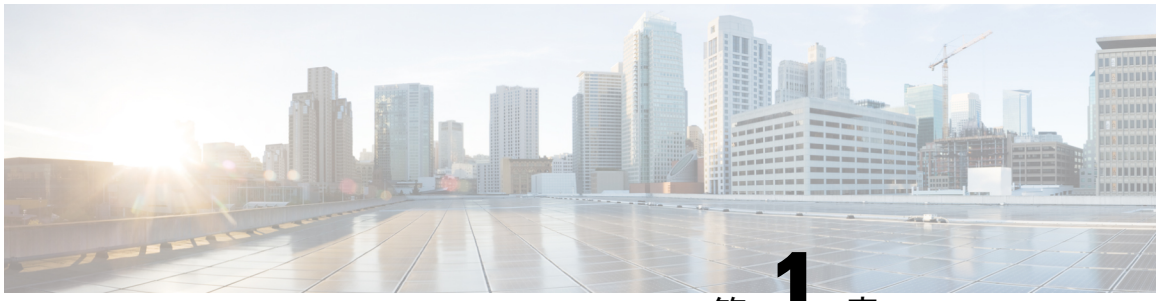
Cisco Unified Communications Manager リリース 15 アドミニストレーション ガイド

最終更新：2024 年 8 月 22 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

【注意】シスコ製品をご使用になる前に、安全上の注意（**www.cisco.com/jp/go/safety_warning/**）をご確認ください。本書は、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。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

目 次



第 1 章

新規および変更情報

新規および変更情報

次の表は、この最新リリースに関するこのガイドでの機能に対する大幅な変更の概要を示したものです。ただし、このリリースに関するガイドの変更点や新機能のなかには、この表に記載されていないものもあります。

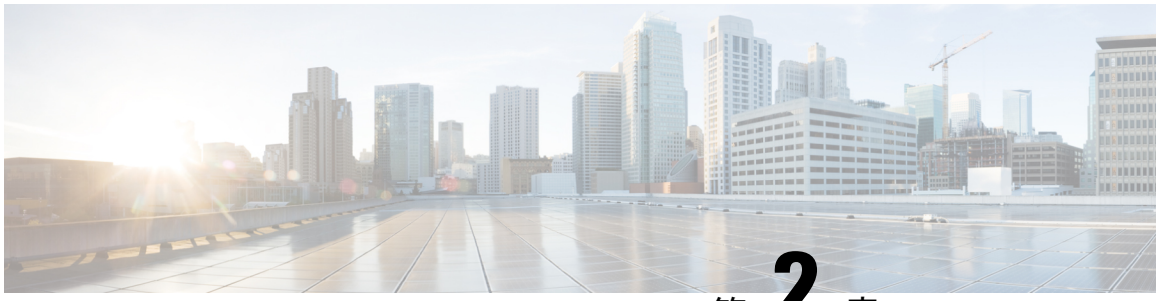
表 *1 : Unified Communications Manager* と *IM* およびプレゼンスサービスでの新機能と変更された動作

	説明	参照先
2024 年 2 月 13 日	リモート監査ログの双方向 x.509 認証に関する情報を更新。	リモート監査ログの転送プロトコルの設定 （145 ページ）
2023 年 12 月 18 日	「IPsec ポリシーの管理」の項に IPsec ポリシーに関するメモを追加。	IPsec ポリシーの管理 （421 ページ）
2023 年 12 月 18 日	「Cisco Unified Serviceability トラブルシューティング ツール」の項に .gzo ファイルに関するメモを追加。	Cisco Unified Serviceability トラブルシューティング ツール （529 ページ）

新規および変更情報

第 I 部

管理の概要



第 2 章

管理の概要

Cisco Unified CM の管理概要

Cisco Unified CM の管理は、Cisco Unified Communications Manager の主要な管理および設定インターフェイスとなる、Web ベースのアプリケーションです。 Cisco Unified CM の管理を使用して、一般的なシステム コンポーネント、機能、サーバ設定、コール ルーティング ルール、電話機、エンド ユーザ、メディア リソースなど、システムの幅広い項目を設定できます。

設定メニュー

Cisco Unified CM の管理の設定ウィンドウは、以下のメニューで編成されています。

- [システム（System）]：このメニューに分類されている設定ウィンドウを使用して、一般的なシステム設定（サーバ情報、NTP 設定、日時グループ、リージョン、DHCP、LDAP 統合、エンタープライズ パラメータなど）を構成します。
- [コール ルーティング（Call Routing）]：このタブに分類されている設定ウィンドウを使用して、Cisco Unified Communications Manager によるコールのルーティング方法に関連する項目（ルート パターン、ルート グループ、ハント パイロット、ダイヤル ルール、パーティション、コール サーチ スペース、電話番号、変換パターンなど）を設定します。
- [メディア リソース（Media Resources）]：このタブに分類されている設定ウィンドウを使用して、メディア リソース グループ、会議ブリッジ、アナンシエータ、トランスコーダなどの項目を設定します。
- [拡張機能（Advanced Features）]：このタブに分類されている設定ウィンドウを使用して、ボイスメール パイロット、メッセージ受信、コール制御エージェント プロファイルなどの機能を設定します。

- [デバイス（Device）]：このタブに分類されている設定ウィンドウを使用して、電話機などのデバイス、IP Phone サービス、トランク、ゲートウェイ、ソフトキーテンプレート、SIP プロファイルを設定します。
- [アプリケーション（Application）]：このタブに分類されている設定ウィンドウを使用して、Cisco Unified JTAPI、Cisco Unified TAPI、Cisco Unified Real-Time Monitoring Tool などのプラグインをダウンロードおよびインストールします。
- [ユーザ管理（User Management）]：[ユーザ管理（User Management）] タブに分類されている設定ウィンドウを使用して、システムのエンド ユーザおよびアプリケーション ユーザを設定します。
- [一括管理（Bulk Administration）]：一括管理ツールを使用して、多数のエンドユーザやデバイスを同時にインポートおよび設定します。
- [ヘルプ（Help）]：このメニューをクリックすることで、オンライン ヘルプ システムにアクセスできます。 オンライン ヘルプ システムには、システム上の各種設定ウィンドウの設定を構成する際に役立つドキュメントが含まれています。

オペレーティング システムの管理の概要

[Cisco Unified Communications オペレーティング システムの管理（Cisco Unified Communications Operating System Administration）] を使用して、オペレーティング システムの設定と管理、および以下の管理タスクを実行します。

- ソフトウェアとハードウェアのステータスを確認する
- IP アドレスの確認と更新を行う
- 他のネットワーク デバイスに ping を送信する
- NTP サーバを管理する
- システム ソフトウェアおよびオプションをアップグレードする
- ノードのセキュリティを管理する（IPSec や証明書を含む）
- リモート サポート アカウントを管理する
- システムを再起動する

オペレーティング システムのステータス

以下のものを含め、各種のオペレーティング システム コンポーネントのステータスを確認できます。

- クラスタおよびノード
- ハードウェア
- ネットワーク
- System
- インストールされているソフトウェアとオプション

オペレーティング システムの設定

オペレーティング システムの次の設定を表示し、更新できます。

- [IP]：アプリケーションのインストール時に入力したIPアドレスおよびDHCPクライアントの設定を更新します。
- [NTP サーバの設定（NTP Server Settings）]：外部 NTP サーバの IP アドレスの設定、および NTP サーバの追加を行います。
- [SMTP 設定（SMTP settings）]：オペレーティング システムが E メール通知の送信に使用する Simple Mail Transfer Protocol（SMTP）ホストを設定します。

オペレーティング システムのセキュリティ設定

セキュリティ証明書およびIPsecの設定を管理できます。 [セキュリティ（Security）]メニューでは、次のセキュリティ オプションを選択できます。

- [証明書の管理（Certificate Management）]：証明書および証明書署名要求（CSR）を管理します。 証明書の表示、アップロード、ダウンロード、削除、および再作成を行うことができます。 [証明書の管理（Certificate Management）] を使用して、ノード上の証明書の有効期限をモニタすることもできます。
- [IPsec の管理（IPsec Management）]：既存の IPsec ポリシーの表示や更新、新規の IPsec ポリシーとアソシエーション設定を行います。

ソフトウェア アップグレード

オペレーティング システムで実行中のソフトウェア バージョンをアップグレードしたり、特定のソフトウェア オプション（Cisco Unified Communications オペレーティング システム ロケール インストーラ、ダイヤル プラン、TFTP サーバ ファイルなど）をインストールできます。

[インストール/アップグレード（Install/Upgrade）]メニュー オプションで、ローカル ディスクまたはリモート サーバからシステム ソフトウェアをアップグレードできます。 アップグレードしたソフトウェアは非アクティブなパーティションにインストールされ、その後でシステムの再起動とパーティションの切り替えができます。これにより、システムで新しいソフトウェア バージョンが実行されます。 詳細については、『*Upgrade Guide for the Cisco Unified Communications Manager*』（http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-guides-list.html）を参照してください。

（注） Cisco Unified Communications オペレーティング システムのインターフェイスと CLI に含まれるソフトウェア アップグレード機能を使用して、すべてのソフトウェアのインストールとアップグレードを実行する必要があります。 このシステムでアップロードおよび処理できるソフトウェアは、シスコによって承認されたものだけです。 サードパーティー製またはWindowsベースのソフトウェア アプリケーションはインストールまたは使用できません。

サービス

このアプリケーションでは、次のオペレーティング システム ユーティリティを使用できます。

- ping：他のネットワーク デバイスとの接続を確認します。
- リモート サポート：シスコのサポート担当者がシステムへのアクセスに使用できるアカウントを設定します。 このアカウントは、指定した日数が経過すると自動的に失効します。

CLI

CLI には、オペレーティング システムからアクセスすることも、サーバへのセキュア シェル接続を使用してアクセスすることもできます。 詳細については、『*Command Line Interface Reference Guide for Cisco Unifed Communications Solutions*』（http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html）を参照してください。

認証済み Network Time Protocol のサポート

Cisco Unified Communications Manager リリース 12.0(1) では、Unified Communications Manager の認証済み Network Time Protocol（NTP）機能がサポートされています。 このサポートは、Unified Communications Manager へのセキュアな NTP サーバ接続を確立するために追加されています。 以前のリリースでは、NTP サーバに対する Unified Communications Manager の接続はセキュアではありませんでした。

この機能は、対称キーベースの認証に基づいており、NTPv3 および NTPv4 サーバによってサポートされています。 Unified Communications Manager は、SHA1 ベースの暗号化のみをサポートしています。 SHA1 ベースの対称キーのサポートは、NTP バージョン 4.2.6 以降で利用できます。

- 対称キー
- 認証なし

NTP サーバの認証ステータスは、**Cisco Unified OS Administration**アプリケーションの管理 CLI または **[NTP サーバの一覧（NTP Server List）]** ページで確認できます。

自動キー認証済み Network Time Protocol のサポート

Cisco Unified Communications Manager は、自動キー機能（公開キー インフラストラクチャベースの認証）による Network Time Protocol（NTP）認証もサポートしています。 この機能は、パブリッシャ ノードでのみ適用できます。

RedHat は自動キーよりも対称キー認証を推奨しています。 詳細については、https://access.redhat.com/support/cases/#/case/01871532 を参照してください。

この機能は、コモン クライテリア認定のために PKI ベースの認証が必須であるため追加されました。

Cisco Unified Communications Manager でコモン クライテリア モードを有効にしている場合にのみ、NTP サーバで IFF ID スキームによる PKI ベースの認証を設定できます。

Cisco Unified Communications Manager で、対称キーまたは PKI ベースの NTP 認証を有効にできます。

PKI 対応サーバで対称キーを有効にしようとすると、次の警告メッセージが表示されます。

警告 Autokeyを使用したNTP認証が現在有効になっており、対称キーを有効にする前に無効にする必要があります。（NTP authentication using Autokey is currently enabled and must be disabled before the symmetric key is enabled.） コマンド「utils ntp auth auto-key disable」を使用してNTP認証を無効にしてから、このコマンドを再試行してください。（Use the command 'utils ntp auth auto-key disable' to disable NTP authentication, then retry this command.）

対称キー対応サーバで Autokey を有効にしようとすると、次の警告メッセージが表示されます。

警告 対称キーを使用するNTP認証が現在有効になっており、Autokeyを有効にする前に無効にする必要があります。（NTP authentication using symmetric key is currently enabled and must be disabled before Autokey is enabled.） コマンド「utils ntp auth symmetric-key disable」を使用してNTP認証を無効にしてから、このコマンドを再試行してください。（Use the command 'utils ntp auth symmetric-key disable' to disable NTP authentication, then retry this command.）

（注） NTP サーバには ntp バージョン 4 と rpm バージョン ntp-4.2.6p5-1.el6.x86_64.rpm 以上が必要です。

NTP サーバの認証ステータスは、Cisco Unified OS の管理アプリケーションの管理 CLI または [NTPサーバの一覧(NTP Server List)] ページで確認できます。

Cisco Unified Serviceability の概要

Cisco Unified Serviceability は、管理者がシステムを管理する際の、サービス、アラーム、支援ツールのホストを提供する、Web ベースのトラブルシューティング ツールです。 Cisco Unified Serviceability が提供する機能を利用して、管理者は以下の作業を行うことができます。

- サービスの開始と停止：管理者はシステムを管理する上で役立つさまざまなサービスを設定できます。 たとえば、Cisco CallManager Serviceability RTMT サービスを開始することにより、管理者は Real-Time Monitoring Tool を使ってシステムの正常性をモニタできます。
- SNMP：アプリケーション層プロトコルである SNMP を使用すると、ノードやルータなどのネットワーク デバイス間の管理情報を簡単に交換できます。 TCP/IP プロトコル スイートの一部である SNMP を使用すると、管理者はリモートでネットワークのパフォーマンス

を管理し、ネットワークの問題を検出および解決し、ネットワークの拡張計画を立てることができます。

- アラーム：アラームは、システムの実行時のステータスと状態に関する情報を提供するため、システムに関する問題をトラブルシューティングできます。
- トレース：トレース ツールは、音声アプリケーションの問題をトラブルシューティングするのに役立ちます。
- Cisco Serviceability Reporter：Cisco Serviceability Reporter は、Cisco Unified Serviceability 内で日次レポートを生成します。
- SNMP：アプリケーション層プロトコルである SNMP を使用すると、ノードやルータなどのネットワーク デバイス間の管理情報を簡単に交換できます。 TCP/IP プロトコル スイートの一部である SNMP を使用すると、管理者はリモートでネットワークのパフォーマンスを管理し、ネットワークの問題を検出および解決し、ネットワークの拡張計画を立てることができます。
- CallHome：Cisco Unified Communications Manager の Call Home 機能を設定し、Cisco Unified Communications Manager が通信し、診断アラート、インベントリおよびその他のメッセージを Smart Call Home バックエンド サーバに送信できるようにします。

その他の管理インターフェイス

Cisco Unified Serviceability を使用して、サービスを開始し以下の他の管理インターフェイスを使用できます。

- Real-Time Monitoring Tool：Real-Time Monitoring Tool は、システムの正常性をモニタするために利用できる Web ベースのインターフェイスです。 RTMT を使用して、アラームやカウンタを確認したり、システムの正常性に関する詳細情報が記載されたレポートを表示したりできます。
- Dialed Number Analyzer：Dialed Number Analyzer は、管理者がダイヤル プランの問題をトラブルシューティングする際に役立つ、Web ベースのインターフェイスです。
- Cisco Unified CDR Analysis and Reporting：CDR Analysis and Reporting は、システムで行われたコールの詳細を記録したレコードを収集します。

Cisco Unified Serviceability の使用方法の詳細については、『*Cisco Unified Serviceability Administration Guide*』（http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html）を参照してください。

Cisco Unified Reporting の概要

Cisco Unified Reporting Web アプリケーションは、クラスタ データをトラブルシューティングまたは検査するための統合レポートを生成します。 このアプリケーションには、Unified

Communications Manager および Unified Communications Manager IM and Presence Service のコンソールでアクセスできます。

このツールは、クラスタ データのスナップショットを簡単に作成する方法を提供します。 このツールは、既存のソースからのデータの収集、データの比較、および異常の報告を行います。 Cisco Unified Reporting でレポートを生成すると、レポートでは、1 台以上のサーバにある 1 つ以上のソースからのデータを結合して、1 つの出力ビューを作成します。 システムを管理する際には、たとえば以下のレポートを表示して利用できます。

- [Unified CM クラスタ概要（Unified CM Cluster Overview）]：Cisco Unified Communications Manager and IM and Presence Service のバージョン、サーバのホスト名、ハードウェアの詳細といったクラスタのスナップショットを取得するときに、このレポートを参照します。
- [電話機機能リスト（Phone Feature List）]：機能を設定する際は、このレポートを表示します。 このレポートは、どの電話機がどの Cisco Unified Communications Manager 機能をサポートしているかを一覧します。
- [回線未使用の Unified CM 電話（Unified CM Phones Without Lines）]：電話回線を使用していない、クラスタ内の電話機を確認するには、このレポートを表示します。

Cisco Unified Reporting が提供するレポートをすべて網羅したリスト、およびこのアプリケーションの使用方法については、『*Cisco Unified Reporting Administration Guide*』（http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html）を参照してください。

ディザスタ リカバリ システムの概要

ディザスタ リカバリ システム（DRS）は、[Cisco Unified Communications Manager 管理（Cisco Unified Communications Manager Administration）] から呼び出すことができるシステムで、完全なデータ バックアップおよび復元の機能を提供します。 ディザスタ リカバリ システムでは、定期的にスケジュールされた自動データ バックアップまたはユーザ起動のデータ バックアップを実行できます。

DRS は、プラットフォームのバックアップ/復元の一環として、独自の設定（バックアップ デバイス設定およびスケジュール設定）を復元します。 DRS は `drfDevice.xml` ファイルと `drfSchedule.xml` ファイルをバックアップおよび復元します。 これらのファイルとともにサーバを復元するときは、DRS バックアップ デバイスおよびスケジュールを再設定する必要がありません。

ディザスタ リカバリ システムには、次の機能があります。

- バックアップおよび復元タスクを実行するためのユーザ インターフェイス。
- バックアップおよび復元機能を実行するための分散システム アーキテクチャ。
- バックアップのスケジューリング。
- 物理的なテープ ドライブまたはリモート SFTP サーバへのバックアップのアーカイブ。

一括管理ツールの概要

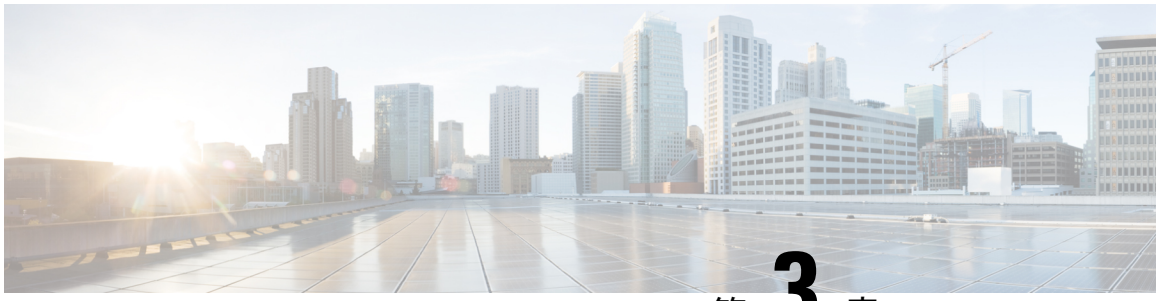
Cisco Unified Communications Manager 内にエンティティを設定するには、Unified CM の管理の [一括管理（Bulk Administration）] メニューおよびサブメニュー オプションで一括管理ツールを使用します。

Unified Communications Manager の一括管理ツール（BAT）は Web ベースのアプリケーションであり、管理者が Unified Communications Manager データベースに対する一括トランザクションを行うために使用できます。 BAT では、多数の同じような電話、ユーザ、またはポートを同時に追加、更新、削除できます。 Cisco Unified CM の管理を使用する場合、データベース トランザクションごとに個々の手動操作が必要になりますが、BAT はこのプロセスを自動化し、追加、更新、削除の操作を短時間で実行できるようにします。

以下のタイプのデバイスとレコードを処理する場合は BAT を使用できます。

- Cisco IP Phone、ゲートウェイ、電話機、Computer Telephony Interface（CTI）ポート、H.323 クライアントの追加、更新、削除
- ユーザ、ユーザ デバイス プロファイル、Cisco Unified Communications Manager Assistant マネージャおよびアシスタントの追加、更新、削除
- 強制承認コードとクライアント マター コードの追加、削除
- コール ピックアップ グループの追加、削除
- リージョン マトリクスの実装、実装解除
- アクセス リストの挿入、削除、エクスポート
- リモート宛先およびリモート宛先プロファイルの挿入、削除、エクスポート
- インフラストラクチャ デバイスの追加

一括管理ツールの使用方法の詳細については、『*Bulk Administration Guide for Cisco Unified Communications Manager*』を参照してください。



第 3 章

はじめに

管理インターフェイスへのログイン

システム内の管理インターフェイスのいずれかにサインインする場合に、次の手順を使用します。

手順

ステップ 1 ご使用の Web ブラウザで、Unified Communications Manager インターフェイスを開きます。

ステップ 2 [ナビゲーション（Navigation）]ドロップダウン リストから管理インターフェイスを選択します。

ステップ 3 [移動（Go）]をクリックします。

ステップ 4 ユーザ名とパスワードを入力します。

ステップ 5 [ログイン（Login）]をクリックします。

管理者またはセキュリティ パスワードのリセット

管理者パスワードを消失し、システムにアクセスできない場合は、次の手順を使用してパスワードをリセットします。

（注） IM and Presence ノードのパスワードを変更する場合は、管理者パスワードをリセットする前に、すべての IM and Presence ノードの Cisco Presence Engine サービスを停止します。 パスワードをリセットした後に、すべてのノードの Cisco Presence Engine サービスを再起動します。 PE が停止されるとプレゼンスの問題が発生する可能性があるため、このタスクはメンテナンス中に実行してください。

始める前に

- この手順を実行するノードに物理的にアクセスできる必要があります。
- どの時点でも、CD または DVD メディアを挿入するように求められたら、VMWare サーバ用の vSphere クライアントを用いて ISO ファイルをマウントする必要があります。 指示については、「『Adding DVD or CD Drives to a Virtual Machine』」 https://www.vmware.com/support/ws5/doc/ws_disk_add_cd_dvd.htmlを参照してください。
- セキュリティ パスワードは、クラスタ内のすべてのノードで一致している必要があります。 セキュリティ パスワードは、すべてのマシン上で変更してください。変更していない場合、クラスタ ノードが通信不能になります。

手順

ステップ 1 次のユーザ名とパスワードを使用して、パブリッシャ ノードで CLI にサインインします。

a) ユーザ名：**pwrecovery**
b) パスワード：**pwreset**

ステップ 2 任意のキーを押して続行します。

ステップ 3 ディスク ドライブに有効な CD または DVD が入っている場合、または ISO ファイルをマウントしてある場合は、VMWare クライアントから取り出します。

ステップ 4 任意のキーを押して続行します。

ステップ 5 有効な CD または DVD をドライブに挿入するか、ISO ファイルをマウントします。

（注） このテストでは、データ専用のディスクまたは ISO ファイルを使用する必要があります。

ステップ 6 最後のステップが確認されると、次のいずれかのオプションを入力して続行するように指示されます。

- **a** を入力して、管理者パスワードをリセットします。
- セキュリティ パスワードをリセットする場合は、**s** を入力します。

（注） セキュリティパスワードを変更したら、クラスタ内の各ノードをリセットする必要があります。 ノードをリブートしない場合、システム サービスで問題が発生するほか、サブスクライバ サーバ上の管理ウィンドウで問題が発生します。

ステップ 7 新しいパスワードを入力し、確認のためにもう一度入力します。

管理者のクレデンシャルは、先頭がアルファベットで 6 文字以上必要です。英数字、ハイフン、およびアンダースコアを使用できます。

ステップ 8 新しいパスワードの強度が検証された後、パスワードがリセットされ、任意のキーを押してパスワード リセット ユーティリティを終了するように指示されます。

異なる管理者パスワードを設定する場合は、CLI コマンド **set password** を使用します。 詳細については、『*Command Line Interface Reference Guide for Cisco Unified Solutions*』（http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html）を参照してください。

システムのシャットダウンまたは再起動

設定を変更した後などにシステムをシャットダウンまたは再起動する必要がある場合、次の手順を使用します。

始める前に

仮想マシンからサーバのシャットダウンおよび再起動が強制されると、ファイル システムが破損する可能性があります。 強制シャットダウンを回避します。代わりに、この手順の実行後または CLI からの **utils system shutdown** の実行後に、サーバが適切にシャットダウンするまで待ちます。

（注） VMware 管理ツール (vCenter または Embedded Host Client) から仮想マシンのシャットダウンまたは再起動を強制する場合:

- 12.5(1)SU3 以前のバージョンでは、これは不適切なシャットダウンや再起動となり、ファイル サイズが破損する可能性があります。 不適切なシャットダウンが system-history.log に表示されます。 代わりに、シャットダウン CLI コマンドを使用して、段階的にシャットダウン/再起動してください (このコマンドは、適切なシャットダウン/再起動として system-history.log に表示されます)。

