アップグレード前のタスク(手動プロセス)

この付録の手動アップグレード前のタスクは、10.0 (1) より前のリリースからアップグレードする場合、またはアップグレード前のタスクを手動で実行する場合に使用できます。

- アップグレード前の作業 （1 ページ）

アップグレード前の作業

アップグレードまたは移行を開始する前に、次のタスクを実行します。

（注） このタスクフローの手順は、特に明記されていない限り、すべてのアップグレードおよび移行に適用されます。

手順

	コマンドまたはアクション	目的
ステップ 1	新しいリリースの場合は、リリースノートをお読みください。 http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-release-notes-list.html	新機能を理解し、アップグレードがシステムに関連付けられている他のシスコ製品とどのように相互作用するかを確認します。すべてのアップグレードおよび移行の方法について、この手順を実行します。
ステップ 2	アップグレード準備 COP ファイルの実行（アップグレード前）	アップグレードの準備状況 COP ファイルは、アップグレードに干渉する可能性のある問題がないかシステムをチェックします。 （注） アップグレードの失敗の可能性を減らすために、COP ファイルを実行することを強くお勧めします。

	コマンドまたはアクション	目的
ステップ 3	スマートライセンスの要件を考慮する	リリース12.x では、プライムライセンスマネージャの代替としてスマートライセンスが導入されています。顧客のスマートアカウントを設定し、組織の構造に基づいてスマートアカウントの下に仮想アカウント (オプション) を作成する必要があります。シスコスマートアカウントの詳細については、https://www.cisco.com/c/en/us/buy/smart-accounts.html を参照してください。スマートソフトウェアライセンシングの概要の詳細については、https://www.cisco.com/c/en/us/buy/smart-accounts/software-licensing.html を参照してください。
ステップ 4	アップグレードする元のソフトウェアバージョンが仮想マシンで実行されていることを確認します。	ソフトウェアが MCS ハードウェアで実行されている場合は、PCD 移行タスクを完了する必要があります。http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html にある『*Cisco Prime Collaboration Deployment* アドミニストレーション ガイド』を参照してください。
ステップ 5	要件および制約事項このリリースのを確認します。	システムがすべてのネットワーク要件、プラットフォーム要件、およびソフトウェア要件を満たしていることを確認します。 このステップは、すべてのアップグレードおよび移行方法で実行します。
ステップ 6	ネットワークの健全性を確認します。 • アップグレードの時間要件に影響する要因を読み、システムがそのセクションに記載されている条件を満たしていることを確認します。 • データベース ステータス レポートの生成 （9 ページ） • データベースのレプリケーションの確認 （10 ページ）	システムの健全性は、アップグレードに必要な時間に影響します。システムがこれらのセクションで説明されている条件を満たしていることを確認することで、アップグレードに必要な時間を短縮できます。

	コマンドまたはアクション	目的
	• パフォーマンス レポートの確認 （11 ページ） • CLI の診断を実行する （11 ページ）	
ステップ 7	証明書チェーン内の信頼証明書を含め、期限切れの証明書がパーティションにないことを確認します。期限切れの証明書がある場合： • 信頼証明書の削除 （12 ページ） • 証明書の再作成 （13 ページ） ID 証明書の有効期限が切れている場合。	直接アップグレードの場合は、システムがすべての証明書要件を満たしていることを確認します。 （注） マルチサーバー（SAN）証明書の場合は、SANエントリがクラスタのすべてのノードに存在することを確認します。
ステップ 8	新規のバックアップを取る （17 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 （18 ページ）	TFTPディレクトリにカスタム呼出音または背景イメージがある場合は、それらのファイルがシステムバックアップに含まれていないため、これらのファイルに対して個別のバックアップを作成します。
ステップ 10	ネットワーク接続の確認 （19ページ）	この手順を使用して、ネットワーク内のUnified Communications Manager ノードとサービス(NTP、SMTP、DNS など)間の接続を確認します。
ステップ 11	IPv6 ネットワーキングの確認 （19ページ）	Unified Communications Manager ノードのみ。パブリッシャノードとサブスクライバノード間の IPv6 ネットワーキングを確認します。IPv6 が正しく設定されていない場合、ロードの検出に 20 分ほどかかることがあります。
ステップ 12	IM and Presence と Cisco Unified Communications Manager との間の接続の確認 （20 ページ）	IM and Presence Service が、Unified CM と接続されていることを確認します。

	コマンドまたはアクション	目的
		アップグレードの場合のみ。移行の場合は、このタスクをスキップできます。
ステップ 13	設定およびログイン情報の収集 （20 ページ）	アップグレードプロセス中に問題が発生した場合に備えて、Unified Communications Manager ノードの現在の設定とログイン情報を記録します。
ステップ 14	登録済みデバイスの数を記録する （21 ページ）	リアルタイムモニタリングツール (RTMT) を使用してデバイス数をキャプチャします。これにより、アップグレードの完了後にエンドポイントとリソースを確認できます。
ステップ 15	割り当てられたユーザ数を記録する （22 ページ）	アップグレードの完了後にこの情報を確認できるように、 IM and Presence Service ノードに割り当てられたユーザの数を記録します。
ステップ 16	TFTP パラメータの記録 （22 ページ）	アップグレードプロセスによって、TFTPパラメータが変更されます。アップグレードの完了後にパラメータをリセットできるように、現在の設定を記録します。
ステップ 17	エンタープライズ パラメータの記録 （23 ページ）	アップグレード中は、設定が異なっている場合、Unified Communications Manager のエンタープライズパラメータの設定によって IM and Presence Service の enteprise パラメータ設定が上書きされることがあります。
ステップ 18	ユーザ レコードのエクスポート （23 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 （24 ページ）	アップグレード後の電話機のダウンタイムを最小限に抑えるために、アップグレード前のタスクとして、新しいリリースに対応するファームウェアに IP フォンをアップグレードできます。 移行ではこのタスクをスキップできます。

