アップグレード後のタスク（手動プロセス）

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

（注） アップグレード元のリリースが 10.x 以降のアップグレードパスでは、アップグレード準備 COP ファイルを実行してその解決要求を完了することが、これらのアップグレード後のタスクの代わりとなります。COP ファイルは、9.x からアップグレードするための機能が制限されており、9.x より前のリリースからアップグレードする場合にも機能しません。

- 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と移行の方法については、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	シリアル ポートの削除 （4 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 のパフォーマンスが影響を受けないようにします。 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 2	エクステンション モビリティの再起動 （5 ページ）	アップグレード前のタスクの一部として Cisco Extension Mobility を無効にした場合は、ここで再起動できます。

	コマンドまたはアクション	目的
ステップ 3	TFTP サービスの再起動 （5 ページ）	この手順を使用して、Unified CM ノードで TFTP サービスを再起動します。
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 によって一連のテストが実行され、システムの安定性が検証されます。これらのテストでは、アップグレード前後の設定を比較して相違点を特定します。この表の手順をすべて完了したら、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） 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。ここに表示されるのは、そのノードに少なくとも 1 回は登録されたことがあるデバイスです。たとえば、デバイスを subscribe 2 に登録した後、登録解除して subscribe 1 に移動した場合、このコマンドを subscribe 2 で実行すると、デバイスは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 （7 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 （8 ページ）	IM and Presence Service ノードで、アップグレードプロセス中に上書きされた可能性のあるエンタープライズ パラメータ設定を復元します。
ステップ 7	基準値の上限および下限のリセット （8 ページ）	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。 PCD 移行で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 （9 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。

	コマンドまたはアクション	目的
		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 （10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 （12 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大きくしていた場合には、この手順を使用します。 この手順は Unified Communications Manager でのみ実行します。
ステップ 11	登録済みのデバイス数の確認 （12 ページ）	この手順を使用して、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します。
ステップ 12	割り当て済みのユーザを確認する （13 ページ）	この手順を使用して、アップグレードの完了後にインスタント メッセージングとプレゼンス ノードに割り当てられているユーザ数を確認します。
ステップ 13	機能のテスト （13 ページ）	アップグレード後に電話機の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 （14 ページ）	Cisco Unified Real Time Monitoring Tool（RTMT）を使用する場合は、新しいソフトウェアの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 （15 ページ）	これはオプションです。電話の呼び出し音、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 Unfiied CM ノードで使用できるようにするには、この手順を使用します。
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 （16 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。

	コマンドまたはアクション	目的
ステップ 17	IPsec ポリシーの設定 （17 ページ）	リリース 6.1(5) からの PCD 移行を実行している場合、IPSec ポリシーは新しいリリースに移行されないため、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 （18 ページ）	アップグレード前に Manager Assistant が展開されていて、ユーザが InterCluster Peer-User または Admin-CUMA ロールに割り当てられていた場合、これらのロールは現在のリリースに存在しないため、ユーザをロールに割り当て直す必要があります。
ステップ 19	IM and Presence Service のデータ移行の検証 （18 ページ）	アップグレードまたは Cisco Unified Presence リリース 8.x から IM and Presence Service リリースへの移行を実行した場合にのみ、この手順を使用します。
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 （19 ページ）	アップグレードプロセスの前にインスタント メッセージングとプレゼンス サービスの高可用性を無効にした場合は、この手順を使用して有効に戻します。
ステップ 21	IM and Presence Sync Agent の再起動 （20 ページ）	アップグレードプロセスの開始前にインスタントメッセージングとプレゼンス 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。
ステップ 22	CER サービスの再起動 （21 ページ）	Unified Communications Manager のアップグレード後に AXL 接続を確立するために、CER サービスを再起動します。 また、Unified CM Publisher ノードの AXL 変更通知切り替えを再起動する必要があります。

シリアル ポートの削除

アップグレード前の作業では、アップグレード ログを取得するため、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が正常に完了した後は、仮想マシンのパフォーマンスに影響が及ばないように、このシリアル 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タスクの一部として Cisco Extension Mobility を無効にした場合は、この手順を使用して、Unified Communications Manager ノードで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 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。

TFTP サービスの再起動

アップグレードの完了後、次の手順を使用して、Unified Communications Manager ノードで TFTP 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 TFTP** 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）

アップグレードが完了したら、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、次の項目がチェックされます。

- 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複製のステータス
- データベースの健全性
- 最新 DRS バックアップのステータス
- サービス ステータス
- インストールされた COP およびロケール
- 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 バージョンと非アクティブ バージョン

