アップグレード前のタスク（手動プロセス）

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

（注） アップグレード前のリリースが 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前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。

アップグレード前の作業

アップグレードや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、特に記載がない限り、すべてのアップグレードと移行に適用されます。

手順

	コマンドまたはアクション	目的
ステップ 1	新しいリリースの場合は、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。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。

	コマンドまたはアクション	目的
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）	アップグレード準備 COP ファイルは、システムにアップグレードを妨げる可能性のある問題がないかどうかをチェックします。 （注） シスコでは、アップグレードに失敗する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推奨します。
ステップ 3	Smart Licensing 要件の検討	リリース 12.x では、Prime License Manager に代わってスマート ライセンシングが導入されました。顧客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下でバーチャルアカウント（必要に応じて）を作成する必要があります。Cisco 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 移行タスクを実行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	このリリースの要件および制約事項を確認します。	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。

	コマンドまたはアクション	目的
ステップ 6	ネットワークの状態の確認： • 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 （8 ページ） • データベース レプリケーションの確認 （8 ページ） • パフォーマンス レポートの確認 （9 ページ） • CLI の診断を実行する （10 ページ）	システムの状態は、アップグレードに必要な時間に影響します。アップグレードに必要な時間は、これらのセクションに記載されている条件をシステムが満たしていることを確認することによって、削減することができます。
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上に存在し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 （10 ページ） • 証明書の再作成 （11 ページ） ID 証明書が期限切れの場合	更新アップグレードのみ。期限切れの証明書は、更新アップグレード時にインポートされないため、エラーの原因になる可能性があります。
ステップ 8	新規のバックアップを取る （13 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 （14 ページ）	TFTPディレクトリにカスタムの着信音や背景画像がある場合、これらのファイルはシステムバックアップに含まれないため、別途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 （15ページ）	この手順を使用して、Unified Communications Managerノードと、ネットワーク内の NTP、SMTP、DNS などのサービスと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 （15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

	コマンドまたはアクション	目的
		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 （16 ページ）	IM and Presence Service が Unified CM と接続できることを確認します。 アップグレードのみ。移行で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 （16 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は、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 （17 ページ）	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できるようにデバイスの数をキャプチャするには、Real Time Monitoring Tool（RTMT）を使用します。
ステップ 15	割り当てられたユーザ数を記録する （18 ページ）	IM and Presence Service ノードに割り当てられているユーザ数を記録して、アップグレードの完了後にこの情報を検証できるようにします。
ステップ 16	TFTP パラメータの記録 （18 ページ）	アップグレード プロセスは、TFTP パラメータを変更します。アップグレードが完了した後、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 （19 ページ）	アップグレード中には、Unified Communications Manager のエンタープライズパラメータ設定によって IM and Presence Service のエンタープライズパラメータ設定が上書きされることがあります（両者の設定が異なる場合）。
ステップ 18	ユーザ レコードのエクスポート （19 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 （20 ページ）	アップグレード後の電話のダウンタイムを最小限に抑えるために、アップグレード前のタスクとして、IP 電話を新

	コマンドまたはアクション	目的
		しいリリースに対応するファームウェアにアップグレードできます。 移行ではこのタスクをスキップできます。
ステップ 20	重要なサービスの確認 （21 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 （21 ページ）	リリース 9.x 以前からのアップグレードのみ。アップグレード前に、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	TFTP サービスの非アクティブ化 （22 ページ）	アップグレードを開始する前に、Unified Communications Manager ノードで TFTP サービスを停止します。
ステップ 23	IM and Presence Sync Agent の停止 （22 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 24	使用可能な共通のパーティション領域を確認する （23 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 25	十分な共通パーティション領域がない場合は、次の手順を 1 つ以上実行します。 • 基準値の上限および下限の調節 （23 ページ） • 使用可能なディスク容量の最大化 （24 ページ）	このステップは、Unified CM OS 管理インターフェイスまたは PCD アップグレード タスクのいずれかを使用してアップグレードを実行する、直接アップグレードの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。

