



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 \(1 ページ\)](#)

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 (6 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 (6 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 (7 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
		<p>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。</p> <p>(注) COP ファイルを使用してアップグレードしようとする、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。</p> <p>(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。</p>
ステップ 5	TFTP パラメータのリセット (9 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 (9 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 (10 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 (11 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 (11 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 (13 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 (13 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 (14 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 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 (14 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 (15 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 (16 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 (18 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 (19 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 (19 ページ)	アップグレード前に Manager Assistant を導入していて、クラス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 (20 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 (21 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 (21 ページ)	アップグレードプロセスを開始する前に IM and Presence Service 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 (22 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
		<p>確立されるようにするには、CER サービスを再起動します。</p> <p>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。</p>

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](#)

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 Manager 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 Manager Administration > 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一値、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ペ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 サブスクリバ 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 サブスクリバ 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、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 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、
- CiscoRTMTPlugin.zip ファイルを解凍します。
 - 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、
- CiscoRTMTPlugin.zip ファイルを解凍します。
 - 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。
 - 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 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が。

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 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する前に Cisco Emergency Responder 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。
-

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。