポートを使用したインストールを行い、その後 PCD 以降または、データインポートをリリース 15 にフレッシュインストールします。 **例**: 10.5 より前の Unified CM または 10.5 より前の IM and Presence Service から 15 へのアップグレード希望。	詳細については、レガシーリリースからのアップグレード（149 ページ）を参照してください。

現行システムを記録する

アップグレードを開始する前に、現在のシステム設定内のバージョン管理を記録します。現行システムで使用されているバージョンがわかったら、アップグレードの計画を開始できます。次の作業が含まれます。

- Unified Communications Manager および IM and Presence サービスのアップグレード前バージョン
- 現在のハードウェアバージョン
- VMware バージョン管理

（注） VMware は、Unified CM 8.x および 9.x でオプションの展開として導入されました。 リリース 10.x 以降、VMware は必須になりました。

Pre-upgrade Upgrade Readiness COP ファイルを実行することでバージョン情報を取得できます。詳細については、Upgrade Readiness COP ファイルの実行（アップグレード前） （54 ページ）を参照してください。

COP ファイルでサポートされているアップグレードおよび移行パス

次の表では、Cisco Unified Communications Manager および IM and Presence Service のリリース 15 以降へのアップグレードでサポートされているアップグレードパスを示します。 また、COP ファイルを必要とするアップグレードパスも示します。 アップグレードを開始する前に Cisco Unified OS 管理者インターフェイスを使用して、またはアップグレードまたは移行を開始する前に、Cisco Prime Collaboration Deployment（PCD）ツールを使用して、各ノードに COP ファイルをインストールする必要があります。 PCD を使用している場合、アップグレードを開始する前に、COP ファイルの一括インストールを実行できます。

（注） 特に明記されていない限り、各リリースカテゴリには、そのカテゴリ内の SU リリースが含まれます。

Cisco Unified Communications Manager および IM and Presence Service の COP ファイルは、https://software.cisco.com/download/home/268439621 からダウンロードできます。 アップグレードの移行先バージョンを選択したら、**[Unified Communications Manager ユーティリティ（Unified Communications Manager Utilities）]** を選択して COP ファイルの一覧を表示します。

（注） 必須ではありませんが、アップグレードを成功させるために、アップグレードの前にアップグレードの準備 COP ファイルを実行することを強くお勧めします。 Cisco TAC は、効果的なテクニカルサポートを提供するために、この COP ファイルの実行を要求する場合があります。

（注） ソースが FIPS モードおよび/または PCD が FIPS モードの場合、https://www.cisco.com/web/software/286319173/139477/ciscocm.ciscossl7_upgrade_CSCwa48315_CSCwa77974_v1.0.k4.cop-ReadMe.pdf にある COP ファイル `ciscocm.ciscossl7_upgrade_CSCwa48315_CSCwa77974_v1.0.k4.cop` に関する情報を参照してください。 このドキュメントでは、15 の移行先バージョンへの直接アップグレードまたは直接移行に必要な前提条件について詳しく説明します。

（注） リリース 15 以降への直接の標準アップグレードがソースリリースから利用可能な場合、シングルノードまたはクラスター全体のアップグレードのいずれかを選択できます。

クラスタ全体をアップグレードするときに、継続時間、ダウンタイム、サービスへの影響、または管理者の介入が最小になると予想される場合は、Unified OS Admin アップグレードまたは CLI アップグレードを使用した Unified CM Publisher 経由のクラスタアップグレードの詳細を示す「クラスタ全体のアップグレードタスクフロー（直接標準）」手順を使用します。 ここでは、Unified CM Publisher のみをアップグレードし、クラスタ内の他のすべてのノードのアップグレードまたは再起動を調整します。

ソースをノードごとにアップグレードするか、ローカルの Unified OS Admin アップグレードまたは CLI アップグレードを使用してシングルノードのみを使用する場合は、「クラスタノードをアップグレードする（直接標準）」の項を参照してください。 詳細については、『Cisco Unified Communications Manager および IM and Presence Service アップグレードおよび移行ガイド』を参照してください。

（注） 『アップグレードガイド』に記載されているとおり、アップグレード計画がノードのシーケンスルールに従っていることを確認する必要があります。 IM and Presence Service ノードのバージョンを切り替える前に、まず Unified Communications Manager ノードを切り替える必要があります。パブリッシャノードから開始して、サブスクライバノードを開始します。

上記の順序に従わず、Unified Communications Manager パブリッシャノードがバージョン 15 以降に切り替わり、IM and Presence Service パブリッシャノードのバージョンが 12.5.x または 14 および SU のままでアップグレードされていない場合、[ソフトウェアアップグレード（Software Upgrades）] メニューの以下のページは IM and Presence Service ノードでは表示されず、または機能しません。

- クラスタの再起動/バージョンの切り替え
- クラスタ ソフトウェア ロケーション
- ソフトウェアのインストールおよびクラスタのアップグレード

（注） Unified Communications Manager および IM and Presence Service リリース 15 以降のバージョンには、直接のアップグレードの更新でサポートされているパスはありません。 12.5.x 以前の更新元からリリース 15 以降へのアップグレードの更新はサポートされていません。

表 *2 : Cisco Unified Communications Manager* および *IM Presence Service* でサポートされているアップグレードパスおよび *COP* ファイル

ソース（Source）	通知先（Destination）	メカニズム	前提条件	バージョン切り替え*（ソースから移行先およびその逆）
10.0	15	PCD 15 移行タスク（V2V）	15 への直接アップグレードはサポートされていません。 移行先のバージョンが 15、移行元のバージョンが 10.0 の場合、移行には Cisco Prime Collaboration Deployment（PCD）を使用する必要があります。 移行先のバージョンが 15 で移行元のバージョンが 10.0 が FIPS モードの場合、Cisco Prime Collaboration Deployment（PCD）は非 FIPS モードである（または非 FIPS モードにする）必要があります。	なし

ソース（Source）	通知先（Destination）	メカニズム	前提条件	バージョン切り替え*（ソースから移行先およびその逆）
10.5	15	PCD 15 移行タスク（V2V）	pre-upgrade-check COP ファイルを実行します。 移行の前に ciscocm.CSCwi52160_15-direct-migration_v1.0.k4.cop.sha512 COP ファイルをインストールする必要があります。 15 への直接アップグレードはサポートされていません。 移行先のバージョンが 15、移行元のバージョンが 10.5 の場合、移行には Cisco Prime Collaboration Deployment（PCD）を使用する必要があります。 移行先のバージョンが 15 で、移行元のバージョンが 10.5 が FIPS モードの場合、次のいずれかになります。 • PCD が非 FIPS モードである（または配置されている）必要があります。 • PCD 移行タスクを使用する代わりに、データインポートでフレッシュインストールを使用します。	なし
		フレッシュインストールとデータインポート（V2V）	• pre-upgrade-check COP ファイルを実行します。 • ciscocm.CSCwi52160_15-direct-migration_v1.0.k4.cop.sha512 • ciscocm.DataExport_v1.0.cop.sgn	サポート対象外

ソース（Source）	通知先（Destination）	メカニズム	前提条件	バージョン切り替え*（ソースから移行先およびその逆）
11.0	15	PCD 15 移行タスク（V2V）	pre-upgrade-check COP ファイルを実行します。 移行の前に ciscocm.CSCwi52160_15-direct-migration_v1.0.k4.cop.sha512 COP ファイルをインストールする必要があります。 移行先のバージョンが 15 で、移行元のバージョンが 11.0 が FIPS モードの場合、次のいずれかになります。 • PCD が非 FIPS モードである（または配置されている）必要があります。 • PCD 移行タスクを使用する代わりに、データインポートでフレッシュインストールを使用します。	サポート対象外
		フレッシュインストールとデータインポート（V2V）	• pre-upgrade-check COP ファイルを実行します。 • ciscocm.CSCwi52160_15-direct-migration_v1.0.k4.cop.sha512 • ciscocm.DataExport_v1.0.cop.sgn	サポート対象外

ソース（Source）	通知先（Destination）	メカニズム	前提条件	バージョン切り替え*（ソースから移行先およびその逆）
11.5	15	PCD 15 移行タスク（V2V）	pre-upgrade-check COP ファイルを実行します。 移行の前に ciscocm.CSCwi52160_15-direct-migration_v1.0.k4.cop.sha512 COP ファイルをインストールする必要があります。 移行先のバージョンが 15 で、移行元のバージョンが 11.5 が FIPS モードの場合、次のいずれかになります。 • PCD が非 FIPS モードである（または配置されている）必要があります。 • PCD 移行タスクを使用する代わりに、データインポートでフレッシュインストールを使用します。	サポート対象外
		フレッシュインストールとデータインポート（V2V）	• pre-upgrade-check COP ファイルを実行します。 • ciscocm.CSCwi52160_15-direct-migration_v1.0.k4.cop.sha512 • ciscocm.DataExport_v1.0.cop.sgn	サポート対象外

ソース（Source）	通知先（Destination）	メカニズム	前提条件	バージョン切り替え*（ソースから移行先およびその逆）
12.0	15	PCD 15 移行タスク（V2V）	pre-upgrade-check COP ファイルを実行します。 移行の前に ciscocm.CSCwi52160_15-direct-migration_v1.0.k4.cop.sha512 COP ファイルをインストールする必要があります。 移行元バージョンが Unified Communications Manager（12.0.1.10000-10）のリリース 12.0 (1) である場合、COP ファイル ciscocm-slm-migration.k3.cop.sgn をインストールする必要があります。 これは、たとえば、リリース 12.0(1)SU1 のように、移行元バージョンの方が高い場合には必要ありません。	サポート対象外
		フレッシュインストールとデータインポート（V2V）	• pre-upgrade-check COP ファイルを実行します。 • ciscocm.CSCwi52160_15-direct-migration_v1.0.k4.cop.sha512 • ciscocm.DataExport_v1.0.cop.sgn	サポート対象外

ソース（Source）	通知先（Destination）	メカニズム		前提条件	バージョン切り替え*（ソースから移行先およびその逆）
12.5	15	直接標準アップグレード（シンプルアップグレード）	OS 管理または CLI 経由	• pre-upgrade-check COP ファイルを実行します。	サポートされる
		直接標準アップグレード	PCD 15 アップグレードタスク経由		サポートされる

ソース（Source）	通知先（Destination）	メカニズム		前提条件	バージョン切り替え*（ソースから移行先およびその逆）

				• pre-upgrade-check COP ファイルを実行します。
				• Unified CM ソースが 12.5.1.14900-63 より古い場合、ciscocm.enable-sha512sum-2021-signing-key-v1.0.cop.sgn の COP ファイルをインストールします。
				• IM and Presence Service の移行元が 12.5.1.14900-4 より古い場合、ciscocm.enable-sha512sum-2021-signing-key-v1.0.cop.sgn の COP ファイルをインストールします。
				• 移行先のバージョンが 15 で、移行元のバージョンが 12.5 が FIPS モードの場合、次のいずれかになります。
				  • PCD が非 FIPS モードである（または配置されている）必要があります。
				  • PCD アップグレードタスクを使用する代わりに、データインポートでフレッシュインストールを使用します。
				• Cisco Prime Collaboration Deployment を使用して、IM and Presence Service クラスターをリリース 12.5.x からリリース 15 にアップグレードする場合、アップグレードを開始する前に、ciscocm.imp15_upgrade_v1.0.k4.cop.sha512 の COP ファイルをリリース 12.5.x システムにインストールする必要があります。
				COP ファイルは次の場合にのみ適用	

ソース（Source）	通知先（Destination）	メカニズム		前提条件	バージョン切り替え*（ソースから移行先およびその逆）
				できます。 • Unified Communications Manager の移行先バージョンはリリース 15 です。 • Unified Communications Manager の移行先バージョンがリリース 15 で、IM and Presence Serive の移行元を制限付きバージョンから無制限バージョンにアップグレードしようとしています。	
		PCD 15 移行タスク（V2V）		pre-upgrade-check COP ファイルを実行します。 移行の前に ciscocm.CSCwi52160_15-direct-migration_v1.0.k4.cop.sha512 COP ファイルをインストールする必要があります。 移行先のバージョンが 15 で、移行元のバージョンが 12.5 が FIPS モードの場合、次のいずれかになります。 • PCD が非 FIPS モードである（または配置されている）必要があります。 • PCD 移行タスクを使用する代わりに、データインポートでフレッシュインストールを使用します。	サポート対象外
		フレッシュインストールとデータインポート（V2V）		• pre-upgrade-check COP ファイルを実行します。 • ciscocm.CSCwi52160_15-direct-migration_v1.0.k4.cop.sha512 • ciscocm.DataExport_v1.0.cop.sgn	サポート対象外

ソース（Source）	通知先（Destination）	メカニズム		前提条件	バージョン切り替え*（ソースから移行先およびその逆）
14 および SU	15	直接標準アップグレード（シンプルアップグレード）	OS 管理または CLI 経由	pre-upgrade-check COP ファイルを実行します。	サポートされる
		直接標準アップグレード	PCD アップグレードタスク経由		サポートされる

ソース（Source）	通知先（Destination）	メカニズム		前提条件	バージョン切り替え*（ソースから移行先およびその逆）
				pre-upgrade-check COP ファイルを実行します。 • 移行先のバージョンが 15 で、移行元のバージョンが 14 で、FIPS モードが SU の場合、次のいずれかになります。 • PCD が非 FIPS モードである（または配置されている）必要があります。 • PCD アップグレードタスクを使用する代わりに、データインポートでフレッシュインストールを使用します。 • Cisco Prime Collaboration Deployment を使用して、IM and Presence Service クラスターをリリース 14 または SU からリリース 15 にアップグレードする場合、アップグレードを開始する前に、ciscocm.imp15_upgrade_v1.0.k4.cop.sha512 の COP ファイルをリリース 14 または SU のシステムにインストールする必要があります。 COP ファイルは次の場合にのみ適用できます。 • Unified Communications Manager の移行先バージョンはリリース 15 で、IM and Presence Service の移行元ノードは 14 または 14SU1 バージョンです。 • Unified Communications Manager の移行先バージョンがリリース 15 で、IM and Presence Serive の移行元を制限付きバージョンから無制限バージョンにアップグ	

ソース（Source）	通知先（Destination）	メカニズム	前提条件	バージョン切り替え*（ソースから移行先およびその逆）
			レードしようとしています。	
		PCD 15 移行タスク（V2V）	pre-upgrade-check COP ファイルを実行します。 移行の前に ciscocm.CSCwi52160_15-direct-migration_v1.0.k4.cop.sha512 COP ファイルをインストールする必要があります。 移行先のバージョンが 15 で、移行元のバージョンが FIPS モードで 14 または SU の場合、次のいずれかになります。 • PCD が非 FIPS モードである（または配置されている）必要があります。 • PCD 移行タスクを使用する代わりに、データインポートでフレッシュインストールを使用します。	サポート対象外
		フレッシュインストールとデータインポート（V2V）	• pre-upgrade-check COP ファイルを実行します。 • ciscocm.CSCwi52160_15-direct-migration_v1.0.k4.cop.sha512 • ciscocm.CSCwi52160_15-direct-migration_v1.0.k4.cop.sha512 • ciscocm.DataExport_v1.0.cop.sgn	サポート対象外

* バージョン切り替えとは、非アクティブバージョンとして新しいバージョンをインストールして新しいバージョンに切り替え、必要なときにいつでも古いバージョンに戻す機能を指します。この機能はほとんどの直接アップグレードでサポートされていますが、移行ではサポートされていません。

（注） PCD アップグレードと移行：上記の表の PCD アップグレードタスクまたは PCD 移行タスクを使用したすべてのサポートされているパスでは、PCD リリース 15 を使用する必要があります。

アップグレードツールを選択する

複数のメカニズムから選択できる場合に、使用するアップグレードツールを決定するのに役立つ情報については、下の表を参照してください。

（注） レガシーのアップグレードの詳細については、「レガシーリリースからのアップグレード（149 ページ）」を参照してください。

表 3: アップグレード方法を選択する

アップグレード方法	サポート	このメソッドの使用タイミング...	アップグレードまたは移行の完了方法
Unified OS Admin または CLI のアップグレード	Cisco Unified OS Administration GUI または CLI からの直接アップグレード（標準または更新）。	次のような場合にこのツールを検討します: • クラスタ全体のアップグレードを簡素化する場合。 • アプリケーションソフトウェアのみを変更し、ハードウェアまたは VMware を更新しません。 • 直接アップグレードパスが存在します。 • Unified CM および IM and Presence サービスのみをアップグレードします。 他の UC アプリケーションはありません。 • 単一の Unified CM クラスタと単一の IM and Presence サブクラスタをアップグレードします。 （注） CLI アップグレードは、Unified OS Admin アップグレードと同じサポートを提供しますが、インターフェイスは異なります。	アップグレードタスク（49 ページ） に進みます。

アップグレード方法	サポート	このメソッドの使用タイミング...	アップグレードまたは移行の完了方法
PCD アップグレード	Cisco Prime Collaboration Deployment のアップグレードタスク経由で直接アップグレード (標準または更新) を処理します。	次のような場合にこのツールを検討します: • アップグレードするクラスターが複数あります。 • クラスタに多数のノードがあり、スケジュールを進めるためにアップグレードを調整するのにはサポートが必要です。 • Cisco Unity Connection や Cisco Unified Contact Center Express など、他のアプリケーションをアップグレードする必要があります。	**From Release は 10.x 以降です** **1.** Upgrade Readiness COP ファイルの実行（アップグレード前） （54 ページ） **2.** 「Cisco Prime Collaboration 導入アドミニストレーション ガイド」を参照して、アップグレードまたは移行タスクを実行します。 **3.** アップグレードの準備 COP ファイルの実行 (アップグレード後) （72 ページ） （注） From リリースが 9.x より前の場合、アップグレードの準備 COP ファイルは機能しません。 付録のアップグレード前のタスクとアップグレード後のタスクを手動で実行する必要があります。
PCD の移行	Cisco Prime Collaboration Deployment 経由で移行を処理します。	次のような場合にこのツールを検討します: • VMware を使用していない以前のリリースからアップグレードしています。 • お使いのソースリリースは古いため、VMware をサポートしていません。 • アプリケーションバージョンのアップグレードに加えて、ESXi の更新も行う必要があります。 • インフラストラクチャ ハードウェアとプラットフォームを変更しようとしています。 • ソースリリースが pre-11.5 バージョンから以前にアップグレードされており、ディスク容量不足の問題が発生しています。使用可能なディスク容量を最大にするために、最新のスタックを再インストールする必要がある場合があります。 • 一時的にコピーされた VM と必要なハードウェアに対して利用可能なインフラストラクチャがあります。	

アップグレード方法	サポート	このメソッドの使用タイミング...	アップグレードまたは移行の完了方法
データインポートを伴うフレッシュインストール	ソースリリースデータをSFTPにエクスポートし、そのデータのインポートを使用して新しい15クラスタをタッチレスインストールすることで、移行を処理します。	次のような場合にこのツールを検討します: • 15への直接アップグレードの更新を実行したくないが、それが利用可能な唯一の直接アップグレードパスタイプの場合。 • 直接更新アップグレードの代わりに、PCDで直接移行 (再アドレスと一時的な追加ハードウェアを含む) を行いたくはありません。	1. ソースリリースが10.5、11.5、および12.5.1から12.5(1)SU4の場合、COPをインストールします。 2. CLIを実行してデータをSFTPにエクスポートします。 3. タッチレスインストール (インストールガイドを参照) には、新しい応答ファイルフィールドと、SFTPからデータをインポートするための新しいインストーラGUIフィールドが追加されました。

要件および制約事項

次のセクションでは、このリリースへのアップグレードの要件と制限について説明します。

ハードウェア要件

次のタイプのハードウェアでホストされている仮想サーバに、Unified Communications ManagerとIM and Presence Serviceをインストールできます。 現在の展開でこれらのサーバのいずれかが使用されていない場合、サポートされているハードウェアプラットフォームに移行する必要があります。

- Cisco Business Edition 6000または7000アプライアンス
- VMware vSphere ESXiを含む仮想Ciscoハードウェア (Cisco UCSまたはCisco HyperFlexなど)
- VMware vSphere ESXiを使用する仮想化されたサードパーティハードウェア

要件とサポートポリシーは、これらのオプションごとに異なります。 アップグレードを開始する前に、現在のハードウェアが新しいリリースの要件を満たしていることを確認してください。 要件の詳細は、[https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/

virtualization/cisco-collaboration-virtualization.html] に移動して Unified Communications Manager および IM and Presence Service アプリケーションのリンクをたどることで確認できます。

プラットフォームの要件

このセクションでは、仮想マシンに Unified Communications Manager と IM and Presence Service をデプロイする前に満たすべきプラットフォーム要件について説明します。

このリリースでは、Unified Communications Manager および IM and Presence Service を直接サーバーハードウェアにインストールすることはできません。これらのアプリケーションは、仮想マシンで実行する必要があります。

仮想マシン上でソフトウェアをインストールまたはアップグレードする前に、次の作業を行う必要があります。

- プラットフォームを設定します。
- ESXi 仮想化ソフトウェアをインストールして設定します。

（注） 最新の Unified Communications Manager 互換/サポート対象の ESXi バージョンは、 https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/virtualization-cisco-unified-communications-manager.html および https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/cisco-collaboration-infrastructure.html#VMwareCompatibilityを参照してください。

- Cisco が提供するそのリリースに適した OVA ファイルから仮想マシンを展開します。 使用するインストール方法によっては、追加の手順が必要です。

仮想マシンの設定

アップグレードまたは移行を開始する前に、現在の仮想マシン (VM) ソフトウェアが新しいリリースの要件を満たしていることを確認してください。

表 *4*：仮想マシンの要件

項目	説明
OVA テンプレート	OVA ファイルは、仮想マシン設定用の定義済みテンプレート一式を提供します。これらは、サポートされている容量レベルや、必要な OS/VM/SAN 連携などの項目をカバーしています。Unified Communications Manager および IM and Presence Service アプリケーション用に提供された OVA ファイルから VM 設定を使用する必要があります。 OVA ファイルから使用する正しい VM 設定は、展開のサイズに基づきます。OVA ファイルについての情報は、次の場所で「Unified Communications Virtualization サイジングガイドライン」を検索してください https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/collaboration-virtualization-sizing.html。
VMware vSphere ESXi	互換性とリリースのサポート要件を満たす vSphere ESXi ハイパーバイザーのバージョンをインストールする必要があります。 Cisco Prime Collaboration Deployment (PCD) を使用してアップグレードまたは移行を実行する場合、vSphere ESXi を正しいライセンスタイプでインストールしていることを確認する必要があります。PCD は、vSphere ESXi のすべてのライセンスタイプと互換性があるわけではありません。これらのライセンスの一部は必要な VMware API を有効にしないためです。
VMware vCenter	Unified Communications Manager または IM and Presence Service を、Business Edition 6000/7000 アプライアンスまたは UC on UCS テスト済み参照設定ハードウェアにデプロイする場合、VMware vCenter は任意です。 VMware vCenter は、UCS 仕様ベースおよびサードパーティ サーバ仕様ベースのハードウェアで UC に展開する場合に必須です。

項目	説明
VM 設定の仮想ハードウェアの仕様	Unified Communications Manager または IM and Presence Service の新しいリリースにアップグレードするために、VM の vRAM を変更する必要があるかどうかを確認します。 お使いの Unified Communications Manager または IM and Presence Service では、現在実行しているよりも多くの vRAM が必要な場合があります。 古いリリースバージョンに十分な vRAM サイズがない場合、 IM and Presence Service リリース 15 への直接アップグレードは失敗します。 ファイルシステムタイプとゲスト OS パーティションは最新である必要があります。そうでないと、スワップサイズ、パーティションの問題、または第 3 の拡張ファイルシステム (ext3) により、Release 15 への直接アップグレードが失敗する可能性があります。 「アップグレード準備 COP ファイル (アップグレード前)」を実行して、アップグレードを妨げる可能性がある問題についてシステムを確認します。 これらの問題に直面した場合、直接アップグレードの代わりに直接移行方法を使用したり、直接アップグレードが成功するように、まずソースリリースをバックアップまたは復元します。 Unified Communications Manager または IM and Presence Service リリース 15 バージョンには、より多くの GB と現在実行中のパーティションとは別のパーティションが必要になる場合があります。 Unified Communications Manager および IM and Presence Service リリース 15 への直接アップグレードは、HDD サイズを手動で 110 GB にサイズ変更した場合でも、すべての単一の 80 GB vDisk 展開で失敗します。 アップグレードの前に vRAM および vDisk の仕様書を確認して、リリース 15 のベース OVA の Readme を参照するか、または QuoteCollab ツールを使用します。 詳細については、次を参照してください。 • VMware を更新する 仮想マシンの設定タスク （77 ページ）。 • vDisk を更新するには、リリース 12.5 または 14 および SU バージョンのいずれかを、ここで直接アップグレードが成功した 110GB として vDisk がインストールされた新しい VMware にバックアップまたは復元します。 または、PCD 移行またはデータ インポート タスク移行を伴うフレッシュ インストールのいずれかを使用して、Unified CM Release 15 OVA テンプレートで展開された新しいノードに移動します。

廃止された電話機のモデル

次の表では、Cisco Unified Communications Manager のこのリリースで廃止される電話機のモデルと、その電話機モデルが最初に廃止される Unified CM リリースを示します。 たとえば、最初にリリース 11.5 (1) で廃止された電話機のモデルは、すべての 12.x リリースを含む以降のすべてのリリースで廃止されます。

現行リリースの Cisco Unified Communications Manager にアップグレードしていて、これらのモデルの電話を展開している場合、その電話はアップグレード後に機能しなくなります。

表 *5:* このリリースで廃止された電話機のモデル

このリリースで廃止された電話機のモデル	初めて廃止予定となった日...
廃止される追加のエンドポイントはありません	リリース 15
廃止される追加のエンドポイントはありません	リリース 14
• Cisco Unified IP 電話 7970G • Cisco Unified IP Phone 7971G-GE • Cisco Unified ワイヤレス IP 電話 7921G	12.0(1) 以降のリリース
• Cisco IP 電話 12 SP+ および関連モデル • Cisco IP Phone 30 VIP および関連モデル • Cisco Unified IP Phone 7902 • Cisco Unified IP Phone 7905 • Cisco Unified IP Phone 7910 • Cisco Unified IP 電話 7910SW • Cisco Unified IP Phone 7912 • Cisco Unified ワイヤレス IP 電話 7920 • Cisco Unified IP Conference Station 7935	11.5(1) 以降のリリース

追加情報については、「フィールドの通知」を参照してください。

推奨されない電話を含むアップグレード

以前のリリースでこれらの電話を使用していて、このリリースにアップグレードする場合は、次の手順を実行します。

1. ネットワーク内の電話がこのリリースでサポートされるかどうかを確認します。
2. サポートされていない電話を特定します。

3. サポートされていない電話の場合は、電話の電源を切り、ネットワークから切断してください。
4. 電話ユーザーに対して、サポートされている電話をプロビジョニングしてください。 移行 FX ツールを使用して、古いモデルから新しいモデルの電話に移行できます。 詳細については、「https://www.unifiedfx.com/products/unifiedfx-migrationfx#endpoint_refresh_tool」を参照してください。
5. ネットワーク内のすべての電話がこのリリースでサポートされるようになったら、システムをアップグレードします。

（注） 廃止された電話もアップグレード後に削除できます。 アップグレードの完了後に管理者が Unified Communications Manager にログインすると、システムは警告メッセージを表示し、管理者に廃止予定の電話を通知します。

ライセンス

廃止された電話をサポート対象の電話に置き換えるために、新しいデバイス ライセンスを購入する必要はありません。 廃止された電話機をシステムから削除するか、新しい Unified Communications Manager バージョンに切り替えて非推奨の電話機の登録に失敗した場合、デバイスライセンスが新しい電話機で使用可能になります。

ネットワーク要件

この項では、Unified Communications Manager と IM and Presence Service を展開する前にネットワークが満たす必要がある要件を示します。

IP アドレスの要件

完全なコラボレーション ソリューションは、多くのサービスが正しく機能するために DNS に依存しているため、可用性の高い DNS 構造を設定する必要があります。 基本的な IP テレフォニーを導入していて、DNS を使用したくない場合は、ゲートウェイおよびエンドポイントデバイスと通信するためにホスト名の代わりに IP アドレスを使用するように Unified Communications Manager と IM and Presence サービスを設定できます。

サーバが固定 IP アドレスを取得するように、静的 IP アドレスを使用するようにサーバを構成する必要があります。 静的 IP アドレスを使用することで、電話をネットワークに接続したときに、Cisco Unified IP Phone をアプリケーションに登録することができます。

DNS の要件

次の要件に注意してください。

- 混合モードの DNS 導入はサポートされていません—Cisco は混合モード導入をサポートしていません。 Unified Communications Manager と IM and Presence Service の両方が DNS を使用するか、使用しないかのいずれかでなければなりません。

- 展開で DNS を使用する場合、Unified Communications Manager かつ IM and Presence Service で同じ DNS サーバを使用する必要があります。 IM and Presence Service と Unified Communications Manager で異なる DNS サーバを使用すると、システムが異常な動作をする可能性があります。
- 展開で DNS を使用しない場合、以下の [ホスト名/IP アドレス] フィールドを編集する必要があります。
  - サーバ—Cisco Unified CM の管理 **サーバ構成** ウィンドウで、クラスタノードの IP アドレスを設定します。
  - IM and Presence UC サービス—Cisco Unified CM Administration **UC サービス設定**ウィンドウで、IM and Presence データベース パブリッシャノードの IP アドレスを指す IM and Presence UC サービスを作成します。
  - CCMCIP プロファイル—Cisco Unified CM IM and Presence 管理 **CCMCIP プロファイルの設定**ウィンドウで、任意の CCMCIP プロファイルからホストの IP アドレスを指定します。
- マルチノードに関する考慮事項—IM and Presence Serviceでマルチノード機能を使用している場合、DNS 設定オプションに関するマルチノードの導入に関する項を IM and Presence Service の設定および管理ガイド で参照してください。
- DNS サーバが Windows 2019 以降で構成されているか、Linux マシンで構成されている DNS サーバを使用していることを確認します。

ファイアウォールの要件

ポート 22 への接続が開き、スロットリングされないようにファイアウォールを構成していることを確認してください。 Unified Communications Manager および IM and Presence サブスクライバノードのインストール中、Unified Communications Manager パブリッシャノードへの複数の接続が立て続けに開きます。 これらの接続を調整すると、インストールが失敗する可能性があります。 セキュリティ全般については、 Cisco Unified Communications Manager セキュリティガイドを参照してください。

（注） ファイアウォール機能はアップグレードやインストールの失敗の原因となることが知られているため、アップグレード中やインストール中は [侵入者/侵入検知] および/または [ブルートフォース攻撃] 機能を無効にすることを推奨します。

ポートの使用の詳細については、 Cisco Unified Communications Manager システム設定ガイドの「Cisco Unified Communications Manager TCP および UDP ポートの使用」の章を参照してください。

SFTP サーバーのサポート

以下の表示に記載されている情報を参考に、システムで使用する SFTP サーバ ソリューションを決定してください。

表 *6 : SFTP* サーバ情報

SFTP サーバ	情報
Cisco Prime Collaboration Deployment の SFTP サーバ	このサーバーはシスコが提供およびテストした唯一の SFTP サーバーであり、Cisco TAC が完全にサポートします。 バージョンの互換性は、使用している Unified Communications Manager および Cisco Prime Collaboration Deployment のバージョンに依存します。 バージョン（SFTP）または Unified Communications Manager をアップグレードする前に、『Cisco Prime Collaboration Deployment Administration Guide』を参照して、互換性のあるバージョンであることを確認してください。
テクノロジー パートナーの SFTP サーバ	これらのサーバーはサードパーティが提供およびテストしたものです。 バージョンの互換性は、サード パーティによるテストに依存します。 テクノロジー パートナーの SFTP サーバまたは Unified Communications Manager をアップグレードする場合、テクノロジー パートナーのページで、互換性のあるバージョンを確認してください。 https://marketplace.cisco.com
他のサードパーティの SFTP サーバ	これらのサーバーはサードパーティが提供するものであり、Cisco TAC はこれらのサーバーを正式にサポートしていません。 バージョンの互換性は、SFTP バージョンと Unified Communications Manager バージョンの互換性を確立するためのベストエフォートに基づきます。 （注） これらの製品はシスコによってテストされていないため、機能を保証することはできません。 Cisco TAC はこれらの製品をサポートしていません。 完全にテストされてサポートされる SFTP ソリューションとしては、Cisco Prime Collaboration Deployment またはテクノロジーパートナーの SFTP サーバーを利用してください。

サブネットの制限

多数のデバイスを含む大きなクラス A またはクラス B サブネットには、 Unified Communications Manager をインストールしないでください。 詳細は、 Cisco Collaboration System 12.x ソリューションリファレンスネットワーク設計 (SRND) を参照してください。

クラスタサイズ

クラスタ内の Unified Communications Manager サブスクライバノードの数は、4 つのサブスクライバノードと 4 つのスタンバイノード、合計 8 つのサブスクライバを超えることはできません。 Unified Communications Managerパブリッシャノード、TFTP サーバーおよびメディアサーバーを含むクラスタ上のサーバーの合計数は 21 を超えることはできません。

クラスター内の IM and Presence Service ノードの最大数は 6 です。

詳細については、http://www.cisco.com/go/ucsrnd の「*Cisco* コラボレーション ソリューション設計ガイダンス」を参照してください。

IP サブネット マスク

24 ビット IP サブネットマスクを使用している場合、次の形式を使用していることを確認してください:255.255.255.0。 255.255.255.000 の形式は使用しないでください。 255.255.255.000 も有効な形式ですが、アップグレード中に問題が発生する可能性があります。 問題を避けるために、アップグレードを開始する前に形式を変更しておくことをお勧めします。 **set network ip eth0 <server_IP_address> 255.255.255.0** コマンドを実行することでサブネットマスクを変更できます。

他の形式はサブネットマスクでサポートされており、この制限は 24 ビットのサブネットマスクにのみ適用されます。

ソフトウェア要件

このセクションでは、Cisco Unified Communications Manager および IM and Presence サービスのアップグレードと移行のアプリケーションソフトウェア要件について記載しています。

Cisco Unified Mobile Communicator のデバイス名

Cisco Unified Mobile Communicator デバイスのデバイス名が 15 文字以下であることを確認してください。 デバイス名が Cisco Unified Mobile Communicator で 15 文字以上の場合、デバイスはアップグレード中に移行されません。

エクスポート制限付きソフトウェアとエクスポート制限なしソフトウェア

Unified Communications Manager および IM and Presence Service のこのリリースでは、輸出制限 (K9) バージョンに加えて、輸出制限なし (XU) バージョンをサポートしています。

（注） ソフトウェアの制限なしバージョンは、さまざまなセキュリティ機能を必要としない特定の顧客のみを対象としています。制限なしバージョンは、一般的な導入を想定していません。