手順

ステップ 1 [Cisco Unified OS の管理] から、**[設定]** > **[バージョン]** を選択します。

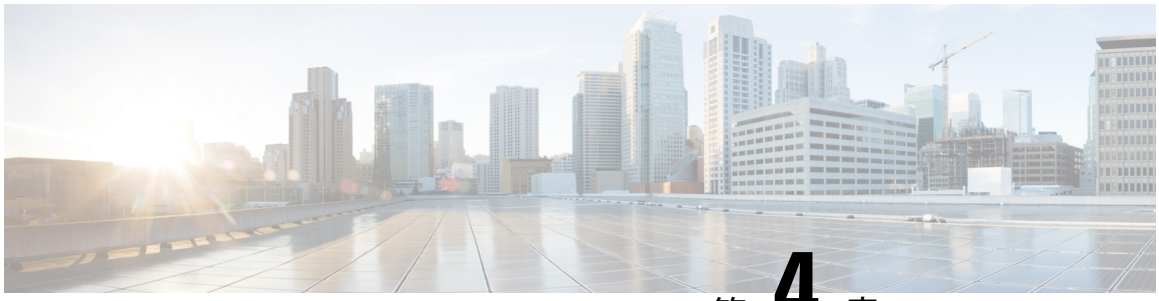
ステップ 2 次のいずれかの操作を実行します。

- すべてのプロセスを停止し、システムをシャットダウンするには、[シャットダウン（Shutdown）]をクリックします。

- すべてのプロセスを停止し、システムを再起動するには、[再起動（Restart）]をクリックします。

第 II 部

ユーザの管理



第 4 章

ユーザ アクセスの管理

ユーザ アクセスの概要

次の項目を設定して、Cisco Unified Communications Manager に対するユーザ アクセスを管理します。

- [アクセス制御グループ（Access Control Groups）]
- [ロール（Roles）]
- [ユーザ ランク（User Rank）]

アクセス制御グループの概要

アクセス制御グループは、ユーザのリストと、それらのユーザに割り当てられているロールのリストです。 エンド ユーザ、アプリケーション ユーザ、または管理者ユーザをアクセス制御グループに割り当てると、そのユーザは、そのグループに関連付けられているロールのアクセス権限を取得します。類似するアクセス権限を持つユーザを、必要なロールとアクセス許可のみを含むアクセス制御グループに割り当てることによって、システム アクセスを管理できます。

アクセス制御グループには、次の 2 つのタイプがあります。

- 標準アクセス制御グループ：これらは定義済みのデフォルト グループであり、一般的な導入ニーズを満たすロールが割り当てられています。 標準グループ内のロール割り当てを編集することはできません。 ただし、ユーザの追加または削除、ユーザのランク要件の編集

は可能です。標準アクセス制御グループのリストと、それらに関連付けられているロールについては、「標準ロールとアクセス制御グループ（36ページ）」を参照してください。

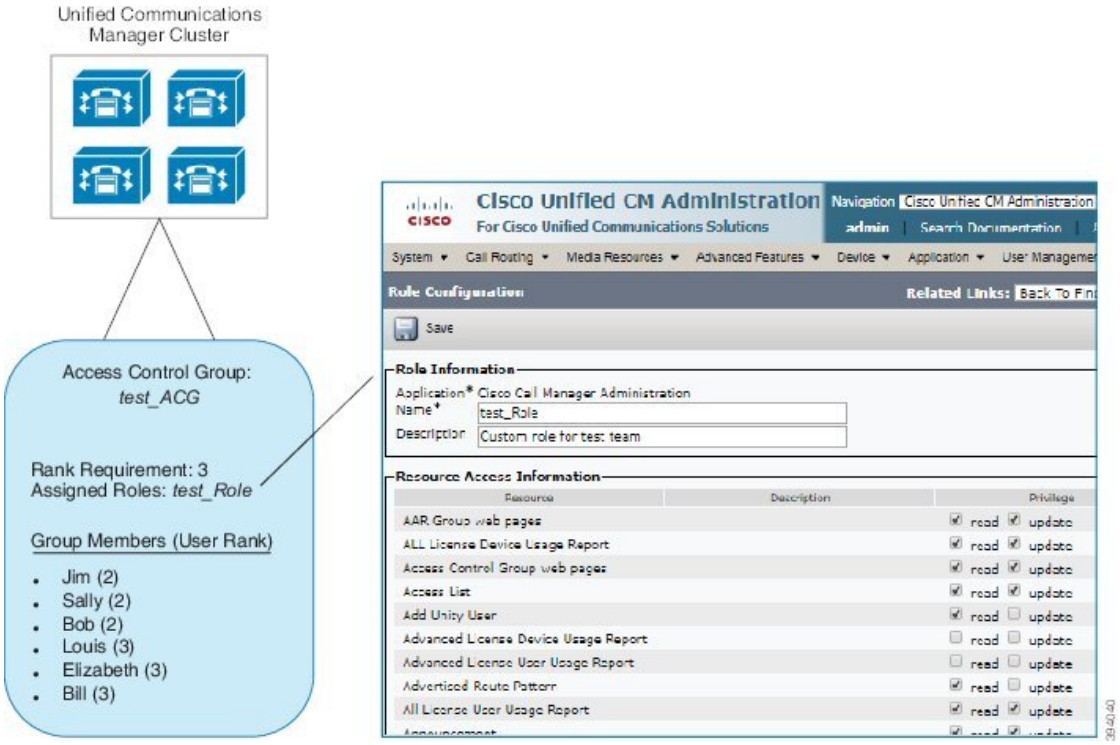
- カスタムアクセス制御グループ：必要条件を満たすロールの権限が標準のグループに含まれていない場合は、独自のアクセス制御グループを作成します。

ユーザランクのフレームワークによって、ユーザの割り当てが可能なアクセス制御グループに対する一連の制御が提供されます。アクセス制御グループにユーザを割り当てるためには、そのグループの最小ランク要件をユーザが満たしている必要があります。たとえば、ユーザランクが 4 のエンドユーザは、最小ランク要件が 4 から 10 までのアクセス制御グループにのみ割り当てることができます。最小ランク要件が 1 のグループに割り当てることはできません。

例：アクセス制御グループを使用したロールの権限

次の例は、テストチームのメンバーがアクセス制御グループ **test_ACG** に割り当てられているクラスタを示しています。右側のスクリーンキャプチャには、このアクセス制御グループに関連付けられているロールである test_Role のアクセス設定が表示されています。また、このアクセス制御グループの最小ランク要件は3であるため、グループに参加するには、グループのすべてのメンバーのランクが 1 以上 3 以下であることが必要です。

図 *1:* アクセス制御グループを使用したロールの権限



ロールの概要

ユーザは、そのユーザがメンバーとなっているアクセス制御グループに関連付けられたロールを介して、システムアクセス権限を取得します。 各ロールには、Cisco Unified CM Administration または CDR Analysis and Reporting などの特定のリソースまたはアプリケーションに割り当てられた一連の権限が含まれています。 Cisco Unified CM Administration などのアプリケーションの場合、ロールには、アプリケーション内の特定の GUI ページを表示または編集できるアクセス許可が含まれている場合があります。 リソースまたはアプリケーションに割り当てることができるアクセス許可には、次の 3 つのレベルがあります。

- [読み取り（Read）]：ユーザがリソースの設定を表示することを許可します。
- [更新（Update）]：ユーザはリソースの設定を編集できます。
- [アクセスなし（No Access）]：ユーザが読み取りと更新のどちらのアクセス権も持っていない場合、そのユーザは、特定のリソースの設定を表示も編集もできません。

ロール タイプ

ユーザをプロビジョニングする場合は、適用するロールを決定してから、そのロールを含むアクセス制御グループにユーザを割り当てる必要があります。 Cisco Unified Communications Manager には、主に 2 つのロール タイプがあります。

- 標準ロール：一般的な展開のニーズを満たすように設計された、プレインストールされたデフォルトのロールです。 標準ロールの権限を編集することはできません。
- カスタム ロール：必要な権限を持つ標準ロールがない場合に、カスタム ロールを作成します。 さらに細かいレベルのアクセス制御が必要な場合は、高度な設定を適用して、管理者がキーのユーザ設定を編集できるように制御することができます。 詳細については、該当する項を参照してください。

高度なロール設定

カスタマイズされたロールを作成する際に、**[アプリケーション ユーザ（Application User）]** と **[エンド ユーザ（End User）]** 設定ウィンドウで選択されたフィールドに、詳細レベルの制御を追加できます。

[高度なロール設定（Advanced Role Configuration）]ウィンドウでは、Cisco Unified CM Administration へのアクセスを設定する一方で、次のようなタスクの使用を制限できます。

- ユーザの追加
- パスワードを編集
- ユーザランクの編集
- アクセス制御グループの編集

次の表に、この構成で適用できるその他のコントロールを詳しく示します。

表 *2:* 高度なリソースアクセス情報

高度なリソース	アクセス制御
権限情報	アクセス制御グループを追加または編集する機能を制御します： • [表示（View）]：ユーザは、アクセス制御グループを表示することはできますが、追加、編集、または削除することはできません。 • [更新（Update）]：ユーザは、アクセス制御グループを追加、編集、または削除できます。 （注） 両方の値が選択されていないと、[権限情報（Permission Information）]セクションは使用できません。 （注） **表示 (View)**を選択すると、**ユーザが[ユーザ (user)]フィールドの権限情報を更新できるように いいえ (No)**に設定され、無効になります。 このフィールドを編集できるようにする場合は、**アクセス許可情報**フィールドを**更新**するように設定する必要があります。
ユーザは自分のユーザの権限情報を更新できる	ユーザが自分のアクセス権を編集できるかどうかを制御します。 • **はい (Yes)**: ユーザは自分のアクセス権情報を更新できます。 • **いいえ (No)**: ユーザは自分のアクセス権情報を更新できません。ただし、ユーザは同じユーザまたは下位レベルのユーザのアクセス権情報を表示または変更できます。 （注） **[ユーザは自分のユーザの権限情報を更新できる（User can update Permissions Information for own user）]**フィールドが**いいえ (No)**に設定され、**権限情報(Permission information)**の**更新 (Update)** チェックボックスがオフになっている場合は無効になります。
[ユーザ ランク（User Rank）]	ユーザランクを変更する機能を制御します。 • [表示（View）]：ユーザは、ユーザ ランクを表示できますが、変更することはできません。 • [更新（Update）]：ユーザは、ユーザ ランクを変更できます。 （注） 両方の値が選択されていないと、[ユーザランク（User Rank）]セクションは使用できません。 （注） **表示 (View)**を選択すると、**ユーザが[ユーザ (user)フィールドのユーザランクを更新できるように いいえ (No)**に設定され、無効になります。 このフィールドを編集できるようにする場合は、**ユーザランク**フィールドを**更新**するように設定する必要があります。

高度なリソース	アクセス制御
ユーザは自分のユーザのランクを更新できる	ユーザが自分のユーザランクを編集できるかどうかを制御します。 • **はい**: ユーザは自分のユーザランクを更新できます。 • **いいえ** : ユーザは自分のユーザランクを更新できません。 ただし、ユーザは同じユーザまたは下位レベルのユーザのランクを表示または変更できます。 （注） **[ユーザは自分のユーザのランクを更新できる（User can update User Rank for own user）]** フィールドが**いいえ (No)**に設定され、**ユーザランク**の**更新 (Update)** チェックボックスがオフになっている場合は無効になります。
新規ユーザの追加	新しいユーザを追加する機能を制御します。 • [はい（Yes）] : ユーザは、新しいユーザを追加できます。 • [いいえ（No）] : [新規追加（Add New）]ボタンを使用できません。
[パスワード（Password）]	パスワードを変更する機能を制御します。 • **はい** - ユーザーは**アプリケーションユーザー情報**セクションでユーザーパスワードを変更できます。 • **いいえ** - **アプリケーションユーザー情報**セクションの**パスワード**および**パスワードの確認入力**は使用できません。

ユーザ ランクの概要

ユーザ ランクのアクセス制御では、管理者がエンド ユーザやアプリケーション ユーザに提供できるアクセス レベルに対する一連の制御を行います。

エンド ユーザやアプリケーション ユーザをプロビジョニングする場合、管理者は各ユーザのユーザ ランクを割り当てる必要があります。 管理者は、各アクセス制御グループにもユーザ ランクを割り当てる必要があります。 Conttrol グループにアクセスするユーザを追加する場合、管理者は、ユーザのユーザのランク要件がグループのランク要件を満たしているグループにのみユーザを割り当てることができます。 たとえば、あるユーザのユーザランクが 3 の場合、ユーザランク要件が 3 ～ 10 であるアクセス制御グループに割り当てることはできますが、ユーザランク要件が 1 または 2 であるアクセス制御グループに割り当てることはできません。

管理者は、[ユーザ順位の**設定**] ウィンドウ内に独自のユーザランク階層を作成し、ユーザをプロビジョニングし、アクセス制御グループを使用して、その階層を使用することができます。 ユーザランクの階層を設定しない場合や、ユーザをプロビジョニングするとき、または conrol グループにアクセスするときにユーザランクの設定を指定しない場合は、すべてのユーザとアクセス制御グループにはデフォルトのユーザランク 1 (可能な限り高いランク) が割り当てられます。

ユーザ アクセスの前提条件

ユーザに必要なアクセス レベルを判断できるよう、ユーザのニーズを確認してください。ユーザが必要とするアクセス権限を与える一方で、ユーザがアクセスすべきではないシステムへのアクセス権を付与しないよう、ロールを割り当てる必要があります。

新しいロールとアクセス コントロール グループを作成する前に、標準のロールとアクセス コントロール グループの一覧を確認して、既存のアクセス コントロール グループに必要なロールとアクセス権限があるかどうかを確認します。詳細については、標準ロールとアクセス制御グループ （36 ページ）を参照してください。

ユーザ アクセスの設定タスク フロー

以下のタスクを実行して、ユーザ アクセスを設定します。

始める前に

デフォルトのロールとアクセス制御グループを使用する場合は、カスタマイズされた役割を作成するタスクをスキップし、制御グループにアクセスできます。ユーザーを既存のデフォルトのアクセス制御グループに割り当てる場合があります。

手順

	コマンドまたはアクション	目的
ステップ 1	ユーザ ランク階層の設定 （25 ページ）	ユーザ ランク階層を設定します。 このタスクをスキップすると、すべてのユーザとアクセス コントロール グループには、デフォルトのユーザ ランク 1（最高ランク）が割り当てられます。
ステップ 2	カスタム ロールの作成 （25 ページ）	必要なアクセス権限がデフォルト ロールに割り当てられていない場合は、カスタムロールを作成します。
ステップ 3	管理者の高度なロール設定 （26 ページ）	これはオプションです。 カスタムロールの高度な権限を使用すると、主な設定に対する管理者の編集権限を制御することができます。
ステップ 4	アクセス制御グループの作成 （27 ページ）	デフォルトのグループに必要なロールが割り当てられていない場合は、カスタム アクセス コントロール グループを作成します。

	コマンドまたはアクション	目的
ステップ 5	アクセス制御グループへのユーザの割り当て （28 ページ）	標準またはカスタムのアクセス制御グループに対してユーザを追加または削除します。
ステップ 6	アクセス制御グループの重複する特権ポリシーの設定 （29 ページ）	これはオプションです。 この設定は、権限が競合する複数のアクセス コントロール グループにユーザが割り当てられている場合に使用します。

ユーザ ランク階層の設定

カスタムのユーザ ランク階層を作成するには、この手順を使用します。

（注） ユーザ ランク階層を設定しない場合は、すべてのユーザおよびアクセス制御グループにデフォルトで 1（最高ランク）が割り当てられます。

手順

ステップ 1 Cisco Unified CM Administration から、**[ユーザ管理（User Management）]** > **[ユーザ設定（User Settings）]** > **[ユーザランク（User Rank）]** を選択します。

ステップ 2 [新規追加] をクリックします。

ステップ 3 [ユーザランク（User Rank）]ドロップダウン メニューから、1 ～ 10 のランク設定を選択します。 最も高いランクは 1 です。

ステップ 4 [ランク名（Rank Name）]と [説明（Description）]を入力します。

ステップ 5 **[保存]** をクリックします。

ステップ 6 ユーザ ランクをさらに追加するには、この手順を繰り返します。
ユーザおよびアクセス制御グループにユーザ ランクを割り当てることで、ユーザをどのグループに割り当てることができるかを制御できます。

カスタム ロールの作成

カスタマイズされた権限で新しいロールを作成するには、この手順を使用します。 必要な権限を備えた標準のロールがない場合に、この方法を使用できます。 ロールを作成する方法は2つあります。

- 新規のロールを白紙の状態から作成して設定するには、[新規追加（Add New）] ボタンを使用します。

- 必要なアクセス権限に近いアクセス権限が既存のロールにある場合は、[コピー（Copy）]ボタンを使用します。 既存のロールの権限を、編集可能な新しいロールにコピーできます。

手順

ステップ 1 Cisco Unified CM Administration で、**[ユーザ管理（User Management）] > [ユーザ設定（User Settings）] > [権限（Role）]** をクリックします。

ステップ 2 次のいずれかを実行します。

- 新しいロールを作成するには、**[新規追加（Add New）]** をクリックします。 このロールを関連付ける [アプリケーション（Application）]を選択し、[次へ(Next)] をクリックします。
- 既存のロールから設定をコピーするには、[検索（Find）]をクリックして、既存のロールを開きます。 [コピー（Copy）]をクリックし、新しいロールの名前を入力します。 **OK**をクリックします。

ステップ 3 このロールの [名前（Name）]と [説明（Description）]を入力します。

ステップ 4 リソースごとに、該当するチェックボックスをオンにします。

- ユーザがリソースの設定を表示できるようにする場合には、[読み取り（Read）]チェックボックスをオンにします。
- ユーザがリソースの設定を編集できるようにする場合は、[更新（Update）]チェックボックスをオンにします。
- リソースに対するアクセスを提供しない場合は、両方のチェックボックスをオフにします。

ステップ 5 この権限のページに表示されるすべてのリソースに特権を付与する場合は、[すべてにアクセス権を付与（Grant access to all）]ボタンをクリックし、すべてのリソースから特権を削除する場合は、[すべてにアクセスを許可しない（Deny access to all）]をクリックします。

（注） リソースのリストが複数のページにわたって表示される場合、このボタンは、現在のページに表示されるリソースに限り適用されます。 他のページのリストにあるリソースのアクセス権を変更するには、それらのページを表示し、表示されたページでこのボタンを使用する必要があります。

ステップ 6 **[保存（Save）]** をクリックします。

管理者の高度なロール設定

[高度なロール設定（Advanced Role Configuration）] を使用すると、カスタム ロールの権限をより細かいレベルで編集できます。 **[エンドユーザの設定（End User Configuration）]** ウィンドウおよび **[アプリケーションユーザの設定（Application User Configuration）]** ウィンドウで、次の主な設定に対する管理者の編集権限を制御することができます。

- ユーザ ランクの編集
- アクセス コントロール グループの割り当ての編集
- 新規ユーザの追加
- ユーザ パスワードの編集

手順

ステップ 1 Cisco Unified CM Administration で、**[ユーザ管理（User Management）] > [ユーザ設定（User Settings）] > [ロール（Role）]**を選択します。

ステップ 2 [**検索（Find**）] をクリックしてカスタムロールを選択します。

ステップ 3 [**関連リンク（Related Links**）] で、[**詳細なロール設定（Advanced Role Configuration**）] を選択し、[**Go（移動**）] をクリックします。

ステップ 4 [**リソース（Resource**）**Web ページ**] で、[**アプリケーション ユーザ（Application User**）**Web ページ**] または [**ユーザ（User**）**Web ページ**] を選択します。

ステップ 5 設定の編集 フィールドとその設定のヘルプについては、オンラインヘルプを参照してください。

ステップ 6 **[保存（Save）]** をクリックします。

アクセス制御グループの作成

新しいアクセス制御グループを作成する必要がある場合に、この手順を使用します。 必要なロールとアクセス権限を持つ標準のグループがない場合に、この方法を使用できます。 カスタマイズされたグループを作成する方法には、次の 2 つがあります。

- **[新規追加（Add New）]** ボタンを使用して、scatch から新しいアクセス制御グループを作成および設定します。
- 必要な内容に近いロールが既存のグループ割り当てられてい場合は、[コピー（Copy）]ボタンを使用します。 既存のグループから、新しい編集可能なグループに設定をコピーできます。

手順

ステップ 1 Cisco Unified CM Administration で、**[ユーザ管理（User Management）] > [ユーザ設定（User Settings）] > [アクセス制御グループ（Access Control Group）]** を選択します。

ステップ 2 次のいずれかを実行します。

- 新しいグループを最初から作成するには、**[新規追加（Add New）]** をクリックします。

- 既存のグループから設定をコピーするには、**[検索（Find）]**をクリックして、既存のアクセス制御グループを開きます。 [コピー（Copyt）]をクリックして、新しいグループの名前を入力します。 **OK**をクリックします。

ステップ 3 アクセス制御グループの**名前**を入力します。

ステップ 4 **[ユーザで利用できるユーザランク（Available for Users with User Rank as）]** ドロップダウンから、このグループに割り当てる、ユーザの最低ランクを選択します。 デフォルトのユーザ ランクは 1 です。

ステップ 5 **[保存]** をクリックします。

ステップ 6 アクセス制御グループにロールを割り当てます。 選択したロールは、グループのメンバーに割り当てられます。

a) **[関連リンク（Related Links）]** から、**[アクセス制御グループへの権限の割り当て（Assign Roles to Access Control Group）]** を選択して **[実行（Go）]** をクリックします。
b) **[検索（Find）]** をクリックして、既存のロールを検索します。
c) 追加するロールをオンにして、**[選択の追加 (add Selected)]** をクリックします。
d) **[保存（Save）]** をクリックします。

次のタスク

アクセス制御グループへのユーザの割り当て （28 ページ）

アクセス制御グループへのユーザの割り当て

標準またはカスタムのアクセス制御グループに対してユーザを追加または削除します。 .

（注） ユーザのランクがアクセス制御グループの最低ユーザ ランクと同じかそれより上のユーザのみを追加できます。

（注） 会社のLDAPディレクトリから新しいユーザを同期する場合に、適切な権限を持つランク階層とアクセス制御グループが作成される場合、LDAP同期の一部としてグループを同期ユーザに割り当てる場合があります。 LDAP ディレクトリ同期の設定方法については、『*Cisco Unified Communications Manager* システム構成ガイド』を参照してください。

手順

ステップ 1 **[ユーザ管理(User Management)]** > **[ユーザ設定(User Settings)]** > **[アクセスコントロールグループ(Access Control Group)]** を選択します。

[アクセスコントロールグループの検索/一覧表示(Find and List Access Control Group)] ウィンドウが表示されます。

ステップ 2 [検索（Find）]をクリックして、ユーザリストを更新するアクセス制御グループを選択します。

ステップ 3 **[ユーザで利用できるユーザランク（Available for Users with User Rank as）]** ドロップダウンから、このグループに割り当てるために必要なユーザのランク要件を選択します。

ステップ 4 **[ユーザ]**セクションで、**[検索（Find）]** をクリックして、ユーザリストを表示します。

ステップ 5 エンドユーザまたはアプリケーション ユーザをアクセス制御グループに追加するには、次の手順を実行します。

a) [エンドユーザをアクセス制御グループに追加（Add End Users to Access Control Group）]または [アプリケーション ユーザをアクセス制御グループに追加（Add App Users to Access Control Group）]をクリックします。
b) 追加するユーザを選択します。
c) **[選択項目の追加(Add Selected)]** をクリックします。

ステップ 6 アクセス制御グループからユーザを削除するには、次の手順を実行します。

a) 削除するユーザを選択します。
b) **[選択項目の削除(Delete Selected)]** をクリックします。

ステップ 7 **[保存（Save）]** をクリックします。

アクセス制御グループの重複する特権ポリシーの設定

Cisco Unified Communications Manager がアクセス制御グループの割り当てにより発生する可能性がある、ユーザ権限の重複を処理する方法を設定します。 これにより、エンドユーザが複数のアクセス制御グループに割り当てられ、ロールや権限の設定に不整合が生まれる状況に対処できます。

手順

ステップ 1 Cisco Unified CM Administration で、**[システム（System）]** > **[エンタープライズパラメータ（Enterprise Parameters）]** を選択します。

ステップ 2 [ユーザ管理パラメータ（User Management Parameters）]で、[重複したユーザ グループとロールの実質的なアクセス権（Effective Access Privileges For Overlapping User Groups and Roles）]に次のいずれかの値を設定します。

- [最大（Maximum）]—実質的な権限は、重複したすべてのアクセス制御グループの最大限の権限になります。 これがデフォルトのオプションです。
- [最小（Minimum）]—実質的な権限は、重複したすべてのアクセス制御グループの最小限の権限になります。

ステップ 3 **[保存（Save）]** をクリックします。

ユーザ権限レポートの表示

既存のエンドユーザや既存のアプリケーションユーザのユーザ権限レポートを表示するには、次の手順を実行します。 ユーザ権限レポートは、エンド ユーザまたはアプリケーション ユーザに割り当てられたアクセス コントロール グループ、ロール、およびアクセス権限が表示されます。

手順

ステップ 1 Cisco Unified CM の管理で、次の手順のいずれかを実行します。

- エンド ユーザの場合は、**[ユーザの管理（User Management）] > [エンド ユーザ（End User）]**を選択します。
- アプリケーション ユーザの場合は、**[ユーザの管理（User Management）] > [アプリケーション ユーザ（Application User）]**を選択します。

ステップ 2 [検索（Find）] をクリックして、アクセス権限を表示するユーザを選択します。

ステップ 3 **[関連リンク（Related Links）]** ドロップダウンメニューから **[ユーザ権限レポート（User Privilege Report）]** を選択し、**[移動（Go）]** をクリックします。
[ユーザ権限（User Privilege）] ウィンドウが表示されます。

カスタム ヘルプ デスク ロールの作成タスク フロー

企業によっては、ヘルプデスク担当者に特定の管理タスクを実行できる権限を与える必要があると考えている場合があります。 このタスク フロー内の手順に従って、電話機の追加やエンド ユーザの追加などのタスクをヘルプ デスク チームのメンバーが実行できるようにする、ヘルプ デスク チームのメンバー用のロールとアクセス コントロール グループを設定します。

手順

	コマンドまたはアクション	目的
ステップ 1	カスタム ヘルプ デスク ロールの作成（31 ページ）	ヘルプ デスク チームのメンバーのカスタム ロールを作成し、新しい電話機の追加や新しいユーザの追加などの項目のロール権限を割り当てます。
ステップ 2	カスタム ヘルプ デスク アクセス コントロール グループの作成 （31 ページ）	ヘルプ デスク ロール用の新しいアクセス コントロール グループを作成します。
ステップ 3	アクセス制御グループへのヘルプ デスク ロールの割り当て （32 ページ）	ヘルプデスク アクセス コントロール グループにヘルプ デスク ロールを割り当てます。 このアクセス コントロール グ

