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

初版：2023 年 12 月 18 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.

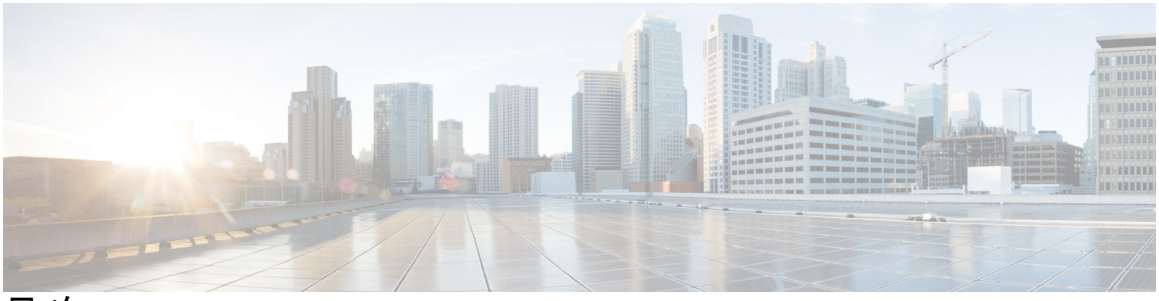
IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY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

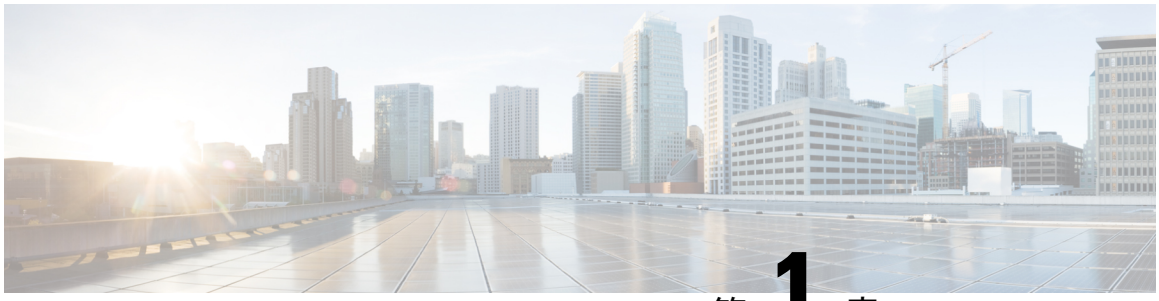
All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

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

新機能および変更された機能に関する情報

新機能および変更された機能に関する情報

次の表は、この最新リリースまでのガイドでの機能の主な変更点の概要を示したものです。ただし、今リリースまでのガイドにおける変更点や新機能の一部は表に記載されていません。

新機能および変更された機能に関する情報

表 *1:*

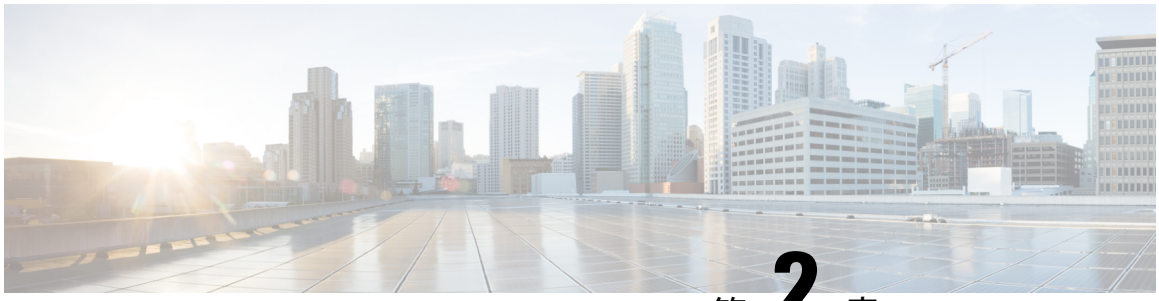
日付	説明	参照先
2023 年 12 月 18 日		• 要件および制約事項 （25 ページ） • 仮想マシンの構成 （26 ページ） • COP ファイルでサポートされているアップグレードおよび移行パス （10 ページ） • アップグレード準備 COP ファイルの実行（アップグレード前） （54 ページ） • VMware ツールの更新 （145 ページ） • IPSec の要件 （40 ページ）

新機能および変更された機能に関する情報

日付	説明	参照先
	Unified Communications Manager、IM and Presence Service、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行されました。 影響を受ける領域の一部は次のとおりです。 • Unified Communications Manager および IM and Presence Service 15 には、ESXi バージョン 7.0 U3 または 8.0 U1 が必要です。 • Unified Communications Manager のリリース 15 は、インストール時に最小 110 GB 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。 • 12.5.x より前の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、Unified Communications Manager と IM and Presence Service の新しいチェックが追加されました。 • Unified Communications Manager と IM and Presence Service 15 は、オープン VM ツールのみをサポートします。 • 3DES アルゴリズムを使用した IPSec ポリシーは、リリース 15 の FIPS モードではサポートされてい	

新機能および変更された機能に関する情報

日付	説明	参照先
	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の両方のオペレーティングシステムで実行されてい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（149 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

このマニュアルの手順では、Cisco Unified Communications Manager および 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ます。

このマニュアルの手順は、すべてのアップグレードおよび移行パスの開始点として使用してください。このガイドで使用されている「アップグレード」という用語を読む場合は、次のアップグレードの使用用語に注意してください。

- 「アップグレード」という用語は、すべてのクラスタノードがエンドツーエンドプロセスに必要な手順を完了するシナリオを指します。その結果、クラスタ全体がアップグレードされた宛先バージョンで実行されます。その後、アップグレードは「完了/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、すべてのノードがスイッチバージョンのリブートを完了し、すべてのクラスタノードでデータベースレプリケーションが完了することとして定義されます。アップグレードステータスの確認については、手動によるバージョン切り替え (クラスタ全体) （61 ページ） セクションを参照してください。
- 「非アクティブなバージョン」または「非アクティブな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、switch-version-reboot を実行しない、または実行する前に、非アクティブな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考慮事項

1. 「直接アップグレード」方法を選択します。単純なアップグレードを選択することをお勧めしますが、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が完了する必要があります。
   - 非アクティブなバージョンのアップグレード
   - スイッチ バージョンの再起動
   - クラスタ内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まで待機します。
3. 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、「シーケンス ルールと時間要件」の章に記載されているノード順序付けルールに従っていることを確認する必要があります。
4. ステップ 2 のすべての要件が満たされていないと、アップグレードは完了しません。Cisco Unified OS Administration のユーザ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、CLI コマンドを使用してステータスをモニタできます。また、すべてのクラスタでステップ 2 のすべての条件が満たされるまで、クラスタノードへのブロックの可能性について警告するバナーメッセージをユーザインターフェイスに表示し、機能を追加/更新/削除することもできます。

アップグレード方法

次の表では、アップグレードを完了するために使用できる、Cisco Unified Communications Manager、IM and Presence Service、およびアップグレードツールを使用して実行できるアップグレードのタイプについて説明します。

アップグレードタイプ	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直接アップグレードであり、基盤となるオペレーティングシステムではなく、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ります。これは通常、アップグレードの最も単純な形式であり、通常は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。この場合、OSは両方のリリースで同じです。 元のリリース 12.5 以降の場合、直接の標準アップグレードによって、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す。 **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) 以降の標準アップグレードでは、簡素化されたクラスタ規模のアップグレードを使用してクラスタ全体をアップグレードすることができます。	標準アップグレードを実行する際に、次のツールを使用できます。 • Unified OS 管理者 • CLI • PCD アップグレードタスク
直接更新アップグレード	直接更新アップグレードは直接アップグレードの一種で、アプリケーション ソフトウェアと、基盤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ります。多くの場合に、OS が異なる 2 つのリリース（メジャー/マイナー）間でアップグレードを行う場合に使用します。 **例**：12.5.x より前の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。	更新アップグレード プロセスを実行する際に、次のツールを使用できます。 • Unified OS 管理者 • CLI • PCD アップグレードタスク

アップグレードタイプ	説明	アップグレードツール
直接移行	直接の移行には、直接のアップグレードだけでは対処できない複数の要因が存在する場合の「再配置」が含まれます。直接移行は、次の場合に使用されます。 • サイトの移動 • アップグレードでインフラストラクチャ ハードウェアおよびプラットフォームの変更が必要とされる場合。 **例**：ESXi 5.5 および Cisco UCS M3 世代ハードウェア上の Unified CM 10.5(x) から ESXi 7.0 および Cisco UCS M5 世代ハードウェア上の 12.5(x) へのアップグレード。 • 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 • アップグレードで、元のリリースに存在しない直接アップグレード パスが必要になる場合。 **例**：ESXi 上の Unified CM 8.5(1) から ESXi 上の 12.5(x) へのアップグレード（直接アップグレード パスが存在しないため移行が必須）。 • V2V（Virtual to Virtual）の移行では、直接アップグレード パスがある場合でも、期間、サービスへの影響、短時間の停止時間など、アップグレード パスの複雑さの要因を軽減するために、直接移行が推奨されます。	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 インポートを使用した新規インストール

アップグレードタイプ	説明	アップグレードツール
データ インポートを使用したインストール	リリース 10.5 以降からリリース 15 へ移行する場合は、直接アップグレードや直接移行の代わりに、データ インポートを使用して新規インストールできます。次の手順を行います。 • 元のリリース（10x または 11x）に、COP ファイル **ciscocm.DataExport_v1.0.cop.sgn** をインストールします。 • 元のリリースのデータを Secure FTP（SFTP）サーバ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手順化されている場合は、ゼロタッチ クラスタ インストールになります）。 何らかの理由で以前のリリースにロール バックすることを決定した場合は、**ciscocm.DataExport_rollback_v1.0.cop.sgn** の COP ファイルをインストールします。	CLI はデータ インポートによるインストールを完了するために使用されます。
レガシー リリースからの移行	レガシー リリースとは、リリース 15 への直接アップグレード パスや直接移行パスが存在しないほど古いリリースを指します。PCD 移行、またはデータ インポートを使用したインストール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を行ってから、PCD 移行、またはデータ インポートを使用した新規インストールを行うしか、リリース 15 にアップグレードする方法はありません。 **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 への必要なアップグレード。	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（157 ページ）」を参照してください。

現在のシステムの記録を取得する

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の記録を取得します。現在の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。次のような機能があります。

- Cisco Unified Communications Manager および IM and Presence Service のアップグレード前のバージョン
- 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 でオプションの導入として導入されました。リリース4.x 以降では、VMware が必須になりました。

アップグレード前アップグレード準備状況 COP ファイルを実行することによって、バージョンを取得できます。詳細については、「アップグレード準備 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

次の表に、Cisco Unified Communications Manager のリリース 15 と IM and Presence Service にアップグレードするためにサポートされているアップグレード パスを示します。次の表は、COP ファイルが必要なアップグレード パスを示しています。Cisco Unified OS 管理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 Cisco 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は、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） 特に指定がない限り、各リリースカテゴリにはそのカテゴリ内の SU リリースが含まれています。

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。アップグレードの宛先バージョンを選択した後、[**Unified Communications Manager ユーティリティ（Unified Communications Manager Utilities**）] を選択して、COP ファイルのリストを表示します。

（注） 必須ではありませんが、アップグレードの成功を最大化するためにアップグレード前にアップグレード準備の COP ファイルを実行することを強く推奨します。Cisco TAC では、有効なテクニカルサポートを提供するために、この COP ファイルを実行する必要がある場合があります。

（注） ソースが FIPS モードおよび/または PCD が FIPS モードの場合、COP ファイル `ciscocm.ciscossl7_upgrade_CSCwa48315_CSCwa77974_v1.0.k4.cop` に関する情報については、https://www.cisco.com/web/software/286319173/139477/ciscocm.ciscossl7_upgrade_CSCwa48315_CSCwa77974_v1.0.k4.cop-ReadMe.pdf 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） ソースリリースからリリース 15 への直接標準アップグレードが利用可能な場合は、単一ノードまたはクラスタ全体のアップグレードを選択できます。

クラスタ全体をアップグレードし、期間、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ようにするには、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 パブリッシャ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）」の手順を使用します。ここでは、Unified CM パブリッシャ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単一ノードのみを使用する場合は、「クラスタノードのアップグレード（直接更新）」セクション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』で説明されているように、アップグレード計画がノードシーケンシング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 ノードでバージョンを切り替える前に、まずパブリッシャノード、サブスクライバノードの順に Unified Communications Manager ノードを切り替える必要があります。

上記の手順に従わず、Unified Communications Manager Publisher ノードがバージョン 15 に切り替えられ、IM and Presence Service Publisher ノードのバージョンが 12.5.x または 14 および SU のバージョンのままであり、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）] メニューの次のページは、IM and Presence Service ノードでは表示または機能しません。

- クラスタの再起動/バージョン切り替え
- クラスタソフトウェアの場所
- ソフトウェアのインストールおよびアップグレードクラスタ

（注） Unified Communications Manager および IM and Presence Service リリース 15 でサポートされている直接リフレッシュの更新のパスはありません。12.5.x より前の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 *2 : Cisco Unified Communications Manager* および *IM and Presence Service* のアップグレード パス

送信元	送信先	メカニズム	前提条件	バージョンスイッチング * (送信元から宛先、またはその逆)
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。移行先バージョンが 15 で、ソースバージョンが 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。 移行先バージョンが 15 で、ソースバージョン 10.0 が FIPS モードの場合、Cisco Prime Collaboration Deployment (PCD) は非 FIPS モードである (または置かれる) 必要があります。	N/A

送信元	送信先	メカニズム	前提条件	バージョンスイッチング * (送信元から宛先、またはその逆)
10.5	15	PCD 15 移行タスク（V2V）	アップグレード前チェック 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。移行先バージョンが 15 で、ソースバージョンが 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。 移行先バージョンが 15 で、ソースバージョン 10.5 が FIPS モードの場合は、次のいずれかを実行します。 • PCD は非 FIPS モードである（または置かれている）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。	N/A
		データインポートを使用したフレッシュインストール（V2V）	• アップグレード前チェック 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

送信元	送信先	メカニズム	前提条件	バージョンスイッチング * (送信元から宛先、またはその逆)
11.0	15	PCD 15 移行タスク（V2V）	アップグレード前チェック 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。 移行先バージョンが 15 で、ソースバージョン 11.0 が FIPS モードの場合は、次のいずれかを実行します。 • PCD は非 FIPS モードである（または置かれている）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
		データインポートを使用したフレッシュインストール（V2V）	• アップグレード前チェック 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

送信元	送信先	メカニズム	前提条件	バージョンスイッチング * (送信元から宛先、またはその逆)
11.5	15	PCD 15 移行タスク（V2V）	アップグレード前チェック 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。 移行先バージョンが 15 で、ソースバージョン 11.5 が FIPS モードの場合は、次のいずれかを実行します。 • PCD は非 FIPS モードである（または置かれている）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
		データインポートを使用したフレッシュインストール（V2V）	• アップグレード前チェック 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

送信元	送信先	メカニズム	前提条件	バージョンスイッチング * (送信元から宛先、またはその逆)
12.0	15	PCD 15 移行タスク（V2V）	アップグレード前チェック 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。 ソースバージョンが Unified Communications Manager (12.0.1.10000-10) のリリース 12.0(1) の場合、次の COP ファイルをインストールする必要があります：ciscocm-slm-migration.k3.cop.sgn。これは、ソースバージョンがより高い場合（リリース 12.0(1)SU1 など）は必要ありません。	サポート対象外
		データインポートを使用したフレッシュインストール（V2V）	• アップグレード前チェック 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

送信元	送信先	メカニズム		前提条件	バージョンスイッチング * (送信元から宛先、またはその逆)
12.5	15	標準の直接アップグレード（シンプル アップグレード）	OS 管理者または CLI 経由	• アップグレード前チェック COP ファイルを実行します。	サポート対象
		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		サポート対象

送信元	送信先	メカニズム		前提条件	バージョンスイッチング * (送信元から宛先、またはその逆)
				• アップグレード前チェック COP ファイルを実行します。 • Unified CM ソースが 12.5.1.14900-63 より古い場合は、次の COP ファイルをインストールします。 ciscocm.enable-sha512sum-2021-signing-key-v1.0.cop.sgn • IM and Presence Service のソースが 12.5.1.14900-4 より古い場合は、次の COP ファイルをインストールします： ciscocm.enable-sha512sum-2021-signing-key-v1.0.cop.sgn。 • 移行先バージョンが 15 で、ソースバージョン 12.5 が FIPS モードの場合は、次のいずれかを実行します。 • PCD は非 FIPS モードである（または置かれている）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は、アップグレードを開始する前に、リリース 12.5.x システムに次の COP ファイルをインストールします： ciscocm.imp15_upgrade_v1.0.k4.cop.sha512。 COP ファイルは、次の場合にのみ適用されることに注意してください。 • Unified Communications Manager の接続先バージョンはリリース	

送信元	送信先	メカニズム		前提条件	バージョンスイッチング * (送信元から宛先、またはその逆)
				15 です。 • Unified Communications Manager の接続先バージョンがリリース 15 であり、IM and Presence Service の送信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）		アップグレード前チェック 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。 移行先バージョンが 15 で、ソースバージョン 12.5 が FIPS モードの場合は、次のいずれかを実行します。 • PCD は非 FIPS モードである（または置かれている）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
		データインポートを使用したフレッシュインストール（V2V）		• アップグレード前チェック 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

送信元	送信先	メカニズム		前提条件	バージョンスイッチング * (送信元から宛先、またはその逆)
14 および SU	15	標準の直接アップグレード（シンプル アップグレード）	OS 管理者または CLI 経由	アップグレード前チェック COP ファイルを実行します。	サポート対象
		直接標準アップグレード	PCD アップグレード タスク経由		サポート対象

送信元	送信先	メカニズム		前提条件	バージョンスイッチング * (送信元から宛先、またはその逆)
				アップグレード前チェック COP ファイルを実行します。 • 移行先バージョンが 15 で、ソースバージョン 14 が FIPS モードの場合は、次のいずれかを実行します。 • PCD は非 FIPS モードである（または置かれている）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は、アップグレードを開始する前に、リリース 14 または SU システムに次の COP ファイルをインストールする必要があります：`ciscocm.imp15_upgrade_v1.0.k4.cop.sha512`。COP ファイルは、次の場合にのみ適用されることに注意してください。 • Unified Communications Manager の接続先バージョンはリリース 15 で、IM and Presence Service の送信元ノードは 14 または 14SU1 バージョンです。 • Unified Communications Manager の接続先バージョンがリリース 15 であり、IM and Presence Service の送信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	

送信元	送信先	メカニズム	前提条件	バージョンスイッチング * (送信元から宛先、またはその逆)
			ます。	
		PCD 15 移行タスク（V2V）	アップグレード前チェック 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。 接続先バージョンが 15 で、送信元バージョンが 14 または SU が FIPS モードの場合は、次のいずれかを実行します。 • PCD は非 FIPS モードである（または置かれている）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
		データインポートを使用したフレッシュインストール（V2V）	• アップグレード前チェック 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、新しいバージョンを非アクティブバージョンとしてインストールし、必要に応じて新しいバージョンと古いバージョンを切り替えることができる機能です。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ますが、移行ではサポートされません。

（注） PCD の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てサポートされているすべてのパスでは、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

選択可能な複数のメカニズムがあ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、次の表を参照してください。

（注） レガシー アップグレードについては、「レガシー リリースからのアップグレード （157 ページ）」を参照してください。

表 3: アップグレード方法の選択

アップグレード方法	サポート	このメソッドを使用するタイミング	アップグレードまたは移行を完了する方法
統合された OS 管理または CLI のアップグレード	Cisco Unified OS 管理 GUI または CLI を使用した直接アップグレード (標準または更新)。	このツールは次の場合に考慮してください。 • クラスタ全体のアップグレードを簡素化するため • アプリケーションソフトウェアを変更するだけで、ハードウェアまたは VMware は更新されません。 • 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 Service のみをアップグレードする場合。その他の 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ています。 （注） CLI のアップグレードでは、Unified OS 管理者のアップグレードと同じサポートが提供されますが、別のインターフェイスからもサポートされます。	アップグレード作業 （49 ページ）に進みます。

アップグレード方法	サポート	このメソッドを使用するタイミング	アップグレードまたは移行を完了する方法
PCD のアップグレード	Cisco Prime Collaboration 導入のアップグレードタスクを使用して、直接アップグレード (標準または更新) を処理します。	このツールは、次の場合に考慮してください。 • 複数のクラスタをアップグレードすることができます。 • クラスタに多数のノードがあるため、アップグレードのオーケストレーションを行って予定を早める必要がある場合。 • Cisco Unity Connection や Cisco Unified Contact Center Express などの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。	リリースから 10. x 以降 1. アップグレード準備 COP ファイルの実行（アップグレード前） （54 ページ） 2. アップグレードまたは移行タスクを実行するには、『Cisco Prime Collaboration Deployment Administration Guide』を参照してください。 3. アップグレード準備 COP ファイルの実行（アップグレード後） （72 ページ） （注） リリースのリリースが 9.x よりも前の場合、アップグレード準備状況の COP ファイルは機能しません。付録では、手動で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完了する必要があります。
PCD 移行	Cisco Prime Collaboration Deployment による移行を処理します。	次の場合にこのツールを検討してください。 • 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ようとしています。 • ソースのリリースは、VMware をサポートしていないため、古いリリースです。 • 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の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。 • ソースリリースは以前の11.5 バージョンから直接アップグレードされており、ディスク容量の問題が発生しています。使用可能なディスク領域を最大化するために、最新のスタックに再インストールする必要がある場合があります。 • 一時的に重複する Vm とそのハードウェアが必要なインフラストラクチャを使用できます。	

アップグレード方法	サポート	このメソッドを使用するタイミング	アップグレードまたは移行を完了する方法
データインポートを使用した新規インストール	元のリリース データを SFTP にエクスポートし、そのデータがインポートされた新しい 15 クラスタをゼロタッチでインストールすることで移行を処理します。	このツールは、次の場合に考慮してください。 • 直接 15 に更新アップグレードを行う必要はありませんが、これ以外に直接アップグレードを行う方法はありません。 • 直接更新アップグレードの代替策として、PCD（アドレスを付け変えた一時的な追加ハードウェア）を使用した直接移行を行う必要はありません。	1. ソースリリースが 10.5、11.5、および 12.5.1 ～ 12.5(1)SU4 の場合は、COP をインストールします。 2. データを SFTP にエクスポートするには CLI を実行します。 3. そのデータを SFTP からインポートするには、新しい応答ファイルフィールドと新しいインストーラ GUI フィールドを使用してゼロタッチインストールを行います（『インストール ガイド』を参照）。

要件および制約事項

ここでは、このリリースへのアップグレードの要件と制限事項について説明します。

ハードウェア要件

次のタイプUnified Communications ManagerのIM and Presence Serviceハードウェアでホストされている仮想サーバ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を使用していない場合は、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
- 仮想化された Cisco ハードウェア（Cisco UCS や Cisco HyperFlex など）は、VMware vSphere ESXi を使用しています。
- VMware vSphere ESXi を搭載した仮想化されたサードパーティ製ハードウェア

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ます。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、Unified Communications Manager および IM and Presence Service アプリケーションのリンクを参照することで確認できます。

プラットフォームの要件

ここでは、仮想マシンに Unified Communications Manager と IM and Presence Service を展開する前に満たす必要がある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、サーバ ハードウェアで Unified Communications Manager と IM and Presence Service を直接インストールまたは実行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、次の操作を実行する必要があります。

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

（注） 最新の Unified Communications Manager 対応/サポートの ESXi バージョンについては、 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。

- リリース用にシスコが提供する正しい 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。

仮想マシンの構成

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ます。

表 *4*：仮想マシンの要件

項目	説明
OVA テンプレート	OVA ファイルには、仮想マシン設定用の一連の定義済みテンプレートが用意されています。サポートされているキャパシティレベル、必要な OS/VM/SAN の配置などの項目について説明します。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いています。OVA ファイルの詳細については、https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/collaboration-virtualization-sizing.html の「Unified Communications 仮想化のサイジングに関するガイドライン」のトピックを検索してください。
VMware vSphere ESXi	リリースの互換性とサポート要件を満たすvSphere ESXi ハイパーバイザ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は、正しいライセンスタイプで vSphere ESXi がインストールされていることも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りません。これらのライセンスの一部では、必要な VMware Api が有効になっていないためです。
VMware vCenter	VMware vCenter は、Business Edition 6000/7000 Unified Communications Managerアプライアンス IM and Presence Service 、または UCS テスト済みリファレンス構成ハードウェアで UC 上に展開する場合はオプションです。 VMware vCenter は、UC に UCS 仕様ベースおよびサードパーティ製のサーバ仕様ベースのハードウェアに導入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仕様	またはUnified Communications ManagerIM 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 の仮想ハードウェア仕様を変更する必要があるかどうかを確認します。 Unified Communications Manager または IM and Presence Service リリース 15 バージョンには、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 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。 アップグレード前に vRAM と vDisk の仕様を確認するには、リリース 15 のベース OVA の Readme を参照するか、QuoteCollab ツールを使用します。 その他の参考資料については、次を参照してください。 • 仮想マシン設定タスク （79 ページ） 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 バージョンを、vDisk が 110GB としてインストールされている新しい VMware にバックアップまたは復元します。ここでは、直接アップグレードが成功します。または、PCD 移行またはデータインポートタスクの移行を伴う新規インストールを使用して、Unified CM リリース 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。