	コマンドまたはアクション	目的
ステップ 20	重要なサービスの確認 （25 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 （25 ページ）	リリース9.x以前からのアップグレードの場合のみ。アップグレードする前に、Unified CM ノードで Cisco Extension Mobility サービスを停止する必要があります。 移行ではこのタスクをスキップできます。
ステップ 22	IM and Presence Sync Agent の停止 （26 ページ）	IM and Presence のアップグレードの一部として Unified Communications Manager をアップグレードする必要がある場合は、アップグレードを開始する前に IM and Presence Sync Agent サービスを停止する必要があります。 移行ではこのタスクをスキップできます。
ステップ 23	使用可能な共通のパーティション領域を確認する （26 ページ）	アップグレードに十分な共通パーティション領域があることを確認します。 移行ではこのタスクをスキップできます。
ステップ 24	十分な共通パーティション領域がない場合は、次の手順の1つまたは複数を実行します。 • 基準値の上限および下限の調節 （27 ページ） • 使用可能なディスク領域の最大化 （27 ページ）	この手順は、アップグレードを実行するために、Unified CM OS 管理インターフェイスまたは PCD アップグレードタスクのいずれかを使用する直接アップグレードの場合にのみ実行してください。 **注意** 十分なディスク領域がない状態でアップグレードを実行すると、アップグレードが失敗する可能性があります。
ステップ 25	アップグレード ファイルの取得 （29 ページ）	必要なアップグレードファイルをダウンロードします。更新アップグレードの場合は、必要な COP ファイルもダウンロードする必要があります。

	コマンドまたはアクション	目的
		（注） 12.5.x より前のソースからリリース 15 への更新アップグレードはサポートされていません。 移行ではこのタスクをスキップできます。
ステップ 26	データベース レプリケーションのタイムアウトを増やす （30 ページ）	オプション。Unified Communications Manager パブリッシャ ノードのみ。大規模クラスタをアップグレードする場合は、次の手順を使用します。 移行ではこのタスクをスキップできます。
ステップ 27	プレゼンス冗長グループに対するハイアベイラビリティの無効化 （31 ページ）	IM and Presence Service のみ。ハイアベイラビリティが有効になっている場合は、アップグレードの前に無効にします。 移行ではこのタスクをスキップできます。
ステップ 28	仮想マシンにシリアル ポートを追加する （31 ページ）	アップグレードが失敗した場合にログをダンプできるように、仮想マシンにシリアルポートを追加します。この手順は、すべてのノードに対して実行します。
ステップ 29	RTMT の高可用性の設定 （32 ページ）	RTMT を使用してモニタするメガクラスタ展開では、クラスタ全体のアップグレード中に接続が失われないように、RTMT のハイアベイラビリティを設定することを推奨します。
ステップ 30	Microsoft SQL Server を使用したアップグレードに必要なデータベース移行 （32 ページ）	この手順は、IM and Presence Service ノードのみに適用されます。Microsoft SQL Server を IM and Presence Service で外部データベースとして展開していて、11.5(1)、11.5(1)SU1 または 11.5(1)SU2 からアップグレードする場合は、新しい SQL Server データベースを作成して新しいデータベースに移行する必要があります。

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

アップグレード準備 COP ファイルの実行（アップグレード前）

アップグレード準備状況 COP ファイルは、次の点を確認します。

- インストールされた COP ファイル
- ネットワークサービスと接続 (DNS、NTP、クラスタ内)
- ライセンスの同期
- VMware ツールの互換性

- ハード ディスク パーティション サイズ
- スワップサイズチェック
- ファイルシステムのタイプとゲスト OS のチェック
- 宛先バージョンに使用可能なディスク容量
- ESXi バージョン チェック
- SIP および h.323 トランクの登録
- データベース認証および複製のステータス
- データベースの健全性
- 最後の DRS バックアップのステータス
- リモート コール制御（RCC）機能のステータス
- サービスステータス
- インストールされている COPs とロケール
- デバイス登録ステータス数
- エンタープライズ パラメータおよびサービス パラメータの設定
- TFTP 最大サービス数
- アクティブおよび非アクティブのバージョン
- 期限切れの証明書がある場合：
- FIPS モードのパスワード長の制限
- FIPS モードでの ESP および暗号化アルゴリズムの IPSec ポリシー設定チェック

（注）
- アップグレードの失敗の可能性を大幅に低減するため、アップグレードする前にアップグレード準備の COP ファイルを実行することを強くお勧めします。
- COP ファイルは、アップグレード前のバージョンが 10. x 以降の場合に完全にサポートされます。
- 3DES アルゴリズムは FIPS モードでサポートされていないため、3DES アルゴリズムを使用する IPSec ポリシーを削除し、IPSec トンネルが確立される両方のノードで、3DES 以外の暗号化および ESP アルゴリズムを使用して IPSec ポリシーを再作成する必要があります。

手順

ステップ 1 アップグレード準備状況の COP ファイルをダウンロードして、アップグレード前のテストを実行します。

a) ダウンロードサイトに移動します。
b) 宛先のリリースを選択し、**[ユUnified Communications Manager ユーティリティ（Unified Communications Manager Utilities）]** を選択します。
c) アップグレード準備状況の COP ファイルをダウンロードして、**アップグレード前のテストを実行**します (例: `ciscocm preUpgradeCheck-00019 COP`)。最新のファイルのファイル名とバージョンが異なる場合があることに注意してください。

ステップ 2 アップグレードに関するシステムの準備状況を確認します。

a) COP ファイルを実行します。
b) COP ファイルが返す問題を解決します。
c) COP ファイルを再度実行します。
d) COP ファイルがエラーを返さないようにするまで、このプロセスを繰り返します。

ステップ 3 GUI または CLI から cop ファイルをインストールします。インストールが完了したら、CLI から **file view install PreUpgradeReport.txt** を実行してレポートを表示します。

