アップグレード後のタスク

アップグレード後のタスクフロー

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

手順

	コマンドまたはアクション	目的
ステップ 1	CTL ファイルの更新 （6 ページ）	クラスタが混合モードの場合、CTL ファイルを手動で更新します。 電話をリセットして最新の更新を反映します。 （注） Unified Communications Manager の移行の場合は、これをスキップできます。
ステップ 2	シリアルポートを削除する （6 ページ）	アップグレード前のタスクで追加したシリアルポートを削除して、VM のパフォーマンスに影響を与えないようにします。 すべてのノードに対してこの手順を実行します。
ステップ 3	エクステンションモビリティの再起動 （6 ページ）	アップグレード前タスクの一部として Cisco Extension Mobility を無効にした場合、再起動できます。
ステップ 4	アップグレード後の COP を実行します。	アップグレード後の COP は、システムの安定性を確認するために一連のテストを実行します。 これらのテストで

	コマンドまたはアクション	目的
		は、違いを特定するためにアップグレード前とアップグレード後の設定を比較します。この表のすべての手順を完了したら、post-upgrade COP ファイルを再実行して、COP レポートを確認します。 （注） COP ファイルを使用してアップグレードしようとすると、システムにインストールされているファイル数が表示されます。アップグレードが完了すると、COP ファイルのリストは以前のバージョンと一致しなくなります。以前のファイルが必要な場合は、COP ファイルを手動でインストールする必要があります。 （注） CLI コマンド である show risdb query cti を実行すると、ノードに登録されたデバイスの詳細が表示されます。デバイスは、エントリを作成するために、そのノードで少なくとも 1 回登録されている必要があります。たとえば、サブスクライブ 2 で登録されたデバイスが登録解除され、サブスクライブ 1 に移動された場合、サブスクライブ 2 でこのコマンドを実行すると、未登録として表示されます。
ステップ 5	TFTP パラメータのリセット （9 ページ）	アップグレードプロセス中に変更される TFTP パラメータをリセットします。
ステップ 6	エンタープライズパラメータの復元（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 ノードのエンタープライズパラメータ設定を復元します。
ステップ 7	最高水準点と最低水準点のリセット（10 ページ）	トレースの時期を過ぎた消去を避けるために、この手順を使用して高ウォーターマークと低ウォーターマークを元の値に復元します。

	コマンドまたはアクション	目的
		PCD 移行の場合は、このタスクをスキップできます。
ステップ 8	VMware Tools の更新 （10 ページ）	アップグレードが完了したら、VMWare Tools を更新する必要があります。 すべてのノードに対してこの手順を実行します。
ステップ 9	ロケールのインストール （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る米国英語を除き、使用中のロケールを再インストールする必要があります。 すべてのノードに対してこの手順を実行します。
ステップ 10	データベースリプリケーションタイムアウトを復元する （12 ページ）	アップグレードを開始する前にデータベース複製のタイムアウト値を増やした場合、この手順を使用します。 Unified Communications Manager ノードのみでこの手順を実行します。
ステップ 11	登録済みデバイス数の確認 （13 ページ）	アップグレードが完了した後、この手順を使用して、Unified CM ノード上のエンドポイントとリソースを確認します。
ステップ 12	割り当てられたユーザを確認する （14 ページ）	アップグレードが完了した後、この手順で IM and Presence Service ノードに割り当てられたユーザーの数を確認します。
ステップ 13	テスト機能 （14 ページ）	アップグレード後に電話の機能が正常に動作していることを確認します。
ステップ 14	RTMT のアップグレード （15 ページ）	Cisco Unified Real Time Monitoring Tool (RTMT) を使用する場合、新しいソフトウェアバージョンにアップグレードします。
ステップ 15	TFTP サーバファイルの管理 （16 ページ）	これはオプションです。 この手順を実行して、電話の呼び出し音、コールバックトーン、および背景を TFTP サーバーにアップロードして、Unified CM ノードで使用できるようにします。

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

ソフトウェア バージョンを切り替える

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

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

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

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

始める前に

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

バージョンの切り替えについて で情報を確認します。

手順

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

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

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

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

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

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

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

CTL ファイルの更新

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

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

手順

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

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

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

ステップ 3 電話をリセットして更新を反映します。

シリアルポートを削除する

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

手順

ステップ 1 仮想マシンの電源をオフにします。

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

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

エクステンション モビリティの再起動

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

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

手順

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

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

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

ステップ 4 **再起動（Restart）**をクリックします。

アップグレードの準備 COP ファイルの実行 (アップグレード後)