非推奨の電話のモデル

次の表に、このリリースのCisco Unified Communications Managerで廃止されたすべての電話機モデルと、電話モデルが最初に廃止されたUnified CMリリースを示します。たとえば、リリース 11.5 (1) で最初に廃止された電話機モデルは、すべてのリリース (12.x リリースを含む) では廃止されています。

これらの電話機モデルのいずれかを使用している場合、現在のリリースの Cisco Unified Communications Manager にアップグレードすると、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モデル

このリリースで廃止された電話のモデル	最初は廃止予定
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 Phone 7970G • Cisco Unified IP Phone 7971G-GE • Cisco Unified Wireless IP Phone 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 電話 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 Phone 7910SW • Cisco Unified IP Phone 7912 • Cisco Unified Wireless IP Phone 7920 • Cisco Unified IP Conference Station 7935	11.5 (1) 以降のリリース

この問題の追加情報は、「Field Notice」を参照してください。

非推奨の電話機を含むアップグレード

以前のリリースのこれらの電話機のいずれかを使用していて、このリリースにアップグレードする場合は、次の操作を実行します。

1. ネットワーク内の電話機がこのリリースでサポートされているかどうかを確認します。
2. サポートされていない電話機を確認します。
3. サポートされていない電話機の場合は、電話の電源を切り、ネットワークから電話を切断します。
4. この電話機のユーザに、サポートされる電話機をプロビジョニングします。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機に移行することができます。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機がこのリリースでサポートされたら、システムをアップグレードします。

（注） 非推奨の電話機は、アップグレード後に削除することもできます。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、システムから非推奨の電話機について管理者に通知する警告メッセージが表示されます。

ライセンシング

非推奨の電話機とサポートされている電話機を交換するために、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。システムから廃止された電話機を削除するか、新しい Unified Communications Manager に切り替えて非推奨の電話機が登録できなくなると、新しい電話機のデバイス ライセンスが使用可能になります。

ネットワーク要件

ここでは、を導入Unified Communications Managerする前に、 IM and Presence Serviceネットワークが満たす必要がある要件を示します。

IP アドレス要件

多数のサービスを適切に動作させるために、コラボレーション ソリューション全体は DNS に依存しているので、可用性の高い DNS 構成を適切な場所に配置する必要があります。基本的な IP テレフォニー展開で DNS を使用したくない場合は、Unified Communications Manager および IM and Presence Service を設定することで、ゲートウェイやエンドポイント デバイスとの通信にホスト名ではなく IP アドレスを使用できます。

静的 IP アドレッシングを使用するようにサーバを設定し、サーバが固定 IP アドレスを取得できるようにします。また、静的 IP アドレスを使用することで、Cisco Unified IP Phoneをネットワークに接続したときにアプリケーションに登録できるようにもなります。

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ません。シスコでは混合モードの導入をサポートしていません。Unified Communications Manager と IM and Presence Service の両方で DNS を使用するか、使用しないかのいずれかにする必要があります。
- 展開で DNSUnified Communications ManagerをIM and Presence Service使用する場合は、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、システムの動作に異常が発生する場合があります。
- 展開が DNS を使用していない場合は、次の [ホスト名/IP アドレス（Host Name/IP Address）] フィールドを編集する必要があります。
  - サーバー（Server）：Cisco Unified CM Administration の **[Server Configuration（サーバ設定）]** 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 Service：Cisco Unified CM Administration の **[UC サービスの設定（UC Service Configuration）]** 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 アドレスを指している IM and Presence UC サービスを作成します。
- CCMCIP プロファイル（COMCIP Profiles）：Cisco Unified CM IM and Presence Administration の **[CCMCIP プロファイルの設定（COMCIP Profile Configuation）]** ウィンドウで、いずれかの CCMCIP プロファイルでホストの IP アドレスを指定します。

- マルチノードの考慮事項：IM and Presence Service でマルチノード機能を使用する場合は、DNS 設定オプションについて、『IM and Presence Service の設定および管理ガイド』のマルチノード展開に関する項を参照してください。
- DNS サーバーが Windows 2019 以降で設定されていることを確認するか、任意の Linux マシンで設定された DNS サーバーを使用します。

ファイアウォールの要件

ポート 22 への接続がオープンで、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ます。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は、Unified Communications Manager パブリッシャノードへの複数の接続が連続してすばやく開かれます。これらの接続をスロットリングすると、インストールが失敗する可能性があります。一般的なセキュリティの考慮事項については、『Cisco Unified Communications Manager セキュリティ ガイド』を参照してください。

（注） これらのファイアウォール機能はアップグレードとインストールの失敗を引き起こす可能性があるため、アップグレードおよびインストール中は [侵入者/侵入検知（Intruder/Intrusion Detection）] および/または [ブルートフォースアタック（Brut Force Attack）] 機能を無効にすることをお勧めします。

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

SFTP サーバのサポート

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 SFTP サーバのみであり、Cisco TAC がサポートします。 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） これらの製品がシスコでテストされていない場合、シスコはその機能を保証することができません。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規模な Class A または Class B サブネットに Unified Communications Manager をインストールしないでください。詳細については、『Cisco Collaboration システム 12.x ソリューション リファレンス ネットワーク デザイン（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 個のサブスクライバ ノードと 4 個のスタンバイ ノードの合計 8 個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、メディア サーバなどのクラスタ内のサーバ ノードの合計数は、21 個を超えることはできません。

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

詳細については、http://www.cisco.com/go/ucsrnd にある『シスコ 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ビットのIPサブネットマスクを使用している場合は、255.255.255.0という形式を使用してください。255.255.255.000の形式は使用しないでください。255.255.255.000は有効な形式ですが、アップグレードプロセス中に問題が発生する可能性があります。問題を回避するには、アップグレードを開始する前にフォーマットを変更することを推奨します。サブネットマスクを変更するには、 **set network ip eth0 <server_IP_address> 255.255.255.0**コマンドを実行します。

サブネットマスクでは他の形式が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のみに適用されます。

ソフトウェア要件

この項では、Cisco Unified Communications Manager および IM and Presence Service のアップグレードと移行に関するソフトウェア要件を説明します。

Cisco Unified Mobile Communicator のデバイス名

Cisco Unified Mobile Communicator のデバイス名が 15 文字以内であることを確認します。Cisco Unified Mobile Communicator のデバイス名が 15 文字より多い場合、アップグレード時にデバイスが移行されません。

Export Restricted および Export Unrestricted ソフトウェア

このリリースの Unified Communications Manager と IM and Presence Service は、Export Restricted（K9）バージョンに加えて、Export Unrestricted（XU）バージョンもサポートしています。

（注） 無制限（Unrestricted）バージョンのソフトウェアは、さまざまなセキュリティ機能を必要としない特定のカスタマーのみを対象としています。無制限バージョンは一般的な展開用ではありません。

Export Unrestricted バージョンは、次の点で制限（restricted）バージョンと異なります。

- ユーザ ペイロード（情報交換）の暗号化はサポートされません。

- 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ません。
- 無制限バージョンのリリースをインストールすると、制限バージョンにアップグレードできなくなります。無制限バージョンを含むシステムでの制限バージョンの更新インストールもサポートされません。
- 単一クラスタ内のすべてのノードを同じモードにする必要があります。たとえば、同じクラスタ内の Unified Communications Manager と IM and Presence Service ノードは、すべてが無制限モードまたは制限モードでなければなりません。
- IP フォンのセキュリティ設定が変更され、シグナリングおよびメディアの暗号化（VPN Phone 機能で提供される暗号化を含む）が無効になります。

（注） 無制限バージョンのリリースをインストールすると、制限バージョンにアップグレードできなくなるので注意してください。無制限バージョンを含むシステムでは、制限バージョンの更新インストールを実行できません。

すべてのグラフィカル ユーザ インターフェイス（GUI）とコマンドライン インターフェイス（CLI）で、管理者は製品バージョン（restricted または export unrestricted）を表示できます。

次の表は、Unified Communications Manager の無制限バージョンと IM and Presence Service では使用できない GUI 項目を示しています。

GUI の項目	場所	説明
Cisco Unified CM Administration		
VPN の設定	**[拡張機能（Advanced Features）] > [VPN]**	このメニューとオプションはありません。
電話セキュリティ プロファイルの設定	**[システム（System）] > [セキュリティ（Security）] > [電話セキュリティ プロファイル（Phone Security Profile）]**	[デバイス セキュリティ モード（Device Security Mode）] は、[非セキュア（Non Secure）] に設定されており、設定はできません。
Cisco Unified CM IM and Presence Administration		

GUI の項目	場所	説明
セキュリティ設定	**[システム（System）] > [セキュリティ（Security）] > [設定（Settings）]**	• **[XMPP クライアントと IM/P サービス間のセキュア モードの有効化（Enable XMPP Client To IM/P Service Secure Mode）]** 設定はオンにできません。 • **[XMPP ルータ ツールータ セキュア モードの有効化（Enable XMPP Router-to-Router Secure Mode）]** 設定はオンにできません。 • **[Web クライアントと IM/P サービス間のセキュア モードの有効化（Enable Web Client to IM/P Service Secure Mode）]** 設定はオンにできません。 • **[SIP クラスタ間プロキシ ツープロキシ転送プロトコル（SIP intra-cluster Proxy-to-Proxy Transport Protocol）]** を **TLS** に設定するオプションは削除されました。
Cisco SIP Proxy サービスのための **[サービス パラメータ設定（Service Parameter Configuration）]**	**[システム（System）] > [サービス パラメータ（Service Parameters）]** から **[サービス（Service）]** として、**[Cisco SIP プロキシ（Cisco SIP Proxy）]** を選択します。	• **[Transport Preferred Order]** パラメータの TLS オプションはすべて削除されました。 • TLS オプションは、**[SIP ルート ヘッダー トランスポート タイプ（SIP Route Header Transport Type）]** パラメータから削除されました。

GUI の項目	場所	説明
SIP フェデレーテッド ドメイン	**[プレゼンス（Presence）]**> ドメイン間フェデレーション（**Interdomain Federation**）]> **[SIP**フェデレーション（**SIP Federation**）]	OCS/Lync とのドメイン間フェデレーションを設定するとポップアップが表示され、エンタープライズ内の別の OCS/Lync とのみ直接フェデレーションを行うことができるとの警告が出されます。エンタープライズ外の OCS/Lync と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（**Interdomain Federation**）]> **[XMPP**フェデレーション（**XMPP Federation**）]> **[**設定（**Settings**）]	セキュリティ モードを構成できません。**TLS なし**に設定されています。
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**）]	優先プロキシ リスナーとして TLS または HTTPS リスナーを設定できません。

Unified CM 9.x からのアップグレード

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

- Standard SIP Profile
- Standard SIP Profile For Cisco VCS
- Standard SIP Profile For TelePresence Conferencing
- Standard SIP Profile For TelePresence Endpoint
- Standard SIP Profile for Mobile Device

これらの名前のいずれかを持つ SIP プロファイルがある場合は、アップグレードを続行する前に名前を変更または削除する必要があります。

CLI によって開始される IM and Presence のアップグレードに必要な OS 管理者アカウント

utils system upgrade CLI コマンドを使用して、IM and Presence Service ノードをアップグレードする場合は、管理者権限を持つユーザではなく、デフォルト OS 管理者アカウントを使用する必要があります。デフォルト OS 管理者アカウントを使用しないと、必須のサービスをインス

トールするためにアップグレードに必要な特権レベルがなくなり、アップグレードが失敗する可能性があります。**show myself** CLI コマンドを実行すると、アカウントの特権レベルを確認できます。アカウントには特権レベル 4 が必要です。

この制限は、IM and Presence Service の CLI によって開始されるアップグレードにのみ適用され、Unified Communications Manager には適用されないことに注意してください。また、この制限は、新しい ISO ファイルでは修正される可能性があることに注意してください。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 を使用したアップグレードに必要なデータベース移行

Microsoft SQL Server を IM and Presence Service の外部データベースとして展開していて、11.5(1)、11.5(1)SU1、または 11.5(1)SU2 からアップグレードする場合は、新しい SQL Server データベースを作成し、その新しいデータベースに移行する必要があります。この作業は、このリリースで強化されたデータ タイプのサポートのために必要です。データベースを移行しないと、既存の SQL Server データベースでスキーマの検証に失敗し、持続チャットなどの外部データベースに依存するサービスが開始されません。

IM and Presence Service をアップグレードした後、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 の外部データベースでは必要ありません。

はじめる前に

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。コピーを入手するには、Cisco TAC にお問い合わせください。

表 *7:*

手順	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、『Database Setup Guide for the IM and Presence Service』の次の章を参照してください。 **1.** 「Microsoft SQL Installation and Setup」：アップグレードされた IM and Presence サービスで新しい SQL Server 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 Service External Database Setup」：新しいデータベースを作成した後、この章を参照して、IM and Presence Service にデータベースを外部データベースとして追加します。

手順	タスク
ステップ 3	システム トラブルシュータを実行して、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.** **[外部データベーストラブルシュータ（External Database Troubleshooter）]** セクションにエラーが表示されていないことを確認します。
ステップ 4	すべての IM and Presence Service のクラスタノード上で Cisco XCP ルータを再起動します。 **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ー-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）]** メニューから、IM and Presence Service ノードを選択し、**[移動（Go）]** をクリックします。 **3.** **IM and Presence Services**の下で、**Cisco XCP Router**を選択して、**再起動**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（Server）] メニューから、IM and Presence ノードを選択し、[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 IM and Presence Services）] の下で、次のサービスを選択します。 Cisco XCP Text Conference Manager Cisco XCP File Transfer Manager Cisco XCP Message Archiver **4.** [停止（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にデータを移行します。`MSSQL_migrate_script.sql` **（注）** このスクリプトのコピーを入手するには、Cisco TAC にお問い合わせください。

手順	タスク
ステップ 7	システム トラブルシュータを実行して、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.** **[外部データベーストラブルシュータ（External Database Troubleshooter）]** セクションにエラーが表示されていないことを確認します。
ステップ 8	以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（Server）] メニューから、IM and Presence ノードを選択し、[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 （IM and Presence Services）]** の下で、次のサービスを選択します。 Cisco XCP Text Conference Manager Cisco XCP File Transfer Manager Cisco XCP Message Archiver **4.** [開始（Start）] をクリックします。
ステップ 9	外部データベースが稼働していることと、すべてのチャット ルームが Cisco Jabber クライアントから認識可能であることを確認します。新しいデータベースが動作していることが確かな場合にのみ、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に関する考慮事項

Unified Communications Manager リリース 12.5 SU1 で FIPS モードを有効にすると、低いキーサイズの 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を使用して IPsec ポリシーをすでに設定しており、FIPS モードを有効にしている場合は、Unified Communications Manager リリース 12.5 SU1 へのアップグレードがブロックされます。

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

- 以前に設定した 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 の IPsec ポリシーを再設定します。

- DH グループ 14 ~ 18 をサポートする COP ファイル (latest_version、COP) 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、3DES アルゴリズムは IPSec 通信でサポートされません。ESP および 3DES として暗号化アルゴリズムを使用して IPsec ポリシーをすでに設定しており、FIPS モードを有効にしている場合は、Unified Communications Manager リリース 15 へのアップグレードがブロックされます。

（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 configuration] 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は、3DES アルゴリズムを使用した IPSec ポリシーが FIPS モードでサポートされていないことに注意してください。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 アルゴリズムを使用して IPSec ポリシーを削除して再作成し、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 ポリシーの設定の詳細については、 *Cisco Unified* オペレーティングシステム管理の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を使用して IPSec が設定されている場合は、IPsec ポリシーが 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。自己署名証明書で証明書ベースの認証を使用するように設定された IPsec を使用して 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バージョンを実行しているクラスタに対して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検索するには、『Cisco Unified Communications Manager と IM and Presence Service の互換性マトリクス』の「サポートされている統合」の章を参照してください。

アップグレード中の Spectre と Meltdown の脆弱性

このリリースの Unified Communications Manager、Cisco IM and Presence Service、Cisco Emergency Responder および Cisco Prime Collaboration の導入には、Meltdown および Spectre のマイクロプロセッサの脆弱性に対処するためのソフトウェア 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、Cisco Collaboration Sizing Tool を使用して、現在の展開をアップグレード済みの展開と比較するように、チャネルパートナーまたはアカウントチームと連携させることをお勧めします。必要に応じて、VM リソースを変更して、アップグレードされた導入環境で最適なパフォーマンスが得られるようにします。

10.5(2) からの ENUM 切断のアップグレードと移行の重複

リリース 10.5(2) または 11.0(1) から任意の後続の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、アップグレードと移行の失敗を引き起こす古いロケールのインストールで問題が発生します。この問題は、次の CUCM 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 CUCM 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、この問題は、その日付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、2017年8月31日よりも古いロケールを使用するように、Unified Communications Manager と電話のロケールのインストールを更新します。ロケールのインストールを更新すると、アップグレードまたは移行を開始できます。回避策の詳細については、https://bst.cloudapps.cisco.com/bugsearch/bug/CSCuz97687 を参照してください。

ライセンス要件

ここでは、Unified Communications Manager と IM and Presence Service のライセンス要件について説明します。

スマート ソフトウェア ライセンシングの概要

シスコ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） ライセンス承認は、30 日間に少なくとも 1 回更新することで 90 日間有効になります。Cisco Smart Software Manager または Cisco Smart Software Manager サテライトに接続しないと、90 日後に承認の期限が切れます。

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 Smart Software Manager 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 Smart Software Manager 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構成されたサテライトをサポートします。

（注） Cisco Smart Software Manager Satellite 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 Smart Software Manager 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。Session Management Edition の登録には、Unified Communications Manager と同じプロセスを使用できます。Cisco Unified Communications Manager が登録されているバーチャルアカウントまたは別のバーチャルアカウントに登録し、最小のライセンス要件を満たします。

（注） 特定ライセンス予約（SLR）に登録された SME では、SLR 承認コードの生成時に最小セットのライセンスが CSSM に予約されている必要があります。

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。

特定ライセンス予約

特定のライセンス予約（SLR）を使用すると、お客様が仮想アカウントからライセンスを予約し、それらのライセンスをデバイス UDI に関連付け、それらの予約済みライセンスを使用してデバイスを切断モードで使用することができます。この場合、仮想アカウントから UDI の特定の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*：特定のライセンス予約コマンド

コマンド	説明
ライセンスのスマート予約の有効化	ライセンス予約機能を有効にするには、このコマンドを使用します。
ライセンスのスマート予約の無効化	ライセンス予約機能を無効にするには、このコマンドを使用します。
ライセンスのスマート予約要求	予約要求コードを生成するには、このコマンドを使用します。
許可証のスマート予約のキャンセル	承認コードがインストールされる前に予約プロセスをキャンセルするには、このコマンドを使用します。
ライセンススマート予約インストール "< 認証-コード >"	Cisco Smart Software Manager で生成されたライセンス予約承認コードをインストールするには、このコマンドを使用します。
スマート許可証予約に戻ります。	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承認コードと予約済み権限のリストを削除します。デバイスは未登録の状態に移行します。
license smart reservation return-authorization "<承認コード>"	ユーザが入力したライセンス予約の承認コードを削除するには、このコマンドを使用します。

（注） 12.0から上位バージョンにアップグレードし、アップグレードされたサーバ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をダウンロードし、アップグレードした 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 and Presence Service ライセンスの要件

IM and Presence Service には、サーバー ライセンスやソフトウェア バージョン ライセンスは必要ありません。ただし、ユーザーを割り当て、その割り当てたユーザごとに IM and Presence Service を有効にする必要があります。

（注） Jabber for Everyone オファーを使用している場合、IM and Presence Service 機能を有効にするためのエンドユーザーライセンスは不要です。詳細については、『Jabber for Everyone クイック スタート ガイド』を参照してください。

IM and Presence Service は、各ユーザに関連付けられているクライアントの数に関係なく、ユーザ単位で割り当てることができます。IM and Presence Service をユーザに割り当てると、ユーザが IM とアベイラビリティ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ユーザは、IM and Presence Service サーバにログインして他のユーザのアベイラビリティを確認したり、IM を送受信したりすることはできません。また、そのユーザのアベイラビリティ ステータスを他のユーザが確認することもできません。

次のいずれかのオプションを使用して、IM and Presence Service のユーザを有効にすることができます。

- Unified Communications Manager の [**エンドユーザの設定（End User Configuration**）]ウィンドウ。詳細については、『Cisco Unified Communications Manager アドミニストレーション ガイド』を参照してください。
- 一括管理ツール（BAT）
- Unified Communications Manager の [**ユーザ/電話のクイック追加（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 IM and Presence Service を割り当てる。

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。

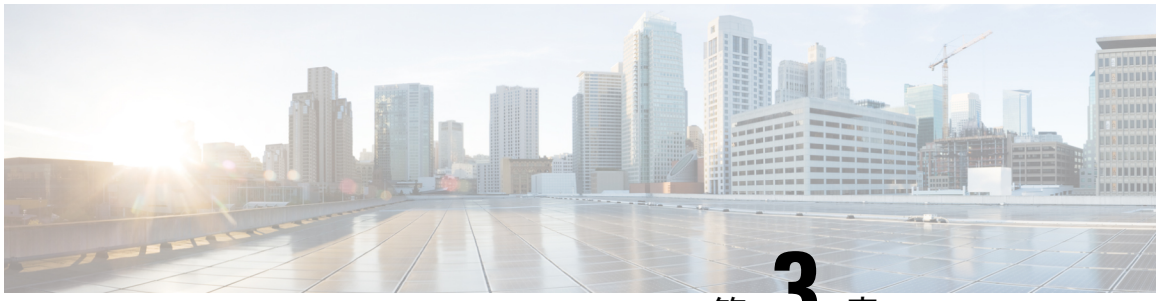
IM and Presence Service 機能は、User Connect Licensing（UCL）と Cisco Unified Workspace Licensing（CUWL）の両方に含まれています。また、Unified Communications Manager IP テレフォニー ユーザでないユーザに対しても、Jabber for Everyone オファーを通じて IM and Presence Service 機能を入手できます。詳細については、『Jabber for Everyone クイック スタート ガイド』を参照してください。

サポート文書

次のドキュメントには、特定のケースでのアップグレードに役立つ追加のサポート情報が記載されています。

タスク	
仮想化されたCiscoハードウェアをセットアップします。	仮想化プラットフォームを設定するには、「仮想サーバでのシスココラボレーション」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。
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* のインストールガイド：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* のインストールガイド：https://www.cisco.com/c/en/us/support/unified-communications/business-edition-7000/tsd-products-support-series-home.html
設定を保持しながら既存のハードウェアを交換する	『*Cisco Unified Communications Manager* 単一サーバまたはクラスタの置換』：https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-guides-list.html
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 ベンダーのマニュアルについては、http://www.VMware.com を参照してください。

タスク	
追加の計画およびサイジングのリソース	これらのドキュメントには、アップグレードされたシステムの計画とサイジングに役立つ情報も記載されています。 • 『シスコ コラボレーション システム ソリューション リファレンス ネットワーク デザイン（*SRND*）』：http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-system/products-implementation-design-guides-list.html • シスコの推奨アーキテクチャガイドおよびシスコ検証済み設計ガイド：http://www.cisco.com/c/en/us/solutions/enterprise/design-zone-collaboration/index.html • コラボレーション仮想マシンの交換ツール：http://ucs.cloudapps.cisco.com/ • Cisco Quote Collab Tool：http://www.cisco.com/go/quotecollab • Cisco Collaboration Sizing Tool ：http://tools.cisco.com/cucst



第 3 章

アップグレード作業

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、次のアップグレードタイプのいずれかを実行するには、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ついて説明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は 12.5 (1) 以上である必要があります。それ以外の場合は、もう一方の方法を使用する必要があります。
- CLI を介したクラスタ ノードのアップグレード（直接標準）

（注） 12.5 より前のソースからリリース 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、クラスタ内のノードは認証されません。サブスクライバ 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 導入を使用するアップグレードおよび移行については、『Cisco Prime Collaboration Deployment Administration Guide』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。

はじめる前に

注意 すべての設定タスクを終了します。アップグレード中は、設定を変更しないでください。たとえば、パスワードを変更したり、LDAP同期を実行したり、自動化ジョブを実行したりしないでください。アップグレードプロセス中に、クラスタ内のノードを削除、再追加、または再インストールしないでください。設定を変更できるのは、すべてのノードでアップグレードと事後のタスクが完了した場合のみです。アップグレードによって、アップグレード中に行った設定変更が上書きされ、いくつかの設定変更によってアップグレードが失敗することがあります。