	コマンドまたはアクション	目的
		ループに割り当てられたユーザには、ヘルプ デスク ロールの権限が割り当てられます。
ステップ 4	アクセス制御グループへのヘルプ デスク メンバーの割り当て （33 ページ）	カスタム ヘルプ デスク ロールの権限をヘルプ デスク チームのメンバーに割り当てます。

カスタム ヘルプ デスク ロールの作成

この手順を実行して、組織内のヘルプ デスク メンバーに割り当てることができるカスタム ヘルプ デスク権限を作成します。

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified Communications Manager Administration）]で、**[ユーザ管理（User Management）] > [ユーザ設定（User Settings）] > [権限（Role）]** をクリックします。

ステップ 2 [新規追加] をクリックします。

ステップ 3 [アプリケーション（Application）] ドロップダウン リストから、この権限に割り当てるアプリケーションを選択します。 たとえば、[Cisco CallManager Administration] を選択します。

ステップ 4 [次へ（Next）]をクリックします。

ステップ 5 新しいロールの [名前（Name）]を入力します。 たとえば、**`Help Desk`** です。

ステップ 6 [読み込みおよび更新権限（Read and Update Privileges）]の下で、ヘルプ デスク ユーザに割り当てる権限を選択します。 たとえば、ヘルプ デスク メンバーがユーザおよび電話を追加できるようにする場合は、[ユーザ（User）] Web ページと [電話（Phone）] Web ページの [読み込み（Read）]および [更新（Update）]チェック ボックスをオンにします。

ステップ 7 **[保存（Save）]** をクリックします。

次のタスク

カスタム ヘルプ デスク アクセス コントロール グループの作成 （31 ページ）

カスタム ヘルプ デスク アクセス コントロール グループの作成

始める前に

カスタム ヘルプ デスク ロールの作成 （31 ページ）

手順

ステップ 1 Cisco Unified CM の管理で、**[ユーザ管理（User Management）]**>**[ユーザ設定（User Settings）]**>**[アクセス コントロール グループ（Access Control Group）]** を選択します。

ステップ 2 [新規追加] をクリックします。

ステップ 3 アクセス制御グループの名前を入力します。 たとえば、「**Help_Desk**」と入力します。

ステップ 4 **[保存（Save）]** をクリックします。

次のタスク

アクセス制御グループへのヘルプ デスク ロールの割り当て （32 ページ）

アクセス制御グループへのヘルプ デスク ロールの割り当て

次の手順を実行して、ヘルプ デスク ロールからの権限を持つヘルプ デスク アクセス コントロール グループを設定します。

始める前に

カスタム ヘルプ デスク アクセス コントロール グループの作成 （31 ページ）

手順

ステップ 1 Cisco Unified CM の管理で、**[ユーザ管理（User Management）]**>**[ユーザ設定（User Settings）]**>**[アクセス コントロール グループ（Access Control Group）]** を選択します。

ステップ 2 [検索（Find）]をクリックし、ヘルプデスク用に作成したアクセス コントロール グループを選択します。
[アクセス コントロール グループの設定（Access Control Group Configuration）]ウィンドウが開きます。

ステップ 3 [関連リンク（Related Links）]ドロップダウン リスト ボックスで、[アクセス コントロール グループに権限を割り当て（Assign Role to Access Control Group）]オプションを選択し、[移動（Go）]をクリックします。
[ロールの検索/一覧表示（Find and List Roles）]ポップアップが表示されます。

ステップ 4 [グループに権限を割り当て（Assign Role to Group）]ボタンをクリックします。

ステップ 5 [検索（Find）]をクリックし、ヘルプ デスク ロールを選択します。

ステップ 6 **[選択項目の追加(Add Selected)]** をクリックします。

ステップ 7 **[保存（Save）]** をクリックします。

次のタスク

アクセス制御グループへのヘルプ デスク メンバーの割り当て （33 ページ）

アクセス制御グループへのヘルプ デスク メンバーの割り当て

始める前に

アクセス制御グループへのヘルプ デスク ロールの割り当て （32 ページ）

手順

ステップ 1 Cisco Unified CM の管理で、**[ユーザ管理（User Management）]** > **[ユーザ設定（User Settings）]** > **[アクセス コントロール グループ（Access Control Group）]** を選択します。

ステップ 2 [検索（Find）]をクリックし、作成したカスタム ヘルプ デスク アクセス コントロール グループを選択します。

ステップ 3 次のいずれかの手順を実行します。

- ヘルプ デスク チームのメンバーがエンド ユーザとして設定されている場合は、[グループにエンド ユーザを追加（Add End Users to Group）]をクリックします。
- ヘルプデスク チームのメンバーがアプリケーション ユーザとして設定されている場合は、[グループにアプリケーション ユーザを追加（Add App Users to Group）]をクリックします。

ステップ 4 [検索（Find）]をクリックし、ヘルプ デスク ユーザを選択します。

ステップ 5 **[選択項目の追加(Add Selected)]** をクリックします。

ステップ 6 **[保存]** をクリックします。
Cisco Unified Communications Manager が、作成したカスタム ヘルプ デスク ロールの権限をヘルプ デスク チームのメンバーに割り当てます。

アクセス制御グループの削除

アクセス コントロール グループ全体を削除するには、次の手順を使用します。

始める前に

アクセス コントロール グループを削除すると、Cisco Unified Communications Manager がデータベースからすべてのアクセス コントロール グループ データを削除します。 アクセス コントロール グループを使用しているロールが判明していることを確認します。

手順

ステップ 1 **[ユーザ管理(User Management)]** > **[ユーザ設定(User Settings)]** > **[アクセスコントロールグループ(Access Control Group)]** を選択します。

[アクセス コントロール グループの検索と一覧表示（Find and List Access Control Groups）] ウィンドウが表示されます。

ステップ 2 削除するアクセス コントロール グループを検索します。

ステップ 3 削除するアクセス ポイント グループの名前をクリックします。

選択したアクセス コントロール グループが表示されます。 このアクセス コントロール グループ内のユーザがアルファベット順に一覧表示されます。

ステップ 4 アクセス コントロール グループ全体を削除するには、[削除（Delete）]をクリックします。

アクセス コントロール グループを削除すると元に戻せないことを警告するダイアログボックスが表示されます。

ステップ 5 アクセス コントロール グループを削除するには、[OK]をクリックします。アクションをキャンセルするには、[キャンセル（Cancel）]をクリックします。 [OK]をクリックすると、Cisco Unified Communications Manager がデータベースからアクセス コントロール グループを削除します。

既存の OAuth 更新トークンの取り消し

既存の OAuth 更新トークンを取り消すには、AXL API を使用します。 たとえば、ある従業員が退社した場合、この API を使用してその従業員の現在の更新トークンを取り消し、その従業員が新しいアクセス トークンを取得したり、企業アカウントへログインできないようにすることができます。 API は、AXL クレデンシャルで保護されている REST ベースの API です。 任意のコマンドライン ツールを使用して API を呼び出すことができます。 次のコマンドは、更新トークンを取り消すために使用できる cURL コマンドの例を示しています。

```
curl -k -u "admin:password" https://<UCMaddress:8443/ssosp/token/revoke?user_id=<end_user>
```

引数の説明

- `admin:password` は、Cisco Unified Communications Manager の管理者アカウントのログイン ID とパスワードです。
- `UCMaddress` は、Cisco Unified Communications Manger のパブリッシャ ノードの FQDN または IP アドレスです。
- `end_user` は、更新トークンを取り消すユーザのユーザ ID です。

非アクティブなユーザ アカウントの無効化

Cisco Database Layer Monitor サービスを使用して非アクティブなユーザ アカウントを無効にするには、次の手順を実行します。

Cisco Database Layer Monitor は、指定日数内に Cisco Unified Communications Manager にログインしていない場合、スケジュールされたメンテナンス タスク時にユーザ アカウント ステータスを非アクティブに変更します。 無効にされたユーザは、その後の監査ログで自動的に監査対象になります。

始める前に

Cisco Database Layer Monitor サービスで選択したサーバの **[メンテナンス時間（Maintenance Time）]**を入力します（**[システム]** > **[サービス パラメータ]**）。

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified CM Administration）] で、**[システム]** > **[サービス パラメータ]** 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 ボックスからサーバを選択します。

ステップ 3 [サービス（Service）] ドロップダウンリスト ボックスから [Cisco Database Layer Monitor] パラメータを選択します。

ステップ 4 [詳細設定（Advanced）]をクリックします。

ステップ 5 [この期間未使用のユーザ アカウントを無効化する（Disable User Accounts unused for（days））] フィールドに、日数を入力します。 例: 90。システムはこの入力された値を、非アクティブとしてアカウントの状態を宣言するためのしきい値として使用します。 自動無効化をオフにするには、値を 0 と入力します。

（注） これは必須フィールドです。 デフォルトおよび最小値は 0 で、単位は日数です。

ステップ 6 **[保存]** をクリックします。
非アクティブなまま設定された日数（たとえば 90 日間）が経過すると、ユーザは無効になります。監査ログにエントリが作成され、次のメッセージが表示されます。「<userID>ユーザは非アクティブとマークされています（<userID> user is marked inactive）」。

リモート アカウントの設定

シスコ サポートがトラブルシューティングのためにご使用のシステムに一時的にアクセスできるよう、Unified Communications Manager でリモート アカウントを設定します。

手順

ステップ 1 [Cisco Unified オペレーティング システムの管理（Cisco Unified Operating System Administration）] で、**[サービス（Services）]** > **[リモート サポート（Remote Support）]** を選択します。

ステップ 2 [アカウント名（Account Name）]フィールドに、リモート アカウントの名前を入力します。

ステップ 3 [アカウントの有効期限（Account Duration）]フィールドに、アカウントの有効期限を日数で入力します。

ステップ 4 **[保存]** をクリックします。
システムは、暗号化パス フレーズを生成します。

ステップ 5 シスコのサポート担当者に連絡して、リモート サポート アカウント名とパス フレーズを提供します。

標準ロールとアクセス制御グループ

次の表は、Cisco Unified Communications Manager にあらかじめ設定されている標準権限およびアクセス制御グループの概要です。 標準権限が持つ特権はデフォルトで設定されています。また、標準権限に関連付けられたアクセス制御グループも、デフォルトで設定されています。

標準権限、および標準権限に関連付けられたアクセス制御グループの両方で、特権または権限の割り当てを編集できません。

表 *3:* 標準権限、特権 およびアクセス制御グループ

標準権限	権限に対する特権およびリソース	関連付けられた標準アクセス制御グループ
標準 AXL API アクセス	AXL データベース API へのアクセスを許可します。	標準 CCM スーパーユーザ
標準 AXL APIユーザ	AXL API を実行するログイン権限を付与します。	
標準 AXL 読み取り専用 API アクセス	AXL 読み取り専用 API（API の一覧表示、API の取得、SQL Query API の実行）の実行をデフォルトで許可します。	
標準管理 Rep Tool 管理	Cisco Unified Communications Manager CDR Analysis and Reporting（CAR）の表示および設定が可能になります。	標準 CAR 管理ユーザ、標準 CCM スーパー ユーザ

標準権限	権限に対する特権およびリソース	関連付けられた標準アクセス制御グループ
標準監査ログ管理	監査ロギング機能の次のタスクを実行できます。 • Cisco Unified Serviceability の [監査ログ設定（Audit Log Configuration）] ウィンドウでの、監査ロギングの表示および設定 • Cisco Unified Serviceability でのトレースの表示と設定、および Real-Time Monitoring Tool の監査ログ機能向けトレースの収集 • Cisco Unified Serviceability での Cisco Audit Event Service の表示、開始、停止 • RTMT での、関連付けられたアラートの表示および更新	標準監査ユーザ
標準 CCM 管理ユーザ	Cisco Unified Communications Manager Administration へのログイン権限を付与します。	標準 CCM 管理ユーザ、標準 CCM ゲートウェイ管理、標準 CCM 電話管理、標準 CCM 読み取り専用、標準 CCM サーバ モニタリング、標準 CCM スーパーユーザ、標準 CCM サーバ メンテナンス、標準パケット スニファ ユーザ
標準CCMエンドユーザ	Cisco Unified Communications セルフケアポータルにログインする権限をエンドユーザに付与します。	標準CCMエンドユーザ

標準権限	権限に対する特権およびリソース	関連付けられた標準アクセス制御グループ

標準 CCM 機能管理	Cisco Unified Communications Manager Administration で、次のタスクを実行できます。
	• 一括管理ツールによる次の項目の表示、削除、挿入：
	  • クライアント関連のコードと強制承認コード
	  • コール ピックアップ グループ
	• Cisco Unified Communications Manager Administration で、の次の項目を表示、設定できます。
	  • クライアント関連のコードと強制承認コード
	  • コール パーク
	  • コール ピックアップ
	  • ミートミーの番号またはパターン
	  • メッセージ待機
	  • Cisco Unified IP Phone サービス
	  • ボイスメールパイロット、ボイスメールポートウィザード、ボイスメールポート、ボイスメールプロファイル
		標準 CCMサーバメンテナンス

標準 CCM ゲートウェイ管理	Cisco Unified Communications Manager Administration で、次のタスクを実行できます。 • 一括管理ツールによるゲートウェイテンプレートの表示および設定 • ゲートキーパー、ゲートウェイ、およびトランクの表示および設定	標準 CCM ゲートウェイ管理

標準権限	権限に対する特権およびリソース	関連付けられた標準アクセス制御グループ

標準 CCM 電話管理	Cisco Unified Communications Manager Administration で、次のタスクを実行できます。
	• 一括管理ツールによる電話の表示とエクスポート
	• 一括管理ツールによるユーザデバイスプロファイルの表示と挿入
	• Cisco Unified Communications Manager Administration で、の次の項目を表示、設定できます。
	  • BLF 短縮ダイヤル
	  • CTI ルート ポイント
	  • デフォルトデバイスプロファイルまたはデフォルト プロファイル
	  • 電話番号、および回線の状態
	  • ファームウェア ロード情報
	  • 電話ボタンテンプレートまたはソフトキー テンプレート
	  • 電話機
	  • [電話の設定（Phone Configuration）] ウィンドウの [ボタン項目を変更（Modify Button Items）] をクリックすることによる、特定の電話に対する電話ボタンの情報の並べ替え
		標準 CCM 電話管理

標準権限	権限に対する特権およびリソース	関連付けられた標準アクセス制御グループ
標準 CCM ルート プラン計画管理	Cisco Unified Communications Manager Administration で、次のタスクを実行できます。 • アプリケーション ダイヤル ルールの表示および設定 • コーリング サーチ スペースおよびパーティションの表示および設定 • ダイヤル ルール パターンを含むダイヤル ルールの表示および設定 • ハント リスト、ハント パイロット、回線グループの表示および設定 • ルート フィルタ、ルート グループ、ルート ハント リスト、ルート リスト、ルート パターン、ルート プラン レポートの表示および設定 • 時間帯およびスケジュールの表示および設定 • トランスレーション パターンの表示および設定	

標準権限	権限に対する特権およびリソース	関連付けられた標準アクセス制御グループ
標準 CCM サービス管理	Cisco Unified Communications Manager Administration で、次のタスクを実行できます。 • 次の項目を表示および設定できます。 • アナンシエータ、会議ブリッジ、トランスコーダ • オーディオ ソースおよび MOH サーバ • メディア リソース グループおよびメディア リソース グループ リスト • Media Termination Point; メディア ターミネーション ポイント • Cisco Unified Communications Manager Assistant ウィザード • 一括管理ツールの [マネージャの削除（Delete Managers）]、[マネージャ/アシスタントの削除（Delete Managers/Assistants）] および [マネージャ/アシスタントの挿入（Insert Managers/Assistants）] ウィンドウでの表示および設定ができます。	標準 CCMサーバメンテナンス

標準権限	権限に対する特権およびリソース	関連付けられた標準アクセス制御グループ
標準 CCM システム管理	Cisco Unified Communications Manager Administration で、次のタスクを実行できます。 • 次の項目を表示および設定できます。 • 代替ルーティング（AAR）グループの自動化 • Cisco Unified Communications Manager（Cisco Unified CM）および Cisco Unified Communications Manager グループ • 日時グループ • デバイス デフォルト • デバイス プール • エンタープライズ パラメータ • エンタープライズ電話の設定 • ロケーション（Locations） • Network Time Protocol（NTP）サーバ • プラグイン • Skinny Call Control Protocol（SCCP）または Session Initiation Protocol（SIP）を実行する電話用のセキュリティプロファイル、SIP トランク用のセキュリティ プロファイル • Survivable Remote Site Telephony（SRST）の参照 • サーバ • 一括管理ツールの、[ジョブ スケジューラ（Job Scheduler）] ウィンドウでの表示と設定	標準 CCMサーバメンテナンス

標準権限	権限に対する特権およびリソース	関連付けられた標準アクセス制御グループ
標準 CCM ユーザ権限管理	Cisco Unified Communications Manager Administration で、アプリケーション ユーザの表示および設定を実行できます。	
標準CCMADMIN管理	CCMAdmin システムのすべての面を利用できます。	
標準CCMADMIN管理	Cisco Unified Communications Manager Administration および一括管理ツールのすべての項目を表示および設定できます。	標準 CCM スーパーユーザ
標準CCMADMIN管理	Dialed Number Analyzer の情報を表示および設定できます。	
標準CCMADMIN読み取り専用	すべての CCMAdmin リソースの読み取りを許可します。	
標準CCMADMIN読み取り専用	Cisco Unified Communications Manager Administration および一括管理ツールの項目を表示できます。	標準 CCM ゲートウェイ管理、標準 CCM 電話管理、標準 CCM 読み取り専用、標準 CCM サーバ メンテナンス、標準 CCM サーバ モニタリング
標準CCMADMIN読み取り専用	Dialed Number Analyzer で、ルーティング設定の分析ができます。	
標準 CCMUSER 管理	Cisco Unified Communications セルフケアポータルへのアクセスを許可します。	標準CCMエンドユーザ
標準CTI通話モニタリング許可	CTIアプリケーションまたはデバイスでコールをモニタできます。	標準 CTI 通話モニタリング許可
標準CTI コール パーク モニタリング許可	CTIアプリケーションまたはデバイスでコール パークを使用できます。 **重要** 開いている回線およびパーク回線の最大数は 65,000 を超えてはいけません。 合計が 65,000 を超える場合は、アプリケーション ユーザーから標準 CTI 許可コール パーク モニタリングのロールを削除するか、設定されているパーク回線の数を減らします。	標準 CTI コール パーク モニタリング許可

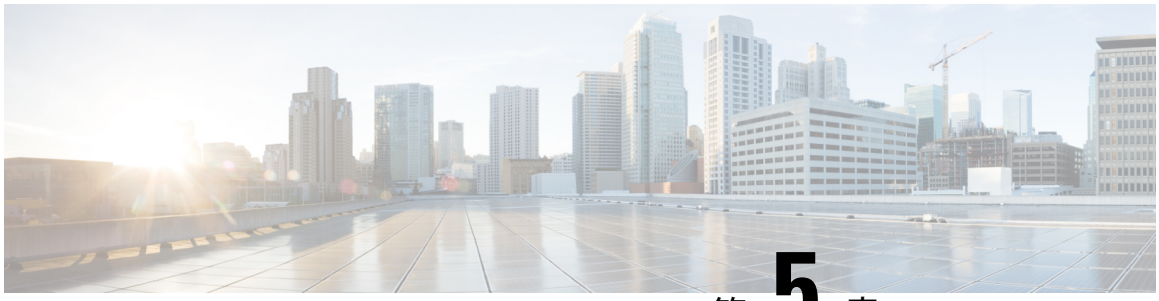
標準権限	権限に対する特権およびリソース	関連付けられた標準アクセス制御グループ
標準CTI通話録音許可	CTIアプリケーション/デバイスで通話を録音できます。	標準 CTI 通話録音許可
標準CTI発信者番号の変更許可	CTI アプリケーションが発信者番号を通話中に変更できます。	標準CTI発信者番号の変更許可
[標準 CTI によるすべてのデバイスの制御（Standard CTI Allow Control of All Devices）]	CTI で制御可能なすべてのデバイスを制御できます。	[標準CTIによるすべてのデバイスの制御（Standard CTI Allow Control of All Devices）]
標準CTI接続された転送と会議をサポートする電話の制御許可	接続された転送および会議をサポートするすべての CTI デバイスを制御できます。	[標準CTIによる接続時の転送および会議をサポートする電話の制御（Standard CTI Allow Control of Phones supporting Connected Xfer and conf）]
標準 CTI ロールオーバーモードをサポートする電話の制御許可	ロールオーバーモードをサポートするすべての CTI デバイスを制御できます。	[標準CTIによるロールオーバーモードをサポートする電話の制御の許可（Standard CTI Allow Control of Phones supporting Rollover Mode）]
標準 CTI SRTP 重要素材の受信許可	CTI アプリケーションが、SRTP を使用する重要な素材にアクセスしたり、その素材を配信したりできるようにします。	標準 CTI SRTP 重要素材の受信許可
[標準CTIを有効にする（Standard CTI Enabled）]	CTI アプリケーションの制御を可能にします。	[標準CTIを有効にする（Standard CTI Enabled）]
標準CTIセキュア接続	Cisco Unified Communications Manager へのセキュアな CTI 接続が可能になります。	標準 CTI セキュア接続
標準CUReporting	アプリケーション ユーザが、さまざまなソースからレポートを作成できます。	
標準CUReporting	Cisco Unified Reporting での、レポートの表示、ダウンロード、作成、およびアップロードができます。	標準 CCM 管理ユーザ、標準 CCM スーパー ユーザ

標準権限	権限に対する特権およびリソース	関連付けられた標準アクセス制御グループ
標準 EM 認証プロキシ権限	アプリケーションで使用する Cisco Extension Mobility（EM）の認証権限を管理します。この権限は、（Cisco Unified Communications Manager Assistant や Cisco Web Dialer などの）Cisco Extension Mobility と対話するすべてのアプリケーション ユーザに必要です。	標準 CCM スーパー ユーザ、標準 EM 認証プロキシ権限
標準パケット スニッフィング	Cisco Unified Communications Manager の管理にアクセスし、パケット スニッフィング（キャプチャ）ができます。	標準パケット スニファ ユーザ
標準 RealtimeAndTraceCollection	Cisco Unified Serviceability および Real-Time Monitoring Tool にアクセスし、次の項目を表示および使用できます。 • Simple Object Access Protocol（SOAP）Serviceability AXL API • SOAP コール レコード API • SOAP 診断ポータル（Analysis Manager）データベース サービス • 監査ログ機能のトレースの設定 • トレース収集などの、Real-Time Monitoring Tool の設定	標準 RealtimeAndTraceCollection

標準権限	権限に対する特権およびリソース	関連付けられた標準アクセス制御グループ
標準 SERVICEABILITY	Cisco Unified Serviceability または Real-Time Monitoring Tool で、次のウィンドウを表示および設定できます。 • [アラーム設定およびアラーム定義（Alarm Configuration and Alarm Definitions）]（Cisco Unified Serviceability） • [監査トレース（Audit Trace）]（読み取りおよび表示のみ可能なマークが付けられています） • SNMP 関連のウィンドウ（Cisco Unified Serviceability） • [トレースの設定（Trace Configuration）]および[トレース設定のトラブルシューティング（Troubleshooting of Trace Configuration）]（Cisco Unified Serviceability） ） • ログ パーティションのモニタリング • [アラートの設定（Alert Configuration）]（RTMT）、[プロファイルの設定（Profile Configuration）]（RTMT）、および [トレース収集（Trace Collection）]（RTMT） SOAP Serviceability AXL API、SOAP Call Record API、および SOAP 診断ポータル（Analysis Manager）データベース サービスを表示および使用できます。 SOAP コールレコード API については、RTMT Analysis Manager Call Record の権限が、このリソースを介して制御されます。 SOAP 診断ポータル データベース サービスについては、RTMT Analysis Manager Hosting Database アクセスが、このリソースを介して制御されます。	標準 CCM サーバ モニタリング、標準 CCM スーパーユーザ

標準権限	権限に対する特権およびリソース	関連付けられた標準アクセス制御グループ
標準SERVICEABILITY管理	有用性の管理者は、Cisco Unified Communications Manager の管理に表示されるプラグイン ウィンドウにアクセスでき、このウィンドウからプラグインをダウンロードできます。	
標準SERVICEABILITY管理	Dialed Number Analyzer の有用性をすべての面で管理できます。	
標準SERVICEABILITY管理	Cisco Unified Serviceability および Real-Time Monitoring Tool のすべてのウィンドウを表示および設定できます（[監査トレース（Audit Trace）] では表示のみ可能です）。 すべての SOAP Serviceability AXL API を表示および使用できます。	
標準SERVICEABILITY読み取り専用	Dialed Number Analyzer のコンポーネントで使用する有用性に関するすべてのデータを表示できます。	標準 CCM 読み取り専用
標準SERVICEABILITY読み取り専用	Cisco Unified Serviceability および Real-Time Monitoring Tool で、設定を表示できます。（標準監査ログ管理の権限により表示される監査設定ウィンドウは除きます） SOAP Serviceability AXL API、SOAP Call Record API、および SOAP 診断ポータル（Analysis Manager）データベース サービスをすべて表示できます。	
標準システムサービス管理	Cisco Unified Serviceability で、サービスを表示、アクティベート、開始、および停止できます。	
標準 SSO 設定管理	SAML SSO の設定をすべての面で管理できます。	
標準機密アクセス レベル ユーザ	すべての機密アクセス レベル ページにアクセスできます。	標準 Cisco Call Manager 管理
標準CCMADMIN管理	CCMAdmin システムをすべての面で管理できます。	標準Cisco Unified CM IM およびプレゼンスの管理
標準CCMADMIN読み取り専用	すべての CCMAdmin リソースの読み取りを許可します。	標準Cisco Unified CM IM およびプレゼンスの管理