ステップ 4 RTMT からレポートを表示するには

a) RTMT にログインします。
b) **[トレースとログ セントラル（Trace and Log Central）]** で、**[リモート参照（Remote Browse）]** をダブルクリックして、**[ファイルのトレース（Trace files）]** を選択して、**[次へ（Next）]** をクリックします。
c) **すべてのサーバーのすべてのサービスを選択**し、**[次へ（Next）]** をクリックします。
d) **[終了（Finish）]**、**[閉じる（Close）]** を順にクリックします。
e) ノードをダブルクリックして、**[CUCM パブリッシャ（Publisher）]>[システム（System）]>[インストール アップグレード ログ（ Install upgrade Logs）]** を展開します。
f) **[インストール（Install）]** をダブルクリックして、必要なファイルを選択してダウンロードします。

データベース ステータス レポートの生成

Cisco Unified Reporting Tool（CURT）を使用して、データベースステータスレポートを生成し、クラスタノード間にネットワークの問題がないことを確認します。たとえば、ノード間のデータベースレプリケーションに影響する到達可能性または遅延に関する問題がないこと、または音声およびビデオシグナリングの quality of service (QoS) に影響する問題がないことを確認します。

手順

ステップ 1 ノードのレポーティングインターフェイスにログインします。

- Unified CM ノードの場合は、Cisco Unified Reporting インターフェイスにログインします。
- IM and Presence ノードの場合は、 Cisco Unified IM and Presence レポートインターフェイスにログインします。

ステップ 2 [**システム レポート**（**System Reports**）] を選択します。

ステップ 3 ノードでデータベースのレプリケーションを確認します。

- Unified CM の場合は、[**Unified CM Database Status**] を選択します。
- IM and Presence の場合は、 **IM and Presence データベースのステータス**を選択します。

ステップ 4 [**レポート**（**Reports**）] ウィンドウで、[**レポートの生成**（**Generate Report**）]（棒グラフ）アイコンをクリックします。

ステップ 5 [**詳細の表示**（**View Details**）] リンクをクリックして、自動的に表示されないセクションの詳細情報を表示します。

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

データベースのレプリケーションの確認

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

手順

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

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

ステップ 2 **utils dbreplication status** コマンドを実行して、データベース テーブルのエラーまたは不一致を確認します。

ステップ 3 **utils dbreplication runtimestate** コマンドを実行して、ノードでデータベース レプリケーションがアクティブであることを確認します。

出力にはすべてのノードが一覧表示されます。データベース レプリケーションがセットアップされて正常であれば、各ノードの **replication setup** の値は **2** になります。

2 以外の値が返された場合は、続行する前にエラーを解決する必要があります。

パフォーマンス レポートの確認

手順

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

ステップ 2 リンクをクリックして、最新のレポートを選択します。

ステップ 3 **CallActivitiesRep**をクリックして新しいタブでコールアクティビティレポートを開き、試行された**コール**数が仮想マシンのキャパシティに対して高すぎることを確認します。https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-system/products-implementation-design-guides-list.html にある**『シスココラボレーションシステムソリューションリファレンスネットワークデザイン（SRND）』**でシステムの推奨事項を確認することで、試行されたコール数のしきい値を決定できます。

ステップ 4 Cisco Unified Serviceability インターフェイスに戻り、各ノードの [**PerformanceRep**] リンクをクリックして、パフォーマンス保護統計情報レポートを表示します。

ステップ 5 各パフォーマンス保護統計情報レポートで、システムが展開サイズに対して指定されているクラスタ全体またはノードごとの制限を超えていないことを確認します。

展開のサイジングの詳細については、次を参照してください。

- https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-system/products-implementation-design-guides-list.html にある『シスコ コラボレーション システム ソリューション リファレンス ネットワーク デザイン（*SRND*）』
- http://tools.cisco.com/cucst にある「Collaboration Sizing Tool」。パートナーは、このツールを使用して、お客様の設定を評価することができます。

CLI の診断を実行する

コマンドラインインターフェイス (CLI) の診断コマンドを使用して、ネットワークの問題を診断および解決してから、アップグレードを開始およびアップグレードします。

手順

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

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

ステップ 2 **utils diagnose test** コマンドを実行します。

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

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

信頼証明書の削除

削除できる証明書は、信頼できる証明書だけです。システムで生成される自己署名証明書は削除できません。

注意 証明書を削除すると、システムの動作に影響する場合があります。また、証明書が既存のチェーンの一部である場合、証明書チェーンが壊れることがあります。この関係は、**[証明書の一覧（Certificate List）]** ウィンドウ内の関連する証明書のユーザ名とサブジェクト名から確認します。この操作は取り消すことができません。

手順

ステップ 1 [Cisco Unified OS の管理（Cisco Unified OS Administration）] から **[セキュリティ（Security）] > [証明書の管理（Certificate Management）]** を選択します。

ステップ 2 証明書の一覧をフィルタするには、[検索（Find）] コントロールを使用します。

ステップ 3 証明書のファイル名を選択します。

ステップ 4 [削除（Delete）] をクリックします。

ステップ 5 [OK] をクリックします。

（注）
- 削除する証明書が 「CAPF-trust」、「tomcat-trust」、「CallManager-trust」、または 「Phone-SAST-trust」 証明書タイプの場合、証明書はクラスタ内のすべてのサーバで削除されます。
- 電話エッジトラストからの証明書の削除は、パブリッシャから行う必要があります。
- 証明書をCAPF-trustにインポートする場合、それはその特定のノードでのみ有効になり、クラスタ全体で複製されることはありません。

証明書の再作成

アップグレードを開始する前に、証明書チェーン内の信頼証明書を含め、期限切れの証明書がパーティションにないことを確認します。証明書が期限切れの場合は、再作成します。電話機を再起動してサービスを再起動する必要があるため、営業時間後にこの手順を実行します。Cisco Unified OS の管理に「cert」 タイプとしてリストされている証明書のみ再作成できます。