制限なしバージョンは制限付きバージョンと以下の点で異なります。

- ユーザペイロードの暗号化 (情報交換) はサポートされていません。

- Microsoft OCS/Lync または AOL との外部 SIP ドメイン間フェデレーションはサポートされていません。
- 制限なしリリースをインストールした後は、制限付きバージョンにアップグレードすることはできません。 無制限バージョンを含むシステムへの制限付きバージョンのフレッシュインストールもサポートされていません。
- 単一クラスター内のすべてのノードは同じモードである必要があります。 たとえば、同じクラスタ内の Unified Communications Manager と IM and Presence Service は、すべて無制限モードか、すべて制限モードである必要があります。
- IP 電話のセキュリティ設定が変更され、シグナリングとメディア暗号化 (VPN 電話機能により提供される暗号化を含む) が無効になります。

（注） 制限なしリリースをインストールした後では制限付きバージョンにはアップグレードできないことに注意してください。 制限なしバージョンを含むシステム上で制限付きバージョンのフレッシュインストールを実行することは許可されていません。

すべてのグラフィックユーザインターフェース (GUI) およびコマンドラインインターフェース (CLI) で、管理者は製品バージョンを表示できます (制限ありまたは輸出制限なし)。

次の表では、Unified Communications Manager と IM and Presence Service のエクスポート制限なしのバージョンでは利用できない GUI 項目について説明しています。

GUI アイテム	Location	説明
Cisco Unified CM 管理		
VPN の設定	**高度な機能** > **VPN**	このメニューとそのオプションは利用できません。
電話セキュリティ プロファイルの設定	**システム** > **セキュリティ** > **電話セキュリティプロファイル**	**端末セキュリティモード** が **保護なし** に設定されているため、設定することはできません。
Cisco Unified CM IM and Presence Administration		

GUI アイテム	Location	説明
セキュリティ設定	システム > セキュリティ > 設定	• **XMPP** クライアントから **IM/P** サービスのセキュアモードを有効にする 設定を確認できません。 • **[XMPPルータ間セキュアモードを有効にする（Enable XMPP Router-to-Router Secure Mode）]** 設定はオンにできません。 • **[ウェブクライアントで IM/Pサービスセキュアモードを有効化する（Enable Web Client to IM/P Service Secure Mode）]** 設定はオンにできません。 • **SIP** クラスター内 **Proxy-to-Proxy Transport Protocol** を **TLS** に設定するオプションが削除されました。
Cisco SIP Proxy サービスのサービスパラメータ設定	**[システム（System）]** > **[サービスパラメータ（Service Parameters）]** の順に選択し、**[サービス（Service）]** として **[Cisco SIP Proxy]** を選択します。	• **Transport Preferred Order** パラメータのすべての TLS オプションが削除されました。 • TLS オプションが **SIP Route Header Transport Type** パラメータから削除されました。

GUI アイテム	Location	説明
SIP フェデレーション ドメイン	**[プレゼンス（Presence）]>[ドメイン間フェデレーション（Inter-domain Federation）]>[SIPフェデレーション（SIP Federation）]**	OCS/Lync へのドメイン間フェデレーションを構成する場合、エンタープライズ内の別の OCS/Lync とは直接フェデレーションできることしかできないことを示す警告ポップアップが表示されます。 エンタープライズ外部の OCS/Lync へのドメイン間フェデレーションは、無制限モードではサポートされていません。
XMPP フェデレーション設定	**[プレゼンス（Presence）]>[ドメイン間フェデレーション（Inter-domain Federation）]>[XMPPフェデレーション（XMPP Federation）]>[設定（Settings）]**	セキュリティモードを設定することはできません。 **TLS なし**に設定されている。
プロキシの構成設定	**[プレゼンス（Presence）]>[ルーティング（Routing）]>[設定（Settings）]**	TLS または HTTPS リスナを優先プロキシ リスナとして設定することはできません。

Unified CM 9.x からのアップグレード

Unified Communications Manager バージョン 9.x から 10.x 以降へのアップグレードは、バージョン 9.x で次のいずれかの名前の SIP プロファイルがある場合に失敗します。

- 標準 SIP プロファイル
- Cisco VCS の標準 SIP プロファイル
- TelePresence 電話会議の標準 SIP プロファイル
- TelePresence エンドポイントの標準 SIP プロファイル
- モバイル端末用の標準 SIP プロファイル

これらの名前の SIP プロファイルがある場合は、アップグレードを進める前に、名前を変更するか削除する必要があります。

CLI で開始する IM および Presence のアップグレードには OS 管理者アカウントが必要です

utils system upgrade CLI コマンドを使用して IM and Presence サービスノードをアップグレードする場合、管理者権限を持つユーザーではなく、デフォルトの OS 管理者アカウントを使用する必要があります。 さもないと、アップグレードは必須のサービスをインストールするのに必

要な権限レベルを持たず、アップグレードが失敗します。 アカウントの権限レベルは、**show myself** CLI コマンドを実行して確認できます。 このアカウントには権限レベル 4 が必要です。

この制限は、CLI で開始される IM and Presence サービスのアップグレードにのみ存在し、Unified Communications Manager には適用されません。 また、この制限は新しい ISO ファイルでは修正されている可能性があることにも注意してください。 特定の ISO ファイルの詳細については、ISO Readme ファイルを参照してください。 この制限に関する最新情報については、CSCvb14399 を参照してください。

Microsoft SQL Server のアップグレードに必要なデータベースの移行

Microsoft SQL サーバーを、IM and Presence サービスを使用して、外部データベースとしてデプロイし、11.5(1)、11.5(1)SU1、 または11.5(1)SU2 にアップグレードする場合、新しい SQL サーバーデータベースを作成して、それを新しいデータベースに移行する必要があります。 これは、このリリースで強化されたデータ型のサポートに必要です。 データベースを移行しない場合、既存の SQL サーバーデータベースでスキーマ検証が失敗し、常設チャットなどの外部データベースに依存するサービスは起動しません。

IM および Presence サービスをアップグレードしたら、この手順を使用して新しい SQL Server データベースを作成し、新しいデータベースにデータを移行します。

（注） この移行は、Oracle または PostgreSQL 外部データベースには必要ありません。

事前準備

データベースの移行は、`MSSQL_migrate_script.sql` スクリプトに依存します。 Cisco TAC に連絡してコピーを入手してください。

表 *7:*

ステップ	タスク
ステップ 1	外部 Microsoft SQL Server データベースのスナップショットを作成します。
ステップ 2	新しい (空の) SQL Server データベースを作成します。 詳細については、『IM and Presence サービス用データベースセットアップガイド』の次の章を参照してください: **1.** 「Microsoft SQL のインストールとセットアップ」—アップグレードされた IM およびプレゼンスサービスに新しい SQL サーバデータベースを作成する方法の詳細については、この章を参照してください。 **2.** 「IM and Presence サービスの外部データベースのセットアップ」—新しいデータベースが作成されたら、この章を参照して、IM and Presence サービスの外部データベースとしてデータベースを追加します。

ステップ	タスク
ステップ 3	システム トラブルシューティングを実行して、新しいデータベースにエラーがないことを確認します。 **1.** Cisco Unified CM IM and Presence Administration から、**[診断]** > **[システム トラブルシュータ]** の順に選択します。 **2.** [**外部データベースのトラブルシューティング**] セクションにエラーが表示されないことを確認します。
ステップ 4	すべての IM and Presence サービス クラスタ ノードで Cisco XCP Router を再起動します。 **1.** [Cisco Unified IM and Presence のサービスアビリティ（Cisco Unified IM and Presence Serviceability）] から、**[ツール（Tools）]** > **[コントロールセンタ-ネットワークサービス（Control Center - Network Services）]** を選択します。 **2.** **[サーバー（Server）]** メニューで、IM and Presence サービスを選択して、**[移動（Go）]** をクリックします。 **3.** **[IM and Presenceサービス（IM and Presence Services）]** の下で、**[Cisco XCPルータ（Cisco XCP Router）]** を選択し、**[リスタート(Restart)]** をクリックします
ステップ 5	外部データベースに依存するサービスをオフにする: **1.** [Cisco Unified IM and Presenceのサービスアビリティ（Cisco Unified IM and Presence Serviceability）] から、**[ツール（Tools）]** > **[コントロールセンター-機能サービス（Control Center - Feature Services）]** を選択します。 **2.** **[サーバー（Server）]** メニューで、IM and Presence ノードを選択して、**[移動（Go）]** をクリックします。 **3.** **[IM and Presenceサービス（IM and Presence Services）]** で、次のサービスを選択します。 Cisco XCP Text Conference Manager Cisco XCP ファイル転送マネージャ Cisco XCP Message Archiver **4.** [Stop] をクリックします。
ステップ 6	次のスクリプトを実行して、古いデータベースから新しいデータベース `MSSQL_migrate_script.sql` にデータを移行します。 （**注**） Cisco TAC に連絡してこのスクリプトのコピーを入手してください

ステップ	タスク
ステップ 7	システム トラブルシューティングを実行して、新しいデータベースにエラーがないことを確認します。 **1.** Cisco Unified CM IM and Presence Administration から、**[診断（Diagnostics）]**>**[システムトラブルシュータ（System Troubleshooter）]** を選択します。 **2.** **外部データベースのトラブルシューティング** セクションにエラーが表示されないことを確認します。
ステップ 8	前に停止したサービスを開始します。 **1.** [Cisco Unified IM and Presenceのサービスアビリティ（Cisco Unified IM and Presence Serviceability）] から、**[ツール（Tools）]**>**[コントロールセンター-機能サービス（Control Center - Feature Services）]** を選択します。 **2.** **[サーバー（Server）]** メニューで、IM and Presence ノードを選択して、**[移動（Go）]** をクリックします。 **3.** [**IM およびプレゼンスサービス**] から次のサービスを選択します: Cisco XCP Text Conference Manager Cisco XCP ファイル転送マネージャ Cisco XCP Message Archiver **4.** [開始] をクリックします。
ステップ 9	外部データベースが実行中で、Cisco Jabber クライアントからすべてのチャットルームが表示されていることを確認します。 新しいデータベースが機能していることを確認してから、古いデータベースを削除してください。

FIPS モードでのアップグレードの考慮事項

Unified Communications Manager リリース 12.5 SU1 で FIPS モードを有効にすると、小さい方のキーサイズの IPsec DH グループ 1、2、または 5 が無効になります。 DH グループ 1、2 または 5 ですでに IPSec ポリシーを設定しており、FIPS モードを有効にしている場合、Unified Communications Manager リリース 12.5 SU1 へのアップグレードはブロックされます。

Unified Communications Manager リリース 12.5 SU1 にアップグレードする前に、以下のいずれかの手順を実行します。

- 構成済みの IPsec ポリシーを削除し、アップグレードを実行します。 アップグレードが完了したら、DH グループ 14–18 で IPsec ポリシーを再構成します。
- DH グループ 14-18 をサポートする COP ファイル (latest_version.xxxx.cop.sgn) をインストールし、IPsec ポリシーを再設定してからアップグレードを実行します。

Unified Communications Manager リリース 15 で FIPS モードを有効にすると、IPSec 通信で 3DES アルゴリズムがサポートされなくなります。 すでに ESP および暗号化アルゴリズムを 3DES として IPSec ポリシーを設定しており、FIPS モードを有効にしている場合、Unified Communications Manager リリース 15 へのアップグレードはブロックされます。

（注） COP ファイルのインストール後に FIPS モードを無効にすると、IPSEC 設定ページは表示されません。

（注） リリース 15 へのアップグレードまたは移行を計画している場合、FIPS モードでは 3DES アルゴリズムの IPSec ポリシーはサポートされていないことに注意してください。 両方のノードで、暗号化と 3DES 以外の ESP アルゴリズムを使用する IPSec ポリシーを削除して再作成し、IPSec トンネルを確立するためのアップグレードまたは移行を計画する必要があります。

IPSec ポリシーの設定についての詳細は、 *Cisco Unified* オペレーティングシステムの管理オンラインヘルプを参照してください。

IPSec の要件

証明書ベースの認証で IPSec を構成している場合、IPSec ポリシーで CA 署名付き証明書を使用していることを確認してください。 自己署名証明書による証明書ベースの認証を使用するように設定された IPsec で Unified Communications Manager をアップグレードしようとすると、アップグレードは失敗します。 CA 署名付き証明書を使用するには、IPsec ポリシーを再設定する必要があります。

（注） 移行を開始する前に、クラスターのすべてのノードで IPsec ポリシーを無効にします。

クラスタ間ピアのサポート

IM and Presence Service は、異なるソフトウェアのバージョンを実行しているクラスタへのクラスタ間ピアをサポートします。サポートされているドメイン間フェデレーションを確認するには、 Cisco Unified Communications Manager と IM and Presence サービスの互換性マトリックスの「クラスタ間ピアリングのサポート」を参照してください。

アップグレード中の Spectre/Meltdown の脆弱性

Unified Communications Manager、Cisco IM and Presence Service、Cisco Emergency Responder、Cisco Prime Collaboration Deployment のリリースには、Meltdown および Spectre マイクロプロセッサの脆弱性に対処するソフトウェア パッチが含まれています。

リリース 12.5 (1) 以降にアップグレードする前に、チャネル パートナーまたはアカウント チームと協力して、Cisco Collaboration サイジング ツールを使用して、現在の展開とアップグレー

ドした展開を比較することをお勧めします。 必要に応じて VM リソースを変更し、アップグレードした展開で最高のパフォーマンスが得られるようにします。

10.5(2) からのアップグレードと移行を壊す重複する ENUMS

リリース 10.5 (2) または 11.0 (1) から新しいリリースに直接アップグレードまたは直接移行する場合、古いロケールのインストールに問題があり、アップグレードと移行が失敗します。この問題は、次の Unified CM 結合ネットワーク ロケールのいずれかがインストールされている場合に発生します。

- cm-locale-combined_network-9.1.2.1100-1
- cm-locale-combined_network-10.5.2.2200-1
- cm-locale-combined_network-11.0.1.1000-1

この問題は、次の Unified CM ロケールが同じクラスタに同時にインストールされている場合にも発生する可能性があります。

- cm-locale-en_GB-9.1.2.1100-1
- cm-locale-pt_BR-9.1.2.1100-1
- cm-locale-en_GB-10.5.2.2200-1
- cm-locale-pt_BR-10.5.2.2200-1
- cm-locale-en_GB-11.0.1.1000-1
- cm-locale-pt_BR-11.0.1.1000-1

アップグレードが失敗しないようにするには、Unified Communications Manager と電話機のロケールのインストールを更新して、2017 年 8 月 31 日より後の日付のロケールを使用してください。この問題は、2017 年 8 月 31 日以降に発行されたロケールファイルには存在しないためです。 ロケールのインストールを更新したら、アップグレードまたは移行を開始できます。ワークロードの詳細については、「https://bst.cloudapps.cisco.com/bugsearch/bug/CSCuz97687」を参照してください。

ライセンス要件

以下のセクションでは、Unified Communications Manager および IM and Presence サービスのライセンス要件に関する情報を提供します。

スマート ソフトウェア ライセンシングの概要

Ciscoスマート ソフトウェア ライセンシングは、ライセンスに関する新しい考え方を提供しています。 ライセンスの柔軟性が増し、企業全体のライセンスがシンプルになります。 また、ライセンスの所有権および消費が可視化されます。

Ciscoスマート ソフトウェア ライセンシングを使用すると、デバイスが自己登録し、ライセンス消費を報告し、製品アクティベーション キー（PAK）が必要なくなり、ライセンスの調達、

展開、管理が簡単にできるようになります。 ライセンス資格を単一のアカウントにプールして、必要に応じてネットワーク経由でライセンスを自由に移動することができます。 Cisco製品全体で有効化され、直接クラウドベースまたは間接導入モデルによって管理されます。

Cisco スマート ソフトウェア ライセンシング サービスでは、製品インスタンスを登録し、ライセンスの使用状況を報告し、Cisco Smart Software Manager または Cisco Smart Software Manager サテライトから必要な認証を取得します。

スマート ライセンシングでは次のことを実行できます。

- ライセンスの使用状況とライセンス数の表示
- 各ライセンス タイプのステータスの表示
- Cisco Smart Software Manager または Cisco Smart Software Manager サテライトによる利用可能な製品ライセンスの表示
- Cisco Smart Software Manager または Cisco Smart Software Manager サテライトによるライセンス認証の更新
- ライセンス登録の更新
- Cisco Smart Software Manager または Cisco Smart Software Manager サテライトによる登録解除

（注） ライセンス認証は 90 日間有効で、更新は 30 日に 1 回以上行われます。 Cisco Smart Software Manager または Cisco Smart Software Manager サテライトに接続しないと、認証の期限は 90 日後に切れます。

Cisco Smart Software Manager サテライトのオプションを選択する場合、このサテライトが認証を行うために、Cisco Smart Software Manager へのインターネット接続が必要になります。 Cisco Smart Software Manager サテライトは、接続時間が設定可能な接続済みモードと、手動同期が必要な切断モードの 2 つのモードで動作できます。

スマート ライセンシングの導入オプションには、主に次の 2 つがあります。

- Cisco Smart Software Manager
- Cisco Smart Software Manager サテライト

Cisco Smart Software Manager

Cisco Smart Software Manager は、システムのライセンスを処理するクラウドベースのサービスです。 Unified Communications Manager が直接またはプロキシ サーバ経由で、cisco.com に接続できる場合に、このオプションを使用します。 Cisco Smart Software Manager によって、次のことを行うことができます。

- ライセンスの管理およびトラック
- バーチャル アカウント間でのライセンスの移動

- 登録済みの製品インスタンスの削除

オプションで、Unified Communications Manager が直接 Cisco Smart Software Manager に接続できない場合、接続を管理するプロキシ サーバを導入することができます。

（注） Cisco スマート ソフトウェア マネージャに登録されている Unified Communications Manager を 15 より前のリリースからリリース 15 以降にアップグレードする場合、Cisco Unified Communications Manager は製品インスタンスの Cisco スマート ソフトウェア マネージャ UI で製品バージョンを 15 に更新しません。 詳細については、CSCwf94088 を参照してください。

Cisco Smart Software Manager の詳細については、https://software.cisco.com に進みます。

Cisco Smart Software Manager サテライト

Cisco Smart Software Manager サテライトは、セキュリティ上または可用性上の理由で、Unified Communications Manager が直接 cisco.com に接続できない場合に、ライセンスのニーズを処理できるオンプレミス導入です。 このオプションを導入すると、Unified Communications Manager は、ライセンスの使用を登録し、サテライトに報告します。この際、cisco.com でホストされているバックエンドの Cisco Smart Software Managerとそのデータベースを定期的に同期します。

サテライトが cisco.com に直接接続できるかどうかに応じて、Cisco Smart Software Manager サテライトを接続または切断のいずれかのモードで導入できます。

- 接続（Connected）：Smart Software Manager サテライトから cisco.com への直接の接続がある場合に使用されます。 スマート アカウントの同期が自動的に実行されます。
- 切断（Disconnected）：Smart Software Manager サテライトから cisco.com への接続がない場合に使用されます。 Smart Account の同期を手動でアップロードおよびダウンロードする必要があります。

（注） デュアルスタックモードで実行される Unified CM は、IPv4 アドレスと IPv6 アドレスを使用して設定されたサテライトをサポートします。

（注） Cisco スマート ソフトウェア マネージャ サテライトに登録されている Unified Communications Manager を 15 より前のリリースからリリース 15 以降にアップグレードする場合、Cisco Unified Communications Manager は製品インスタンスの Cisco スマート ソフトウェア マネージャ UI で製品バージョンを 15 に更新しません。 詳細については、CSCwf94088 を参照してください。

Cisco Smart Software Manager サテライトの情報およびドキュメントについては、https://www.cisco.com/c/en/us/buy/smart-accounts/software-manager-satellite.html に進みます。

ライセンスタイプ

ニーズをカバーするために、次のライセンス タイプを使用できます。

Cisco Unified Workspace Licensing

Cisco Unified Workspace Licensing（UWL）は、シスコ コラボレーション アプリケーションおよびサービスの最も一般的なバンドルをコスト効率の高いシンプルなパッケージで提供します。 このパッケージには、ソフト クライアント、アプリケーション サーバ ソフトウェア、およびユーザごとのライセンスが含まれています。

Cisco User Connect Licensing

User Connect Licensing（UCL）は、個々の Cisco Unified Communications アプリケーションに対するユーザベースのライセンスで、アプリケーション サーバ ソフトウェア、ユーザ ライセンス、ソフト クライアントが含まれています。 UCL は、必要なデバイスのタイプとデバイスの数に応じて、Essential、Basic、Enhanced、Enhanced Plus の各バージョンから選択できます。

これらのライセンス タイプと使用可能なバージョンの詳細については、「http://www.cisco.com/c/en/us/products/unified-communications/unified-communications-licensing/index.html」を参照してください。

Session Management Edition

Session Management Edition は、Cisco Smart Software Manager または Cisco Smart Software Manager サテライトのいずれかに登録できます。 Unified Communications Manager と同じプロセスを使用して Session Management Edition を登録し、Cisco Unified Communications Manager が登録されている仮想アカウントまたは別の仮想アカウントに登録し、最小限のライセンス要件を満たすことができます。

（注） 特定ライセンス予約 (SDSL) に登録された SME には、SDSL 承認コードの生成中に CSSM に予約された最小ライセンス セットが必要です。

製品インスタンスの評価モード

Unified Communications Manager は、インストール後 90 日間は評価期間として実行されます。評価期間が終了すると、Cisco Smart Software Manager または Cisco Smart Software Manager サテライトに登録されるまで、Unified Communications Manager で新規ユーザや新規端末の追加ができなくなります。

（注） 製品が登録されると評価期間は終了します。

特定のライセンスの予約

Specific License Reservation（SLR）を使用すると、お客様は、仮想アカウントからライセンスを予約でき、それをデバイス UDI と関連付け、オフラインモードで予約済みライセンス付き

デバイスを使用できます。 この場合、バーチャル アカウントから UDI 用の特定ライセンスと数量を予約します。 以下のオプションは、特定予約向けの新機能および設計要素の説明です。

表 *8*: 特定ライセンス予約コマンド

コマンド	説明
license smart reservation enable	このコマンドを使用してライセンスの予約機能を有効にします。
license smart reservation disable	ライセンスの予約機能を無効にするには、このコマンドを使用します。
license smart reservation request	このコマンドを使用して予約リクエストコードを生成します。
license smart reservation cancel	承認コードがインストールされる前にこのコマンドを使って予約プロセスをキャンセルします。
license smart reservation install "<authorization-code>"	このコマンドを使用して、Cisco Smart Software Manager で生成されたライセンス予約認証コードをインストールします。
license smart reservation return	このコマンドを使用して、インストールされているライセンス予約認証コードおよび予約された権利のリストを削除します。デバイスは未登録の状態に戻ります。
license smart reservation return-authorization "<authorization code>"	このコマンドを使用して、ユーザが入力したライセンス予約認証コードを削除します。

（注） 12.0から上位バージョンにアップグレードし、アップグレードしたサーバーでライセンス予約機能を有効にする場合は、予約機能を有効にする前に、CCO から `ciscocm-ucm-resetudi.k3.cop.sgn` をダウンロードして、アップグレードされた CUCM にインストールする必要があります。

（注） ライセンス予約が有効になっている 12.5 システムを 14 にアップグレードする場合は、「Cisco Unified Communications Manager システム設定ガイド」を参照してください。

IM および Presence サービス ライセンス要件

IM and Presence Service には、サーバーライセンスまたはソフトウェア バージョン ライセンスは不要です。 ただし、ユーザを割り当て、割り当てられた各ユーザに対して IM and Presence Service を有効にする必要があります。

（注） Jabber for Everyone では、IM およびプレゼンスサービス機能を有効にするために、エンドユーザーライセンスは必要ありません。 詳細については、「Jabber for Everyone 向けクイックスタートガイド」を参照してください。

各ユーザーに関連付けたクライアントの数に関係なく、ユーザーごとに IM and Presence Service を割り当てることができます。 IM and Presence Service をユーザーに割り当てると、そのユーザーは IM や空き状況の更新を送受信できるようになります。 IM and Presence Serviceが有効になっていない場合、ユーザーは IM and Presence Service サーバーにログインして他のユーザーの空き状況を表示したり、IM の送受信を行うことができません。また、他のユーザーは彼らの空き状況を確認することができません。

次のいずれかのオプションを使用して、ユーザを IM and Presence Service 有効にできます:

- **[エンドユーザー設定（End User Configuration）]** ウィンドウは、Unified Communications Manager にあります。 詳細については、『Administration Guide for Cisco Unified Communications Manager』を参照してください。
- 一括管理ツール (BAT)
- IM and Presence Service を、Unified Communications Manager の **[クイックユーザー/電話追加（Quick User/Phone Add）]** ウィンドウから参照できる機能グループテンプレートに割り当てます。

詳細については、Cisco Unified Communications Manager システム設定ガイドを参照してください。

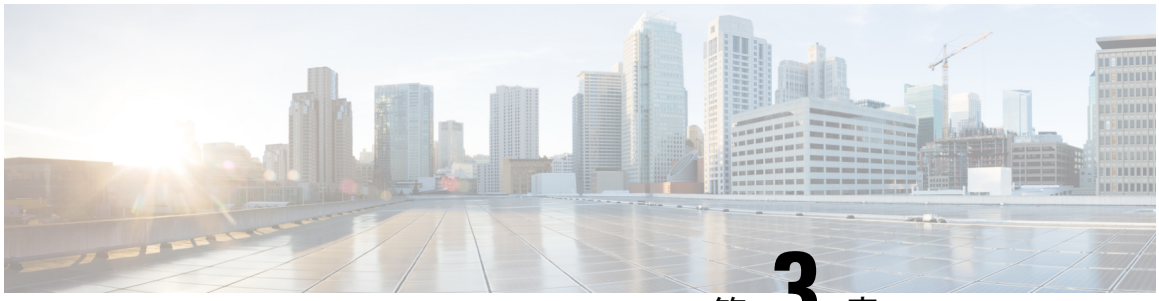
IM and Presence Service 機能には、User Connect Licensing（UCL）と Cisco Unified Workspace Licensing（CUWL）の両方が含まれます。IM and Presence Service 機能は、Unified Communications Manager IP テレフォニーユーザーでないユーザーも、Jabber for Everyone のオファーで取得できます。 詳細については、「Jabber for Everyone 向けクイックスタートガイド」を参照してください。

サポートドキュメンテーション

以下のドキュメントには、特定のケースでアップグレードするのに役立つ追加のサポート情報が含まれています。

タスク	
仮想Ciscoハードウェアをセットアップします。	仮想プラットフォームをセットアップする方法については、「仮想サーバー上の *Cisco Collaboration*」を参照してください。 詳細については、https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-guides-list.htmlを参照してください。

タスク	
Cisco Business Edition 6000/7000 アプライアンスのセットアップ	参照先: • *Cisco Business Edition 6000* および *7000* の設置ガイド—https://www.cisco.com/c/en/us/support/unified-communications/business-edition-6000/tsd-products-support-series-home.html • *Cisco Business Edition 6000* および *7000* の設置ガイド—https://www.cisco.com/c/en/us/support/unified-communications/business-edition-7000/tsd-products-support-series-home.html
設定を維持しながら既存のハードウェアを置き換え	https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-guides-list.html の *Cisco Unified Communications Manager* の単一サーバーまたはクラスタを交換する
VMware の要件を確認する	VMware の要件とベストプラクティスについては、https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/cisco-collaboration-virtualization.html を参照してください。 VMware ベンダーのドキュメントについては、http://www.VMware.com を参照してください。
プランニングとサイジングに関するその他のリソース	これらのドキュメントには、アップグレードしたシステムの計画とサイズ設定に役立つ情報も含まれています。 • http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-system/products-implementation-design-guides-list.html の *Cisco Collaboration Systems Solution Reference Network Designs*（*SRND*） • http://www.cisco.com/c/en/us/solutions/enterprise/design-zone-collaboration/index.html の *Cisco* 推奨アーキテクチャガイドおよび*Cisco* 検証済み設計ガイド。 • http://ucs.cloudapps.cisco.com/ の Collaboration Virtual Machine Replacement ツール。 • http://www.cisco.com/go/quotecollab の Cisco Quote Collab ツール。 • http://tools.cisco.com/cucst の Cisco Collaboration Sizing ツール。



第 3 章

アップグレードタスク

アップグレードの概要

Cisco Unified OS 管理 GUI または CLI のいずれかを使用して、以下のアップグレードタイプのいずれかを完了するには、この章の手順を使用します。 手順については、アップグレードタイプに対応するタスクフローを参照してください。

- クラスタ全体のアップグレード（直接標準）—アップグレード前のバージョンが最低12.5 (1) である必要があります。 そうでない場合は、もう一方の方法を使用する必要があります。
- クラスタノードのアップグレード（直接標準）

（注） pre-12.5 ソースから Release 15 への直接アップグレードはサポートされていません。

（注） Unified Communications Manager パブリッシャノードがリリース 15 で、サブスクライバノードがリリース 12.5.x または 14、および SU である場合、クラスタのノードは認証されません。 サブスクライバー ノードがリリース 15 にアップグレードされた場合にのみ、すべてのノードが認証済み状態になります。

（注） Cisco Prime Collaboration Deployment を使用するアップグレードと移行については、『Cisco Prime Collaboration Deployment 管理ガイド』を参照して、アップグレードタスクまたは移行タスクを設定してください。

事前準備

注意 すべての構成タスクを停止します。 アップグレード中は設定の変更を行わないでください。 たとえば、パスワードの変更、LDAP 同期の実行、自動ジョブの実行は行わないでください。 アップグレードプロセス中にクラスター内のノードを削除、再追加、または再インストールしないでください。 すべてのノードでアップグレードを完了し、アップグレード後のタスクを完了した場合にのみ、構成の変更を行うことができます。 アップグレードは、アップグレード中に行った構成の変更を上書きします。構成の変更によっては、アップグレードが失敗する場合があります。

LDAP とのユーザ同期を一時停止することをお勧めします。 すべての Unified Communications Manager および IM and Presence Service クラスタノードのアップグレードが完了するまでは同期を再開しないでください。

- アップグレードファイルの名前を変更したり圧縮したりしないでください。 そうしないと、システムはファイルを有効なアップグレードファイルとして拒否します。
- IM and Presence サービスをアップグレードする場合、ユーザーの連絡先リストのサイズが最大値を下回っているか確認します。 Cisco Unified CM IM and Presence Administration のシステム トラブルシューティングを使用して、制限を超えるユーザーがいないことを確認します。
- アップグレード プロセスの前に、ネットワーク アダプタを VMXNET3 に変更します。 詳細については、OVA の readme ファイルを参照してください。
- FIPS モードのノードをアップグレードする場合、セキュリティ パスワードが 14 文字以上であることを確認してください。 パスワードを変更するには、『はじめに』の章の「管理者パスワードまたはセキュリティ パスワードのリセット」を参照してください『Administration Guide for Cisco Unified Communications Manager』。

（注） リリース 12.5 (1) SU2 以降、同じメンテナンスウィンドウ中に両方のアップグレード段階 [バージョンのインストールと切り替え] を実行して、他の AXL 依存型インテグレーションへの影響を回避することをお勧めします。

（注） バージョンを切り替える間、動的テーブル (numplandynamic、devicedynamic など) のユーザ向け機能 (UFF) のみが更新されます。 他のテーブルはアップグレード中に移行されます。 アップグレード後、またはバージョンを切り替える前の設定の変更は失われます。

（注） アップグレードログでは、特定の間隔で時間の不一致または時間のジャンプが観察されます。ハードウェアの時計はシステムが NTP サーバと同期するまで無効になっているため、この時間のジャンプは予期された動作です。

（注） アクティブなバージョンと非アクティブなバージョンで異なるセキュリティパスワードを使用し、下位のバージョンに切り替えるときに、下位のバージョンのセキュリティパスワードが上位バージョンと同じになるように変更してください。 これらの手順に従ってセキュリティパスワードを変更します:

1. パブリッシャノードを下位のバージョンに切り替えてください。
2. パブリッシャノードのセキュリティパスワードを上位バージョンと同じ新しいパスワードに変更します。
3. サブスクライバーを下位のバージョンに切り替えてください。
4. サブスクライバノードのセキュリティパスワードを上位バージョンと同じ新しいパスワードに変更します。

（注） リリース 15 にアップグレードする前に、この手順を使用して NTP 設定を確認します。

1. 信頼できるソースからのオフセットと jitter が小さい NTP ソースを常に使用するように確認してください。
2. 時刻同期用に設定された 1 つの良好な NTP サーバを用意することを推奨します。 複数の NTP サーバーを設定する場合、各クロックが異なるタイムゾーンを指している場合に chrony がタイブレーカーを持つことができるように、少なくとも 4 つの NTP サーバーを設定してください。
3. Cisco 音声オペレーティングシステム (VOS) サーバによってサポートされる互換性のあるバージョンに一致するように、常に ESXi をアップグレードする必要があります。
4. 異なる主催者間のネットワーク移行の間、信頼できるクロックで同じ NTP ソース（または）NTP ソースを使用するように確認してください。

アップグレードファイルのダウンロード

アップグレードする前に、必要なファイルをダウンロードします。

（注） アップグレードを最適化するために、ダウンロードしたファイルを同じディレクトリに保存してください。

表 *9:* ダウンロードするアップグレードファイル

ダウンロードするファイル	ダウンロード サイト
Unified CM アップグレード ISO	[Unified Communications Managerダウンロード（Unified Communications Manager Downloads）] に移動します。—お使いのバージョンを選択し、**[Unified Communications Managerを更新（Unified Communications Manager Updates）]** で ISO のアップグレードを検索します。 例: `UCSInstall_UCOS_<XXXXXXXX>.sha512.iso`
IM および Presence サービスアップグレード ISO	[IM and Presenceサービスのダウンロード（IM and Presence Service Downloads）] に移動します。—お使いのバージョンを選択し、[Unified Presence Server（CUP）更新（Unified Presence Server (CUP) updates）] で ISO のアップグレードを検索します。 例: `UCSInstall_CUP_<XXXXXXXX>.sha512.iso`
アップグレードの準備 COP ファイル (アップグレード前およびアップグレード後)	アップグレード前の COP ファイルおよびアップグレード後の COP ファイルは、上記のいずれかのダウンロードサイトからダウンロードできます。 • Unified CM の場合、COP ファイルは **Unified Communications Manager の更新の下に表示されます。** • IM and Presence サービスの場合、COP ファイルは、**[Unified Presence Server（CUP）更新（Unified Presence Server (CUP) updates）] > [UTILS]** で表示されます。 たとえば、 `ciscocm.preUpgradeCheck-XXXXX.cop.sgn` および `ciscocm.postUpgradeCheck-XXXXX.cop.sgn` などです。 （注） COP ファイルを使用してアップグレードしようとすると、システムにインストールされているファイル数が表示されます。アップグレードが完了すると、COP ファイルのリストは以前のバージョンと一致しなくなります。 以前のファイルが必要な場合は、COP ファイルを手動でインストールする必要があります。