標準権限	権限に対する特権およびリソース	関連付けられた標準アクセス制御グループ
標準CUReporting	アプリケーション ユーザが、さまざまなソースからレポートを作成できます。	標準 Cisco Unified CM IM & Presenceのレポーティング



第 5 章

エンドユーザの管理

エンドユーザの概要

稼働中のシステムを管理する際に、システム内に設定済みのエンドユーザのリストを更新しなければならない場合があります。 次の作業が含まれます。

- 新しいユーザの設定
- 新しいエンドユーザの電話機の設定
- エンドユーザのパスワードまたは PIN の変更
- IM and Presence Service に対するエンドユーザの有効化

Cisco Unified CM の管理の [エンドユーザの設定（End User Configuration）] ウィンドウで、Unified CM エンドユーザに関する情報を追加、検索、表示、保守できます。 また、[ユーザ/電話のクイック追加（Quick User/Phone Add）] ウィンドウを使用して、新規エンドユーザとそのエンドユーザの新規電話を迅速に設定することもできます。

エンドユーザ管理タスク

手順

	コマンドまたはアクション	目的
ステップ 1	ユーザ テンプレートの設定 （50 ページ）	ユニバーサル回線テンプレートとデバイス テンプレートを含むユーザ プロファイルまたは機能グループ テンプレートを使用してシステムを設定していない場合は、次のタスクを実行してセットアップします。

	コマンドまたはアクション	目的
		これらのテンプレートを新しいエンドユーザに適用することにより、新しいユーザと電話機を簡単に設定できます。
ステップ 2	次の方法のいずれかを使用して新しいエンド ユーザを追加します • LDAP からのエンド ユーザのインポート （56 ページ） • エンド ユーザの手動追加 （57 ページ）	システムが設定済みであり会社の LDAP ディレクトリと同期している場合は、新しいエンド ユーザを LDAP から直接インポートできます。 まだ設定していない場合は、エンドユーザを手動で追加して設定できます。
ステップ 3	次のタスクのどちらかを実行することにより、新しいまたは既存のエンド ユーザに電話機を割り当てます。 • エンド ユーザ用の新しい電話機の追加 （58 ページ） • エンド ユーザへの既存の電話機の移動 （59 ページ）	「新しい電話機の追加」手順に従い、ユニバーサル デバイス テンプレートの設定を使用して、エンド ユーザの新しい電話機を設定できます。 また、「移動」手順に従って、すでに設定済みの既存の電話機を割り当てることもできます。
ステップ 4	エンド ユーザ PIN の変更 （60 ページ）	（オプション）Cisco Unified Communications Manager Administration でエンド ユーザの PIN を変更する。
ステップ 5	エンド ユーザ パスワードの変更 （60 ページ）	（オプション）Cisco Unified Communications Manager Administration でエンド ユーザのパスワードを変更する。
ステップ 6	Cisco Unity Connection ボイス メールボックスの作成 （61 ページ）	（オプション）Cisco Unified Communications Manager Administration で個別の Cisco Unity Connection ボイス メールボックスを作成する。

ユーザ テンプレートの設定

次のタスクを実行して、ユーザ プロファイルおよび機能グループ テンプレートを設定します。新しいエンド ユーザを追加したら、回線およびデバイス設定を使用してすばやくエンド ユーザを設定し、エンド ユーザの電話を設定できます。

手順

	コマンドまたはアクション	目的
ステップ 1	ユニバーサル回線テンプレートの設定（51 ページ）	電話番号に一般的に適用される共通設定を使用して、ユニバーサル回線テンプレートを設定します。
ステップ 2	ユニバーサル デバイス テンプレートの設定 （52 ページ）	電話に一般的に適用される共通設定を使用して、ユニバーサル デバイス テンプレートを設定します。
ステップ 3	ユーザ プロファイルの設定 （53 ページ）	ユニバーサル回線テンプレートとユニバーサル デバイス テンプレートをユーザ プロファイルに割り当てます。 セルフプロビジョニング機能を設定している場合は、このプロファイルを使用するユーザに対してセルフプロビジョニングを有効化できます。
ステップ 4	機能グループ テンプレートの設定 （55 ページ）	機能グループ テンプレートにユーザ プロファイルを割り当てます。 LDAP 同期ユーザの場合は、機能グループ テンプレートによってユーザ プロファイル設定がエンド ユーザに関連付けられます。

ユニバーサル回線テンプレートの設定

ユニバーサル回線テンプレートを使用すると、新しく割り当てられたディレクトリ番号に共通の設定を簡単に適用できます。 さまざまなユーザ グループのニーズに合わせて、異なるテンプレートを設定します。

手順

ステップ 1 Cisco Unified CM Administration で、**[ユーザ管理（User Management）]** > **[ユーザ/電話の追加（User/Phone Add）]** > **[ユニバーサル回線テンプレート（Universal Line Template）]** を選択します。

ステップ 2 [新規追加] をクリックします。

ステップ 3 [ユニバーサル回線テンプレートの設定（Universal Line Template 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 代替番号を使用したグローバル ダイヤル プラン レプリケーションを展開する場合は、[エンタープライズ代替番号（Enterprise Alternate Number）]セクションと [+E.164代替番号（+E.164 Alternate Number）]セクションを展開して、次の手順を実行します。

a) [エンタープライズ代替番号の追加（Add Enterprise Alternate Number）]ボタンまたは[+E.164代替番号の追加（Add +E.164 Alternate Number）]ボタンのいずれか、または両方をクリックします。
b) 代替番号への割り当に使用する[番号マスク（Number Mask）]を追加します。 たとえば、4桁の内線番号では、エンタープライズ番号マスクとして5 XXXXを使用し、+E.164代替番号マスクとして1972555XXXXを使用することが考えられます。
c) 代替番号を割り当てるパーティションを割り当てます。
d) ILSを通じてこの番号をアドバタイズする場合は、[ILS経由でグローバルにアドバタイズ（Advertise Globally via ILS）]チェックボックスをオンにします。 アドバタイズされたパターンを使用して一定の代替番号の範囲を要約している場合は、個別の代替番号をアドバタイズする必要はありません。
e) [PSTNフェールオーバー（PSTN Failover）]セクションを展開して、通常のコールルーティングが失敗した場合に使用するPSTNフェールオーバーとして、[エンタープライズ番号（Enterprise Number）]または[+E.164代替番号（+E.164 Alternate Number）]を選択します。

ステップ5 **[保存（Save）]**をクリックします。

次のタスク

ユニバーサル デバイス テンプレートの設定 （52 ページ）

ユニバーサル デバイス テンプレートの設定

ユニバーサル デバイス テンプレートを使用すると、新しくプロビジョニングしたデバイスに簡単に設定を適用できます。 プロビジョニングされたデバイスは、ユニバーサル デバイス テンプレートの設定を使用します。 さまざまなユーザ グループのニーズを満たすために、異なるデバイス テンプレートを設定できます。 設定したプロファイルをこのテンプレートに割り当てることもできます。

始める前に

ユニバーサル回線テンプレートの設定 （51 ページ）

手順

ステップ1 Cisco Unified CM Administrationで、**[ユーザの管理（User Management）]** > **[ユーザ/電話の追加（User/Phone Add）]** > **[ユニバーサル デバイス テンプレート（Universal Device Template）]**を選択します。
ステップ2 [新規追加]をクリックします。
ステップ3 次の必須フィールドに入力します。
a) テンプレートの[デバイスの説明（Device Description）]を入力します。
b) [デバイスプールタイプ（Device Pool Type）]をドロップダウン リストから選択します。
c) [デバイスのセキュリティプロファイル（Device Security Profile）]をドロップダウン リストから選択します。

d) [SIPプロファイル（SIP Profile）]をドロップダウンリストから選択します。
e) [電話ボタンテンプレート（Phone Button Template）]をドロップダウンリストから選択します。

ステップ 4 [ユニバーサルデバイステンプレートの設定（Universal Device Template Configuration）]ウィンドウで、残りのフィールドを入力します。フィールドの説明については、オンラインヘルプを参照してください。

ステップ 5 [電話の設定（Phone Settings）]で、次の任意指定のフィールドを入力します。

a) [共通の電話プロファイル（Common Phone Profile）]を設定した場合は、そのプロファイルを割り当てます。
b) [共通デバイス設定（Common Device Configuration）]を設定した場合は、その設定を割り当てます。
c) [機能管理ポリシー（Feature Control Policy）]を設定した場合は、そのポリシーを割り当てます。

ステップ 6 **[保存（Save）]** をクリックします。

次のタスク

ユーザ プロファイルの設定 （53 ページ）

ユーザ プロファイルの設定

ユーザ プロファイルを使用して、ユニバーサル回線テンプレートとユニバーサル デバイス テンプレートをユーザに割り当てます。 さまざまなユーザ グループ用に複数のユーザ プロファイルを設定します。 このサービス プロファイルを使用するユーザに対してセルフプロビジョニングを有効にすることもできます。

始める前に

ユニバーサル デバイス テンプレートの設定 （52 ページ）

手順

ステップ 1 [Cisco Unified CM 管理（Cisco Unified CM Administration）] から、以下を選択します。 **[ユーザ管理（User Management）] > [ユーザ設定（User Settings）] > [ユーザプロファイル（User Profile）]**。

ステップ 2 [新規追加] をクリックします。

ステップ 3 ユーザ プロファイルの [名前（Name）]および [説明（Description）]を入力します。

ステップ 4 ユーザの **[デスクフォン（Desk Phones）]**、**[モバイルおよびデスクトップデバイス（Mobile and Desktop Devices）]**、および **[リモート接続先/デバイスプロファイル（Remote Destination/Device Profiles）]** に、**[ユニバーサルデバイステンプレート（Universal Device Template）]** を割り当てます。

ステップ 5 [ユニバーサル回線テンプレート（Universal Line Template）]を割り当て、このユーザプロファイルのユーザの電話回線に適用します。

ステップ 6 このユーザプロファイルのユーザに自分の電話機をプロビジョニングするセルフプロビジョニング機能の使用を許可するには、次の手順を実行します

a) [エンドユーザに自分の電話のプロビジョニングを許可（Allow End User to Provision their own phones）]チェックボックスをオンにします。

b) [エンドユーザがプロビジョニングする電話機数を制限（Limit Provisioning once End User has this many phones）]フィールドに、ユーザがプロビジョニングできる電話の最大数を入力します。 最大値は 20 です。

c) このプロファイルに関連付けられたエンドユーザーに、別のユーザーがすでに所有しているデバイスを移行または再割り当てする権限があるかどうかを判断するには、**[すでに別のエンドユーザーに割り当てられた電話機のプロビジョニングを許可する（Allow Provisioning of a phone already assigned to a different End User）]** チェックボックスをオンにします。 デフォルトでは、このチェックボックスはオフになっています。

ステップ 7 このユーザープロファイルに関連付けられた Cisco Jabber ユーザーがモバイルおよびリモートアクセス機能を使用できるようにするには、**[モバイルおよびリモートアクセスの有効化（Enable Mobile and Remote Access）]** チェックボックスをオンにします。

（注）
- デフォルトでは、このチェックボックスはオンになっています。このチェックボックスをオフにすると、**[クライアントポリシー（Client Policies）]** セクションが無効になり、サービス クライアント ポリシー オプションは、デフォルトで選択されません。
- この設定は、OAuth 更新ログインを使用している Cisco Jabber のユーザにのみ必須です。 Jabberユーザではない場合、この設定を行わずともモバイルおよびリモートアクセス機能を使用できます。 モバイルおよびリモート アクセス機能は、Jabber モバイルおよびリモートアクセスのユーザにのみ適用され、他のエンドポイントやクライアントには適用されません。

ステップ 8 このユーザプロファイルに Jabber ポリシーを割り当てます。**[デスクトップ クライアント ポリシー（Desktop Client Policy）]** と **[モバイル クライアント ポリシー（Mobile Client Policy）]** のドロップダウンメニューから、次のオプションのいずれかを選択します。

- サービスなし：このポリシーは、すべての Cisco Jabber サービスへのアクセスを禁止します。
- IMとプレゼンスのみ：このポリシーは、インスタントメッセージとプレゼンス機能のみを有効にします。
- IM とプレゼンス、音声とビデオ通話：このポリシーは音声やビデオ デバイスを使うすべてのユーザに対して、インスタントメッセージ、プレゼンス、ボイスメールと会議機能を有効化します。 これがデフォルトのオプションです。

（注） Jabber デスクトップクライアントには Windows 版 Cisco Jabber および Mac 版 Cisco Jabber が含まれています。 Jabber モバイルクライアントには、iPad/iPhone ユーザ用 Cisco Jabber および Android 版 Cisco Jabber が含まれています。

ステップ 9 このユーザ プロファイルのユーザが Cisco Unified Communications セルフケア ポータルで Extension Mobility または Extension Mobility Cross Cluster の最大ログイン時間を設定できるようにするには、[エンドユーザにエクステンションモビリティの最大ログイン時間の設定を許可する（Allow End User to set their Extension Mobility maximum login time）]チェックボックスをオンにします。

（注） デフォルトでは [エンドユーザにエクステンションモビリティの最大ログイン時間の設定を許可する（Allow End User to set their Extension Mobility maximum login time）]チェックボックスはオフになっています。

ステップ 10 **[保存（Save）]** をクリックします。

次のタスク

機能グループ テンプレートの設定 （55 ページ）

機能グループ テンプレートの設定

機能グループテンプレートは、プロビジョニングされたユーザ用に、電話、回線、および機能をすばやく設定できるようにすることで、システムの展開をサポートします。 企業の LDAP ディレクトリからユーザを同期している場合は、ディレクトリからユーザを同期させるユーザ プロファイルおよびサービス プロファイルを使用して機能グループ テンプレートを設定します。 このテンプレートを使用して、同期されたユーザに対して IM and Presence Service を有効化することもできます。

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified CM Administration）] で、**[ユーザ管理（User Management）] > [ユーザ/電話の追加（User/Phone Add）] > [機能グループ テンプレート（Feature Group Template）]** を選択します。

ステップ 2 [新規追加] をクリックします。

ステップ 3 機能グループ テンプレートの [名前（Name）]と [説明（Description）]を入力します。

ステップ 4 このテンプレートを使用するすべてのユーザのホーム クラスタとしてローカル クラスタを使用する場合は、[ホーム クラスタ（Home Cluster）]チェック ボックスをオンにします。

ステップ 5 このテンプレートを使用するユーザがインスタント メッセージおよびプレゼンス情報を交換できるようにするには、[Unified CM IM and Presenceのユーザを有効化（Enable User for Unified CM IM and Presence）]チェックボックスをオンにします。

ステップ 6 ドロップダウン リストから、[サービスプロファイル（Services Profile）]および [ユーザプロファイル（User Profile）]を選択します。

ステップ 7 [機能グループ テンプレートの設定（Feature Group Template Configuration）]ウィンドウの残りのフィールドに入力します。 フィールドの説明については、オンライン ヘルプを参照してください。

ステップ 8 **[保存]** をクリックします。

次のタスク

新規エンド ユーザを追加します。 システムが会社の LDAP ディレクトリと統合されている場合は、LDAPディレクトリから直接ユーザをインポートできます。そうでない場合は、手動でエンド ユーザを作成します。

- LDAP からのエンド ユーザのインポート （56 ページ）
- エンド ユーザの手動追加 （57 ページ）

LDAP からのエンド ユーザのインポート

社内 LDAP ディレクトリから新しいエンド ユーザを手動でインポートするには、次の手順に従います。 LDAP 同期設定に、機能グループ テンプレートとユーザ プロファイル（ユニバーサル回線テンプレート、ユニバーサル デバイス テンプレートを含む）、および DN プールが含まれている場合、インポート プロセスによりエンド ユーザとプライマリ エクステンションが自動的に設定されます。

（注） 初回同期の実行後には、新しい設定（たとえば、機能グループテンプレートの追加）をLDAPディレクトリ同期に追加することはできません。 既存の LDAP 同期を編集する場合は、一括管理を使用するか、または新しい LDAP 同期を設定する必要があります。

始める前に

この手順を開始する前に、Cisco Unified Communications Manager が社内の LDAP ディレクトリとすでに同期していることを確認します。 LDAP同期には、ユニバーサル回線テンプレートおよびユニバーサル デバイス テンプレートと機能グループ テンプレートが含まれている必要があります。

手順

ステップ 1 Cisco Unified CM の管理で、**[システム（System）]** > **[LDAP（LADP）]** > **[LDAP ディレクトリ（LDAP Directory）]** を選択します。

ステップ 2 [検索（Find）]をクリックし、ユーザの追加先 LDAP ディレクトリを選択します。

ステップ 3 [完全同期を実施（Perform Full Sync）]をクリックします。
Cisco Unified Communications Manager が、外部の LDAP ディレクトリと同期します。 LDAP ディレクトリ内の新しいエンドユーザが Cisco Unified Communications Manager データベースにインポートされます。

次のタスク

セルフプロビジョニングが有効になっている場合、エンドユーザがセルフプロビジョニング自動音声応答（IVR）を使用して新しい電話機をプロビジョニングできます。有効になっていない場合は、次のタスクのいずれかを実行して、電話機をエンド ユーザに割り当てます。

- エンド ユーザ用の新しい電話機の追加 （58 ページ）
- エンド ユーザへの既存の電話機の移動 （59 ページ）

エンド ユーザの手動追加

次の手順を実行して、新しいエンドユーザを追加し、そのエンドユーザをアクセス コントロール グループとプライマリ回線内線番号を指定して設定します。

（注） ユーザを割り当てる役割の権限を持つアクセス制御グループがすでに設定されていることを確認してください。詳細については、「ユーザーアクセスの管理」の章を参照してください。

始める前に

ユニバーサル回線テンプレートを含むユーザ プロファイルが設定されていることを確認します。新しい内線番号を設定する必要がある場合は、Cisco Unified Communications Manager でユニバーサル回線テンプレートの設定を使用してプライマリ内線番号を設定します。

手順

ステップ 1 Cisco Unified CM Administration で、**[ユーザ管理（User Management）] > [ユーザ/電話の追加（User/Phone Add）] > [ユーザ/電話のクイック追加（Quick User/Phone Add）]** を選択します。

ステップ 2 ユーザの**ユーザID**と**姓**を入力します。

ステップ 3 [機能グループ テンプレート（Feature Group Template）]ドロップダウン リストで、機能グループ テンプレートを選択します。

ステップ 4 **[保存]** をクリックします。

ステップ 5 [ユーザ プロファイル（User Profile）]ドロップダウン リストで、選択したユーザ プロファイルにユニバーサル回線テンプレートが含まれていることを確認します。

ステップ 6 [アクセス コントロール グループ メンバーシップ（Access Control Group Membership）]セクションで、[+]アイコンをクリックします。

ステップ 7 [ユーザの所属グループ（User is a member of）]ドロップダウン リストで、アクセス コントロール グループを選択します。

ステップ 8 [プライマリ内線番号（Primary Extension）]の下で、[+]アイコンをクリックします。

ステップ 9 [内線番号（Extension）]ドロップダウン リストで、[（使用可能）（available）]として表示されている DN を選択します。

ステップ 10 すべての回線内線番号が [（使用済み）（used）]と表示されている場合は、次の手順を実行します。

a) [新規...（New...）]ボタンをクリックします。
[新規内線の追加（Add New Extension）]ポップアップが表示されます。

b) [電話番号（Directory Number）]フィールドに、新しい回線内線番号を入力します。

c) **[回線テンプレート（Line Template）]** ドロップダウン リストから、ユニバーサル回線テンプレートを選択します。

d) **OK**をクリックします。
Cisco Unified Communications Manager が、ユニバーサル回線テンプレートの設定を使用して電話番号を設定します。

ステップ 11 （任意） [ユーザ/電話のクイック追加設定（Quick User/Phone Add Configuration）]ウィンドウで、追加のフィールドに値を入力します。

ステップ 12 **[保存]** をクリックします。

次のタスク

次の手順のいずれかを実行して、このエンド ユーザに電話機を割り当てます。

- エンド ユーザ用の新しい電話機の追加 （58 ページ）
- エンド ユーザへの既存の電話機の移動 （59 ページ）

エンド ユーザ用の新しい電話機の追加

次の手順を実行して、新しいエンド ユーザまたは既存のエンド ユーザ用の新しい電話機を追加します。エンドユーザのユーザ プロファイルにユニバーサル デバイス テンプレートが含まれていることを確認します。 Cisco Unified Communications Manager が、ユニバーサル デバイス テンプレートの設定を使用して電話機を設定します。

始める前に

次の手順のいずれかを実行して、エンド ユーザを追加します。

- エンド ユーザの手動追加 （57 ページ）
- LDAP からのエンド ユーザのインポート （56 ページ）

手順

ステップ 1 Cisco Unified CM Administration で、**[ユーザ管理（User Management）]** > **[ユーザ/電話の追加（User/Phone Add）]** > **[ユーザ/電話のクイック追加（Quick User/Phone Add）]** を選択します。

ステップ 2 [検索（Find）] をクリックして、新しい電話機を追加するユーザを選択します。

ステップ 3 **[デバイスの管理（Manage Devices）]** ボタンをクリックします。

[デバイスの管理（Manage Devices）] ウィンドウが表示されます。

ステップ 4 [電話の新規追加（Add New Phone）] をクリックします。
[ユーザに電話を追加（Add Phone to User）] ポップアップが表示されます。

ステップ 5 [製品タイプ（Product Type）]ドロップダウン リストで、電話機モデルを選択します。

ステップ 6 **[デバイス プロトコル（Device Protocol）]** ドロップダウン リストから、プロトコルとして [SIP] または [SCCP] を選択します。

ステップ 7 [デバイス名（Device Name）]テキスト ボックスに、デバイスの MAC アドレスを入力します。

ステップ 8 [ユニバーサル デバイス テンプレート（Universal Device Template）] ドロップダウン リストで、ユニバーサル デバイス テンプレートを選択します。

ステップ 9 電話機が拡張モジュールをサポートしている場合は、展開する拡張モジュールの数を入力します。

ステップ 10 エクステンションモビリティを使用して電話機にアクセスするには、[エクステンションモビリティ内（In Extension Mobility）]チェック ボックスをオンにします。

ステップ 11 [電話の追加（Add Phone）]をクリックします。
[電話の新規追加（Add New Phone）] ポップアップが閉じます。 Cisco Unified Communications Manager が、電話機をユーザに追加し、ユニバーサル デバイス テンプレートを使用してその電話機を設定します。

ステップ 12 電話機の設定に追加の編集を加えるには、対応する鉛筆アイコンをクリックして、**[電話の設定（Phone Configuration）]** ウィンドウで電話機を開きます。

エンド ユーザへの既存の電話機の移動

次の手順を実行して、既存の電話機を新しいまたは既存のエンド ユーザに移動します。

手順

ステップ 1 Cisco Unified CM Administration で、**[ユーザ管理（User Management）]** > **[ユーザ/電話の追加（User/Phone Add）]** > **[ユーザ/電話のクイック追加（Quick User/Phone Add）]** を選択します。

ステップ 2 [検索（Find）] をクリックして、既存の電話機を移動するユーザを選択します。

ステップ 3 [デバイスの管理（Manage Devices）]ボタンをクリックします。

ステップ 4 [このユーザに移動する電話の検索（Find a Phone to Move To This User）]ボタンをクリックします。

ステップ 5 このユーザに移動する電話機を選択します。

ステップ 6 [選択項目の移動（Move Selected）]をクリックします。

エンド ユーザ PIN の変更

手順

ステップ 1 Cisco Unified Communications Manager Administration で、**[ユーザ管理（User Management）] > [エンド ユーザ（End User）]** を選択します。
[ユーザの検索と一覧表示（Find and List Users）]ウィンドウが表示されます。

ステップ 2 既存のユーザを選択するには、[ユーザを次の条件で検索（Find User where）]フィールドで適切なフィルタを指定し、[検索（Find）]をクリックしてユーザのリストを取得した後、リストからユーザを選択します。
[エンド ユーザ設定（End User Configuration）] ウィンドウが表示されます。

ステップ 3 [PIN]フィールドで、暗号化された既存の PIN をダブルクリックして、新しい PIN を入力します。 割り当てられている資格情報ポリシーに指定されている文字数以上（1 ～ 127 文字）を入力する必要があります。

ステップ 4 [PIN の確認（Confirm PIN）]フィールドで、既存の暗号化された PIN をダブルクリックし、もう一度、新しい PIN を入力します。

ステップ 5 **[保存]** をクリックします。

（注） Cisco Unity Connection の **[アプリケーションサーバの設定（Application Server Configuration）]** ウィンドウで **[エンドユーザ PIN の同期（End User Pin synchronization）]** チェックボックスが有効になっている場合は、エクステンションモビリティ、開催中の会議、モバイルコネクト、およびCisco Unity Connection ボイスメールに同じエンドユーザ PIN を使用してログインできます。 エンド ユーザは、同じ PIN を使用して、エクステンション モビリティにログインし、自分のボイスメールにアクセスできます。

エンド ユーザ パスワードの変更

LDAP 認証が有効になっている場合は、エンド ユーザ パスワードを変更できません。

手順

ステップ 1 Cisco Unified Communications Manager Administration で、**[ユーザ管理（User Management）] > [エンド ユーザ（End User）]** を選択します。
[ユーザの検索と一覧表示（Find and List Users）]ウィンドウが表示されます。

ステップ 2 既存のユーザを選択するには、[ユーザを次の条件で検索（Find User where）]フィールドで適切なフィルタを指定し、[検索（Find）]をクリックしてユーザのリストを取得した後、リストからユーザを選択します。
[エンド ユーザ設定（End User Configuration）] ウィンドウが表示されます。

ステップ 3 [パスワード（Password）]フィールドで、暗号化された既存のパスワードをダブルクリックして、新しいパスワードを入力します。割り当てられている資格情報ポリシーに指定されている文字数以上（1 ～ 127 文字）を入力する必要があります。