（注） 12.5.x より前のソースからリリース 15 への更新アップグレードはサポートされていません。

（注） アップグレード中は、ITLRecovery証明書がクラスタごとに生成されます。クラスタが混合モードの場合は、CTLファイルを手動で更新します。電話機をリセットして、最新の更新を反映します。これは、更新アップグレードにのみ適用されます。リリース 12.5(1)SU3 以降、CTL は必要なくなりました。

注意 証明書を再作成すると、システムの動作に影響する場合があります。証明書を再作成すると、サードパーティの署名付き証明書（アップロードされている場合）を含む既存の証明書が上書きされます。

手順

ステップ 1 [Cisco Unified OS の管理（Cisco Unified OS Administration）] から **[セキュリティ（Security）]** > **[証明書の管理（Certificate Management）]** を選択します。

検索パラメータを入力して、証明書を検索して設定の詳細を表示します。すべての条件に一致したレコードが [**Certificate List**] ウィンドウに表示されます。

証明書の詳細ページで **[再生成（Regenerate）]** ボタンをクリックすると、同じキー長を持つ自己署名証明書が再生成されます。

（注） 証明書を再生成する場合、**[再生成（Regeneration）]** ウィンドウを閉じて、新しく生成された証明書を開くまで、**[証明書の説明（Certificate Description）]** フィールドは更新されません。

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

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

ステップ 3 [生成（Generate）] をクリックします。

ステップ 4 再作成された証明書の影響を受けるサービスをすべて再起動します。詳細については、証明書の名前と説明 （14 ページ）を参照してください。

ステップ 5 CAPF 証明書、ITLRecovery 証明書、または CallManager 証明書の再生成後に CTL ファイルを更新します（設定している場合）。

（注） 証明書を再作成したら、システムのバックアップを実行して、最新のバックアップに再作成した証明書が含まれるようにします。バックアップに再作成した証明書が含まれていない状態でシステムの復元タスクを実行する場合は、システム内の各電話機のロックを手動で解除して、電話機を登録できるようにする必要があります。

次のタスク

証明書を再作成したら、システムのバックアップを実行して、最新のバックアップに再作成した証明書が含まれるようにします。

関連トピック

証明書の名前と説明 （14 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	再起動サービス
tomcat tomcat-ECDSA	この証明書は、SIP Oauth モードが有効な場合に Web サービス、Cisco DRF サービス、および Cisco CallManager サービスで使用されます。	（注） 以下のサービスの再起動は、リリース 14 以降に適用されます。 Cisco Tomcat サービス、Cisco Disaster Recovery System（DRS）ローカルおよびマスターサービス、Cisco UDS Tomcat および Cisco AXL Tomcat ウェブサービス。 SAML SSO が Tomcat 証明書で有効になっている場合は、IDP で SP メタデータを再プロビジョニングする必要があります。
ipsec	この自己署名ルート証明書は、Unified Communications Manager、MGCP、H.323、および IM and Presence サービスとの IPsec 接続のインストール中に生成されます。	IPsec サービス。

名前	説明	再起動サービス
CallManager CallManager-ECDSA	SIP、SIP トランク、SCCP、TFTP などに使用されます。	（注） リリース 14 の場合、次のサービスを再起動します。 Cisco Call Manager サービスおよびその他の関連サービス（Cisco CTI Manager、HAProxy サービスなど）：サーバーがセキュアモードの場合に CTL ファイルを更新します。 （注） 以下のサービスの再起動は、リリース 14 SU1 以降に適用されます。 CallManager：HAProxy サービスで、サーバーがセキュアモードの場合は CTL ファイルを更新します。 CallManager-ECDSA：Cisco CallManager サービス、HAProxy サービス。
CAPF	Unified Communications Manager パブリッシャで実行されている CAPF サービスで使用されます。この証明書は、エンドポイントに LSC を発行するために使用されます（オンラインおよびオフライン CAPF モードを除く）。	該当なし
信頼検証サービス（TVS）	これは信頼検証サービスで使用され、サーバ証明書が変更された場合に、電話機のセカンダリ信頼検証メカニズムとして機能します。	該当なし

（注）

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

重要 これは、リリース 14SU2 以降に適用されます。

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

新規のバックアップを取る

アップグレードを実行する前に、システムをバックアップして、バックアップファイルが現在インストールされているソフトウェアと完全に一致することを確認する必要があります。現在のバージョンと一致しないバックアップファイルからシステムを復元しようすると、復元は失敗します。

すべてのアップグレードおよび移行の方法について、次の手順を実行します。

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

始める前に

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

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

ます。また、バージョン 11.5.1.10000-1 のバックアップ ファイルを作成することも必要です。

- バックアップ プロセスは、リモート サーバに利用可能な容量がないためや、ネットワーク接続が中断されたために失敗することがあります。バックアップが失敗する原因となった問題に対処した後、新規のバックアップを開始する必要があります。
- クラスタ セキュリティ パスワードのレコードがあることを確認します。このバックアップの完了後に、クラスタ セキュリティ パスワードを変更した場合は、パスワードを認識している必要があります。パスワードを認識していないと、バックアップ ファイルを使用してシステムを復元できなくなります。

手順

ステップ 1 ディザスタ リカバリ システムから、**[バックアップ（Backup）]**>**[手動バックアップ（Manual Backup）]** の順に選択します。

ステップ 2 [手動バックアップ（Manual Backup）] ウィンドウで、[バックアップデバイス名（Backup Device Name）] 領域を選択します。