クラスタ全体のアップグレードタスクフロー(直接、標準)

簡素化されたクラスタ全体のアップグレードを完了するには、以下のタスクを実行します。これにより、クラスタ全体の直接標準アップグレードが完了します。

（注） クラスター全体のアップグレード オプションは、アップグレード前バージョンが 12.5 (1) の最小リリースである直接の標準アップグレードでのみ利用できます。

（注） アップグレードプロセスを開始する前に、各ノードのソフトウェアの場所の詳細を確認してください。

始める前に

アップグレード ISO ファイルと Upgrade Readiness COP ファイルをダウンロードし、同じディレクトリに保存します。ダウンロード情報については、アップグレードファイルのダウンロード （52 ページ） に移動してください。

手順

	コマンドまたはアクション	目的
ステップ 1	Upgrade Readiness COP ファイルの実行（アップグレード前） （54 ページ）	Upgrade Readiness COP ファイルを実行して、システムの接続性と正常性を確認します。 問題がある場合は、アップグレードを進める前に修正してください。
ステップ 2	クラスタ全体の再起動シーケンスを設定する （56 ページ）	ダウンタイムを最小限に抑えるために、再起動シーケンスを事前に指定します。
ステップ 3	クラスター ソフトウェアの場所の構成（57 ページ）	アップグレードの前に、クラスター内で関連付けられたすべてのノードに対して、クラスター ソフトウェアのロケーションの詳細を構成することを選択できます。
ステップ 4	以下のいずれかの方法でクラスターをアップグレードします。	アップグレード中に、バージョンを自動的に切り替えることができます。または、アップグレードされたバージョンを

	コマンドまたはアクション	目的
	• OS Admin からのクラスタ全体のアップグレードの完了 （58 ページ） • CLI による完全なクラスタ全体のアップグレード （59 ページ）	非アクティブパーティションに保存することができます。
ステップ 5	手動でバージョンを切り替える (クラスター全体) （61 ページ）	これはオプションです。 アップグレード中にバージョンを自動的に切り替えないように選択した場合、手動でバージョンを切り替えます。
ステップ 6	アップグレードの準備 COP ファイルの実行 (アップグレード後) （62 ページ）	post-upgrade COP ファイルを実行して、システムのアップグレード後の正常性を評価します。

Upgrade Readiness COP ファイルの実行（アップグレード前）

アップグレードの準備 COP ファイルは次の項目をチェックします。

- インストールされた COP ファイル
- ネットワーク サービスと接続 (DNS、NTP、クラスター内)
- ライセンスの同期
- VMware ツールの互換性
- ハードディスクパーティションサイズ
- スワップサイズチェック
- ファイルシステムタイプとゲスト OS のチェック
- 宛先バージョンに使用可能なディスク容量
- ESXi バージョン確認
- SIP および H.323 トランク登録
- データベース認証およびレプリケーションの状況
- データベースの健全性
- 最後の DRS バックアップの状況
- リモート通話コントロール (RCC) 機能の状況
- サービス状況
- インストールされている COP とロケール

- デバイス登録状態数
- エンタープライズ パラメータとサービス パラメータの設定
- TFTP 最大サービス数
- アクティブおよび非アクティブ バージョン
- 期限切れの証明書を一覧表示する
- FIPS モードのパスワードの長さの制限
- FIPS モードでの ESP および暗号化アルゴリズムの IPSec ポリシー設定確認

（注）
- アップグレードが失敗する可能性を大幅に減らすため、アップグレード前にアップグレードの準備 COP ファイルを実行することを強くお勧めします。
- COP ファイルはアップグレード前のバージョンが 10.x 以降の場合に完全にサポートされます。
- 3DES アルゴリズムは FIPS モードではサポートされていないため、3DES アルゴリズムを含む IPSec ポリシーを削除し、IPSec トンネルが確立される両方のノードで、3DES 以外の暗号化および ESP アルゴリズムを含む IPSec ポリシーを再作成する必要があります。

手順

ステップ 1 アップグレード準備COPファイルをダウンロードしてアップグレード前テストを実行します。
a) ダウンロード サイトに移動します。
b) 移動先のリリースを選択し、**[Unified Communications Manager ユーティリティ] を選択します。**
c) **アップグレード前テストを実行するために Upgrade Readiness COP ファイル**をダウンロードします（たとえば、`ciscocm.preUpgradeCheck-00019.cop.sgn`）。 最新のファイルは別のファイル名とバージョンを持つ場合があることに注意してください)。

ステップ 2 アップグレードに対してシステムの準備ができているか確認します。
a) COP ファイルを実行します。
b) COP ファイルが返す問題を解決します。
c) COP ファイルを再度実行します。
d) COP ファイルがエラーを返さなくなるまで、このプロセスを繰り返します。

ステップ 3 GUI または CLI から cop ファイルをインストールします。 インストールが完了したら、CLI から **file view install PreUpgradeReport.txt** を実行してレポートを表示します。

ステップ 4 RTMT からレポートを表示するには
a) RTMT にログインします。

b) **[Trace and Log Central]** で、**[リモートブラウザ（Remote Browse）]** をダブルクリックし、**[トレースファイル（Trace files）]** を選択したら、**[次へ（Next）]** をクリックします。
c) **[すべてのサーバー上のすべてのサービス（Select all Services on all servers）]** を選択して、**[次へ（Next）]** をクリックします。
d) **[完了（Finish）]**> **[閉じる（Close）]** の順に選択します。
e) ノードをダブルクリックして、**[CUCMパブリッシャ（CUCM Publisher）]** > **[システム（System）]** > **[アップグレードログのインストール（Install upgrade Logs）]** の順にします。
f) **[インストール（Install）]** をダブルクリックして、ダウンロードする必要なファイルを選択します。

クラスタ全体の再起動シーケンスを設定する

簡素化されたクラスタ全体のアップグレードの場合、アップグレードする前にこの手順を使用して、クラスタアップグレードの再起動シーケンスを設定します。 このオプションはアップグレード前のバージョンが 12.5(1) 以上の場合にのみ利用できます。

（注） 再起動シーケンスを構成しない場合、クラスター全体のアップグレードは、最後に保存された再起動シーケンスまたはデフォルトのシーケンスを使用します。

手順

ステップ 1 パブリッシャノードで、Cisco Unified OS Administration または Cisco Unified CM IM and Presence OS Administration にログインします。

ステップ 2 **[ソフトウェアアップグレード（Software Upgrades）]** > **[再起動/バージョン クラスタの切り替え（Restart/Switch-Version Cluster）]** の順に選択します。
[クラスタ設定を再起動] ウィンドウが表示されます。スライダには各ノードの再起動の順番を示します。

ステップ 3 スライダーを使用して、必要に応じて再起動の順序を調整します。

ステップ 4 **[保存（Save）]** をクリックします。

次のタスク

使用するインターフェイスに応じて、以下のいずれかのタスクを実行します。

- OS Admin からのクラスタ全体のアップグレードの完了 （58 ページ）
- CLI による完全なクラスタ全体のアップグレード （59 ページ）

クラスター ソフトウェアの場所の構成

この手順を使用して、同じクラスター内のノードの既存の構成を追加、編集、または変更します。

（注） この機能は、クラスタ内のすべてのノードが Release 14SU2 以降である場合にのみ使用できます。

手順

ステップ 1 **Cisco Unified OS Administration** ユーザーインターフェイスにログインします。

ステップ 2 **[ソフトウェアアップグレード（Software Upgrades）]>[クラスタソフトウェアの場所（Cluster Software Location）]** の順に選択します。

ステップ 3 追加するノードを選択するか、リストからサーバ ロケーションの詳細を編集します。

ステップ 4 パブリッシャを含むクラスタ内の他のすべてのノードに同じソフトウェアロケーションの詳細を適用する場合は、 **[すべてのノードに適用する**] チェックボックスを選択します。

このチェックボックスは、**[ノードを選択（Select Node）]** ドロップダウンメニューで [Unified CMパブリッシャ（Unified CM publisher）] を選択した場合のみ表示されます。

ステップ 5 パブリッシャノードのソース設定とソフトウェアロケーション詳細を使用する場合は、**[パブリッシャからのダウンロード資格情報とソフトウェアロケーションを使用する]** チェックボックスを使用します。

発行元からのダウンロード資格情報とソフトウェアの場所を使用する オプションがデフォルトで選択されています。

（注） このオプションはサブスクライバノードでのみ利用できます。

ステップ 6 （オプション）**[パブリッシャからのダウンロード資格情報とソフトウェアロケーションを使用する（Use download credentials and software location from Publisher）]** オプションを使用しない場合は、サーバーをアップグレードする前に、**[以下のダウンロード資格情報とソフトウェアロケーションを使用する（Use below download credentials and software location）]** を使用します。

（注） このオプションはサブスクライバノードでのみ利用できます。

ステップ 7 **[ソース（Source）]** ドロップダウンメニューで、アップグレードファイルの保存先と一致するオプションを選択します。

- **DVD/CD**
- **ローカルファイルシステム**—このオプションは、キャンセルされた前回のアップグレードを再開する場合にのみ利用できます。

- **SFTP サーバ**: ディレクトリ、サーバアドレス、ログイン資格情報など、SFTP サーバの詳細を入力する必要があります。

ステップ 8 （オプション）アップグレード完了時にメール通知を受信するには、**SMTP サーバー**アドレスと**メールの宛先**を入力します。これにより、アップグレード完了時にメール通知を受信できます。

ステップ 9 アップグレードファイルのダウンロード後にアップグレードを自動的に開始する場合は、[**ダウンロード後にアップグレードを続行**] チェックボックスを選択します。 このチェックボックスをオンにしない場合、**[ソース（Source）]** と設定された **[ローカルファイルシステム（Local filesystem）]** を使用して後で、アップグレードを手動で開始する必要があります。

ステップ 10 **アップグレード後にサーバのバージョンを切り替える (ISO に対してのみ有効)** チェックボックスを選択すると、アップグレードが完了した後にシステムが自動的に再起動されます。

ステップ 11 **[保存（Save）]** をクリックして、追加または修正された特定のノードに対するすべての設定変更を更新します。

OS Admin からのクラスタ全体のアップグレードの完了

この手順を使用して、Unified Communications Manager および IM and Presence サービスの簡素化されたクラスタ全体のアップグレードを完了します。 このオプションは、アップグレード前のバージョンが 12.5 (1) 以降の標準アップグレードでのみ利用できます。

（注） また、`utils system upgrade cluster` CLI コマンドを実行しても、標準のクラスタ全体のアップグレードを完了できます。

始める前に

アクセス可能な場所にアップグレードファイルをダウンロードしていることを確認してください。

手順

ステップ 1 **Cisco Unified OS Administration** または **Cisco Unified IM and Presence OS Administration** にログインします。

ステップ 2 **[ソフトウェアアップグレード（Software Upgrades）]>[クラスタのインストール/アップグレード（Cluster Install/Upgrade）]** の順に選択します。 開始バージョンが 12.5 (1) より前の場合、このオプションは利用できません。

ステップ 3 既存のノードをアップグレードするために必要な以下の構成情報を表示することができます。

（注） リリース 14 SU2 以降では、すべてのクラスタノードの [ソフトウェアロケーション（Software Location）] 設定が、ローカルの各クラスタノードではなく、パブリッシャから一元的に管理されます。同じクラスタの任意のノードに対する既存の設定を追加、編集、修正する場合、Cisco Unified OS Administration ユーザーインターフェイスで、**[ソフトウェアアップグレード（Software Upgrades）] > [クラスタソフトウェアの場所（Cluster Software Location）]** の順に選択します。

- **資格情報—**アップグレードイメージが保存されているサーバの資格情報を表示します。
- **アップグレードファイルのソース**: アップグレードファイルが保存されているサーバの場所を表示します。 ローカルソース（CD または DVD）からアップグレードできます。また、FTP または SFTP を使用してリモートアップグレードファイルをダウンロードできます。また、キャンセル操作後にアップグレードを再開する場合は、ローカルイメージソースオプションを通じて以前にダウンロードしたアップグレードファイルを使用できます。
- **ダウンロード後にアップグレードを続行**: アップグレードファイルがダウンロードされたら、自動的にアップグレードを行うかどうかで選択されたオプションを示します (デフォルト値は「はい」です)。 自動アップグレードを選択した場合、チェックサムまたは SHA の詳細は表示されません。 [はい（Yes）] または [いいえ（No）] の値を設定していた場合は、その設定はシステムに残ります。
- **バージョン切り替え**: アップグレードが完了したら新しいバージョンに自動的に切り替えるかどうかを指定します (デフォルトでは「いいえ」)。 「yes」を入力した場合、システムは新しいバージョンに切り替わり、アップグレードの完了後に自動的にリブートします。 値を「はい」または「いいえ」に設定した場合、設定はシステムに残ります。

ステップ 4 [次へ（Next）] をクリックします。

ステップ 5 インストールするアップグレードバージョンを選択して、**[次へ]** をクリックします。
アップグレードが開始されます。**[インストールの状態（Installation Status）]** ページにアップグレードに関する情報が表示されます。

（注） クラスタ全体のアップグレード中、最初の 3 桁が選択した Unified Communications Manager と IM and Presence サービスのアップグレードファイルで共通であることを確認してください。

ステップ 6 アップグレードが完了したら **[完了]** をクリックします。
バージョンを自動的に切り替えることを選択した場合、クラスターはクラスターの再起動シーケンスに従って、アップグレードされたバージョンで再起動します。そうしないと、アップグレードは非アクティブパーティションに保存され、アップグレードされたソフトウェアを使用するために、バージョンを手動で切り替える必要があります。

CLI による完全なクラスタ全体のアップグレード

この手順を使用して、コマンドラインインターフェースを使用して簡素化されたクラスタ全体のアップグレードを完了します。

（注） このオプションは、アップグレード前のバージョンが 12.5(x) 以降の直接の標準アップグレードでのみ利用できます。

始める前に

クラスタ全体の再起動シーケンスを設定する（56 ページ）- アップグレード後に自動的にバージョンを切り替えたい場合は、再起動の順序を事前に設定します。 そうでない場合、クラスターは最後に保存されたシーケンスを使用して再起動します。 再起動シーケンスが保存されていない場合、デフォルトのシーケンスが使用されます。

（注） リリース 14 SU2 以降では、すべてのクラスタノードの [ソフトウェアロケーション（Software Location）]設定が、ローカルの各クラスタノードではなく、パブリッシャから一元的に管理されます。 システムのアップグレードを開始する前に、同じクラスタ内の任意のノードの既存の設定を追加、編集、または変更する場合は、Cisco Unified OS Administration ユーザーインターフェイスで、**[ソフトウェアアップグレード（Software Upgrades）] > [クラスタソフトウェアの場所（Cluster Software Location）]**メニューの順に選択します。

手順

ステップ 1 Unified CM パブリッシャノードのコマンド ライン インターフェイスにログインします。

ステップ 2 `utils system upgrade cluster` CLI コマンドを実行すると、ウィザードに、ソフトウェアの場所の詳細が表示され、同じクラスタ内のすべてのノードを設定します。

ステップ 3 既存のノードをアップグレードするために必要な以下の構成情報を表示することができます。

- **資格情報—**アップグレードイメージが保存されているサーバの資格情報を表示します。
- **アップグレードファイルのソース**: アップグレードファイルが保存されているサーバの場所を表示します。 ローカルソース（CD または DVD）からアップグレードできます。また、FTP または SFTP を使用してリモートアップグレードファイルをダウンロードできます。また、キャンセル操作後にアップグレードを再開する場合は、ローカルイメージソースオプションを通じて以前にダウンロードしたアップグレードファイルを使用できます。
- **ダウンロード後にアップグレードを続行**: アップグレードファイルがダウンロードされたら、自動的にアップグレードを行うかどうかで選択されたオプションを示します (デフォルト値は「はい」です)。 自動アップグレードを選択した場合、チェックサムまたは SHA の詳細は表示されません。 [はい（Yes）] または [いいえ（No）] の値を設定していた場合は、その設定はシステムに残ります。
- **バージョン切り替え**: アップグレードが完了したら新しいバージョンに自動的に切り替えるかどうかを指定します (デフォルトでは「いいえ」)。 「yes」を入力した場合、システムは新しいバージョンに切り替わり、アップグレードの完了後に自動的にリブートします。 値を「はい」または「いいえ」に設定した場合、設定はシステムに残ります。

ステップ 4 インストールを開始するように促されたら、「**はい**」と入力します。
アップグレード後に、バージョンの自動切り替えを選択した場合、アップグレード後に、クラスタがアップグレードされたバージョンで再起動します。そうでない場合、アップグレードは非アクティブパーティションに保存するため、後で手動でバージョンを切り替えることができます。

手動でバージョンを切り替える (クラスター全体)

直接標準アップグレードでは、他のノードで UI または CLI を使用する必要なく、Unified Communications Manager パブリッシャノード経由ですべてのクラスタノードで非アクティブとアクティブのバージョンを切り替える場合は、この手順を実行します。

（注） この手順は、次の場合にのみ使用できます。

- 直接標準アップグレード
- シンプルアップグレードを使用するクラスタ全体の自動化
- アップグレード前バージョン 12.5 (1) 以降

（注） 1 つ以上のクラスターノードが非アクティブバージョンのアップグレード、バージョンの再起動、およびデータベースのレプリケーションのうちの 1 つ以上で完了していないため、追加/更新/削除機能は許可されません。 Cisco Unified OS Administration UI から、**[ソフトウェアアップグレード（Software Upgrades）] > [インストール/アップグレード（Install/Upgrade）]** の順に選択するか、**[ソフトウェアアップグレード（Software Upgrades）]>[クラスタのインストール/アップグレード（Cluster Install/Upgrade）]** の順に選択して、アップグレード状態を表示します。 または、**utils system upgrade status** コマンドか **utils system cluster upgrade status** コマンドを実行して、アップグレード状態を監視します。 詳細については、アップグレードと移行の概要 （5 ページ）を参照してください。

手順

ステップ 1 Cisco Unified OS の管理または Cisco Unified CM IM and Presence OS の管理にログインします。

ステップ 2 **[ソフトウェアの更新（Software Upgrades）] > [クラスタの再起動（Reboot Cluster）]** の順に選択します。

ステップ 3 これはオプションです。 再起動の順序をまだ設定していない場合は、スライダを使って再起動の順序を編集し、**[保存]** をクリックします。

ステップ 4 **[バージョンの切り替え（Switch Versions）]** をクリックします。

（注） CLI を使用する場合、シンプル アップグレード クラスタ スイッチ バージョンの自動化のための CLI がないことに注意してください。 代わりに、`utils system switch-version` CLI コマンドで、単一ノードスイッチバージョンを使用できますが、これは、ノードごとに実行する必要があります。

アップグレードの準備 COP ファイルの実行 (アップグレード後)

アップグレード後、post-upgrade COP ファイルを実行し、以下を確認します。

- インストールされた COP ファイル
- ネットワーク サービスと接続 (DNS、NTP、クラスター内)
- FIPS モードのパスワードの長さの制限
- ライセンスの同期
- VMware ツールの互換性
- ディスク容量
- SIP および H.323 トランク登録
- データベース認証およびレプリケーションの状況
- データベースの健全性
- 最後の DRS バックアップの状況
- サービス状況
- インストールされている COP とロケール
- デバイス登録状態数
- エンタープライズ パラメータとサービス パラメータの設定
- TFTP 最大サービス数
- アクティブおよび非アクティブ バージョン

（注） システムの正常性を確認するために、Upgrade Readiness COP ファイルを実行してアップグレード後の確認をすることが推奨されます。

手順

ステップ 1 アップグレードの準備 COP ファイルをダウンロードしてアップグレード後のテストを実行します。

a) ダウンロードサイトに移動します。
b) 移動先のリリースを選択し、**[Unified Communications Managerユーティリティ（Unified Communications Manager Utilities）]** を選択します。
c) **アップグレード前テストを実行ために、Upgrade Readiness COP ファイル**をダウンロードします（たとえば、`ciscocm.postUpgradeCheck-00019.cop.sgn`）。 最新のファイルは別のファイル名とバージョンを持つ場合があることに注意してください。)

ステップ 2 アップグレード後のシステムの状態を確認します。

a) COP ファイルを実行します。
b) COP ファイルが返す問題を解決します。
c) COP ファイルがエラーを返さなくなるまで、これらの手順を繰り返します。

ステップ 3 アップグレード後のレポートを CLI で表示するには、**file get install/PostUpgradeReport.txt** コマンドを実行します。

ステップ 4 RTMT からレポートを表示するには

a) RTMT にログインします。
b) **[Trace and Log Central]** で、**[リモートブラウザ（Remote Browse）]** をダブルクリックし、**[トレースファイル（Trace files）]** を選択したら、**[次へ（Next）]** をクリックします。
c) **[すべてのサーバー上のすべてのサービス（Select all Services on all servers）]** を選択して、**[次へ（Next）]** をクリックします。
d) **[完了（Finish）]> [閉じる（Close）]** の順に選択します。
e) ノードをダブルクリックして、**[CUCMパブリッシャ（CUCM Publisher）] > [システム（System）] > [アップグレードログのインストール（Install upgrade Logs）]** の順に展開します。
f) [**インストール**] をダブルクリックして、必要なファイルを選択してダウンロードします。

次のタスク

アップグレードが完了しました。 新しいソフトウェアの使用を開始することができます。

クラスタノードのアップグレード（直接標準）

これらのタスクを完了して、ノードごとにクラスターノードをアップグレードします。 Unified OS Admin または CLI インターフェイスを使用して直接標準アップグレードを完了する場合、このプロセスを使用する必要があります。

（注） Pre-12.5.x ソースからリリース 15 への直接更新アップグレードはサポートされていません。まずソースをリリース 12.5.x または 14 および SU にアップグレードし、それからソースをリリース 15 にアップグレードします。

始める前に

アップグレード ISO ファイルと Upgrade Readiness COP ファイルをダウンロードし、同じディレクトリに保存します。ダウンロード情報については、アップグレードファイルのダウンロード （52 ページ） に移動してください。

手順

	コマンドまたはアクション	目的
ステップ 1	Upgrade Readiness COP ファイルの実行（アップグレード前） （54 ページ）	アップグレードの準備 COP ファイルを実行して、システムの接続性と状態を確認します。 問題がある場合は、アップグレードを進める前に修正してください。
ステップ 2	クラスター ソフトウェアの場所の構成（57 ページ）	アップグレードの前に、クラスター内で関連付けられたすべてのノードに対して、クラスター ソフトウェアのロケーションの詳細を構成することを選択できます。
ステップ 3	GUI または CLI インターフェイスのいずれかを使用して、クラスター ノードをアップグレードします。 • OS 管理経由でクラスターノードをアップグレードする (直接、標準)（68 ページ） • CLI経由でクラスターノードをアップグレードする (直接、標準) （69 ページ）	クラスタノードをクラスタでアップグレードします。
ステップ 4	手動でバージョンを切り替える （71 ページ）	これはオプションです。 アップグレード中にバージョンを自動的に切り替えなかった場合は、この手順を使用してバージョンを手動で切り替えます。
ステップ 5	アップグレードの準備 COP ファイルの実行 (アップグレード後) （72 ページ）	アップグレード後、アップグレード後 COP ファイルを実行して、システムの

	コマンドまたはアクション	目的
		アップグレード後の正常性を測定します。

Upgrade Readiness COP ファイルの実行（アップグレード前）

アップグレードの準備 COP ファイルは次の項目をチェックします。

- インストールされた COP ファイル
- ネットワーク サービスと接続 (DNS、NTP、クラスター内)
- ライセンスの同期
- VMware ツールの互換性
- ハードディスクパーティションサイズ
- スワップサイズチェック
- ファイルシステムタイプとゲスト OS のチェック
- 宛先バージョンに使用可能なディスク容量
- ESXi バージョン確認
- SIP および H.323 トランク登録
- データベース認証およびレプリケーションの状況
- データベースの健全性
- 最後の DRS バックアップの状況
- リモート通話コントロール (RCC) 機能の状況
- サービス状況
- インストールされている COP とロケール
- デバイス登録状態数
- エンタープライズ パラメータとサービス パラメータの設定
- TFTP 最大サービス数
- アクティブおよび非アクティブ バージョン
- 期限切れの証明書を一覧表示する
- FIPS モードのパスワードの長さの制限
- FIPS モードでの ESP および暗号化アルゴリズムの IPSec ポリシー設定確認

（注）
- アップグレードが失敗する可能性を大幅に減らすため、アップグレード前にアップグレードの準備 COP ファイルを実行することを強くお勧めします。
- COP ファイルはアップグレード前のバージョンが 10.x 以降の場合に完全にサポートされます。
- 3DES アルゴリズムは FIPS モードではサポートされていないため、3DES アルゴリズムを含む IPSec ポリシーを削除し、IPSec トンネルが確立される両方のノードで、3DES 以外の暗号化および ESP アルゴリズムを含む IPSec ポリシーを再作成する必要があります。

手順

ステップ 1 アップグレード準備 COP ファイルをダウンロードしてアップグレード前テストを実行します。
a) ダウンロード サイトに移動します。
b) 移動先のリリースを選択し、**[Unified Communications Manager ユーティリティ] を選択します。**
c) **アップグレード前テストを実行するために Upgrade Readiness COP ファイル**をダウンロードします（たとえば、`ciscocm.preUpgradeCheck-00019.cop.sgn`）。 最新のファイルは別のファイル名とバージョンを持つ場合があることに注意してください)。

ステップ 2 アップグレードに対してシステムの準備ができているか確認します。
a) COP ファイルを実行します。
b) COP ファイルが返す問題を解決します。
c) COP ファイルを再度実行します。
d) COP ファイルがエラーを返さなくなるまで、このプロセスを繰り返します。

ステップ 3 GUI または CLI から cop ファイルをインストールします。 インストールが完了したら、CLI から **file view install PreUpgradeReport.txt** を実行してレポートを表示します。

ステップ 4 RTMT からレポートを表示するには
a) RTMT にログインします。
b) **[Trace and Log Central]** で、**[リモートブラウザ（Remote Browse）]** をダブルクリックし、**[トレースファイル（Trace files）]** を選択したら、**[次へ（Next）]** をクリックします。
c) **[すべてのサーバー上のすべてのサービス（Select all Services on all servers）]** を選択して、**[次へ（Next）]** をクリックします。
d) **[完了（Finish）]> [閉じる（Close）]** の順に選択します。
e) ノードをダブルクリックして、**[CUCMパブリッシャ（CUCM Publisher）] > [システム（System）] > [アップグレードログのインストール（Install upgrade Logs）]** の順にします。
f) **[インストール（Install）]** をダブルクリックして、ダウンロードする必要なファイルを選択します。

クラスター ソフトウェアの場所の構成

この手順を使用して、同じクラスター内のノードの既存の構成を追加、編集、または変更します。

（注） この機能は、クラスタ内のすべてのノードが Release 14SU2 以降である場合にのみ使用できます。

手順

ステップ 1 **Cisco Unified OS Administration** ユーザーインターフェイスにログインします。

ステップ 2 **[ソフトウェアアップグレード（Software Upgrades）]>[クラスタソフトウェアの場所（Cluster Software Location）]** の順に選択します。

ステップ 3 追加するノードを選択するか、リストからサーバ ロケーションの詳細を編集します。

ステップ 4 パブリッシャを含むクラスタ内の他のすべてのノードに同じソフトウェアロケーションの詳細を適用する場合は、 **[すべてのノードに適用する**] チェックボックスを選択します。

このチェックボックスは、**[ノードを選択（Select Node）]** ドロップダウンメニューで [Unified CMパブリッシャ（Unified CM publisher）] を選択した場合のみ表示されます。

ステップ 5 パブリッシャノードのソース設定とソフトウェアロケーション詳細を使用する場合は、**[パブリッシャからのダウンロード資格情報とソフトウェアロケーションを使用する]** チェックボックスを使用します。

発行元からのダウンロード資格情報とソフトウェアの場所を使用する オプションがデフォルトで選択されています。

（注） このオプションはサブスクライバノードでのみ利用できます。

ステップ 6 （オプション）**[パブリッシャからのダウンロード資格情報とソフトウェアロケーションを使用する（Use download credentials and software location from Publisher）]** オプションを使用しない場合は、サーバーをアップグレードする前に、**[以下のダウンロード資格情報とソフトウェアロケーションを使用する（Use below download credentials and software location）]** を使用します。

（注） このオプションはサブスクライバノードでのみ利用できます。

ステップ 7 **[ソース（Source）]** ドロップダウンメニューで、アップグレードファイルの保存先と一致するオプションを選択します。

- **DVD/CD**
- **ローカルファイルシステム**—このオプションは、キャンセルされた前回のアップグレードを再開する場合にのみ利用できます。

- **SFTP サーバ**: ディレクトリ、サーバアドレス、ログイン資格情報など、SFTP サーバの詳細を入力する必要があります。

ステップ 8 （オプション）アップグレード完了時にメール通知を受信するには、**SMTP サーバー**アドレスと**メールの宛先**を入力します。これにより、アップグレード完了時にメール通知を受信できます。

ステップ 9 アップグレードファイルのダウンロード後にアップグレードを自動的に開始する場合は、[**ダウンロード後にアップグレードを続行**] チェックボックスを選択します。 このチェックボックスをオンにしない場合、**[ソース（Source）]** と設定された **[ローカルファイルシステム（Local filesystem）]** を使用して後で、アップグレードを手動で開始する必要があります。

ステップ 10 **アップグレード後にサーバのバージョンを切り替える (ISO に対してのみ有効)** チェックボックスを選択すると、アップグレードが完了した後にシステムが自動的に再起動されます。

ステップ 11 **[保存（Save）]** をクリックして、追加または修正された特定のノードに対するすべての設定変更を更新します。

OS 管理経由でクラスターノードをアップグレードする (直接、標準)

この手順を使用して、Cisco Unified Communications Manager または IM and Presence サービスクラスタノードの直接標準アップグレードを行います。

（注） 一部のアップグレードオプションは、アップグレードするバージョンによって若干異なる場合があります。

（注） Pre-12.5.x ソースからリリース 15 への直接更新アップグレードはサポートされていません。 まずソースをリリース 12.5.x または 14 および SU にアップグレードし、それからソースをリリース 15 にアップグレードする場合があります。

手順

ステップ 1 **Cisco Unified OS Administration** または **Cisco Unified IM and Presence OS Administration** にログインします。

ステップ 2 **[ソフトウェアアップグレード（Software Upgrades）] > [インストール/アップグレード（Install/Upgrade）]** の順に選択します。

ステップ 3 既存のノードをアップグレードするために必要な以下の構成情報を表示することができます。

（注） リリース 14SU3 以降では、すべてのクラスター ノードのソフトウェアの場所設定は、各クラスター ノードでローカルにではなく、パブリッシャーから一元管理されます。システムのアップグレードを開始する前に、同じクラスタ内の任意のノードの既存の設定を追加、編集、または変更する場合は、Cisco Unified OS Administration ユーザーインターフェイスで、**[ソフトウェアアップグレード（Software Upgrades）] > [クラスタソフトウェアの場所（Cluster Software Location）]**メニューの順に選択します。

- **資格情報**—アップグレードイメージが保存されているサーバの資格情報を表示します。
- **アップグレードファイルのソース**—アップグレードファイルが保存されているサーバの場所を表示します。 ローカルソース（CD または DVD）からアップグレードできます。また、FTP または SFTP を使用してリモート アップグレードファイルをダウンロードできます。また、キャンセル操作後にアップグレードを再開する場合は、ローカルイメージソースオプションを通じて以前にダウンロードしたアップグレードファイルを使用できます。
- **ダウンロード後にアップグレードを続行**: アップグレードファイルがダウンロードされたら、自動的にアップグレードを行うかどうかで選択されたオプションを示します (デフォルト値は「はい」です)。 自動アップグレードを選択した場合、チェックサムまたは SHA の詳細は表示されません。 [はい（Yes）] または [いいえ（No）] の値を設定していた場合は、その設定はシステムに残ります。
- **バージョン切り替え**: アップグレードが完了したら新しいバージョンに自動的に切り替えるかどうかを指定します (デフォルトでは「いいえ」)。 「yes」を入力した場合、システムは新しいバージョンに切り替わり、アップグレードの完了後に自動的にリブートします。 値を「はい」または「いいえ」に設定した場合、設定はシステムに残ります。

ステップ 4 [次へ（Next）]をクリックします。

ステップ 5 インストールするアップグレードバージョンを選択して、[**次へ**] をクリックします。
アップグレードが開始されます。 **インストール状況** ページにアップグレードに関する情報が表示されます。

ステップ 6 アップグレードが完了したら **[完了（Finish）]** をクリックします。
アップグレード後にバージョンを自動的に切り替えることを選択した場合、ノードはアップグレード後にアップグレードされたバージョンでリブートします。 そうでない場合、アップグレードは非アクティブパーティションに保存するため、後で手動でバージョンを切り替えることができます。

ステップ 7 追加のクラスターノードに対してこの手順を繰り返します。

CLI 経由でクラスターノードをアップグレードする (直接、標準)

この手順を使用して、CLI 経由で個々のクラスターノードをアップグレードします。

（注） アップグレードオプションは、アップグレードするバージョンによって異なります。

（注） Pre-12.5.x ソースからリリース 15 への直接更新アップグレードはサポートされていません。 まずソースをリリース 12.5.x または 14 および SU にアップグレードし、それからソースをリリース 15 にアップグレードする場合があります。

（注） リリース 14SU3 以降では、すべてのクラスター ノードのソフトウェア ロケーション設定は、各クラスター ノードでローカルにではなく、パブリッシャーから一元管理されます。 システムのアップグレードを開始する前に、同じクラスタ内の任意のノードの既存の設定を追加、編集、または変更する場合は、Cisco Unified OS Administration ユーザーインターフェイスで、**[ソフトウェアアップグレード（Software Upgrades）] > [クラスタ ソフトウェアの場所（Cluster Software Location）]**メニューの順に選択します。

手順

ステップ 1 アップグレードするノードのコマンド ライン インターフェースにログインします。

ステップ 2 `utils system upgrade initiate` CLI コマンドを実行すると、ウィザードに、ソフトウェアの場所の詳細が表示され、同じクラスタ内のすべてのノードを構成します。

ステップ 3 プロンプトが表示されたら、次のいずれかを選択します。

- **[はい]**を選択すると、アップグレードプロセスはソースファイルとして使用できるアップグレードファイルをチェックし、ステップ **8** に進みます。
- **[いいえ（No）]** を選択すると、ソースを選択するプロンプトが表示されます（手順 **4**から **8** を実行します）。

ステップ 4 プロンプトが表示されたら、アップグレードファイルが保存されているソースを選択します。

- **SFTP または FTP 経由のリモートファイルシステム**—サーバーの詳細と資格情報の入力が求められます。
- **ローカル DVD/CD**—ローカルの CD または DVD のみ。
- **ローカルイメージ**:このオプションは、以前にアップグレードを開始し、まだアップグレードを完了していない場合にのみ利用できます。