ステップ 4 [パスワードの確認（Confirm Password）]フィールドで、既存の暗号化されたパスワードをダブルクリックし、もう一度、新しいパスワードを入力します。

ステップ 5 **[保存（Save）]** をクリックします。

Cisco Unity Connection ボイス メールボックスの作成

始める前に

- Cisco Unified Communications Manager をボイス メッセージング用に設定する必要があります。 Cisco Unity Connection を使用するように Cisco Unified Communications Manager を設定する方法については、次で *Cisco Unified Communications Manager* システム設定ガイドを参照してください。

  http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html

- デバイスとプライマリ内線番号をエンド ユーザに関連付ける必要があります。
- このセクションで説明する手順を実行する代わりに、Cisco Unity Connection で使用可能なインポート機能を使用できます。 インポート機能の使用方法については、『*User Moves, Adds, and Changes Guide for Cisco Unity Connection*』を参照してください

手順

ステップ 1 Cisco Unified Communications Manager Administration で、**[ユーザ管理（User Management）]** > **[エンド ユーザ（End User）]** を選択します。
[ユーザの検索と一覧表示（Find and List Users）]ウィンドウが表示されます。

ステップ 2 既存のユーザを選択するには、[ユーザを次の条件で検索（Find User where）]フィールドで適切なフィルタを指定し、[検索（Find）]をクリックしてユーザのリストを取得した後、リストからユーザを選択します。
[エンド ユーザ設定（End User Configuration）] ウィンドウが表示されます。

ステップ 3 プライマリ内線番号がこのユーザに関連付けられていることを確認します。

（注） 主要内線番号を定義する必要があります。そうしなかった場合は、**[関連リンク（Related Links）]** ドロップダウンメニューに Cisco Unity ユーザリンクが表示されません。

ステップ 4 [関連リンク（Related Links）]ドロップダウン リストで、[Cisco Unity ユーザの作成（Create Cisco Unity User）]リンクを選択してから、[移動（Go）]をクリックします。

[Cisco Unity ユーザの追加（Add Cisco Unity User）]ダイアログボックスが表示されます。

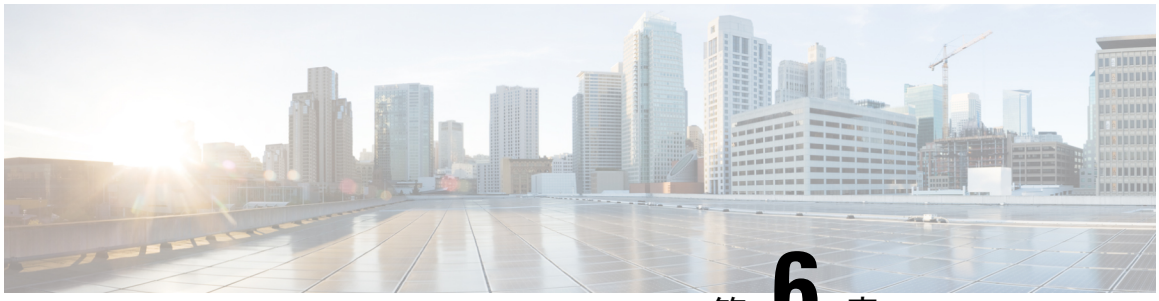
ステップ 5 **[アプリケーションサーバ（Application Server）]** ドロップダウンメニューで、Cisco Unity Connection ユーザを作成する Cisco Unity Connection サーバを選択してから、**[次へ（Next）]** をクリックします。

ステップ 6 [サブスクライバ テンプレート（Subscriber Template）] ドロップダウン リストで、使用するサブスクライバ テンプレートを選択します。

ステップ 7 **[保存]** をクリックします。

メールボックスが作成されます。 **[エンドユーザの設定（End User Configuration）]** ウィンドウの **[関連リンク（Related Links）]** ドロップダウンメニュー内のリンクが [Cisco Unity ユーザの編集（Edit Cisco Unity User）] に変化します。 これで、Cisco Unity Connection Administration で、作成したユーザを確認できます。

（注） Cisco Unity Connection ユーザと Cisco Unified Communications Manager エンドユーザを統合した後は、[エイリアス（Alias）]（Cisco Unified CM の管理内のユーザ ID）、[名（First Name）]、[姓（Last Name）]、[内線番号（Extension）]（Cisco Unified CM の管理内のプライマリ内線番号）などの Cisco Unified CM の管理内のフィールドを編集できなくなります。 これらのフィールドは、Cisco Unified CM の管理でしか更新できません。



第 6 章

アプリケーション ユーザの管理

アプリケーション ユーザの概要

Cisco Unified CM の管理の [アプリケーションユーザの設定（Application User Configuration）] ウィンドウで管理者は、Cisco Unified Communications Manager アプリケーション ユーザに関する情報を追加、検索、表示、および保守することができます。

Cisco Unified CM の管理には、デフォルトで以下のアプリケーション ユーザが設定されています。

- CCMAdministrator
- CCMSysUser
- CCMQRTSecureSysUser
- CCMQRTSysUser
- IPMASecureSysUser
- IPMASysUser
- WDSecureSysUser
- WDSysUser
- TabSyncSysUser
- CUCService

（注） Standard CCM Super Users グループの管理者ユーザは、Cisco Unified Communications Manager Administration、Cisco Unified Serviceability、および Cisco Unified Reporting のいずれかにシングル サインオンすることによって、このすべてのアプリケーションにアクセスできます。

アプリケーション ユーザのタスク フロー

手順

	コマンドまたはアクション	目的
ステップ 1	新規アプリケーション ユーザの追加（64 ページ）	新しいアプリケーション ユーザを追加します。
ステップ 2	デバイスとアプリケーション ユーザの関連付け （65 ページ）	アプリケーション ユーザに関連付けるデバイスを割り当てます。
ステップ 3	Cisco Unity または Cisco Unity Connection への管理者ユーザの追加 （65 ページ）	Cisco Unity または Cisco Unity Connection に管理者ユーザとしてユーザを追加します。 Cisco Unified CM の管理でアプリケーション ユーザを設定します。その後で、Cisco Unity または Cisco Unity Connection で、そのユーザの追加の設定を構成します。
ステップ 4	アプリケーション ユーザ パスワードの変更 （67 ページ）	アプリケーション ユーザ パスワードを変更します。
ステップ 5	アプリケーション ユーザ パスワード クレデンシャル情報の管理 （67 ページ）	関連する認証ルール、関連するクレデンシャル ポリシー、アプリケーション ユーザの直前のパスワード変更の時刻などのクレデンシャル情報を変更または表示します。

新規アプリケーション ユーザの追加

手順

ステップ 1 Cisco Unified CM の管理で **[ユーザの管理（User Management）] > [アプリケーション ユーザ（Application User）]** を選択します。

ステップ 2 [新規追加] をクリックします。

ステップ 3 [アプリケーション ユーザの設定（Application User Configuration）] 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 4 **[保存（Save）]** をクリックします。

次のタスク

デバイスとアプリケーション ユーザの関連付け （65 ページ）

デバイスとアプリケーション ユーザの関連付け

手順

ステップ 1 Cisco Unified CM Administration から、**[ユーザ管理（User Management）] > [アプリケーション ユーザ（Application User）]** を選択します。
[ユーザの検索と一覧表示（Find and List Users）]ウィンドウが表示されます。

ステップ 2 既存のユーザを選択するには、[次の条件でユーザを検索（Find User Where）]フィールドに適切なフィルタを指定し、[検索（Find）]を選択してユーザのリストを取得し、リストからユーザを選択します。

ステップ 3 [使用可能なデバイス（Available Devices）]リストで、アプリケーション ユーザに関連付けするデバイスを選択し、リストの下にある**下向き矢印**をクリックします。 選択したデバイスが[制御対象のデバイス（Controlled Devices）]リストに移動します。

（注） 使用可能なデバイスのリストを制限するには、[別の電話を検索（Find more Phones）]ボタンまたは [別のルート ポイントを検索（Find more Route Points）]ボタンをクリックします。

ステップ 4 [別の電話を検索（Find more Phones）]ボタンをクリックすると、[電話の検索/一覧表示（Find and List Phones）]ウィンドウが表示されます。 検索を実行して、このアプリケーション ユーザに関連付ける電話機を検索します。

アプリケーション ユーザに割り当てるデバイスごとに、上記ステップを繰り返します。

ステップ 5 [別のルート ポイントを検索（Find more Route Points）]ボタンをクリックすると、[CTI ルート ポイントの検索/一覧表示（Find and List CTI Route Points）]ウィンドウが表示されます。 検索を実行して、このアプリケーション ユーザに関連付ける CTI ルート ポイントを検索します。

アプリケーション ユーザに割り当てるデバイスごとに、上記ステップを繰り返します。

ステップ 6 **[保存（Save）]** をクリックします。

Cisco Unity または Cisco Unity Connection への管理者ユーザの追加

Cisco Unified Communications Manager と Cisco Unity Connection 7.x 以降を統合する場合は、このセクションで説明する手順を実行する代わりに、Cisco Unity Connection 7.x 以降で使用可能なインポート機能を使用できます。 インポート機能の使用方法については、次で『Cisco Unity Connection 7.x 以降の *User Moves, Adds, and Changes* ガイド』を参照してください。

http://www.cisco.com/c/en/us/support/unified-communications/unity-connection/products-maintenance-guides-list.html.

Cisco Unity または Cisco Unity Connection ユーザが Cisco Unified CM アプリケーション ユーザと統合されている場合は、フィールドを編集できません。 これらのフィールドは、Cisco Unified Communications Manager Administration でしか更新できません。

Cisco Unity と Cisco Unity Connection は、Cisco Unified Communications Manager からのデータの同期をモニタします。 ツール メニューの [Cisco Unity Administration]または [Cisco Unity Connection Administration]で同期時刻を設定できます。

始める前に

Cisco Unity または Cisco Unity Connection にプッシュする予定のユーザに適切なテンプレートが定義されていることを確認します

[Cisco Unity ユーザの作成（Create Cisco Unity User）]リンクは、適切な Cisco Unity または Cisco Unity Connection ソフトウェアがインストールされ、設定されている場合にのみ表示されます。 Cisco Unity に関する『*Cisco Unified Communications Manager Integration Guide*』または Cisco Unity Connection に関する『*Cisco Unified Communications Manager SCCP Integration Guide*』を次で参照してください。

http://www.cisco.com/c/en/us/support/unified-communications/unity-connection/products-installation-and-configuration-guides-list.html.

手順

ステップ 1 Cisco Unified CM Administration から、**[ユーザ管理（User Management）] > [アプリケーション ユーザ（Application User）]** を選択します。

ステップ 2 既存のユーザを選択するには、[次の条件でユーザを検索（Find User Where）]フィールドに適切なフィルタを指定し、[検索（Find）]を選択してユーザのリストを取得し、リストからユーザを選択します。

ステップ 3 [関連リンク（Related Links）]ドロップダウン リストで、[Cisco Unity アプリケーション ユーザの作成（Create Cisco Unity Application User）]リンクを選択し、[移動（Go）]をクリックします。
[Cisco Unity ユーザの追加（Add Cisco Unity User）]ダイアログが表示されます。

ステップ 4 [アプリケーション サーバ（Application Server）]ドロップダウン リストで、Cisco Unity または Cisco Unity Connection ユーザを作成する Cisco Unity または Cisco Unity Connection サーバを選択し、[次へ（Next）]をクリックします。

ステップ 5 [アプリケーション ユーザ テンプレート（Application User Template）] ドロップダウン リストで、使用するテンプレートを選択します。

ステップ 6 **[保存]** をクリックします。
Cisco Unity または Cisco Unity Connection で管理者アカウントが作成されます。 **[アプリケーション ユーザの設定（Application User Configuration）]** ウィンドウの [関連リンク（Related Links）] 内のリンクが **[Cisco Unity ユーザの編集（Edit Cisco Unity User）]** に変化します。 これで、Cisco Unity Administration または Cisco Unity Connection Administration で作成したユーザを表示できるようになります。

アプリケーション ユーザ パスワードの変更

手順

ステップ 1 Cisco Unified CM Administration から、**[ユーザ管理（User Management）] > [アプリケーション ユーザ（Application User）]** を選択します。
[ユーザの検索と一覧表示（Find and List Users）]ウィンドウが表示されます。

ステップ 2 既存のユーザを選択するには、[次の条件でユーザを検索（Find User Where）]フィールドに適切なフィルタを指定し、[検索（Find）]を選択してユーザのリストを取得し、リストからユーザを選択します。
[アプリケーション ユーザの設定（Application User Configuration）]ウィンドウに、選択されたアプリケーション ユーザに関する情報が表示されます。

ステップ 3 [パスワード（Password）]フィールドで、既存の暗号化されたパスワードをダブルクリックし、新しいパスワードを入力します。

ステップ 4 [パスワードの確認（Confirm Password）]フィールドで、既存の暗号化されたパスワードをダブルクリックし、もう一度、新しいパスワードを入力します。

ステップ 5 **[保存（Save）]** をクリックします。

アプリケーション ユーザ パスワード クレデンシャル情報の管理

次の手順を実行して、アプリケーション ユーザ パスワードに関するクレデンシャル情報を管理します。 これにより、パスワードのロック、パスワードへのクレデンシャル ポリシーの適用、最後に失敗したログイン試行時などの情報の表示などの管理業務を実行できます。

手順

ステップ 1 Cisco Unified CM Administration から、**[ユーザ管理（User Management）] > [アプリケーション ユーザ（Application User）]** を選択します。
[ユーザの検索と一覧表示（Find and List Users）]ウィンドウが表示されます。

ステップ 2 既存のユーザを選択するには、[次の条件でユーザを検索（Find User Where）]フィールドに適切なフィルタを指定し、[検索（Find）]を選択してユーザのリストを取得し、リストからユーザを選択します。
[アプリケーション ユーザの設定（Application User Configuration）]ウィンドウに、選択されたアプリケーション ユーザに関する情報が表示されます。

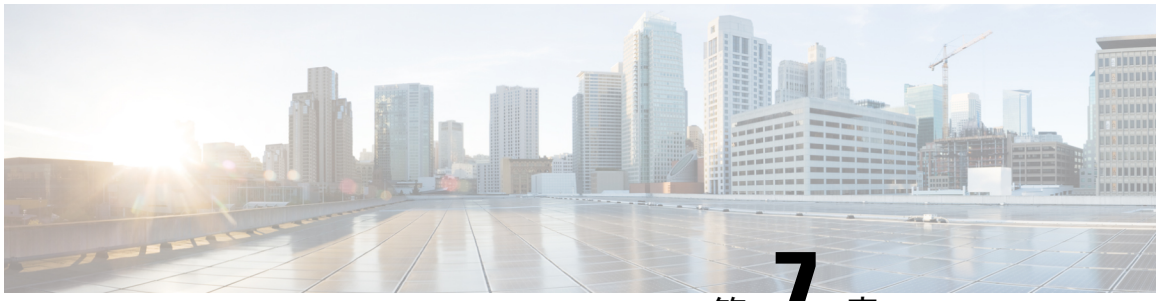
ステップ 3 パスワード情報を変更または表示するには、[パスワード（Password）]フィールドの横にある[クレデンシャルの編集（Edit Credential）]ボタンをクリックします。
ユーザの [クレデンシャル設定（Credential Configuration）]が表示されます。

ステップ 4 [クレデンシャル設定（Credential 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 5 いずれかの設定を変更した場合は、[保存（Save）]をクリックします。

第 III 部

デバイスの管理



第 7 章

電話の管理

電話管理の概要

この章では、ネットワーク内の電話を管理する方法について説明します。 このトピックでは、新しい電話の追加、既存の電話の別のユーザへの移動、電話のロック、電話のリセットなどのタスクについて説明します。

ご使用の電話機モデルの『Cisco IP 電話 アドミニストレーションガイド』には、該当する電話機モデルに固有の設定情報が記載されています。

[電話ボタンテンプレート(Phone Button Template)]

電話ボタン テンプレートは、電話機モデルに基づいて作成されます。 一部の電話機モデルでは、特定の電話ボタンテンプレートを使用しませんが、一部電話機モデルには、個々のテンプレートまたはデバイスのデフォルトテンプレートのいずれかの特定されたテンプレートが必要です。

[エンタープライズ パラメータの設定（Enterprise Parameters Configuration）] ページの [非サイズ セーフ電話機の電話テンプレートの選択（Phone Template Selection for Non-Size Safe Phone）] と[自動登録レガシー モード（Auto Registration Legacy Mode）] エンタープライズ パラメータは、使用される電話ボタン テンプレートのタイプを指定します。 フィールドの詳細については、オンライン ヘルプを参照してください。

表 *4:* さまざまなシナリオにおける電話ボタン テンプレート

非サイズ セーフ電話機の電話テンプレートの選択	自動登録レガシー モード	電話（Phone）
個々のテンプレートの作成	False	ユニバーサル デバイス テンプレートからの電話を追加するときに、個々の電話ボタン テンプレートが作成されます。
デバイスのデフォルトからのテンプレートの使用	False	個々の電話ボタン テンプレートは作成されず、デバイスのデフォルトからの電話ボタン テンプレートを取得します。
デバイスのデフォルトからのテンプレートの使用	True	デバイス プール、電話テンプレート、コーリング サーチ スペース、電話ボタン テンプレートの値は、デバイスのデフォルトから取得されます。
個々のテンプレートの作成	True	デバイス プール、電話テンプレート、コーリング サーチ スペース、電話ボタン テンプレートの値は、デバイスのデフォルトから取得されます。 個々のテンプレートは作成されません。 自動登録レガシー モードには、優先度があります。

電話機管理タスク

手順

	コマンドまたはアクション	目的
ステップ 1	エンドユーザの有無にかかわらないテンプレートからの新しい電話機の追加（74 ページ）	エンドユーザの有無にかかわらないユニバーサル デバイス テンプレートからの新しい電話機の追加
ステップ 2	電話機の手動での追加 （73 ページ）	デバイス テンプレートなしでのエンドユーザの新しい電話機の追加

	コマンドまたはアクション	目的
ステップ 3	エンドユーザがあるテンプレートからの新しい電話機の追加 （76 ページ）	エンドユーザ用の新しい電話機を追加して、ユニバーサル デバイス テンプレートを割り当てます。
ステップ 4	既存の電話機の移動 （85 ページ）	設定された電話機を別のエンドユーザに移動します。
ステップ 5	現在ログイン中のデバイスの検索 （86 ページ）	特定のデバイスを検索するか、ユーザが現在ログインしているすべてのデバイスを列挙します。
ステップ 6	リモートでログイン中のデバイスの検索 （87 ページ）	特定のデバイスを検索するか、ユーザがリモートでログインしているすべてのデバイスを列挙します。
ステップ 7	電話機のリモート ロック （88 ページ）	一部の電話機は、リモートでロックすることができます。 電話機をリモートでロックすると、ロックを解除するまで使用できなくなります。
ステップ 8	工場出荷時の初期状態への電話機のリセット （88 ページ）	電話機を工場出荷時の設定にリセットします。
ステップ 9	電話ロック/ワイプレポート （89 ページ）	リモートでロックされたデバイスまたはリモートでファクトリーデフォルト設定にリセットされたデバイスを検索します。
ステップ 10	電話の LSC ステータスの表示および CAPF レポートの生成 （90 ページ）	電話機で LSC 失効ステータスを検索し、CAPF レポートも生成します。

電話機の手動での追加

次の手順を実行して、ユーザ用の新しい電話機を手動で追加します。

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified CM Administration）] から、**[デバイス（Device）] > [電話（Phone）] > [電話の検索とリスト（Find and List Phones）]** の順に選択します。

ステップ 2 [電話の検索とリスト（Find and List Phones）] ページから [新規追加（Add New）] をクリックして電話機を手動で追加します。

[新しい電話の追加（Add a New Phone）] ページが表示されます。

[新しい電話の追加（Add a New Phone）] ページから、[「ここをクリックしてユニバーサル デバイス テンプレートを追加（click here to add a new phone using a Universal Device Template）」] ハイパーリンクをクリックすると、ページは [新しい電話の追加（Add a New Phone）] ページにリダイレクトされ、ユーザの追加の有無にかかわらずテンプレートから電話を追加します。詳細については、エンドユーザの有無にかかわらないテンプレートからの新しい電話機の追加（74 ページ）を参照してください。

ステップ 3 [電話のタイプ（Phone Type）] ドロップダウンリストから、電話機モデルを選択します。

ステップ 4 [次へ（Next）] をクリックします。
[電話機の設定（Phone Configuration）] ページが表示されます。

ステップ 5 [電話機の設定（Phone Configuration）] ページで、必須フィールドに値を入力します。 フィールドの詳細については、オンライン ヘルプを参照してください。

[製品固有の設定（Product Specific Configuration）] 領域のフィールドの詳細については、ご使用の電話機モデルの『*Cisco IP Phone Administration Guide*』を参照してください。

ステップ 6 電話の設定を保存する場合は、[保存（Save）] をクリックします。

次のタスク

エンド ユーザへの既存の電話機の移動 （59 ページ）

エンドユーザの有無にかかわらないテンプレートからの新しい電話機の追加

次の手順を実行して、ユーザを追加するかどうかにかかわらず、テンプレートから新しい電話機を追加します。 Cisco Unified Communications Manager が、ユニバーサル デバイス テンプレートの設定を使用して電話機を設定します。

始める前に

Cisco Unified Communications Manager でユニバーサル デバイス テンプレートが設定済みであることを確認します。

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified CM Administration）] から、**[デバイス（Device）] > [電話（Phone）] > [電話の検索とリスト（Find and List Phones）]** の順に選択します。

ステップ 2 [電話の検索とリスト（Find and List Phones）] ページから、[テンプレートからの新規の追加（Add New From Template）] をクリックして、エンド ユーザの追加にかかわりなくデバイス テンプレートからの電話を追加します。

[新しい電話の追加（Add a New Phone）] ページが表示されます。

[新しい電話の追加（Add a New Phone）] ページから、[「ここをクリックしてすべての電話設定を手動で入力する（click here to enter all phone settings manually）」] ハイパーリンクをクリックすると、ページは電話を手動で追加できる既存の [新しい電話の追加（Add a New Phone）] ページにリダイレクトされます。 詳細については、電話機の手動での追加 （73 ページ）を参照してください。

ステップ 3 [製品タイプ（およびプロトコル）（Phone Type (and Protocol)）] ドロップダウン リストで、電話機モデルを選択します。

プロトコルのドロップダウンリストは、電話が複数のプロトコルをサポートしている場合にのみ表示されます。

ステップ 4 [名前または MAC アドレス（Name or MAC Address）]テキスト ボックスに、名前または MAC アドレスを入力します。

ステップ 5 [デバイステンプレート（Device Template）] ドロップダウン リストで、ユニバーサル デバイス テンプレートを選択します。

ステップ 6 [電話番号（回線1）（Directory Number (Line 1)）] ドロップダウンリストで、電話番号を選択します。

ドロップダウンリストのディレクトリ番号がドロップダウンリストの上限を越えている場合、[検索（Find）]タブが表示されます。[検索（Find）]をクリックすると、ディレクトリ番号の検索条件を示すポップアップ ダイアログボックスが開きます。

ステップ 7 （オプション）新しいディレクトリ番号を作成してデバイスに割り当てる場合には、[新規（New）]をクリックしてディレクトリ番号を入力し、ユニバーサル回線テンプレートを選択します。

[ユーザ管理（User Management）] > [ユーザ/電話の追加（User/Phone Add）] > [ユーザ/電話のクイック追加（Quick/User Phone Add）] に移動して、ユーザに関連付けられたディレクトリ番号を使用して電話を作成することもできます。

ステップ 8 （オプション）[ユーザ（User）] ドロップダウンリストから、新しい電話機を追加するエンドユーザを選択します。

（注） Cisco デュアル モード（モバイル）デバイスのユーザを選択する場合には必須です。

ドロップダウンリストのエンドユーザ数が最大ドロップダウン数を超えると、**[検索（Find）]** タブが表示されます。**[検索（Find）]**をクリックすると、「エンドユーザーの検索基準を検索する」というポップアップダイアログボックスが表示されます。

ステップ 9 **[Add（追加）]** をクリックします。

（注） 非サイズセーフ電話機の場合、電話テンプレートは [エンタープライズパラメータの設定（Enterprise Parameters Configuration）] ページの [非サイズ セーフ電話機の電話テンプレートの選択（Phone Template Selection for Non-Size Safe Phone）] と [自動登録レガシー モード（Auto Registration Legacy Mode）] パラメータの選択に基づいて作成されます。

追加が成功したとのメッセージが表示されます。 Cisco Unified Communications Manager で電話機が追加され、[電話の設定（Phone Configuration）]ページが表示されます。 [電話の設定（Phone

Configuration）]ページのフィールドの詳細については、オンライン ヘルプを参照してください。

次のタスク

エンド ユーザへの既存の電話機の移動 （59 ページ）

エンド ユーザがあるテンプレートからの新しい電話機の追加

次の手順を実行して、エンド ユーザ用の新しい電話機を追加します。

始める前に

電話機追加対象のエンド ユーザは、ユニバーサル デバイス テンプレートを含むユーザ プロファイルがセットアップされています。 Cisco Unified Communications Manager が、ユニバーサル デバイス テンプレートの設定を使用して電話機を設定します。

- エンド ユーザ管理タスク （49 ページ）

手順

ステップ 1 Cisco Unified CM Administration で、**[ユーザ管理（User Management）] > [ユーザ/電話の追加（User/Phone Add）] > [ユーザ/電話のクイック追加（Quick User/Phone Add）]** を選択します。

ステップ 2 [検索（Find）] をクリックして、新しい電話機を追加するユーザを選択します。

ステップ 3 **[デバイスの管理（Manage Devices）]** ボタンをクリックします。
[デバイスの管理（Manage Devices）] ウィンドウが表示されます。

ステップ 4 [電話の新規追加（Add New Phone）] をクリックします。
[ユーザに電話を追加（Add Phone to User）] ポップアップが表示されます。