LDAPを使用してユーザの同期を中断することを推奨します。すべてのUnified Communications ManagerおよびIM and Presence Serviceのクラスタノード上でアップグレードが完了するまで、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、ファイルを圧縮したりしないでください。これらを行うと、有効なアップグレード ファイルであることをシステムが拒否します。
- IM and Presence Serviceのアップグレードについて、ユーザの連絡先リストのサイズが最大値を下回っていることを確認します。Cisco Unified CM IM and Presence Administrationの[システムトラブルシュータ（System Troubleshooter）]を使用して、制限を超えているユーザ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は、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、Cisco Unified Communications Managerアドミニストレーション ガイドにある『Cisco Unified Communications Managerアドミニストレーション ガイド』の「はじめに」の章に記載されている「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。

（注） リリース12.5(1) SU2以降では、他のAXL依存統合への影響を回避するために、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 ステージ[バージョンのインストールと切り替え（Install and Switch Version）]を実行することをお勧めします。

（注） バージョンの切り替え中、動的テーブル(numplandynamic、devicedynamicなど)のユーザー向け機能(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、またはスイッチ バージョンが失われる前に構成が変更されます。

（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あることが確認されています。この時間ジャンプは、システムが NTP サーバーと同期するまでハードウェアクロックが無効になるため、予期される動作です。

（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セキュリティ パスワードが異なる場合、下位のバージョンに戻す場合は、下位のバージョンのセキュリティ パスワードを上位のバージョンと同じに変更してください。セキュリティパスワードを変更するには、次の手順を実行します。

1. パブリッシャ ノードを下位バージョンに切り替えます。
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. サブスクライバを下位バージョンに切り替えます。
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、次の手順を使用して 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ジッターが小さいNTP ソースを常に使用するようにしてください。
2. 時刻同期用に 1 台の適切な NTP サーバーを設定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は、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 サーバーを設定する必要があります。
3. Cisco Voice Operating System（VOS）サーバーでサポートされている互換性のあるバージョンと一致するように、常に ESXi をアップグレードする必要があります。
4. 異なるホスト間のネットワーク移行中は、信頼できるクロックで同じ NTP ソース（OR）NTP ソースを使用していることを確認します。

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には、ダウンロードしたファイルが同じディレクトリに保存されていることを確認してください。

表 *9:* ダウンロードするファイルのアップグレード

ダウンロードするファイル	サイトのダウンロード
Unified CM アップグレード ISO	[Unified Communications Manager のダウンロード（Unified Communications Manager Downloads）] に移動します。ご使用のバージョンを選択してから、ISO アップグレードの **Unified Communications Manager の更新**で確認してください。 例：`UCSInstall_UCOS_ .sha512.iso`
IM and Presence Service アップグレード ISO	[IM and Presence Service のダウンロード（IM and Presence Service Downloads）] に移動します。ご使用の バージョンを選択してから、ISO アップグレードの **Unified Presence Server（CUP）の更新**を確認します。 例：`UCSInstall_CUP_ .sha512.iso`
アップグレード準備状況 COP ファイル (アップグレード前およびアップグレード後)	上記のダウンロードサイトのいずれかから、アップグレード前の COP ファイルとアップグレード後の COP ファイルを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 Service の場合、COP ファイルは**Unified Presence Server（CUP）Updates > ユーティリティ**の下に表示されます。 たとえば、`ciscocm.preUpgradeCheck-XXXXX.cop.sgn` と `ciscocm.postUpgradeCheck-XXXXX.cop.sgn` というようになります。 （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の数が表示されます。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のタスク フロー（直接標準）

クラスタ全体のアップグレードを簡素化するには、次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） クラスタ全体のアップグレードオプションは、アップグレード前のバージョンが 12.5 (1) 以上の最小リリースである場合に、直接の標準アップグレードでのみ使用できます。

（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 ファイルをダウンロードし、準備状況 COP ファイルをアップグレードして、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 （51 ページ）」を参照してください。

手順

	コマンドまたはアクション	目的
ステップ 1	アップグレード準備 COP ファイルの実行（アップグレード前） （54 ページ）	アップグレード準備状況 COP ファイルを実行して、システムの接続性と健全性を確認します。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	クラスタ全体のリブート シーケンスの設定 （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 ソフトウェアの場所の構成（57 ページ）	アップグレード前に、クラスタ内で関連付けられたすべてのノードのクラスタ ソフトウェア 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	次のいずれかの方法を使用してクラスタをアップグレードします。	アップグレード中は、アップグレードの一部として自動的にバージョンを切り替えることができます。または、アップグ

	コマンドまたはアクション	目的
	• OS 管理者によるクラスタ全体のアップグレードの完了 （58 ページ） • CLI によるクラスタ全体のアップグレードの完了 （60 ページ）	レードされたバージョンを非アクティブなパーティションに保存することもできます。
ステップ 5	手動によるバージョン切り替え (クラスタ全体) （61 ページ）	オプション。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ことを選択した場合は、バージョンを手動で切り替えます。
ステップ 6	アップグレード準備 COP ファイルの実行（アップグレード後） （62 ページ）	アップグレード後の COP ファイルを実行して、システムのアップグレード後の健全性を guage します。

アップグレード準備 COP ファイルの実行（アップグレード前）

アップグレード準備状況 COP ファイルは、次の点を確認します。

- 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
- ファイルシステムのタイプとゲスト 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 チェック
- SIP および h.323 トランクの登録
- データベース認証および複製のステータス
- データベースの健全性
- 最後の DRS バックアップのステータス
- リモート コール制御（RCC）機能のステータス
- サービスステータス
- インストールされている COPs とロケール

- デバイス登録ステータス数
- エンタープライズ パラメータおよびサービス 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のバージョン
- 期限切れの証明書がある場合：
- FIPS モードのパスワード長の制限
- FIPS モードでの ESP および暗号化アルゴリズムの IPSec ポリシー設定チェック

（注）
- アップグレードの失敗の可能性を大幅に低減するため、アップグレードする前にアップグレード準備の 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 モードでサポートされていないため、3DES アルゴリズムを使用する 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 アルゴリズムを使用して 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状況の COP ファイルをダウンロードして、アップグレード前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) 宛先のリリースを選択し、**[ユUnified Communications Manager ユーティリティ（Unified Communications Manager Utilities）]** を選択します。
c) アップグレード準備状況の COP ファイルをダウンロードして、**アップグレード前のテストを実行**します (例: `ciscocm preUpgradeCheck-00019 COP`)。最新のファイルのファイル名とバージョンが異なる場合があることに注意してください。

ステップ 2 アップグレードに関するシステムの準備状況を確認します。
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 ファイルを再度実行します。
d) COP ファイルがエラーを返さないようにするまで、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) **[トレースとログ セントラル（Trace and Log Central）]** で、**[リモート参照（Remote Browse）]** をダブルクリックして、**[ファイルのトレース（Trace files）]** を選択して、**[次へ（Next）]** をクリックします。
c) **すべてのサーバーのすべてのサービスを選択**し、**[次へ（Next）]** をクリックします。
d) **[終了（Finish）]**、**[閉じる（Close）]** を順にクリックします。
e) ノードをダブルクリックして、**[CUCM パブリッシャ（Publisher）]>[システム（System）]>[インストール アップグレード ログ（ Install upgrade Logs）]** を展開します。
f) **[インストール（Install）]** 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。

クラスタ全体のリブート シーケンスの設定

クラスタ全体のアップグレードを簡素化するために、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) 以上の場合にのみ使用できます。

（注） リブートシーケンスを設定しない場合、クラスタ全体のアップグレードでは、最後に保存されたリブートシーケンスまたはデフォルトシーケンスが使用されます。

手順

ステップ 1 パブリッシャノードで、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 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）]** を選択します。
[**Reboot Cluster Settings**] ウィンドウに、ノードごとのリブートシーケンスを表示するスライダが表示されます。

ステップ 3 スライダを使用して、必要に応じてリブートシーケンスを調整します。

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、次のいずれかのタスクを実行します。

- OS 管理者によるクラスタ全体のアップグレードの完了 （58 ページ）
- CLI によるクラスタ全体のアップグレードの完了 （60 ページ）

クラスタ ソフトウェアの場所の構成

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

Note クラスタ内のすべてのノードが、リリース 14SU2 以降の場合のみこの機能を使用します。

Procedure

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 ロケーション（Cluster Software Location）]** を選択します。

ステップ 3 リストからサーバーの場所の詳細を追加または編集するノードを選択します。

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（Apply to All Nodes）]** チェックボックスをオンにします。

このチェック ボックスは、**[ノードの選択（Select Node）]** ドロップダウン リストから Unified CM パブリッシャを選択した場合にのみ表示されます。

ステップ 5 パブリッシャ ノードからのソース構成とソフトウェアの場所の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 ログイン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）]** を使用します。

デフォルトでは、**[パブリッシャからのダウンロード ログイン情報とソフトウェアの場所を使用（Use download credentials and software location from Publisher）]** オプションが選択されています。

Note このオプションは、サブスクライバ ノードでのみ使用できます。

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 ログイン情報とソフトウェアの場所を使用する（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 ログイン情報とソフトウェアの場所を使用する（Use below download credentials and software location）]** オプションを使用します。

Note このオプションは、サブスクライバ ノードでのみ使用できます。

ステップ 7 **[ソース (Source)]** ドロップダウン リストから、アップグレード ファイルが保存されている場所に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、キャンセルされた以前のアップグレードを再開する場合にのみ使用できます。

- **SFTP サーバー**：ディレクトリ、サーバー アドレス、ログイン情報などの SFTP サーバの詳細も入力する必要があります。

ステップ 8 （オプション）アップグレードが完了したときに電子メールでの通知を受信するには、**SMTP サーバー**のアドレスと**電子メールの宛先**を入力します。これにより、アップグレードが完了したときに電子メールで送信できるようになります。

ステップ 9 アップグレードファイルがダウンロードされた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 (continue with upgrade after download)]** をオンにします。このチェックボックスをオンにしない場合は、**ソース**として**ローカルファイルシステム**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バージョン サーバーを切り替える (ISO の場合のみ有効)（Switch-version server after upgrade (valid only for ISO)）]** チェックボックスをオンにして、アップグレードが正常に完了した後にシステムを自動的に再起動します。

ステップ 11 **[保存（Save）]** をクリックして、追加または変更された特定のノードのすべての構成変更を更新します。

OS 管理者による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 と IM and Presence Service のクラスタ全体のアップグレードを簡素化します。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) 以降の場合にのみ、標準のアップグレードで使用できます。

Note また、`utils system upgrade cluster` CLI コマンドを実行し、プロンプトに従って、標準的なクラスタ全体のアップグレードを実行することもできます。

Before you begin

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

Procedure

ステップ 1 **Cisco Unified OS の管理**または **Cisco Unified 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（Install/Upgrade Cluster）**] を選択します。このオプションは、[From version] が 12.5 (1) より前の場合は使用できません。

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次の構成情報を表示できます。

Note リリース 14 SU2 以降で、すべてのクラスタノードのソフトウェアの場所の設定は、各クラスタノードでローカルではなく、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 のユーザー インターフェイスから **[ソフトウェアのアップグレード（Software Upgrades）] > [クラスタ ソフトウェア ロケーション（Cluster Software Location）]** メニューに移動します。

- **ログイン情報（Credentials Information）**：：アップグレード画像が保存されるサーバーのログイン情報を表示します。
- **ファイル ソースのアップグレード（Upgrade file source）**：アップグレード ファイルが保存されるサーバー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することも、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することもできます。または、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 オプションを使用して、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（Continue with upgrade after download）**：アップグレードファイルがダウンロードされると、アップグレードを自動的に続行するかどうかを指定する必要があります（デフォルト値は [はい（yes）] です）。自動的にアップグレードすることを選択した場合、チェックサムまたは SHA の詳細は表示されません。値を [はい（yes）] または [いいえ（no）] に設定すると、設定はシステムに残ります。
- **バージョン スイッチング（Version switching）**：アップグレードが完了すると、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する必要があります（デフォルト値は [いいえ（no）] です）。Yes と入力すると、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再起動します。値を [はい（yes）] または [いいえ（no）] に設定すると、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、**[次へ（Next）]** 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 ステータス（Installation Status）]** ページには、アップグレードに関する情報が表示されます。

Note クラスタ全体のアップグレード中に、最初の 3 桁が、選択した Unified Communications Manager と IM and Presence Service のアップグレード ファイル間で共通になるようにしてください。

ステップ 6 アップグレードが完了したら、**[完了（Finish）]** 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は、クラスタのリブートシーケンスに従って、アップグレードされたバージョンにクラスタがリブートされます。それ以外の場合、アップグレードは非アクティブパーティションに保存され、アップグレードされたソフトウェアを使用するには、手動でバージョンを切り替える必要があります。

CLI によるクラスタ全体のアップグレードの完了

コマンドラインインターフェイスを使用してクラスタ全体のアップグレードを簡素化するには、次の手順を実行します。

Note このオプションは、アップグレード前のバージョンがリリース 12.5 (x) 以降の場合に、直接の標準アップグレードでのみ使用できます。

Before you begin

クラスタ全体のリブート シーケンスの設定, on page 56：アップグレード後にバージョンを自動的に切り替える場合は、再起動シーケンスを事前に設定します。それ以外の場合は、最後に保存されたシーケンスを使用してクラスタがリブートします。リブートシーケンスが保存されていない場合は、デフォルトのシーケンスが使用されます。

Note リリース 14 SU2 以降で、すべてのクラスタノードのソフトウェアの場所の設定は、各クラスタノードでローカルではなく、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、システムのアップグレードを開始する前に、Cisco Unified OS Administration のユーザー インターフェイスから **[ソフトウェアのアップグレード（Software Upgrades）] > [クラスタ ソフトウェア ロケーション（Cluster Software Location）]** メニューに移動します。

Procedure

ステップ 1 Unified CM Publisher 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 system upgrade cluster CLI` コマンドを実行すると、同じクラスタ内のすべてのノードを構成するためのソフトウェア ロケーションの詳細がウィザードに表示されます。

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次の構成情報を表示できます。

- **ログイン情報（Credentials Information）**—アップグレード画像が保存されるサーバーのログイン情報を表示します。
- **ファイル ソースのアップグレード（Upgrade file source）**—アップグレード ファイルが保存されるサーバー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することも、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することもできます。または、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 オプションを使用して、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（Continue with upgrade after download）**：アップグレードファイルがダウンロードされると、アップグレードを自動的に続行するかどうかを指定する必要があります（デフォルト値は [はい（yes）] です）。自動的にアップグレー

ドすることを選択した場合、チェックサムまたはSHAの詳細は表示されません。値を [はい（yes）] または [いいえ（no）] に設定すると、設定はシステムに残ります。

- **バージョンスイッチング（Version switching）**:アップグレードが完了すると、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する必要があります（デフォルト値は [いいえ（no）] です）。Yes と入力すると、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再起動します。値を [はい（yes）] または [いいえ（no）] に設定すると、設定はシステムに残ります。

ステップ 4 インストールの開始を求めるプロンプトが表示されたら、 **Yes**と入力します。
アップグレード後に自動的にバージョンを切り替えることを選択した場合は、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に再起動します。それ以外の場合、アップグレードは非アクティブパーティションに保存され、後でバージョンを手動で切り替えることができます。

手動によるバージョン切り替え (クラスタ全体)

他のノードへの UI または CLI を使用せずに、Unified Communications Manager パブリッシャ ノードを介してすべてのクラスタ ノード間で非アクティブ バージョンとアクティブ バージョンを切り替える、直接標準アップグレードには、次の手順を使用します。

（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のクラスタ全体の自動化の使用
- アップグレード前バージョン 12.5(1) 以降

（注） 1つ以上のクラスタノードが、非アクティブなバージョンのアップグレード、スイッチバージョンの再起動、およびデータベースレプリケーションの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、 **[Software Upgrade] > [Install/Upgrade]** または **[Software Upgrade] > [Cluster Install/Upgrade]** に移動して、アップグレードステータスを表示します。または、 **utils system upgrade status** または **utils system cluster upgrade status** コマンドを実行して、アップグレード ステータスをモニターします。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 アップグレード（Software Upgrades）]**>**[クラスタのリブート（Reboot Cluster）]** を選択します。

ステップ 3 オプション。リブートシーケンスをまだ設定していない場合は、スライダを使用してリブートシーケンスを編集し、[**保存 (Save)**] をクリックします。

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

（注） CLI を使用する場合は、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。CLI を使用する場合は、`utils system switch-version` CLI コマンドを使用してバージョンを切り替えることができますが、ノード単位で実行する必要があります。

アップグレード準備 COP ファイルの実行（アップグレード後）

アップグレード後に、アップグレード後の COP ファイルを実行します。これにより、次のことが確認されます。

- 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、クラスタ内)
- FIPS モードのパスワード長の制限
- 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 トランクの登録
- データベース認証および複製のステータス
- データベースの健全性
- 最後の DRS バックアップのステータス
- サービスステータス
- インストールされている COPs とロケール
- デバイス登録ステータス数
- エンタープライズ パラメータおよびサービス 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のバージョン

（注） システムの健全性を確認するには、アップグレード後にアップグレード後のチェックのためにアップグレード準備の COP ファイルを実行することを強くお勧めします。

手順

ステップ 1 アップグレード後のテストを実行するには、アップグレード準備状況の COP ファイルをダウンロードします。

a) ダウンロードサイトに移動します。
b) 宛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) アップグレード準備状況の COP ファイルをダウンロードして、**アップグレード前のテストを実行**します (例: `ciscocm postUpgradeCheck-00019 COP`)。最新のファイルのファイル名とバージョンが異なる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健全性を確認します。

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いようにするには、これらの手順を繰り返します。

ステップ 3 アップグレード後に CLI からレポートを表示するには、**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 をログインします。
b) **[トレースとログ セントラル（Trace and Log Central）]** で、**[リモート参照（Remote Browse）]** をダブルクリックして、**[ファイルのトレース（Trace files）]** を選択して、**[次へ（Next）]** をクリックします。
c) **すべてのサーバーのすべてのサービスを選択**し、**[次へ（Next）]** をクリックします。
d) **[終了（Finish）]**、**[閉じる（Close）]** を順にクリックします。
e) ノードをダブルクリックして、**[CUCM パブリッシャ（Publisher）]>[システム（System）]>[インストール アップグレード ログ（ Install upgrade Logs）]** を展開します。
f) **[インストール（Install）]** 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

これでアップグレードは完了です。新しいソフトウェアの使用を開始できます。

CLI を介したクラスタノードのアップグレード（直接標準）

ノード単位でノードのクラスタノードをアップグレードするには、次のタスクを実行します。このプロセスは、ユニファイド OS 管理インターフェイスまたは CLI インターフェイスを使用して直接更新アップグレードを完了する場合に使用する必要があります。

（注） 12.5.x より前の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。最初にソースをリリース 12.5.x または 14 および SU にアップグレードしてから、ソースをリリース 15 にアップグレードすることができます。

始める前に

アップグレード ISO ファイルをダウンロードし、準備状況 COP ファイルをアップグレードして、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 （51 ページ）」を参照してください。

手順

	コマンドまたはアクション	目的
ステップ 1	アップグレード準備 COP ファイルの実行（アップグレード前） （54 ページ）	アップグレード準備状況 COP ファイルを実行して、システムの接続性と健全性を確認します。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 ソフトウェアの場所の構成（57 ページ）	アップグレード前に、クラスタ内で関連付けられたすべてのノードのクラスタ ソフトウェア 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 のいずれかのインターフェイスを使用してクラスタノードをアップグレードします。 • OS 管理を介したクラスタノードのアップグレード（直接標準） （68 ページ） • CLI を介したクラスタノードのアップグレード（直接標準） （70 ページ）	クラスタ内のクラスタノードをアップグレードします。

	コマンドまたはアクション	目的
ステップ 4	手動によるバージョン切り替え （71 ページ）	オプション。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、次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）	アップグレード後に、アップグレード後の COP ファイルを実行して、システムのアップグレード後の健全性を guage します。

アップグレード準備 COP ファイルの実行（アップグレード前）

アップグレード準備状況 COP ファイルは、次の点を確認します。

- 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
- ファイルシステムのタイプとゲスト 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 チェック
- SIP および h.323 トランクの登録
- データベース認証および複製のステータス
- データベースの健全性
- 最後の DRS バックアップのステータス
- リモート コール制御（RCC）機能のステータス
- サービスステータス
- インストールされている COPs とロケール
- デバイス登録ステータス数
- エンタープライズ パラメータおよびサービス 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のバージョン
- 期限切れの証明書がある場合：
- FIPS モードのパスワード長の制限
- FIPS モードでの ESP および暗号化アルゴリズムの IPSec ポリシー設定チェック

（注）
- アップグレードの失敗の可能性を大幅に低減するため、アップグレードする前にアップグレード準備の 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 モードでサポートされていないため、3DES アルゴリズムを使用する 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 アルゴリズムを使用して 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状況の COP ファイルをダウンロードして、アップグレード前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) 宛先のリリースを選択し、**[ユUnified Communications Manager ユーティリティ（Unified Communications Manager Utilities）]** を選択します。
c) アップグレード準備状況の COP ファイルをダウンロードして、**アップグレード前のテストを実行**します (例: `ciscocm preUpgradeCheck-00019 COP`)。最新のファイルのファイル名とバージョンが異なる場合があることに注意してください。

ステップ 2 アップグレードに関するシステムの準備状況を確認します。
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 ファイルを再度実行します。
d) COP ファイルがエラーを返さないようにするまで、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) **[トレースとログ セントラル（Trace and Log Central）]** で、**[リモート参照（Remote Browse）]** をダブルクリックして、**[ファイルのトレース（Trace files）]** を選択して、**[次へ（Next）]** をクリックします。

c) **すべてのサーバーのすべてのサービスを選択**し、**[次へ（Next）]** をクリックします。
d) **[終了（Finish）]**、**[閉じる（Close）]** を順にクリックします。
e) ノードをダブルクリックして、**[CUCM パブリッシャ（Publisher）]>[システム（System）]>[インストール アップグレード ログ（ Install upgrade Logs）]** を展開します。
f) **[インストール（Install）]** 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。

クラスタ ソフトウェアの場所の構成

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

Note クラスタ内のすべてのノードが、リリース 14SU2 以降の場合のみこの機能を使用します。

Procedure

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 ロケーション（Cluster Software Location）]** を選択します。

ステップ 3 リストからサーバーの場所の詳細を追加または編集するノードを選択します。

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（Apply to All Nodes）]** チェックボックスをオンにします。

このチェック ボックスは、**[ノードの選択（Select Node）]** ドロップダウン リストから Unified CM パブリッシャを選択した場合にのみ表示されます。

ステップ 5 パブリッシャ ノードからのソース構成とソフトウェアの場所の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 ログイン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）]** を使用します。

デフォルトでは、**[パブリッシャからのダウンロード ログイン情報とソフトウェアの場所を使用（Use download credentials and software location from Publisher）]** オプションが選択されています。

Note このオプションは、サブスクライバ ノードでのみ使用できます。

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 ログイン情報とソフトウェアの場所を使用する（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ログイン情報とソフトウェアの場所を使用する（Use below download credentials and software location）]** オプションを使用します。

Note このオプションは、サブスクライバ ノードでのみ使用できます。

ステップ 7 **[ソース (Source)]** ドロップダウン リストから、アップグレード ファイルが保存されている場所に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、キャンセルされた以前のアップグレードを再開する場合にのみ使用できます。
- **SFTP サーバー**：ディレクトリ、サーバー アドレス、ログイン情報などの SFTP サーバの詳細も入力する必要があります。

ステップ 8 （オプション）アップグレードが完了したときに電子メールでの通知を受信するには、**SMTP サーバー**のアドレスと**電子メールの宛先**を入力します。これにより、アップグレードが完了したときに電子メールで送信できるようになります。

ステップ 9 アップグレードファイルがダウンロードされた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 (continue with upgrade after download)]** をオンにします。このチェックボックスをオンにしない場合は、**ソース**として**ローカルファイルシステム**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バージョン サーバーを切り替える (ISO の場合のみ有効)（Switch-version server after upgrade (valid only for ISO)）]** チェックボックスをオンにして、アップグレードが正常に完了した後にシステムを自動的に再起動します。

ステップ 11 **[保存（Save）]**をクリックして、追加または変更された特定のノードのすべての構成変更を更新します。

OS 管理を介したクラスタノードのアップグレード（直接標準）

Cisco Unified Communications Manager または IM and Presence Service クラスタノードの直接更新アップグレードを完了するには、次の手順を使用します。

（注） アップグレードのオプションによっては、アップグレード元のバージョンによって若干異なる場合があります。

（注） 12.5.x より前の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。最初にソースをリリース 12.5.x または 14 および SU にアップグレードしてから、ソースをリリース 15 にアップグレードすることができます。

手順

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

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

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次の構成情報を表示できます。

（注） リリース 14SU3 以降で、すべてのクラスタノードのソフトウェアの場所の設定は、各クラスタノードでローカルではなく、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、システムのアップグレードを開始する前に、Cisco Unified OS Administration のユーザー インターフェイスから **[ソフトウェアのアップグレード（Software Upgrades）] > [クラスタ ソフトウェア ロケーション（Cluster Software Location）]** メニューに移動します。