ステップ 5 (オプション) アップグレードが完了したことを知らせるメール通知の **SMTP ホスト** を入力します。

ステップ 6 プロンプトが表示されたら、アップグレードファイルのダウンロード後、自動的にアップグレードを続行するかどうかを入力します。

- **はい**:すべてのノードにファイルがダウンロードされたら、アップグレードを開始します。

- **いいえ**—アップグレードファイルはローカルイメージとして保存されます。アップグレードは後ほど再開できます。

ステップ 7 プロンプトが表示されたら、アップグレード後にバージョンを自動的に切り替えるかどうかを入力します。

- **はい**: アップグレード後、クラスターは自動的に新しいバージョンに切り替わり、再起動します。
- **いいえ**—アップグレードは非アクティブパーティションに保存されます。 後ほど手動でバージョンを切り替えることができます。

ステップ 8 インストール開始のプロンプトに対して、 **「はい」** を入力します。
アップグレード後にバージョンを自動的に切り替えることを選択した場合、ノードはアップグレード後にアップグレードされたバージョンでリブートします。 そうでない場合、アップグレードは非アクティブパーティションに保存するため、後で手動でバージョンを切り替えることができます。

手動でバージョンを切り替える

アップグレードの一部としてバージョンを自動的に切り替えなかった場合は、この手順を使用してクラスターノードのバージョンを手動で切り替えることができます。 GUI または CLI のいずれかを使用できます。

（注） クラスタ全体のバージョン切り替えオプションは、アップグレード前のバージョンが 12.5(x) 以上の直接の標準アップグレードでのみ利用できます。 詳細は、 手動でバージョンを切り替える (クラスター全体) （61 ページ）

手順

ステップ 1 GUI を使用する場合:

a) 切り替えるノードの Cisco Unified OS Administration インターフェイスまたは Cisco Unified IM and Presence OS Administration インターフェイスにログインして、以下を実行します。
b) **[設定（Settings）]** > **[バージョン（Version）]** の順に選択します。
c) アクティブおよび非アクティブなソフトウェアのバージョンを確認します。
d) **[バージョンの切り替え（Switch Version）]** をクリックして、バージョンを切り替えて、ノードを再起動します。
e) 追加のクラスターノードに対してこれらの手順を繰り返します。

ステップ 2 CLI を使用する場合:

a) ノードのコマンド ライン インターフェースにログインします。

b) `utils system switch-version` CLI コマンドを実行します。
c) 追加のクラスターノードに対してこれらの手順を繰り返します。

アップグレードの準備 COP ファイルの実行 (アップグレード後)

アップグレード後、post-upgrade COP ファイルを実行し、以下を確認します。

- インストールされた COP ファイル
- ネットワーク サービスと接続 (DNS、NTP、クラスター内)
- FIPS モードのパスワードの長さの制限
- ライセンスの同期
- VMware ツールの互換性
- ディスク容量
- SIP および H.323 トランク登録
- データベース認証およびレプリケーションの状況
- データベースの健全性
- 最後の DRS バックアップの状況
- サービス状況
- インストールされている COP とロケール
- デバイス登録状態数
- エンタープライズ パラメータとサービス パラメータの設定
- TFTP 最大サービス数
- アクティブおよび非アクティブ バージョン

（注） システムの正常性を確認するために、Upgrade Readiness COP ファイルを実行してアップグレード後の確認をすることが推奨されます。

手順

ステップ 1 アップグレードの準備 COP ファイルをダウンロードしてアップグレード後のテストを実行します。

a) ダウンロードサイトに移動します。

b) 移動先のリリースを選択し、**[Unified Communications Managerユーティリティ（Unified Communications Manager Utilities）]** を選択します。
c) **アップグレード前テストを実行ために、Upgrade Readiness COP ファイル**をダウンロードします（たとえば、`ciscocm.postUpgradeCheck-00019.cop.sgn`）。 最新のファイルは別のファイル名とバージョンを持つ場合があることに注意してください。)

ステップ 2 アップグレード後のシステムの状態を確認します。

a) COP ファイルを実行します。
b) COP ファイルが返す問題を解決します。
c) COP ファイルがエラーを返さなくなるまで、これらの手順を繰り返します。

ステップ 3 アップグレード後のレポートを CLI で表示するには、**file get install/PostUpgradeReport.txt** コマンドを実行します。

ステップ 4 RTMT からレポートを表示するには

a) RTMT にログインします。
b) **[Trace and Log Central]** で、**[リモートブラウザ（Remote Browse）]** をダブルクリックし、**[トレースファイル（Trace files）]** を選択したら、**[次へ（Next）]** をクリックします。
c) **[すべてのサーバー上のすべてのサービス（Select all Services on all servers）]** を選択して、**[次へ（Next）]** をクリックします。
d) **[完了（Finish）]> [閉じる（Close）]** の順に選択します。
e) ノードをダブルクリックして、**[CUCMパブリッシャ（CUCM Publisher）] > [システム（System）] > [アップグレードログのインストール（Install upgrade Logs）]** の順に展開します。
f) [**インストール**] をダブルクリックして、必要なファイルを選択してダウンロードします。

次のタスク

アップグレードが完了しました。 新しいソフトウェアの使用を開始することができます。

クラスタを前のバージョンに切り替える

クラスタを前のバージョンに戻すには、これらの主要なタスクを実行します。

手順

ステップ 1 パブリッシャノードを戻します。
ステップ 2 すべてのバックアップサブスクライバノードを元に戻す。
ステップ 3 すべてのプライマリサブスクライバノードを元に戻します。
ステップ 4 古い製品リリースに戻す場合は、クラスター内のデータベースレプリケーションをリセットします。

ノードを前のバージョンに切り替える

手順

ステップ 1 アップグレードしているノードの管理ソフトウェアにログインします。

- IM and Presence Service ノードをアップグレードする場合は、Cisco Unified IM and Presence Operating System Administration にログインします。
- Unified Communications Manager ノードをアップグレードする場合は、Cisco Unified Communications Operating System Administration にログインします。

ステップ 2 **設定** > **バージョン**を選択します。

[バージョン設定] ウィンドウが表示されます。

ステップ 3 [**バージョンを切り替える**] ボタンをクリックします。

システムの再起動を確認すると、システムが再起動します。処理が完了するまでに、最大で15分かかることがあります。

ステップ 4 バージョンの切り替えが成功したことを確認するには、次の手順に従います。

a) アップグレードするノードの管理ソフトウェアに再度ログインします。
b) **[設定（Settings）]** > **[バージョン（Version）]** の順に選択します。

[バージョン設定] ウィンドウが表示されます。

c) 正しい製品バージョンがアクティブパーティションで実行中であることを確認してください。
d) すべてのアクティブ化されたサービスが実行中であることを確認します。
e) パブリッシャノードの場合は、Cisco Unified CM Administration にログインします。
f) ログインできること、および構成データが存在することを確認します。

データベース レプリケーションのリセット

古い製品リリースを実行するためにクラスター内のサーバを戻す場合、クラスター内のデータベース複製を手動でリセットする必要があります。

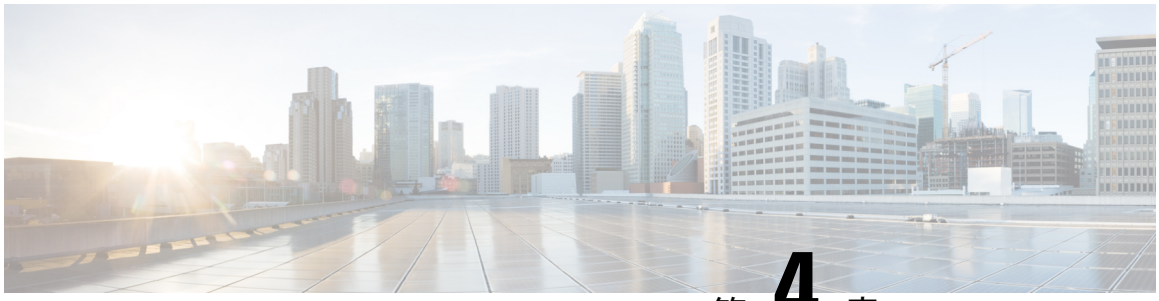
手順

ステップ 1 パブリッシャ ノードでコマンドライン インターフェイスにログインします。

ステップ 2 `utils dbreplication reset all` コマンドを実行します。

第 部

付録



第 4 章

仮想化ソフトウェアの変更

アップグレードでVMwareの更新が必要な場合にのみ、この付録の手順を実行してください。

- 仮想マシンの設定タスク （77 ページ）

仮想マシンの設定タスク

アップグレードするソフトウェアバージョンの要件を満たすために仮想マシンの設定を変更する必要がある場合、この章の手順を使用してください。

始める前に

新しいリリースの要件を満たすために仮想マシンをアップグレードする必要があるかどうかを確認します。 Cisco Collaboration Virtualization に移動し、 Unified Communications Manager および IM and Presence Service アプリケーションのリンクをたどることで、要件を確認できます。

手順

	コマンドまたはアクション	目的
ステップ 1	VMware vCenter のインストールと構成（79 ページ）	VMware vCenter は、Cisco Business Edition またはテスト済みの参照設定 (TRC) ハードウェアから UC on UCS の仕様ベースまたはサードパーティのサーバ仕様ベースのハードウェアに移行する場合にのみ必要です。 VMware vCenter が必要な場合は、まずそれをインストールして設定します。 VMware vCenter の使用は、UC on UCS テスト済みリファレンス設定ハードウェアに Unified Communications Manager または IM and Presence Service を展開する場合は、任意です。

	コマンドまたはアクション	目的
ステップ 2	vSphere ESXi のアップグレード （79 ページ）	リリースの要件を満たす vSphere ESXi ハイパーバイザーのバージョンをインストールする必要があります。 Unified Communications Manager または IM and Presence Serviceのアップグレードを開始する前に、ESXiハイパーバイザーをアップグレードしておくことをお勧めします。ただし、これらのアプリケーションの現在インストールされているバージョンが、新しいリリースに必要な ESXi バージョンと互換性がない場合、Cisco アプリケーションをアップグレードした後で、ESXi バージョンをアップグレードできます。
ステップ 3	OVA テンプレートのダウンロードとインストール （80 ページ）	OVA ファイルは、仮想マシン設定用の定義済みテンプレート一式を提供します。 これらは、サポートされている容量レベルや、必要な OS/VM/SAN 連携などの項目をカバーしています。 この手順は省略可能です。 すでに Unified Communications Manager または IM and Presence Service を実行していて、展開サイズを変更していない場合、新しい OVA テンプレートをダウンロードしてインストールする必要はありません。システムのサイズを変更する場合、展開に適した新しいリリースの OVA テンプレートをダウンロードしてインストールします。
ステップ 4	仮想マシン構成の仕様の変更 （81 ページ）	Unified Communications Manager または IM and Presence Service の新しいリリースへアップグレードする場合は、仮想マシン（VM）の vCPU、vRAM、vDisk 座椅子または vNIC タイプを変更する際に、次の手順を実行します。 このステップは、Unified CM OS 管理インターフェイスまたは PCD アップグレードタスクのいずれかを使用してアップグレードを実行する直接アップグレードのみに行います。

	コマンドまたはアクション	目的
ステップ 5	単一から複数の vDisk 仮想マシンへの移行 （82 ページ）	複数の vDisk を必要とする、より大きな仮想マシン (VM) 展開に移行する場合は、この手順を使用します。

VMware vCenter のインストールと構成

VMware vCenter の使用は、UC on UCS テスト済みリファレンス設定ハードウェアに Unified Communications Manager または IM and Presence Service を展開する場合は、任意です。 VMware vCenter は、UCS 仕様ベースおよびサードパーティ サーバ仕様ベースのハードウェアで UC に展開する場合に必須です。

VMware vCenter では、パフォーマンスデータを収集することができます。 アプリケーションのインストールと設定の方法については、VMware のドキュメントを参照してください。

手順

ステップ 1 VMware vCenter をインストールします。

ステップ 2 パフォーマンス統計で追跡する詳細レベルを設定します。 統計レベルの範囲は 1 から 4 で、レベル 4 に最も多くのデータが含まれます。 UCS 仕様または HP/IBM 仕様ベースの展開では、統計レベルを 4 に設定する必要があります。

ステップ 3 データ サイズの見積もりを表示して、すべての統計を保持するのに十分なスペースがあることを確認します。

vSphere ESXi のアップグレード

Unified Communications Manager の新しいリリースにアップグレードするために vSphere ESXi ハイパーバイザーを更新する必要がある場合は、次の手順を実行します。

手順

ステップ 1 次のいずれかの方法を使用して、実行中の仮想マシン Unified Communications Manager をホストサーバから移動します:

- ホットスタンバイホストがある場合、vMotion を使用して、仮想マシンを物理サーバーから別の物理サーバーに移行します。
- ホットスタンバイホストがない場合は、仮想マシンの電源を切り、別の場所にコピーします。

ステップ 2 VMware が提供するアップグレード手順を使用して、vSphere ESXi をアップグレードします。

ステップ 3 vSphere ESXi が正常にアップグレードされたことを確認します。

ステップ 4 次のいずれかの方法で、実行中の仮想マシン Unified Communications Manager をホストサーバーに戻します:

- ホットスタンバイホストがある場合、vMotion を使用して、仮想マシンを物理サーバーから別の物理サーバーに移行します。
- ホットスタンバイホストがない場合は、仮想マシンの電源を切り、ホストサーバーにそれをコピーします。

OVA テンプレートのダウンロードとインストール

OVA ファイルは、仮想マシン設定用の定義済みテンプレート一式を提供します。 これらは、サポートされている容量レベルや、必要な OS/VM/SAN 連携などの項目をカバーしています。 OVA ファイルについての情報は、 https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/cisco-collaboration-virtualization.html で"Unified Communications Virtualization サイジングガイドライン"を検索してください。

この手順は省略可能です。 すでに Unified Communications Manager または IM and Presence Service を仮想マシンで実行しており、展開サイズを変更していない場合、新しい OVA テンプレートをダウンロードしてインストールする必要はありません。 システムのサイズを変更する場合、展開に適したサイズの OVA テンプレートをダウンロードしてインストールします。

手順

ステップ 1 お使いのリリースの OVA テンプレートを探します。

- Unified Communications Managerについては、 https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/cisco-collaboration-virtualization.html に移動してトピック"Cisco Unified Communications Manager の仮想化" を検索してください。
- IM and Presence Serviceについては、 https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/cisco-collaboration-virtualization.html に移動してトピック「Unified CM IM and Presence の仮想化」を検索してください。

ステップ 2 単一の OVA ファイルをダウンロードするには、そのファイルの隣にある [**ファイルをダウンロード**] ボタンをクリックします。 複数の OVA ファイルをダウンロードするには、ダウンロードする各ファイルの隣にある **[カートに追加（Add to Cart）]** ボタンをクリックし、**[カートをダウンロード（Download Cart）]** リンクをクリックします。

ステップ 3 **[カートをダウンロード（Download Cart）]** ページで **[ダウンロードを続行（Proceed with Download）]** ボタンをクリックします。

ステップ 4 [**ソフトウェア使用許諾契約**] ページの情報を読み、[**同意する**] ボタンをクリックします。

ステップ 5 次のいずれかのリンクをクリックします。

- **ダウンロード マネージャ** (Java が必要)
- **非 Java ダウンロードオプション**

新しいブラウザウィンドウが表示されます。

ステップ 6 ファイルを保存します。

- **[ダウンロードマネージャ（Download Manager）]** を選択すると、**[場所を選択（Select Location）]** ダイアログボックスが表示されます。 ファイルを保存する場所を指定し、**[開く（Open）]** をクリックしてローカルマシンにファイルを保存します。
- **非 Java ダウンロードオプション**を選択した場合は、新しいブラウザウィンドウで表示される [**ダウンロード**] リンクをクリックします。 場所を指定し、ファイルをローカルマシンに保存します

仮想マシン構成の仕様の変更

Unified Communications Manager または IM and Presence Service の新しいリリースへアップグレードする場合は、仮想マシン（VM）の vCPU、vRAM、vDisk または vNIC を変更する際に、次の手順を実行します。

VM の要件の詳細については、お使いのリリースに対応する OVA テンプレートの Readme ファイルを参照してください。 OVA テンプレートと要件の詳細については、 www.cisco.com go virtualized-collaboration に移動して、トピック「Implementing Virtualization Deployments」を検索してください。

始める前に

vDisk のストレージ容量を増やす必要がある場合は、事前に仮想マシン（VM）のスナップショットを削除する必要があります。 そうでない場合、ディスクサイズを増やすオプションはグレー表示されます。 「スナップショットを使用する」を参照してください。

手順

ステップ 1 災害復旧システム (DRS) バックアップを実行します。

ステップ 2 （任意） 9.x 以前からのアップグレードで、更新アップグレードのスペース要件を満たすために vDisk のスペースを増やす必要がある場合は、次の COP ファイルをインストールします:

```
ciscocm.vmware-disk-size-reallocation-<latest_version>.cop.sgn
```

（注） Pre-12.5.x ソースからリリース 15 への更新アップグレードはサポートされていません。

ステップ 3 仮想マシンをシャットダウンします。

ステップ 4 必要に応じて仮想マシンの構成を変更します。

a) 新しいリリースの要件に一致するように、ゲスト OS バージョンを変更します。

b) vCPU を変更するには、vSphere Client で変更を行います。 新しいリリースの仕様に一致するように予約値を変更してください。

c) vRAM を変更するには、vSphere Client で変更を行います。 新しいリリースの仕様に一致するように予約値を変更してください。

d) vDisk の容量を増やすには、vSphere Client を使用してストレージサイズを編集します。 仮想マシンに 2 つのディスクがある場合、2 つ目のディスクを拡張します。

仮想マシンを再起動すると、新しいスペースが自動的に共通パーティションに追加されます。

（注） アップグレードを完了するために追加のスペースが必要な場合にのみ、ディスクサイズを変更する必要があります。 ディスクスペースの要件は、OVA テンプレートの Readme ファイルで指定されています。

共通パーティションにスペースを追加するためにディスクサイズを拡張しても、システムのユーザ容量は増加しません。 システムのユーザ容量を拡張する必要がある場合、単一ディスクの仮想マシンから複数ディスクの仮想マシンに移行する必要があります。

vDisk を縮小するか、vDisk の数を変更する必要がある場合は、vDisk を再インストールするか、新しい vDisk をインストールする必要があります。

e) vSphere Client で、ネットワークアダプタが VMXNET 3 アダプタタイプを使用するように構成されていることを確認します。 ネットワークアダプタが別のタイプに設定されている場合は、変更します。

vSphere Client を使用した構成変更の詳細については、製品のユーザマニュアルを参照してください。

ステップ 5 アップグレードを続行してから仮想マシンの電源をオンにしてください。

単一から複数の vDisk 仮想マシンへの移行

複数の vDisk を必要とする、より大きな仮想マシン (VM) 展開に移行する場合、次の手順を実行します。 この手順が完了したら、仮想マシン構成の仕様の変更 （81 ページ） を確認して、仕様がリリースの要件に合っていることを確認する必要があります。

手順

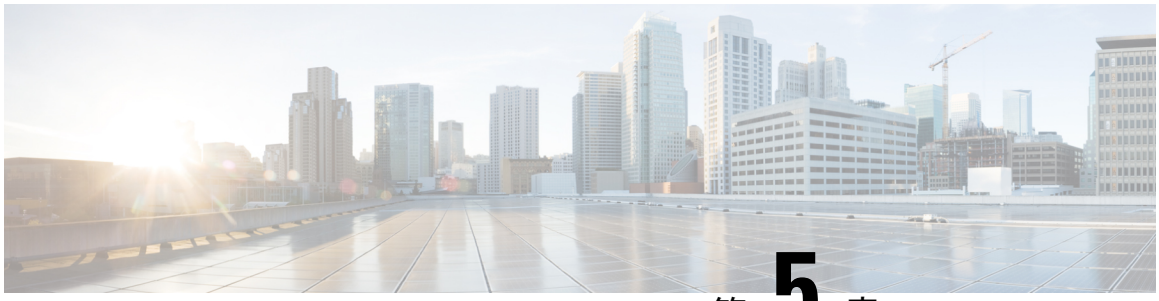
ステップ 1 災害復旧システム (DRS) を使用して、既存の仮想マシン (VM) のバックアップを実行します。

ステップ 2 既存の VM の電源をオフにして、ネットワークから削除します。

ステップ 3 適切な OVA テンプレートを使用して、新しい VM を正しいユーザ数で展開します。

ステップ 4 新しい VM 上で、同じホスト名と IP アドレスを使用して IM and Presence Service または Unified Communications Manager の同じソフトウェアリリースを新規インストールします。

ステップ 5 新しい VM で DRS 復元を実行します。



第 5 章

シーケンスルールと時間の要件

アップグレードの順序と所要時間

アップグレード手順を実行する順序は、展開によって異なり、ユーザへの影響のレベルとアップグレードを完了するために必要な時間のバランスをどのように取るかによって異なります。アップグレードプロセスを実行する前に、従うシーケンスを特定する必要があります。

このセクションの情報は、Unified CM OS の管理インターフェイスまたは PCD アップグレードタスクのいずれかを使用して直接アップグレードを実行している場合にのみ適用されます。PCD 移行ではこの手順は必要ありません。

バージョンの切り替えについて

ノードをアップグレードすると、新しいソフトウェアが非アクティブバージョンとしてインストールされます。新しいソフトウェアをアクティベートするには、ノードを新しいソフトウェアバージョンに切り替える必要があります。新しいソフトウェアバージョンに切り替えるには 2 つの方法があります。

- 自動切り替え—システムはアップグレードプロセスの一部として自動的にバージョンを切り替えます
- 手動切り替え—アップグレード プロセスが完了した後で、OS 管理インターフェイスを使用して、バージョンを物理的に切り替えます。

選択する方法は、実行しているアップグレードのタイプによって異なります。アップグレードプロセスの間、ウィザードはアップグレードされたパーティションをリブートすることによってソフトウェアバージョンを自動的に切り替えるか、または後で手動でバージョンを切り替えるかどうかを選択するようにプロンプトします。アップグレードの種類ごとの切り替え方法は以下の表の通りです。

アップグレードの種類	切り替えタイプ	プロンプトが表示された場合。 . .	結果
標準アップグレード	自動	**GUI:** アップグレードされたパーティションをリブート **CLI:** アップグレード後に新しいバージョンに切り替える	このオプションを選択すると、システムは新しいソフトウェアバージョンでリブートします。
	手動	**GUI:** アップグレード後にリブートしない **CLI:** アップグレード後に新しいバージョンに切り替えないでください	このオプションを選択すると、アップグレードが完了したときに、システムは古いソフトウェアバージョンを実行し続けます。 後ほど手動で新しいソフトウェアに切り替えることができます。
アップグレードの更新	自動	**GUI:** アップグレードされたパーティションをリブート **CLI:** アップグレード後に新しいバージョンに切り替える	アップグレード直後に新しいソフトウェアバージョンを使用するには、このオプションを選択します。
	手動	**GUI:** アップグレード後にリブートしない **CLI:** アップグレード後に新しいバージョンに切り替えないでください	更新アップグレードを段階的に実行する場合にのみ、このオプションを使用します。 このオプションを選択すると、アップグレードが完了したときにシステムは古いソフトウェアバージョンでリブートします。後ほど手動で新しいソフトウェアに切り替えることができます。

バージョンを切り替えると、構成情報はアクティブパーティション上のアップグレードされたバージョンに自動的に移行されます。

何らかの理由でアップグレードを中止した場合、システムを再起動して、古いバージョンのソフトウェアを含む非アクティブパーティションを使用することができます。 ただし、ソフトウェアのアップグレード以降に行った構成の変更は失われます。

別の製品バージョンにアップグレードしてから Unified Communications Manager をインストールするか、スイッチオーバーした後の時間で、電話ユーザーが行った変更が失われる場合があります。 電話ユーザ設定の例には、コール転送やメッセージ ウェイティング表示ライトの設定が含まれます。 これは、インストールまたはアップグレード後に、Unified Communications Manager がデータベースを同期し、電話ユーザー設定の変更が上書きされるために発生します。

順序ルール

Unified CM OS Admin インタフェースまたは PCD アップグレードタスクのいずれかを使ってアップグレードを行う場合は、以下の順序付けルールを必ず考慮してください。

- Unified Communications Manager パブリッシャーノードを最初にアップグレードしてください。 新しいソフトウェアが非アクティブバージョンとしてインストールされます。
- 新しいソフトウェアの非アクティブなバージョンでパブリッシャノードがアップグレードされたら、すぐに Unified Communications Manager サブスクライバノードのアップグレードを開始できます。
- Unified Communications Manager パブリッシャーノードを新しいソフトウェアバージョンに切り替え、サブスクライバーノードでバージョンを切り替える前に再起動する必要があります。 パブリッシャノードは、新しいソフトウェアバージョンに切り替えて再起動する最初のノードである必要があります。
- サブスクライバノードのグループをアップグレードする場合、ソフトウェアバージョンを切り替えてリブートした後、すべてのサブスクライバノードでデータベースの複製が完了するのを待ってから、COP ファイルのインストールまたは設定の変更を行う必要があります。
- Unified Communications Manager ノードを Maintenance Release（MR）または Engineering Special（ES）Releaseにアップグレードし、IM and Presence Service ノードはアップグレードしない場合、Unified Communications Manager アップグレードを完了してから、すべての IM and Presence ノードを再起動する必要があります。
- IM and Presence Service ノードに加えて Unified Communications Manager ノードをアップグレードする場合:
    - IM and Presence Service データベース公開者ノードは、アップグレードする最初の IM and Presence Service ノードでなければなりません。 新しいソフトウェアが非アクティブバージョンとしてインストールされます。

- パブリッシャノードが新しいソフトウェアの非アクティブバージョンでアップグレードされるとすぐに、サブスクライバノード IM and Presence Service のアップグレードを開始することができます。
- すべての Unified Communications Manager ノードの非アクティブバージョンへのアップグレードが完了するまで待ってから IM and Presence Service データベースパブリッシャノードをアップグレードするか、並行してアップグレードするかを選択できます。 並行してアップグレードする場合は、サブスクライバーノード IM and Presence Service をアップグレードするのと同時に、 Unified Communications Manager データベースパブリッシャーノードのアップグレードを開始してください。
- IM and Presence Service ノードでバージョンを切り替える前に、新しいソフトウェアのバージョンに切り替え、パブリッシャノードから始まるすべての Unified Communications Manager ノードを再起動する必要があります。
- IM and Presence Service データベースのパブリッシャノードを新しいソフトウェアバージョンに切り替えて再起動してから、 IM and Presence Service サブスクライバノードのソフトウェアバージョンを切り替える必要があります。
- IM and Presence Service サブスクライバノードのグループをアップグレードする場合、ソフトウェアバージョンを切り替えて再起動した後、すべてのサブスクライバノードでデータベースの複製が完了するのを待ってから続行してください。

- IM and Presence Service ノードを Maintenance Release（MR）または Engineering Special（ES）Release にアップグレードするが、Unified Communications Manager ノードをアップグレードしない場合は、次の追加ルールに従います。
  - Unified CM OS Admin インターフェイスを使用したアップグレードの場合、Unified Communications Manager パブリッシャノードをアップグレードしてから、IM and Presence Service を Maintenance Release（MR）または Engineering Special（ES）Release にアップグレードする必要があります。
  - Prime Collaboration Deployment 移行タスクを使用している場合は、IM and Presence Service ノードに加えて、Unified Communications Manager パブリッシャノードを選択する必要があります。
  - Prime Collaboration Deployment アップグレードタスクを使用している場合、Unified Communications Manager の新しいバージョンの最初の 3 桁が IM and Presence Service の現在インストールされているバージョンの最初の 3 桁と一致する限り、パブリッシャノードを選択する必要はありませんUnified Communications Manager。

アップグレードの所要時間

ソフトウェアのアップグレードに必要な時間は様々な要因によって異なります。 次のセクションの情報を使用して、アップグレードプロセスを最適化するための手順を理解してください。

以下のセクションでは、アップグレードに必要な時間を見積もるのに役立つ情報と例も記載しています。

アップグレード所要時間に影響を与える要素

下の表は、アップグレードに必要な時間に影響を与える要素を示しています。システムがこれらの条件を満たしていることを確認することで、アップグレードに必要な時間を短縮することができます。

表 *10*：所要時間に影響する要素

項目	説明
外部サービスおよびツール	所要時間は、NTP サーバ、DNS サーバ、LDAP ディレクトリ、その他のネットワークサービスなどの外部サービスやツールが、パケットの欠落なく、可能な限り短い応答時間で到達できる場合に短縮されます。 ESXi サーバと Unified Communications Manager パブリッシャーノードが同じ NTP サーバを指すように設定することを推奨します。 （注） VM の時刻同期の問題によるアップグレードの失敗を回避するには、http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1189 のリンクに記載されている回避策を使用して、ESXi ホストとの VM の NTP 同期を無効にします。
アップグレードイメージのアクセシビリティ	ISO イメージが DVD 上にある、またはすでにダウンロードされており、Unified Communications Manager および IM and Presence Service 仮想マシン（VM）と同じ LAN 上に展開されていることを確認して、時間を節約します。

項目	説明
システムヘルス	仮想マシンの設定はアップグレードの所要時間に影響します。展開サイズに適した仮想マシンの仕様を使用してください。データベースが仮想マシンの設定制限を超えている場合、アップグレードプロセスは完了するまでに時間がかかるか、失敗します。たとえば、VM 設定に対してデバイスが多すぎると、アップグレードに影響します。
	低メモリまたはメモリリークはアップグレードに影響を与えます。
	ノード間の往復時間 (RTT) は必要な時間を延長します。
	データベースに OutOfSynch（OOS）テーブルがないことを確認します。
	Unified Communications Manager ノードで SD リンクの停止中のイベントがないことを確認してください。 これらのイベントは通常ネットワークの問題を示しており、アップグレードを開始する前に対処しておく必要があります。
	システムエラーはアップグレード時間に影響を与えます。 Real Time Monitoring Tool (RTMT) インターフェイスでは、左側のナビゲーションペインにある [Alert Central] をダブルクリックし、エラーがないことを確認します。

項目	説明
物理および仮想ハードウェア インフラストラクチャ	インフラストラクチャが大容量で低遅延に設定されていて、他のトラフィックからの競合が低い場合、アップグレード時間は短縮されます。 例えば、以下を確認することでアップグレードプロセスを最適化できます。 • 同じ ESXi ホスト、同じ Direct Attached Storage（DAS）ボリューム、同じ Logical Unit Number（LUN）または同じ輻輳ネットワークリンクを共有する VM でインフラストラクチャの問題はありません。 • ストレージレイテンシは、.. www.cisco.com go virtualized-collaboration で指定されている要件を満たしています。 • 物理 CPU コアと仮想化設計は、Unified Communications Manager と IM and Presence Service の仮想化要件に準拠しています。 仮想マシンがホストリソースを共有することで、CPU をオーバーサブスクライブしないでください。論理コアまたはリソース予約を使用してください。 • Unified Communications Manager と IM and Presence Service 仮想マシンは同じホスト上にあるか、または他のトラフィックからの競合が少ない 1GbE LAN を持つホスト上にあります。 • クラスタが WAN 上にある場合は、http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-system/products-implementation-design-guides-list.html にある *Cisco Collaboration Systems Solution Reference Network Design*（*SRND*）に記載されているすべての帯域幅とレイテンシルールに従います。
システム容量	次のような不要なファイルを削除することで、アップグレード時間を短縮します。 • 通話詳細記録（CDR）レコード • TFTP ファイル、ファームウェア、ログファイルなどの古いファイル
スロットリング	IM and Presence Service ノードでは、システムがアップグレードプロセスを抑制し、アップグレード中のシステムの安定性を維持します。 スロットリングにより、アップグレードが完了するまでの時間が長くなる場合があります。 スロットリングを無効にしてアップグレードにかかる時間を減らすことができますが、システムパフォーマンスが低下する場合があります。

最小時間要件を見積もる

下の表は、理想的な条件下でのアップグレードプロセスの各タスクで予想される最小経過時間を示しています。ネットワークの状態や従うべきアップグレードの順序によっては、アップグレードにはこの表に記載されている時間よりも長くかかる場合があります。

（注） アップグレードプロセスを開始すると、アップグレードが完了し、アップグレード後のタスクをすべて実行するまで、構成を変更することはできません。 構成の変更には以下が含まれます。

- Unified Communications Manager または IM and Presence Service グラフィカル ユーザーインターフェイス（GUI）、コマンドライン インターフェイス（CLI）または AXL API を介した変更
- LDAP 同期 (Oracle LDAP から Unified Communications Manager にプッシュされる増分同期を含む)
- 自動ジョブ
- 自動登録を試みているデバイス

（注） Pre-12.5.x ソースからリリース 15 へのアップグレードの更新はサポートされていません。

表 *11* : アップグレードタスクの最小所要時間

タスク	最小時間	サービスへの影響
Unified Communications Manager パブリッシャノードを非アクティブバージョンにアップグレードする	2 から 4 時間 更新アップグレードの場合は 1 時間を追加します	アップグレードの更新: UI にアクセスできません
Unified Communications Manager サブスクライバノードを非アクティブバージョンにアップグレードします	1 から 2 時間	アップグレードの更新: バックアップサブスクライバが設定されていない場合、電話を利用できません
Unified Communications Manager パブリッシャーノードを新しいソフトウェアバージョンに切り替えて再起動してください	30 分	—

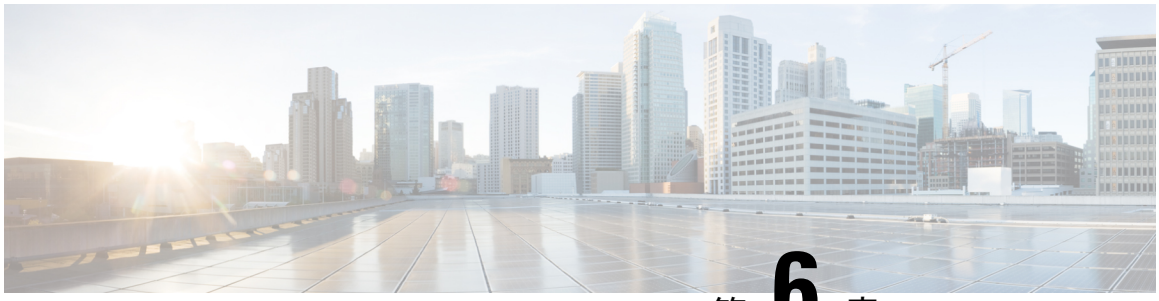
タスク	最小時間	サービスへの影響
Unified Communications Manager サブスクライバノードを新しいソフトウェアバージョンに切り替えて再起動してください	30 分	標準アップグレード: バックアップサブスクライバが設定されていない場合、電話を利用できません
Unified Communications Manager データベースリプリケーション	小規模クラスターまたは小規模データベースの展開の場合は 30 分 メガクラスターまたは大きなデータベースの場合は 2 時間 （注） 80ms 以上の WAN 遅延では、これらの時間が大幅に長くなる可能性があります。	電話はダイヤルトーンを使用して利用可能ですが、エンドユーザー機能はアップグレードが完了するまで利用できません
IM and Presence Service データベースパブリッシャノードを非アクティブバージョンにアップグレードします	2 から 4 時間 更新アップグレードの場合は 1 時間を追加します	L2 アップグレード時は、電話サービスも IM and Presence も影響を受けません IM および Presence は更新アップグレードの場合にのみ影響を受けるはずです
IM and Presence Service サブスクライバノードを非アクティブバージョンにアップグレードする	1 から 2 時間	バージョンを切り替える間、L2 またはアップグレードの更新に関係なく、IM と Presence が影響を受けている間も電話サービスは機能し続けます
IM and Presence Service パブリッシャーノードを新しいソフトウェアバージョンに切り替えて再起動してください	30 分	IM および Presence 高可用性が無効になっています Jabber は利用できません