	コマンドまたはアクション	目的
ステップ 26	アップグレード ファイルの取得 （25 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では、必要な COP ファイルもすべてダウンロード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 27	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 （28 ページ）	オプション。Unified Communications Manager パブリッシャ ノードのみ。大規模なクラスタをアップグレードするときは、こ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 28	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 （29 ページ）	IM and Presence Service のみ。高可用性が有効になっている場合は、アップグレード前に無効にします。 移行ではこのタスクをスキップできます。
ステップ 29	仮想マシンにシリアル ポートを追加する （30 ページ）	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。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 30	RTMT の高可用性の設定 （30 ページ）	RTMT を使用して監視するメガクラスタ展開では、クラスタ全体の簡易アップグレードの実行中に接続が失われるのを避けるために、RTMT で高可用性を設定することを推奨します。

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完了 COP ファイルによって、次の項目が確認されます。

- 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）

- アップグレードの前に、アップグレード準備 COP ファイルを実行することを強く推奨します。これにより、アップグレードに失敗する可能性を大幅に減らすことができます。
- 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。アップグレード前のバージョンが 9.x の場合は、一部のオプションを使用できます。アップグレード前のバージョンが 8.x 以前の場合、COP ファイルは動作しません。アップグレード前のバージョンが 8.x 以前の場合は、付録の アップグレード前のタスク（手動プロセス） （1 ページ） を参照してください。

手順

ステップ 1 アップグレード準備 COP ファイルをダウンロードして、アップグレード前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) **アップグレード前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.preUpgradeCheck-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 アップグレードのためのシステム準備を確認してください。

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 ファイルを再度実行します。

d) COP ファイルからエラーが返されなくなるまで、この手順を繰り返します。

データベース ステータス レポートの生成

クラスタ ノード間のネットワークの問題がないことを確認するには、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 レプリケーションや、音声およびビデオのシグナリングの Quality of Service（QoS）に影響する、到達可能性や遅延の問題がないことを確認します。

手順

ステップ 1 ノードのレポート インターフェイスにログインします。

- Unified CM ノードの場合は、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 Reporting 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データベース ステータス（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 ステータス（IM and Presence Database Status**）] を選択します。

ステップ 4 [**レポート（Reports**）] ウィンドウで、[**レポートの生成（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示された場合は、[**レポートの説明（Report Descriptions**）] レポートを選択して、トラブルシューティング情報と対処方法を確認します。

データベース レプリケーションの確認

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

手順

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

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

ステップ 2 **utils dbreplication status** コマンドを実行して、データベース テーブルのエラーまたは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 以外の値が返される場合は、続行する前にエラーを解決する必要があります。

パフォーマンス レポートの確認

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）] > [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、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のコール アクティビティ レポートを開き、**[試行済みコール（Calls Attempted）]** の数が仮想マシンの容量に対して大きすぎないことを確認します。https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-system/products-implementation-design-guides-list.html にある「*Cisco Collaboration Systems Solution Reference Network Designs (SRND)*」でシステムの推奨事項を確認することで、**[試行済みコール（Calls Attempted）]** の数のしきい値を決定できます。

ステップ 4 Cisco Unified Serviceability の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の統計レポートを表示します。

ステップ 5 各パフォーマンス保護統計レポートで、システムが、導入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。

導入サイジングについては、以下を参照してください。

- https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-system/products-implementation-design-guides-list.html の「*Cisco Collaboration Systems Solution Reference Network Designs (SRND)*」

- http://tools.cisco.com/cucst の「Collaboration Sizing Tool」。パートナーは、このツールを使用して顧客の設定を評価できます。

CLI の診断を実行する

コマンド行インターフェイス（CLI）診断コマンドを使用して、開始およびアップグレードを行う前にネットワークの問題を診断および解決します。

手順

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

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

ステップ 2 **utils 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一覧を確認できます。

ステップ 3 **utils diagnose fix** コマンドを実行して、システムの問題の自動修正を試みます。

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 [**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。
- 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上に存在し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） アップグレード中には、クラスタごとに ITLRecovery 証明書が生成されます。