（注） アップグレード後には、システムの正常性を検証するために、アップグレード準備 COP ファイルでアップグレード後のチェックを実行することを強く推奨します。

手順

ステップ 1 アップグレード準備 COP ファイルをダウンロードして、アップグレード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) 移行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) **アップグレード後のテストを実行するためのアップグレード COP ファイル**をダウンロードします（たとえば `ciscocm.postUpgradeCheck-00019.cop.sgn`。ただし、最新のファイルはファイル名とバージョンが異なっている場合があります）。

ステップ 2 アップグレード後のシステムの正常性をチェックします。

a) COP ファイルを実行します。
b) COP ファイルから返された問題を解決します。
c) COP ファイルからエラーが返されなくなるまで、これらの手順を繰り返します。

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を使い始めることができます。

TFTP パラメータのリセット

アップグレード プロセス中に、TFTP サービス パラメータの [**最大サービス数（Maximum Serving Count**）] は、増加したデバイス登録要求数を許可するように変更されます。アップグレードが完了した後、パラメータをリセットするには、こ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（Maximum Serving Count**）] を、アップブレードする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。

- 1500（シングル プロセッサ システムの場合）
- 3000（デュアル プロセッサ システムの場合）
- 3500（高性能 CPU 構成の専用 TFTP サーバの場合）

エンタープライズ パラメータの復元

いくつかのエンタープライズ パラメータは、Unified Communications Manager ノードと インスタント メッセージングとプレゼンス 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は、アップグレード中に Unified Communications Manager ノードの設定によって インスタント メッセージングとプレゼンス ノードの設定が上書きされます。インスタント メッセージングとプレゼンス ノードに固有のエンタープライズ パラメータは、アップグレード中も保持されます。

アップグレード プロセス中に上書きされた インスタント メッセージングとプレゼンス ノードの設定を再設定するには、こ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環として記録した設定へのアクセス権を持っ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、**[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 必要に応じて、エンタープライズパラメータのアップグレードと更新の前に存在した設定と現在の設定を比較します。

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）の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 **[アラート セントラル（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、**[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 に調節します。

ステップ 5 **[システム（System）]** タブで、**[LogPartitionHighWaterMarkExceeded]** を右クリックし、**[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 に調節します。

VMware ツールの更新

VMware ツールは、管理とパフォーマンスの最適化のためのユーティリティのセットです。システムでは、次の VMware ツールのいずれかが使用されます。

- ネイティブ VMware ツール (VMware によって提供されます)
- オープン VMware ツール (シスコが提供)
- リリース 11.5(x) よりも前のバージョンから Unified Communications Manager をアップグレードするには、ネイティブ VMware ツールのオプションを使用する必要があります。アップグレード後に VMware ツールを開くように変更できます。
- Unified Communications Manager リリース 11.5(1) 以降から（たとえば上位の SU に）アップグレードする場合は、システムでネイティブ VMware とオープン VMware ツールのどちらを使用するかを選択できます。
- 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。

手順

ステップ 1 コマンド **utils vmtools status** を実行して、VMware ツールが現在実行中であることを確認します。

ステップ 2 必要に応じて、目的の VMware ツール プラットフォームに切り替えます。そのためには、コマンド [**utils vmtools switch native**] または [**utils vmtools switch open**] を実行します。

ステップ 3 ネイティブ *VMware* ツールを使用する場合は、次のいずれかの操作を実行します。

- viClient を使用してツールの自動更新を開始します。

  （注） ESXI 6.5 VM ツールの更新には、設定パラメータを更新する前に VM の電源をオフにします。[設定の編集（Edit settings）] > [オプション（options）] > [詳細（Advanced）] > [全般（General）] > [設定パラメータ（Configuration parameters）] を選択し、次のパラメータを追加します。

  ```
  tools.hint.imageName=linux.iso
  ```

- VM の電源投入時に自動的にバージョンをチェックしてアップグレードするようにツールを設定します。

これらのオプションの設定方法については、VMware のドキュメントを参照してください。また、https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/

virtualization-software-requirements.html#vmtools で「VMware Tools」というトピックを検索すると、より詳しい情報を得ることができます。

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、この手順を使用します。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 インスタント メッセージングとプレゼンス 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。

ロケールは、Unified Communications Manager または インスタント メッセージングとプレゼンス ノードに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、アナンシエータ、およびゲートウェイ トーンを含む）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。
  - `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 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 およびインスタント メッセージングとプレゼンス 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 およびインスタント メッセージングとプレゼンス 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。インスタント メッセージングとプレゼンス 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）です。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*** 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。*[timeout]* には、データベース レプリケーションのタイムアウト値を秒単位で指定します。値を 300（5 分）に設定します。