ステップ 5 [製品タイプ（Product Type）]ドロップダウン リストで、電話機モデルを選択します。

ステップ 6 **[デバイス プロトコル（Device Protocol）]** ドロップダウン リストから、プロトコルとして [SIP] または [SCCP] を選択します。

ステップ 7 [デバイス名（Device Name）]テキスト ボックスに、デバイスの MAC アドレスを入力します。

ステップ 8 [ユニバーサル デバイス テンプレート（Universal Device Template）]ドロップダウン リストで、ユニバーサル デバイス テンプレートを選択します。

ステップ 9 電話機が拡張モジュールをサポートしている場合は、展開する拡張モジュールの数を入力します。

ステップ 10 エクステンション モビリティを使用して電話機にアクセスするには、[エクステンション モビリティ内（In Extension Mobility）]チェック ボックスをオンにします。

ステップ 11 [電話の追加（Add Phone）]をクリックします。

[電話の新規追加（Add New Phone）] ポップアップが閉じます。 Cisco Unified Communications Manager が、電話機をユーザに追加し、ユニバーサル デバイス テンプレートを使用してその電話機を設定します。

ステップ 12 電話機の設定に追加の編集を加えるには、対応する鉛筆アイコンをクリックして、**[電話の設定（Phone Configuration）]** ウィンドウで電話機を開きます。

コラボレーション モバイル コンバージェンス仮想デバイスの概要

CMC デバイスは、それに関連付けられたリモート接続先を表す仮想デバイスです。 エンタープライズ電話で CMC デバイスにコールすると、コールはリモート接続先にリダイレクトされます。この機能は、デバイス タイプ [Collaboration モバイル コンバージェンス（Collaboration Mobile Convergence）] を作成することを目的としています。このデバイス タイプはいくつかのカスタマイズがされた Spark リモート デバイスと同じであり、以下の利点を提供します。

- Spark リモート デバイスと同様の機能を持つネイティブ モバイル デバイスを Cisco Unified Communications Manager 上でサポートします。
- 将来の開発機能パリティを含む機能を持つ Spark-RD として利用します。
- モバイルからデスクフォン、デスクフォンからモバイルへコールの移動などの、モバイル固有のユース ケースのカスタマイズができます。 （ID ページで deskpickup タイマーを追加し、製品サポート機能の設定で有効にします）。
- CMC デバイスは、ハント グループに含めることができます。
- Spark リモート デバイスで共有回線に対応できます。
- ライセンス：ライセンス使用パースペクティブに応じて個別のデバイスとしてカウントします。 複数デバイス ライセンス バンドルはいずれも、CMC RD をサポートする必要があります。

CMC RD デバイス ライセンスの調整

新しいCMCデバイスは、追加されると、ユーザに関連付けられているデバイスの数/タイプに基づいてライセンスを使用します。CMCデバイスによって使用されるライセンスのタイプは、それに関連付けられているエンド ユーザが所有するデバイスの数によって異なります。

- CMC デバイスのみを導入する場合は、拡張ライセンスを使用します。
- CMC デバイスと Spark RD を導入する場合は、拡張ライセンスを使用します。
- CMC と物理デバイス：拡張 Plus ライセンス
- CMC、Spark RD、および物理デバイスの場合：拡張 Plus ライセンス

Collaboration モバイル コンバージェンスの仮想デバイスの追加

エンド ユーザ用に Cisco Collaboration モバイル コンバージェンス（CMC）リモート デバイスを追加する次の手順を実行します。

始める前に

電話機追加対象のエンド ユーザは、ユニバーサル デバイス テンプレートを含むユーザ プロファイルがセットアップされている必要があります。 Cisco Unified Communications Manager が、ユニバーサル デバイス テンプレートの設定を使用して電話機を設定します。

手順

ステップ 1 Cisco Unified CM 管理で、**[デバイス]** > **[電話]** を選択します。

ステップ 2 [新規追加（Add New）]ボタンをクリックします。

ステップ 3 [ここをクリックしてすべての電話設定を手動で入力する（Click here to enter all phone settings manually）]リンクをクリックします。
[新規電話を追加（Add a New Phone）]ウィンドウが表示されます。

ステップ 4 [電話のタイプ（Phone Type）] ドロップダウン リストから、[Cisco Collaboration モバイル コンバージェンス（Cisco Collaboration Mobile Convergence）] を選択し、[次へ（Next）] をクリックします。
[電話の設定（Phone Configuration）]ウィンドウが表示されます。

ステップ 5 [オーナーのユーザ ID（Owner User ID）]ドロップダウンから、デバイスを所有するエンドユーザを選択します。

ステップ 6 [デバイス プール（Device Pool）]ドロップダウンから、デバイス プールを選択します。

ステップ 7 **[保存]** をクリックします。
[設定の適用（Apply Config）] ボタンをクリックして変更を有効にすることを求める警告メッセージがポップアップします。 [OK]をクリックします。 デバイスは正常に追加されました。

ステップ 8 [電話番号（Directory Number）] を設定するには、追加された CMC デバイスをクリックし、[電話番号（Directory Number）] を入力して、[保存（Save）] をクリックします。

ステップ 9 追加された CMC デバイスの新しい [リモート接続先（Remote Destination）] を追加するには、アイデンティティ ボックス内のリンクをクリックします。

ステップ 10 [リモート接続先の設定（Remote Destination Configuration）] ウィンドウで、[名前（Name）]、[接続先の番号（Destination number）] をクリックして、[保存（Save）] をクリックします。

（注） 追加された 1 つの CMC デバイスに対して、1 つだけのリモート接続先を追加できます。

ステップ 11 既存のリモート接続先を更新するには、[新しい名前（New Name）] をクリックして、[保存（Save）]をクリックします。

ステップ 12 既存のリモート接続先を削除するには、メニューで [削除（Delete）] ボタンをクリックします。
永続的な削除を確認する Web ページからのメッセージが表示されます。 [OK]をクリックします。

ステップ 13 [デバイス（Device）]ページからCMCデバイスを削除するには、[デバイス（Device）]チェック ボックスを選択し、メニューから [選択の削除（Delete Selected）] をクリックします。

CMC RD 機能の相互作用

表 *5 : CMC RD* 機能の相互作用

機能	データのやり取り
共有回線の処理	• CMC RD および Spark RD と関連付けられている共有デスク フォンがあるセットアップで、ユーザがエンタープライズ電話から CMC デバイス DN にコールすると、CMC RD、Spark RD、および共有デスク フォンの 3 つすべてが鳴ります。 • リモート接続先のいずれかから応答すると、共有デスク フォンに「リモートで使用中（Remote in Use）」メッセージが表示されます。 • 共有デスク フォンのいずれかから応答すると、両方のリモート接続先電話（CMC RD と Spark RD 電話）が切断されます。
Call Manager グループ（CMG）セットアップで動作する CMC デバイス	• CMC デバイスが Call Manager グループに関連付けられている場合は、必ずプライマリ サーバで実行され、プライマリ サーバがダウンした場合にのみ、Call Manager グループの次のアクティブなセカンダリ サーバで実行されます。 • プライマリ サーバがコール中にダウンした場合、進行中のコールは引き続き維持され、コールが終了した後にCMCデバイスがセカンダリ サーバに登録されます。 （注） コールが保持モードの場合、電話間のメディアは引き続きアクティブですが、コールの切断を除く他の操作は実行できません。 • 最初にプライマリ サーバがダウンし、CMCデバイスがセカンダリ サーバに登録されているときにコールが開始され、プライマリ サーバが進行中のコール中に起動した場合、コールは保持モードになり、コールの終了後にCMCデバイスがプライマリ サーバに登録されます。

機能	データのやり取り
コール アンカリング	CMCデバイスからのすべての基本着信コールおよび番号からリモート接続先へのコールは、エンタープライズ ネットワークでは固定されています。 CMCのリモートデバイスが設定されている場合、エンタープライズに固定されているすべてのコールにより、ユーザはモバイル デバイスからコールを発信および受信できます。 • ユーザは、エンタープライズ番号からCMCリモート宛先に直接ダイヤルすることができます。コールはエンタープライズネットワークでは固定されています。 このシナリオでは、デスク フォン（CMCデバイスの共有回線）は鳴りませんが、[リモートで使用中（Remote in Use）] の状態のままになります。 • ユーザは、CMCリモート接続先から任意のエンタープライズ番号にダイヤルできます。 コールは固定されています。このシナリオでは、デスク フォン（CMCデバイスの共有回線）は鳴りませんが、[リモートで使用中（Remote in Use）] の状態のままになります。

機能	データのやり取り
シングル ナンバー リーチ	• [リモート接続先の設定（Remote Destination configuration）] ページで、[シングル ナンバー リーチを有効にする（Enable Single Number Reach）] チェックボックスがオフになっている場合、コールは CMC RD まで拡張されず、拒否されます。 • リモート接続先からの着信コールと、[番号からリモート接続先へ（Number to Remote Destination）] の発信コールは、[シングル ナンバー リーチを有効にする（Enable Single Number Reach）] チェックボックスの選択に関係なく、影響を受けません。 • CMC デバイスがある共有デスク フォンがあり、[シングル ナンバー リーチを有効にする（Enable Single Number Reach）] チェックボックスがオフになっている場合、コールは CMC RD ではなく共有デスク フォンに拡張されます。 （注） **[シングル ナンバー リーチ ボイスメール ポリシー（Single Number Reach Voicemail Policy）]** が **[ユーザ制御（user control）]** に設定されている場合は、主要内線番号への**ブラインド転送**が行われても、モビリティの通知先番号はトリガー**されません**。プライマリ内線番号のみがトリガーされます。 [**ユーザ制御（User control）**] 設定は、打診転送をサポートしています。[**タイマー制御（Timer Control）**] のボイスメール回避ポリシーは、打診転送とブラインド転送の両方をサポートしています。

機能	データのやり取り
時刻（ToD）に基づくコール ルーティング	• リング スケジュールを設定するために、リモート接続先の [時刻（Time of Day）] 設定を使用できます（たとえば、月曜日から金曜日の 9 am ～ 5 pm などといった特定の時間を設定できます）。 コールは、これらの時間にのみリモート接続先にリダイレクトされます。 エンタープライズ電話からCMC番号へのコールは、[リモート接続先の設定（Remote Destination configuration）] ページで修正されたリング スケジュールに基づいてルーティングされます。 リング スケジュールは次のように指定できます。 • [すべての時間（All the Time）]：コールは常時ルーティングされます。 制限はありません。 • [曜日（Day(s) of the week）]: 選択した特定の曜日にのみコールはルーティングされます。 • [特定の時間（Specific time）]：コールは選択した就業時間内にのみルーティングされます。 必ずタイムゾーンを選択します。 • リング スケジュール中にコールを受信する場合、エンタープライズ電話から CMC 番号へのコールは、[リモート接続先の設定（Remote Destination configuration）] ページでアクセス許可リストまたはアクセスブロッキング リストに追加されたコール番号またはパターンに基づいてルーティングされます。 • [アクセス許可リスト（Allowed access list）]：発信者番号またはパターンがアクセス許可リスト内にある場合にのみ接続先が鳴ります。 • [アクセス ブロッキング リスト（Blocked access list）]：発信者番号またはパターンがアクセス ブロッキング リスト内にある場合には接続先は鳴りません。 （注） 任意の時点で、アクセス許可リストまたはアクセス ブロッキング リストのみを使用できます。

機能	データのやり取り
ユーザ ロケールの設定	CMC 仮想デバイスでは、[電話の設定（Phone Configuration）] ウィンドウで設定されているロケール設定を使用して、電話のディスプレイと電話アナウンスのロケールを判断します。 このポリシーは、通常のコールと Conference Now 番号に適用されます。 アナウンスの部分は、[ユーザ ロケール（User Locale）] の設定で同じ言語が選択された発信側（任意のエンタープライズ電話）および着信側（CMC デバイス）電話では、発信側とリモート接続先の両方のアナウンスは、[電話の設定（Phone Configuration）] ページで選択された [ユーザ ロケール（User Locale）] 設定に基づくものになります。 （注） たとえば、CMC デバイスに関連付けられている [リモート接続先（Remote Destination）] から [Conference Now 番号（Conference Now 番号）]に発信するときに、アナウンスは CMC デバイスの [電話の設定（Phone configuration）] ページで選択されている [ユーザ ロケール（User Locale）] の設定に基づくものになります。
HLogin および HLogout の新しいアクセス コード	この機能は、管理者が追加のサービス パラメータを使用して、CMC デバイスのハント グループのログインおよびログアウト数を設定するために役立ちます。 • ハント グループ ログインのためのエンタープライズ機能アクセス番号。 • ハント グループ ログアウトのためのエンタープライズ機能アクセス番号。 ユーザが CMC デバイスに関連付けられている RD から Hlogin 番号を入力すると、そのときに限りコールは CMC デバイスに関連付けられているハント パイロット番号のダイヤル時に RD にリダイレクトされます。 ユーザが CMC デバイスに関連付けられている RD から Hlogout 番号を入力すると、コールは CMC デバイスに関連付けられているハント パイロット番号のダイヤル時に RD にリダイレクトされません。 デフォルトでは、CMC デバイスは Hloggedin です。 いずれの場合でも、CMC デバイスへの直接コールには影響はありません。

機能	データのやり取り
データベースに設定された [呼び出し前の遅延タイマー（Delay Before Ringing Timer）] に基づく CMC リモート接続先コール エクステンション	**DB の [呼び出し前の遅延タイマー（Delay Before Ringing Timer）] が 5000 に設定されている場合** • エンタープライズ電話から CMC 番号に発信する場合、共有回線が鳴り、コールは 5 秒後にリモート接続先に到達します。 • エンタープライズ電話から CMC 番号に発信する場合、共有回線が 5 秒前にコールに応答すると、コールはリモート接続先に拡張されません。 • エンタープライズ電話から CMC 番号に発信する場合、共有回線が鳴り、発信側が 5 秒前にコールを切断すると、コールはリモート接続先に拡張されません。 **DB の [呼び出し前の遅延タイマー（Delay Before Ringing Timer）] が 0 に設定されている場合** エンタープライズ電話から CMC 番号へのすべてのコールは、リモート接続先と共有回線に同時にアラートを出します。
一括管理ツール（BAT）サポート	BAT サポートは CMC デバイス向けに提供されています

CMC RD 機能の制約事項

表 *6 : CMC RD* 機能の制約事項

機能	制約事項
CMC リモート接続先の関連付け	次の制約事項が適用されます。 • CMC デバイスには、1 つのリモート接続先のみを関連付けることができます。 . • エンド ユーザが削除されると、その関連付けられている CMC デバイスおよび RD（リモート接続先）も削除されます。 （注） [モビリティの有効化（Enable Mobility）] チェック ボックスがオンまたはオフになっていても、CMC および RD は影響を受けません。 CMC デバイスは削除されません。 （注） Cisco Unified Communications Manager は、CMC デバイスのコール ハンドル保護をサポートしていません。

既存の電話機の移動

次の手順を実行して、設定された電話機をエンド ユーザに移動します。

手順

ステップ 1 Cisco Unified CM Administration で、**[ユーザ管理（User Management）] > [ユーザ/電話の追加（User/Phone Add）] > [ユーザ/電話のクイック追加（Quick User/Phone Add）]** を選択します。

ステップ 2 [検索（Find）] をクリックして、既存の電話機を移動するユーザを選択します。

ステップ 3 [デバイスの管理（Manage Devices）]ボタンをクリックします。

ステップ 4 [このユーザに移動する電話の検索（Find a Phone to Move To This User）]ボタンをクリックします。

ステップ 5 このユーザに移動する電話機を選択します。

ステップ 6 [選択項目の移動（Move Selected）]をクリックします。

現在ログイン中のデバイスの検索

Cisco Extension Mobility 機能と Cisco Extension Mobility Cross Cluster 機能により、ユーザが現在ログインしているデバイスの記録が維持されます。Cisco Extension Mobility 機能では、現在ログイン中のデバイスのレポートでローカルユーザが現在ログインしているローカル電話が追跡され、Cisco Extension Mobility Cross Cluster 機能では、現在ログイン中のデバイスのレポートでリモート ユーザが現在ログインしているローカル電話が追跡されます。

Unified Communications Manager には、ユーザがログインしているデバイスを検索するための特定の検索ウィンドウがあります。特定のデバイスを検索する場合、またはユーザが現在ログインしているすべてのデバイスを一覧表示する場合は、次の手順に従います。

手順

ステップ 1 **[デバイス（Device）]** > **[電話（Phone）]** の順に選択します。

ステップ 2 右上隅にある **[関連リンク（Related Links）]** ドロップダウンメニューから **[現在ログイン中のデバイスのレポート（Actively Logged In Device Report）]** を選択し、**[移動（Go）]** をクリックします。

ステップ 3 データベース内で現在ログイン中のデバイスのレコードをすべて検索するには、ダイアログボックスが空であることを確認して、ステップ 4 に進みます。

レコードをフィルタまたは検索する手順は、次のとおりです。

a) 最初のドロップダウン リストで、検索パラメータを選択します。
b) 2 番目のドロップダウン リストで、検索パターンを選択します。
c) 必要に応じて、適切な検索テキストを指定します。

（注） その他の検索条件を追加するには、[+] ボタンをクリックします。 条件を追加した場合は、指定したすべての条件に一致するレコードが検索されます。 条件を削除する場合、最後に追加した条件を削除するには、**[-]**ボタンをクリックします。追加した検索条件をすべて削除するには、**[フィルタのクリア（Clear Filter）]** ボタンをクリックします。

ステップ 4 **[検索(Find)]** をクリックします。

一致するすべてのレコードが表示されます。 [ページあたりの行数(Rows per Page)]ドロップダウン リストから異なる値を選択すると各ページに表示される項目数を変更できます。

ステップ 5 表示されたレコード リストから、目的のレコードのリンクをクリックします。

（注） ソート順を逆にするには、リストのヘッダーにある上矢印または下矢印をクリックします（使用可能な場合）。

選択した項目がウィンドウに表示されます。

リモートでログイン中のデバイスの検索

Cisco Extension Mobility Cross Cluster 機能は、ユーザがリモートからログインしているデバイスをトラッキングします。 リモートからログインしたデバイス レポートは、他のクラスタが所有している電話機のうち、EMCC 機能を使用しているローカル ユーザが現在ログイン中の電話機をトラッキングします。

Unified Communications Manager には、ユーザがリモートからログインしているデバイスを検索するための特別な検索ウィンドウがあります。ユーザがリモートからログインしている特定のデバイスを検索する手順またはすべてのデバイスを一覧表示する手順は、次のとおりです。

手順

ステップ 1 **[デバイス（Device）]** > **[電話（Phone）]** の順に選択します。

ステップ 2 右上にある **[関連リンク（Related Links）]** ドロップダウンメニューで **[リモートログインデバイス（Remotely Logged In Device）]** を選択し、**[移動（Go）]** をクリックします。

ステップ 3 データベース内のリモートでログイン中のすべてのデバイスのレコードを検索するには、ダイアログボックスが空であることを確認して、ステップ 4 に進みます。

レコードをフィルタまたは検索する手順は、次のとおりです。

a) 最初のドロップダウン リストで、検索パラメータを選択します。
b) 2 番目のドロップダウン リストで、検索パターンを選択します。
c) 必要に応じて、適切な検索テキストを指定します。

（注） その他の検索条件を追加するには、[+] ボタンをクリックします。 条件を追加した場合は、指定したすべての条件に一致するレコードが検索されます。 条件を削除する場合、最後に追加した条件を削除するには、**[-]** ボタンをクリックします。追加した検索条件をすべて削除するには、[フィルタのクリア（Clear Filter）] ボタンをクリックします。

ステップ 4 **[検索(Find)]** をクリックします。

一致するすべてのレコードが表示されます。 [ページあたりの行数(Rows per Page)]ドロップダウン リストから異なる値を選択すると各ページに表示される項目数を変更できます。

ステップ 5 表示されたレコード リストから、目的のレコードのリンクをクリックします。

（注） ソート順を逆にするには、リストのヘッダーにある上矢印または下矢印をクリックします（使用可能な場合）。

選択した項目がウィンドウに表示されます。

電話機のリモート ロック

一部の電話機は、リモートでロックすることができます。 電話機をリモートでロックすると、ロックを解除するまで使用できなくなります。

電話機でリモートロック機能がサポートされている場合は、右上の隅に[ロック（Lock）]ボタンが表示されます。

手順

ステップ 1 **[デバイス（Device）]** > **[電話（Phone）]** の順に選択します。

ステップ 2 [電話の検索/一覧表示（Find and List Phones）]ウィンドウから、検索条件を入力し、[検索（Find）]をクリックして特定の電話機を見つけます。

検索条件に一致する電話機のリストが表示されます。

ステップ 3 リモート ロックを実行する電話機を選択します。

ステップ 4 [電話の設定（Phone Configuration）]ウィンドウで [ロック（Lock）]をクリックします。

電話機が登録されていない場合は、電話機が次回登録されたときにロックされることを伝えるポップアップ ウィンドウが表示されます。 [ロック（Lock）]をクリックします。

[デバイスのロック/ワイプのステータス（Device Lock/Wipe Status）]セクションが表示され、最新の要求、保留中かどうか、および最新の確認応答に関する情報が示されます。

工場出荷時の初期状態への電話機のリセット

一部の電話機では、リモート ワイプ機能がサポートされます。 リモートで電話機をワイプすると、電話機が工場出荷時の設定にリセットされます。 電話機に以前に保存されたすべてのデータが消去されます。

電話機でリモート ワイプ機能がサポートされている場合は、右上の隅に [ワイプ（Wipe）]ボタンが表示されます。

⚠

注意 この操作は取り消すことができません。 この操作は、確実に電話機を工場出荷時の設定にリセットする必要がある場合にのみ、実行してください。

手順

ステップ 1 **[デバイス（Device）]** > **[電話（Phone）]** の順に選択します。

ステップ 2 [電話の検索/一覧表示（Find and List Phones）]ウィンドウで、検索条件を入力し、[検索（Find）]をクリックして特定の電話機を見つけます。

検索条件に一致する電話機のリストが表示されます。

ステップ 3 リモート ワイプを実行する電話機を選択します。

ステップ 4 [電話の設定（Phone Configuration）]ウィンドウで [ワイプ（Wipe）]をクリックします。

電話機が登録されていない場合は、電話機が次回登録されたときにワイプされることを伝えるポップアップ ウィンドウが表示されます。 [ワイプ（Wipe）]をクリックします。

[デバイスのロック/ワイプのステータス（Device Lock/Wipe Status）]セクションが表示され、最新の要求、保留中かどうか、および最新の確認応答に関する情報が示されます。

電話ロック/ワイプレポート

Unified Communications Manager には、リモートでロックまたはリモートでワイプされたデバイスを検索するための特定の検索ウィンドウがあります。 次の手順に従って、特定のデバイスを検索したり、リモートでロックされたまたはリモートでワイプされたすべてのデバイスを列挙したりします。

手順

ステップ 1 **[デバイス（Device）]** > **[電話（Phone）]** の順に選択します。

[電話の検索/一覧表示（Find and List Phones）] ウィンドウが表示されます。 このウィンドウには、アクティブな（以前の）クエリーのレコードも表示されることがあります。

ステップ 2 ウィンドウの右上にある **[関連リンク（Related Links）]** ドロップダウンメニューで **[電話のロック/ワイプレポート（Phone Lock/Wipe Report）]** を選択し、**[移動（Go）]** をクリックします。

ステップ 3 データベース内のリモートでロックされたデバイスまたはリモートでワイプされたデバイスのすべてのレコードを検索するには、テキストボックスが空であることを確認して、ステップ 4 に進みます。

特定のデバイスのレコードを絞り込むまたは検索するには：

a) 1 つ目のドロップダウン リストで、検索するデバイス稼働タイプを選択します。
b) 2 番目のドロップダウン リストで、検索パラメータを選択します。
c) 3 番目のドロップダウン リストで、検索パターンを選択します。
d) 必要に応じて、適切な検索テキストを指定します。

（注） その他の検索条件を追加するには、[+] ボタンをクリックします。 条件を追加した場合は、指定したすべての条件に一致するレコードが検索されます。 条件を削除する場合、最後に追加した条件を削除するには、[-]ボタンをクリックします。追加した検索条件をすべて削除するには、[フィルタのクリア（Clear Filter）] ボタンをクリックします。

ステップ 4 **[検索(Find)]** をクリックします。

一致するすべてのレコードが表示されます。 [ページあたりの行数(Rows per Page)]ドロップダウン リストから異なる値を選択すると各ページに表示される項目数を変更できます。

ステップ 5 表示されたレコード リストから、目的のレコードのリンクをクリックします。

（注） ソート順を逆にするには、リストのヘッダーにある上矢印または下矢印をクリックします（使用可能な場合）。

選択した項目がウィンドウに表示されます。

電話の LSC ステータスの表示および CAPF レポートの生成

この手順を使用して、Cisco Unified Communications Manager インタフェース内からローカルで有効な証明書（LSC）の有効期限情報を監視します。 次の検索フィルタは、LSC情報を表示します。

- [LSC 有効期日（LSC Expires）]：電話の LSC 有効期日を表示します。
- [LSC 発行元（LSC Issued By）]：発行元の名前を表示します。これは、CAPF またはサードパーティのいずれかです。
- [LSC 発行元の有効期日（LSC Issuer Expires By）]：発行元の有効期日を表示します。

（注） 新しいデバイスにLSCが発行されていない場合、**[LSC 有効期日（LSC Expires）]**および**[LSC 発行元の有効期日（LSC Issuer Expires by）]**フィールドのステータスは「[該当なし（NA）]」に設定されます。

Cisco Unified Communications Manager 11.5(1) へのアップグレード前に LSC がデバイスに発行された場合は、**[LSC 有効期日（LSC Expires）]** および **[LSC 発行元の有効期日（LSC Issuer Expires by）]** フィールドのステータスは 「 [不明（Unknown）」] に設定されます。