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。

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

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

ステップ 3 [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。

ステップ 5 CAPF 証明書または CallManager 証明書の再作成後に CTL クライアントを再実行します（設定している場合）。

（注） tomcat 証明書を再作成するときは、TFTP サービスを無効にし、その後有効にします。それ以外の場合は、TFTP は古いキャッシュの自己署名された tomcat 証明書を提供し続けます。

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 （12 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 *1*：証明書の名前と説明

名前	説明	関連サービス
tomcat tomcat-ECDSA	この自己署名ルート証明書は、HTTPS ノードのインストール中に作成されます。	Tomcat と TFTP
ipsec	この自己署名ルート証明書は、MGCP ゲートウェイおよび H.323 ゲートウェイとの IPsec 接続のインストール中に生成されます。	Cisco Disaster Recovery System（DRS）Local と Cisco DRF Master DR バックアップおよび復元サービス

名前	説明	関連サービス
CallManager CallManager-ECDSA	この自己署名ルート証明書は、Unified Communications Manager のインストール時に自動的にインストールされます。この証明書は、ノード名およびグローバル固有識別子（GUID）など、ノードの ID を提供します。	CallManager、CAPF、電話機の確認、および CTI
CAPF	このルート証明書は、Cisco クライアント設定を完了すると、現在のノードまたはクラスタ内のすべてのノードにコピーされます。	CallManager と CAPF
TVS	自己署名ルート証明書です。	電話/エンドポイント：ITL ファイル

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とすると、復元は失敗します。

この手順は、すべてのアップグレードおよび移行方法で実行してください。

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。

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 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、同じバージョンの インスタント メッセージングとプレゼンス 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着信音または背景画像がある場合、これらのファイル用に別のバックアップを作成する必要があります。これらはディザスタ 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 Web ブラウザまたは TFTP クライアントを使用して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します。

ステップ 2 `Ringlist.xml` ファイルと `List.xml` ファイルをバックアップします。

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

ステップ 4 背景イメージをバックアップします。これらは TFTP ディレクトリの `/Desktops` フォルダ（およびそのサブフォルダ）にあります。

ネットワーク接続の確認

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、次の手順を使用します。

手順

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

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

ステップ 2 ネットワーク内の各ノードで **show network cluster** コマンドを実行して、クラスタ内の Unified Communications Manager サーバー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 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、ネットワーク内の各ノードで **show network eth0** 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 名前解決が正しく動作していることを次のように確認します。

a) 各 Unified Communications Manager ノードの FQDN に ping を送信して、IP アドレスに解決されることを確認します。

b) 各 Unified Communications Manager の IP アドレスに ping を送信して、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 ノードで IPv6 ネットワーキングを確認します。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*** 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 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

インスタント メッセージングとプレゼンス Service ノードが Unified Communications Manager と接続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、**[診断（Diagnostics）] > [システムトラブルシュータ（System Troubleshooter）]** を選択します。
システムが自動でトラブルシューティング チェックを実行します。

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、すべての**[Sync Agent トラブルシュータ（Sync Agent Troubleshooter）]** のテストで、**[結果（Outcome）]**列に合格したことを示す緑色のチェックマークがあることを確認します。

ステップ 3 **[Sync Agent トラブルシュータ（Sync Agent Troubleshooter）]** のテストのいずれかが失敗した場合は、**[問題（Problem）]** と **[解決策（Solution）]** 列の情報を使用して問題を解決してから、アップグレード プロセスを続行します。

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。

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。

- DRS、AXL などの、すべてのアプリケーション ユーザ クレデンシャル、および他のサードパーティ統合用のアカウント
- 管理者、クラスタ セキュリティ、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、コールの詳細記録（CDR）サーバ、および SMTP 情報
- サーバのバージョンおよびタイム ゾーン
- 各サーバで実行されているサービスおよび関連するアクティベーション ステータス
- LDAP 情報およびアクセスの詳細
- SNMP 情報

登録済みデバイスの数を記録する

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の数をキャプチャします。また、導入する仮想マシン（VM）のキャパシティを超えていないことを確認するために、この情報を使用することもできます。