登録済みのデバイス数の確認

アップグレードが完了後に、デバイス数を表示し、エンドポイントとリソースを確認するためには、リアルタイム モニタリング ツール（RTMT）を使用します。

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 サマリ（Device Summary）]** の順に選択します。

ステップ 2 次の登録済みのデバイス数を記録する。

項目	数
登録済みの電話機（Registered Phones）	
登録済みのゲートウェイ（Registered Gateways）	
登録済みのメディア リソース（Registered Media Resources）	
その他の登録済みのステーション デバイス（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のユーザ数と比較し、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。

  これにより一連のテストが実行され、システムが安定していることが確認されます。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。このリストの手順をすべて完了したら、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、電話機能を確認します。
  - ボイスメール
  - 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

- インスタント メッセージングとプレゼンス の次の機能をテストします。
  - 使用可能、使用不可、およびビジーなどの基本的なプレゼンスの状態
  - ファイルの送受信
  - 永続チャット、フェデレーテッド ユーザ、およびメッセージ アーカイブなどの拡張機能

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 Unified Communications Manager 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、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、以前のバージョンをアンインストール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　次のいずれかの操作を実行します。

- Microsoft Windows オペレーティング システムを実行しているコンピュータにツールをインストールするには、[**Cisco Unified Real-Time Monitoring Tool - Windows] の [ダウンロード（Download**）] リンクをクリックします。
- Linux オペレーティング システムを実行しているコンピュータにツールをインストールするには、[Cisco Unified Real-Time Monitoring Tool - Linux] の [**ダウンロード（Download**）] リンクをクリックします。

ステップ 4 優先ロケーションにインストール ファイルをダウンロードします。

ステップ 5 インストール ファイルを特定して実行します。
抽出プロセスが開始されます。

ステップ 6 RTMT のようこそウィンドウで、[**次へ（Next**）] をクリックします。

ステップ 7 アップグレードのインストール場所は変更できないため、[**次へ（Next**）] をクリックします。[セットアップ ステータス（Setup Status）] ウィンドウが表示されます。[キャンセル（Cancel）] をクリックしないでください。

ステップ 8 [**メンテナンス完了（Maintenance Complete**）] ウィンドウで、[**完了（Finish**）] をクリックします。

TFTP サーバ ファイルの管理

電話機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は、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（Upload File**）] 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に成功すると、[ステータス（Status）]領域にそのことが表示されます。

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。

サービスの再起動については、『*Cisco Unified Serviceability Administration Guide*』を参照してください。

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（Delete Selected**] 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。

[ログインメッセージのカスタマイズ（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 **[Upload File（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

リリース 6.1(5) から PCD の移行を実行している場合にのみ、この手順を使用します。リリース 6.1(5) からの IPSec ポリシーが新しいリリースに移行されていないため、PCD の移行が完了した後に、IPSec ポリシーを作り直す必要があります。

- 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

Cisco Unified Communications Manager Assistant 機能を使用するために以前のリリースが設定されていて、クラスタ間ピア ユーザ権限または Admin-CUMA 権限のいずれかを使用するためにアプリケーション ユーザを割り当てた場合にのみ、この手順を実行します。クラスタ間ピア ユーザ権限と Admin-CUMA 権限はリリース 10.0(1) 以降は廃止され、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権限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「ユーザの管理」の章を参照してください。

ステップ 2 インスタント メッセージングとプレゼンス 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 インスタント メッセージングとプレゼンス Service リリースにアップグレードすると、ユーザ プロファイルが Unified Communications Manager に移行されます。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。これにより一連のテストが実行され、システムが安定していることが確認されます。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 インスタント メッセージングとプレゼンス 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に対してハイ アベイラビリティをディセーブルにしている場合は、ここで、次の手順を使用してイネーブルにします。

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 インスタント メッセージングとプレゼンス 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 リストからインスタント メッセージングとプレゼンス ノードを選択し、**[移動（Go）]** をクリックします。

ステップ 3 **[IM 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 による最初の同期が完了したら、新しい Tomcat 証明書を手動で Unified Communications Manager にロードします。これにより、同期が失敗していないことが保証されます。

（注） アップグレード後のCOPを実行します。これにより一連のテストが実行され、システムが安定していることが確認されます。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。

CER サービスの再起動

手順

アップグレード プロセスの開始前に Cisco Emergency Responder 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。

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 Emergency Responder]** を選択し、[**再起動（Restart）**] をクリックします。