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

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

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

手順

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

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

ステップ 2 アップグレード後のシステムの状態を確認します。

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

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

ステップ 4 RTMT からレポートを表示するには

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

次のタスク

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

TFTP パラメータのリセット

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

手順

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

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

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

ステップ 4 [詳細設定（Advanced）]をクリックします。

ステップ 5 **[保存（Save）]** をクリックします。

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

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

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

エンタープライズパラメータの復元

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

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

始める前に

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

手順

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

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

ステップ 3 **[保存（Save）]** をクリックします。

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

最高水準点と最低水準点のリセット

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

手順

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

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

ステップ 3 [次へ（Next）]を選択します。

ステップ 4 スライダの値を 80 に調整します。

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

ステップ 6 [次へ（Next）]を選択します。

ステップ 7 スライダの値を 85 に調整します。

VMware Tools の更新

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

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

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

ロケールのインストール

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

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

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

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

手順

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

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

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

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

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

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

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

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

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

ステップ 6 [次へ（Next）]をクリックします。

ステップ 7 サーバにロケールをダウンロードしてインストールします。

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

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

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

データベースリプリケーション タイムアウトを復元する

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

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

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

手順

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

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

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

登録済みデバイス数の確認

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

手順

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

ステップ 2 登録済みデバイスの数を記録します。

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

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

割り当てられたユーザを確認する

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

手順

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

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

テスト機能

アップグレード後、以下のタスクを実行します。

- post-upgrade COP を実行します。

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

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

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

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

RTMT のアップグレード

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

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

始める前に

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

手順

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

ステップ 2 **[検索（Find）]** をクリックします。

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

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

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

ステップ 5 Windows 版をインストールするには、

a) CiscoRTMTPlugin.zip ファイルを解凍します。

b) `run.bat` ファイルをダブルクリックします。

ステップ 6 Linux 版をインストールするには、

a) CiscoRTMTPlugin.zip ファイルを解凍します。

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

c) `run.sh` ファイルをダブルクリックします。

TFTP サーバファイルの管理

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

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

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

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

手順

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

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

ステップ 2 ファイルをアップロードするには、次の手順に従います:

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

[ファイルのアップロード] ダイアログボックスが開きます。

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

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

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

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

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

ステップ 3 ファイルを削除するには、次の手順に従います。

a) 削除するファイルの隣にあるチェックボックスを選択します。

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

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

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

カスタム ログオン メッセージのセットアップ

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

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

手順

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

[ログオンメッセージのカスタマイズ] ウィンドウが表示されます。

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

（注） 10kB を超えるファイルをアップロードすることはできません。

カスタマイズしたログオンメッセージが表示されます。

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

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

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

IPSec ポリシーを設定する

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

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

手順

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

ステップ 2 [新規追加] をクリックします。

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

ステップ 4 **[保存]** をクリックします。

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

新しい Manager Assistant の役割を指定する

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

手順

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

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

IM および Presence サービス データ移行の確認

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

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

説明: 移行されたサービス プロファイル番号 x

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

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

手順

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

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

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

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

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

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

次のタスク

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

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

プレゼンス冗長グループの高可用性を有効にする

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

始める前に

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

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

手順

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

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

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

ステップ 4 **[保存（Save）]** をクリックします。

ステップ 5 各プレゼンス冗長性グループでこの手順を繰り返します。

IM および Presence 同期エージェントを再起動する

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

手順

ステップ 1 Cisco Unified Serviceability インターフェイスで、**[ツール（Tools）]** > **[コントロールセンター - ネットワークサービス（Control Center - Network Services）]** の順に選択します。

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

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

例

（注） Cisco Intercluster Sync Agent が初期同期を完了した後、手動で新しい Tomcat 証明書を Unified Communications Managerにロードします。 これにより、同期が失敗することがなくなります。

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

Cisco Emergency Responder サービスを再起動する

手順

アップグレードを開始する前に Cisco Emergency Responder サービスを停止している場合は、今すぐ再起動してください。

ステップ 1 Cisco Emergency Responder 保守インタフェースから、[**ツール**] >[**コントロールセンター]** を選択します。

ステップ 2 [**Cisco Emergency Responder**] を選択し、[**再起動**] をクリックします。

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。