タスク	最小時間	サービスへの影響
IM and Presence Service サブスクライバノードを新しいソフトウェアのバージョンに切り替えて再起動してください	30 分	IM および Presence 高可用性が無効になっています Jabber は利用できません
IM and Presence Service データベースの複製	小規模クラスターまたは小規模データベースの展開の場合は 30 分 メガクラスターまたは大きなデータベースの場合は 2 時間 （注） WAN 遅延により、これらの時間が大幅に長くなる可能性があります。 許容される最大 WAN 遅延は 80m です。	IM および Presence 高可用性が無効になっています Jabber は利用できません

例

このセクションの例は、以下のアップグレードシナリオに基づいています。

- Unified Communications Manager ノードとインスタントメッセージングおよびプレゼンスノードを含むメガクラスタ
- 75,000 ユーザ
- アップグレード所要時間に影響を与える要素 （87 ページ） で記載されているように、アップグレードに向けて最適化された正常なシステム



第 6 章

アップグレード前のタスク(手動プロセス)

10.0 (1) より前のリリースからアップグレードする場合、またはアップグレード前のタスクを手動で完了する場合は、この付録の手動アップグレード前タスクを使用できます。

- アップグレード前のタスク （93 ページ）

アップグレード前のタスク

アップグレードまたは移行を開始する前に、以下のタスクを完了します。

（注） このタスクフローのステップは、特に明記されていない限り、すべてのアップグレードと移行に適用されます。

手順

	コマンドまたはアクション	目的
ステップ 1	新しいリリースのリリースノートをお読みください http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-release-notes-list.html。	新しい機能と、アップグレードがシステムに関連する他の製品とどのように相互作用するかを理解していることを確認してください。すべてのアップグレードおよび移行方法に対してこの手順を実行します。
ステップ 2	Upgrade Readiness COP ファイルの実行（アップグレード前） （54 ページ）	アップグレードの準備 COP ファイルは、アップグレードを妨げる可能性がある問題について、システムをチェックします。 （注） アップグレードの失敗の可能性を減らすために、COP ファイルを実行することを強くお勧めします。

	コマンドまたはアクション	目的
ステップ 3	スマートライセンスの要件を検討する	リリース 12.x では、Prime License Manager の代替としてスマート ライセンスが導入されています。 顧客のスマートアカウントをセットアップし、組織構造に基づいてスマートアカウントの下にバーチャル アカウント (オプション) を作成する必要があります。 Cisco Smart Account の詳細については、「https://www.cisco.com/c/en/us/buy/smart-accounts.html」を参照してください。 スマート ソフトウェア ライセンシングの詳細については、「https://www.cisco.com/c/en/us/buy/smart-accounts/software-licensing.html」を参照してください。
ステップ 4	アップグレード元のソフトウェアバージョンが仮想マシンで実行中であることを確認してください。	ソフトウェアが MCS ハードウェア上で実行されている場合、PCD 移行タスクを完了する必要があります。 http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html の「*Cisco Prime Collaboration* 導入アドミニストレーション ガイド」を参照してください。
ステップ 5	このリリースの 要件および制約事項（25 ページ） を確認してください。	システムがすべてのネットワーク、プラットフォーム、およびソフトウェア要件を満たしていることを確認してください。 すべてのアップグレードおよび移行方法に対してこの手順を実行します。
ステップ 6	ネットワークの健全性を確認します。 • アップグレード所要時間に影響を与える要素を読み、システムがこのセクションで説明されている条件を満たしていることを確認してください。 • データベース状態レポートを生成する （101 ページ） • データベース レプリケーションの確認 （102 ページ）	システムの状態はアップグレードに必要な時間に影響します。 システムがこれらのセクションで説明されている条件を満たしていることを確認することで、アップグレードに必要な時間を減らすことができます。

	コマンドまたはアクション	目的
	• パフォーマンス レポートを確認する （102 ページ） • CLI 診断の実行 （103 ページ）	
ステップ 7	証明書チェーンの信頼できる証明書も含め、パーティションに期限切れの証明書がないことを確認します。 期限切れの証明書がある場合: • 信頼証明書の削除 （104 ページ） • 証明書の再作成 （104 ページ） ID 証明書の有効期限が切れている場合。	直接アップグレードの場合、システムがすべての証明書の要件を満たしていることを確認してください。 （注） マルチサーバー（SAN）証明書の場合、SANエントリがクラスタのすべてのノードに存在することを確認します。
ステップ 8	最新のバックアップを取る （108 ページ）	システムバックアップを完了します。 注意 バックアップが古い場合、データを失ったり、システムを復元できなくなったりする可能性があります。
ステップ 9	カスタム着信音と背景画像のバックアップ （109 ページ）	TFTPディレクトリにカスタムの着信音または背景画像がある場合、これらのファイルはシステムバックアップには含まれないため、個別のバックアップを作成してください。
ステップ 10	ネットワーク接続の確認 （109ページ）	Unified Communications Manager ノードと NTP、SMTP、DNS などのネットワークサービス間の接続を確認するにはこの手順を使用します。
ステップ 11	IPv6 ネットワークの確認 （110ページ）	Unified Communications Manager ノードのみ。 パブリッシャとサブスクライバノード間の IPv6 ネットワークを確認します。 IPv6 が正しく設定されていない場合、負荷検出に 20 分かかる場合があります。
ステップ 12	IM および Presence と Cisco Unified Communications Manager 間の接続を確認する （111 ページ）	IM およびプレゼンスサービス に Unified CM との接続があることを確認します。 アップグレードの場合のみ。 移行の場合はこのタスクをスキップできます。

	コマンドまたはアクション	目的
ステップ 13	構成およびログイン情報の収集 （111 ページ）	アップグレード中に問題が発生した場合に備えて、 Unified Communications Manager ノードの現在の設定とログイン情報を記録します。
ステップ 14	登録済みデバイス数を記録する （112 ページ）	Real Time Monitoring Tool (RTMT) を使用してデバイス数をキャプチャし、アップグレードが完了した後にエンドポイントとリソースを確認できるようにします。
ステップ 15	割り当てられたユーザ数の記録 （113 ページ）	アップグレード完了後に情報を確認できるように、IMおよびプレゼンスサービス ノードに割り当てられたユーザ数を記録します。
ステップ 16	TFTP パラメータの記録 （113 ページ）	アップグレードプロセスは TFTP パラメータを変更します。アップグレードの完了後にパラメータをリセットできるように、現在の設定を記録します。
ステップ 17	エンタープライズ パラメータの記録 （113 ページ）	アップグレード中に、設定が異なる場合、IM and Presence サービスのエンタープライズパラメータ設定が Unified Communications Manager のエンタープライズパラメータ設定によって上書きされる場合があります。
ステップ 18	ユーザ レコードのエクスポート （114 ページ）	一括管理ツール (BAT) を使用してユーザレコードをエクスポートします。
ステップ 19	IP 電話ファームウェアのアップグレード （115 ページ）	アップグレード後の電話のダウンタイムを最小限に抑えるために、アップグレード前タスクとして、IP 電話を新しいリリースに対応するファームウェアにアップグレードできます。 移行の場合はこのタスクをスキップできます。
ステップ 20	重要なサービスの確認 （116 ページ）	すべての重要なサービスがアクティブになっていることを確認します。
ステップ 21	Cisco エクステンション モビリティを無効にする （116 ページ）	リリース 9.x 以前からのアップグレードのみ。 アップグレードする前に、Unified CM ノード上の Cisco エクステ

	コマンドまたはアクション	目的
		ンションモビリティサービスを停止する必要があります。 移行の場合はこのタスクをスキップできます。
ステップ 22	IM および Presence 同期エージェントを停止する （117 ページ）	IM and Presence アップグレードの一環として、Unified Communications Manager をアップグレードする場合、アップグレードする前に IM and Presence Sync Agent サービスを停止する必要があります。 移行の場合はこのタスクをスキップできます。
ステップ 23	利用可能な共通パーティションスペースの確認 （117 ページ）	アップグレードのための十分な共通パーティションスペースがあることを確認してください。 移行の場合はこのタスクをスキップできます。
ステップ 24	十分な共通パーティションのスペースがない場合、以下の手順の 1 つまたは複数を実行します。 • 高水準点と低水準点 （118ページ） • 使用可能なディスク容量を最大化する （118 ページ）	このステップは、Unified CM OS Administration インターフェイスまたは PCD アップグレードタスクのいずれかを使用してアップグレードを実行する直接アップグレードのみに行います。 **注意** 十分なディスク容量がない状態でアップグレードを実行すると、アップグレードが失敗する場合があります。
ステップ 25	アップグレードファイルを入手する （120 ページ）	必要なアップグレードファイルをダウンロードします。 更新アップグレードの場合、必要な COP ファイルもダウンロードする必要があります。 （注） Pre-12.5.x ソースからリリース 15 への更新アップグレードはサポートされていません。 移行の場合はこのタスクをスキップできます。
ステップ 26	データベースリプリケーションのタイムアウト時間を長くする （121ページ）	これはオプションです。 Unified Communications Manager パブリッ

	コマンドまたはアクション	目的
		シャーノードのみ。 大規模なクラスターをアップグレードする場合は、この手順を使用します。 移行の場合はこのタスクをスキップできます。
ステップ 27	プレゼンス冗長グループに対するハイアベイラビリティの無効化 （121 ページ）	IM and Presence サービス のみ。 高可用性が有効になっている場合、アップグレードの前に無効にします。 移行の場合はこのタスクをスキップできます。
ステップ 28	シリアルポートを仮想マシンに追加する （122 ページ）	アップグレードが失敗した場合にログをダンプできるように、仮想マシンにシリアルポートを追加します。 すべてのノードに対してこの手順を実行します。
ステップ 29	RTMT の高可用性を設定する （123 ページ）	RTMT で監視するメガクラスタ展開の場合、Cisco は、RTMT に高可用性を設定して、簡素化されたクラスタ全体のアップグレード中に接続が失われないようにすることを推奨しています。
ステップ 30	Microsoft SQL Server のアップグレードに必要なデータベースの移行 （123 ページ）	この手順は、IM and Presence Service ノードのみに適用されます。 Microsoft SQL サーバーを、IM and Presence サービスを使用して、外部データベースとしてデプロイし、11.5(1)、11.5(1)SU1、または11.5(1)SU2 にアップグレードする場合、新しい SQL サーバーデータベースを作成して、それを新しいデータベースに移行する必要があります。
ステップ 31	システムをアップグレードする前に、[Cisco Unified CM Administrationエンタープライズパラメータ（Cisco Unified CM Administration Enterprise Parameters）] ページで、**[HTTPリファラ/ホストヘッダーの信頼できるホストのリスト（Trusted List of Hosts in HTTP Referer/Host Header）]**を設定し、パブリック IP アドレスまたはDNS	この設定は、ネットワークトポロジに、クラスター内の個々のノードのプライベート IP アドレスに加えて、外部インターフェース用に設定されたパブリック IP アドレスがある場合に必要です。 Unified CM は、Unified CM へのアクセスを許可する前に、まず Unified CM クラスタで設定されたサーバーで、Host ヘッダーにある IP アドレスまたは

	コマンドまたはアクション	目的
	エイリアスを追加されたことを確認します。	ホスト名を検証するようになりました。また、ホストの信頼済みリスト設定で、Unified CM にアクセスするために使用されるDNSエイリアスを設定する必要があります。たとえば、サーバが cm1.example.local で、phone.example.local を使用してサーバにアクセスする場合、phone.example.local を信頼できるホスト一覧の設定に追加する必要があります。 Cisco Unified CM Administration ユーザーインターフェイスで、**[システム（System）] > [エンタープライズパラメータ（Enterprise Parameters）]** の順に選択し、外部IPアドレスまたは使用した DNS エイリアスを設定します。 （注） アップグレード後にこのアクティビティを実行する場合、すべてのウェブページを正しくロードするために、Cisco Tomcatサービスを再起動する必要があります。

Upgrade Readiness COP ファイルの実行（アップグレード前）

アップグレードの準備 COP ファイルは次の項目をチェックします。

- インストールされた COP ファイル
- ネットワーク サービスと接続 (DNS、NTP、クラスター内)
- ライセンスの同期
- VMware ツールの互換性
- ハードディスクパーティションサイズ
- スワップサイズチェック
- ファイルシステムタイプとゲスト OS のチェック
- 宛先バージョンに使用可能なディスク容量
- ESXi バージョン確認
- SIP および H.323 トランク登録

- データベース認証およびレプリケーションの状況
- データベースの健全性
- 最後の DRS バックアップの状況
- リモート通話コントロール (RCC) 機能の状況
- サービス状況
- インストールされている COP とロケール
- デバイス登録状態数
- エンタープライズ パラメータとサービス パラメータの設定
- TFTP 最大サービス数
- アクティブおよび非アクティブ バージョン
- 期限切れの証明書を一覧表示する
- FIPS モードのパスワードの長さの制限
- FIPS モードでの ESP および暗号化アルゴリズムの IPSec ポリシー設定確認

（注）
- アップグレードが失敗する可能性を大幅に減らすため、アップグレード前にアップグレードの準備 COP ファイルを実行することを強くお勧めします。
- COP ファイルはアップグレード前のバージョンが 10.x 以降の場合に完全にサポートされます。
- 3DES アルゴリズムは FIPS モードではサポートされていないため、3DES アルゴリズムを含む IPSec ポリシーを削除し、IPSec トンネルが確立される両方のノードで、3DES 以外の暗号化および ESP アルゴリズムを含む IPSec ポリシーを再作成する必要があります。

手順

ステップ 1 アップグレード準備COPファイルをダウンロードしてアップグレード前テストを実行します。
a) ダウンロード サイトに移動します。
b) 移動先のリリースを選択し、**[Unified Communications Manager ユーティリティ] を選択します。**
c) **アップグレード前テストを実行するために Upgrade Readiness COP ファイル**をダウンロードします（たとえば、`ciscocm.preUpgradeCheck-00019.cop.sgn`）。 最新のファイルは別のファイル名とバージョンを持つ場合があることに注意してください)。

ステップ 2 アップグレードに対してシステムの準備ができているか確認します。
a) COP ファイルを実行します。

b) COP ファイルが返す問題を解決します。
c) COP ファイルを再度実行します。
d) COP ファイルがエラーを返さなくなるまで、このプロセスを繰り返します。

ステップ 3 GUI または CLI から cop ファイルをインストールします。 インストールが完了したら、CLI から **file view install PreUpgradeReport.txt** を実行してレポートを表示します。

ステップ 4 RTMT からレポートを表示するには

a) RTMT にログインします。
b) **[Trace and Log Central]** で、**[リモートブラウザ（Remote Browse）]** をダブルクリックし、**[トレースファイル（Trace files）]** を選択したら、**[次へ（Next）]** をクリックします。
c) **[すべてのサーバー上のすべてのサービス（Select all Services on all servers）]** を選択して、**[次へ（Next）]** をクリックします。
d) **[完了（Finish）]> [閉じる（Close）]** の順に選択します。
e) ノードをダブルクリックして、**[CUCMパブリッシャ（CUCM Publisher）] > [システム（System）] > [アップグレードログのインストール（Install upgrade Logs）]** の順にします。
f) **[インストール（Install）]** をダブルクリックして、ダウンロードする必要なファイルを選択します。

データベース状態レポートを生成する

Cisco Unified Reporting Tool (CURT) を使用してデータベース ステータス レポートを生成し、クラスタ ノード間にネットワークの問題がないことを確認します。 たとえば、ノード間のデータベース レプリケーションに影響を与える、または音声およびビデオ シグナリングのサービスの質 (QoS) に影響を与える到達可能性または遅延の問題がないことを確認します。

手順

ステップ 1 ノードのレポート インターフェイスにログインします。

- Unified CM ノードについては、 Cisco Unified Reporting インターフェースにログインします。
- IM および Presence ノードについては、 Cisco Unified IM and Presence レポーティング インターフェイスにログインします。

ステップ 2 [システム レポート（System Reports）]を選択します。

ステップ 3 ノードのデータベースレプリケーションを確認します:

- Unified CM では、 **Unified CM データベースの状況**を選択します。
- IM and Presence の場合、**[IM and Presence データベース状態（IM and Presence Database Status）]** を選択します。

ステップ 4 **[レポート（Reports）]ウィンドウで、[レポートの生成]**（棒グラフ）アイコンをクリックします。

ステップ 5 **[詳細の表示（View Details）]** リンクをクリックすると、自動表示されないセクションの詳細が表示されます。

ステップ 6 レポートでエラーがあることが示されている場合、**[説明の報告（Report Descriptions）]** レポートを選択し、可能な解決策が記載されたトラブルシューティング情報を確認します。

データベース レプリケーションの確認

アップグレードを開始する前にデータベース レプリケーションが正常に機能していることを確認するには次の手順を使用します。

手順

ステップ 1 次のいずれかの方法を使用して、CLI セッションを開始します。

- リモート システムの場合は、SSH を使用して Cisco Unified オペレーティング システムにセキュアに接続します。 SSH クライアントで、**ssh *adminname@hostname*** およびパスワードを入力します。
- シリアルポートへの直接接続を介して、自動的に表示されるプロンプトでクレデンシャルを入力します。

ステップ 2 **utils dbreplication status** コマンドを実行して、データベーステーブルのエラーまたはミスマッチを確認します。

ステップ 3 **utils dbreplication runtimestate** コマンドを実行して、データベースリプリケーションがノードでアクティブであることを確認します。

出力にはすべてのノードが一覧表示されます。データベース レプリケーションがセットアップされて正常であれば、各ノードの **replication setup** の値は **2** になります。

2 以外の値が返される場合は、続行する前にエラーを解決する必要があります。

パフォーマンス レポートを確認する

手順

ステップ 1 Cisco Unified Serviceability インターフェイスから、**[ツール（Tools）]** > **[保守性レポートのアーカイブ（Serviceability Reports Archive）]** の順に選択します。

ステップ 2 リンクをクリックして、最新のレポートを選択します。

ステップ 3 **[CallActivitiesRep]** をクリックして、[コールアクティビティレポート（Call Activities Report）] を新しいタブで開き、**[呼び出し試行回数（Calls Attempted）]** が、仮想マシンの容量に対して高すぎないことを確認します。**[呼び出し試行回数（Calls Attempted）]** の数のしきい値については、https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-system/products-implementation-design-guides-list.html の *Cisco Collaboration Systems Solution Reference Network Design*（*SRND*）に記載されているシステムの推奨事項を確認してください。

ステップ 4 Cisco Unified Serviceability のインタフェースに戻り、各ノードの **PerformanceRep** リンクをクリックして、パフォーマンス保護統計レポートを表示します。

ステップ 5 各パフォーマンス保護統計レポートで、システムが展開サイズに対して指定されたクラスター全体またはノードごとの制限を超えていないことを確認します。

展開のサイズ設定については、次を参照してください。

- https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-system/products-implementation-design-guides-list.html の*Cisco Collaboration Systems Solution Reference Network Designs*（*SRND*）
- http://tools.cisco.com/cucst の Collaboration Sizing ツール。 パートナーはこのツールを使用して、顧客の設定を評価できます。

CLI 診断の実行

アップグレードを開始する前に、コマンドラインインターフェース (CLI) の診断コマンドを使用して、ネットワークの問題を診断し、解決します。

手順

ステップ 1 次のいずれかの方法を使用して、CLI セッションを開始します。

- リモート システムの場合は、SSH を使用して Cisco Unified オペレーティング システムにセキュアに接続します。 SSH クライアントで、**`ssh adminname@hostname`** およびパスワードを入力します。
- シリアル ポートへの直接接続を介して、自動的に表示されるプロンプトでクレデンシャルを入力します。

ステップ 2 **utils 診断テスト** コマンドを実行します。

このコマンドはすべての診断コマンドを実行しますが、問題の修正は試みません。 すべての診断コマンドを一覧するには、**utils diagnose list** コマンドを実行します。

ステップ 3 **utils diagnose fix** コマンドを実行すると、システムの問題の自動修正が試行されます。

信頼証明書の削除

削除できる証明書は、信頼できる証明書だけです。 システムで生成される自己署名証明書は削除できません。

⚠

注意 証明書を削除すると、システムの動作に影響する場合があります。 また、証明書が既存のチェーンの一部である場合、証明書チェーンが壊れることがあります。 この関係は、**[証明書の一覧（Certificate List）]** ウィンドウ内の関連する証明書のユーザ名とサブジェクト名から確認します。 この操作は取り消すことができません。

手順

ステップ 1 Cisco Unified OS の管理から、**[セキュリティ（Security）] > [証明書の管理（Certificate Management）]** を選択します。

ステップ 2 証明書の一覧をフィルタするには、**[検索（Find）]** コントロールを使用します。

ステップ 3 証明書のファイル名を選択します。

ステップ 4 [削除（Delete）]をクリックします。

ステップ 5 **OK**をクリックします。

（注）
- 削除する証明書が 「CAPF-trust」、「tomcat-trust」、「CallManager-trust」、または「Phone-SAST-trust」 証明書タイプの場合、証明書はクラスタ内のすべてのサーバで削除されます。
- 電話機のエッジトラストからの証明書の削除は、発行元から行う必要があります。
- 証明書を CAPF-trust にインポートする場合、それはその特定のノードでのみ有効になり、クラスタ全体で複製されることはありません。

証明書の再作成

アップグレードを開始する前に、証明書チェーン内の信頼できる証明書を含め、パーティションに期限切れの証明書がないことを確認してください。 証明書が期限切れの場合は、再作成します。 電話機を再起動してサービスを再起動する必要があるため、営業時間後にこの手順を実行します。 Cisco Unified OS の管理に 「cert」 タイプとしてリストされている証明書のみ再作成できます。

（注） Pre-12.5.x から リリース 15 へのアップグレードの更新はサポートされていません。

（注） アップグレード中、ITLRecovery 証明書はクラスターごとに生成されます。 クラスタが混合モードの場合は、CTL ファイルを手動で更新します。 電話をリセットして最新の更新を反映します。 これは更新アップグレードにのみ適用できます。 リリース 12.5(1)SU3 更新以降は、CTL が不要になりました。

注意 証明書を再生成すると、システムの動作に影響する場合があります。 証明書を再作成すると、サードパーティの署名付き証明書（アップロードされている場合）を含む既存の証明書が上書きされます。

手順

ステップ 1 Cisco Unified OS の管理から、**[セキュリティ（Security）]** > **[証明書の管理（Certificate Management）]** を選択します。

検索パラメータを入力して、証明書を検索して設定の詳細を表示します。 すべての条件に一致したレコードが [**Certificate List**] ウィンドウに表示されます。

証明書の詳細ページで**[再生成（Regenerate）]**ボタンをクリックすると、同じキー長を持つ自己署名証明書が再生成されます。

（注） 証明書を再生成した場合、**[再生成（Regeneration）]** ウィンドウを閉じて、新しく生成された証明書を開くまで、**[証明書の説明（Certificate Description）]** フィールドは更新されません。

3072 または 4096 の新しいキー長の自己署名証明書を再生成するには、[**自己署名証明書の生成（Generate Self-Signed Certificate**）] をクリックします。

ステップ 2 [**自己署名証明書の新規作成（Generate New Self-Signed Certificate**）] ウィンドウのフィールドを設定します。 フィールドおよびその設定オプションの詳細については、オンライン ヘルプを参照してください。

ステップ 3 [Generate]をクリックします。

ステップ 4 再作成された証明書の影響を受けるサービスをすべて再起動します。 詳細については、証明書の名前と説明 （106 ページ）を参照してください。

ステップ 5 CAPF、ITLRecovery 証明書または CallManager 証明書の再生成後に CTL ファイルを更新します（設定している場合）。

（注） 証明書を再作成したら、システムのバックアップを実行して、最新のバックアップに再作成した証明書が含まれるようにします。 バックアップに再作成した証明書が含まれていない状態でシステムの復元タスクを実行する場合は、システム内の各電話機のロックを手動で解除して、電話機を登録できるようにする必要があります。

重要 CallManager、CAPF、TVS 証明書の再生成/更新後に、更新された ITL ファイル を受信するために、電話機は自動的にリセットされます。

次のタスク

証明書を再作成したら、システムのバックアップを実行して、最新のバックアップに再作成した証明書が含まれるようにします。

関連トピック

証明書の名前と説明 （106 ページ）

証明書の名前と説明

次の表に、再作成可能なシステムのセキュリティ証明書と、再起動する必要がある関連サービスを示します。 TFTP 証明書の再作成の詳細については、http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html の『*Cisco Unified Communications Manager Security Guide*』を参照してください。

表 *12*：証明書の名前と説明

名前	説明	再起動が必要なサービス
tomcat tomcat-ECDSA	この証明書は、SIP Oauth モードが有効になっているときに Web サービス、Cisco DRF サービス、および Cisco CallManager サービスで使用されます。	（注） 以下に記載されているサービスの再起動は、リリース 14 以降に適用されます。 Cisco Tomcat サービス、Cisco Disaster Recovery System（DRS）ローカルサービスおよびマスターサービス、Cisco UDS Tomcat、および Cisco AXL Tomcat Web サービス。 SAML SSO が Tomcat 証明書で有効になっている場合は、IDP で SP メタデータを再プロビジョニングする必要があります。
ipsec	この自己署名ルート証明書は、ユニファイドコミュニケーション マネージャ、MGCP、H.323、IM およびプレゼンス サービスとの IPsec 接続のインストール中に生成されます。	IPSec サービス。

名前	説明	再起動が必要なサービス
CallManager CallManager-ECDSA	これはSIP、SIP トランク、SCCP、TFTP などに使用されます。	重要　リリース 14 では、次のサービスを再起動します。 • Cisco Call Manager Service およびその他の関連サービス（Cisco CTI Manager、HAProxy Service など）- サーバーがセキュアモードの場合、CTL ファイルを更新します。 重要　以下に記載されているサービスの再起動は、リリース 14 SU1 以降に適用されます。 • CallManager：HAProxy サービス - サーバーがセキュアモードの場合、CTL ファイルを更新します。 • CallManager-ECDSA：Cisco CallManager サービスおよび HAProxy サービス。
CAPF	Unified Communications Manager Publisherで実行されている CAPF サービスによって使用されます。この証明書は、エンドポイントに LSC を発行するために使用されます (オンラインとオフラインの CAPF モードを除く)。	該当なし
TVS	これはTrust検証サービスで使用されます。これは、サーバ証明書が変更された場合に電話機のセカンダリ信頼検証メカニズムとして機能します。	該当なし

（注）

- TVS、CAPF、またはTFTP証明書のいずれかを更新した場合に、手動または自動で電話機をリセットするには、証明書の更新に関する新しいエンタープライズパラメータの電話機の相互操作を導入します。 このパラメータは、デフォルトで電話機を自動的にリセットするために設定されています。
- 証明書の再生成、削除、更新後に、「再起動するサービス」の列で説明されているサービスを必ず再起動してください。

重要 この注意事項は、リリース 14SU2 以降に適用されます。

CLI 経由の複数 SAN 証明書のアップロードはサポートしていません。 これらの証明書は、常に OS 管理 GUI 経由でアップロードする必要があります。

最新のバックアップを取る

アップグレードを実行する前にシステムをバックアップして、バックアップファイルが現在インストールされているソフトウェアと完全に一致していることを確認する必要があります。現在のバージョンと一致しないバックアップファイルからシステムを復元しようとすると、復元は失敗します。

すべてのアップグレードおよび移行方法に対してこの手順を実行してください。

注意 バックアップが古い場合、データを失ったり、システムを復元できなくなったりする可能性があります。

始める前に

- バックアップ ファイルの格納場所としてネットワーク デバイスを使用していることを確認します。 Unified Communications Manager の仮想化された展開では、バックアップファイルを保存するためのテープドライブの使用はサポートされていません。
- システムがバージョン要件を満たしていることを確認します。
  - すべての Unified Communications Manager クラスタノードは、同じバージョンのアプリケーション Unified Communications Manager を実行している必要があります。
  - すべての IM and Presence Service クラスタノードは、同じバージョンの IM and Presence Service アプリケーションを実行する必要があります。

各アプリケーションについて、バージョン文字列全体が一致している必要があります。たとえば、IMおよびPresenceデータベースパブリッシャノードのバージョンが11.5.1.10000-1である場合、すべての IM および Presence サブスクライバノードは 11.5.1.10000-1 である

必要があり、バージョン 11.5.1.10000-1 のバックアップ ファイルを作成する必要があります。

- バックアップ プロセスは、リモート サーバに利用可能な容量がないためや、ネットワーク接続が中断されたために失敗することがあります。バックアップが失敗する原因となった問題に対処した後、新規のバックアップを開始する必要があります。
- クラスタ セキュリティ パスワードのレコードがあることを確認します。 このバックアップの完了後に、クラスタ セキュリティ パスワードを変更した場合は、パスワードを認識している必要があります。パスワードを認識していないと、バックアップ ファイルを使用してシステムを復元できなくなります。

手順

ステップ 1 ディザスタ リカバリ システムから、**[バックアップ（Backup）]>[手動バックアップ（Manual Backup）]** の順に選択します。

ステップ 2 [手動バックアップ（Manual Backup）] ウィンドウで、[バックアップ デバイス名（Backup Device Name）] 領域を選択します。

ステップ 3 [機能の選択（Select Features）] 領域から機能を選択します。

ステップ 4 [バックアップの開始（Start Backup）] をクリックします。

カスタム着信音と背景画像のバックアップ

TFTP ディレクトリにカスタムの着信音または背景画像がある場合、これらのファイル用に別のバックアップを作成する必要があります。 これらは Disaster Recovery System (DRS) バックアップファイルには含まれません。

手順

ステップ 1 ウェブブラウザまたは TFTP クライアントを使って、着信音と背景画像が保存されているディレクトリにアクセスします。

ステップ 2 次のファイルをバックアップします: `Ringlist.xml` および `List.xml`

ステップ 3 カスタム着信音をバックアップします。 これらは TFTP ディレクトリにあります。

ステップ 4 背景画像をバックアップします。 これらは TFTP ディレクトリの `/Desktops` フォルダおよびそのサブフォルダにあります。

ネットワーク接続の確認

この手順を使用して、ネットワーク内のすべてのノードとサービス間の接続を確認します。

手順

ステップ 1 次のいずれかの方法を使用して、CLI セッションを開始します。

- リモート システムの場合は、SSH を使用して Cisco Unified オペレーティング システムにセキュアに接続します。 SSH クライアントで、**ssh *adminname@hostname*** およびパスワードを入力します。
- シリアル ポートへの直接接続を介して、自動的に表示されるプロンプトでクレデンシャルを入力します。

ステップ 2 ネットワーク内の各ノードで **show network cluster** コマンドを実行し、クラスタ内の Unified Communications Manager サーバー間の通信を確認する。

ステップ 3 NTP サーバーがある場合、**utils ntp status** コマンドを実行して NTP サーバーへの接続を確認します。

ステップ 4 SMTP サーバがある場合は、サーバに ping を送信して接続を確認します。

ステップ 5 DNS を使用している場合、ネットワークの各ノードで **show network eth0** コマンドを実行し、DNS とドメインが設定されていることを確認します。

ステップ 6 DNS 名前解決が正しく機能していることを確認します。

a) 各ノード Unified Communications Manager の FQDN を ping して、IP アドレスに解決されることを確認します。

b) 各 Unified Communications Manager の IP アドレスを ping して、FQDN が解決しているか確認します。

IPv6 ネットワークの確認

この手順は Unified Communications Manager ノードにのみ適用されます。

最初のノード（Unified Communications Manager データベース パブリッシャノード）と Unified Communications Manager サブスクライバノードで IPv6 ネットワーキングが有効になっていることを確認します。 Unified Communications Manager サブスクライバノードで IPv6 が正しく設定されていない場合、負荷検出に 20 分かかる場合があります。

手順

ステップ 1 次のいずれかの方法を使用して、CLI セッションを開始します。

- リモート システムの場合は、SSH を使用して Cisco Unified オペレーティング システムにセキュアに接続します。 SSH クライアントで、**ssh *adminname@hostname*** およびパスワードを入力します。
- シリアル ポートへの直接接続を介して、自動的に表示されるプロンプトでクレデンシャルを入力します。

ステップ 2 **utils network ipv6 ping***destination [count]* のコマンドを入力します。

- 宛先 は ping を実行する有効な IPv6 アドレスまたはホスト名です
- *count* は外部サーバを ping する回数です。 デフォルトは 4 です。

IM および Presence と Cisco Unified Communications Manager 間の接続を確認する

IM and Presence Service サービスノードが Unified Communications Manager と接続していることを確認します。

手順

ステップ 1 Cisco Unified CM IM and Presence Administration インターフェイスで、**[診断（Diagnostics）]** > **[システムトラブルシューター（System Troubleshooter）]** の順に選択します。
システムはトラブルシューティングの確認を自動的に実行します。

ステップ 2 トラブルシューティング チェックの結果が読み込まれたら、すべての **Sync Agent トラブルシューター**テストの**結果**列にテストに合格したことを示すに緑色のチェックマークが付いていることを確認します。

ステップ 3 **Sync Agent トラブルシューター**テストのいずれかが不合格だった場合、**[問題（Problem）]** 列と**[ソリューション（Solution）]** 列の情報を参照して、アップグレードプロセスを続行する前に問題を解決します。

構成およびログイン情報の収集

アップグレードプロセス中に問題が発生した場合に備えて、Unified Communications Manager ノードの現在の設定とログイン情報を記録しておきます。

手順

ステップ 1 次のログインとパスワード情報を記録します。

- すべてのアプリケーション ユーザの資格情報 (DRS、AXL、その他のサードパーティ連携のアカウントなど)
- 管理者、クラスターセキュリティ、および証明書信頼リスト(CTL)セキュリティトークンパスワード

ステップ 2 ネットワーク設定に関する次の情報を記録します。

- IP アドレス、ホスト名、ゲートウェイ、ドメイン名、DNS サーバ、NTP サーバ、通話詳細録音 (CDR) サーバ、および SMTP 情報
- サーババージョンおよびタイムゾーン
- 各サーバで実行されているサービス、および関連するアクティベーション ステータス
- LDAP 情報およびアクセスの詳細
- SNMP 情報