手順

ステップ 1 **[デバイス（Device）]** > **[電話（Phone）]** の順に選択します。

ステップ 2 [電話の検索条件（Find Phone where）]の最初のドロップダウン リストから、次の基準の 1 つを選択します。

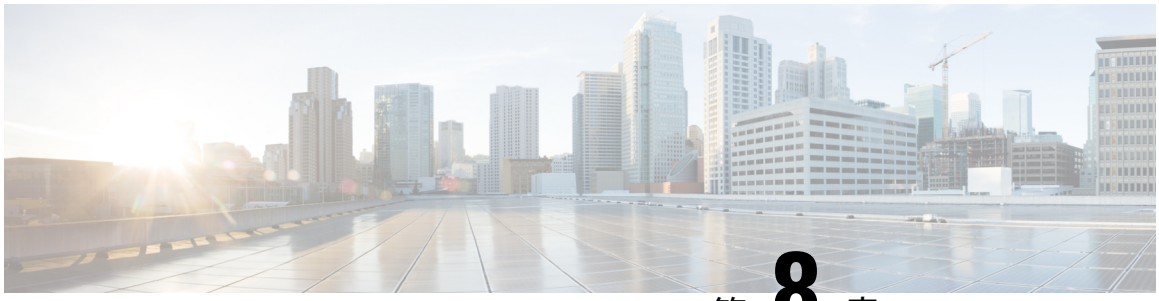
- LSC 有効期日（LSC Expires）
- LSC 発行元（LSC Issued By）
- LSC 発行元の有効期日（LSC Issuer Expires by）

[電話の検索条件（Find Phone where）]の 2 番目のドロップダウン リストから、次の基準の 1 つを選択します。

- [が次の日付より前（is before）]
- [が次の文字列と等しい(is exactly)]
- [が次の日付より後（is after）]
- [が次の文字列で始まる(begins with)]
- [が次の文字列を含む(contains)]
- [が次の文字列で終わる(ends with)]
- [が次の文字列と等しい(is exactly)]
- [が空である(is empty)]
- [が空ではない(is not empty)]

ステップ 3 **[検索(Find)]** をクリックします。
検索された電話機のリストが表示されます。

ステップ 4 [関連リンク（Related Links）]ドロップダウン リストから [ファイルでの CAPF レポート（CAPF Report in File）]を選択し、[移動（Go）]をクリックします。
レポートがダウンロードされます。



第 8 章

デバイス ファームウェアの管理

デバイス ファームウェアのアップデートの概要

デバイス ロードとは、IP Phone、Telepresence Systems、および Cisco Unified Communications Manager でプロビジョニングおよび登録されているその他のデバイスを対象としたソフトウェアおよびファームウェアのことです。 Cisco Unified Communications Manager はインストールまたはアップグレード時に、Cisco Unified Communications Manager の該当するバージョンがリリースされた時期に基づいて、利用可能な最新のロードをインクルードします。 シスコでは、新しい機能やソフトウェア フィックスを導入するために更新されたファームウェアを定期的にリリースしています。したがって、新しいロードをインクルードした Cisco Unified Communications Manager アップグレードを待たずに、電話機を新しいロードに更新することができます。

エンドポイントをソフトウェアの新しいバージョンにアップグレードするには、エンドポイントがアクセス可能な場所に新しいロードに必要なファイルがダウンロード可能になっていなければなりません。 最も一般的な場所は、Cisco TFTP サービスがアクティブにされている、「TFTP サーバ」と呼ばれる Cisco UCM ノードです。 一部の電話機は、「ロード サーバ」と呼ばれる別のダウンロード場所もサポートしています。

任意のサーバ上の tftp ディレクトリ内にあるファイルのリストを取得したり、それらのファイルを表示またはダウンロードしたりするには、CLI コマンドの file list tftp（tftp ディレクトリ内のファイルを一覧表示する場合）、file view tftp（ファイルを表示する場合）、file get tftp（tftp ディレクトリ内のファイルのコピーを取得する場合）を使用します。 詳細については、『*Command Line Interface Reference Guide for Cisco Unified Communications Solutions*』を参照してください。 また、Web ブラウザで URL 「http://<tftp_server>:6970/<filename>」 にアクセスして、任意の TFTP ファイルをダウンロードすることもできます。

ヒント　新しいロードをシステム全体のデフォルトとして設定する前に、単一のデバイスに新規ロードを適用することもできます。 この手法は、テスト目的で役立ちます。 ただし、該当するタイプのその他すべてのデバイスは、新しいロードでシステム全体のデフォルトを更新するまでは、古いロードを使用することに注意してください。

デバイス パックまたは個々のファームウェアのインストール

デバイス パッケージをインストールして、新しい電話タイプを導入し、複数の電話モデルのファームウェアをアップグレードします。

- 既存のデバイスの個々のファームウェアは次のオプションでインストールまたはアップグレードできます。Cisco Options Package（COP）ファイル：COP ファイルには、ファームウェア ファイルとデータベース アップデートが含まれています。このためパブリッシャにインストールすると、ファームウェア ファイルがインストールされ、さらにデフォルトのファームウェアが更新されます。
- ファームウェア ファイルのみ：zip ファイルで提供されます。zip ファイルに含まれている個々のデバイス ファームウェア ファイルは手動で解凍し、TFTP サーバの適切なディレクトリにおよびアップロードする必要があります。

（注）　COP またはファームウェア ファイル パッケージに固有のインストール手順については、README ファイルを参照してください。

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 サービスを実行しているすべてのノードで [Cisco TFTP] サービスを再起動します。

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 の管理から、**[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）]** の順に選択し、新しいロードに（特定のデバイスに対して）ロード ファイル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。

ステップ 11 すべてのクラスタ ノードで **Cisco Tomcat** サービスを再起動します。

ステップ 12 次のいずれかを実行します。

- 11.5(1)SU4 以下、12.0(1)、または 12.0(1)SU1 を実行している場合は、クラスタを再起動します。
- 11.5(1)SU5 以上での11.5(x) リリース、12.0(1)SU2 以上での任意のリリースを実行している場合は、パブリッシャ ノード上で **Cisco CallManager** サービスを再起動します。 ただし、サブスクライバ ノードでのみ **Cisco CallManager** サービスを実行している場合は、このタスクをスキップできます。

ファームウェアのインストールの潜在的な問題

デバイス パックのインストール後に発生する可能性があるいくつかの潜在的な問題を次に示します。

問題	原因/解決
新しいデバイスが登録されません	これはデバイス タイプの不一致により発生する可能性があります。次の原因が考えられます。 • デバイスが [電話の設定（Phone Configuration）] ウィンドウで、不適切なデバイス タイプを使用して追加されました。 たとえば、Cisco DX80 が Cisco TelePresence DX80 ではなく電話タイプとして選択されました。 適切なデバイス タイプを使用して、デバイスを再設定します。 • **Cisco CallManager** サービスが新しいデバイス タイプを認識しません。 この場合、パブリッシャ ノード上で **Cisco CallManager** サービスを再起動します。
エンドポイントが新しいファームウェアにアップグレードしません	**考えられる理由**： • デバイス パックが TFTP サーバにインストールされていません。その結果、ファームウェアは電話機でダウンロードできません。 • **Cisco TFTP** サービスは、インストール後に再起動されなかったので、新しいファイルについて認識しません。 必ず TFTP サーバーにデバイス パックをインストールします。

問題	原因/解決
Cisco Unified CM Administration の [電話の設定（Phone Configuration）] ウィンドウで、新しいデバイス タイプのアイコン イメージがあるはずの場所に、破損したリンクが表示されます。	CLI からすべてのノードで **Cisco Tomcat** サービスを再起動します。
エンドポイントのファームウェアのダウンロードが失敗し、ダウンロード全体が再起動したり、ダウンロードが非常に遅いように思われます。 **重要** リリース 14SU1 以降で適用されます。	**考えられる理由**： これは、ネットワークの問題や輻輳が原因である可能性が高く、一括アップグレードのシナリオではより一般的である可能性があります。 14SU1 を実行している場合は、TFTP およびプロキシ TFTP での HTTP 範囲要求（RFC7233）のサポートによりメリットが得られる可能性があります(ダウンロード ファイルが 100 MB 以上の場合)。 HTTP 範囲要求をサポートするエンドポイントでは、信頼性とダウンロード速度が向上する可能性があります（特に一括での電話機のアップグレード シナリオやネットワーク条件が不十分である場合）。 HTTP 範囲の要求では、ダウンロードの一時停止と再開を許可する必要があります。つまり、中断したダウンロードでは、ダウンロード全体を再び再起動することなく、最後に成功したバイト範囲から継続できます。 Cisco Webex Wireless Phone 840 および 860 は RFC7233 をサポートします。 RFC7233 をサポートしていないデバイスは、この機能の影響を受けません。

システムからの未使用のファームウェアの削除

[デバイス ロード管理（Device Load Management）]ウィンドウでは、システムから未使用のファームウェア（デバイス ロード）および関連するファイルを削除して、ディスク容量を増やすことができます。たとえば、アップグレード前に未使用のロードを削除して、ディスク容量の不足が原因でアップグレードが失敗しないようにすることができます。ファームウェア ファイルの中には、[デバイス ロード管理（Device Load Management）]ウィンドウにリストされない依存ファイルを持っているものがあります。ファームウェアを削除すると、依存ファイルも削除されます。ただし、その依存ファイルが他のファームウェアに関連付けられている場合は削除されません。

（注） クラスタ内の各サーバで、個別に未使用のファームウェアを削除する必要があります。

始める前に

注意 未使用のファームウェアを削除する前に、適切なロードを削除していることを確認します。削除されたロードは、クラスタ全体の DRS 復元を実行しないと復元できません。 ファームウェアを削除する前にバックアップすることを推奨します。

複数のファイルのロードを使用するデバイスのファイルを削除しないようにしてください。たとえば、特定の CE エンドポイントは複数のロードを使用します。 ただし、**[デバイスロード管理（Device Load Management）]** ウィンドウで **[使用中（In Use）]** として参照されるロードは 1 つだけです。

手順

ステップ 1 [Cisco Unified OS の管理（Cisco Unified OS Administration）] 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）]** の順に選択します。

ステップ 2 検索条件を指定して、[検索（Find）] をクリックします。

ステップ 3 削除するデバイス ロードを選択します。 必要な場合は、複数のロードを選択できます。

ステップ 4 [選択されたロードの削除（Delete Selected Loads）]をクリックします。

ステップ 5 **OK**をクリックします。

電話モデルのデフォルト ファームウェアの設定

この手順を使用して、特定の電話モデルにデフォルトのファームウェア ロードを設定します。新しい電話が登録されると、Cisco Unified Communications Manager は、[電話の設定（Phone Configuration）]ウィンドウでデフォルトを上書きするファームウェア ロードが指定されていないかぎり、デフォルトのファームウェアを電話に送信しようとします。

（注） 個々の電話については、[電話の設定（Phone Configuration）]ウィンドウの [電話ロード名（Phone Load Name）]フィールドの設定により、その特定の電話のデフォルト ファームウェア ロードが上書きされます。

始める前に

ファームウェアが TFTP サーバにロードされていることを確認します。

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified CM Administration）] で、**[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）]** を選択します。[デバイスのデフォルト設定（Device Defaults Configuration）]ウィンドウが表示され、Cisco Unified Communications Manager がサポートする様々な電話モデルのデフォルト ファームウェア ロードが示されます。 ファームウェアは [ロード情報（Load Information）]列に表示されます。

ステップ 2 [デバイス タイプ（Device Type）]で、デフォルト ファームウェアを割り当てる電話モデルを指定します。

ステップ 3 横にある [ロード情報（Load Information）]フィールドに、ファームウェア ロードを入力します。

ステップ 4 （任意）[デバイス プール（Device Pool）] にデフォルトのデバイス プールを入力し、[電話テンプレート（Phone Template）]に該当する電話モデルのデフォルトの電話テンプレートを入力します。

ステップ 5 **[保存（Save）]** をクリックします。

電話機のファームウェア ロードの設定

この手順を使用して、特定の電話にファームウェア ロードを割り当てます。 [デバイスのデフォルト設定（Device Defaults Configuration）]ウィンドウに指定されているデフォルトとは異なるファームウェア ロードを使用する場合に、この手順を実行します。

（注） 多数の電話に1つのバージョンを割り当てる場合は、一括管理ツールを使用し、CSVファイルまたはクエリを使用して、[電話ロード名（Phone Load Name）]フィールドを設定できます。詳細については、『*Bulk Administration Guide for Cisco Unified Communications Manager*』を参照してください。

手順

ステップ 1 Cisco Unified CM の管理で、**[デバイス（Device）] > [電話（Phone）]** を選択します。

ステップ 2 [検索（Find）]をクリックし、個別の電話を選択します。

ステップ 3 [電話ロード名（Phone Load Name）]フィールドに、ファームウェアの名前を入力します。 この電話では、ここで指定したファームウェア ロードによって、[デバイスのデフォルト設定

（Device Defaults Configuration）]ウィンドウで指定されているデフォルトのファームウェアロードが上書されます。

ステップ 4 [電話の設定（Phone Configuration）]ウィンドウで、残りのフィールドを入力します。 フィールドとその設定の詳細については、オンライン ヘルプを参照してください。

ステップ 5 **[保存]** をクリックします。

ステップ 6 [設定の適用（Apply Config）]をクリックして、変更したフィールドを電話にプッシュします。

ロード サーバの使用

電話が TFTP サーバ以外のサーバからファームウェアの更新をダウンロードするようにするには、電話の [電話の設定（Phone Configuration）] ページで「ロード サーバ」を設定できます。ロード サーバには、別の Cisco Unified Communications Manager またはサードパーティのサーバを指定できます。 サードパーティのサーバは、電話が TCP ポート 6970 で HTTP を使用して（推奨）、または UDP ベースの TFTP プロトコルを使用して要求するすべてのファイルを提供できる必要があります。 DX ファミリの Cisco TelePresence デバイスなどの一部の電話モデルでは、ファームウェアのアップデートで HTTP のみをサポートしています。

（注） 多数の電話に 1 つのロード サーバを割り当てる場合は、一括管理ツールを使用し、CSV ファイルまたはクエリを使用して、[ロードサーバ（Load Server）]フィールドを設定できます。 詳細については、『*Bulk Administration Guide for Cisco Unified Communications Manager*』を参照してください。

手順

ステップ 1 Cisco Unified CM の管理で、**[デバイス（Device）]** > **[電話（Phone）]** を選択します。

ステップ 2 [検索（Find）]をクリックし、個別の電話を選択します。

ステップ 3 [ロードサーバ（Load Server）]フィールドに、別のサーバの IP アドレスまたはホスト名を入力します。

ステップ 4 [電話の設定（Phone Configuration）]ウィンドウで、残りのフィールドを入力します。 フィールドとその設定の詳細については、オンライン ヘルプを参照してください。

ステップ 5 **[保存（Save）]** をクリックします。

ステップ 6 [設定の適用（Apply Config）]をクリックして、変更したフィールドを電話にプッシュします。

デフォルト以外のファームウェア ロードを使用するデバイスの検索

Unified Communications Managerページの [ファームウェアロード情報(Firmware Load Information)] ウィンドウを使用すると、デバイス タイプにデフォルトのファームウェア ロードを使用しないデバイスを、すばやく特定することができます。

（注） 各デバイスには、デフォルトを上書きするファームウェア ロードを個別に割り当てることができます。

デフォルトのファームウェア ロードを使用しないデバイスを特定する手順は、次のとおりです。

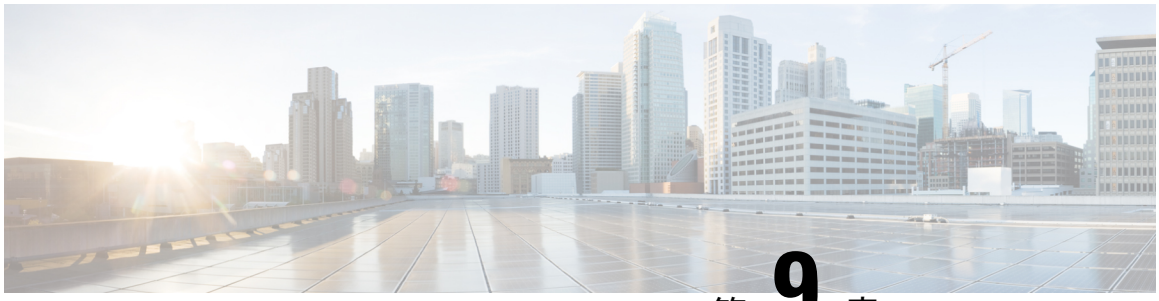
手順

ステップ 1 **[デバイス(Device)] > [デバイスの設定(Device Settings)] > [ファームウェアロード情報(Firmware Load Information)]** を選択します。

ページが更新され、ファームウェア ロードを必要とするデバイス タイプのリストが表示されます。デバイス タイプごとに、[デフォルトロードを使用していないデバイス(Device Not Using Default Load)] 列が、デフォルト以外のロードを使用するデバイスの設定値にリンクします。

ステップ 2 デフォルト以外のデバイス ロードを使用する特定のデバイス タイプのデバイスのリストを表示するには、[デフォルトロードを使用していないデバイス(Device Not Using Default Load)] 列で、そのデバイス タイプのエントリをクリックします。

デフォルトのファームウェア ロードを実行していない、特定のデバイス タイプのデバイスがリストされたウィンドウが開きます。



第 9 章

インフラストラクチャ デバイスの管理

インフラストラクチャの管理の概要

この章では、ロケーション対応機能の一部として、スイッチとワイヤレスアクセスポイントなどのネットワーク インフラストラクチャ デバイスを管理するタスクについて説明します。 ロケーション対応を有効にすると、Cisco Unified Communications Manager データベースには、各スイッチまたはアクセスポイントに現在関連付けられているエンドポイントのリストを含め、ネットワークのスイッチとアクセスポイントのステータス情報が保存されます。

エンドポイントからインフラストラクチャ デバイスへのマッピングは、Cisco Unified Communications Manager と Cisco Emergency Responder が発信者の物理的な場所を特定するのに役立ちます。 たとえば、モバイルクライアントがローミング中に緊急通報を行っている場合、Cisco Emergency Responder はこのマッピングを使用して緊急サービスを送る場所を判断します。

データベースに保存されるインフラストラクチャ情報も、インフラストラクチャの使用状況をモニタするのに役立ちます。 Unified Communications Manager インターフェイスから、スイッチやワイヤレス アクセスポイントなどのネットワーク インフラストラクチャのデバイスを確認できます。 現時点で特定のアクセスポイントまたはスイッチに関連付けられているエンドポイントのリストを表示することもできます。 インフラストラクチャ デバイスが使用されていない場合は、インフラストラクチャデバイスを非アクティブ化して追跡されないようにできます。

インフラストラクチャの管理の前提条件

Cisco Unified Communications Manager インターフェイス内でワイヤレス インフラストラクチャを管理するには、その前に、ロケーション認識機能を設定する必要があります。 有線インフラストラクチャの場合、この機能はデフォルトで有効になっています。

構成の詳細については、『Feature Configuration Guide for Cisco Unified Communications Manager』の「場所の認識の構成」の章を参照してください。

また、ネットワーク インフラストラクチャをインストールする必要もあります。 詳細については、ワイヤレス LAN コントローラ、アクセス ポイント、スイッチなどのインフラストラクチャ デバイスに付属しているハードウェア ドキュメントを参照してください。

インフラストラクチャの管理のタスク フロー

次のタスクを実行して、ネットワーク インフラストラクチャ デバイスを監視および管理します。

手順

	コマンドまたはアクション	目的
ステップ 1	インフラストラクチャデバイスのステータスの表示 （102 ページ）	ワイヤレス アクセス ポイントまたはイーサネット スイッチの現在のステータスを、関連付けられているエンドポイントの一覧とともに取得します。
ステップ 2	インフラストラクチャ デバイス トラッキングの非アクティブ化 （103 ページ）	使用されていないスイッチまたはアクセス ポイントがある場合は、そのデバイスに非アクティブのマークを付けます。そのインフラストラクチャ デバイスのステータスまたは関連付けられているエンドポイントの一覧が更新されなくなります。
ステップ 3	非アクティブ化されたインフラストラクチャ デバイス トラッキングのアクティブ化 （104 ページ）	非アクティブなインフラストラクチャ デバイスのトラッキングを開始します。Cisco Unified Communications Manager が、インフラストラクチャ デバイスのステータスおよび関連付けられているエンドポイントの一覧により、データベースの更新を開始します。

インフラストラクチャ デバイスのステータスの表示

この手順を使用して、ワイヤレス アクセス ポイントやイーサネット スイッチなどのインフラストラクチャ デバイスの現在のステータスを取得します。 Cisco Unified Communications Manager インターフェイス内で、アクセス ポイントまたはスイッチのステータスおよび現在関連付けられているエンドポイントの一覧を表示できます。

手順

ステップ 1 Cisco Unified CM Administration で、**[詳細機能（Advanced Features）]** > **[デバイスの位置のトラッキング サービス（Device Location Tracking Services）]** > **[スイッチとアクセス ポイント（Switches and Access Points）]** 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 ステータスを表示するスイッチまたはアクセス ポイントをクリックします。
[スイッチおよびアクセス ポイントの設定（Switches and Access Point Configuration）]ウィンドウに、そのアクセスポイントまたはスイッチに現在関連付けられているエンドポイントの一覧を含み、現在のステータスが表示されます。

インフラストラクチャ デバイス トラッキングの非アクティブ化

スイッチやアクセス ポイントなどの特定のインフラストラクチャ デバイスのトラッキングを削除するには、次の手順を使用します。 使用されていないスイッチまたはアクセス ポイントで、この手順を実行できます。

（注） インフラストラクチャデバイスのトラッキングを削除すると、デバイスはデータベースに残ったまま、非アクティブになります。 Cisco Unified Communications Manager は、その後、そのインフラストラクチャ デバイスに関連するエンドポイントの一覧も含めて、そのデバイスのステータスを更新しません。 **[スイッチとアクセスポイント（Switches and Access Points）]** ウィンドウの **[関連リンク（Related Links）]** ドロップダウンで、非アクティブなスイッチとアクセスポイントを表示できます。

手順

ステップ 1 Cisco Unified CM Administration で、**[詳細機能（Advanced Features）]** > **[デバイスの位置のトラッキング サービス（Device Location Tracking Services）]** > **[スイッチとアクセス ポイント（Switches and Access Points）]** を選択します。

ステップ 2 [検索（Find）]をクリックして、追跡を停止するスイッチまたはアクセス ポイントを選択します。

ステップ 3 [選択項目の非アクティブ化（Deactivate Selected）]をクリックします。

非アクティブ化されたインフラストラクチャ デバイス トラッキングのアクティブ化

この手順を使用して、非アクティブ化されたインフラストラクチャデバイスのトラッキングを開始します。 スイッチまたはアクセス ポイントがアクティブになると、Cisco Unified Communications Managerでは、スイッチまたはアクセスポイントに関連付けられているエンドポイントの一覧を含むステータスを動的にトラッキングし始めます。

始める前に

Location Awareness を設定する必要があります。 詳細については、『*System Configuration Guide for Cisco Unified Communications Manager*』の「Location Awareness」の章を参照してください。

手順

ステップ 1 Cisco Unified CM Administration で、**[詳細機能（Advanced Features）] > [デバイスの位置のトラッキング サービス（Device Location Tracking Services）] > [スイッチとアクセス ポイント（Switches and Access Points）]** を選択します。

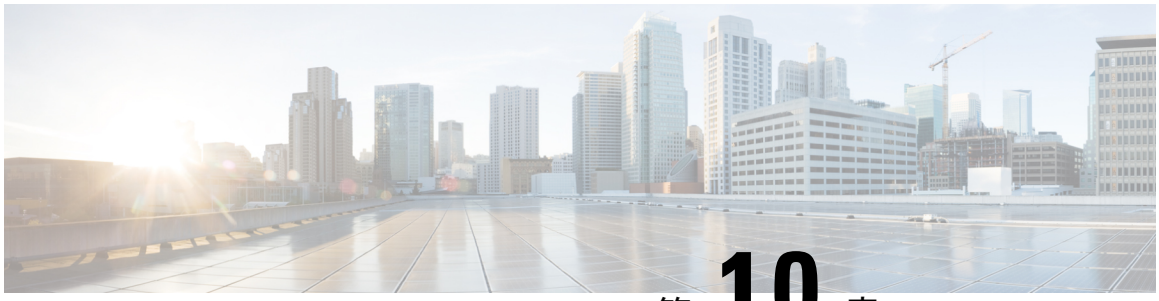
ステップ 2 [関連リンク（Related Links）]から、[非アクティブなスイッチおよびアクセス ポイント（Inactive Switches and Access Points）] を選択し、[移動（Go）]をクリックします。
[非アクティブなスイッチおよびアクセス ポイントの検索および表示（Find and List Inactive Switches and Access Points）]ウィンドウに、トラッキングされていないインフラストラクチャデバイスが表示されます。

ステップ 3 トラッキングを開始するスイッチまたはアクセス ポイントを選択します。

ステップ 4 [選択項目の再アクティブ化（Reactivate Selected）]をクリックします。

第 IV 部

システムの管理



第 10 章

システム ステータスのモニタ

クラスタ ノード ステータスの表示

この手順を使用して、クラスタ内のノードに関する情報を表示します。

手順

ステップ 1 [Cisco Unified オペレーティング システムの管理（Cisco Unified Operating System Administration）] で、**[表示（Show）] > [クラスタ（Cluster）]** を選択します。

ステップ 2 [クラスタ（Cluster）]ウィンドウのフィールドを調べます。 フィールドの詳細については、オンライン ヘルプを参照してください。

ハードウェア ステータスの表示

ハードウェア ステータスおよびシステム内のハードウェア リソースに関する情報を表示するには、この手順を実行します。

手順

ステップ 1 [Cisco Unified オペレーティング システムの管理（Cisco Unified Operating System Administration）]で、**[表示（Show）]** > **[ハードウェア（Hardware）]** を選択します。