ステップ 3 [機能の選択（Select Features）] 領域から機能を選択します。

ステップ 4 [バックアップの開始（Start Backup）] をクリックします。

カスタム着信音と背景イメージのバックアップ

TFTP ディレクトリにカスタム呼出音または背景イメージがある場合は、これらのファイル用に別のバックアップを作成する必要があります。これらは、ディザスタリカバリシステム(DRS)のバックアップファイルには含まれていません。

手順

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

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

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

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

ネットワーク接続の確認

ネットワーク内のすべてのノードとサービスの間の接続を確認するには、次の手順を実行します。

手順

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

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

ステップ 2 ネットワーク内**show network cluster**の各ノードでコマンドを実行し、クラスタ内Unified Communications Managerのサーバ間の通信を確認します。

ステップ 3 NTP サーバがある場合は、 **utils ntp status**コマンドを実行して、ntp サーバへの接続を確認します。

ステップ 4 SMTP サーバがある場合は、サーバに ping を実行して接続を確認します。

ステップ 5 DNS を使用している場合は**show network eth0** 、ネットワーク内の各ノードでコマンドを実行して、dns とドメインが設定されていることを確認します。

ステップ 6 DNS 名前解決が正しく機能していることを確認します。

a) 各Unified Communications Managerノードの FQDN に対して Ping を実行し、IP アドレスに解決されることを確認します。

b) 各Unified Communications Managerの IP アドレスに Ping を実行して、FQDN に解決されることを確認します。

IPv6 ネットワーキングの確認

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

最初のノード (Unified Communications Managerデータベースパブリッシャノード) とUnified Communications Managerサブスクライバノード上の IPv6 ネットワーキングがあることを確認します。Unified Communications Manager サブスクライバ ノードで IPv6 が正しく設定されていないと、ロードの検出に 20 分ほどかかることがあります。

手順

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

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

ステップ 2 コマンド **utils network ipv6 ping***destination [count]* を実行します。

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

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

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

手順

ステップ 1 Cisco Unified CM IM and Presence の管理インターフェイスから、**[診断（Diagnostics）] > [システムトラブルシュータ（System Troubleshooter）]** を選択します。
システムはトラブルシューティングチェックを自動的に実行します。

ステップ 2 トラブルシューティングチェックの結果がロードされたら、**同期エージェントのトラブルシューティング**テストのすべてが、[**結果**(results)]列に緑色のチェックマークが付いていることを確認し、テストが合格したことを示します。

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

設定およびログイン情報の収集

アップグレードプロセス中に問題が発生したUnified Communications Manager場合に備えて、ノードの現在の設定とログイン情報を記録します。

手順

ステップ 1 次のログインおよびパスワード情報を記録します。

- すべてのアプリケーションユーザクレデンシャル (DRS、AXL、その他のサードパーティ統合のアカウントなど)
- 管理者、クラスタセキュリティ、および証明書信頼リスト (CTL) のセキュリティトークンパスワード

ステップ 2 ネットワークの設定に関する次の情報を記録します。

- IP アドレス、ホスト名、ゲートウェイ、ドメイン名、DNS サーバ、NTP サーバ、コール詳細記録 (CDR) サーバ、および SMTP 情報
- サーバのバージョンとタイムゾーン
- 各サーバで実行されているサービスと、関連するアクティベーションステータス
- LDAP 情報とアクセスの詳細
- SNMP 情報

登録済みデバイスの数を記録する

アップグレードの完了後にエンドポイントとリソースを確認できるように、アップグレードを開始する前に、Real Time Monitoring Tool (RTMT) を使用してデバイスの数をキャプチャします。また、この情報を使用して、展開している仮想マシン (VM) の容量を超えていないことを確認することもできます。

手順

ステップ 1 統合 RTMT インターフェイスから**CallManager** > **デバイス** > **デバイスの概要**を選択します。

ステップ 2 各ノードの登録済みデバイスの数を記録します。

項目	Count
Registered Phones	
FXS	
FSO	
T1 CAS	
PRI	
MOH	
MTP	
CFB	

項目	Count
XCODE	

割り当てられたユーザ数を記録する

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

手順

ステップ 1 Cisco Unified CM IM and Presence の管理インターフェイスから、**[システム（System）]** > **[クラスタ トポロジ（Cluster Topology）]** の順に選択します。
[Cluster Topology Details] ページには、ノードとサブクラスタに関する情報が表示されます。

ステップ 2 各ノードとクラスタに割り当てられているユーザの数を記録します。

TFTP パラメータの記録

アップグレードプロセス中に、TFTP サービスパラメータの**最大サービス数**が変更され、デバイス登録要求の数が増加します。アップグレードの完了後にパラメータをリセットできるように、既存の設定を記録します。

手順

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

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

ステップ 3 [**サービス**（**Service**）] ドロップダウン リストから、[**Cisco TFTP サービス**（**Cisco TFTP service**）] を選択します。

ステップ 4 [詳細設定（Advanced）] をクリックします。

ステップ 5 [保存（Save）] をクリックします。

ステップ 6 **サービスの最大数**に設定されている値を記録します。

エンタープライズ パラメータの記録

ノードとUnified Communications ManagerIM and Presence Serviceサービスノードの両方でエンタープライズパラメータの設定を記録します。一部のエンタープライズパラメータは、Unified Communications ManagerノードとIM and Presence Serviceサービスノードの両方に存在します。同じパラメータが存在する場合、ノードにUnified Communications Manager設定されている設定は、アップグレードIM and Presence Serviceプロセス中にサービスノードに設定されている設定を上書きします。サービスノードにIM and Presence Service固有のエンタープライズパラメータは、アップグレード中に保持されます。

アップグレードが完了した後で必要に応じて復元できるように、設定を記録します。

手順

ステップ 1 Cisco Unified CM の管理インターフェイスから、**[システム（System）]** > **[エンタープライズ パラメータ（Enterprise Parameters）]** の順に選択します。