登録済みデバイス数を記録する

アップグレードを開始する前に、Real Time Monitoring Tool (RTMT) を使用してデバイス数をキャプチャし、アップグレードが完了した後でエンドポイントとリソースを確認できるようにします。 この情報を使用して、展開している仮想マシン (VM) の容量を超過していないことを確認することもできます。

手順

ステップ 1 Unified RTMT インターフェイスから、**[CallManager]** > **[デバイス（Device）]** > **[デバイスの概要（Device Summary）]** の順に選択します。

ステップ 2 各ノードの登録済みデバイスの数を記録します。

項目	カウント
登録済みの電話機（Registered Phones）	
FSX	
FSO	
T1 CAS	
PRI	
MOH	
MTP	
CFB	
XCODE	

割り当てられたユーザ数の記録

アップグレードが完了した後に確認できるように、IM and Presence サービスノードに割り当てたユーザー数を記録します。

手順

ステップ 1 Cisco Unified CM IM and Presence の管理インターフェイスから、 **システム** > **クラスタートポロジ**を選択します。
[Cluster Topology Details] ページには、ノードおよびサブクラスタに関する情報が表示されます。

ステップ 2 各ノードとクラスターに割り当てられているユーザの数を記録します。

TFTP パラメータの記録

アップグレード中に、TFTP サービスパラメータ **Maximum Serving Count** が変更され、より多くのデバイス登録要求に対応できるようになります。アップグレードの完了後にパラメータをリセットできるように、既存の設定を記録します。

手順

ステップ 1 Cisco Unified CM Administration インターフェイスで、**[システム（System）]** > **[サービスパラメータ（Service Parameters）]** の順に選択します。

ステップ 2 [**サーバ**] ドロップダウンリストから、TFTP サービスを実行しているノードを選択します。

ステップ 3 **サービス** ドロップダウンリストから **Cisco TFTP サービス**を選択します。

ステップ 4 [詳細設定（Advanced）]をクリックします。

ステップ 5 **[保存（Save）]** をクリックします。

ステップ 6 **[最大サービングカウント（Maximum Serving Count）]** で設定した値を記録します。

エンタープライズ パラメータの記録

Unified Communications Manager ノードと IM and Presence Service サービスノードの両方でエンタープライズパラメータの設定を記録します。 一部のエンタープライズパラメータが Unified Communications Manager ノードと IM and Presence Service サービスノードの両方に存在しています。 同じパラメータが存在する場合、Unified Communications Manager ノードで構成した設定は、アップグレード中に IM and Presence Service サービスノードで構成した設定を上書きします。 IM and Presence Service サービスノードに固有のエンタープライズパラメータは、アップグレード中も保持されます。

アップグレードの完了後に必要に応じて復元できるように、設定を記録します。

手順

ステップ 1 Cisco Unified CM Administration インターフェイスで、**[システム（System）]** > **[エンタープライズパラメータ（Enterprise Parameters）]** の順に選択します。

ステップ 2 画面をキャプチャして構成した設定を記録し、アップグレード完了後に設定を復元できるように情報を保存します。

ステップ 3 Cisco Unified CM IM and Presence Administration インターフェイスで、**[システム（System）]** > **[エンタープライズパラメータ（Enterprise Parameters）]** の順に選択します。

ステップ 4 画面をキャプチャして構成した設定を記録し、アップグレード完了後に設定を復元できるように情報を保存します。

ユーザ レコードのエクスポート

一括管理ツール (BAT) を使用してユーザレコードをエクスポートします。

手順

ステップ 1 Cisco Unified CM Administration から、**[一括管理（Bulk Administration）]** > **[ユーザ（Users）]** > **[ユーザのエクスポート（Export Users）]** の順に選択します。

ステップ 2 すべてのユーザ記録を表示するには、[**検索**] をクリックします。

ステップ 3 [次へ（Next）]をクリックします。

ステップ 4 **[ファイル名（File Name）]** テキストボックスにファイル名を入力し、**[ファイル形式（File Format）]** ドロップダウンメニューでファイル形式を選択します。

ステップ 5 **[ジョブ情報(Job Information)]** 領域に、ジョブの説明を入力します。

ステップ 6 **今すぐ実行** をクリックしてユーザ記録をすぐにエクスポートします

ステップ 7 [送信（Submit）]をクリックします。

ステップ 8 エクスポートしたファイルをダウンロードするには、[**一括管理** > **ファイルのアップロード/ダウンロード**] を選択します。

ステップ 9 生成したファイルの検索条件を入力し、**[検索（Find）]** をクリックします。

ステップ 10 ダウンロードするファイルのチェックボックスをオンにして、**[選択したファイルをダウンロード（Download Selected）]** をクリックします。

ステップ 11 [ファイルのダウンロード] ポップアップウィンドウで、[保存] **をクリックします**。

ステップ 12 [名前を付けて保存] ポップアップウィンドウで、ファイルを保存する場所を選択し、[保存] **をクリックします**。 サーバからファイルをコピーして、リモート PC またはデバイスに保存していることを確認してください。

IP 電話ファームウェアのアップグレード

アップグレード前タスクとして、IP電話を新しいリリースに対応するファームウェアにアップグレードできます。電話機はアップグレード後に新しいファームウェアを自動的にダウンロードしますが、アップグレード後の電話機のダウンタイムを最小限に抑えるために、アップグレード前に制御された方法でエンドポイントに新しいファームウェアファイルを適用することもできます。

グループの電話機に新しいファームウェアを適用する場合、アップグレード後の TFTP サーバの負荷を排除し、個々のデバイスのアップグレードを加速させることができます。 その後、Unified Communications Manager サーバの TFTP サービスを再起動し、ダウンタイムを最小限に抑えるために制御された順序で IP 電話を再起動します。 ファームウェアのアップグレード中は電話を通話に使用できないため、アップグレード ウィンドウ外のメンテナンス ウィンドウを使用して、電話のファームウェアをアップグレードすることを推奨します。

始める前に

- TFTP サーバー（/usr/local/cm/tftp）の次のデータベースリプリケーションに新しいファームウェアロードをコピーします。
- IP 電話と登録済みエンドポイントのシステム デフォルト設定とデバイスごとの割り当てを記録します。

手順

ステップ 1 Cisco Unified OS の管理から、**[ソフトウェア アップグレード（Software Upgrades）] > [インストール/アップグレード（Install/Upgrade）]** の順に選択します。

ステップ 2 ソフトウェアの場所セクションに適切な値を入力し、[**次へ（Next）**] をクリックします。

ステップ 3 [**使用可能なソフトウェア（Available Software**）] ドロップダウン リストで、デバイス パッケージ ファイルを選択して、[**次へ（Next**）] をクリックします。

ステップ 4 MD5 の値が正しいことを確認し、[**次へ（Next**）] をクリックします。

ステップ 5 警告ボックスで、正しいファームウェアを選択したことを確認し、[**インストール（Install**）] をクリックします。

ステップ 6 成功メッセージを受信したことを確認します。

（**注**） クラスタを再起動している場合は、ステップ 8 に進みます。

ステップ 7 TFTP サーバーを停止し、再起動します。

ステップ 8 新しいロードにデバイスをアップグレードするには、影響を受けたデバイスをリセットします。

ステップ 9 Cisco Unified CM Administration で、**[デバイス（Device）] > [デバイス設定（Device Settings）] > [デバイスのデフォルト（Device Defaults）]** の順に選択し、TFTP サーバー上の新しいロードに対する特定の [デバイスタイプ（Device Type）] フィールドで、「ロード情報」と「非アクティブロード情報」の名前を手動で変更します。

ステップ 10 [保存（Save）]をクリックし、デバイスをリセットします。

重要なサービスの確認

Cisco Unified Real Time Monitoring Tool (RTMT) を使用して、すべての重要なサービスがアクティブになっていることを確認します。

手順

ステップ 1 Unified RTMT インターフェイスで、**[システム（System）]** > **[サーバー（Server）]** > **[重要サービス（Critical Services）]** の順に選択します。

ステップ 2 システムの重要なサービスを表示するには、[システム（System）]タブを選択します。

ステップ 3 Unified Communications Manager 重要サービスを表示するには、ドロップダウンメニューで、Unified Communications Manager ノードを選択し、**[音声/ビデオ（Voice/Video）]** タブをクリックします。

ステップ 4 IM and Presence サービスの重要サービスを表示するには、**[IM and Presence]** タブをクリックして、ドロップダウンメニューで、[IM and Presence Service サービスノード（Service node）] を選択します。

ステップ 5 重要なサービスが停止していることが状況に示されている場合は、アップグレードを開始する前に再アクティベートしてください。

Cisco エクステンション モビリティを無効にする

リリース 9.x 以前からアップグレードする場合にのみ、この手順を実行します。 リリース 9.x 以前からのアップグレードの場合、アップグレードを開始する前に Unified Communications Manager ノードで Cisco エクステンションモビリティを停止する必要があります。

手順

ステップ 1 Cisco Unified Serviceability から、**[ツール（Tools）]** > **[サービスの有効化（Service Activation）]** を選択します。

ステップ 2 [サーバ（Server）]リストから、サービスを非アクティブ化するノードを選択し、[移動（Go）]をクリックします。

ステップ 3 **Cisco エクステンション モビリティ** サービスの選択を解除します。

ステップ 4 [Stop]をクリックします。

ステップ 5 **Cisco Extension Mobility** サービスを実行している各ノードに対して、ステップ 2 ～ 4 を繰り返します。

ステップ 6 これらのサービスを無効にしたすべてのノードのリストを作成します。 アップグレードが完了したら、サービスを再起動する必要があります。

IM および Presence 同期エージェントを停止する

IM and Presence Service アップグレードの一環として Unified Communications Manager をアップグレードする場合、アップグレードプロセスを開始する前に、IM and Presence Service Sync Agen サービスを停止する必要があります。

手順

ステップ 1 Cisco Unified Serviceability インターフェースから **[ツール]** > **Control Center - [ネットワークサービス]** の順に選択します。

ステップ 2 **[サーバー（Server）]** ドロップダウンメニューで IM and Presence Service サービスノードを選択し、**[移動（Go）]** をクリックします。

ステップ 3 **[IMおよびPresence サービス（IM and Presence Services）]** セクションで、**[Cisco Sync Agent]** を選択して、**[停止（Stop）]** をクリックします。

利用可能な共通パーティションスペースの確認

リアルタイム監視ツール (RTMT) を使用して、アップグレードのための十分な共通パーティションのスペースがあることを確認します。

手順

ステップ 1 Real-Time Monitoring Tool の左にあるナビゲーションペインにある、**[システム（System）]** カウンターのリストで、**[ディスク使用量（Disk Usage）]** を選択します。
ページにディスク使用量に関する詳細情報が表示されます。

ステップ 2 ページ下部の表を表示し、共通パーティションの **[合計容量（Total Space）]** と**[使用済み容量（Used Space）]** を比較します。 アップグレードを開始する前に、最低 25G の共通パーティションスペースが必要です。 ただし、多数の TFTP データ (デバイスファームウェアのロード)、保留音 (MOH) ファイルがある場合、または多くのロケールファイルがインストールされている場合は、展開により多くのスペースが必要になる場合があります。 場合によっては、25GB の空き容量がある場合でも、アップグレードが失敗し、容量が不十分であるというエラーメッセージが表示されることがあります。回避策は、不要なファイルを削除し、共通パーティションにより多くの容量を作成することです。

高水準点と低水準点

この手順を使用して最低水準点と最高水準点を調整し、トレースを減らし、不要なログファイルを削除します。アップグレード後、トレースの早過ぎる消去を避けるために、最高水準点と最低水準点を元の値に復元する必要があります。 最高水準点のデフォルト値は 85 です。最低水準点のデフォルト値は 80 です。

手順

ステップ 1 Real Time Monitoring Tool（RTMT）インタフェースの左側ナビゲーションペインで、**[Alert Central]** をダブルクリックします。

ステップ 2 **[システム（System）]** タブで、**[LogPartitionLowWaterMarkExceeded]** を右クリックしたら、**[アラート/プロパティの設定（Set Alert/Properties）]**を選択します。

ステップ 3 [次へ（Next）]を選択します。

ステップ 4 スライダの値を 30 に調整します。

ステップ 5 **[システム（System）]** タブで、**[LogPartitionHighWaterMarkExceeded]** を右クリックしたら、**[アラート/プロパティの設定（Set Alert/Properties）]**を選択します。

ステップ 6 [次へ（Next）]を選択します。

ステップ 7 スライダの値を 40 に調整します。

使用可能なディスク容量を最大化する

11.5(X) から 12.5 にアップグレードする場合、ダウンロードが必要な COP ファイルを検証します。 COP ファイルと Readme ファイルをダウンロードするには、https://software.cisco.com に移動し、> **[ダウンロードとアップグレード（Download & Upgrade）]** セクションの **[ソフトウェアのダウンロード（Software Download）]** リンクをクリックし、,**[Unified Communications]** > **[呼制御（Call Control）]** > **[Cisco Unified Communications Manager（CallManager）]** > ***<Version>*** > **[Unified Communications Manager/CallManager/Cisco Unity Connection Utilities]** の順に選択します。

共通パーティションに追加のスペースを作成するには、この手順の 1 つまたはそれ以上を実行できます。

現在のバージョンが、11.5(x) より前のバージョンからのアップグレードにシリアル接続を使用していた場合、古い OS パーティションスキームと仮想ディスクレイアウトになっている可能性があります。 これにより「ディスクスペース不足」の問題が増幅され、仮想ディスクスペースを追加する効果が制限されます。 アップグレード準備 COP ファイルはこれらの問題をチェックし、それらを解決する方法に関するガイダンスを提供します。

手順

ステップ 1 以下のいずれかのオプションを使用して、古いまたは未使用のファームウェアファイルを TFTP ディレクトリから手動で削除します。

- Cisco Unified OS Administration で、**[ソフトウェアアップグレード（Software Upgrades）]** > **[TFTP ファイル管理]** の順に選択し、不要なファイルを削除します。
- コマンドライン インターフェイスで、`[file list tftp]` コマンドと `[file delete tftp]` コマンドを使用して不要なファイルを削除します。
- Cisco Unified OS の管理インターフェイスから、[**ソフトウェアのアップグレード** > **デバイス負荷管理**] を選択し、不要なファイルを削除します。

（注） **show diskusage tftp <sort>** コマンドを実行して、tftp デバイスの負荷サイズをファイルサイズの降順にソートして確認します。

show diskusage common <sort> コマンドを実行して、共通パーティションの利用可能サイズと空き容量をファイルサイズの降順にソートして確認します。

ステップ 2 これまでの手順でアップグレードに必要なディスク容量が作成されなかった場合にのみ、この手順を実行します。 Free Common Space COP ファイル (ciscocm.free_common_space_v<latest_version>.cop.sgn) を使用してください。

この COP ファイルは、システムを再構築することなく、利用可能なディスクスペースを増やすために、共通パーティションの非アクティブ側を削除します。 続行する前に、この COP ファイルをサポートする Readme ファイルを確認してください。

（注） 非アクティブパーティションは使用できなくなるため、このファイルをインストールした後は非アクティブバージョンに切り替えることができなくなります。

（注） 110G または 2 つの 80G ディスク展開の場合、アップグレードに利用できるスペースは、アクティブパーティションのディスクスペースの少なくとも 2 倍である必要があります。 たとえば、2 つの 80G ディスク展開では、アクティブなパーティションは 25G を超えてはならず、利用可能なスペースは少なくとも 50G でなければなりません。 ディスク使用率を確認するためのコマンドは以下の通りです。

1. **show diskusage activelog <sort>** コマンドを実行して、ファイルサイズの大きい順にソートされているアクティブ側のパーティションサイズを確認します。
2. **show diskusage common <sort>** コマンドを実行して、共通パーティションの利用可能サイズと空き容量をファイルサイズの降順にソートして確認します。
3. **show diskusage tftp <sort>** コマンドを実行して、tftp デバイスの負荷サイズをファイルサイズの降順にソートして確認します。
4. **file delete activelog <filename>** コマンドを実行してアクティブなパーティションからログを削除します。

アップグレードファイルを入手する

新しいリリースのアップグレード ファイルと、必要なアップグレード Cisco オプション パッケージ (COP) ファイルをダウンロードする必要があります。

手順

ステップ 1 必要に応じて、この手順の下の表を参照して、必要な COP ファイルを特定します。

ステップ 2 Cisco.com からアプリケーションのアップグレードファイルをダウンロードしてください。 このソフトウェアには輸出制限版 (K9) および輸出制限なしバージョン (XU) があります。正しいファイルを選択していることを確認してください。

- Unified Communications Manager アップグレードファイルをダウンロードするには、https://software.cisco.com に移動して、>**[ダウンロードおよびアップグレード（Download & Upgrade）]** セクションにある**[ソフトウェアをダウンロード（Software Download）]** リンクをクリックし、**[Unified Communications]** > **[呼制御（Call Control）]** > **[Cisco Unified Communications Manager（CallManager）]** > **<*Version*>** > **[Unified Communications Manager/CallManager/Cisco Unity Connectionの更新（Unified Communications Manager/CallManager/Cisco Unity Connection Updates）]** の順に選択します。
- IM and Presence Service サービス アップグレード ファイルをダウンロードするには、https://software.cisco.com に移動し、> **[ダウンロードとアップグレード（Download & Upgrade）]** セクションにある **[ソフトウェアをダウンロード（Software Download）]** リンクをクリックし、**[Unified Communications]** > **[Unified Communicationsアプリケーション]** > **[Presenceソフトウェア（Presence Software）]** > **[Unified Communications Manager IMおよびプレゼンスサービス（Unified Communications Manager IM and Presence Service）]** > **<*Version*>** > **[Unified Presence Service（CUP）の更新（Unified Presence Service (CUP) Updates）]** の順に選択します。

ステップ 3 https://software.cisco.com に移動し、> **[ダウンロードとアップグレード（Download & Upgrade）]** セクションにある **[ソフトウェアをダウンロード（Software Download）]** リンクをクリックし、**[Unified Communications]** > **[呼制御（Call Control）]** > **[Cisco Unified Communications Manager（CallManager）]** > **<*Version*>** > **[Unified Communications Manager/CallManager/Cisco Unity Connection Utilities]** の順に選択し、Unified Communications Manager に COP ファイルをダウンロードします。

ステップ 4 https://software.cisco.com に移動し、> **[ダウンロードとアップグレード（Download & Upgrade）]** セクションにある **[ソフトウェアをダウンロード（Software Download）]** リンクをクリックし、**[Unified Communications]** > **[Unified Communicationsアプリケーション]** > **[Presenceソフトウェア（Presence Software）]** > **[Unified Communications Manager IMおよびプレゼンスサービス（Unified Communications Manager IM and Presence Service）]** > **<*Version*>** > **[Unified Presence Service（CUP）更新]** の順に選択し、**[UTILS]** を選択して、IMおよびプレゼンスサービスに COP ファイルをダウンロードします。

必要な COP ファイル

下の表は COP ファイルを必要とするアップグレードパスの一覧です。 Cisco Unified OS Admin インターフェイスを使用してアップグレードを開始する前、または Prime Collaboration Deployment (PCD) ツールを使用してアップグレードまたは移行を開始する前に、各ノードに COP ファイルをインストールする必要があります。 PCD を使用している場合、アップグレードを開始する前に、COP ファイルの一括インストールを実行できます。

必要な COP ファイルの詳細は、「*COP* ファイルでサポートされているアップグレードおよび移行パス 」のセクションを参照してください。

データベースリプリケーションのタイムアウト時間を長くする

Unified Communications Manager パブリッシャーノードでのみこの手順を実行します。

大規模なクラスタをアップグレードする際に、データベースレプリケーションのタイムアウト値を増やしてください。これにより、 Unified Communications Manager より多くのサブスクライバノードがレプリケーションをリクエストするための十分な時間が与えられます。 タイマーが切れると、最初の Unified Communications Manager サブスクライバノード、およびその期間内にレプリケーションをリクエストした他のすべての Unified Communications Manager サブスクライバノードが、Unified Communications Manager データベース パブリッシャノードとのバッチデータのレプリケーションを開始します。

手順

ステップ 1 次のいずれかの方法を使用して、CLI セッションを開始します。

- リモート システムの場合は、SSH を使用して Cisco Unified オペレーティング システムにセキュアに接続します。 SSH クライアントで、**ssh *adminname@hostname*** およびパスワードを入力します。
- シリアル ポートへの直接接続を介して、自動的に表示されるプロンプトでクレデンシャルを入力します。

ステップ 2 **utils dbreplication setrepltimeout***timeout* コマンドを実行します。ここの *timeout* は、秒単位のデータベースリプリケーション タイムアウトです。 値が 300 から 3600 の間であることを確認してください。

デフォルトのデータベース複製のタイムアウト値は 300 (5 分) です。

プレゼンス冗長グループに対するハイ アベイラビリティの無効化

この手順は、IM and Presence Service サービス ノードにのみ適用されます。 IM and Presence Service プレゼンス冗長グループのハイ アベイラビリティを無効にするために使用します。

始める前に

各プレゼンス冗長グループの各クラスタノードに割り当てられたアクティブユーザ数を記録します。 この情報は、[Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）] の **[システム（System）]** > **[プレゼンス トポロジ（Presence Topology）]** ウィンドウで見つけることができます。 後で高可用性を再度有効にするときに、この情報が必要になります。

手順

ステップ 1 Cisco Unified CM Administration のユーザ インターフェイスから、**[システム（System）]** > **[プレゼンス冗長グループ（Presence Redundancy Groups）]** を選択します。

ステップ 2 **検索**をクリックしてグループを選択します。

ステップ 3 [プレゼンス冗長グループの設定（Presence Redundancy Group Configuration）] ウィンドウで、[ハイ アベイラビリティを有効にする（Enable High Availability）]チェックボックスをオフにします。

ステップ 4 **[保存]** をクリックします。

ステップ 5 各プレゼンス冗長グループに対してこの手順を繰り返します。

ステップ 6 完了したら、さらに変更を加える前に、新しいHA設定がクラスタ全体にわたって同期されるまで、少なくとも 2 分待機します

シリアルポートを仮想マシンに追加する

シリアルポートを仮想マシンに追加して、アップグレードが失敗した場合にログをダンプできるようにします。

手順

ステップ 1 仮想マシンの電源をオフにします。

ステップ 2 設定を編集してシリアルポートを追加します。 vSphere Client を使用した構成変更の詳細については、製品のユーザマニュアルを参照してください。

ステップ 3 シリアルポートを .tmp ファイルに添付します。

ステップ 4 仮想マシンの電源をオンにして、アップグレードを続行します。

次のタスク

システムのアップグレードに成功したら、シリアルポートを削除する （132 ページ） の手順に従ってください。 アップグレードに失敗した場合は、「アップグレード失敗後にログファイルをダンプする （151 ページ）」を参照してください。

RTMT の高可用性を設定する

Cisco Unified Real-Time Monitoring Tool (RTMT) を使用し、メガクラスタを展開する場合、Cisco は、RTMT に高可用性を設定して、簡素化されたクラスタ全体のアップグレード中の接続損失を避けることを推奨します。

手順

ステップ 1 任意の Cisco Unified Communications Manager ノードにログインします。

ステップ 2 Cisco Unified CM の管理から、**[システム（System）] > [サービス パラメータ（Service Parameters）]** の順に選択します。

ステップ 3 [**サーバ**] ドロップダウンから、Unified CM ノードを選択します。

ステップ 4 **サービス** ドロップダウンから **Cisco AMC サービス**を選択します。

ステップ 5 **Primary Collector** サービスパラメータで、任意のサブスクライバノードを選択します。

ステップ 6 **[フェールオーバーコレクタ（Failover Collector）]** サービスパラメータで別のサブスクライバノードを選択します。

ステップ 7 **[保存（Save）]** をクリックします。

ステップ 8 Cisco Unified Real-Time Monitoring Tool を任意のサブスクライバ ノードに接続します。

Microsoft SQL Server のアップグレードに必要なデータベースの移行

Microsoft SQL サーバーを IM and Presence Service を使用して外部データベースとしてデプロイし、11.5(1)、11.5(1)SU1、または 11.5(1)SU2 にアップグレードする場合、新しい SQL サーバーデータベースを作成して、それを新しいデータベースに移行する必要があります。 これは、このリリースで強化されたデータ型のサポートに必要です。 データベースを移行しない場合、既存の SQL Server データベースでスキーマ検証の失敗が発生し、永続的なチャットなど、外部データベースに依存するサービスは開始されません。

IM and Presence Serviceをアップグレードしたら、次の手順で新しい SQL サーバーデータベースを作成し、新しいデータベースにデータを移行します。

（注） この移行は、Oracle または PostgreSQL 外部データベースには必要ありません。

始める前に

データベースの移行は、`MSSQL_migrate_script.sql` スクリプトに依存します。 Cisco TAC に連絡してコピーを入手してください。

手順

ステップ 1 外部 Microsoft SQL Server データベースのスナップショットを作成します。

ステップ 2 新しい (空の) SQL Server データベースを作成します。 詳細については、「IM and Presence Service データベース セットアップ ガイド」の章を参照してください。

1. 「Microsoft SQL のインストールとセットアップ」—アップグレードされた IM およびプレゼンスサービスに新しいSQLサーバデータベースを作成する方法の詳細については、この章を参照してください。
2. 「IM and Presence サービスの外部データベースのセットアップ」—新しいデータベースが作成されたら、この章を参照して、IM and Presence サービスの外部データベースとしてデータベースを追加します。

ステップ 3 システム トラブルシューティングを実行して、新しいデータベースにエラーがないことを確認します。

1. Cisco Unified CM IM and Presence の管理から、 **診断** > **システムトラブルシューティング**を選択します。
2. **外部データベースのトラブルシューティング** セクションにエラーが表示されないことを確認します。

ステップ 4 すべての IM and Presence サービス クラスタ ノードで Cisco XCP Router を再起動します。

1. Cisco Unified IM and Presence Serviceability から **[ツール]** > **[コントロールセンター] - [ネットワークサービス]**を選択します。
2. **[サーバー（Server）]** メニューで、IM and Presence サービスノードを選択して、**[移動（Go）]** をクリックします。
3. **[IM and Presenceサービス（IM and Presence Services）]** の下で、**[Cisco XCPルータ（Cisco XCP Router）]** を選択し、**[リスタート(Restart)]** をクリックします

ステップ 5 外部データベースに依存するサービスをオフにする:

1. Cisco Unified IM and Presence Serviceability で、**[ツール（Tools）]** > **[コントロールセンター - 機能サービス（Control Center - Feature Services）]** の順に選択します。
2. **[サーバ]** メニューから IM & Presence ノードを選択し、 **[実行] をクリックします。**
3. [**IM およびプレゼンスサービス**] から次のサービスを選択します:

   Cisco XCP Text Conference Manager

   Cisco XCP ファイル転送マネージャ

   Cisco XCP Message Archiver
4. [Stop]をクリックします。

ステップ 6 次のスクリプトを実行して、古いデータベースから新しいデータベース `MSSQL_migrate_script.sql` にデータを移行します。

（注） Cisco TAC に連絡してこのスクリプトのコピーを入手してください。

ステップ 7 新しいデータベースにエラーがないことを確認するためにシステム トラブルシューターを実行します。

1. Cisco Unified CM IM and Presence の管理から、 **診断** > **システムトラブルシューティング**を選択します。
2. [**外部データベースのトラブルシューティング**] セクションでエラーが表示されないことを確認します。

ステップ 8 前に停止したサービスを開始します。

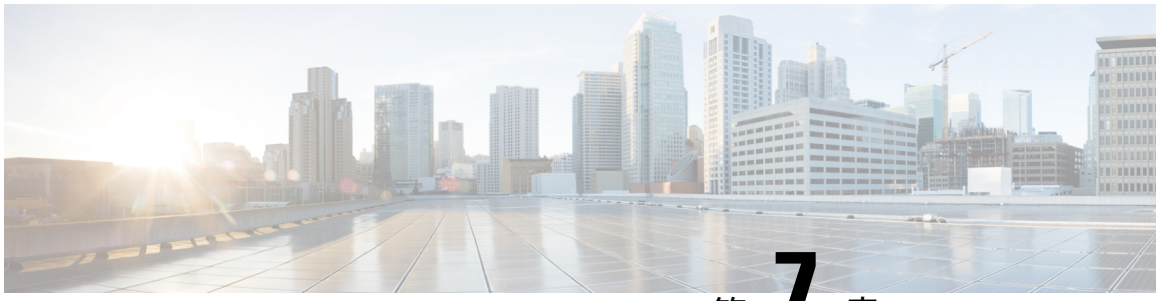
1. Cisco Unified IM and Presence Serviceability から **[ツール]** > **[コントロールセンター] - [機能サービス]**を選択します。
2. **[サーバ]** メニューから IM & Presence ノードを選択し、 **[実行] をクリックします**。
3. [**IM およびプレゼンスサービス**] から次のサービスを選択します:

   Cisco XCP Text Conference Manager

   Cisco XCP ファイル転送マネージャ

   Cisco XCP Message Archiver
4. [開始] をクリックします。

ステップ 9 外部データベースが実行中で、Cisco Jabber クライアントからすべてのチャットルームが表示されていることを確認します。 新しいデータベースが機能していることを確認してから、古いデータベースを削除してください。



第 7 章

アップグレード後のタスク

アップグレード後のタスクフロー

すべてのアップグレードおよび移行方法について、このリストのタスクを実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	CTL ファイルの更新 （132 ページ）	クラスタが混合モードの場合、CTL ファイルを手動で更新します。 電話をリセットして最新の更新を反映します。 （注） Unified Communications Manager の移行の場合は、これをスキップできます。
ステップ 2	シリアルポートを削除する （132 ページ）	アップグレード前のタスクで追加したシリアルポートを削除して、VM のパフォーマンスに影響を与えないようにします。 すべてのノードに対してこの手順を実行します。
ステップ 3	エクステンションモビリティの再起動 （132 ページ）	アップグレード前タスクの一部として Cisco Extension Mobility を無効にした場合、再起動できます。
ステップ 4	アップグレード後の COP を実行します。	アップグレード後の COP は、システムの安定性を確認するために一連のテストを実行します。 これらのテストで

	コマンドまたはアクション	目的
		は、違いを特定するためにアップグレード前とアップグレード後の設定を比較します。この表のすべての手順を完了したら、post-upgrade COP ファイルを再実行して、COP レポートを確認します。 （注） COP ファイルを使用してアップグレードしようとすると、システムにインストールされているファイル数が表示されます。アップグレードが完了すると、COP ファイルのリストは以前のバージョンと一致しなくなります。以前のファイルが必要な場合は、COP ファイルを手動でインストールする必要があります。 （注） CLI コマンド である show risdb query cti を実行すると、ノードに登録されたデバイスの詳細が表示されます。デバイスは、エントリを作成するために、そのノードで少なくとも 1 回登録されている必要があります。たとえば、サブスクライブ 2 で登録されたデバイスが登録解除され、サブスクライブ 1 に移動された場合、サブスクライブ 2 でこのコマンドを実行すると、未登録として表示されます。
ステップ 5	TFTP パラメータのリセット（135 ページ）	アップグレードプロセス中に変更される TFTP パラメータをリセットします。
ステップ 6	エンタープライズパラメータの復元（135 ページ）	アップグレードプロセス中に上書きされた可能性がある IM and Presence Service ノードのエンタープライズパラメータ設定を復元します。
ステップ 7	最高水準点と最低水準点のリセット（136 ページ）	トレースの時期を過ぎた消去を避けるために、この手順を使用して高ウォーターマークと低ウォーターマークを元の値に復元します。

	コマンドまたはアクション	目的
		PCD 移行の場合は、このタスクをスキップできます。
ステップ 8	VMware Tools の更新 （136 ページ）	アップグレードが完了したら、VMWare Tools を更新する必要があります。 すべてのノードに対してこの手順を実行します。
ステップ 9	ロケールのインストール （137ページ）	アップグレード後、デフォルトでインストールされる米国英語を除き、使用中のロケールを再インストールする必要があります。 すべてのノードに対してこの手順を実行します。
ステップ 10	データベースリプリケーションタイムアウトを復元する （138 ページ）	アップグレードを開始する前にデータベース複製のタイムアウト値を増やした場合、この手順を使用します。 Unified Communications Manager ノードのみでこの手順を実行します。
ステップ 11	登録済みデバイス数の確認 （139 ページ）	アップグレードが完了した後、この手順を使用して、Unified CM ノード上のエンドポイントとリソースを確認します。
ステップ 12	割り当てられたユーザを確認する （140 ページ）	アップグレードが完了した後、この手順で IM and Presence Service ノードに割り当てられたユーザーの数を確認します。
ステップ 13	テスト機能 （140 ページ）	アップグレード後に電話の機能が正常に動作していることを確認します。
ステップ 14	RTMT のアップグレード （141 ページ）	Cisco Unified Real Time Monitoring Tool (RTMT) を使用する場合、新しいソフトウェアバージョンにアップグレードします。
ステップ 15	TFTP サーバファイルの管理 （142 ページ）	これはオプションです。 この手順を実行して、電話の呼び出し音、コールバックトーン、および背景を TFTP サーバーにアップロードして、Unified CM ノードで使用できるようにします。

	コマンドまたはアクション	目的
ステップ 16	カスタムログオンメッセージのセットアップ （143 ページ）	これはオプションです。 Unified CM ノードの場合のみ、カスタマイズされたログオンメッセージを含むテキストファイルをアップロードします。
ステップ 17	IPSec ポリシーを設定する （144 ページ）	リリース 6.1 (5) からの PCD 移行を完了する場合、IPSec ポリシーは新しいリリースに移行されないため、再度作成する必要があります。
ステップ 18	新しい Manager Assistant の役割を指定する （145 ページ）	アップグレード前に Manager Assistant が展開されていて、ユーザに InterCluster Peer-User または Admin-CUMA の役割が割り当てられている場合、ユーザに役割を割り当て直す必要があります。これらの役割は現行リリースには存在しないためです。
ステップ 19	IM および Presence サービス データ移行の確認 （145 ページ）	この手順は、Cisco Unified Presence リリース 8.x から IM and Presence サービスリリースへのアップグレードまたは移行を実行した場合にのみ使用してください。
ステップ 20	プレゼンス冗長グループの高可用性を有効にする （146 ページ）	アップグレード前に IM and Presence Service サービスの高可用性を無効にした場合、この手順で再び有効にしてください。
ステップ 21	IM および Presence 同期エージェントを再起動する （147 ページ）	アップグレードを開始する前に IM and Presence Service Sync Agent サービスを停止していた場合は、今すぐ再開してください。
ステップ 22	Cisco Emergency Responder サービスを再起動する （148 ページ）	アップグレード Unified Communications Manager 後に AXL 接続を確立するには、CER サービスを再起動してください。 また、Unified CM パブリッシャノードで AXL 変更通知トグルを再起動する必要があります。