手順

ステップ 1 Unified RTMT インターフェイスから、**[CallManager]** > **[デバイス（Device）]** > **[デバイスの概要（Device Summary）]** 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	数
登録済みの電話機（Registered Phones）	
FSX	
FSO	
T1 CAS	
PRI	
MOH	
MTP	

項目	数
CFB	
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。
クラスタ トポロジの詳細ページには、ノードおよびサブクラスタに関する情報が表示されます。

ステップ 2 各ノードとクラスタに割り当てられているユーザ数を記録します。

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（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 **[最大サービス数（Maximum Serving Count）]** 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

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 サービス ノードの両方のエンタープライズパラメータの設定を記録します。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 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は、アップグレードプロセス中に 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 サービス 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 サービス ノードに固有のエンタープライズ パラメータは、アップグレード中も保持されます。

アップグレードが完了した後、必要なときに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 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。

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 **[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。このファイルは、サーバの外部にコピーし、リモート PC またはリモート デバイスに保存するようにしてください。

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のダウンタイムを最小限に抑えるために、アップグレード前に制御された方法でエンドポイントに新しいファームウェア ファイルを適用することができます。

グループの電話機に新しいファームウェアを適用すると、アップグレード後の TFTP サーバの負荷を取り除き、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 サーバ上で 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限に抑えます。ファームウェアをアップグレードしているときは電話を呼び出しに使用できないため、アップグレードウィンドウ以外のメンテナンス ウィンドウを使用して電話ファームウェアをアップグレードすることを推奨します。

始める前に

- TFTP サーバのディレクトリ（`/usr/local/cm/tftp`）に新しいファームウェア ロードをコピーします。
- IP フォンと登録済みのエンドポイントにシステムのデフォルトとデバイスごとの割り当てのレコードを作成します。

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

ステップ 9 Cisco Unified CM Administration 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

すべての重要なサービスが有効になっていることを確認するには、Cisco Unified Real Time Monitoring Tool（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、**[システム（System）] > [サーバ（Server）] > [重要なサービス（Critical Services）]** の順に選択します。

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

ステップ 3 Unified Communications Manager の重要なサービスを表示するには、ドロップダウン リストから Unified Communications Manager ノードを選択し、[**音声/ビデオ（Voice/Video）**] タブをクリックします。

ステップ 4 IM and Presence Service の重要なサービスを表示するには、[**IM and Presence**] タブをクリックし、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 サービス ノードを選択します。

ステップ 5 重要なサービスが停止されていることをステータスが示している場合、アップグレードを開始する前にそれらを再度有効にします。

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ます。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、Unified Communications Manager ノードで 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** サービスを選択解除します。

ステップ 4 **[停止（Stop）]** をクリックします。

ステップ 5 **Cisco Extension Mobility** サービスを実行している各ノードに対し、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。アップグレードの完了後にサービスを再起動する必要があります。

TFTP サービスの非アクティブ化

アップグレードを開始する前に、次の手順を使用して、Unified Communications Manager ノードで TFTP サービスを停止します。

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** サービスを選択解除します。

ステップ 4 **[停止（Stop）]** をクリックします。

ステップ 5 **Cisco TFTP** サービスを実行している各ノードに対し、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。アップグレードの完了後に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

インスタント メッセージングとプレゼンス 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、アップグレードプロセスを開始する前に 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 インスタント メッセージングとプレゼンス 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 ウィンドウの [**System（システム**）] カウンタのリストから [**Disk Usage（ディスク使用状況**）] を選択します。
ディスク使用状況についての詳細情報が、ページに表示されます。

ステップ 2 ページの下部の表を表示して、共通パーティションの [**合計領域（Total Space**）] と [**使用済み領域（Used Space**）] を比較します。アップグレードを開始する前に、25G以上の共通パーティション領域が必要です。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、展開にさらに多くの領域が必要となることがあります。場合によっては、25 GB の空き容量がある場合でも、領域が不足しているというエラー メッセージが表示されてアップグレードに失敗することがあります。この回避策は、不要なファイルを削除し、共通パーティションの空き容量を増やすことです。