- **ログイン情報（Credentials Information）**: アップグレード画像が保存されるサーバーのログイン情報を表示します。
- **ファイルソースのアップグレード（Upgrade file source）**: アップグレードファイルが保存されるサーバー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することも、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することもできます。または、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 オプションを使用して、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（Continue with upgrade after download）**: アップグレードファイルがダウンロードされると、アップグレードを自動的に続行するかどうかを指定する必要があります（デフォルト値は [はい（yes）] です）。自動的にアップグレードすることを選択した場合、チェックサムまたは SHA の詳細は表示されません。値を [はい（yes）] または [いいえ（no）] に設定すると、設定はシステムに残ります。
- **バージョン スイッチング（Version switching）**: アップグレードが完了すると、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する必要があります（デフォルト値は [いいえ（no）] です）。Yes と入力すると、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再起動します。値を [はい（yes）] または [いいえ（no）] に設定すると、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、[**次へ（Next）**] をクリックします。アップグレードが開始されます。[**インストールステータス (Installation Status)**] ページには、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自動的にバージョンを切り替えることを選択した場合は、アップグレード後にノードがアップグレードされたバージョンに再起動します。それ以外の場合、アップグレードは非アクティブパーティションに保存され、後でバージョンを手動で切り替えることができます。

ステップ 7 追加のクラスタノードについても、この手順を繰り返します。

CLI を介したクラスタノードのアップグレード（直接標準）

CLI を使用して個々のクラスタノードをアップグレードするには、次の手順を実行します。

（注） アップグレードのオプションは、アップグレード元のバージョンによって異なる場合があります。

（注） 12.5.x より前の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。最初にソースをリリース 12.5.x または 14 および SU にアップグレードしてから、ソースをリリース 15 にアップグレードすることができます。

（注） リリース 14SU3 以降で、すべてのクラスタノードのソフトウェアの場所の設定は、各クラスタノードでローカルではなく、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、システムのアップグレードを開始する前に、Cisco Unified OS Administration のユーザー インターフェイスから **[ソフトウェアのアップグレード（Software Upgrades）] > [クラスタ ソフトウェア ロケーション（Cluster Software Location）]** メニューに移動します。

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 インターフェイ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、同じクラスタ内のすべてのノードを構成するためのソフトウェア ロケーションの詳細がウィザードに表示されます。

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（Yes）]** 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、ソースを選択するように求められます（ステップ **4** ～ **8** に従います）。

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**: サーバの詳細とクレデンシャルを入力するように求められます。

- **ローカル DVD/CD（Local DVD/CD）**：ローカル CD または DVD のみ。
- **ローカルイメージ（Local image）**：このオプションは、アップグレードを以前に開始し、アップグレードを完了しなかった場合にのみ使用できます。

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通知する電子メール通知用の **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に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（Yes）]**: ファイルがすべてのノードにダウンロードされると、アップグレードが開始されます。
- [**いいえ (No)**: 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で再起動できます。

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自動的にバージョンを切り替えるかどうかを入力します。

- **[はい (Yes)]**: アップグレード後、クラスタは新しいバージョンに切り替わり、自動的に再起動します。
- [**いいえ (No)**: アップグレードは非アクティブパーティションに保存します。バージョンは後で手動で切り替えることができます。

ステップ 8 インストールの開始を確認するプロンプトが表示されたら、「**Yes**」と入力します。
アップグレード後に自動的にバージョンを切り替えることを選択した場合は、アップグレード後にノードがアップグレードされたバージョンに再起動します。それ以外の場合、アップグレードは非アクティブパーティションに保存され、後でバージョンを手動で切り替えることができます。

手動によるバージョン切り替え

アップグレードの一環として自動的にバージョンを切り替えなかった場合は、この手順を使用してクラスタ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) 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使用できます。詳しくは、「手動によるバージョン切り替え (クラスタ全体) （61 ページ）」を参照してください。

手順

ステップ 1 GUI を使用する場合は、次のようにします。

a) スイッチするノードの Cisco Unified OS の管理インターフェイスまたは Cisco Unified IM and Presence OS の管理インターフェイスにログインし、次の手順を実行します。

b) **[設定（Settings）] > [バージョン（Version）]** を選択します。

c) 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。

d) [**バージョンの切り替え（Switch Versions**）] 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) これらの手順を追加のクラスタノードに対して繰り返します。

ステップ 2 CLI を使用する場合は、次のようにします。

a) 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。

b) `utils system switch-version` CLI コマンドを実行します。

c) これらの手順を追加のクラスタノードに対して繰り返します。

アップグレード準備 COP ファイルの実行（アップグレード後）

アップグレード後に、アップグレード後の COP ファイルを実行します。これにより、次のことが確認されます。

- 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、クラスタ内)
- FIPS モードのパスワード長の制限
- 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 トランクの登録
- データベース認証および複製のステータス
- データベースの健全性
- 最後の DRS バックアップのステータス
- サービスステータス
- インストールされている COPs とロケール
- デバイス登録ステータス数
- エンタープライズ パラメータおよびサービス 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のバージョン

（注） システムの健全性を確認するには、アップグレード後にアップグレード後のチェックのためにアップグレード準備の COP ファイルを実行することを強くお勧めします。

手順

ステップ 1 アップグレード後のテストを実行するには、アップグレード準備状況の COP ファイルをダウンロードします。

a) ダウンロードサイトに移動します。
b) 宛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) アップグレード準備状況の COP ファイルをダウンロードして、**アップグレード前のテストを実行**します (例: `ciscocm postUpgradeCheck-00019 COP`)。最新のファイルのファイル名とバージョンが異なる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健全性を確認します。

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いようにするには、これらの手順を繰り返します。

ステップ 3 アップグレード後に CLI からレポートを表示するには、**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 をログインします。
b) **[トレースとログ セントラル（Trace and Log Central）]** で、**[リモート参照（Remote Browse）]** をダブルクリックして、**[ファイルのトレース（Trace files）]** を選択して、**[次へ（Next）]** をクリックします。
c) **すべてのサーバーのすべてのサービスを選択**し、**[次へ（Next）]** をクリックします。
d) **[終了（Finish）]**、**[閉じる（Close）]** を順にクリックします。
e) ノードをダブルクリックして、**[CUCM パブリッシャ（Publisher）]>[システム（System）]>[インストール アップグレード ログ（ Install upgrade Logs）]** を展開します。
f) **[インストール（Install）]** 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

これでアップグレードは完了です。新しいソフトウェアの使用を開始できます。

以前のバージョンへのクラスタの切り替え

以前のバージョンにクラスタを切り替えるには、次の基本タスクを実行します。

手順

ステップ 1 パブリッシャ ノードをスイッチバックします。
ステップ 2 すべてのバックアップ サブスクライバ ノードをスイッチバックします。
ステップ 3 すべてのプライマリ サブスクライバ ノードをスイッチバックします。
ステップ 4 以前の製品リリースに戻す場合は、クラスタ内のデータベース複製を再設定します。

以前のバージョンへのノードの切り替え

手順

ステップ 1 アップグレードす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 オペレーティング システムの管理にログインします。
- ノードUnified Communications Managerをアップグレードしたら、Cisco Unified Communications Operating System Administration にログインします。

ステップ 2 **[設定（Settings）]** > **[バージョン（Version）]** を選択します。

[バージョン設定（Version Settings）] ウィンドウが表示されます。

ステップ 3 [**バージョンの切り替え（Switch Versions**）] 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正常に完了したことを確認するには、次の手順を実行します。

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）]** を選択します。

[バージョン設定（Version Settings）] ウィンドウが表示されます。

c) アクティブなパーティションで、適切な製品バージョンが実行されていることを確認します。
d) アクティブにしたサービスがすべて動作してい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 の管理（Cisco Unified CM Administration）] にログインします。

f) ログインできること、および設定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

以前の製品リリースを実行するようにクラスタ内のサーバの設定を元に戻すには、クラスタ内のデータベース レプリケーションを手動でリセットする必要があります。

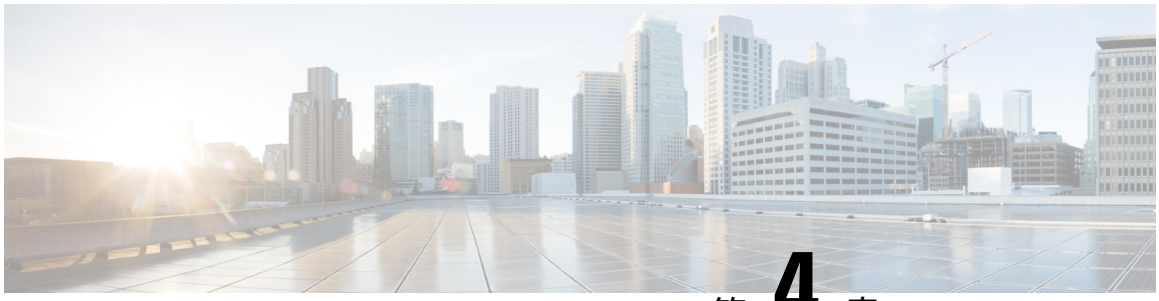
手順

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を更新する必要がある場合にのみ、この付録の手順を実行してください。

- 仮想マシン設定タスク （79 ページ）

仮想マシン設定タスク

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ように仮想マシンの設定を変更する必要がある場合は、この章の手順を使用します。

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。要件を確認するには、「シスココラボレーション仮想化」に進み、 Unified Communications ManagerおよびIM and Presence Serviceアプリケーションのリンクに従ってください。

手順

	コマンドまたはアクション	目的
ステップ 1	VMware のインストールと設定 vCenter （81 ページ）	VMware vCenter は、UCS 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で、Cisco Business Edition またはテスト済みリファレンス構成 (TRC) ハードウェアから UC に移行する場合にのみ必要です。VMware vCenter が必要な場合は、先にインストールして設定します。 UC on UCS テスト済みリファレンス構成ハードウェアに Unified Communications Manager または IM and Presence Service

	コマンドまたはアクション	目的
		を展開する場合、VMware vCenter の使用は任意です。
ステップ 2	vSphere ESXi のアップグレード （81 ページ）	リリースの要件を満たす vSphere ESXi ハイパーバイザのバージョンをインストールする必要があります。 またはUnified Communications ManagerIM and Presence Serviceのアップグレードを開始する前に、ESXi ハイパーバイザをアップグレードすることを推奨します。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は、シスコアプリケーションをアップグレードした後に 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 （82 ページ）	OVA ファイルには、仮想マシン設定用の一連の定義済みテンプレートが用意されています。サポートされているキャパシティレベル、必要な OS/VM/SAN の配置などの項目について説明します。 この手順は任意です。すでに仮想マシンUnified Communications ManagerをIM and Presence Service実行している場合や、導入サイズが変更されていない場合は、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は、展開用にサイジングされ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	仮想マシン構成仕様の変更 （83 ページ）	またはUnified Communications Managerの新しいリリースにアップグレードするために、仮想マシン (VM) の vcpu、VRAM、vDisk サイズ、または vNIC タイプを変更する必要がある場合IM and Presence Serviceは、次の手順を使用します。 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

	コマンドまたはアクション	目的
		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場合にのみ実行してください。
ステップ 5	単一からマルチ vDisk 仮想マシンへの移行 （84 ページ）	複数の vDisks が必要な大規模な仮想マシン (VM) 導入環境に移行する場合は、この手順を使用します。

VMware のインストールと設定 vCenter

VMware vCenter の使用は、UCS テストUnified Communications Manager済みIM and Presence Serviceリファレンス構成ハードウェアにUCを導入する場合はオプションです。VMware vCenterは、UC on UCS 仕様ベースのハードウェア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に導入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 のマニュアル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情報によって追跡される詳細レベルを設定します。統計レベルの範囲は 1 ~4 で、レベル4は最も多くのデータを含んでいます。UCS 仕様ベースまたは HP/IBM 仕様ベースの導入では、統計レベルを4に設定する必要があります。

ステップ 3 すべての統計情報を保持するのに十分な領域があることを確認するために、データサイズの見積もりを表示します。

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 ハイパーバイザを更新する必要がある場合は、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、Unified Communications Manager を実行している仮想マシンをホスト サーバから移動します。

- ホット スタンバイ ホストがある場合は、vMotion を使用して別の物理サーバに仮想マシンを移行します。

- 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 によって示され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を使用して、Unified Communications Manager を実行している仮想マシンをホスト サーバに戻します。

- ホットスタンバイ ホストがある場合は、vMotion を使用して別の物理サーバに仮想マシンを移行します。
- 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、ホストサーバにコピーします。

OVA テンプレートのダウンロードとインストール

OVA ファイルには、仮想マシン設定用の一連の定義済みテンプレートが用意されています。サポートされているキャパシティレベル、必要な OS/VM/SAN の配置などの項目について説明します。OVA ファイルに関する情報については、https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/cisco-collaboration-virtualization.html で「Unified Communications Virtualization Sizing Guidelines」のトピックを検索してください。

この手順は任意です。すでに仮想マシンUnified Communications ManagerをIM and Presence Service実行している場合や、導入サイズが変更されていない場合は、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は、導入環境に合わせてサイズ変更された 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 ご使用のリリースの OVA テンプレートを見つけます。

- のUnified Communications Manager場合は、 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、「Virtualization for Cisco Unified Communications Manager」というトピックを検索します。
- IM and Presence Serviceでは、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 CM IM and Presence のための仮想化（Virtualization for Unified CM IM and Presence）」というトピックを検索します。

ステップ 2 単一の OVA ファイルをダウンロードするには、そのファイルの横にある [**ファイルのダウンロード (Download file)**] 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横にある [**カートに追加 (Add To cart)**] ボタンをクリックし、[**カートのダウンロード (download cart)**] リンクをクリックします。

ステップ 3 [カートのダウンロード（**Download Cart**）] ページの [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 ライセンス契約書（**Software License Agreement**）] のページの情報を読み、[同意する（**Agree**）] ボタンをクリックします。

ステップ 5 次のリンクの 1 つをクリックします。

- **ダウンロードマネージャ（Download Manager）**(Java が必要)
- **非 Java ダウンロード オプション（Non Java Download Option）**

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）]** を選択した場合は、**[ロケーションの選択（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（Non Java Download Option）]** を選択した場合は、新しいブラウザウィンドウで **[ダウンロード（Download）]** リンクをクリックします。場所を指定して、ローカル マシンにファイルを保存します

仮想マシン構成仕様の変更

またはUnified Communications ManagerIM and Presence Serviceの新しいリリースにアップグレードするために、仮想マシン (VM) の Vcpu、vRAM、VDisk、または vNIC を変更する必要がある場合は、次の手順を使用します。

VM 要件の詳細については、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、「仮想化導入の実装」のトピックを検索してください。

始める前に

VDisk ストレージ領域を増やす必要がある場合は、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。それ以外の場合は、[ディスクサイズの増加（increase disk size）] オプションがグレー表示されます。「スナップショットの操作」を参照してください。

手順

ステップ 1 ディザスタリカバリシステム（DRS）の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の場合、更新アップグレードのスペース要件を満たすために vDisk 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） 12.5.x より前の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設定を変更します。

a) 新しいリリースの要件に合わせて、ゲスト OS のバージョンを変更します。

b) vCPU を変更するには、vSphere クライアントで変更を行います。必ず、新しいリリースの仕様に合わせて予約値を変更してください。

c) vRAM を変更するには、vSphere クライアントで変更を行います。必ず、新しいリリースの仕様に合わせて予約値を変更してください。

d) VDisk スペースを増やすには vSphere クライアント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 台のディスクがある場合は、2 番目のディスクを拡張します。

仮想マシンを再起動すると、共通パーティションに新しい領域が自動的に追加されます。

（注） アップグレードを完了させるために追加の容量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。ディスク容量は OVA テンプレートの Readme ファイルで指定されます。

ディスク サイズを拡大して共通パーティションに領域を追加しても、システムのユーザ キャパシティは増加しません。システムのユーザ容量を拡張する必要がある場合は、単一ディスクからマルチディスク仮想マシンに移行する必要があります。

VDisk を縮小したり、vDisk の数量を変更したり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 クライアントで、VMXNET 3 アダプタタイプを使用するようにネットワークアダプタが設定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 クライアントを使用した設定の変更については、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、仮想マシンの電源をオンにします。

単一からマルチ vDisk 仮想マシンへの移行

複数の vDisks を必要とする大規模な仮想マシン (VM) 導入に移行する場合は、次の手順を実行します。この手順を完了したら、「仮想マシン構成仕様の変更 （83 ページ）」で仕様がリリースの要件と一致していることを確認する必要があります。

手順

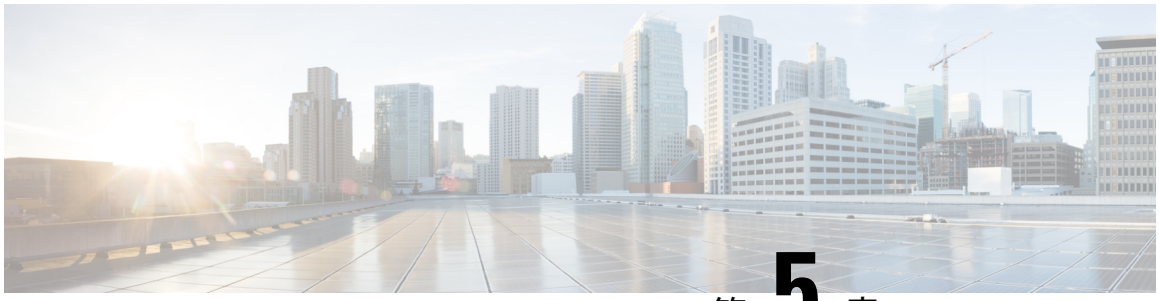
ステップ 1 ディザスタリカバリシステム (DRS) を使用して、既存の仮想マシン (VM) のバックアップを実行します。

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、正しいユーザ数で新しい VM を展開します。

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

ステップ 5 新しい VM の DRS の復元を実行します。



第 5 章

シーケンス ルールと時間要件

アップグレードの手順および時間要件

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ます。また、アップグレードを完了するために必要な時間とユーザの影響レベルをどのようにバランスす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準備が整う前に、従うべき順序を特定する必要があります。

この項の情報は、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 の移行では、この手順は必要ありません。

バージョンの切り替えの理解

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な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ブにするには、新しいソフトウェア バージョンにノードを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、次の 2 つの方法があります。

- 自動切り替え：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（Manual switching）：アップグレードプロセスが完了した後、OS の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。

どちらの方法を選択するかは、実行するアップグレードのタイプに応じて異なります。アップグレードプロセス中、再起動してアップグレード済みパーティションにソフトウェアバージョンを自動的に切り替えるか、後で手動でバージョンを切り替えるかについて、ウィザードから選択を求められます。次の表は、アップグレードの各タイプに使用する切り替え方式を示しています。

アップグレードタイプ	切り替えタイプ	要求に応じて選択..	Result
標準アップグレード	自動（Automatic）	**GUI**：アップグレードされたパーティションにリブート（Reboot to Upgraded Partition） **CLI**：アップグレード後に新バージョンに切り替える（Switch to new version after upgrade）	このオプションを選択した場合、システムがリブートして新しいソフトウェア バージョンになります。
	手動	**GUI**：アップグレード後にリブートしない（Do not reboot after upgrade） **CLI**：アップグレード後に新バージョンに切り替えない（Do not switch to new version after upgrade）	このオプションを選択した場合、アップグレードが完了すると、古いソフトウェア バージョンが引き続き実行されます。後で新しいソフトウェアに手動で切替えることができます。

アップグレードタイプ	切り替えタイプ	要求に応じて選択..	Result
更新アップグレード	自動（Automatic）	**GUI**：アップグレードされたパーティションにリブート（Reboot to Upgraded Partition） **CLI**：アップグレード後に新バージョンに切り替える（Switch to new version after upgrade）	アップグレード後に、ソフトウェア バージョンを使用する場合、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（Do not reboot after upgrade） **CLI**：アップグレード後に新バージョンに切り替えない（Do not switch to new version after upgrade）	このオプションは、段階的に更新アップグレードを実行する場合にのみ使用します。このオプションを選択した場合、アップグレードが完了すると、システムがリブートして古いソフトウェア バージョンが実行されます。後で新しいソフトウェアに手動で切り替えることができます。

アクティブ パーティションにあるアップグレード バージョンにスイッチのバージョンと設定情報は自動的に移行されます。

何らかの理由でアップグレードから元の状態に戻す場合、ソフトウェアの以前のバージョンがある非アクティブ パーティションからシステムを再起動できます。ただし、ソフトウェアのアップグレード後に行った設定の変更はすべて失われます。

Unified Communications Manager のインストール後の短期間、または別の製品バージョンにアップグレードして切り替えた後の短期間、電話機ユーザによる変更がすべて失われることがあります。電話機ユーザが行う設定には、コール転送の設定やメッセージ待機インジケータ ライトの設定などがあります。この現象は、Unified Communications Manager によるデータベースの同

期がインストール後またはアップグレード後に行われるため発生します。つまり、電話機ユーザによる設定変更が上書きされる可能性があります。

シーケンスルール

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予定の場合は、計画が次の順序付けルールを考慮する必要があります。

- Unified Communications Managerパブリッシャノードは、アップグレードする最初のノードである必要があります。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ています。
- パブリッシャノードが新しいUnified Communications Managerソフトウェアの非アクティブな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のアップグレードを開始できます。
- サブスクライバノードのバージョンUnified Communications Managerを切り替える前に、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する必要があります。新しいソフトウェアバージョンに切り替えて再起動するには、パブリッシャノードが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レプリケーションが完了するまで待機してから、COPファイルのインストールまたは設定の変更を続行する必要があります。
- Unified Communications Manager ノードをメンテナンス リリース（MR）またはエンジニアリング スペシャル（ES）リリースにアップグレードし、IM and Presence Service ノードをアップグレードしない場合は、Unified Communications Managerのアップグレードが完了した後に、すべての IM and Presence ノードをリブートする必要があります。
- ノードに加えてIM and Presence ServiceノードをUnified Communications Managerアップグレードする場合は、次のようにします。
  - IM and Presence Serviceデータベースパブリッシャノードは、アップグレードする最初IM and Presence Serviceのノードである必要があります。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ています。
  - パブリッシャノードが新しいIM and Presence Serviceソフトウェアの非アクティブな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のアップグレードを開始できます。
  - 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前Unified Communications Managerに、すべてのノードが非アクティブバージョンにアップグレードされるまで待つことができます。または、同時にアップグレードすることを選択することもできます。 IM and Presence Service並行してアップグレードする場合は、 IM and Presence ServiceUnified Communications Managerサブスクライバノードをアップグレードするのと同時にデータベースパブリッシャノードのアップグレードを開始します。

- ノードのバージョンを切り替える前に、新しいソフトウェアバージョンUnified Communications Managerに切り替え、パブリッシャノードから開始してすべてのノードをリブートする必要があります。 IM and Presence Service
- サブスクライバノードのソフトウェアIM and Presence Serviceバージョンを切り替える前に、データベース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する必要があります。 IM and Presence Service
- サブスクライバノードのIM and Presence Serviceグループをアップグレードする場合は、ソフトウェアバージョンを切り替えて再起動した後に、すべてのサブスクライバノードでデータベースレプリケーションが完了するまで待機してから続行する必要があります。

- ノードをメンテナンスリリースIM and Presence Service (MR) またはエンジニアリングスペシャル (ES) リリースにアップグレードしていて、ノードをアップグレードUnified Communications Managerしていない場合は、次の追加のシーケンスルールが適用されます。
  - Unified CM OS 管理インターフェイスを使用してアップグレードするにはUnified Communications Manager 、パブリッシャノードをアップグレードしIM and Presence Serviceてから、メンテナンスリリース (MR) またはエンジニアリングスペシャル (ES) リリースにノードをアップグレードする必要があります。
  - プライムコラボレーション導入の移行タスクを使用している場合は、 Unified Communications ManagerIM and Presence Serviceノードに加えてパブリッシャノードを選択する必要があります。
  - プライムコラボレーション導入のアップグレードタスクを使用している場合は、新しいバージョンの最初Unified Communications Managerの3桁が、現在インストールされているバージョンのIM and Presence Service最初の3桁と一致する限り、パブリッシャノードUnified Communications Managerを選択する必要はありません。

アップグレードの時間の要件

ソフトウェアのアップグレードに必要な時間は一定ではなく、いくつかの要因によって異なります。次の項の情報を使用して、アップグレードプロセスを最適化するために実行できる手順を理解してください。次の項では、アップグレードの時間要件を見積もるのに役立つ情報と例についても説明します。

アップグレードの時間要件に影響する要因

次の表に、アップグレードに必要な時間に影響を与える要因を示します。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できます。