ステップ 2 画面キャプチャを使用して設定した設定を記録し、その情報を保存して、アップグレードの完了後に設定を復元できるようにします。

ステップ 3 Cisco Unified CM IM and Presence の管理インターフェイスから、**[システム（System）]** > **[エンタープライズパラメータ（Enterprise Parameters）]** の順に選択します。

ステップ 4 設定した内容を記録するためにスクリーン キャプチャを取り、アップグレードが完了した後に、設定を復元できるように情報を保存します。

ユーザ レコードのエクスポート

一括管理ツール（BAT）を使用して、ユーザ レコードをエクスポートします。

手順

ステップ 1 Cisco Unified CM Administration から、**[一括管理（Bulk Administration）]** > **[ユーザ（Users）]** > **[ユーザのエクスポート（Export Users）]** の順に選択します。

ステップ 2 **[検索（Find）]** をクリックして、すべてのユーザ レコードを表示します。

ステップ 3 [次へ（Next）] をクリックします。

ステップ 4 **[ファイル名 (File Name)]** テキストボックスにファイル名を入力し、[ファイル形式 (file **format**)] ドロップダウンリストからファイル形式を選択します。

ステップ 5 [ジョブ情報（Job Information）] 領域に、ジョブの説明を入力します。

ステップ 6 ユーザ レコードをすぐにエクスポートする場合は、[今すぐ実行（Run Immediately）] をクリックします。

ステップ 7 [送信（Submit）] をクリックします。

ステップ 8 エクスポートしたファイルをダウンロードするには、**[一括管理（Bulk Administration）]**>**[ファイルをアップロード/ダウンロード（Upload/Download Files）]** を選択します。

ステップ 9 生成したファイルの検索条件を入力し、[**検索（Find**）] をクリックします。

ステップ 10 ダウンロードするファイルに該当するチェックボックスをオンにし、[**選択項目のダウンロード（Download Selected**）] をクリックします。

ステップ 11 [ファイルのダウンロード（File Download）] ポップアップ ウィンドウで、[**保存（Save**）] をクリックします。

ステップ 12 [名前をつけて保存（Save As）] ポップアップ ウィンドウで、ファイルの保存場所を選択して [**保存（Save**）] をクリックします。サーバのファイルをコピーして、リモート PC またはデバイスに保存してください。

IP フォンのファームウェアのアップグレード

アップグレード前のタスクとして、新しいリリースに対応するファームウェアに IP フォンをアップグレードすることができます。アップグレード後に電話機が自動的に新しいファームウェアをダウンロードしますが、アップグレード後の電話機のダウンタイムを最小限に抑えるために、アップグレードの前に制御された方法でエンドポイントに新しいファームウェアファイルを適用することを選択できます。

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

始める前に

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

手順

ステップ 1 Cisco Unified OS の管理から、**[ソフトウェア アップグレード（Software Upgrades）]** > **[インストール/アップグレード（Install/Upgrade）]** の順に選択します。

ステップ 2 ソフトウェアの場所セクションに適切な値を入力し、[次へ（Next）] をクリックします。

ステップ 3 [使用可能なソフトウェア（Available Software）] ドロップダウン リストで、デバイス パッケージ ファイルを選択して、[次へ（Next）] をクリックします。

ステップ 4 MD5 の値が正しいことを確認し、[次へ（Next）] をクリックします。

ステップ 5 警告ボックスで、正しいファームウェアを選択したことを確認し、[インストール（Install）] をクリックします。

ステップ 6 成功メッセージを受信したことを確認します。

（注） クラスタを再起動している場合は、ステップ 8 に進みます。

ステップ 7 TFTP サーバを停止し、再起動します。

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

ステップ 9 Cisco Unified CM Administration から、**[デバイス（Device）] > [デバイスの設定（Device Settings）] > [デバイスのデフォルト（Device Defaults）]** を選択し、TFTP サーバ上の新しいロードについて、特定の [デバイスタイプ（Device Type）] フィールドに対する [ロード情報（Load Information）] と [非アクティブロード情報（Inactive Load Information）] の名前を手動で変更します。

ステップ 10 [保存（Save）] をクリックし、デバイスをリセットします。

重要なサービスの確認

Cisco Unified Real Time Monitoring Tool（RTMT）を使用して、すべての重要なサービスがアクティブになっていることを確認します。

手順

ステップ 1 Unified RTMT インターフェイスから、**[システム（System）] > [サーバ（Server）] > [重要なサービス（Critical Services）]** を選択します。

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

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

ステップ 4 IM and Presence Service の重要なサービスを表示するには、[**IM and Presence Service**] タブをクリックし、ドロップダウンリストからIM and Presence Serviceサービスノードを選択します。

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

Cisco Extension Mobility の非アクティブ化

この手順は、リリース9.x 以前からアップグレードする場合にのみ実行してください。リリース9.x 以前からのアップグレードでは、アップグレードを開始する前に、ノードUnified Communications Managerで Cisco extension mobility を停止する必要があります。

手順

ステップ 1 Cisco Unified Serviceability から、**[ツール（Tools）] > [サービスのアクティブ化（Service Activation）]** を選択します。

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

ステップ 3 **Cisco Extension Mobility** サービスを選択解除します。

ステップ 4 [Stop] をクリックします。

ステップ 5 **Cisco Extension Mobility**サービスを実行している各ノードについて、ステップ 2 ~ 4 を繰り返します。

ステップ 6 これらのサービスを無効にしたすべてのノードのリストを作成します。アップグレードが完了したら、サービスを再起動する必要があります。

IM and Presence Sync Agent の停止

アップグレードのUnified Communications ManagerIM and Presence Service一環としてアップグレードする必要がある場合は、アップグレードIM and Presence Serviceプロセスを開始する前に、Sync Agent サービスを停止する必要があります。

手順

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

ステップ 2 [**サーバ（Server**）] ドロップダウン リストから IM and Presence Service Service ノードを選択し、[**移動（Go**）] をクリックします。