基準値の上限および下限の調節

この手順を使用して、基準値の上限と下限を調節し、トレースの削減と不要ログ ファイルの削除を行います。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）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 30 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 40 に調節します。

使用可能なディスク容量の最大化

11.5(X) から 12.5 にアップグレードする場合、ダウンロードが必要な COP ファイルを確認します。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。

共通のパーティションに追加のスペースを作成するには、この手順の 1 つ以上のステップを実行できます。

（注） 現在のバージョンで、以前にシリアル接続を使用して 11.5(x) より前のバージョンからアップグレードしたことがある場合は、古い OS パーティション スキームと仮想ディスク レイアウトが使用されている可能性があります。これによって「ディスクスペースが不足しています」の問題が増幅するため、仮想ディスク スペース追加の効果が制限されます。アップグレード準備 COP ファイルではこれらの問題がチェックされ、解決するためのガイダンスが提供されます。

手順

ステップ 1 次のいずれかのオプションを使用して、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。

- Cisco Unified OS の管理インターフェイスから、**[ソフトウェア アップグレード（Software Upgrades）] > [TFTP ファイルの管理（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` と `file delete tftp` コマンドを使用し、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、**[ソフトウェアアップグレード（Software Upgrades）] > [デバイスロード管理（Device Load Management）]** を選択し、不要なファイルを削除します。

（注） 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。

共通パーティションで利用可能な空き容量のサイズを確認するには、[**show diskusage common <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。

ステップ 2 前のステップでアップグレードに十分なディスク容量が作成されなかった場合にのみ、この手順を実行します。Free Common Space COP ファイル（ciscocm.free_common_space_v<latest_version>.cop.sgn）を使用します。

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は使用できなくなるため、このファイルのインストール後は非アクティブなバージョンに戻せなくなります。

（注） 110 GB または 80 GB の単一ディスク、あるいは 2 台の 80 GB ディスクを使用する展開では、アップグレードのための容量として、アクティブ パーティションのディスク容量の少なくとも 2 倍が必要です。たとえば、2 台の 80 GB ディスクの展開では、アクティブ パーティションを 25 GB 以下にする必要があり、使用可能な容量は 50 GB 以上必要です。ディスクの使用量は次のコマンドで確認できます。

1. アクティブ側のパーティション サイズを確認するには、[**show diskusage activelog <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。
2. 共通パーティションで利用可能な空き容量のサイズを確認するには、[**show diskusage common <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。
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. アクティブ パーティション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 ファイルのダウンロードと、必要な Cisco オプション パッケージ（COP）ファイルのアップグレードを行う必要があります。

手順

ステップ 1 必要 COP ファイルがあれば、下の表の手順を参照して特定します。

ステップ 2 Cisco.comからアプリケーションのアップグレードファイルをダウンロードします。ソフトウェアは、export restricted（K9）バージョンと export unrestricted（XU）バージョンを使用できるため、適切な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 のアップグレード ファイルをダウンロードするには、https://software.cisco.com に移動し、[**ダウンロードとアップグレード（Download & Upgrade）**] セクションにある [**ソフトウェアのダウンロード（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の更新（Unified Communications Manager/CallManager/Cisco Unity Connection Updates）]** に移動します。
- インスタント メッセージングとプレゼンス Service のアップグレード ファイルをダウンロードするには、https://software.cisco.com に移動し、[**ダウンロードとアップグレード（Download & Upgrade）**] セクションにある [**ソフトウェアのダウンロード（Software Download）**] リンクをクリックします。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（Version）>]*** > **[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、[ダウンロードとアップグレード（Download & Upgrade）] セクションの [ソフトウェアダウンロード（Software Download）] リンクをクリックしてから、**[Unified Communications]** > **[Unified Communicationsアプリケーション（Unified Communications Applications）]** > **[プレゼンスソフトウェア（Presence Software）]** > **[Unified Communications Manager IM and Presenceサービス（Unified Communications Manager IM and Presence Service）]** > ***[<Version>]*** > **[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 サービスの 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。

表 *2 : Unified Communications Manager* リリース *12.0(1)* へのアップグレードおよび移行に必要な *COP* ファイル