表 *10* : 時間要件に影響する要因

項目	説明
外部サービスとツール	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とツールが、ドロップされたパケットなしで可能な限り短時間で応答すると、時間の要件が軽減されます。 同じ NTP サーバを指すように ESXi サーバとUnified Communications Managerパブリッシャノードを設定することを推奨します。 （注） VM との時間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、次のリンクに記載されている回避策を使用して、VM の NTP 同期を ESXi ホストとの間で無効にします。http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1189
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 上にあることを確認するか、 Unified Communications ManagerおよびIM and Presence Service仮想マシン (VM) と同じ LAN 上ですでにダウンロードおよびステージングされていることを確認して、時間を節約します。
システム ヘルス	仮想マシンの設定は、アップグレードの時間要件に影響します。導入サイズに適した仮想マシンの仕様を使用します。データベースが仮想マシンの設定制限を超えると、アップグレードプロセスの完了に時間がかかります。たとえば、VM設定のデバイス数が多すぎると、アップグレードに影響します。
	メモリ不足またはメモリリークは、アップグレードに影響します。
	ノード間のラウンドトリップ時間 (RTT) によって、必要な時間が延長されます。
	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ノードに SD リンクのアウトオブサービスイベントがないことを確認します。これらのイベントは通常、ネットワークの問題を示しています。これは、アップグレードプロセスを開始する前に対処する必要があります。
	システムエラーは、アップグレードの時間に影響を与える可能性があります。Real Time Monitoring Tool (RTMT) インターフェイスで、左側のナビゲーションウィンドウで [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高容量および低遅延に設定されている場合、および他のトラフィックからの競合が少ない場合は、アップグレード時間が短縮されます。たとえば、次のことを確認することによって、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、同一のダイレクトアタッチドストレージ (DAS) ボリューム、同じ論理ユニット番号 (LUN)、または同じ輻輳ネットワークリンクを共有する Vm からのインフラストラクチャのボトルネックはありません。 • ストレージの遅延は、.. www.cisco.com go virtualized-collaboration で指定された要件を満たしています。 • 物理 CPU コアと仮想化設計は、および Unified Communications ManagerIM and Presence Service の仮想化要件に準拠しています。Vm でホストリソースを共有することによって、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の使用 • Unified Communications Manager および 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 1 gbe LAN を持つホスト上にあります。 • クラスタが WAN を経由している場合は、http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-system/products-implementation-design-guides-list.html にある『シスココラボレーションシステムソリューションリファレンスネットワークデザイン（*SRND*）』に記載されているすべての帯域幅および遅延ルールに従っていることを確認してください。
システム性能	次のような不要なファイルを消去することによって、アップグレードの時間を短縮します。 • 呼詳細レコード（CDR）記録 • 古いファイル (TFTP ファイル、ファームウェア、ログファイルなど)

項目	説明
スロットリング	ノードIM and Presence Serviceでは、アップグレード中にシステムの安定性を維持するために、システムはアップグレードプロセスをスロットルします。スロットリングを行うと、アップグレードを完了するために必要な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、アップグレードの実行にかかる時間を短縮することはできますが、システムのパフォーマンスが低下することがあります。

最小時間要件の見積もり

次の表に、理想的な条件下で、アップグレードプロセスの各タスクに予想される経過時間の最小値を示します。アップグレードには、ネットワークの状況および従うアップグレードの順序に応じて、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すべてのタスクが実行されるまで、設定を変更することはできません。設定の変更内容は次のとおりです。

- Unified Communications ManagerまたはIM and Presence Serviceグラフィカルユーザインターフェイス (GUI)、コマンドラインインターフェイス (CLI)、または AXL API を使用して行われた変更
- LDAP 同期 (Oracle LDAP Unified Communications Managerからプッシュされる差分同期を含む)
- 自動化されたジョブ
- デバイスの自動登録を試行しています

（注） 12.5.x より前の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。

表 *11* : アップグレードタスクに必要な最小時間

タスク	最小時間	サービスへの影響
パブリッシャノードUnified Communications Managerを非アクティブなバージョンにアップグレードします。	2 ~ 4 時間 更新アップグレードの場合は1時間追加	更新アップグレード: UIにアクセスできない

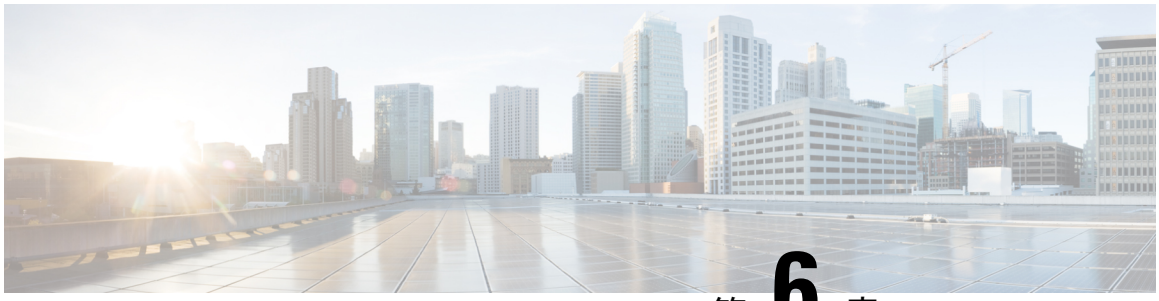
タスク	最小時間	サービスへの影響
サブスクライバノードUnified Communications Managerを非アクティブなバージョンにアップグレードします。	1 ~ 2 時間	更新アップグレード: バックアップサブスクライバが設定されていない場合、電話機は使用できません
パブリッシャノードUnified Communications Managerを新しいソフトウェアバージョンに切り替えて再起動します。	30 分	—
サブスクライバノードUnified Communications Managerを新しいソフトウェアバージョンに切り替えて再起動します。	30 分	標準アップグレード: バックアップサブスクライバが設定されていない場合、電話機は使用できません。
Unified Communications Manager データベースレプリケーション	小規模クラスタまたは小規模データベースを使用した導入の場合は30分 メガクラスタまたは大規模データベースの場合は2時間 （注） WAN の遅延が80ミリ秒以上になると、これらの時間が大幅に長くなる可能性があります。	電話機はダイヤルトーンで使用できますが、アップグレードが完了するまでエンドユーザ機能は使用できません。
データベースパブリッシャIM and Presence Service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 ~ 4 時間 更新アップグレードの場合は1時間追加	L2のアップグレード時に、電話サービスもIM and Presence も影響を受けません。 更新アップグレードの場合にのみ、IM and Presence が影響を受けます。

タスク	最小時間	サービスへの影響
サブスクライバノードIM and Presence Serviceを非アクティブなバージョンにアップグレードします。	1 ~ 2 時間	スイッチのバージョンでは、L2 または更新アップグレード電話サービスに関係なく、IM and Presence が影響を受けても動作を継続する必要があります。
パブリッシャノードIM and Presence Service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ます。	30 分	IM and Presence のハイアベイラビリティが無効になっています Jabber は使用できません。
サブスクライバノードIM and Presence Service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ます。	30 分	IM and Presence のハイアベイラビリティが無効になっています Jabber は使用できません。
IM and Presence Service データベース レプリケーション	小規模クラスタまたは小規模データベースを使用した導入の場合は30分 メガクラスタまたは大規模データベースの場合は2時間 （注） WAN 遅延は、これらの時間を大幅に長くすることができます。許容される最大 WAN 遅延は80m です。	IM and Presence のハイアベイラビリティが無効になっています Jabber は使用できません。

例

この項の例は、次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（IM）および Presence ノードを含むメガクラスタ
- 75000 ユーザ
- 「アップグレードの時間要件に影響する要因 （91 ページ）」に記載されているように、正常で、アップグレード用に最適化されているシステム。



第 6 章

アップグレード前のタスク(手動プロセス)

この付録の手動アップグレード前のタスクは、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実行する場合に使用できます。

- アップグレード前の作業 （99 ページ）

アップグレード前の作業

アップグレードまたは移行を開始する前に、次のタスクを実行します。

（注） このタスクフローの手順は、特に明記されていない限り、すべてのアップグレードおよび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	新しいリリースの場合は、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	新機能を理解し、アップグレードがシステムに関連付けられている他のシスコ製品とどのように相互作用するかを確認します。すべてのアップグレードおよび移行の方法について、この手順を実行します。
ステップ 2	アップグレード準備 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状況 COP ファイルは、アップグレードに干渉する可能性のある問題がないか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考慮する	リリース12.x では、プライムライセンスマネージャ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設定し、組織の構造に基づいてスマートアカウントの下に仮想アカウント (オプション) を作成する必要があります。シスコスマートアカウントの詳細については、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概要の詳細については、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	アップグレードする元のソフトウェアバージョンが仮想マシンで実行されていることを確認します。	ソフトウェアが MCS ハードウェアで実行されている場合は、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 にある『*Cisco Prime Collaboration Deployment* 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	要件および制約事項 （25 ページ） このリリースのを確認します。	システムがすべてのネットワーク要件、プラットフォーム要件、およびソフトウェア要件を満たしていることを確認します。 このステップは、すべてのアップグレードおよび移行方法で実行します。
ステップ 6	ネットワークの健全性を確認します。 • アップグレードの時間要件に影響する要因を読み、システムがそのセクションに記載されている条件を満たしていることを確認します。 • データベース ステータス レポートの生成 （107 ページ） • データベースのレプリケーションの確認 （108 ページ）	システムの健全性は、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短縮できます。

	コマンドまたはアクション	目的
	• パフォーマンス レポートの確認（109 ページ） • CLI の診断を実行する （109 ページ）	
ステップ 7	証明書チェーン内の信頼証明書を含め、期限切れの証明書がパーティションに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 （110 ページ） • 証明書の再作成 （111 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は、システムがすべての証明書要件を満たしていることを確認します。 （注） マルチサーバー（SAN）証明書の場合は、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	新規のバックアップを取る （115 ページ）	システムのバックアップを実行します。 注意 バックアップが古い場合、データが失われたり、システムを復元できないことがあります。
ステップ 9	カスタム着信音と背景イメージのバックアップ （116 ページ）	TFTPディレクトリにカスタム呼出音または背景イメージがある場合は、それらのファイルがシステムバックアップに含まれていないため、これらのファイルに対して個別のバックアップを作成します。
ステップ 10	ネットワーク接続の確認 （117ページ）	この手順を使用して、ネットワーク内のUnified Communications Manager ノードとサービス(NTP、SMTP、DNS など)間の接続を確認します。
ステップ 11	IPv6ネットワーキングの確認 （117ページ）	Unified Communications Manager ノードのみ。パブリッシャノードとサブスクライバノード間の IPv6 ネットワーキングを確認します。IPv6 が正しく設定されていない場合、ロードの検出に20分ほどかかることがあります。
ステップ 12	IM and Presence と Cisco Unified Communications Manager との間の接続の確認 （118 ページ）	IM and Presence Service が、Unified CM と接続されていることを確認します。

	コマンドまたはアクション	目的
		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。
ステップ 13	設定およびログイン情報の収集 （118 ページ）	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ます。
ステップ 14	登録済みデバイスの数を記録する （119 ページ）	リアルタイムモニタリングツール (RTMT) を使用してデバイス数をキャプチャします。これにより、アップグレードの完了後にエンドポイントとリソースを確認できます。
ステップ 15	割り当てられたユーザ数を記録する （120 ページ）	アップグレードの完了後にこの情報を確認できるように、 IM and Presence Service ノードに割り当てられたユーザの数を記録します。
ステップ 16	TFTP パラメータの記録 （120 ページ）	アップグレードプロセスによって、TFTP パラメータが変更されます。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 （121 ページ）	アップグレード中は、設定が異なっている場合、Unified Communications Manager のエンタープライズパラメータの設定によって IM and Presence Service の enteprise パラメータ設定が上書きされることがあります。
ステップ 18	ユーザ レコードのエクスポート （121 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 フォンのファームウェアのアップグレード （122 ページ）	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、アップグレード前のタスクとして、新しいリリースに対応するファームウェアに IP フォンをアップグレードできます。 移行で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 20	重要なサービスの確認 （123 ページ）	重要なサービスがすべて有効になっていることを確認します。
ステップ 21	Cisco Extension Mobility の非アクティブ化 （123 ページ）	リリース9.x以前からのアップグレードの場合のみ。アップグレードする前に、Unified CM ノードで Cisco Extension Mobility サービスを停止する必要があります。 移行ではこのタスクをスキップできます。
ステップ 22	IM and Presence Sync Agent の停止 （124 ページ）	IM and Presence のアップグレードの一部として Unified Communications Manager をアップグレードする必要がある場合は、アップグレードを開始する前に IM and Presence Sync Agent サービスを停止する必要があります。 移行ではこのタスクをスキップできます。
ステップ 23	使用可能な共通のパーティション領域を確認する （124 ページ）	アップグレードに十分な共通パーティション領域があることを確認します。 移行で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領域がない場合は、次の手順の1つまたは複数を実行します。 • 基準値の上限および下限の調節 （125 ページ） • 使用可能なディスク領域の最大化 （125 ページ）	この手順は、アップグレードを実行するために、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する直接アップグレードの場合にのみ実行してください。 **注意** 十分なディスク領域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可能性があります。
ステップ 25	アップグレード ファイルの取得 （127 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は、必要な COP ファイルもダウンロードする必要があります。

	コマンドまたはアクション	目的
		（注） 12.5.x より前の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。 移行で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 レプリケーションのタイムアウトを増やす （128 ページ）	オプション。Unified Communications Manager パブリッシャ ノードのみ。大規模クラスタをアップグレードする場合は、次の手順を使用します。 移行で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 （129 ページ）	IM and Presence Service のみ。ハイアベイラビリティが有効になっている場合は、アップグレードの前に無効にします。 移行ではこのタスクをスキップできます。
ステップ 28	仮想マシンにシリアル ポートを追加する （129 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。この手順は、すべてのノードに対して実行します。
ステップ 29	RTMT の高可用性の設定 （130 ページ）	RTMT を使用してモニタするメガクラスタ展開では、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、RTMT のハイアベイラビリティを設定することを推奨します。
ステップ 30	Microsoft SQL Server を使用したアップグレードに必要なデータベース移行 （130 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 Server を IM and Presence Service で外部データベースとして展開していて、11.5(1)、11.5(1)SU1 または 11.5(1)SU2 からアップグレードする場合は、新しい SQL Server データベースを作成して新しいデータベースに移行する必要があります。

	コマンドまたはアクション	目的
ステップ 31	システムをアップグレードする前に、**HTTP リファラー/ホスト ヘッダーでホストの信頼できるリスト** を設定し、Cisco Unified CM の管理の [エンタープライズ パラメータ] ページでパブリック IP アドレスまたは DNS エイリアスを追加していることを確認してください。	この構成は、ネットワーク トポロジに、クラスタ内の個々のノードのプライベート IP アドレスとともに外部インターフェイ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。それから Unified CM は、Unified CM へのアクセスを許可する前に、最初に Unified CM クラスタで設定されたサーバーを使用して、ホスト ヘッダーに存在する IP アドレスまたはホスト名を検証します。また、Unified CM へのアクセスに使用される DNS エイリアスを、ホストの信頼済みリスト設定で設定する必要があります。たとえば、サーバーが cm1.example.local であり、phone.example.local を使用してサーバーにアクセスする場合、phone.example.local をホストの信頼済みリスト設定に追加する必要があります。 Cisco Unified CM Administration のユーザー インターフェイスから、**[システム]>[エンタープライズ パラメータ]** を選択して、使用する外部 IP アドレスまたは 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している場合は、すべての Web ページが正しくロードされるように Cisco Tomcat サービスを再起動する必要があります。

アップグレード準備 COP ファイルの実行（アップグレード前）

アップグレード準備状況 COP ファイルは、次の点を確認します。

- 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
- ファイルシステムのタイプとゲスト 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 チェック
- SIP および h.323 トランクの登録
- データベース認証および複製のステータス
- データベースの健全性
- 最後の DRS バックアップのステータス
- リモート コール制御（RCC）機能のステータス
- サービスステータス
- インストールされている COPs とロケール
- デバイス登録ステータス数
- エンタープライズ パラメータおよびサービス 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のバージョン
- 期限切れの証明書がある場合：
- FIPS モードのパスワード長の制限
- FIPS モードでの ESP および暗号化アルゴリズムの IPSec ポリシー設定チェック

（注）
- アップグレードの失敗の可能性を大幅に低減するため、アップグレードする前にアップグレード準備の 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 モードでサポートされていないため、3DES アルゴリズムを使用する 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 アルゴリズムを使用して 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状況の COP ファイルをダウンロードして、アップグレード前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) 宛先のリリースを選択し、[**ユUnified Communications Manager ユーティリティ（Unified Communications Manager Utilities）]** を選択します。
c) アップグレード準備状況の COP ファイルをダウンロードして、**アップグレード前のテストを実行**します (例: `ciscocm preUpgradeCheck-00019 COP`)。最新のファイルのファイル名とバージョンが異なる場合があることに注意してください。

ステップ 2 アップグレードに関するシステムの準備状況を確認します。

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 ファイルを再度実行します。
d) COP ファイルがエラーを返さないようにするまで、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) **[トレースとログ セントラル（Trace and Log Central）]** で、**[リモート参照（Remote Browse）]** をダブルクリックして、**[ファイルのトレース（Trace files）]** を選択して、**[次へ（Next）]** をクリックします。
c) **すべてのサーバーのすべてのサービスを選択**し、**[次へ（Next）]** をクリックします。
d) **[終了（Finish）]**、**[閉じる（Close）]** を順にクリックします。
e) ノードをダブルクリックして、**[CUCM パブリッシャ（Publisher）]>[システム（System）]>[インストール アップグレード ログ（ Install upgrade Logs）]** を展開します。
f) **[インストール（Install）]** 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。

データベース ステータス レポートの生成

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する到達可能性または遅延に関する問題がないこと、または音声およびビデオシグナリングの quality of service (QoS) に影響する問題がないことを確認します。

手順

ステップ 1 ノードのレポーティングインターフェイスにログインします。

- Unified CM ノードの場合は、Cisco Unified Reporting インターフェイスにログインします。
- IM and Presence ノードの場合は、 Cisco Unified IM and Presence レポート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 ノードでデータベースのレプリケーションを確認します。

- Unified CM の場合は、[**Unified CM Database Status**] を選択します。
- IM and Presence の場合は、 **IM and Presence データベースのステータス**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**（**Generate Report**）]（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**）] リンクをクリックして、自動的に表示されないセクションの詳細情報を表示します。

ステップ 6 レポートにエラーがあることが示されている場合は、**レポートの説明**レポートを選択し、トラブルシューティング情報を確認してください。

データベースの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***を入力して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不一致を確認します。

ステップ 3 **utils dbreplication runtimestate** コマンドを実行して、ノードでデータベース レプリケーションが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 以外の値が返された場合は、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 レポートの確認

手順

ステップ 1 Cisco Unified Serviceability インターフェイスから、**[ツール（Tools）]** > **[有用性レポートアーカイブ（Serviceability Reports Archive）]** を選択します。

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**をクリックして新しいタブでコールアクティビティレポートを開き、試行された**コール**数が仮想マシンのキャパシティに対して高すぎることを確認します。https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-system/products-implementation-design-guides-list.html にある**『シスココラボレーションシステムソリューションリファレンスネットワークデザイン（SRND）』**でシステムの推奨事項を確認することで、試行されたコール数のしきい値を決定できます。

ステップ 4 Cisco Unified Serviceability インターフェイスに戻り、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情報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情報レポートで、システムが展開サイズに対して指定されているクラスタ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。

展開のサイジングの詳細については、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 にある『シスコ コラボレーション システム ソリューション リファレンス ネットワーク デザイン（*SRND*）』
- http://tools.cisco.com/cucst にある「Collaboration Sizing Tool」。パートナーは、このツールを使用して、お客様の設定を評価することができます。

CLI の診断を実行する

コマンドラインインターフェイス (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および解決してから、アップグレードを開始およびアップグレードします。

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***を入力して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 diagnose test** 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、問題の修復は試行しません。**utils diagnose list**コマンドを実行すると、すべての診断コマンドのリストを表示できます。

ステップ 3 コマンドを**utils diagnose fix**実行して、システムの問題を自動的に修正します。

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（Cisco Unified OS Administration）] 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。
- 電話エッジトラストからの証明書の削除は、パブリッシャ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証明書を含め、期限切れの証明書がパーティションにないことを確認します。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） 12.5.x より前の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。

（注） アップグレード中は、ITLRecovery証明書がクラスタ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。電話機をリセットして、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されます。リリース 12.5(1)SU3 以降、CTL は必要なくなりました。

注意 証明書を再作成すると、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（Cisco Unified OS Administration）] 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） 証明書を再生成する場合、**[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 3 [生成（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 （112 ページ）を参照してください。

ステップ 5 CAPF 証明書、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。

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 （112 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	再起動サービス
tomcat tomcat-ECDSA	この証明書は、SIP Oauth モードが有効な場合に 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） 以下の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）ローカルおよびマスターサービス、Cisco UDS Tomcat および Cisco AXL Tomcat ウェブサービス。 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、Unified Communications Manager、MGCP、H.323、および IM and Presence 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	再起動サービス
CallManager CallManager-ECDSA	SIP、SIP トランク、SCCP、TFTP などに使用されます。	（注） リリース 14 の場合、次のサービスを再起動します。 Cisco Call Manager サービスおよびその他の関連サービス（Cisco CTI Manager、HAProxy サービスなど）：サーバーがセキュアモードの場合に CTL ファイルを更新します。 （注） 以下の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 サービスで、サーバーがセキュアモードの場合は CTL ファイルを更新します。 CallManager-ECDSA：Cisco CallManager サービス、HAProxy サービス。
CAPF	Unified Communications Manager パブリッシャで実行されている CAPF サービスで使用されます。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（オンラインおよびオフライン CAPF モードを除く）。	該当なし
信頼検証サービス（TVS）	これは信頼検証サービスで使用され、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）

- [セキュリティパラメータ（Security Parameter）] セクションには、新しいエンタープライズパラメータとして [証明書更新時の電話機の動作（Phone Interaction on Certificate Update）] が導入され、TVS、CAPF、TFTP のいずれかの証明書が更新されたときに、電話機のリセットを手動で行うか自動で行うかを設定できます。デフォルトでは、このパラメータは電話機を自動的にリセットするように設定されています。
- 証明書の再生成、削除、および更新後、「再起動サービス」の列に記載されている適切なサービスを再起動してください。

重要 これは、リリース 14SU2 以降に適用されます。

CLI経由のマルチSAN証明書のアップロードはサポートされていません。これらの証明書は、常に OS 管理 GUI を経由してアップロードする必要があります。

新規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す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の方法について、次の手順を実行します。

注意 データが失われるか、バックアップが古い場合はシステムを復元できない可能性があります。

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 の仮想化展開では、テープ ドライブによるバックアップ ファイルの保存はサポートされません。
- システムが次のバージョン要件を満たしていることを確認してください。
  - すべての Unified Communications Manager クラスタノードで、同じバージョンの Unified Communications Manager アプリケーションが実行されている必要があります。
  - すべての IM and Presence Service クラスタノードで、同じバージョンの IM and Presence Service アプリケーションが実行されている必要があります。

アプリケーションごとに、バージョン文字列のすべてが一致する必要があります。たとえば、IM and Presence データベース パブリッシャ ノードが、バージョン 11.5.1.10000-1 の場合、すべての IM and 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

ます。また、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ことも必要です。

- 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イメージのバックアップ

TFTP ディレクトリにカスタム呼出音または背景イメージがある場合は、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、ディザスタリカバリシステム(DRS)のバックアップファイルには含まれていません。

手順

ステップ 1 着信音と背景イメージが保存されているディレクトリにアクセスするには、webブラウザまたは TFTP クライアントを使用します。

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

ステップ 3 カスタム呼出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 背景イメージをバックアップします。これらは、フォルダ/デスクトップ(およびそのサブフォルダ) の TFTP ディレクトリにあります。

ネットワーク接続の確認

ネットワーク内のすべてのノードとサービスの間の接続を確認するには、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 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***を入力して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**show network cluster**の各ノードでコマンドを実行し、クラスタ内Unified Communications Managerのサーバ間の通信を確認します。

ステップ 3 NTP サーバがある場合は、 **utils ntp status**コマンドを実行して、ntp サーバ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 を実行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は**show network eth0** 、ネットワーク内の各ノードでコマンドを実行して、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Unified Communications Managerノードの FQDN に対して Ping を実行し、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 アドレスに Ping を実行して、FQDN に解決されることを確認します。

IPv6 ネットワーキングの確認

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上の IPv6 ネットワーキングがあ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と、ロードの検出に 20 分ほどかかることがあります。

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***を入力して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 コマンド **utils network ipv6 ping***destination [count]* を実行します。

- *destination* は、ping の実行対象として有効な IPv6 アドレスまたはホスト名です。
- *count* は外部のサーバに対する ping の回数です。デフォルトは 4 です。

IM and Presence と Cisco Unified Communications Manager との間の接続の確認

IM and Presence Serviceサービスノードがと Unified Communications Manager接続されていることを確認します。

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、**[診断（Diagnostics）] > [システムトラブルシュータ（System Troubleshooter）]** を選択します。
システムはトラブルシューティングチェック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ロードされたら、**同期エージェントのトラブルシューティング**テストのすべてが、[**結果**(results)]列に緑色のチェックマークが付いていることを確認し、テストが合格したことを示します。

ステップ 3 **同期エージェントトラブルシュータ**テストのいずれかが失敗した場合は、「**問題**と**解決策**」の列に記載されている情報を使用して、アップグレードプロセスを続行する前に問題を解決してください。

設定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Unified Communications Manager場合に備えて、ノードの現在の設定とログイン情報を記録します。