ステップ 3 [**IM and Presence Services**] セクションで [**Cisco Sync Agent**] を選択し、[**停止（Stop**）] をクリックします。

使用可能な共通のパーティション領域を確認する

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

手順

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

ステップ 2 ページの下部にあるテーブルを表示し、共通パーティションに**使用され**ているスペースと**合計領域**を比較します。アップグレードを開始する前に、使用可能な共通パーティションスペースの最小 25 g が必要です。ただし、多数の TFTP データ (デバイスファームウェアロード)、保留音 (MOH) ファイル、または多数のロケールファイルがインストールされている場合は、展開により多くのスペースが必要になることがあります。場合によっては、空き領域の 25 GB が使用可能な場合でも、アップグレードが失敗し、十分なスペースとしてエラーメッセージが表示されないことがあります。回避策は、不要なファイルを削除し、共通のパーティションにさらにスペースを作成することです。

基準値の上限および下限の調節

この手順を使用して、低および高のウォーターマークを調整し、トレースを減らし、不要なログファイルを削除します。トレースの早すぎるパージを避けるために、アップグレード後、基準値の上限と下限を元の値に戻す必要があります。基準値のデフォルトの上限は 85 です。基準値のデフォルトの下限は 80 です。

手順

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

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

ステップ 3 [**Next**] を選択します。

ステップ 4 スライダの値を30に調整します。

ステップ 5 [**System**] タブで、[**LogPartitionHighWaterMarkExceeded**] を右クリックし、[**Set Alert/Properties**] を選択します。

ステップ 6 [**Next**] を選択します。

ステップ 7 スライダの値を40に調整します。

使用可能なディスク領域の最大化

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

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

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

手順

ステップ 1 次のいずれかのオプションを使用して、古い、または使用されていないファームウェアファイルをTFTPディレクトリから手動で削除します。

- Cisco Unified OS管理インターフェイスから、[**Software Upgrade** > **TFTP File Management**] を選択し、不要なファイルを削除します。
- コマンドラインインターフェイスから、`file list tftp`および`file delete tftp`コマンドを使用して、不要なファイルを削除します。
- Cisco Unified OSの管理インターフェイスから、[ソフトウェアのアップグレード] [> **デバイスロード管理**] を選択し、不要なファイルを削除します。

（注） **Show diskusage tftp < sort >**コマンドを実行して、tftpデバイスのロードサイズを確認します。これは、ファイルサイズが降順でソートされます。

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

ステップ 2 前の手順でアップグレードに十分なディスク領域が作成されていない場合にのみ、この手順を実行します。Free Common Space COPファイル（ciscocm.free_common_space_v<latest_version>.cop.sgn）を使用します。

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

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

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

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

アップグレード ファイルの取得

新しいリリースのアップグレードファイル、および必要なアップグレードのCisco Option Package (COP) ファイルをダウンロードする必要があります。

手順

ステップ 1 必要なCOPファイル(存在する場合)を特定するには、この手順の下の表を参照してください。

ステップ 2 Cisco.com からアプリケーションのアップグレード ファイルをダウンロードします。このソフトウェアは、export restricted (K9) および export 無制限バージョン (XU) で使用できます。そのため、正しいファイルを選択していることを確認してください。

- Unified Communications Manager アップグレードファイルをダウンロードするには、https://software.cisco.com に移動して > [**ダウンロードとアップグレード（Download & Upgrade）**] セクションの下にある [**ソフトウェアダウンロード（Software Download）**] リンクをクリックし、[**Unified Communications > Call Control > Cisco Unified Communications Manager（CallManager）** > **<バージョン>** > **の Unified Communications Manager/CallManager/Cisco Unity Connection の更新（Unified Communications Manager/CallManager/Cisco Unity Connection Updates）**に移動します。
- IM and Presence Service サービスアップグレードファイルをダウンロードするには、https://software.cisco.com に移動して> [**ソフトウェアダウンロード（Software Download）**] リンクを [**ダウンロードとアップグレード（Download & Upgrade）**] セクションからクリックします。次に **[Unified Communications] > [Unified Communications アプリケーション（Unified Communications Applications）] > [Presence ソフトウェア（Presence Software）] >**

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

ステップ 3 https://software.cisco.com に移動し、[**ダウンロードとアップグレード（Download & Upgrade**）] セクションにある [**ソフトウェアのダウンロード（Software Download**）] リンクをクリックします。次に、**[Unified Communications]** > **[コール制御（Call Control）]** > **[Cisco Unified Communications Manager (CallManager)]** > ***[<バージョン（Version）>]*** > **[Unified Communications Manager/CallManager/Cisco Unity Connectionユーティリティ（Unified Communications Manager/CallManager/Cisco Unity Connection Utilities）]** に移動して、Unified Communications Manager の COP ファイルをダウンロードします。

ステップ 4 https://software.cisco.com に移動し、[**ソフトウェアのダウンロード（Software Download**）] リンクを [**ダウンロードとアップグレード（Download & Upgrade**）] セクションからクリックします。次に、**[Unified Communications]** > **[Unified Communications アプリケーション（Unified Communications Applications）]** > **[Presence ソフトウェア（Presence Software）]** > **[Unified Communications Manager IM and Presence Service]** > **<バージョン>** > **[Unified Presenceサービス（CUP）の更新（Unified Presence Service (CUP) Updates）]**に移動し、[**UTILS**] を選択して IM and Presence Service の COP ファイルをダウンロードします。

必須 COP ファイル

次の表は、COP ファイルが必要なアップグレード パスを示しています。Cisco Unified OS 管理インターフェイスを使用してアップグレードを開始する前、または Prime Collaboration Deployment（PCD）ツールを使用してアップグレードまたは移行を開始する前に、各ノードに COP ファイルをインストールする必要があります。PCD を使用している場合は、アップグレードを開始する前に COP ファイルの一括インストールを実行できます。