ソフトウェア バージョンを切り替える

標準アップグレードを実行すると、新しいソフトウェアは非アクティブバージョンとしてインストールされます。アップグレードプロセス中に新しいソフトウェアにリブートすることも、後で新しいバージョンに切り替えることもできます。

アップグレードの完了直後にバージョンを切り替えなかった場合は、今すぐ切り替えます。バージョンを切り替えることでアップグレードが完了し、クラスター内のすべてのノードが更新されます。新しいソフトウェアバージョンに切り替えるまでは、バックアップを実行しないでください。

バージョンを切り替えると、システムが再起動し、アクティブではないソフトウェアがアクティブになります。 システムの再起動には最大で 15 分かかります。 この手順を実行すると、アクティブと非アクティブの両方のソフトウェアバージョンが表示されます。

注意 この手順を実行すると、システムが再起動し、一時的に使用できない状態になります。

始める前に

Unified Communications Manager と IM and Presence Service ノードのソフトウェアのバージョンは、手動切り替えルールに従って一致する必要があります。 よって、IM and Presence Service に切り替える前に、Unified Communications Manager に切り替える必要があります。

バージョンの切り替えについて （83 ページ） で情報を確認します。

手順

ステップ 1 マルチノード展開でバージョンを切り替える場合、最初にパブリッシャノードを切り替える必要があります。

ステップ 2 アップグレードしているノードの管理ソフトウェアにログインします。

- IM and Presence Service ノードをアップグレードする場合は、Cisco Unified IM and Presence Operating System Administration にログインします。
- Unified Communications Manager ノードをアップグレードする場合は、Cisco Unified Communications Operating System Administration にログインします。

ステップ 3 **[設定（Settings）] > [バージョン（Version）]** の順で選択します。

ステップ 4 アクティブなソフトウェアと非アクティブなソフトウェアのバージョンを確認します。

ステップ 5 [バージョンの切り替え（Switch Versions）]を選択して、バージョンを切り替え、システムを再起動します。

アップグレード Unified Communications Manager 時にバージョン切り替えを実行した後、IP 電話は新しい構成ファイルを要求します。 このリクエストにより、デバイスのファームウェアが自動的にアップグレードされます。

CTL ファイルの更新

Unified Communications Manager pre 12.0 から 12.0 以降のバージョンへのアップグレード中に、ITLRecovery 証明書がクラスターごとに生成されます。 クラスタが混合モードの場合、CTL ファイルを手動で更新します。 電話をリセットして最新の更新を反映します。

（注） リリース 12.5(1)SU3 更新以降は、CTL が不要になりました。

手順

ステップ 1 **[Unified Communications Manager Administration]** > **[システム（System）]** > **[エンタープライズパラメータの構成（Enterprise Parameters Configuration）]** の順に選択して、Unified Communications Manager セキュリティモードを検証します。

クラスターセキュリティモード フィールドを見つけます。 フィールドの値が 1 と表示される場合、Unified Communications Manager は混合モードに構成されています。

ステップ 2 CTL ファイルを手動で更新します。 CTL ファイルの更新方法の詳細については、「Cisco Unified Communications Manager セキュリティガイド」を参照してください。

ステップ 3 電話をリセットして更新を反映します。

シリアルポートを削除する

アップグレード前のタスク中に、アップグレードログをキャプチャするために仮想マシンにシリアルポートを追加しました。 システムのアップグレードに成功したら、仮想マシンのパフォーマンスに影響を与えないように、シリアルポートを削除する必要があります。

手順

ステップ 1 仮想マシンの電源をオフにします。

ステップ 2 設定を編集してシリアルポートを削除します。 設定の編集方法については、VMware のドキュメントを参照してください。

ステップ 3 仮想マシンの電源を入れて、アップグレード後のタスクを進めます。

エクステンション モビリティの再起動

リリース 9.x 以前からのアップグレードでは、アップグレードを開始する前に Cisco エクステンションモビリティを停止する必要があります。 アップグレード前タスクの一部として Cisco

エクステンション モビリティを無効化した場合、この手順を使用してノード Unified Communications Manager でサービスを再起動してください。

手順

ステップ 1 Cisco Unified Serviceability から、**[ツール（Tools）] > [サービスの有効化（Service Activation）]** を選択します。

ステップ 2 [サーバ（Server）] リストから、サービスを非アクティブ化するノードを選択し、[移動（Go）] をクリックします。

ステップ 3 **Cisco エクステンション モビリティ** サービスを選択します。

ステップ 4 **再起動（Restart）**をクリックします。

アップグレードの準備 COP ファイルの実行 (アップグレード後)

アップグレード後、post-upgrade COP ファイルを実行し、以下を確認します。

- インストールされた COP ファイル
- ネットワーク サービスと接続 (DNS、NTP、クラスター内)
- FIPS モードのパスワードの長さの制限
- ライセンスの同期
- VMware ツールの互換性
- ディスク容量
- SIP および H.323 トランク登録
- データベース認証およびレプリケーションの状況
- データベースの健全性
- 最後の DRS バックアップの状況
- サービス状況
- インストールされている COP とロケール
- デバイス登録状態数
- エンタープライズ パラメータとサービス パラメータの設定
- TFTP 最大サービス数
- アクティブおよび非アクティブ バージョン

（注） システムの正常性を確認するために、Upgrade Readiness COP ファイルを実行してアップグレード後の確認をすることが推奨されます。

手順

ステップ 1 アップグレードの準備 COP ファイルをダウンロードしてアップグレード後のテストを実行します。

a) ダウンロードサイトに移動します。
b) 移動先のリリースを選択し、**[Unified Communications Managerユーティリティ（Unified Communications Manager Utilities）]** を選択します。
c) **アップグレード前テストを実行ために、Upgrade Readiness COP ファイル**をダウンロードします（たとえば、`ciscocm.postUpgradeCheck-00019.cop.sgn`）。 最新のファイルは別のファイル名とバージョンを持つ場合があることに注意してください。)

ステップ 2 アップグレード後のシステムの状態を確認します。

a) COP ファイルを実行します。
b) COP ファイルが返す問題を解決します。
c) COP ファイルがエラーを返さなくなるまで、これらの手順を繰り返します。

ステップ 3 アップグレード後のレポートを CLI で表示するには、**file get install/PostUpgradeReport.txt** コマンドを実行します。

ステップ 4 RTMT からレポートを表示するには

a) RTMT にログインします。
b) **[Trace and Log Central]** で、**[リモートブラウザ（Remote Browse）]** をダブルクリックし、**[トレースファイル（Trace files）]** を選択したら、**[次へ（Next）]** をクリックします。
c) **[すべてのサーバー上のすべてのサービス（Select all Services on all servers）]** を選択して、**[次へ（Next）]** をクリックします。
d) **[完了（Finish）]> [閉じる（Close）]** の順に選択します。
e) ノードをダブルクリックして、**[CUCMパブリッシャ（CUCM Publisher）] > [システム（System）] > [アップグレードログのインストール（Install upgrade Logs）]** の順に展開します。
f) [**インストール**] をダブルクリックして、必要なファイルを選択してダウンロードします。

次のタスク

アップグレードが完了しました。 新しいソフトウェアの使用を開始することができます。

TFTP パラメータのリセット

アップグレード中、TFTP サービスパラメータである **Maximum Serving Count** が変更され、より多くのデバイス登録要求に対応できるようになります。アップグレードの完了後、この手順を使用してパラメータをリセットします。

手順

ステップ 1 Cisco Unified CM Administration インターフェイスで、**[システム（System）]** > **[サービスパラメータ（Service Parameters）]** の順に選択します。

ステップ 2 [**サーバ**] ドロップダウンリストから、TFTP サービスを実行しているノードを選択します。

ステップ 3 **サービス** ドロップダウンリストから **Cisco TFTP サービス**を選択します。

ステップ 4 [詳細設定（Advanced）]をクリックします。

ステップ 5 **[保存（Save）]** をクリックします。

ステップ 6 **最大サービングカウント**を、アップグレード前に使用した値と同じ値、または現在の構成で推奨されている値に設定します。

デフォルト値は 500 です。同じサーバ上で他の Cisco CallManager サービスと共に TFTP サービスを実行する場合は、デフォルト値を使用することをお勧めします。 専用 TFTP サーバの場合、次の値を使用します。

- シングルプロセッサシステムの場合は 1500
- デュアルプロセッサシステムの場合は 3000
- より高い CPU 構成を持つ専用 TFTP サーバの場合は 3500

エンタープライズパラメータの復元

一部のエンタープライズパラメータは、Unified Communications Manager ノードと IM and Presence Service ノードの両方に存在します。 同じパラメータが存在する場合、Unified Communications Manager ノードで構成した設定は、アップグレード中に IM and Presence Service ノードで構成した設定を上書きします。 ノードに固有の IM and Presence Service エンタープライズパラメータは、アップグレード中に保持されます。

この手順で、アップグレード中に上書きされた IM and Presence Service ノードの設定を再構成します。

始める前に

アップグレード前タスクの一部として記録した設定にアクセスできることを確認してください。

手順

ステップ 1 Cisco Unified CM IM and Presence Administration インターフェイスで、**[システム（System）]** > **[エンタープライズパラメータ（Enterprise Parameters）]** の順に選択します。

ステップ 2 現在の設定をアップグレード前の設定と比較し、必要に応じてエンタープライズパラメータを更新します。

ステップ 3 **[保存（Save）]** をクリックします。

ステップ 4 [リセット（Reset）]をクリックし、[OK]をクリックしてすべてのデバイスをリセットします。

最高水準点と最低水準点のリセット

トレースの時期を過ぎた消去を避けるために、この手順を使用して高ウォーターマークと低ウォーターマークを元の値に復元します。

手順

ステップ 1 Real Time Monitoring Tool（RTMT）インタフェースの左側ナビゲーションペインで、**[Alert Central]** をダブルクリックします。

ステップ 2 **[システム（System）]** タブで、**[LogPartitionLowWaterMarkExceeded]** を右クリックしたら、**[アラート/プロパティの設定（Set Alert/Properties）]**を選択します。

ステップ 3 [次へ（Next）]を選択します。

ステップ 4 スライダの値を 80 に調整します。

ステップ 5 **[システム（System）]** タブで、**[LogPartitionHighWaterMarkExceeded]** を右クリックしたら、**[アラート/プロパティの設定（Set Alert/Properties）]**を選択します。

ステップ 6 [次へ（Next）]を選択します。

ステップ 7 スライダの値を 85 に調整します。

VMware Tools の更新

VMware Tools は、管理とパフォーマンス最適化のためのユーティリティ セットです。 Unified Communications Manager 15 は Open VMware Tool のみをサポートします。

- Unified Communications Manager リリース 12.5(1) または 14 から アップグレードまたは移行する場合、および SU を 15 にアップグレードまたは移行する場合（たとえば、上位の SU）、Open VMware ツールはデフォルトでインストールされています。
- Unified Communications Manager リリース 11.5 (1) 以降のフレッシュインストールと PCD 移行では、Open VMware ツールがデフォルトでインストールされます。

utils vmtools status コマンドを実行すると、VMware ツールが現在実行中かを確認できます。

ロケールのインストール

この手順でロケールをインストールします。アップグレード後、デフォルトでインストールされる米国英語を除き、使用中のロケールを再インストールする必要があります。 お使いの Unified Communications Manager ノードまたはIM and Presence Service ノードの major.minor バージョン番号に一致するロケールの最新バージョンをインストールしてください。

ロケールは Unified Communications Manager または IM and Presence Service ノードにインストールできます。 両方の製品にロケールをインストールする場合、次の順序ですべてのクラスターノードにロケールをインストールします。

1. Unified Communications Manager パブリッシャノード
2. Unified Communications Manager サブスクライバ ノード
3. IM and Presence データベース パブリッシャ ノード
4. IM and Presence サブスクライバノード

IM and Presence サービスノードに特定のロケールをインストールする場合、まずは、同じ国の Unified Communications Manager ロケールファイルをUnified Communications Manager クラスタにインストールする必要があります。

手順

ステップ 1 cisco.com でお使いのリリースのロケールインストーラーを検索します。

- Cisco Unified Communications Manager の場合は、 https://software.cisco.com/download/navigator.html?mdfid=268439621&i=rm
- IM and Presence サービスの場合は、https://software.cisco.com/download/navigator.html?mdfid=280448682&i=rm に移動します。

ステップ 2 お使いのリリースのロケール インストーラを、SFTP をサポートするサーバにダウンロードします。 次のファイルが必要です。

- ユーザ ロケール ファイル - これらのファイルには特定の言語と国の言語情報が含まれており、次の規則に従います。
  - `cm-locale-language-country-version.cop` (Cisco Unified Communications Manager)
  - `ps-locale-language_country-version.cop` (IM and Presence サービス)
- 統合ネットワーク ロケール ファイル - 電話トーン、通知音、ゲートウェイ トーンなど、さまざまなネットワーク項目について、すべての国に固有のファイルが含まれています。複合ネットワーク ロケール ファイル名の表記は、次のとおりです。

- cm-locale-combinednetworklocale-version.cop (Cisco Unified Communications Manager)

ステップ 3 管理者アカウントを使用して Cisco Unified OS Administration にログインします。

ステップ 4 **[Software Upgrades（ソフトウェア アップグレード）]** > **[Install/Upgrade（インストール/アップグレード）]**を選択します。

ステップ 5 **[ソフトウェアインストール/アップグレード（Software Installation/Upgrade）]** ウィンドウで、次のフィールドを入力します。

- **ソース**で **リモートファイルシステム**を選択します。
- **[ディレクトリ（Directory）]** に、ロケールインストーラを保存したディレクトリへのパスを入力します。
- **[サーバー（Server）]** フィールドに、リモートファイルシステムのサーバー名を入力します。
- リモートファイルシステムの資格情報を入力します。
- **[トランスファープロトコル（Transfer Protocol）]** ドロップダウンメニューで、**[SFTP]** を選択します。 転送プロトコルには SFTP を使用してください。

ステップ 6 [次へ（Next）]をクリックします。

ステップ 7 サーバにロケールをダウンロードしてインストールします。

ステップ 8 サーバを再起動します。 更新はサーバーの再起動後に有効になります

ステップ 9 規定された順番ですべての Unified Communications Manager および IM and Presence Service クラスタノードに対してこの手順を繰り返します。

（注） すべてのクラスターノードに新しいロケールがインストールされるまで、エンドユーザのユーザロケールをリセットしないでください。 Unified Communications Manager と IM and Presence Service サービスの両方のロケールをインストールする場合、ユーザーロケールをリセットする前に、両方の製品のロケールをインストールする必要があります。 IM and Presence Service サービスのロケールインストールが完了する前にエンドユーザーが電話言語をリセットした場合などの問題が発生した場合、セルフケア ポータルを使用して電話言語を英語にリセットするようにユーザーに依頼します。 ロケールのインストールが完了したら、ユーザは電話の言語をリセットすることができます。または、一括管理を使用して、ロケールを適切な言語に一括で同期できます。

データベースリプリケーション タイムアウトを復元する

この手順は Unified Communications Manager ノードにのみ適用されます。

アップグレードを開始する前にデータベース複製のタイムアウト値を増やした場合、この手順を使用します。

デフォルトのデータベース複製のタイムアウト値は 300 (5 分) です。 クラスタ全体がアップグレードされ、Unified Communications Manager サブスクライバノードが正常にレプリケーションをセットアップした後で、タイムアウトをデフォルト値に戻します。

手順

ステップ 1 次のいずれかの方法を使用して、CLI セッションを開始します。

- リモート システムの場合は、SSH を使用して Cisco Unified オペレーティング システムにセキュアに接続します。 SSH クライアントで、**ssh *adminname@hostname*** およびパスワードを入力します。
- シリアル ポートへの直接接続を介して、自動的に表示されるプロンプトでクレデンシャルを入力します。

ステップ 2 **utils dbreplication setrepltimeout***timeout* コマンドを実行します。ここの *timeout* は、秒単位のデータベース リプリケーション タイムアウトです。 値を 300 (5 分) に設定します。

登録済みデバイス数の確認

Cisco リアルタイム監視ツール (RTMT) を使用してデバイス数を表示し、アップグレードが完了した後にエンドポイントとリソースを確認します。

手順

ステップ 1 Unified RTMT インターフェイスから **[音声/ビデオ]** > **[端末の概要]** を選択します。

ステップ 2 登録済みデバイスの数を記録します。

項目	カウント
登録済みの電話機（Registered Phones）	
登録済みゲートウェイ	
登録済みメディア リソース	
登録済みの他のステーションデバイス	

ステップ 3 この情報をアップグレード前に記録したデバイス数と比較し、エラーがないことを確認します。

割り当てられたユーザを確認する

この手順を使用して、アップグレード完了後にノードに割り当てられたユーザの数を確認します。

手順

ステップ 1 Cisco Unified CM IM and Presence の管理インターフェイスから、 **システム** > **クラスタートポロジ**を選択します。

ステップ 2 この情報を、アップグレード前に記録した割り当てユーザ数と比較し、エラーがないことを確認します。

テスト機能

アップグレード後、以下のタスクを実行します。

- post-upgrade COP を実行します。

  一連のテストを実行して、システムが安定しているかどうかを確認します。また、アップグレード前のさまざまなパラメータと現在のバージョンを比較して、違いを識別します。このリスト内のすべての手順を完了したら、post-upgrade COP ファイルを再実行して、COP レポートを確認します。

- 次の種類のコールを発信して、電話機能を確認します。
  - ボイスメール
  - オフィス間
  - 携帯電話
  - ローカル
  - 国内
  - 国際
  - 共有回線
- 次の電話機能をテストします。
  - 会議
  - 割込み
  - 転送
  - 会議割り込み

- 共有回線で呼び出し音を鳴らす
- 取り込み中
- [プライバシー（Privacy）]
- プレゼンス
- CTI 通話コントロール
- ビジー ランプ フィールド

- IM and Presence Service 機能をテストします。
  - 対応可能、対応不可、取り込み中などの基本在席状態
  - ファイルの送受信
  - 永続的なチャット、フェデレーション ユーザ、メッセージ アーカイブなどの高度な機能

RTMT のアップグレード

ヒント 互換性を確保するために、クラスタ内のすべてのサーバでアップグレードを完了した後で、RTMT をアップグレードすることを推奨します。

RTMT は、ユーザ設定とダウンロードされたモジュール jar ファイルをクライアント マシンのローカルに保存します。システムはユーザーが作成したプロファイルをデータベースに保存するため、これらのアイテムにはツールのアップグレード後に Unified RTMT でアクセスできます。

始める前に

RTMT の新しいバージョンにアップグレードする前に、解凍した CiscoRTMTPlugin.zip フォルダの以前のバージョンまたは古いバージョンを削除することをお勧めします。

手順

ステップ 1 Unified Communications Manager Administration で、**[アプリケーション（Application）] > [プラグイン（Plugins）]** の順に選択します。

ステップ 2 **[検索（Find）]** をクリックします。

ステップ 3 Linux または Microsoft Windows オペレーティングシステムで実行されているクライアントに Unified RTMT をインストールするには、Cisco Unified Real-Time Monitoring の Windows および Linux ツールの **[ダウンロード（Download）]** リンクから CiscoRTMTPlugin.zip をダウンロードします。

ヒント Windows 10 以降に Unified RTMT をインストールすると、権限を持つ管理者のみが RTMT を起動できます。

ステップ 4 CiscoRTMTPlugin.zip をクライアント上の希望の場所にダウンロードします。

ステップ 5 Windows 版をインストールするには、

a) CiscoRTMTPlugin.zip ファイルを解凍します。

b) `run.bat` ファイルをダブルクリックします。

ステップ 6 Linux 版をインストールするには、

a) CiscoRTMTPlugin.zip ファイルを解凍します。

b) ファイルを抽出したら、コマンド **chmod 755 run.sh** を実行して、`run.sh` ファイルにアクセス許可を設定する必要があります。

c) `run.sh` ファイルをダブルクリックします。

TFTP サーバファイルの管理

電話で使用するファイルを TFTP サーバにアップロードできます。アップロードできるファイルには、カスタム呼び出し音、コールバックトーン、バックグラウンドが含まれます。このオプションは、接続した特定のサーバにのみファイルをアップロードし、クラスター内の他のノードはアップグレードされません。

デフォルトでは、ファイルは **tftp** ディレクトリにアップロードされます。**tftp** ディレクトリのサブディレクトリにファイルをアップロードすることもできます。

クラスタに設定された 2 つの Cisco TFTP サーバがある場合、両方のサーバで以下の手順を実行する必要があります。このプロセスはすべてのノードにファイルを配布しません。また、クラスタ内の両方の Cisco TFTP サーバにもファイルを配布しません。

TFTP サーバファイルをアップロードまたは削除するには、次の手順に従います。

手順

ステップ 1 [Cisco Unified Communicationsオペレーティングシステム（Cisco Unified Communications Operating System）] 管理ウィンドウで、**[ソフトウェアアップグレード（Software Upgrades）] > [TFTP] > [ファイル管理（File Management）]** の順に選択します。

TFTP ファイル管理ウィンドウが、現在アップロードされているファイルの一覧を表示します。[検索] コントロールを使用してファイル一覧をフィルタリングできます。

ステップ 2 ファイルをアップロードするには、次の手順に従います:

a) [ファイルのアップロード（Upload File）] をクリックします。

[ファイルのアップロード] ダイアログボックスが開きます。

b) ファイルをアップロードするには、[**参照**] をクリックしてアップロードするファイルを選択します。

c) **tftp** ディレクトリのサブディレクトリにファイルをアップロードするには、**[ディレクトリ（Directory）]** フィールドのサブディレクトリを入力します。
d) アップロードを開始するには、**[ファイルをアップロード（Upload File）]** をクリックします。

[ステータス] 領域に、ファイルのアップロードが正常に完了すると表示されます。

e) ファイルのアップロードが完了したら、Cisco TFTP サービスを再起動してください。

（注） 複数のファイルをアップロードする予定がある場合は、すべてのファイルをアップロードした後で、Cisco TFTP サービスを 1 回だけ再起動してください。

ステップ 3 ファイルを削除するには、次の手順に従います。

a) 削除するファイルの隣にあるチェックボックスを選択します。

[**すべて選択**] をクリックしてすべてのファイルを選択するか、または [**すべて解除**] をクリックしてすべての選択を解除します。

b) **[選択項目の削除(Delete Selected)]** をクリックします。

（注） **tftp** ディレクトリにすでに保存されているファイルを修正する場合は、**file list tftp** CLI コマンドを使用して、TFTP ディレクトリのファイルを閲覧し、**file get tftp** を使用して、TFTP ディレクトリのファイルのコピーを取得します。 詳細については、Cisco Unified Communications ソリューションズコマンドラインインターフェイスリファレンスガイドを参照してください。

カスタム ログオン メッセージのセットアップ

Cisco Unified Communications Operating System Administration、Cisco Unified CM Administration、Cisco Unified Serviceability、Disaster Recovery System Administration、Cisco Prime License Manager およびコマンドラインインターフェイスに表示されるカスタマイズされたログオンメッセージを含むテキストファイルをアップロードできます。

カスタマイズしたログオンメッセージをアップロードするには、次の手順に従います:

手順

ステップ 1 Cisco Unified Communications Operating System 管理ウィンドウで、**[ソフトウェアアップグレード（Software Upgrades）]** > **[カスタマイズされたログオンメッセージ（Customized Logon Message）]** の順に選択します。

[ログオンメッセージのカスタマイズ] ウィンドウが表示されます。

ステップ 2 アップロードするテキストファイルを選択するには、**[参照（Browse）]** をクリックします。
ステップ 3 [ファイルのアップロード（Upload File）]をクリックします。

（注） 10kB を超えるファイルをアップロードすることはできません。

カスタマイズしたログオンメッセージが表示されます。

ステップ 4 デフォルトのログオンメッセージに戻すには、**[削除（Delete）]** をクリックします。

カスタマイズしたログオンメッセージは削除され、システムは既定のログオンメッセージを表示します。

（注） カスタムメッセージを、Cisco Unified Communications Operating System Administration、Cisco Unified CM Administration、Cisco Unified Serviceability、Disaster Recovery System Administration、Cisco Prime License Manager およびコマンド ライン インターフェイスのログイン画面に表示させる場合は、**[ユーザーの確認が必要（Require User Acknowledgment）]** チェックボックスをオンにします。

IPSec ポリシーを設定する

この手順は、リリース 10.5 から PCD 移行を実行する場合にのみ使用してください。 PCD の移行が完了したら、IPSec ポリシーを再設定する必要があります。 移行の前に、クラスターの両方のノードで IPSec ポリシーを無効にする必要があります。 移行に成功したら、IPSec ポリシーを必ず有効にしてください。

- IPSec では、双方向プロビジョニング、または各ホスト (またはゲートウェイ) に対して 1 つのピアが必要です。
- 一方の IPsec ポリシープロトコルが 「[任意（ANY）]」 に、もう一方の IPsec ポリシープロトコルが 「[UDP]」 または 「[TCP]」 に設定されている 2 つの Unified Communications Manager ノードで IPSec ポリシーをプロビジョニングする場合、「[任意（ANY）]」 プロトコルを使用するノードから実行すると、検証が検出漏れになる場合があります。
- IPSec は、特に暗号化を伴う場合、システムのパフォーマンスに影響を与えます。

手順

ステップ 1 Cisco Unified OS の管理から **[セキュリティ（Security）] > [IPSec の設定（IPSec Configuration）]** の順に選択します。

ステップ 2 [新規追加] をクリックします。

ステップ 3 **[IPSEC ポリシーの設定（IPSEC Policy Configuration）]** ウィンドウで各フィールドを設定します。 フィールドとその設定オプションの詳細については、オンライン ヘルプを参照してください。

ステップ 4 **[保存]** をクリックします。

ステップ 5 （任意） IPsec を検証するには、**[サービス（Services）] > [Ping]** の順に選択し、**[IPsec の検証（Validate IPsec）]** チェックボックスをオンにして、**[Ping]** をクリックします。

新しい Manager Assistant の役割を指定する

前のリリースが Cisco Unified Communications Manager Assistant 機能を使用するように構成され、アプリケーションユーザーに InterCluster Peer-User または Admin-CUMA ロールのいずれかを割り当てた場合にのみ、この手順を実行します。 InterCluster Peer-User および Admin-CUMA ロールは、リリース 10.0 (1) 以降で廃止され、アップグレードプロセス中に削除されます。 これらのユーザに新しい役割を割り当てる必要があります。

手順

ステップ 1 ロールとユーザーを構成するには、『Administration Guide for Cisco Unified Communications Manager』 の「ユーザーの管理」を参照してください。

ステップ 2 IM and Presence Service サービス ユーザーインターフェイスで定義された AXL ユーザー（**[プレゼンス（Presence）] > [内部クラスタリング（Inter-Clustering）]**）に、Unified Communications Manager アプリケーション ユーザー ページの標準 AXL API アクセスロールと関連付けられた標準 AXL API アクセスロールが付与されていることを確認します。

IM および Presence サービス データ移行の確認

Cisco Unified Presence Release 8.x から IM and Presence Service サービスにアップグレードする場合、ユーザープロファイルは、Unified Communications Manager に移行されます。 ユーザープロファイル情報は、次の名前形式と説明形式で Unified Communications Manager で新しいサービスプロファイルとして保存されます。

名前: UCServiceProfile_Migration_x (x は 1 から始まる番号です)

説明: 移行されたサービス プロファイル番号 x

Cisco Unified Presence リリース 8.x からのアップグレード後にユーザが Cisco Jabber に正常にログインできるように、ユーザプロファイルデータの移行が成功したことを確認する必要があります。

作成されたが、ユーザーに割り当てられていないプロファイルは、Unified Communications Manager に移行されません。

手順

ステップ 1 Cisco Unified CM Administration で、**[ユーザー管理（User Management）] > [ユーザー設定（User Settings）] > [サービスプロファイル（Service Profile）]** の順に選択します。

ステップ 2 **[検索（Find）]** を選択してすべてのサービスプロファイルを一覧します。

ステップ 3 次の名前形式を持つ移行されたサービス プロファイルがあることを確認します: *UCServiceProfile_Migration_x*

ステップ 4 移行されたサービスプロファイルがない場合、`installdb` ログ ファイルでエラーを確認してください。

ステップ 5 データ移行が失敗した場合、Unified Communications Manager にインポートエラーアラームが発生し、Cisco Sync Agent が Cisco Unified CM IM and Presence Administration GUI に失敗通知を送信します。

ヒント アラームの詳細を表示するには、Cisco Unified Communications Manager の RTMT にログインします。

次のタスク

これらのサービス プロファイルを編集して、より意味のある名前を付けることができます。サービスプロファイルの設定の詳細については、『Administration Guide for Cisco Unified Communications Manager』を参照してください。

アップグレード後 COP ファイルを実行します。 一連のテストを実行して、システムが安定しているかどうかを確認します。 また、アップグレード前のさまざまなパラメータと現在のバージョンを比較して、違いを識別します。

プレゼンス冗長グループの高可用性を有効にする

この手順は IM and Presence Service ノードにのみ適用されます。 アップグレードプロセスを開始する前にプレゼンス冗長性グループの高可用性を無効にした場合、この手順を使用して今すぐ有効にしてください。

始める前に

サービスを再起動してから 30 分以内である場合は、ハイ アベイラビリティを再度有効にする前に Cisco Jabber セッションが再作成されたことを確認します。 そうしないと、プレゼンスはセッションが作成されていない Jabber クライアントでは機能しません。

Jabber セッションの数を取得するには、すべてのクラスタノードで `show perf query counter "Cisco Presence Engine" ActiveJsmSessions` CLI コマンドを実行します。 アクティブなセッションの数は、アップグレード前に高可用性を無効にしたときに記録したユーザの数と一致する必要があります。

手順

ステップ 1 Cisco Unified CM Administration のユーザ インターフェイスから、**[システム（System）]** > **[プレゼンス冗長グループ（Presence Redundancy Groups）]** を選択します。

ステップ 2 [検索] をクリックして、プレゼンス冗長グループを選択します。
[プレゼンス冗長グループの設定(Presence Redundancy Group Configuration)] ウィンドウが表示されます。

ステップ 3 **[ハイ アベイラビリティを有効にする（Enable High Availability）]** チェックボックスをチェックします。

ステップ 4 **[保存（Save）]** をクリックします。

ステップ 5 各プレゼンス冗長性グループでこの手順を繰り返します。

IM および Presence 同期エージェントを再起動する

アップグレードを開始する前に、IM and Presence Service Sync Agent サービスを停止する場合は、今すぐ再起動します。

手順

ステップ 1 Cisco Unified Serviceability インターフェイスで、**[ツール（Tools）]** > **[コントロールセンター - ネットワークサービス（Control Center - Network Services）]** の順に選択します。

ステップ 2 **[サーバー（Server）]** ドロップダウンメニューで IM and Presence Service ノードを選択し、**[移動（Go）]** をクリックします。

ステップ 3 **[IM and Presenceサービス（IM and Presence Services）]** セクションで、**[Cisco Sync Agent]** を選択して、**[再起動（Restart）]** をクリックします。

例

（注） Cisco Intercluster Sync Agent が初期同期を完了した後、手動で新しい Tomcat 証明書を Unified Communications Managerにロードします。 これにより、同期が失敗することがなくなります。

（注） アップグレード後の COP を実行します。 一連のテストを実行して、システムが安定しているかどうかを確認します。 また、アップグレード前のさまざまなパラメータと現在のバージョンを比較して、違いを識別します。

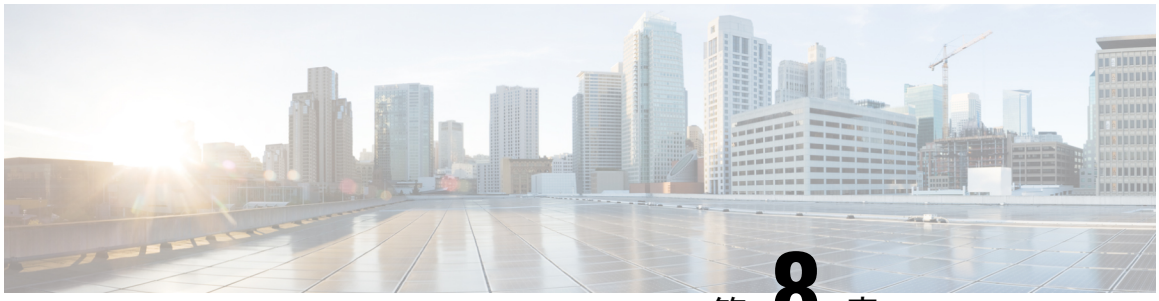
Cisco Emergency Responder サービスを再起動する

手順

アップグレードを開始する前に Cisco Emergency Responder サービスを停止している場合は、今すぐ再起動してください。

ステップ 1 Cisco Emergency Responder 保守インタフェースから、[**ツール**] >[**コントロールセンター]** を選択します。

ステップ 2 [**Cisco Emergency Responder**] を選択し、[**再起動**] をクリックします。



第 8 章

レガシーリリースからのアップグレード

レガシーリリースからのアップグレードと移行

現行リリースからの直接アップグレードまたは移行がサポートされていない場合、以下のプロセスを使用できます。

- Unified CM OS 管理インターフェイスまたは Cisco Prime Collaboration Deployment (PCD) アップグレードタスクを使用して、中間リリースへの直接アップグレードを実行する
- PCD 移行タスクを使用して、中間リリースから現行リリースへの移行を実行する

下の表から開始リリースを見つけ、アップグレードおよび移行プロセスのステップとして使用できる中間リリースを特定します。 中間リリースを特定したら、以下の手順にあるリンクを使用して、そのリリースのドキュメントを見つけます。

開始リリースがリストにない場合、複数の中間リリースへのアップグレードが必要な場合があります。 「Supported Upgrade and MigrationPaths with COP Files」の表を参照してください https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/compat/15_x/cucm_b_compatibility-matrix-cucm-imp-15x.html。

表 *13* : レガシーリリースから *Unified CM* および *IMP and Presence Service Release 15* へのアップグレードする

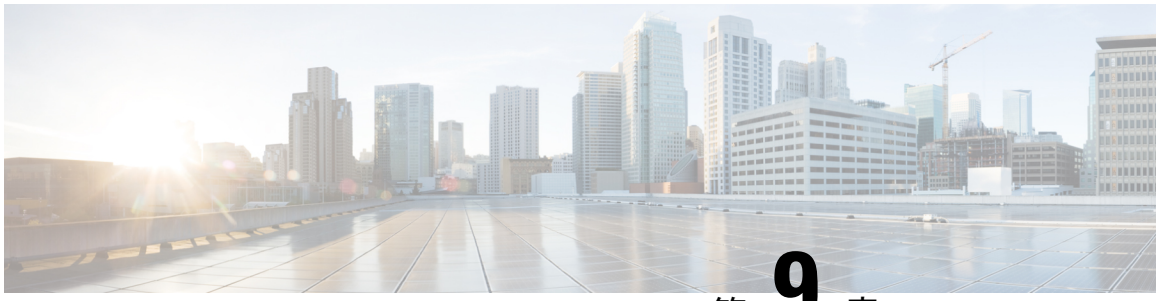
インストールされているバージョン	仮想マシン上でこのバージョンに移行する
7.0 (1) およびそれ以前	移行できません。 最初から最新のリリースに再構築することをお勧めします。
8.0(1) および 9.1	PCD 12.6（PCD 14 または PCD 15 は使用しない）を使用して、バージョン 12.5 に直接移行します。 可能なさまざまな移行オプションについて、このガイドの最初の章を参照してください。