遷移元	目的	アップグレード タイプ
8.6(x)	12.x	更新アップグレード。必須 COP ファイル： • ciscocm.version3-keys.cop.sgn オプションの COP ファイル： • ciscocm.vmware-disk-size-reallocation-<latest_version>.cop.sgn • ciscocm.free_common_space_v<latest_version>.cop.sgn
9.1(x)	12.x	更新アップグレード。必須 COP ファイル： • ciscocm.version3-keys.cop.sgn オプションの COP ファイル： • ciscocm.vmware-disk-size-reallocation-<latest_version>.cop.sgn • ciscocm.free_common_space_v<latest_version>.cop.sgn
10.5(x)	12.x	標準アップグレード：COP ファイルは不要。
11.0(x)	12.x	標準アップグレード：COP ファイルは不要。
11.5(x)	12.x	標準アップグレード。COPファイルが更新され、ディスク容量が増加します。 • ciscocm.free_common_space_v<latest_version>.cop.sgn. COP ファイルと Readme ファイルをダウンロードするには、https://software.cisco.com に移動し、**[ダウンロードとアップグレード（Download & Upgrade）]**セクションの**[ソフトウェアダウンロード（Software Download）]**リンクをクリックしてから、**[Unified Communications]** > **[コール制御（Call Control）]** > **[Cisco Unified Communications Manager (CallManager)]** > **[<*Version*>]** > **[Unified Communications Manager/CallManager/Cisco Unity Connectionのユーティリティ（Unified Communications Manager/CallManager/Cisco Unity Connection Utilities）]** に移動します。

遷移元	目的	アップグレード タイプ
12.0(1)	12.0(1)SU1 以降	PCD 移行には COP ファイルが必要です。 • ciscocm-slm-migration.k3.cop.sgn （注） この要件は、Unified Communications Manager（ビルド 12.0.1.10000-10）のリリース 12.0(1) から Prime Collaboration Deployment を移行する場合にのみ適用されます。Unified Communications Manager 12.0(1)SU1 などの上位リリースから移行する場合、COP ファイルをインストールする必要はありません。

表 *3 : Cisco Unified Presence* リリースからの更新アップグレードに必要な *COP* ファイル

元の Cisco Unified Presence リリース	アップグレード先の IM and Presence Release	アップグレード タイプ
8.5(4) 〜 8.6(1)	12.x	更新アップグレード。以下の COP ファイルが必要： • cisco.com.cup.refresh_upgrade_v<latest_version>.cop • ciscocm.version3-keys.cop.sgn

表 *4 : IM and Presence Service* リリースからの更新アップグレードに必要な *COP* ファイル

元の IM and Presence リリース	アップグレード先の IM and Presence Release	アップグレード タイプ
9.1(x)	12.x	更新アップグレード。以下の COP ファイルが必要： • ciscocm.version3-keys.cop.sgn
10.5(x)	12.x	標準アップグレード：COP ファイルは不要。
11.0(x)	12.x	標準アップグレード：COP ファイルは不要。
11.5(x)	12.x	標準アップグレード：COP ファイルは不要。

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

この手順は Unified Communications Manager パブリッシャ ノードでのみ実行します。

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*** 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。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、インスタント メッセージングとプレゼンス サービス ノードにのみ適用されます。インスタント メッセージングとプレゼンス 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。

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 ポートを追加するように、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後は、シリアル ポートの削除 の手順を実行します。アップグレードに失敗した場合は、アップグレードに失敗した後のログ ファイルのダンプを参照してください。

RTMT の高可用性の設定

メガクラスタ展開で Cisco Unified リアルタイム監視ツール（RTMT）を使用する場合は、クラスタ全体の簡易アップグレードの実行中に接続が失われるのを避けるために、RTMT で高可用性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 Administration 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 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 **[プライマリ コレクタ（Primary Collector）]** サービス パラメータで、任意のサブスクライバ ノードを選択します。

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

ステップ 7 [保存（**Save**）] をクリックします。

ステップ 8 Cisco Unified リアルタイム監視ツールを任意のサブスクライバ ノードに接続します。