必要な COP ファイルの詳細については、*COP* ファイルでサポートされるアップグレードおよび移行パスを参照してください。

データベース レプリケーションのタイムアウトを増やす

Unified Communications Managerパブリッシャノードでのみこの手順を実行します。

大規模なクラスタをアップグレードする場合は、より多くの Unified Communications Manager サブスクライバ ノードが複製を要求する時間を十分に確保できるように、データベース レプリケーションのタイムアウト値を大きくします。タイマーの期限が切れると、最初の Unified Communications Manager サブスクライバ ノードと、その期間内に複製を要求した他のすべての Unified Communications Manager サブスクライバ ノードが、Unified Communications Manager データベース パブリッシャ ノードとの間でバッチ データ レプリケーションを開始します。

手順

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

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

ステップ 2 Timeout コマンドを実行します。この場合、timeout はデータベース レプリケーションのタイムアウト (秒単位) です。 **utils dbreplication setrepltimeout** この値は、300 から 3600 までです。

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

プレゼンス冗長グループに対するハイ アベイラビリティの無効化

この手順は、IM and Presence Service サービス ノードにのみ適用されます。IM and Presence Service プレゼンス冗長グループのハイ アベイラビリティを無効にするために使用します。

始める前に

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

手順

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

ステップ 2 **検索**をクリックして、グループを選択します。

ステップ 3 [プレゼンス冗長グループの設定（Presence Redundancy Group Configuration）] ウィンドウで、**[ハイ アベイラビリティを有効にする（Enable High Availability）]** チェックボックスをオフにします。

ステップ 4 [保存（Save）] をクリックします。

ステップ 5 各プレゼンス冗長グループに対して、この手順を繰り返します。

ステップ 6 完了後、さらに変更を行う前に、新しい HA 設定がクラスタ全体にわたって同期されるまで、少なくとも 2 分待機します。

仮想マシンにシリアル ポートを追加する

アップグレードに失敗した場合にログをダンプできるように、仮想マシンにシリアルポートを追加します。

手順

ステップ 1 仮想マシンの電源をオフにします。

ステップ 2 シリアルポートを追加するには、設定を編集します。vSphere クライアントを使用した設定の変更については、製品のユーザ マニュアルを参照してください。

ステップ 3 シリアルポートを .tmp ファイルに接続します。

ステップ 4 仮想マシンの電源をオンにして、アップグレードを続行します。

次のタスク

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

RTMT の高可用性の設定

Cisco Unified Real-Time Monitoring Tool（RTMT）を使用しており、クラスタを構成している場合は、クラスタ全体のアップグレード中の接続損失を回避するために、RTMT のハイアベイラビリティを設定することを推奨します。

手順

ステップ 1 任意の Cisco Unified Communications Manager ノードにログインします。

ステップ 2 Cisco Unified CM の管理から、**[システム（System）]** > **[サービス パラメータ（Service Parameters）]** の順に選択します。

ステップ 3 [**サーバ（Server）**] ドロップダウンから、Unified CM ノードを選択します。

ステップ 4 [**サービス（Service）**] ドロップダウンから、[**Cisco AMC サービス（Cisco AMC service）**] を選択します。

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

ステップ 6 [**Failover Collector**] サービスパラメータで、別のサブスクライバノードを選択します。

ステップ 7 [保存（Save）] をクリックします。

ステップ 8 Cisco Unified Real-Time Monitoring Tool をサブスクライバノードに接続します。

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

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

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

IM and Presence Service をアップグレードした後、この手順を使用して、新しい SQL Server データベースを作成し、新しいデータベースにデータを移行します。

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

Before you begin

データベースの移行は、`MSSQL_migrate_script.sql` スクリプトに依存します。コピーを入手するには、Cisco TAC にお問い合わせください。

Procedure

ステップ 1 外部 Microsoft SQL Server データベースのスナップショットを作成します。

ステップ 2 新しい（空の）SQL Server データベースを作成します。詳細については、『IM and Presence Service データベース セットアップ ガイド』の次の章を参照してください。

a. 「Microsoft SQL Installation and Setup」：アップグレードされた IM と Presence サービスで新しい SQL Server データベースを作成する方法の詳細については、この章を参照してください。

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

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

a. Cisco Unified CM IM and Presence Administration から、**[診断（Diagnostics）] > [システム トラブルシュータ（System Troubleshooter）]** を選択します。

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

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

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

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

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

ステップ 5 外部データベースに依存するサービスをオフにします。

a. [Cisco Unified IM and Presence のサービスアビリティ（Cisco Unified IM and Presence Serviceability）] から、**[ツール（Tools）] > [コントロールセンター-機能サービス（Control Center - Feature Services）]** を選択します。

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

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

Cisco XCP Text Conference Manager

Cisco XCP File Transfer Manager

Cisco XCP Message Archiver

d. [停止（Stop）] をクリックします。

ステップ 6 次のスクリプトを実行して、古いデータベースから新しいデータベースにデータを移行します。`MSSQL_migrate_script.sql`

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

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

a. Cisco Unified CM IM and Presence Administration から、**[診断（Diagnostics）] > [システムトラブルシュータ（System Troubleshooter）]** を選択します。

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

ステップ 8 以前に停止したサービスを開始します。

a. [Cisco Unified IM and Presence のサービスアビリティ（Cisco Unified IM and Presence Serviceability）] から、**[ツール（Tools）] > [コントロールセンター-機能サービス（Control Center - Feature Services）]** を選択します。

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

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

Cisco XCP Text Conference Manager

Cisco XCP File Transfer Manager

Cisco XCP Message Archiver

d. [開始（Start）] をクリックします。

ステップ 9 外部データベースが稼働していることと、すべてのチャット ルームが Cisco Jabber クライアントから認識可能であることを確認します。新しいデータベースが動作していることが確かな場合にのみ、古いデータベースを削除してください。

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。