手順

ステップ 1 中間リリースのアップグレードドキュメントを参照し、手順に従ってシステムをアップグレードしてください。

- Unified Communications Manager アップグレードのドキュメントについては、「http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-guides-list.html」を参照してください。
- IM and Presence Service（旧称 Cisco Unified Presence）のアップグレードドキュメントについては、「http://www.cisco.com/c/en/us/support/unified-communications/unified-presence/products-installation-guides-list.html」を参照してください。

ステップ 2 『*Cisco Prime Collaboration* 展開管理ガイド http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html』を参照し、手順に従って現行リリースへの PCD の移行を実行してください。



第 9 章

トラブルシューティング

アップグレード失敗後にログファイルをダンプする

Unified Communications Manager または IM and Presence Serviceのアップグレードで障害が発生した場合はこの手順を使用します。

始める前に

ログファイルを開くには、7-Zip ユーティリティが必要です。 http://www.7-zip.org/download.html に進みます。

手順

ステップ 1 新しい空のファイルをシリアルポートに添付します。 VM の設定を編集し、ログをダンプする場所にファイル名を添付します。

（注） アップグレードの失敗によりシステムが停止し、ログダンプのプロンプトが表示された場合は、空のファイルを添付してから **はい** と選択して処理を続行してください。

ステップ 2 VM コンソールに戻り、シリアル ポートにログをダンプします。

ステップ 3 処理が完了したら、**[インベントリ]** > **[データストア]** および **[データストアクラスタ]** をクリックします。

ステップ 4 ファイルを作成したデータストアを選択します。

ステップ 5 右クリックして **[データストアを参照（Browse Datastore）]** を選択し、作成したファイルを参照します。

ステップ 6 ファイルを右クリックして [**ダウンロード**] を選択し、ファイルを保存する PC 上の場所を選択します。

ステップ 7 7-Zip を使用してファイルを開き、ファイルサイズを確認します。

- ファイルのサイズが 0 より大きい場合、ファイルを PC に展開してから、仮想マシンの設定を編集してシリアルポートを削除してください。
- ファイルサイズが 0 の場合、次のステップに進みます。

ステップ 8 ファイルサイズがゼロの場合、以下の手順を完了します。

a) 仮想マシンの電源をオフにします。
b) ログ出力用に新しいファイルを作成します。
c) インストールディスクのマッピングを解除します。
d) **[オプション（Options）]** タブで、**[オプションの起動（Boot Options）]** を選択して、**[強制 BIOSセットアップ（Force BIOS Setup）]** を有効にします。
e) 仮想マシンの電源を入れ、BIOS で起動するのを待ちます。
f) BIOS で、ハードドライブを最初の起動デバイスとして選択し、保存して終了します。システムはハードドライブから起動し、アップグレードが失敗したポイントに戻ります。失敗の通知が表示されます。
g) **[はい（Yes）]** と入力して、ファイルにログの内容をダンプします。
h) ファイルを探し、7-Zip を使用して開きます。

ステップ 9 ファイルのサイズが 0 より大きい場合、ファイルを PC に展開してから、仮想マシンの設定を編集してシリアルポートを削除してください。

Unified Communications Manager アップグレードのトラブルシューティング

この項では、トラブルシューティング Unified Communications Manager アップグレードに関して説明します。

アップグレードの失敗

問題 Unified Communications Manager パブリッシャノードをアップグレードして、新しいバージョンに切り替えた後、またはアップグレードサイクル中に失敗したクライアントでサブスクライバノードの 1 つをアップグレードすると、サブスクライバノードのアップグレードが失敗します。

解決法 次のいずれかを実行します。

- サブスクライバノードでのアップグレード失敗の原因になったエラーを修正します。 クラスタ内のノードのネットワーク接続を確認し、サブスクライバ ノードをリブートし、サブスクライバ ノードのサーバ メモリと CPU 使用率が高すぎないことを確認することができます。 サブスクライバノードを再度アップグレードしてください。

- Unified Communications Manager パブリッシャーノードのアクティブパーティションが、サーバにインストールされたソフトウェアの最新バージョンを実行していることを確認してください。 パブリッシャ ノードのアクティブ パーティションで実行されているのと同じソフトウェア バージョンを使用して、サブスクライバ ノードでフレッシュ インストールを実行します。 サブスクライバノードを再度インストールする場合は、『Administration Guide for Cisco Unified Communications Manager』 で説明されているように、Cisco Unified CM Administration からサーバーを削除してから、サーバーを再度追加する必要があります。

クラスターまたはシングルノードアップグレードの再試行

以前のアップグレードで [バージョンの切り替え] または [再起動] を実行せずにアップグレードを再試行する場合、再試行する前にノードを再起動します。

アップグレードが成功/失敗/キャンセルの場合に含まれる再起動

問題: 以下の段階で再起動しなかった場合、アップグレードに失敗したり、障害が発生する場合があります。

解決方法:次の場合は再起動が必要です:

1. 任意のアップグレード（レガシーアップグレード/シンプルアップグレードまたは PCD 経由のアップグレード）が成功するまたは失敗する:
   - L2アップグレードが失敗し、アップグレードが再度必要な場合にのみ、リブートが必要です。
   - L2アップグレードが正常に完了した後、新しいバージョンに切り替えずに再度アップグレードする場合は、アップグレードを開始する前に、まずノードをリブートする必要があります。
   - RU アップグレードが失敗すると、古いパーティションに自動的に切り替わり、自動リブートが実行されます（アップグレード状態が失敗した場合、アップグレードをキャンセルし、ノードをリブートします）。
2. バージョンの切り替えが失敗した場合、機能に影響を与える可能性があるサービスマネージャやその他のサービスが停止する場合がああるため、これ以上の作業を行う前に、サーバーをリブートする必要があります。
3. いずれかの段階でアップグレードをキャンセルする場合は、他のアップグレードを試みる前に IM&P/UCM サーバを再起動する必要があります。

簡素化されたアップグレードの問題のトラブルシューティング

クラスターの一部のノードでダウンロードが失敗する

問題: 簡易アップグレードの実行中に、クラスタの一部のノードでダウンロードが失敗しました。

解決策: ダウンロードに失敗したノードのソフトウェアの場所の設定を確認します。 無効な場所または間違った資格情報が失敗の原因になる場合があります。「パブリッシャからのダウンロード資格情報を使用する」オプションを使用している場合、障害が発生したノードの構成が正しいことを確認してください。

確認するには、次のいずれかを実行します。

- ユーザーインターフェイス: ノードの **[インストール/アップグレード（Install/Upgrade）]** ページを開き、チェックボックスがオンになっているかを確認します。チェックされている場合、構成が正しいことを示します。 チェックボックスがオフの場合、オンにして、**[次へ（Next）]** をクリックし、設定を保存したら、**[キャンセル（Cancel）]** をクリックして、**[インストール/アップグレード（Install/Upgrade）]** ページを閉じます。
- CLI:[**utils system アップグレード開始**] コマンドを使用し、「パブリッシャーからのダウンロード資格情報を使用する (yes/no)」が「yes」に設定されていることを確認します。「yes」に設定されている場合、構成が正しいことを示します。 [いいえ（No）] になっている場合は、[はい（Yes）] に設定して、[q] を選択して終了し、**utils system upgrade cancel** コマンドを実行して正常に終了します。

（注） **[パブリッシャからのダウンロード資格情報を使用する**] が選択解除されている場合、サブスクライバがパブリッシャのダウンロード資格情報を使用しないため、Unified Communications Manager クラスタのアップグレードが失敗する場合があります。 各サブスクライバに移動して、**[パブリッシャからのダウンロード資格情報を使用（Use download credential from Publisher）]** オプションを選択し、サブスクライバがパブリッシャのダウンロード資格情報を使用できるようにする必要があります。

クラスタの一部のノードでダウンロードまたはインストールに失敗する

問題: 簡易アップグレードの実行中に、クラスタの一部のノードでダウンロードまたはインストールが失敗しました。

ソリューション: ユーザーインターフェイスまたは CLI を使用する**utils system upgrade cluster status** コマンド**[クラスタのインストール/アップグレード（Cluster Install/Upgrade）]** ページを開き、障害が発生したノードを特定します。 CLI から **utils system Upgrade Status** コマンドを実行して、アップグレードまたはインストールの操作がこれらの失敗したノードで進行中でないことを確認します。「Unified Communications Manager アップグレードのトラブルシューティング」セクションの「アップグレードの失敗」サブセクションに記載されている単一ノードのアップグレードのトラブルシューティング手順に従い、アップグレードを続行します。

（注） 簡素化されたアップグレードがダウンロードまたはインストールのフェーズで失敗した場合:

- ユーザーインターフェイス: **[クラスタのインストール/アップグレード（Cluster Install/Upgrade）]** ページに、各ノードの状態が表示されるので、[キャンセル（Cancel）] をクリックするまで、障害が発生したノードを特定でいます。
- CLI: **utils system upgrade cluster initiate** または **utils system upgrade cluster status** に、各ノードの状態が表示されるので、**utils system upgrade cluster cancel** コマンドが実行されるまで、障害が発生したノードを特定します。

クラスタの一部のノードでバージョンの切り替えまたは再起動に失敗する

問題: 簡易アップグレードの実行中に、クラスターの一部のノードでバージョンの切り替えまたは再起動が失敗しました。

ソリューション:ユーザーインターフェイスを使用して、**再起動/バージョンクラスタの切り替え** ページを開き、障害が発生したノードを特定します。 問題を修正して（ネットワーク/証明書の問題など）、**再起動/バージョン クラスタの切り替え**ページで、完了したノードをスキップして、スイッチバージョンを再試行するか、障害が発生したノードを再起動します。

クラスタのアップグレード中に Unified Communications Manager Publisher が再起動/電源が再投入され、クラスタのアップグレードステータスが表示されなくなります。

問題: クラスタのアップグレード中に Unified Communications Manager パブリッシャが再起動/電源が再投入され、クラスタのアップグレードステータスが表示されなくなりました。

解決方法: Unified Communications Manager パブリッシャーがクラスターのアップグレード操作を制御します。 アップグレード中に再起動したり、電源を入れ直してはいけません。 これを行うと、プロセスが強制終了され、他のノードからステータスを取得できなくなります。 また、Unified Communications Manager パブリッシャが他のノードに指示を出すことができないため、アップグレードが失敗します。 各ノードにログインし、アップグレードをキャンセルします。

クラスタのアップグレード中の高 CPU アラート

問題: クラスタのアップグレード中に高 CPU アラートを受信しました

解決方法: サーバの使用率が最も低いときに、クラスターのアップグレードをスケジュールする必要があります。 アップグレードプロセスは CPU およびディスクを大量に消費するため、CPU アラートが発生する可能性があります。

クラスターのアップグレードに失敗した後で、クラスターのアップグレードを再試行する

問題: クラスタのアップグレードに失敗した後で、クラスタのアップグレードを再試行するには?

解決方法: まず、クラスタのアップグレードをキャンセルします。 アップグレードに失敗した後、アップグレードを再試行する前に、ノードを再起動することをお勧めします。

SSL エラーによるダウンロードの失敗

問題: SSL エラーのため、一部のノードでダウンロードに失敗しました。

解決方法: クラスターのノード間にSSL トラストがセットアップされていることを確認します。

スイッチバージョンまたはクラスタノードの再起動が、修正したバッチどおりに実行されませんでした

問題: スイッチバージョンまたは、クラスタノードの再起動が、修正したバッチどおりに実行されませんでした。

解決方法: クラスターの再起動またはバージョンを切り替える前に、変更したバッチオーダーが保存されていることを確認してください。

「スキップ」チェックボックスへの変更が保存されない

問題: スキップチェックボックスの選択は保存されません。

解決方法 : 再起動中やバージョン切り替え中に「スキップ」オプションを使用してノードを除外すると、この選択が保存されません。 毎回オプションを選択する必要があります。

クラスターのアップグレードまたはシングルノードのアップグレードを再試行できません

問題:クラスタのアップグレードまたはシングルノードのアップグレードを再試行できません。

ソリューション: CLI を使用する **utils system upgrade cluster cancel** コマンドを実行して、クラスタアップグレードをキャンセルします。 また、CLI を使用する **utils system upgrade cancel** コマンドを実行して、Unified Communications Managerパブリッシャで単一ノードをキャンセルします。

ディスク容量不足でアップグレードが失敗する

問題 Unified Communications Manager のアップグレードが失敗し、共通パーティションが一杯であることを示すエラーが表示されます。

解決法 通常、少なくとも 25G の共通パーティションスペースが必要です。ただし、多くの TFTP データ (デバイスファームウェアのロード)、保留音 (MOH) ファイルがある場合、または多くのロケールファイルがインストールされている場合は、導入により多くのスペースが必要になる場合があります。以下の操作の 1 つまたは複数を実行して、追加のディスクスペースを作成します。

- Cisco ログパーティション監視ツールを使用してローウォーターマークとハイウォーターマークを調整し、トレースを減らし、不要なログファイルを削除します。 低水準値を 30 に、高水準値を 40 に調整することを推奨します。アップグレード後、トレースの早過ぎる消去を避けるために、高水準と低水準を元の値に復元する必要があります。 最高水準点のデフォルト値は 85 です。最低水準点のデフォルト値は 80 です。Cisco ログパーティショ

ン監視ツールの使用方法の詳細については、 Cisco Unified Real-Time Monitoring Tool アドミニストレーションガイドを参照してください。。

- 仮想環境に追加のディスク容量がある場合、ディスク拡張 COP ファイル（ciscocm.vmware-disk-size-reallocation-<latest_version>.cop.sgn）を使用して vDisk のサイズを拡張します。 続行する前に、この COP ファイルをサポートする Readme ファイルを確認してください。
- Free Common Space COP ファイル (ciscocm.free_common_space_v<latest_version>.cop.sgn) を使用します。 この COP ファイルは、システムを再構築することなく、利用可能なディスクスペースを増やすために、共通パーティションの非アクティブ側を削除します。 続行する前に、この COP ファイルをサポートする Readme ファイルを確認してください。
- 古いまたは未使用のファームウェアファイルを TFTP ディレクトリから手動で削除します。 これらのファイルは、OS 管理インターフェースの TFTP ファイル管理ページを使用して削除できます。または、コマンドラインインターフェイスの `file list tftp` および `file delete tftp` コマンドを使用できます。

COP ファイルと Readme ファイルは Cisco.com からダウンロードできます。 **[サポート（Support）] > [ダウンロード（Downloads）] > [Cisco Unified Communications Managerバージョン 10.0（Cisco Unified Communications Manager Version 10.0）] > [Unified Communications Manager/CallManager/Cisco Unity Connection Utilities]** の順に選択します。

失敗したアップグレードの再開

システムにエラーがあり、アップグレードを再開する前に修正する必要がある場合は、次のプロセスに従ってください。

（注） 障害が発生した場合は、ノードを再起動し、アップグレードプロセスを再開する必要があります。

手順

ステップ 1 アップグレードをキャンセルします。

アップグレードをキャンセルした場合でも、完全にダウンロードされた ISO ファイルのダウンロードは保持されます。

ステップ 2 システムの問題を解決してください。

ステップ 3 アップグレードを再開する準備ができたら、`utils system upgrade initiate` CLI コマンドを実行して、`[ローカルイメージ（Local Image）]` オプションを選択します。

ステップ 4 システムのアップグレードを完了します。

アクセス制御グループの権限の削減

問題 既存のユーザに新しいアクセスコントロールグループを追加すると、既存のアクセスコントロールグループの権限レベルが予期せず低下します。

解決法 ユーザは複数のアクセスコントロールグループに属することができます。 既存のユーザーに新しいアクセス制御グループを追加する際、アクセス制御グループで、「[重複するユーザーグループとロールに対する有効なアクセス権限（Effective Access Privileges for Overlapping User Groups and Roles）]」 エンタープライズパラメータが最小に設定されている場合、一部の既存アクセス制御グループの現在のレベルの権限が削減される場合があります。

アクセス権限の削減は、たとえば、Cisco Unified CM Administration のアップグレード中など不注意によって発生する可能性があります。アップグレードバージョンが、「[重複するユーザーグループとロールに対する有効なアクセス権限（Effective Access Privileges for Overlapping User Groups and Roles）]」 エンタープライズパラメータが最小に設定されている Standard RealTimeAndTrace Collection ユーザーグループをサポートする場合、すべてのユーザーが、アップグレード中にそのユーザーグループに自動追加されます。 この例の権限の問題を解決するには、標準の RealTimeAndTrace コレクションユーザグループからユーザを削除します。

電話設定の消失

他の製品バージョンにアップグレードした後に、Unified Communications Manager をインストールしたり、スイッチオーバーした直後、電話ユーザーが構成した設定がリセットされる場合があります。 電話ユーザが構成する設定の例には、着信の転送や待機メッセージ表示の設定などがあります。 この状況は、アップグレード期間中に構成が変更された場合に発生する可能性があります。 インストールとアップグレード後に Unified Communications Manager がデータベースを同期すると、電話ユーザーが行った設定変更が上書きされる場合があります。 Cisco はアップグレード中に設定を変更しないことを推奨します。

Unified Communications Manager パブリッシャノードのアップグレード後の失敗

問題 アップグレードに成功し、クラスタは新しいリリースを実行していますが、 Unified Communications Manager パブリッシャーノードで障害が発生しました。

解決法 次のいずれかを実行します。

- DRS バックアップファイルを使用する Unified Communications Manager パブリッシャノードを復元する
- DRS バックアップファイルがない場合は、すべての IM and Presence Service ノードを含むクラスタ全体を再インストールする必要があります。

Unified Communications Manager サブスクライバノードのアップグレード後の失敗

問題 アップグレードに成功し、クラスタは新しいリリースを実行していますが、その後、Unified Communications Manager サブスクライバノードが失敗します。

解決法 次のいずれかを実行します。

- DRS バックアップファイルを使用する Unified Communications Manager サブスクライバノードを復元します。
- DRS バックアップ ファイルがない場合、サブスクライバ ノードで再度アップグレードを実行する必要があります。 再インストールする前に、 Unified Communications Manager パブリッシャーノードのサーバページからサブスクライバーノードを削除する必要はありません。

IM および Presence アップグレードのトラブルシューティング

このセクションでは、 IM and Presence Service サービスのアップグレードのトラブルシューティングに関する情報を記載します。

IM and Presence データベースパブリッシャノードのアップグレードの失敗

問題 Unified Communications Manager と IM and Presence Service の両方のノードを含むマルチノードクラスタをアップグレードする際、IM and Presence Service データベース パブリッシャ ノードの更新に失敗しました。

解決法 実行するアクションは、障害が発生したポイントによって異なります。

- IM and Presence Service データベース公開者ノードが新しいソフトウェアのバージョンに切り替えた後に障害が発生した場合、すべてのノードを元に戻し、再度アップグレードを実行する必要があります。 以下のタスクを記載されている順に実行します。
  - Unified Communications Manager パブリッシャーノードを元に戻す
  - Unified Communications Manager サブスクライバノードを元に戻す
  - IM and Presence Service データベース公開者ノードを元に戻す
  - Unified Communications Manager パブリッシャノードを再度アップグレードする
  - Unified Communications Manager パブリッシャノードを新しいソフトウェアのバージョンに切り替える

- Unified Communications Manager サブスクライバノードを再度アップグレードする
- Unified Communications Manager サブスクライバノードを新しいソフトウェアのバージョンに切り替える
- IM and Presence Service データベースパブリッシャノードを再度アップグレードしてください

IM and Presence サブスクライバ ノードのアップグレードの失敗

問題 Unified Communications Manager と IM and Presence Service ノードの両方を含むマルチノードクラスタをアップグレードしようとしていますが、IM and Presence Service サブスクライバノードのアップグレードに失敗しました。

解決法 実行するアクションは、障害が発生したポイントによって異なります。

- ノードを新しいバージョンに切り替えた後に、IM and Presence Service サブスクライバノードでのアップグレードが失敗した場合、一覧されている順番に次のタスクを完了する必要があります。
  - Unified Communications Manager パブリッシャーノードを以前のソフトウェアバージョンに切り替える
  - Unified Communications Manager サブスクライバノードを以前のソフトウェアバージョンに切り替える
  - IM and Presence Service データベース パブリッシャノードを以前のソフトウェアのバージョンに切り替える
  - IM and Presence Service サブスクライバノードを以前のソフトウェアのバージョンに切り替える
  - Unified Communications Manager パブリッシャノード パブ フォワードを新しいソフトウェアのバージョンに切り替える
  - IM and Presence Service データベース パブリッシャノード フォワードを新しいソフトウェアのバージョンに切り替える
  - IM and Presence Service サブスクライバーノードのアップグレードを再度実行する

IM and Presence ユーザー電話プレゼンスの問題

問題 IM and Presence サーバのアップグレード後、すべてのアクティブ化された機能サービスとネットワークサービスが開始されると、IM and Presence がユーザからの電話プレゼンスの更新が遅延したり、遅くなったりする。

解決法 Cisco SIP Proxy サービスを再起動してください。 [Cisco Unified IM and Presenceのサービスアビリティ（Cisco Unified IM and Presence Serviceability）] で、**[ツール（Tools）] > [コントロールセンター-機能サービス（Control Center - Features Services）]** を選択します。

プレゼンスのユーザエクスペリエンス 可用性を得る際の問題

問題 IM and Presence Service サーバーアップグレード後にすべてのアクティブ化された機能サービスとネットワークサービスを起動すると、ユーザーは、プレゼンスの可用性が一貫しないと感じます。 ユーザは IM and Presence Service にログインできますが、主に SIP ベースのクライアントから可用性情報を取得する際に問題が発生します。

解決法 この問題は、 IM and Presence Service のアップグレード中にユーザがプロビジョニングされた場合に発生します。 ユーザの割り当てを解除してから再割り当てしてください。

Cisco SIP Proxy サービスへの Real-Time Monitoring Tool アラート

問題 IM and Presence Service サーバーのアップグレード後、アクティブ化されたすべての機能とネットワークサービスが開始されると、Cisco SIP Proxy サービスに対して、Real-Time Monitoring Tool CoreDumpFileFound アラートが生成されます。

解決法 Cisco SIP Proxy サービスを再起動してください。 [Cisco Unified IM and Presenceのサービスアビリティ（Cisco Unified IM and Presence Serviceability）] で、**[ツール（Tools）] > [コントロールセンター-機能サービス（Control Center - Features Services）]** を選択します。

リモートサーバ上にアップグレードファイルが見つかりません

問題 リモートサーバ上でアップグレードファイルが見つかりません。

解決法 アップグレードファイルが Linux または UNIX サーバ上にある場合、指定するディレクトリパスの先頭にスラッシュを入力する必要があります。 例えば、アップグレードファイルがパッチディレクトリにある場合、**/patches** と入力する必要があります。 アップグレードファイルが Windows サーバ上にある場合、システム管理者に連絡してディレクトリパスを確認してください。

アップグレードファイルのチェックサム値が一致しません

問題 アップグレードファイルのチェックサム値が、Cisco.com に表示されているチェックサムと一致しません。

解決法 アップグレードファイルの信頼性と整合性を確保するために、2 つのチェックサム値が一致する必要があります。 チェックサム値が一致しない場合は、Cisco.com から最新バージョンのファイルをダウンロードし、再度アップグレードを試してください。

データベースのレプリケーションは完了しませんでした

問題 アップグレード後、データベースリプリケーションが完了せず、**utils dbreplication runtimestate** コマンドの結果が 2 ではありませんでした。

解決法 アップグレードが完了し、新しいソフトウェアにバージョンを切り替えると、データベースの複製が自動的に実行されます。 この間、サブスクライバ ノードのコア サービスは開始されません。 大規模な展開におけるデータベースのレプリケーションは、完了までに数時間かかる場合があります。 数時間後、**utils dbreplication runtimestate** コマンドで、データベースリプリケーションが完了しなかったと表示される場合、データベースリプリケーションをリセットする必要があります。 パブリッシャノードで `utils dbreplication reset all` コマンドを実行します。

バージョン エラー

バージョンがアクティブまたは非アクティブのバージョンと一致しない

問題 IM and Presence Service サーバのアップグレード中、ディスクまたはリモートディレクトリからソフトウェアイメージを選択することはできません。 次のエラーが報告されます: 名前から取得したバージョンは、パブリッシャーのアクティブまたは非アクティブバージョンと一致しません。

解決法 バージョン マッチング ルールが満たされていません。 ソフトウェアのバージョンは、次の要件を満たす必要があります。

- IM and Presence Service データベース パブリッシャノードのソフトウェアのバージョン（アップグレードした最初の IM and Presence Service ノード）は、Unified Communications Manager パブリッシャノードにインストールしたソフトウェアのバージョンの最初の 2 桁と一致している必要があります。 Unified Communications Manager パブリッシャーノードにインストールされているソフトウェアのバージョンはアクティブまたは非アクティブの可能性があります。 例えば、 IM and Presence Service ソフトウェアバージョン 10.0.1.10000-1 は、 Unified Communications Manager ソフトウェアバージョン 10.0.1.30000-2 と互換性があります。 Unified Communications Manager および IM and Presence サービスノードをアップグレードする際には、シーケンスルールに従うようにしてください。
- アップグレードする IM and Presence Service サブスクライバノードのソフトウェアのバージョンは、IM and Presence Service データベース パブリッシャノードにインストールされているソフトウェアのバージョンの最初の 5 桁と一致している必要があります。

アップグレードする最初のノードが Unified Communications Manager パブリッシャーノードまたは IM and Presence Service データベースパブリッシャーノードであることを確認するか、またはソフトウェアアップグレード用の別のイメージを選択してください。

Cisco IM and Presence ノードのバージョン切り替えが失敗した

問題 Cisco IM and Presence ノードでのバージョン切り替えが失敗します。 次のエラーが報告されます: バージョンが一致しません。 発行元でバージョンを切り替えてから、もう一度お試しください。

解決法 バージョンマッチングルールが満たされていません。 ソフトウェアのバージョンは、次の要件を満たす必要があります。

- IM and Presence Service データベース パブリッシャノードのソフトウェアのバージョン（アップグレードした最初の IM and Presence Service ノード）は、Unified Communications Manager パブリッシャノードにインストールしたソフトウェアのバージョンの最初の 2 桁と一致している必要があります。 例えば、 IM and Presence Service サービスソフトウェアバージョン 10.0.1.10000-1 は、 Unified Communications Manager ソフトウェアバージョン 10.0.1.30000-2 と互換性があります。
- アップグレードする IM and Presence Service サブスクライバノードのソフトウェアのバージョンは、IM and Presence Service データベース パブリッシャノードにインストールされているソフトウェアのバージョンの最初の 5 桁と一致している必要があります。

このエラーを修正するには、切り替える最初のノードがUnified Communications Manager 公開者ノードまたは IM and Presence Service データベース公開者ノードになっていることを確認してください。

アップグレードがキャンセルされたか、失敗しました

いずれかの段階でアップグレードをキャンセルした場合、またはアップグレードが失敗した場合は、次のアップグレードを試みる前に、 IM and Presence Service サーバを再起動する必要があります。

ディレクトリが見つかり検索されましたが、有効なオプションまたはアップグレードが利用できませんでした

問題 IM and Presence Service アップグレード中、有効なアップグレードパスとファイルにも関わらず、 IM and Presence Service サーバが次のエラーメッセージを表示します:

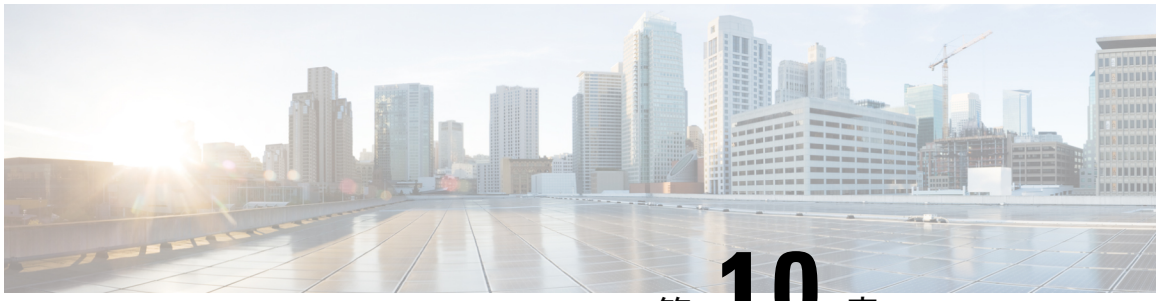
ディレクトリが見つかり検索されましたが、有効なオプションまたはアップグレードはありませんでした。 マシンはダウングレードできないため、以前のリリースのオプションとアップグレードファイルは無視されます。

解決法 アップグレードマネージャはアップグレード中に IM and Presence Service と Unified Communications Manager 間の接続をチェックしてバージョンを検証します。 これに失敗すると、 IM and Presence Service サーバはアップグレードパスとファイルが有効であってもエラーメッセージを表示します。 アップグレードを開始する前に、Cisco Unified CM IM and Presence 管理システムトラブルシューティングなどのツールを使用して、 IM and Presence Service と Unified Communications Manager の間の接続性を確認してください。

共通パーティションのフルアップグレードの失敗

問題 IM and Presence Service のアップグレードが失敗し、共通パーティションが一杯であることを示すエラーが表示されます。

解決法 COP ファイル ciscocm.free_common_cup_space_v<latest_version>.cop.sgn をダウンロードして適用します。 このCOPファイルは共通パーティションをクリーンアップし、その後のアップグレードが通常通り進行できるようにします。



第 10 章

FAQ

FAQ

新しいリリースとは異なる仮想環境要件を持つ Unified Communications Manager または IM and Presence Service のリリースからアップグレードしようとしています。 どうすればよいですか?

表中の情報を使用して新しいリリースの要件を確認します。 新しいリリースの要件を確認したら、手順について 仮想マシンの設定タスク （77 ページ） を参照してください。

表 *14* : 仮想マシンの要件

項目	説明
OVA テンプレート	OVA ファイルは、仮想マシン設定用の定義済みテンプレート一式を提供します。 これらは、サポートされている容量レベルや、必要な OS/VM/SAN 連携などの項目をカバーしています。 Unified Communications Manager および IM and Presence Service アプリケーション用に提供された OVA ファイルから VM 設定を使用する必要があります。 OVA ファイルから使用する正しい VM 設定は、展開のサイズに基づきます。 OVA ファイルについての情報は、次の場所で「Unified Communications Virtualization サイジングガイドライン」を検索してください https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/collaboration-virtualization-sizing.html。

項目	説明
VMware vSphere ESXi	互換性とリリースのサポート要件を満たすvSphere ESXiハイパーバイザーのバージョンをインストールする必要があります。 Cisco Prime Collaboration Deployment (PCD) を使用してアップグレードまたは移行を実行する場合、vSphere ESXi を正しいライセンスタイプでインストールしていることを確認する必要があります。 PCD は、vSphere ESXi のすべてのライセンスタイプと互換性があるわけではありません。これらのライセンスの一部は必要な VMware API を有効にしないためです。
VMware vCenter	Unified Communications Manager または IM and Presence Service を、Business Edition 6000/7000 アプライアンスまたは UC on UCS テスト済み参照設定ハードウェアにデプロイする場合、VMware vCenter は任意です。 UC on UCS 仕様ベースまたはサードパーティサーバー使用ベースのハードウェアをデプロイする場合、VMware vCenter は必須です。

項目	説明
VM 設定の仮想ハードウェアの仕様	Unified Communications Manager または IM and Presence Serviceの新しいリリースにアップグレードするために VM の vRAM を変更する必要があるかどうかを確認してください。 お使いの Unified Communications Manager または IM and Presence Service リリース 15 では、現在実行しているよりも多くの vRAM が必要な場合があります。 古いリリースバージョンに十分な vRAM サイズがない場合、 IM and Presence Service リリース 15 への直接アップグレードは失敗します。 Unified Communications Manager または IM and Presence Service リリース 15 のバージョンでは、現在実行しているよりも多くの GB と異なるパーティションが必要になる場合があります。 Unified Communications Manager および IM and Presence Service リリース 15 への直接アップグレードは、HDD サイズを手動で 110 GB にサイズ変更した場合でも、すべての単一の 80 GB vDisk 展開で失敗します。 アップグレードの前に vRAM および vDisk の仕様書を確認して、リリース 15 のベース OVA の Readme を参照するか、または QuoteCollab ツールを使用します。 詳細については、次を参照してください。 • 仮想マシンの設定タスク （77 ページ） をクリックして VMware を更新します。 • vDisk を更新するには、リリース 12.5 または 14 および SU バージョンのいずれかを、ここで直接アップグレードが成功した 110GB として vDisk がインストールされた新しい VMware にバックアップまたは復元します。 または、PCD 移行またはデータ インポート タスク移行を伴うフレッシュ インストールのいずれかを使用して、Unified CM Release 15 OVA テンプレートで展開された新しいノードに移動します。

仮想環境の要件の詳細については、 .. www.cisco.com go virtualized-collaborationに移動して確認してください:

- Unified Communications Manager および IM and Presence Service アプリケーションのリンクをたどり、リリースの要件を確認し、OVA ファイルをダウンロードします。
- 「Unified Communications VMware 要件」トピックを検索し、機能サポートとベストプラクティスに関する情報を見つけてください。

アップグレードの一環として、別の VM サイズに移動したいです。 VM 設定の仕様を編集することはできますか?

VM 設定の仕様を編集する前に、OVA の「ReadMe」ファイルを読み、アップグレードするリリースに固有の要件を確認してください。 OVA ファイルは、仮想マシン設定用の定義済みテンプレート一式を提供します。 これらは、サポートされている容量レベルや、必要な OS/VM/SAN 連携などの項目をカバーしています。 OVA ファイルから使用する正しい VM 設定は、展開のサイズに基づきます。

OVA ファイルについての情報は、 .. www.cisco.com go virtualized-collaboration で"Unified Communications Virtualization サイジングガイドライン"を検索してください。

OVA ファイルの入手方法については、 OVA テンプレートのダウンロードとインストール （80 ページ） を参照してください。

管理 XML (AXL) インターフェイスを使用して Unified Communications Manager 情報にアクセスして変更するアプリケーションがあります。 私のアプリケーションは Unified Communications Manager へのアップグレード後も引き続き動作しますか?

AXL アプリケーションのアップグレードについては、「https://developer.cisco.com/site/axl/learn/how-to/upgrade-to-a-new-axl-schema.gsp」を参照してください。 お使いのリリースでサポートされている AXL 操作のリストについては、「https://developer.cisco.com/site/axl/documents/operations-by-release/」を参照してください。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。