手順

ステップ 1 次のログインおよび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クレデンシャル (DRS、AXL、その他のサードパーティ統合のアカウントなど)
- 管理者、クラスタセキュリティ、および証明書信頼リスト (CTL) のセキュリティトークンパスワード

ステップ 2 ネットワークの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、コール詳細記録 (CDR) サーバ、および SMTP 情報
- サーバのバージョンとタイムゾーン
- 各サーバで実行されているサービスと、関連するアクティベーションステータス
- LDAP 情報とアクセスの詳細
- SNMP 情報

登録済みデバイスの数を記録する

アップグレードの完了後にエンドポイントとリソースを確認できるように、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の数をキャプチャします。また、この情報を使用して、展開している仮想マシン (VM) の容量を超え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 統合 RTMT インターフェイスから**CallManager** > **デバイス** > **デバイスの概要**を選択します。

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	Count
Registered Phones	
FXS	
FSO	
T1 CAS	
PRI	
MOH	
MTP	
CFB	

項目	Count
XCODE	

割り当てられたユーザ数を記録する

アップグレードが完了した後でこの情報を確認できるように、IM and Presence Service ノードに割り当てられたユーザ数を記録します。

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（System）]** > **[クラスタ トポロジ（Cluster Topology）]** の順に選択します。
[Cluster Topology Details] ページには、ノードと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

アップグレードプロセス中に、TFTP サービスパラメータの**最大サービス数**が変更され、デバイス登録要求の数が増加します。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、既存の設定を記録します。

手順

ステップ 1 Cisco Unified CM の管理インターフェイスから、**[システム（System）]** > **[サービス パラメータ（Service Parameters）]** を選択します。

ステップ 2 [**Server**（**サーバ**）] ドロップダウン リストから TFTP サービスを実行するノードを選択します。

ステップ 3 [**サービス**（**Service**）] ドロップダウン リストから、[**Cisco TFTP サービス**（**Cisco TFTP service**）] 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 **サービスの最大数**に設定されている値を記録します。

エンタープライズ パラメータの記録

ノードとUnified Communications ManagerIM 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は、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ます。同じパラメータが存在する場合、ノードにUnified Communications Manager設定されている設定は、アップグレードIM and Presence Serviceプロセス中にサービスノードに設定されている設定を上書きします。サービスノードにIM and Presence Service固有のエンタープライズパラメータは、アップグレード中に保持されます。

アップグレードが完了した後で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 の管理インターフェイスから、**[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 画面キャプチャを使用して設定した設定を記録し、その情報を保存して、アップグレードの完了後に設定を復元できるようにします。

ステップ 3 Cisco Unified CM IM and Presence の管理インターフェイスから、**[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 設定した内容を記録するためにスクリーン キャプチャを取り、アップグレードが完了した後に、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 **[検索（Find）]** をクリックして、すべてのユーザ レコードを表示します。

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**)] ドロップダウンリストから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 ユーザ レコードをすぐにエクスポートする場合は、[今すぐ実行（Run Immediately）] をクリックします。

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（Bulk Administration）]**>**[ファイルをアップロード/ダウンロード（Upload/Download Files）]** 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に該当するチェックボックスをオンにし、[**選択項目のダウンロード（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（File Download）] ポップアップ ウィンドウで、[**保存（Save**）] をクリックします。

ステップ 12 [名前をつけて保存（Save As）] ポップアップ ウィンドウで、ファイルの保存場所を選択して [**保存（Save**）] をクリックします。サーバの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ください。

IP フォンのファームウェアのアップグレード

アップグレード前のタスクとして、新しいリリースに対応するファームウェアに IP フォンをアップグレードすることができます。アップグレード後に電話機が自動的に新しいファームウェアを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、アップグレードの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を選択できます。

新しいファームウェアをグループ内の電話機に適用する場合は、アップグレード後に TFTP サーバの負荷を解消し、個々のデバイスのアップグレードを高速化できます。その後、Unified Communications Managerサーバの TFTP サービスを再起動し、制御された順序で IP phone を再起動してダウンタイムを最小化します。ファームウェアのアップグレード時に電話機をコールに使用できないため、電話機のファームウェアをアップグレードするには、アップグレードウィンドウ以外のメンテナンスウィンドウを使用することをお勧めします。

始める前に

- 新しいファームウェアロードを TFTP サーバ上の次のディレクトリにコピーします。`/usr/local/cm/tftp`
- IP フォンと登録済みのエンドポイントのシステムデフォルトとデバイスごとの割り当ての記録を作成します。

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 サーバを停止し、再起動します。

ステップ 8 影響を受けるデバイスをリセットし、デバイスを新しいロードにアップグレードします。

ステップ 9 Cisco Unified CM Administration から、**[デバイス（Device）]** > **[デバイスの設定（Device Settings）]** > **[デバイスのデフォルト（Device Defaults）]** を選択し、TFTP サーバ上の新しいロードについて、特定の [デバイスタイプ（Device Type）] フィールドに対する [ロード情報（Load Information）] と [非アクティブロード情報（Inactive Load Information）] 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 インターフェイスから、**[システム（System）]** > **[サーバ（Server）]** > **[重要なサービス（Critical Services）]** を選択します。

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 重要なUnified Communications Managerサービスを表示するにUnified Communications Managerは、ドロップダウンリストからノードを選択し、**[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 Service の重要なサービスを表示するには、[**IM and Presence Service**] タブをクリックし、ドロップダウンリストからIM and Presence Serviceサービスノードを選択します。

ステップ 5 ステータスが、重要なサービスが停止していることを示している場合は、アップグレードを開始する前にそれらを再アクティブ化します。

Cisco Extension Mobility の非アクティブ化

この手順は、リリース9.x 以前からアップグレードする場合にのみ実行してください。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、ノードUnified Communications Managerで Cisco extension mobility 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）] > [サービスのアクティブ化（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 Extension Mobility** サービスを選択解除します。

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ついて、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 and Presence Sync Agent の停止

アップグレードのUnified Communications ManagerIM and Presence Service一環としてアップグレードする必要がある場合は、アップグレードIM and Presence Serviceプロセスを開始する前に、Sync Agent 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 のインターフェイスから、**[ツール（Tools）] > [コントロール センターの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（Server）**] ドロップダウン リストから IM and Presence Service 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 Services**] セクションで [**Cisco Sync Agent**] を選択し、[**停止（Stop）**] をクリックします。

使用可能な共通のパーティション領域を確認する

Real-Time Monitoring Tool（RTMT）を使用して、共通パーティションにアップグレード用の十分な空き領域があることを確認します。

手順

ステップ 1 リアルタイムモニタリングツールで、左側のナビゲーションペインの**システム**カウンタのリストから [**ディスク使用率 (Disk Usage)**] を選択します。
ページには、ディスク使用率に関する詳細情報が表示されます。

ステップ 2 ページの下部にあるテーブルを表示し、共通パーティションに**使用され**ているスペースと**合計領域**を比較します。アップグレードを開始する前に、使用可能な共通パーティションスペースの最小 25 g 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ロード)、保留音 (MOH) ファイル、または多数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ことがあります。場合によっては、空き領域の 25 GB が使用可能な場合でも、アップグレードが失敗し、十分なスペースとしてエラーメッセージが表示されないことがあります。回避策は、不要なファイルを削除し、共通のパーティションにさらにスペースを作成することです。

基準値の上限および下限の調節

この手順を使用して、低および高の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。トレースの早すぎるパージを避けるために、アップグレード後、基準値の上限と下限を元の値に戻す必要があります。基準値のデフォルトの上限は 85 です。基準値のデフォルトの下限は 80 です。

手順

ステップ 1 Real Time Monitoring Tool (RTMT) インターフェイスで、左側のナビゲーションウィンドウで [**Alert Central**] をダブルクリックします。

ステップ 2 [**System**] タブで、[**LogPartitionLowWaterMarkExceeded**] を右クリックし、[**Set Alert/Properties**] を選択します。

ステップ 3 [**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 [**System**] タブで、[**LogPartitionHighWaterMarkExceeded**] を右クリックし、[**Set Alert/Properties**] を選択します。

ステップ 6 [**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領域の最大化

11.5 (X) から12.5 にアップグレードする場合は、ダウンロードする必要がある COP ファイルを確認します。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）**] セクションにある [**ソフトウェアのダウンロード（Software Download）**] リンクをクリックします。次に、**[Unified Communications] > [コール制御（Call Control）] > [Cisco Unified Communications Manager (CallManager)] > <*[バージョン（*Version*）]*>] > [Unified Communications Manager/CallManager/Cisco Unity Connectionユーティリティ（Unified Communications Manager/CallManager/Cisco Unity Connection Utilities）]** に移動します。

共通パーティションに追加の領域を作成するには、この手順の1つ以上の手順を実行します。

現在のバージョンで以前にシリアル接続を使用していた11.5(x)バージョンよりも前のバージョンでは、古いOSパーティショニング方式と仮想ディスクレイアウトがある可能性があります。これにより、「ディスク領域不足」の問題が増加します。これにより、追加の仮想ディスク領域を追加する効果が制限されます。アップグレード準備状況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ついてのガイダンスを提供します。

手順

ステップ1 次のいずれかのオプションを使用して、古い、または使用されていない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管理インターフェイスから、[**Software Upgrade** > **TFTP File Management**]を選択し、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から、`file list tftp`および`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] [> **デバイスロード管理**]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デバイスのロードサイズを確認します。これは、ファイルサイズが降順でソートされます。

Show diskusage common < sort >コマンドを実行して、使用可能な共通パーティションサイズと、降順のファイルサイズでソートされた空き領域を確認します。

ステップ2 前の手順でアップグレードに十分なディスク領域が作成されていない場合にのみ、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）を使用します。

このCOPファイルを使用すると、システムを再構築することなく、共通パーティションの非アクティブ側を削除して使用可能なディスク領域を増やすことができます。先に進む前に、このCOPファイルに関するReadmeファイルを確認してください。

（注） 非アクティブなパーティションが使用できなくなるため、このファイルのインストール後に非アクティブなバージョンに切り替えることはできません。

（注） 110Gまたは2つの80Gディスク展開の場合、アップグレードに使用可能な領域は、少なくともアクティブパーティションのディスク領域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、アクティブパーティションは25G を超えることはできません。また、使用可能な領域は少なくとも50Gにする必要があります。次に、ディスク使用率を確認するコマンドを示します。

1. **Show diskusage activelog < sort >**コマンドを実行して、アクティブなサイドパーティションのサイズを確認します。これは、ファイルサイズが降順でソートされます。
2. **Show diskusage common < sort >**コマンドを実行して、使用可能な共通のパーティションサイズと、降順のファイルサイズでソートされた空き領域を確認します。
3. tftp のデバイス ロード サイズを確認するには、[**show diskusage tftp <sort>**] コマンドを実行します。出力結果はファイル サイズの降順でソートされます。
4. Active partition からログを削除するには、 **file delete activelog < filename >**コマンドを実行します。

アップグレード ファイルの取得

新しいリリースのアップグレードファイル、および必要なアップグレードのCisco Option Package (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 必要なCOPファイル(存在する場合)を特定するには、この手順の下の表を参照してください。

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ます。このソフトウェアは、export restricted (K9) および export 無制限バージョン (XU) で使用できます。そのため、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 > [**ダウンロードとアップグレード（Download & Upgrade）**] セクションの下にある [**ソフトウェアダウンロード（Software Download）**] リンクをクリックし、[**Unified Communications > Call Control > Cisco Unified Communications Manager（CallManager）** > **<バージョン>** > **の Unified Communications Manager/CallManager/Cisco Unity Connection の更新（Unified Communications Manager/CallManager/Cisco Unity Connection Updates）**に移動します。
- 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 に移動して> [**ソフトウェアダウンロード（Software Download）**] リンクを [**ダウンロードとアップグレード（Download & Upgrade）**] セクションからクリックします。次に **[Unified Communications] > [Unified Communications アプリケーション（Unified Communications Applications）] > [Presence ソフトウェア（Presence Software）] >**

[Unified Communications Manager IM and Presence Service] > **<バージョン>** > **[Unified Presenceサービス（CUP）の更新（Unified Presence Service (CUP) Updates）]** に移動します。

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 [**ソフトウェアのダウンロード（Software Download**）] リンクをクリックします。次に、**[Unified Communications]** > **[コール制御（Call Control）]** > **[Cisco Unified Communications Manager (CallManager)]** > ***[<バージョン（Version）>]*** > **[Unified Communications Manager/CallManager/Cisco Unity Connectionユーティリティ（Unified Communications Manager/CallManager/Cisco Unity Connection Utilities）]** に移動して、Unified Communications Manager の 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、[**ソフトウェアのダウンロード（Software Download**）] リンクを [**ダウンロードとアップグレード（Download & Upgrade**）] セクションからクリックします。次に、**[Unified Communications]** > **[Unified Communications アプリケーション（Unified Communications Applications）]** > **[Presence ソフトウェア（Presence Software）]** > **[Unified Communications Manager IM and Presence Service]** > **<バージョン>** > **[Unified Presenceサービス（CUP）の更新（Unified Presence Service (CUP) Updates）]**に移動し、[**UTILS**] を選択して IM and Presence Service の COP ファイルをダウンロードします。

必須 COP ファイル

次の表は、COP ファイルが必要なアップグレード パスを示しています。Cisco Unified OS 管理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は、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 ファイルの詳細については、*COP* ファイルでサポートされるアップグレードおよび移行パスを参照してください。

データベース レプリケーションのタイムアウトを増やす

Unified Communications Managerパブリッシャ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場合は、より多くの Unified Communications Manager サブスクライバ ノードが複製を要求する時間を十分に確保できるように、データベース レプリケーションのタイムアウト値を大きくします。タイマーの期限が切れると、最初の Unified Communications Manager サブスクライバ ノードと、その期間内に複製を要求した他のすべての 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 ノードとの間でバッチ データ 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***を入力して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 Timeout コマンドを実行します。この場合、timeout はデータベース レプリケーションのタイムアウト (秒単位) です。 **utils dbreplication setrepltimeout** この値は、300 から 3600 までです。

デフォルトのデータベース レプリケーションのタイムアウト値は 300（5 分）。

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 ノードのアクティブ ユーザ数を記録します。この情報は、Cisco Unified CM IM and Presence の（**System** > **Presence Topology**）ウィンドウに表示されます。この情報は、後にハイ アベイラビリティを再度有効にする際に必要となります。

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（Save）] 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 完了後、さらに変更を行う前に、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。

仮想マシンにシリアル ポートを追加する

アップグレードに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。

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 シリアルポートを追加するには、設定を編集します。vSphere クライアントを使用した設定の変更については、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 ファイルに接続します。

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が正常に完了したら、「シリアル ポートの削除（140 ページ）」の手順に従います。アップグレードに失敗した場合は、「アップグレードの失敗後のログファイルのダンプ （159 ページ）」を参照してください。

RTMT の高可用性の設定

Cisco Unified Real-Time Monitoring Tool（RTMT）を使用しており、クラスタを構成している場合は、クラスタ全体のアップグレード中の接続損失を回避するために、RTMT のハイアベイラビリティを設定す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（Server）**] 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（Service）**] ドロップダウンから、[**Cisco AMC サービス（Cisco AMC service）**] を選択します。

ステップ 5 [**Primary Collector**] サービスパラメータで、[any subscriber node] を選択します。

ステップ 6 [**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 をサブスクライバノードに接続します。

Microsoft SQL Server を使用したアップグレードに必要なデータベース移行

Microsoft SQL Server を IM and Presence Service の外部データベースとして展開していて、11.5(1)、11.5(1)SU1、または 11.5(1)SU2 からアップグレードする場合は、新しい SQL Server データベー

スを作成し、その新しいデータベースに移行する必要があります。この作業は、このリリースで強化されたデータ タイプのサポートのために必要です。データベースを移行しないと、既存の SQL Server データベースでスキーマの検証に失敗し、持続チャットなどの外部データベースに依存するサービスが開始されません。

IM and Presence Service をアップグレードした後、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。

Note この移行は、Oracle または PostgreSQL の外部データベースでは必要ありません。

Before you begin

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。コピーを入手するには、Cisco TAC にお問い合わせください。

Procedure

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』の次の章を参照してください。

a. 「Microsoft SQL Installation and Setup」：アップグレードされた IM と Presence サービスで新しい SQL Server 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。

b. 「IM and Presence Service External Database Setup」：新しいデータベースを作成した後、この章を参照して、IM and Presence Service にデータベースを外部データベースとして追加します。

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

a. 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。

b. **[外部データベース トラブルシュータ（External Database Troubleshooter）]** セクションにエラーが表示されていないことを確認します。

ステップ 4 すべての IM and Presence Service のクラスタノード上で Cisco XCP ルータを再起動します。

a. Cisco Unified IM and Presence のサービスアビリティから、**ツール > コントロールセンタ - ネットワークサービス**を選択します。

b. **[サーバー（Server）]** メニューから、IM and Presence Service ノードを選択し、**[移動（Go）]** をクリックします。

c. **IM and Presence Services**の下で、**Cisco XCP Router**を選択して、**再起動**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します。

a. [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。

b. [サーバ（Server）] メニューから、IM and Presence ノードを選択し、[移動（Go）] をクリックします。

c. **[IM およびプレゼンスサービス（IM and Presence Services）]** の下で、次のサービスを選択します。

Cisco XCP Text Conference Manager

Cisco XCP File Transfer Manager

Cisco XCP Message Archiver

d. [停止（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にデータを移行します。`MSSQL_migrate_script.sql`

Note このスクリプトのコピーを入手するには、Cisco TAC にお問い合わせください。

ステップ 7 システム トラブルシュータを実行して、新しいデータベースにエラーがないことを確認します。

a. 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。

b. **[外部データベーストラブルシュータ（External Database Troubleshooter）]** セクションにエラーが表示されていないことを確認します。

ステップ 8 以前に停止したサービスを開始します。

a. [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。

b. [サーバ（Server）] メニューから、IM and Presence ノードを選択し、[移動（Go）] をクリックします。

c. **[IM およびプレゼンスサービス（IM and Presence Services）]** の下で、次のサービスを選択します。

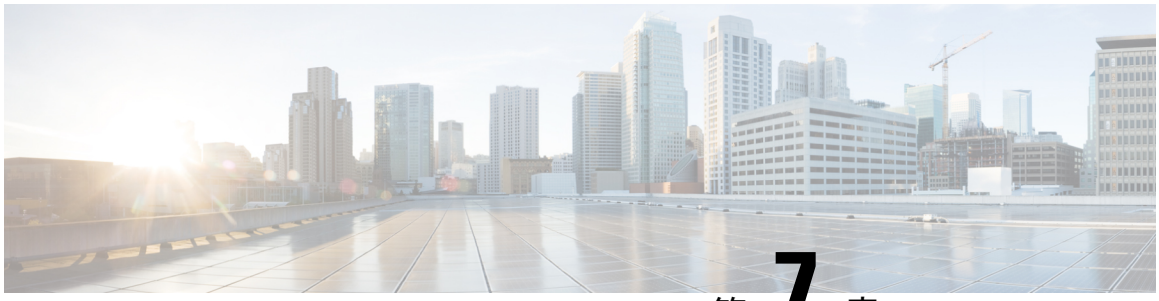
Cisco XCP Text Conference Manager

Cisco XCP File Transfer Manager

Cisco XCP Message Archiver

d. [開始（Start）] をクリックします。

ステップ 9 外部データベースが稼働していることと、すべてのチャット ルームが Cisco Jabber クライアントから認識可能であることを確認します。新しいデータベースが動作していることが確かな場合にのみ、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の方法について、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 （140 ページ）	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。電話機をリセットして、最新の更新を反映します。 （注） Unified Communications Manager の移行では、これをスキップできます。
ステップ 2	シリアル ポートの削除 （140 ページ）	アップグレード前の作業中に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。 この手順は、すべてのノードに対して実行します。
ステップ 3	エクステンション モビリティの再起動 （141 ページ）	アップグレード前のタスクの一部として Cisco extension mobility を非アクティブにした場合は、これを再起動することができます。
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一連のテストを実

	コマンドまたはアクション	目的
		行します。これらのテストでは、不一致を識別するために、アップグレード前の設定とアップグレード後の設定を比較します。このテーブルのすべての手順を完了したら、アップグレード後の COP ファイルを再度実行し、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の数が表示されます。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「show risdb query cti」を実行すると、ノードに登録されているデバイスの詳細が表示されます。このデバイスは、そのノードで少なくとも1回登録してエントリを作成する必要があります。たとえば、デバイスが subscribe 2 に登録され、登録解除されて subscribe 1 に移動した場合、subscribe 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（143 ページ）	アップグレードプロセス中に変更された 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（143 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 ノードで、エンタープライズパラメータの設定を復元します。

	コマンドまたはアクション	目的
ステップ 7	基準値の上限および下限のリセット（144 ページ）	トレースの早期消去を回避するために、この手順を使用して、高および下限のウォーターマークを元の値に復元します。 PCD の移行については、このタスクをスキップできます。
ステップ 8	VMware ツールの更新 （145 ページ）	アップグレードが完了したら、VMware ツールを更新する必要があります。 この手順は、すべてのノードに対して実行します。
ステップ 9	ロケールのインストール（145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ている英語（米国）を除き、使用しているロケールを再インストールする必要があります。 この手順は、すべてのノードに対して実行します。
ステップ 10	データベース レプリケーションのタイムアウトの復元 （147 ページ）	アップグレードプロセスを開始する前に、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た場合は、この手順を使用します。 ノードでのみこのUnified Communications Manager手順を実行します。
ステップ 11	登録済みのデバイス数の確認 （147ページ）	アップグレードの完了後に、Unified CM ノードのエンドポイントとリソースを確認するには、次の手順を使用します。
ステップ 12	割り当て済みのユーザを確認する （148 ページ）	この手順を使用して、アップグレードが完了しIM and Presence Serviceた後に、ノードに割り当てられたユーザの数を確認します。
ステップ 13	機能のテスト （148 ページ）	アップグレード後に電話機の機能と機能が正しく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 （149 ページ）	Cisco Unified Real Time Monitoring Tool（RTMT）を使用する場合は、新しい

	コマンドまたはアクション	目的
		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 （150 ページ）	オプション。この手順を使用して、電話機の呼出音、コールバックトーン、およびバックグラウンドを TFTP サーバにアップロードして、それらのノードが使用可能になるようにします。
ステップ 16	カスタムログインメッセージのセットアップ （152 ページ）	オプション。Unified CM ノードの場合のみ、カスタマイズされたログイ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 ポリシーの設定 （153 ページ）	リリース 6.1 (5) からの PCD 移行を完了した場合は、新しいリリースに移行されないため、IPSec ポリシーを再作成する必要があります。
ステップ 18	新しいマネージャ アシスタント権限の割り当て （153 ページ）	アップグレード前に Manager Assistant を導入していて、クラスタ間ピアユーザまたはCUMA ロールにユーザが割り当てられている場合は、これらのロールが現在のリリースに存在しないため、ロールにユーザを再割り当てする必要があります。
ステップ 19	IM and Presence Service のデータ移行の検証 （154 ページ）	この手順は、Cisco Unified Presence リリース8.x から IM and Presence Service リリースに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に対するハイアベイラビリティの有効化 （155 ページ）	アップグレードプロセスの前にIM and Presence Serviceサービスのハイアベイラビリティを無効にした場合は、次の手順を使用して再度オンにします。
ステップ 21	IM and Presence Sync Agent の再起動 （155 ページ）	アップグレードプロセスを開始IM and Presence Serviceする前に Sync Agent サービスを停止した場合は、ここで再起動してください。
ステップ 22	Cisco Emergency Responder サービスの再起動 （156 ページ）	アップグレード後Unified Communications Managerに AXL 接続が

	コマンドまたはアクション	目的
		確立されるようにするには、CER サービスを再起動します。 また、Unified CM パブリッシャノードで AXL 変更通知の切り替えを再起動する必要があります。

ソフトウェア バージョンの切り替え

標準アップグレードを実行すると、新しいソフトウェアが非アクティブなバージョンとしてインストールされます。アップグレード処理中に新しいソフトウェアでリブートするか、後から新しいバージョンに切り替えることができます。

アップグレードが完了した直後にバージョンを切り替えなかった場合は、ここで実行してください。アップグレードが完了し、クラスタ内のすべてのノードが更新されるように、バージョンを切り替える必要があります。新たなソフトウェア バージョンに切り替えるまで、バックアップは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、非アクティブな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 分ほどかかります。この手順を実行すると、アクティブなソフトウェアバージョンと非アクティブなバージョンの両方が表示されます。

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

およびUnified Communications Managerノードのソフトウェア IM and Presence Serviceバージョンは、手動によるスイッチングルールに従って一致する必要があります。したがって、スイッチ Unified Communications ManagerIM and Presence Serviceを切り替える前に切り替える必要があります。

次の情報を確認してください。バージョンの切り替えの理解 （87 ページ）

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には、まずパブリッシャ ノードから切り替える必要があります。

ステップ 2 アップグレードす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 オペレーティング システムの管理にログインします。
- ノードUnified Communications Managerをアップグレードしたら、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てシステムを再起動します。

Unified Communications Manager のアップグレード時にバージョンの切り替えを実行すると、IP 電話から新しい設定ファイルが要求されます。この要求の結果、デバイスのファームウェアは自動的にアップグレードされます。

CTL ファイルの更新

12.0 より前の Unified Communications Manger から 12.0 以降のバージョンへのアップグレード中に、クラスタごとに ITLRecovery 証明書が生成されます。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。電話機をリセットして、最新の更新を反映します。

（注） リリース 12.5(1)SU3 以降、CTL の更新は必要なくなりました。

手順

ステップ 1 **Unified Communications ManagerAdmionistration > System > エンタープライズ パラメータ構成**で Unified Communications Manager のセキュリティ モードを確認します。

[Cluster Security Mode] フィールドを見つけます。フィールドの値が 1 と表示されている場合、混合モード用に Unified Communications Manager が構成されています。

ステップ 2 CTL ファイルを手動で更新します。CTL ファイルを更新する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 電話機をリセットして、更新を反映させます。

シリアル ポートの削除

アップグレード前のタスクでは、アップグレードログをキャプチャするためのシリアルポートを仮想マシンに追加しました。システムのアップグレードが正常に完了したら、シリアルポートを削除して、仮想マシンのパフォーマンスに影響が及ばないように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 シリアルポートを削除するには、設定を編集します。設定の編集方法については、VMWare のマニュアルを参照してください。

ステップ 3 仮想マシンの電源をオンにして、アップグレード後のタスクを続行します。

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、アップグレードプロセスを開始する前に Cisco extension mobility を停止する必要があります。アップグレード前の作業の一環として Cisco extension mobility を無効にした場合は、次の手順Unified Communications Managerを使用してノードのサービスを再起動します。

手順

ステップ 1 Cisco Unified Serviceability から、**[ツール（Tools）] > [サービスのアクティブ化（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 Extension Mobility** 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）

アップグレード後に、アップグレード後の COP ファイルを実行します。これにより、次のことが確認されます。

- 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、クラスタ内)
- FIPS モードのパスワード長の制限
- 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 トランクの登録
- データベース認証および複製のステータス
- データベースの健全性
- 最後の DRS バックアップのステータス

- サービスステータス
- インストールされている COPs とロケール
- デバイス登録ステータス数
- エンタープライズ パラメータおよびサービス 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のバージョン

（注） システムの健全性を確認するには、アップグレード後にアップグレード後のチェックのためにアップグレード準備の COP ファイルを実行することを強くお勧めします。

手順

ステップ 1 アップグレード後のテストを実行するには、アップグレード準備状況の COP ファイルをダウンロードします。

a) ダウンロードサイトに移動します。
b) 宛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) アップグレード準備状況の COP ファイルをダウンロードして、**アップグレード前のテストを実行**します (例: `ciscocm postUpgradeCheck-00019 COP`)。最新のファイルのファイル名とバージョンが異なる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健全性を確認します。

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いようにするには、これらの手順を繰り返します。

ステップ 3 アップグレード後に CLI からレポートを表示するには、**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 をログインします。
b) **[トレースとログ セントラル（Trace and Log Central）]** で、**[リモート参照（Remote Browse）]** をダブルクリックして、**[ファイルのトレース（Trace files）]** を選択して、**[次へ（Next）]** をクリックします。
c) **すべてのサーバーのすべてのサービスを選択**し、**[次へ（Next）]** をクリックします。
d) **[終了（Finish）]**、**[閉じる（Close）]** を順にクリックします。
e) ノードをダブルクリックして、**[CUCM パブリッシャ（Publisher）]>[システム（System）]>[インストール アップグレード ログ（ Install upgrade Logs）]** を展開します。

f) **[インストール（Install）]** 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

これでアップグレードは完了です。新しいソフトウェアの使用を開始できます。

TFTP パラメータのリセット

アップグレードプロセス中に、TFTP サービスパラメータの**最大サービス数**が変更され、デバイス登録要求の数が増加します。アップグレードの完了後にパラメータをリセットするには、次の手順を使用します。

手順

ステップ 1 Cisco Unified CM の管理インターフェイスから、**[システム（System）]** > **[サービス パラメータ（Service Parameters）]** を選択します。

ステップ 2 [**Server**（**サーバ**）] ドロップダウン リストから TFTP サービスを実行するノードを選択します。

ステップ 3 [**サービス**（**Service**）] ドロップダウン リストから、[**Cisco TFTP サービス**（**Cisco TFTP service**）] 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 **最大サービス数**を、アップグレード前に使用したものと同じ値、または設定に推奨される値に設定します。

デフォルト値は 500 です。同じサーバ上で他の Cisco CallManager サービスを使用して 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推奨します。専用 TFTP サーバの場合は、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
- 3500 (CPU 構成が高い専用 TFTP サーバの場合)

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、ノードにUnified Communications Manager設定されている設定は、アップグレードIM and Presence Service中にノー

ドで設定された設定を上書きします。ノードにIM and Presence Service固有のエンタープライズパラメータは、アップグレード中に保持されます。

アップグレードプロセス中に上書きされたIM and Presence Serviceノードの設定を再設定するには、次の手順を使用します。

始める前に

アップグレード前の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（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 現在の設定とアップグレード前に存在した設定を比較し、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。

基準値の上限および下限のリセット

トレースの早すぎるパージを避けるために、この手順を使用して、基準値の上限と下限を元の値に戻す必要があります。

手順

ステップ 1 Real Time Monitoring Tool (RTMT) インターフェイスで、左側のナビゲーションウィンドウで [**Alert Central**] をダブルクリックします。

ステップ 2 [**System**] タブで、[**LogPartitionLowWaterMarkExceeded**] を右クリックし、[**Set Alert/Properties**] を選択します。

ステップ 3 [**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 [**System**] タブで、[**LogPartitionHighWaterMarkExceeded**] を右クリックし、[**Set Alert/Properties**] を選択します。

ステップ 6 [**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 ツールの更新

VMware ツールは、管理およびパフォーマンスの最適化のための一連のユーティリティです。Unified Communications Manager 15 は、Open VMware ツールのみをサポートします。

- Unified Communications Manager リリース 12.5(1) または 14 および SU から 15 へのアップグレードまたは移行（たとえば、上位の SU へ）の場合、Open VMware ツールがデフォルトでインストールされます。
- Unified Communications Manager リリース 11.5(1) 移行からの新規インストールおよび PCD 移行では、デフォルトでオープン VMware ツールがインストールされます。

コマンドを実行して、VMware ツールが現在実行されていることを確認します。**vmtools status** を実行します。

ロケールのインストール

ロケールをインストールするには、次の手順を実行します。アップグレード後、デフォルトでインストールされている英語（米国）を除き、使用しているロケールを再インストールする必要があります。Unified Communications Manager ノードまたは IM and Presence Service ノードのメジャーおよびマイナーバージョン番号と一致する最新バージョンのロケールをインストールしてください。

Unified Communications ManagerまたはIM and Presence Serviceノードにロケールをインストールできます。両方の製品用のロケールをインストールする場合、次の順番で、すべてのクラスタノードで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 Service ノードに特定のロケールをインストールする場合は、最初に Unified Communications Manager クラスタに同じ国の Unified Communications Manager ロケール ファイルをインストールする必要があります。

手順

ステップ 1 Cisco.com でリリース用のロケール インストーラを検索します。

- Cisco Unified Communications Manager については、次の URL を参照してください。https://software.cisco.com/download/navigator.html?mdfid=268439621&i=rm
- IM and Presence Service については、次の URL を参照してください。 https://software.cisco.com/download/navigator.html?mdfid=280448682&i=rm

ステップ 2 リリースのロケールのインストーラを、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います。次の表記法が使用されます。
  - `cm-locale-language-country-version.cop`（Cisco Unified Communications Manager）
  - `ps-locale-language_country-version.cop`（IM and Presence Service）
- 複合ネットワーク ロケール ファイル：すべての国に対応した、さまざまなネットワーク項目（電話機のトーン、Annunciator、およびゲートウェイ トーンなど）の国固有のファイルが格納されています。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。
  - `locale-combinednetworklocale-version` (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 の管理（Cisco Unified OS Administration）] にログインします。

ステップ 4 **[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）]**を選択します。

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

- [ソース（Source）] で、[リモート ファイル システム（Remote File System）] 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（Server）] フィールドに、リモート ファイル システムのサーバ名を入力します。
- リモート ファイル システムのクレデンシャルを入力します。
- **[転送プロトコル（Transfer Protocol）]** ドロップダウン リストから **[SFTP]** を選択します。転送プロトコル用に SFTP を使用する必要があります。

ステップ 6 [次へ（Next）] をクリックします。

ステップ 7 サーバ上でロケールをダウンロードし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、サーバの再起動後に有効になります。

ステップ 9 すべての Unified Communications Manager および IM and Presence Service クラスタノードで、この手順を所定の順序で繰り返します。

（注） 新しいロケールが、すべてのクラスタノードに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 および IM and Presence Service Service の両方のロケールをインストールする場合、ユーザ 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 Service のロケールインストールが完了する前にエンドユーザが電話の言語をリセットした場合など、何らかの問題が発生した場合は、セルフケア ポータルで電話の言語を英語にリセットするようにユーザに指示します。ロケールのインストールが完了すると、ユーザは電話言語をリセットするか、一括管理を使用してロケールを一括して適切な言語に同期させることができます。

データベース レプリケーションのタイムアウトの復元

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 プロセスを開始する前に、データベース レプリケーションのタイムアウト値を大きくしていた場合には、この手順を使用します。

デフォルトのデータベース レプリケーションのタイムアウト値は 300（5 分）。クラスタ全体のアップグレードが完了し、Unified Communications Manager サブスクライバ ノードでレプリケーションが正しくセットアップされたら、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***を入力して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 Timeout コマンドを実行します。この場合、timeout はデータベースレプリケーションのタイムアウト (秒単位) です。 **utils dbreplication setrepltimeout**　値を 300 (5 分) に設定します。

登録済みのデバイス数の確認

Real Time Monitoring Tool (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（Voice/Video）** > **デバイスの概要（Device Summary）**を選択します。

ステップ 2 次の登録済みのデバイス数を記録する。

項目	Count
Registered Phones	
登録済みゲートウェイ	
登録済みのメディア リソース（Registered Media Resources）	
Registered Other Station Devices	

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の数と比較し、エラーがないことを確認します。

割り当て済みのユーザを確認する

この手順を使用して、アップグレードの完了後にノードに割り当てられているユーザ数を確認します。

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（System）]** > **[クラスタ トポロジ（Cluster Topology）]** の順に選択します。

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済みユーザの数と比較し、エラーがないことを確認します。

機能のテスト

アップグレードの完了後に、次の作業を実行してください。

- アップグレード後の COP を実行します。

  システムが安定していることを確認するために、一連のテストを実行します。また、相違点を特定するために、現在のバージョンとアップグレードする前に、さまざまなパラメータを比較します。このリストのすべての手順を完了したら、アップグレード後のCOPファイルを再度実行し、COP レポートを確認します。

- 次のタイプのコールを発信して、電話機の機能を確認します。
  - Voice mail
  - 局間
  - 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
  - 割り込み
  - 転送
  - C 割り込み
  - 共有回線への着信
  - 応答不可（Do Not Disturb）
  - プライバシー
  - プレゼンス
  - CTI コール制御
  - ビジー ランプ フィールド
- IM and Presence Service の次の機能をテストします。
  - 使用可能、使用不可、ビジーなどの基本的なプレゼンス状態
  - ファイルの送受信
  - 常設チャット、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 互換性を確実にするため、クラスタ内のすべてのサーバでのアップグレードを行ってから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、ツールをアップグレードした後で、これらの項目に統合RTMT でアクセスできます。

始める前に

新しいバージョンの RTMT 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推奨します。

手順

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

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を実行しているクライアントで Unified RTMT をインストールするには、[Cisco Real-Time Monitoring Tool - Windows and Linux Tool] の **[ダウンロード（Download）]** リンクをクリックし、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 クライアント上の優先ロケーションに CiscoRTMTPlugin.zip をダウンロードします。

ステップ 5 Windows バージョン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 バージョン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) ファイルが抽出されたら、 **chmod 755 run.sh** コマンドを実行して、 `run.sh`ファイルに権限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

TFTP サーバに、電話機で使用するファイルをアップロードできます。アップロード可能なファイルには、カスタム呼出音、コールバック トーン、および背景画像などがあります。このオプションは、接続先の特定のサーバにのみファイルをアップロードするもので、クラスタ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もファイルをアップロードできます。

クラスタ内に 2 台の Cisco TFTP サーバが設定されている場合、両方のサーバで次の手順を実行する必要があります。この手順を実行しても、ファイルがすべてのサーバに配信されるわけではなく、クラスタ内の 2 台の Cisco TFTP サーバにも配信されません。

TFTP サーバ ファイルをアップロードまたは削除するには、次の手順を実行します。

手順

ステップ 1 [Cisco Unified Communications オペレーティング システムの管理（Cisco Unified Communications Operating System Administration）] ウィンドウで、**[ソフトウェアのアップグレード（Software Upgrades）] > [TFTP] > [ファイルの管理（File Management）]** を選択します。

[TFTP ファイルの管理（TFTP File Management）] ウィンドウが表示され、現在アップロードされているファイルの一覧が表示されます。[検索（Find）] を使用すると、ファイルの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、次の手順を実行します。

a) [ファイルのアップロード] をクリックします。

[ファイルのアップロード（Upload File）] ダイアログボックスが表示されます。

b) ファイルをアップロードするには、**[参照（Browse）]** をクリックし、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）]** フィールドに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が成功すると、[ステータス（Status）] 領域に表示されます。

e) ファイルをアップロードしたら、Cisco TFTP サービスを再起動します。

（注） 複数のファイルをアップロードする場合は、すべてのファイルをアップロードした後に Cisco TFTP サービスを一度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、次の手順を実行します。

a) 削除するファイルの横にあるチェックボックスをオンにします。

また、**[すべてを選択（Select All）]** をクリックするとすべてのファイルを選択でき、**[すべてをクリア（Clear All）]** をクリックするとすべての選択をクリアできます。

b) **[選択項目の削除]** をクリックします。

（注） `tftp` ディレクトリ内の既存のファイルを修正する場合は、CLI コマンド **file list tftp** を使用して TFTP ディレクトリ内のファイルを表示し、**file get tftp** を使用して TFTP ディレクトリ内のファイルをコピーします。詳細については、『Cisco Unified Communications Solutions のコマンドライン インターフェース リファレンス ガイド』を参照してください。

カスタム ログイン メッセージのセットアップ

カスタマイズされたログイン メッセージを含むテキスト ファイルをアップロードすると、そのメッセージを Cisco Unified Communications オペレーティング システムの管理、Cisco Unified CM Administration、Cisco Unified Serviceability、ディザスタ リカバリ システムの管理、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することができます。

カスタマイズされたログイン メッセージをアップロードするには、次の手順を実行します。

手順

ステップ 1 [Cisco Unified Communicationsオペレーティングシステムの管理（Cisco Unified Communications Operating System Administration）] ウィンドウで、**[ソフトウェアのアップグレード（Software Upgrades）] > [ログインメッセージのカスタマイズ（Customized Logon Message）]** を選択します。

[Customized Logon Message] 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] をクリックします。

（注） アップロードできるファイルは 10kB 以内です。

システムにカスタマイズされたログイン メッセージが表示されます。

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

カスタマイズされたログイン メッセージが削除され、システムにデフォルトのログイン メッセージが表示されます。

（注） カスタム メッセージを Cisco Unified Communications オペレーティング システムの管理、Cisco Unified CM Administration、Cisco Unified Serviceability、ディザスタ リカバリ システムの管理、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するには、**[ユーザの確認応答が必要（Require User Acknowledgment）]** チェックボックスをオンにします。

IPsec ポリシーの設定

この手順は、リリース 10.5 から PCD 移行を実行してい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 ポリシーを再構成する必要があります。移行の前に、クラスタの両方のノードで IPsec ポリシーを無効にする必要があります。移行が成功したら、IPsec ポリシーを有効にしてください。

- IPsec には双方向プロビジョニングが必要です（ホストまたはゲートウェイごとに 1 ピア）。
- 一方の IPsec ポリシー プロトコルが 「ANY」、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 ノードに IPsec ポリシーをプロビジョニングする場合、「ANY」 プロトコルを使用するノードでの検証で検出漏れが発生する可能性があります。
- IPsec はシステムのパフォーマンスに影響します（特に暗号化した場合）。

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（Add New）]** 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（Save）]** 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。

新しいマネージャ アシスタント権限の割り当て

この手順は、以前のリリースが Cisco Unified Communications Manager Assistant 機能を使用するように設定されていて、クラスタ間ピアユーザまたは CUMA ロールのいずれかを使用するようにアプリケーションユーザが割り当てられている場合にのみ実行します。クラスタ間ピアユーザと CUMA ロールは、リリース 10.0 (1) 以降では廃止され、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ロール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設定するには、『Cisco Unified Communications Manager アドミニストレーション ガイド』の「ユーザーの管理」の章を参照してください。

ステップ 2 IM and Presence Service Service のユーザ インターフェイス（**[プレゼンス（Presence）] > [クラスタ間設定（Inter-Clustering）]**）で定義されている AXL ユーザに、Unified Communications Manager アプリケーション ユーザ ページで標準 AXL API アクセス ロールが関連付けられていることを確認します。

IM and Presence Service のデータ移行の検証

Cisco Unified Presence リリース8.x からIM and Presence Serviceサービスリリースにアップグレードすると、ユーザプロファイルはにUnified Communications Manager移行されます。ユーザ プロファイル情報は Unified Communications Manager に新しいサービス プロファイルとして保存されます。このとき、次の名前と説明の形式が使用されます。

名前：UCServiceProfile_Migration_x（x は、1 以降の番号）

説明：移行済みサービス プロファイル番号 x

Cisco Unified Presence Release 8.x からアップグレード後に Cisco Jabber に正常にログインできるようにするには、ユーザ プロファイル データの移行が正しく行われたことを確認する必要があります。

作成されていてもユーザ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 の管理から **[ユーザ管理（User Management）] > [ユーザ設定（User Settings）] > [サービス プロファイル（Service Profile）]** を選択します。

ステップ 2 すべてのサービス プロファイルをリストするには、**[検索（Find）]** を選択します。

ステップ 3 次の名前形式を持つ、移行済みサービス 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 移行済みサービス プロファイルがない場合は、`installdb log` ファイルでエラーがないか確認します。

ステップ 5 データの移行に失敗すると、Unified Communications Manager でインポート エラー アラームが発生し、Cisco Sync Agent から Cisco Unified CM IM and Presence の管理 GUI に障害通知が送信されます。

ヒント アラームの詳細を見るには、RTMT for Cisco Unified Communications Manager にログインします。

次のタスク

サービス プロファイルを編集し、意味のある名前に変更できます。サービス プロファイルの設定方法の詳細については、『Cisco Unified Communications Manager アドミニストレーション ガイド』を参照してください。

アップグレード後の COP ファイルを実行します。システムが安定していることを確認するために、一連のテストを実行します。また、アップグレード前のさまざまなパラメータが現在のバージョンと比較され、相違点が特定されます。

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有効化

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、プレゼンス冗長グループでハイアベイラビリティを無効にした場合は、次の手順を使用してこれを有効にします。

始める前に

サービスが再起動してから30分以内の場合は、ハイ アベイラビリティを有効にする前に Cisco Jabber セッションが再作成されたことを確認します。十分な時間を確保しない場合、セッションが作成されていない Jabber クライアントでプレゼンスは機能しません。

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 セッションの数は、アップグレード前にハイ アベイラビリティを無効にした際に記録したユーザ数と一致するはずです。

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（Find）]** をクリックし、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 ウィンドウが表示されます。

ステップ 3 **ハイ アベイラビリティの有効化**の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 この手順を、各プレゼンス冗長グループで繰り返します。

IM and Presence Sync Agent の再起動

アップグレード プロセスの開始前に IM and Presence Service Sync Agent サービスを停止した場合は、ここでサービスを再起動します。

手順

ステップ 1 Cisco Unified Serviceability インターフェイスから、**[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）]** を選択します。

ステップ 2 [**サーバ（Server**）] ドロップダウン リストから 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 Services**] セクションで [**Cisco Sync Agent**] を選択し、[**再起動（Restart**）] をクリックします。

例

（注） Cisco Intercluster Sync Agent が最初の同期を完了したら、新しい tomcat 証明書をにUnified Communications Manager手動でロードします。これにより、同期に障害が発生しないようにします。

（注） アップグレード後のCOPを実行します。システムが安定していることを確認するために、一連のテストを実行します。また、相違点を特定するために、現在のバージョンとアップグレードする前に、さまざまなパラメータを比較します。

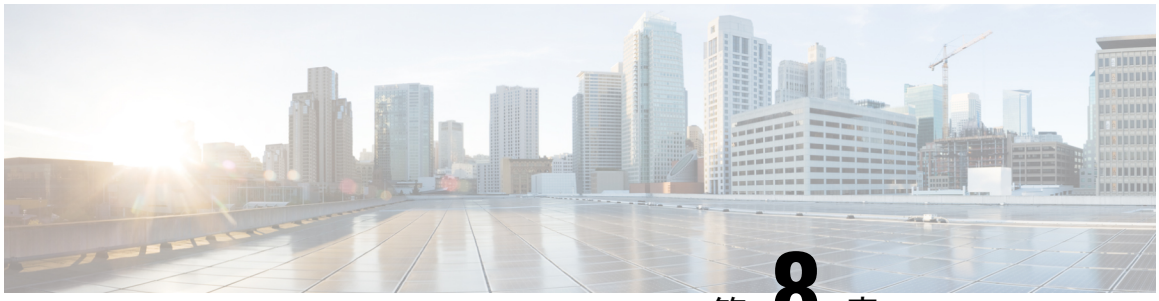
Cisco Emergency Responder サービスの再起動

手順

アップグレードプロセスを開始Cisco Emergency Responderする前にサービスを停止した場合は、ここで再起動してください。

ステップ 1 Cisco Emergency Responder Serviceability インターフェイスから、[**ツール（Tools**）] > [**コントロールセンター（Control Center**）] を選択します。

ステップ 2 [**Cisco 緊急応答側**] 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および移行

現在のリリースから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は、次のプロセスを使用できます。

- Unified CM OS の管理インターフェイスまたは Cisco Prime Collaboration Deployment（PCD）のアップグレード タスクを使用して、中間リリースに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在のリリースへの移行を実行します。

次の表で開始リリースを検索し、それを使用して、アップグレードおよび移行プロセスの手順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、次の手順のリンクを使用して、そのリリースのマニュアルを参照してください。

開始リリースがリストされていない場合は、複数の中間リリースへのアップグレードが必要になることがあります。https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/compat/15_x/cucm_b_compatibility-matrix-cucm-imp-15x.html にある「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」を参照してください。

表 *13 :* レガシーリリースから *Unified CM* および *IMP and Presence Service* リリース *15* へのアップグレード

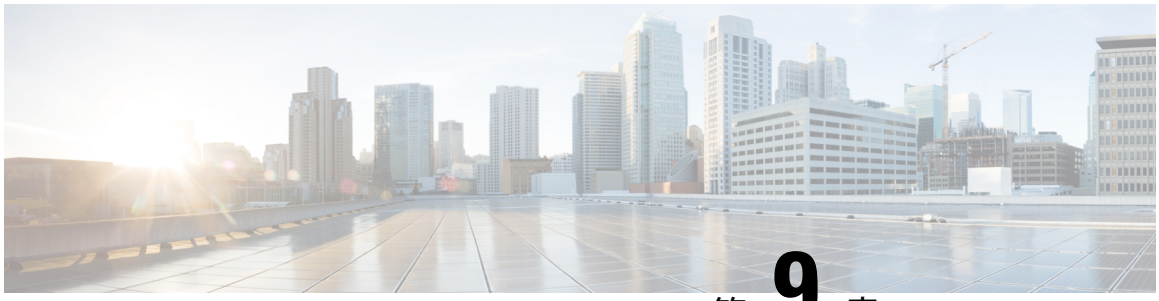
インストールされているバージョン (Installed Version)	仮想マシンでのこのバージョンへの移行
7.0(1) 以前	移行はできません。最初から最新リリースに再構築することをお勧めします。
8.0(1) および 9.1	PCD 12.6（PCD 14 または PCD 15 ではない）を使用して、バージョン 12.5 に直接移行します。可能なさまざまな移行オプションについては、このガイドの最初の章を参照してください。

手順

ステップ 1 中間リリースのアップグレードマニュアルを参照し、手順に従ってシステムをアップグレードします。

- Unified Communications Manager のアップグレードマニュアルについては、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) アップグレードのマニュアルについては、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 http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.htmlにある『*Cisco Prime Collaboration Deployment Administration Guide*』を参照し、現在のリリースへの PCD 移行を実行する手順に従ってください。



第 9 章

トラブルシューティング

アップグレードの失敗後のログファイルのダンプ

アップグレードUnified Communications ManagerまたはでIM and Presence Service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接続します。VM の設定を編集し、ログをダンプするファイル名を添付します。

（注） アップグレードの失敗によってシステムが動作を停止し、ログをダンプするように求められた場合は、「**Yes**」と応答してから続行する前に空のファイルを添付する必要があります。

ステップ 2 VM コンソールに戻り、ログをシリアル ポートにダンプします。

ステップ 3 プロセスが完了したら、**[インベントリ（Inventory）] > [データストアおよびデータストア クラスタ（Datastores and Datastore Clusters）]** 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 [**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 (Download)**] を選択し、ファイルを保存する場所を PC 上で選択します。

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より大きい場合は、PCにファイルを解凍し、仮想マシンの設定を編集してシリアルポートを削除します。
- ファイルサイズが0の場合は、次の手順に進みます。

ステップ 8 ファイル サイズがゼロの場合は、次の手順に従います。

a) 仮想マシンの電源をオフにします。
b) ログ出力用の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) [**Options**] タブで、[**Boot Options**] を選択し、[**Force bios Setup**] を有効にします。
e) 仮想マシンの電源をオンにして、BIOS にブートするまで待機します。
f) BIOS で、最初のブートデバイスとしてハードドライブを選択し、保存して終了します。システムはハードドライブを起動し、アップグレードが失敗したポイントに戻ります。障害通知が表示されます。
g) **[Yes]**を入力すると、ログの内容がファイルにダンプされます。
h) ファイルに移動して、7つの Zip を使用してファイルを開きます。

ステップ 9 ファイル サイズが 0 より大きい場合は、ファイルを PC 上に抽出し、仮想マシンの設定を編集して、シリアル ポートを削除します。

Unified Communications Manager のアップグレードに関するトラブルシューティング

ここでは、アップグレードのUnified Communications Managerトラブルシューティングについて説明します。

アップグレード失敗

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、サブスクライバ ノードのアップグレードに失敗します。または、アップグレード サイクル中に、クラスタのサブスクライバ ノードの 1 つがアップグレードに失敗します。

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、アップグレードの失敗の原因と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てから、サブスクライバ ノードのサーバ メモリおよびCPU 使用率が高すぎないかを確認してください。サブスクライバ ノードを再度アップグレードします。
- Unified Communications Managerパブリッシャ ノードのアクティブ パーティションで、サーバにインストールされている最新バージョンのソフトウェアが実行されていることを確認

します。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 ノードで更新インストールを実行します。サブスクライバ ノードを再インストールする場合は、『Cisco Unified Communications Manager アドミニストレーション ガイド』の手順に従って、Cisco Unified CM の管理からサーバを削除し、そのサーバを再度追加する必要があります。

クラスタまたは単一ノードのアップグレードの再試行

スイッチのバージョンを実行せずにアップグレードを再試行する場合、または以前のアップグレードで再起動する場合は、再試行する前にノードを再起動します。

再起動はアップグレードの成功/失敗/キャンセルのケースに含まれる

問題：以下の段階で再起動しなかった場合、アップグレードが失敗したり障害が発生したりする可能性があります。

解決策：次のシナリオでは、再起動が必要です。

1. 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）は、成功または失敗します。
   - L2 アップグレードが失敗した場合、再起動が必要になるのは、アップグレードが再度必要になった場合のみです。
   - L2 アップグレードが成功した後、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、まずノードを再起動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、自動再起動が実行されます（アップグレード ステータスが失敗の場合は、アップグレードをキャンセルしてノードを再起動します）。
2. バージョンの切り替えが失敗した場合は、サービス マネージャや機能に影響を与える可能性のあるその他のサービスが停止または中断する可能性があるため、サーバーを再起動してからさらにアクションを実行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した場合、IM&P/ UCM サーバーをリブートしてから、もう一度アップグレードを実行してください。

簡易アップグレードの問題のトラブルシューティング

クラスタの一部のノードでのダウンロードエラー

問題: 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が、簡素化されたアップグレードを実行しています。

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。ロケーションが無効であるか、クレデンシャルが間違っていると、障害が発生する可能性があります。[パブリッシャからのクレデンシャルのダウンロード] オプションを使用している場合は、障害が発生したノードの設定が正しいことを確認します。

確認するには、次のいずれかを実行します。

- ユーザインターフェイス: 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どうかを確認します。このチェックボックスをオンにすると、設定が正しいことを示します。チェックボックスがオフになっている場合は、チェックボックスをオンにして [**Next**] をクリックし、設定を保存してから [**Cancel**] をクリックして、[**Install/Upgrade**] ページを終了します。
- CLI:**ユーティリティシステムの upgrade initiate**コマンドを使用して、「use download Credentials from パブリッシャ (yes/no)」が「yes」に設定されていることを確認します。[はい(yes)] に設定されている場合は、設定が正しいことを示します。そうでない場合は、[はい(yes)] に設定し、[q] を選択して、「q」を選択してから、クリーン出口のために**ユーティリティシステムの upgrade cancel**コマンドを実行します。

（注） **[パブリッシャからのダウンロード ログイン情報を使用する（Use download credentials from Publisher）]** が選択されておらず、サブスクライバがパブリッシャの同じダウンロードログイン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。サブスクライバがパブリッシャのダウンロードログイン情報を使用するには、各サブスクライバに移動し、**[パブリッシャからのダウンロード ログイン情報を使用する（Use download credential from Publisher）]** オプションを選択する必要があります。

クラスタの一部のノードでのダウンロードまたはインストールの失敗

問題: 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し、簡素化されたアップグレードを実行しています。

解決策: CLI を使用して、CLI を使用して [**Install/Upgrade cluster**] 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**ユーティリティの system upgrade status**コマンドを実行して、これらの障害が発生したノードでアップグレードまたはインストール操作がまだ進行中でないことを確認します。「Unified Communications Manager のアップグレードのトラブルシューティング」の項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って、アップグレードを続行します。

（注） 簡略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フェーズで失敗すると、次のようになります。

- ユーザインターフェイス: [**クラスタのインストール/アップグレード**] ページには、失敗したノードを特定するために各ノードのステータスが表示されます ([キャンセル (cancel)] をクリックするまで)。
- CLI:**ユーティリティシステムアップグレードクラスタの開始**または起動**システムアップグレードクラスタのステータス**には、コマンド**ユーティリティ 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識別するための各ノードのステータスが表示されます。

クラスタの一部のノードでのスイッチのバージョンまたはリブートの失敗

問題: クラスタの一部のノードでスイッチのバージョンまたは再起動に失敗し、簡素化されたアップグレードを実行しています。

解決策: ユーザインターフェイスを使用して、[**Restart/Switch-Version cluster**] ページを開き、障害が発生したノードを特定します。問題(ネットワーク/証明書の問題など) を修正し、スイッチのバージョンを再試行するか、または障害が発生したノードで再起動するには、[**Restart/Switch-version cluster**] ページで完了したノードをスキップします。

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/電源再投入されましたが、クラスタアップグレードステータスが表示されません

問題: クラスタUnified Communications Managerのアップグレード中にパブリッシャがリブートまたは電源が再投入され、クラスタのアップグレードステータスが表示されませんでした。

解決策: Unified Communications Managerパブリッシャはクラスタのアップグレード操作を制御します。アップグレード中は、再起動または電源の再投入を行わないでください。これを実行すると、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パブリッシャは他のノードへの指示を提供できず、アップグレードの失敗が発生します。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 CPU の高アラート

問題: クラスタのアップグレード中に CPU アラートが大量に受信されました

解決策: サーバの使用率が最も少ない状態でクラスタ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 とディスクに負荷がかかり、CPU アラートが発生する可能性があります。

クラスタのアップグレードが失敗した後のクラスタアップグレードの再試行

問題: クラスタのアップグレードに失敗した後にクラスタのアップグレードを再試行するにはどうすればよいですか。

解決策: 最初に、クラスタのアップグレードをキャンセルします。アップグレードが失敗した場合は、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推奨します。

SSL エラーによるダウンロードの失敗

問題: SSL エラーが原因で、いくつかのノードノードでダウンロードに失敗しました。

解決策: クラスタのノード間で SSL 信頼が設定されていることを確認します。

クラスタノードのスイッチバージョンまたはリブートは、変更されたバッチに従って発生しませんでした

問題: クラスタノードのスイッチバージョンまたはリブートが、変更されたバッチに従って発生しませんでした。

解決策: クラスタのリブートまたはバージョン切り替えを開始する前に、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は保存されません

問題: スキップのチェックボックスの選択は保存されません。

解決策: [スキップ (skip)] オプションは、再起動またはバージョン切り替え中にノードを除外するために使用されます。この選択は保存されません。毎回オプションを選択する必要があります。

クラスタのアップグレードまたは単一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単一ノードのアップグレードを再試行できません。

解決策: CLI を使用して、コマンド**ユーティリティ system upgrade cluster cancel**コマンドを実行して、クラスタアップグレードのキャンセルを実行します。また、CLIを使用して、Unified Communications Manager**ユーティリティシステムの upgrade cancel**コマンドを実行して、パブリッシャで単一ノードのキャンセルを実行します。

ディスク領域不足によるアップグレードの失敗

問題 共通パーティションが一杯であるというエラーが発生し、Unified Communications Manager のアップグレードに失敗します。

解決法 通常、共通パーティション領域として少なくとも 25GB 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）や保留音（MOH）ファイルがある場合、または多数のロケールファイルがインストールされている場合は、展開においてさらに多くの領域が必要となることがあります。追加のディスク領域を作成するには、次の1つ以上の作業を実行します。

- Cisco Log Partition Monitoring Tool を使用して、基準値の上限と下限を調整し、トレースの削減と不要ログ ファイルの削除を行います。下限値を 30、上限値を 40 に調整することをお勧めします。トレースの早すぎるパージを避けるために、アップグレード後、基準値の上限と下限を元の値に戻す必要があります。基準値のデフォルトの上限は 85 です。基準

値のデフォルトの下限は 80 です。Cisco Log Partition Monitoring Tool の使用方法については、『Cisco Unified Real-Time Monitoring Tool Administration Guide』を参照してください。

- 仮想環境に追加の空きディスク領域がある場合は、vDisk のサイズを拡大するためにディスクの拡張 COP ファイル（ciscocm.vmware-disk-size-reallocation-<latest_version>.cop.sgn）を使用します。先に進む前に、この COP ファイルに関する 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 ファイルを使用すると、システムを再構築することなく、共通パーティションの非アクティブ側を削除して使用可能なディスク領域を増やすことができます。先に進む前に、この COP ファイルに関する Readme ファイルを確認してください。
- TFTP ディレクトリから古いまたは未使用のファームウェア ファイルを手動で削除します。OS 管理インターフェイスの [TFTPファイルの管理（TFTP File Management）] ページを使用してこれらのファイルを削除するか、コマンドライン インターフェイスで `file list tftp` と `file delete tftp` コマンドを使用できます。

Cisco.com から cops ファイルおよび readme ファイルを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 Version 10.0] > [Unified Communications Manager/CallManager/Cisco Unity Connection ユーティリティ（Unified Communications Manager/CallManager/Cisco Unity Connection Utilities）]** に移動してください。

失敗したアップグレードの再開

システムでエラーが検出され、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、次のプロセスに従います。

（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起動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。

ISO ファイルのダウンロードは、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ると保持されます。

ステップ 2 システムの問題を修正します。

ステップ 3 アップグレードを再開する準備ができたら、ユーティリティシステムの `upgrade initiate` CLI コマンドを実行し、[`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 コントロール グループの権限の縮小

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、一部の既存アクセス コントロール グループの権限レベルが予期せず縮小します。

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。「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に、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、一部の既存アクセス コントロール グループの現在の権限レベルが縮小することがあります。

アクセス権の削減、Cisco Unified CM のアップグレード中、たとえば、不注意にまたがることがあります。アップグレード バージョンで、「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 グループがサポートされている場合は、アップグレード中に全ユーザがそのユーザ グループに自動的に追加されます。この権限問題を解決するために、Standard RealTimeAndTrace Collection ユーザ グループからユーザを削除することができます。

電話機の設定の消失

Unified Communications Manager のインストール後の短期間、または別の製品バージョンにアップグレードして切り替えた後の短期間、電話機ユーザによって行われた変更が失われることがあります。電話機ユーザが行う設定には、コール転送やメッセージ待機インジケータの設定などがあります。この状況は、アップグレードウィンドウ中に設定が変更された場合に発生する可能性があります。インストール後またはアップグレード後に Unified Communications Manager によってデータベースが同期されると、電話機ユーザによる設定の変更が上書きされる場合があります。シスコでは、アップグレード中に設定を変更しないことを推奨しています。

Unified Communications Manager パブリッシャ ノードのアップグレード後の障害

問題 アップグレードに成功し、クラスタでは新しいリリースが実行されていますが、その後 Unified Communications Manager パブリッシャ ノードで障害が発生します。

解決法 次のいずれかを実行します。

- DRS バックアップUnified Communications Managerファイルを使用したパブリッシャノードの復元
- 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障害

問題 アップグレードに成功し、クラスタでは新しいリリースが実行されていますが、その後 Unified Communications Manager サブスクライバ ノードで障害が発生します。

解決法 次のいずれかを実行します。

- Unified Communications Managerサブスクライバノードを復元するには、DRS バックアップ ファイルを使用します。
- DRS バックアップ ファイルがない場合は、サブスクライバ ノードのアップグレードを再び実行します。再インストール前に Unified Communications Manager パブリッシャ ノードのサーバ ページからサブスクライバ ノードを削除する必要はありません。

IM and Presence のアップグレードに関するトラブルシューティング

このセクションでは、IM and Presence Service Service 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示します。

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に失敗

問題 とUnified Communications ManagerIM 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すると、IM and Presence Serviceデータベースパブリッシャノードのアップグレードが失敗します。

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応じて異なります。

- IM and Presence Service データベース パブリッシャ ノードを新しいバージョンに切り替えた後に障害が発生した場合は、すべてのノードをスイッチバックし、アップグレードを再度実行する必要があります。以下に示す順序でタスクを実行します。
  - Unified Communications Manager パブリッシャ ノードをスイッチバックします
  - サブスクライバノードのUnified Communications Managerスイッチバック
  - データベースパブリッシャノードIM and Presence Serviceのスイッチバック
  - Unified Communications Manager パブリッシャ ノードを再度アップグレードします
  - Unified Communications Manager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る
  - Unified Communications Manager サブスクライバ ノードを再度アップグレードします

- 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ます

IM and Presence サブスクライバ ノードのアップグレードに失敗

問題 とUnified Communications ManagerIM 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すると、IM and Presence Service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 実行するアクションは、障害が発生したポイントに応じて異なります。

- IM and Presence Service サブスクライバ ノードを新しいバージョンに切り替えた後にノードのアップグレードに失敗した場合は、以下のタスクを記載されている順序で実行する必要があります。
  - Unified Communications Managerパブリッシャノードを以前のソフトウェアバージョンに戻す
  - 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ます
  - 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 バージョンに切り替えます
  - IM and Presence Service 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ます
  - パブリッシャノードUnified Communications Managerのパブリッシュを新しい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 ノードを新しいソフトウェア バージョンに切り替えます
  - IM and Presence Service サブスクライバ ノードでアップグレードを再度実行します。

IM and Presence ユーザ電話のプレゼンスの問題

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 サービスの開始時に、ユーザの IM and Presence 電話のプレゼンスは更新に時間がかかったり、遅くなったりします。

解決法 Cisco SIP Proxy サービスを再起動する必要があります。Cisco Unified IM and Presence Serviceアビリティで、**[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。

Presence ユーザによるアベイラビリティの取得で問題が発生する

問題 IM and Presence Service サーバのアップグレード後、アクティブ化されたすべての機能サービスとネットワーク サービスが開始されるときに、プレゼンス アベイラビリティの不整合が発生します。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のアベイラビリティ情報の取得で問題が発生します。

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る場合に発生します。ユーザを割り当て解除してから、再度割り当てる必要があります。

Cisco SIP Proxy サービスのリアルタイム モニタリング ツールのアラート

問題 IM and Presence Service サーバのアップグレード後、アクティブ化されたすべての機能サービスとネットワーク サービスが開始されるときに、リアルタイム監視ツールで Cisco SIP Proxy サービスに対して CoreDumpFileFound アラートが生成されます。

解決法 Cisco SIP Proxy サービスを再起動する必要があります。Cisco Unified IM and Presence Serviceアビリティで、**[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 サーバのアップグレード ファイルが見つからない

問題 リモート サーバのアップグレード 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 サーバ上に存在する場合は、指定するディレクトリ パスの先頭にフォワードスラッシュを付加する必要があります。たとえば、アップグレード ファイルが patches ディレクトリに存在する場合は、**/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 サーバ上に存在する場合は、システム管理者に正しいディレクトリ 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ない

問題 アップグレードファイルのチェックサム値と、Cisco.com に示されるチェックサムが一致しません。

解決法 アップグレード ファイルが本物の整合性のあるファイルであると保証するには、2 つのチェックサム値が一致している必要があります。チェックサム値が一致しない場合、Cisco.com から新しいバージョンのファイルをダウンロードして、再度アップグレードを試みてください。

データベース レプリケーションが完了しなかった

問題 アップグレード後、データベース レ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 アップグレードを完了し、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 レプリケーションが自動的に実行されます。この処理中に、サブスクライバ ノードのコア サービスは起動しません。大規模な展開のデータベース レプリケーションの場合、完了するまで数時間かかる可能性があります。数時間後に **utils dbreplication runtimestate** コマンドを実行しても、データベース レプリケーションが完了していないと示される場合は、データベース レ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、次のコマンドを実行します。`utils dbreplication reset all`

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 バージョンと一致しない

問題 IM and Presence Service サーバで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 イメージを選択できません。次のエラーが報告されます：名前から取得されたバージョンは、パブリッシャのアクティブなバージョンとも非アクティブなバージョンとも一致しません。（`The version obtained from the name does not match the active or inactive version of the publisher.`）

解決法 バージョンの一致ルールに適合していません。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バージョン (アップグレードする最初IM and Presence Serviceのノード) は、 Unified Communications Manager 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バージョンの最初の2つの番号と一致している必要があります。Unified Communications Manager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がアクティブまたは非アクティブである可能性があります。たとえば、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 と Presence Service ノードをアップグレードするときは、シーケンス ルールに従ってください。
- 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 バージョンが、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 バージョンの 5 つの番号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 ノードまたは IM and Presence Service データベース パブリッシャ ノードであることを確認します。または、別のソフトウェア アップグレードのイメージを選択します。

Cisco IM and Presence ノードのバージョンの切り替えに失敗する

問題 Cisco IM and Presence ノードのバージョンの切り替えに失敗します。次のエラーが報告されます。バージョンが一致しません（バージョンの不一致）。パブリッシャのバージョンを切り替えて、再試行してください。（`Please switch versions on the publisher and try again.`）

解決法 バージョンの一致ルールに適合していません。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バージョン (アップグレードする最初IM and Presence Serviceのノード) は、 Unified Communications Manager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バージョンの最初の2つの番号と一致している必要があります。たとえば、IM and Presence Service 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。
- 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 バージョンが、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 バージョンの 5 つの番号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、最初にスイッチするノードがパブリッシャノードUnified Communications ManagerまたはIM and Presence Serviceデータベースパブリッシャノードのいずれかであることを確認します。

アップグレードのキャンセルまたは失敗

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に失敗した場合は、IM and Presence Service サーバをリブートしてから、もう一度アップグレードを実行してください。

ディレクトリが検出されたが、有効なオプションまたはアップグレードがない

問題 IM and Presence Serviceアップグレード中は、アップグレードIM and Presence Serviceパスとファイルが有効であっても、サーバは次のエラーメッセージを生成します。

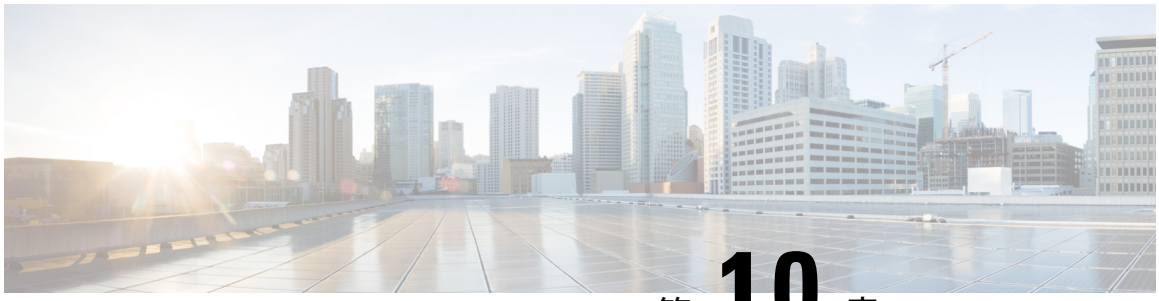
指定されたディレクトリが見つかり、検索されましたが、有効なオプションまたはアップグレードがありませんでした。（`The directory was located and searched but no valid options or upgrades were available.`）マシンはダウングレードできないことに注意してください。以前のアップグレードファイルとオプションファイルは無視されます。（`Note, a machine cannot be downgraded so option and upgrade files for previous releases were ignored.`）

解決法 Upgrade manager は、とIM and Presence ServiceUnified Communications Managerの間の接続を確認し、アップグレード中にバージョンを検証します。これに失敗すると、アップグレード パスとファイルが有効であっても、IM and Presence Service サーバによってエラー メッセージが生成されます。Cisco Unified CM IM and Presence 管理システムトラブルシュータなどのツールを使用して、アップグレードを続行する前に IM and Presence Service と Unified Communications Manager の間に接続があることを確認します。

共通パーティションの完全アップグレードの失敗

問題 共通パーティションがいっぱいであるというエラーが発生し、IM and Presence Service のアップグレードに失敗します。

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。COP ファイルは、共通パーティションをクリーンアップして、その後のアップグレードが通常どおりに進行するようにします。



第 10 章

よく寄せられる質問

よく寄せられる質問

Unified Communications Manager のリリースからアップグレードするか、また IM and Presence Service は新しいリリースとは異なる要件を持つ仮想環境の要件を満たしています。どうすればよいのですか。

次の情報を使用して、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後、手順に仮想マシン設定タスク （79 ページ）ついては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 ファイルには、仮想マシン設定用の一連の定義済みテンプレートが用意されています。サポートされているキャパシティレベル、必要な OS/VM/SAN の配置などの項目について説明します。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いています。OVA ファイルの詳細については、https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/collaboration-virtualization-sizing.html の「Unified Communications 仮想化のサイジングに関するガイドライン」のトピックを検索してください。

項目	説明
VMware vSphere ESXi	リリースの互換性とサポート要件を満たすvSphere ESXiハイパーバイザ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は、正しいライセンスタイプで vSphere ESXi がインストールされていることも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りません。これらのライセンスの一部では、必要な VMware Api が有効になっていないためです。
VMware vCenter	VMware vCenter は、Business Edition 6000/7000 Unified Communications Managerアプライアンス IM and Presence Service 、または UCS テスト済みリファレンス構成ハードウェアで UC 上に展開する場合はオプションです。 VMware vCenterは、UC に UCS 仕様ベースおよびサードパーティ製のサーバ仕様ベースのハードウェアに導入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仕様	またはUnified Communications ManagerIM 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 の仮想ハードウェア仕様を変更する必要があるかどうかを確認します。 Unified Communications Manager または IM and Presence Service リリース 15 バージョンには、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 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。 アップグレード前に vRAM と vDisk の仕様を確認するには、リリース 15 のベース OVA の Readme を参照するか、QuoteCollab ツールを使用します。 その他の参考資料については、次を参照してください。 • 仮想マシン設定タスク （79 ページ） 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 バージョンを、vDisk が 110GB としてインストールされている新しい VMware にバックアップまたは復元します。ここでは、直接アップグレードが成功します。または、PCD 移行またはデータインポートタスクの移行を伴う新規インストールを使用して、Unified CM リリース 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。

.. www.cisco.com go virtualized-collaboration に移動して、仮想化環境の要件に関する詳細情報を確認できます。ここでは、次のことが可能です。

- Unified Communications ManagerおよびIM and Presence Serviceアプリケーションのリンクに従って、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」トピックを検索して、機能サポートとベストプラクティスに関する情報を検索します。

アップグレードの一環として別の VM サイズに移行したいと思います。VM 設定の仕様を編集できますか。

VM 設定の仕様を編集する前に、OVA ReadMe ファイルを確認して、アップグレードするリリースの特定の要件を確認してください。OVA ファイルには、仮想マシン設定用の一連の定義済みテンプレートが用意されています。サポートされているキャパシティレベル、必要な OS/VM/SAN の配置などの項目について説明します。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いています。

OVA ファイルの詳細については、.. www.cisco.com go virtualized-collaboration の「Unified Communications 仮想化のサイジングに関するガイドライン」のトピックを検索してください。

OVA ファイルを取得するには、「OVA テンプレートのダウンロードとインストール （82 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情報にアクセスし、変更Unified Communications Managerするアプリケーションがあります。アプリケーションは、 Unified Communications Managerアップグレード後も動作し続けますか。

AXL アプリケーションのアップグレードの詳細については、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。使用しているリリースでサポートされている AXL 操作のリストを表示するには、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。