ステップ 2 [ハードウェア ステータス（Hardware Status）]ウィンドウのフィールドを調べます。 フィールドの詳細については、オンライン ヘルプを参照してください。

ネットワーク ステータスの表示

イーサネットおよび DNS 情報など、システムのネットワーク ステータスを表示するには、この手順を実行します。

表示されるネットワーク ステータス情報は、ネットワーク耐障害性が有効になっているかどうかによって異なります。

- ネットワーク耐障害性が有効になっていると、イーサネット ポート 0 に障害が発生した場合、イーサネット ポート 1 が自動的にネットワーク通信を管理します。
- ネットワーク耐障害性が有効になっている場合、ネットワーク ポートのイーサネット 0、イーサネット 1、および Bond 0 のネットワーク ステータス情報が表示されます。
- ネットワーク耐障害性が有効になっていない場合、イーサネット 0 のステータス情報のみが表示されます。

手順

ステップ 1 [Cisco Unified オペレーティング システムの管理（Cisco Unified Operating System Administration）]で、**[表示（Show）]** > **[ネットワーク（Network）]** を選択します。

ステップ 2 [ネットワーク構成（Network Configuration）]ウィンドウのフィールドを調べます。 フィールドの詳細については、オンライン ヘルプを参照してください。

インストールされているソフトウェアの表示

ソフトウェアのバージョンおよびインストールされているソフトウェア パッケージに関する情報を表示するには、この手順を実行します。

手順

ステップ 1 [Cisco Unified オペレーティング システムの管理（Cisco Unified Operating System Administration）]で、**[表示（Show）]** > **[ソフトウェア（Software）]** を選択します。

ステップ 2 [ソフトウェア パッケージ（Software Packages）]ウィンドウのフィールドを調べます。 フィールドの詳細については、オンライン ヘルプを参照してください。

システム ステータスの表示

ロケール、稼働時間、CPU使用量、メモリ使用量などのシステム全体の状態を表示するには、この手順を実行します。

手順

ステップ 1 [Cisco Unified オペレーティング システムの管理（Cisco Unified Operating System Administration）]で、**[表示（Show）] > [システム（System）]** を選択します。

ステップ 2 [システム ステータス（System Status）]ウィンドウのフィールドを調べます。 フィールドの詳細については、オンライン ヘルプを参照してください。

IP 設定の表示

この手順を使用して、システムで利用可能な登録済みポートの一覧を表示します。

手順

ステップ 1 [Cisco Unified オペレーティング システムの管理（Cisco Unified Operating System Administration）]で、**[表示（Show）] > [IP 設定（IP Preferences）]** を選択します。

ステップ 2 （任意） レコードをフィルタリングまたは検索するには、次のいずれかのタスクを実行します。

- 最初の一覧から検索パラメータを選択します。
- 2 番目の一覧から検索パターンを選択します。
- 必要に応じて、適切な検索テキストを指定します。

ステップ 3 **[検索(Find)]** をクリックします。

ステップ 4 [システム ステータス（System Status）]ウィンドウに表示されるフィールドを調べます。 フィールドの詳細については、オンライン ヘルプを参照してください。

最終ログインの詳細の表示

エンドユーザ（ローカルまたはLDAPクレデンシャルを持つエンドユーザ）と管理者がCisco Unified Communications ManagerまたはIM and Presence ServiceのWebアプリケーションにログインすると、アプリケーションのメインウィンドウに、最後に成功したログインと最後に失敗したログインの詳細が表示されます。

SAML SSO機能を使用してログインするユーザには、最後に成功したシステムログイン情報だけが表示されます。 ユーザが失敗したSAML SSOログイン情報をトラッキングするには、IDプロバイダー（IdP）アプリケーションを参照できます。

次のWebアプリケーションには、ログイン試行に関する情報が表示されます。

- Cisco Unified Communications Manager:
  - Cisco Unified CMの管理
  - Cisco Unifiedのレポート
  - Cisco Unified Serviceability
- IM and Presence Service
  - Cisco Unified CM IM and Presenceの管理
  - Cisco Unified IM and Presenceのレポート
  - Cisco Unified IM and Presenceサービスアビリティ

Cisco Unified Communications Managerの次のWebアプリケーションでは、管理者だけがログインして最後のログイン詳細を表示できます。

- Disaster Recovery System
- Cisco Unified OS Administration

ノードの ping

pingユーティリティを使用して、ネットワーク内の別のノードにpingします。 この結果は、デバイスの接続の確認やトラブルシューティングに役立ちます。

手順

ステップ 1 Cisco Unified Operating System Administrationで、**[サービス（Services）]** > **[Ping]**を選択します。

ステップ 2 [Pingの設定（Ping 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 3 [Ping]を選択します。

ping の結果が表示されます。

サービス パラメータの表示

クラスタ内のすべてのサーバで特定のサービスに属するサービス パラメータをすべて比較する必要がある場合があります。 また、同期外れパラメータ（サーバ間で値が異なるサービス パラメータ）または提示された値から変更されているパラメータだけを表示する必要がある場合もあります。

次の手順を使用して、クラスタ内のすべてのサーバ上で特定のサービスに関するサービス パラメータを表示します。

手順

ステップ 1 **[System（システム）] > [Service Parameters（サービス パラメータ）]** 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 ボックスから、サーバを選択します。

ステップ 3 [サービス（Service）] ドロップダウン リスト ボックスで、クラスタ内のすべてのサーバ上でサービス パラメータを表示するサービスを選択します。

（注） [サービス パラメータ設定（Service Parameter Configuration）] ウィンドウに、すべてのサービス（アクティブと非アクティブ）が表示されます。

ステップ 4 表示された [サービス パラメータ設定（Service Parameter Configuration）] ウィンドウの [関連リンク（Related Links）] ドロップダウン リスト ボックスで [すべてのサーバに対するパラメータ（Parameters for All Servers）] を選択してから、[移動（Go）] をクリックします。

[すべてのサーバに対するパラメータ（Parameters for All Servers）] ウィンドウが表示されます。現在のサービスに関して、すべてのパラメータがアルファベット順に一覧表示されます。パラメータごとに、パラメータ名の横に推奨値が表示されます。各パラメータ名の下に、そのパラメータを含むサーバのリストが表示されます。各サーバ名の横に、このサーバのパラメータの現在値が表示されます。

特定のパラメータについて、対応するサービス パラメータ ウィンドウにリンクするサーバ名または現在のパラメータ値をクリックし、その値を変更します。 [前へ（Previous）] と [次へ（Next）] をクリックすると、[すべてのサーバに対するパラメータ（Parameters for All Servers）] ウィンドウ間を移動できます。

ステップ 5 同期外れサービス パラメータを表示する必要がある場合は、[関連リンク（Related Links）] ドロップダウン リスト ボックスで、[すべてのサーバに対する同期外れパラメータ（Out of Sync Parameters for All Servers）] を選択してから、[移動（Go）] をクリックします。

[すべてのサーバに対する同期外れパラメータ（Out of Sync Parameters for All Servers）] ウィンドウが表示されます。 現在のサービスに関して、サーバごとに値が異なるサービス パラメータがアルファベット順に表示されます。パラメータごとに、パラメータ名の横に推奨値が表示

されます。各パラメータ名の下に、そのパラメータを含むサーバのリストが表示されます。各サーバ名の横に、このサーバのパラメータの現在値が表示されます。

特定のパラメータについて、対応するサービス パラメータ ウィンドウにリンクするサーバ名または現在のパラメータ値をクリックして、その値を変更します。[前へ（Previous）] と [次へ（Next）] をクリックすると、[すべてのサーバに対する同期外れパラメータ（Out of Sync Parameters for All Servers）] ウィンドウ間を移動できます。

ステップ 6 推奨値から変更されたサービスパラメータを表示する必要がある場合は、[関連リンク（Related Links）] ドロップダウン リスト ボックスで、[すべてのサーバに対する変更済みパラメータ（Modified Parameters for All Servers）] を選択してから、[移動（Go）] をクリックします。

[すべてのサーバに対する変更済みパラメータ（Modified Parameters for All Servers）] ウィンドウが表示されます。 現在のサービスに関して、推奨値とは異なる値を持つサービス パラメータがアルファベット順に表示されます。パラメータごとに、パラメータ名の横に推奨値が表示されます。各パラメータ名の下に、推奨値とは異なる値を持つサーバのリストが表示されます。 各サーバ名の横に、このサーバのパラメータの現在値が表示されます。

特定のパラメータについて、対応するサービス パラメータ ウィンドウにリンクするサーバ名または現在のパラメータ値をクリックして、その値を変更します。[前へ（Previous）] と [次へ（Next）] をクリックすると、[すべてのサーバに対する変更済みパラメータ（Modified Parameters for All Servers）] ウィンドウ間を移動できます。

ネットワーク DNS の設定

DNS ネットワークを設定するには、この手順を使用します

（注） Cisco Unified CM Administration で、DHCP 設定ウィンドウによって DNS プライマリおよびセカンダリ サーバを割り当てることもできます。

手順

ステップ 1 コマンドライン インターフェイスにログインします。

ステップ 2 DNS サーバを割り当てる場合は、パブリッシャ ノードに次の commandson のいずれかを実行します。

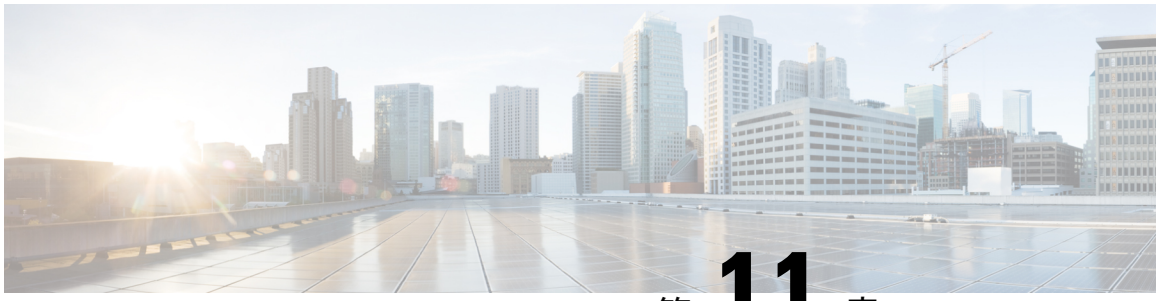
- プライマリ DNS サーバを割り当てるには、**run set network dns primary <ip_address>** を実行します
- セカンダリ DNS サーバを割り当てるには、**run the set network dns secondary <ip_address>** を実行します

ステップ 3 追加の DNS オプションを割り当てるには、**set network dns options [timeout| seconds] [attempts| number] [rotate]** を実行します。

- timout で DNS タイムアウトを設定します
- second はタイムアウトの秒数です
- attempt は DNS 要求の試行回数を設定します
- number は試行回数を指定します
- rotate を指定すると、設定されている DNS サーバのローテーションが行われ、負荷が分散されます

たとえば、set network dns options timeout 60 attempts 4 rotate などとします

サーバは、このコマンドの実行後に再起動します。



第 11 章

アラーム

概要

Cisco Unified Serviceability、Cisco Unified IM and Presence のサービスアビリティ アラームは、実行時のステータスとシステムの状態に関する情報を提供するため、システムに関する問題を修復できます。たとえば、ディザスタ リカバリ システムを使用して問題を特定します。 説明と推奨処置を含むアラーム情報には、トラブルシューティングを支援し、クラスタにも適用するために、アプリケーション名、マシン名なども含まれています。

アラーム情報を複数の場所に送信するようにアラームインターフェイスを設定し、それぞれの場所に独自のアラームイベントレベル（デバッグから緊急まで）を持たせることができます。Syslog ビューア（ローカル syslog）、Syslog ファイル（リモート syslog）、SDL トレース ログ ファイル（Cisco CallManager、CTIManager サービスのみ）、またはすべての宛先にアラームを送信できます。

サービスがアラームを発行すると、アラームインターフェイスはユーザーが設定し、アラーム定義のルーティングリストに指定されている場所（たとえば、SDI トレース）にアラーム情報を送信します。 システムは、SNMP トラップと同様にアラーム情報を転送することや、アラーム情報を最終宛先に書き込むことができます（ログ ファイルなど）。

Cisco Database Layer Monitor などのサービスのアラームを特定のノードで設定したり、クラスタのすべてのノードで特定のサービスのアラームを設定することができます。

（注） Cisco Unity Connection の SNMP ではトラップをサポートしていません。

ヒント　リモート Syslog サーバーの場合は、Cisco Unified Communications Manager サーバーを指定しないでください。このサーバーは他のサーバーからの Syslog メッセージを受け入れることができません。

（注）　リモート Syslog サーバーが Unified Communications Manager で設定された最小の TLS バージョンをサポートしていることを確認してください。

Cisco Unified Real-Time Monitoring Tool（Unifed RTMT）の Trace and Log Central オプションを使用して、SDL トレースログファイルに送信されるアラームを収集します（Cisco CallManager、CTIManager サービスの場合のみ）。 ローカル Syslog に送信されるアラーム情報を表示するには、Unified RTMT で Syslog ビューアを使用します。

アラーム設定

Cisco Unified Serviceability で、Cisco Database Layer Monitor などのサービスのアラームを設定できます。その後、システムがアラーム情報を送信する、Syslog ビューア（ローカル syslog）などのロケーションを設定します。 このオプションでは、次のことが可能です。

- 特定のサーバまたはすべてのサーバ（Unified Communications Manager クラスタのみ）のサービスにアラームを設定する
- 設定済みのサービスまたはサーバーに異なるリモート syslog サーバーを設定する
- 異なる宛先に異なるアラーム イベント レベルを設定する

Cisco Unified Communications Manager の管理 の Cisco Syslog Agent エンタープライズパラメータによって、リモート syslog サーバー名と syslog 重大度の 2 つの設定を使用して、設定されたしきい値を満たしているか、または超えているすべてのアラームをリモート syslog サーバーに転送できます。 これらの Cisco Syslog Agent のパラメータにアクセスするには、使用している構成に対応する次のウィンドウを開きます。

Unified Communications Manager	Cisco Unified Communications Manager の管理 で、**[システム（System）] > [エンタープライズ パラメータ（Enterprise Parameters）]** を選択します。
Cisco Unity Connection	Cisco Unity Connection Administration で、**[システム設定（System Setting）] > [エンタープライズ パラメータ（Enterprise Parameters）]** を選択します。
Cisco IM and Presence	Cisco Unified Communications Manager IM and Presence Administration で、**[システム（System）] > [エンタープライズ パラメータ（Enterprise Parameters）]** を選択します。

このアラームには、システム（OS/ハードウェアプラットフォーム）、アプリケーション（サービス）、およびセキュリティの各アラームが含まれます。

（注） Cisco Syslog Agent アラーム エンタープライズ パラメータとアプリケーション（サービス）アラームの両方を Cisco Unified Serviceability で設定すると、リモートの syslog に同じアラームが 2 回送信されることがあります。

ローカル syslog がアプリケーションアラームに対して有効になっている場合、ローカルの syslog しきい値とエンタープライズしきい値の両方をアラームが超えたときにだけ、エンタープライズリモート syslog サーバーにアラームが送信されます。

Cisco Unified Serviceability でリモートの syslog も有効になっている場合、システムは、Cisco Unified Serviceability で設定されているアプリケーションしきい値を使用してリモート syslog サーバーにアラームを転送します。このため、リモート syslog サーバーにアラームが 2 回送信される場合があります。

イベント レベル/重大度設定は、システムが収集するアラームおよびメッセージにフィルタリング メカニズムを提供します。 この設定は、Syslog およびトレース ファイルが過負荷状態になるのを防ぎます。 設定されたしきい値を超えるアラームおよびメッセージのみが転送されます。

アラームおよびイベントに関連する重大度レベルの詳細については、アラーム定義（117 ページ）を参照してください。

アラーム定義

アラーム定義とは、参照用に使用され、アラームの意味やアラームからの回復方法など、アラーム メッセージについて説明するものです。 アラーム情報は、[アラーム定義（Alarm Definitions）] ウィンドウで検索します。 サービス固有のアラーム定義をクリックすると、アラーム情報に関する説明（追加したユーザ定義のテキストなど）と推奨されるアクションが表示されます。

Serviceability GUI で表示されるすべてのアラームのアラーム定義を検索できます。 問題のトラブルシューティングを支援するため、対応するカタログに存在する定義には、アラーム名、記述、説明、推奨されるアクション、重大度、パラメータ、モニタなどが含まれています。

システムでアラームが生成されると、アラーム情報内のアラーム定義の名前が使用されるため、アラームを識別できます。 アラーム定義では、システムがアラーム情報を送信できる場所が指定されたルーティング リストを表示できます。 ルーティング リストには、次の場所が含まれます。これは、[アラーム設定（Alarm Configuration）] ウィンドウで設定できる場所に対応します。

- Unified Communications Manager のみ：[SDL]：アラームでこのオプションをイネーブルにし、[アラーム設定（Alarm Configuration）] ウィンドウでイベント レベルを指定した場合、アラーム情報は SDL トレースに送られます。

- [SDI]：アラームでこのオプションをイネーブルにし、[アラーム設定（Alarm Configuration）] ウィンドウでイベント レベルを指定した場合、アラーム情報は SDI トレースに送られます。
- システムログ（Sys Log）：アラームでこのオプションをイネーブルにし、[アラーム設定（Alarm Configuration）] ウィンドウでイベントレベルを指定して、リモート Syslog サーバーのサーバー名または IP アドレスを入力した場合、アラーム情報はリモート Syslog サーバーに送られます。
- [イベントログ（Event Log）]：アラームでこのオプションをイネーブルにし、[アラーム設定（Alarm Configuration）] ウィンドウでイベント レベルを指定した場合、アラーム情報はローカル Syslog に送られます。この情報は Cisco Unified Real-Time Monitoring Tool（Unified RTMT）の SysLog ビューアで表示できます。
- [データ コレクタ（Data Collector）]：アラーム情報はリアルタイム情報システム（RIS データ コレクタ）に送られます（アラート目的のみ）。 このオプションは [アラーム設定（Alarm Configuration）] ウィンドウで設定できません。
- [SNMP トラップ（SNMP Traps）]：SNMP トラップが生成されます。 このオプションは [アラーム設定（Alarm Configuration）] ウィンドウで設定できません。

ヒント　SNMP トラップの場所がルーティング リストに表示されている場合、アラーム情報が CCM MIB SNMP エージェントに送られ、CISCO-CCM-MIB 内の定義に従ってトラップが生成されます。

[アラーム設定（Alarm Configuration）] ウィンドウで特定の場所に対して設定されたアラーム イベント レベルが、アラーム定義に設定されている重大度以下の場合、アラームが送信されます。 たとえば、アラーム定義の重大度が WARNING_ALARM で、[アラーム設定（Alarm Configuration）] ウィンドウで特定の宛先のアラーム イベント レベルをそれよりも低い「警告」、「通知」、「情報」、または「デバッグ」として設定した場合、アラームは対応する宛先に送られます。アラームイベント レベルを「緊急」、「アラート」、「重要」、または「エラー」として設定した場合、アラームは対応する場所に送られません。

各アラーム定義について、追加説明または推奨事項を含めることができます。すべての管理者が追加情報にアクセスできます。 [アラームの詳細（Alarm Details）] ウィンドウに表示される [ユーザ定義テキスト（User Defined Text）] ペインに直接情報を入力します。 標準的な水平および垂直スクロールバーでスクロールできます。 Cisco Unified Serviceability により、データベースに情報が追加されます。

アラーム情報

アラーム情報を表示して、問題が存在するかどうかを特定できます。アラーム情報を表示するために使用する方法は、アラームを設定するときに選択した宛先に依存します。 SDL トレース ログ ファイル（Unified Communications Manager）に送信されるアラーム情報を表示するには、Unified RTMT の Trace and Log Central オプションを使用するか、テキスト エディタを使用

します。 ローカル syslog に送信されるアラーム情報を表示するには、Unified RTMT の SysLog ビューアを使用します。

アラームのセットアップ

アラームをセットアップするには、次の手順を実行します。

手順

ステップ 1 Cisco Unified Communications Manager の管理、Cisco Unity Connection Administration または Cisco Unified IM and Presence Administration で、指定したリモート Syslog サーバーにシステム、アプリケーション（サービス）、およびセキュリティのアラーム/メッセージを送信するように Cisco Syslog Agent エンタープライズパラメータを設定します。 Cisco Unified Serviceability でアプリケーション（サービス）アラーム/メッセージを設定する場合は、この手順をスキップしてください。

ステップ 2 Cisco Unified Serviceability では、収集するアプリケーション（サービス）アラーム情報のサーバ、サービス、宛先、およびイベント レベルを設定します。

ステップ 3 （任意）アラームに定義を追加します。

- サービスはすべて SDI ログに出力できます（ただし、トレースでも設定する必要があります）。
- すべてのサービスは SysLog ビューアに出力できます。
- Unified Communications Manager のみ：Cisco CallManager サービスと Cisco CTIManager サービスでのみ、SDL ログを使用します。
- Syslog メッセージをリモート Syslog サーバーに送信するには、宛先として [リモート Syslog（Remote Syslog）] チェックボックスをオンにし、ホスト名を指定します。リモートサーバー名を設定していない場合、Cisco Unified Serviceability はリモート Syslog サーバーに Syslog メッセージを送信しません。

ヒント Unified Communications Manager サーバーをリモート Syslog サーバーとして設定しないでください。

ステップ 4 アラームの宛先として SDL トレース ファイルを選択した場合は、Unified RTMT の Trace and Log Central オプションを使用してトレースの収集と情報の表示を行います。

ステップ 5 アラームの宛先としてローカル Syslog を選択した場合は、Unified RTMT の SysLog ビューアでアラーム情報を表示します。

ステップ 6 説明と推奨されるアクションについては、対応するアラーム定義を参照してください。

アラーム サービスの設定

Syslog Agent エンタープライズ パラメータ

Cisco Syslog Agentエンタープライズパラメータは、設定されたしきい値を超過したシステム、アプリケーション、セキュリティ アラームまたはメッセージを指定したリモート syslog サーバーに送信するように設定できます。 Cisco Syslog Agent のパラメータにアクセスするには、使用している構成に対応する次のウィンドウを開きます。

Unified Communications Manager	Cisco Unified Communications Manager の管理 で、**[システム（System）] > [エンタープライズ パラメータ（Enterprise Parameters）]** を選択します。
Cisco Unity Connection	Cisco Unity Connection Administration で、**[システム設定（System Setting）] > [エンタープライズ パラメータ（Enterprise Parameters）]** を選択します。
Cisco IM and Presence	Cisco Unified Communications Manager IM and Presence Administration で、**[システム（System）] > [エンタープライズ パラメータ（Enterprise Parameters）]** を選択します。

次に、リモート syslog サーバ名（リモート syslog サーバ名 1、リモート syslog サーバ名 2、リモート syslog サーバ名 3、リモート syslog サーバ名 4、およびリモート syslog サーバ名 5）および syslog 重大度を設定します。 サーバ名を設定する際には、有効な IP アドレスを指定してください。 syslog の重大度は、設定するすべてのリモート syslog サーバーに適用できます。 次に [保存（Save）]をクリックします。 [?]ボタンをクリックすると、入力できる有効な値が表示されます。 サーバ名が指定されていないと、Cisco Unified Serviceability は Syslog メッセージを送信しません。

注意 Unified Communications Manager でリモート syslog サーバーを設定する際は、リモート syslog サーバー名に重複するエントリを追加しないでください。 重複するエントリを追加した場合、Cisco Syslog Agent はメッセージをリモート syslog サーバーに送信するときに重複したエントリを無視します。

（注） Unified Communications Manager をリモート Syslog サーバーとして設定しないでください。 Unified Communications Manager ノードは、別のサーバからの Syslog メッセージを受け入れません。

アラーム サービスのセットアップ

ここでは、Cisco Unified Serviceability で管理する機能サービスやネットワーク サービスのアラームを追加または更新する方法について説明します。

（注） SNMP トラップとカタログの設定は変更しないことを推奨します。

Cisco Unity Connection では、Cisco Unity Connection Serviceability で使用可能なアラームも使用します。 Cisco Unity Connection Serviceability ではアラームを設定できません。 詳細については、『*Cisco Unity Connection Serviceability Administration Guide*』を参照してください。

標準のレジストリ エディタの使用方法の詳細については、使用している OS のオンライン ドキュメントを参照してください。

手順

ステップ 1 **[アラーム（Alarm）]** > **[設定（Configuration）]** を選択します。

[アラーム設定（Alarm Configuration）] ウィンドウが表示されます。

ステップ 2 [サーバー（Server）] ドロップダウンリストから、アラームを設定するサーバーを選択し、**[移動（Go）]** をクリックします。

ステップ 3 [サービス グループ（Service Group）] ドロップダウン リストから、アラームを設定するサービスのカテゴリ（[データベースおよび管理サービス（Database and Admin Services）] など）を選択し、[移動（Go）]をクリックします。

ヒント サービス グループに対応するサービスの一覧については、「サービス グループ」を参照してください。

ステップ 4 [サービス（Service）] ドロップダウン リストからアラームを設定するサービスを選択し、[移動（Go）]をクリックします。

サービス グループと設定をサポートするサービスだけが表示されます。

ヒント ドロップダウンリストには、アクティブなサービスと非アクティブのサービスが表示されます。

[アラーム設定（Alarm Configuration）] ウィンドウには、選択したサービスのアラーム モニタとイベント レベルのリストが表示されます。 また、[すべてのノードに適用（Apply to All Nodes）] チェックボックスも表示されます。

ステップ 5 Unified Communications Manager のみ：クラスタをサポートしている設定の場合は、必要に応じて**すべてのノードに適用**チェックボックスをオンにして、クラスタ内のすべてのノードにサービスのアラーム設定を適用することができます。

ステップ 6 「アラーム設定」の説明に従って設定を行います。この項ではモニタおよびイベント レベルについても説明されています。

ステップ 7 設定を保存するには、[保存（Save）]ボタンをクリックします。

（注） デフォルトを設定するには、[デフォルトの設定（Set Default）]ボタンをクリックしてから、[保存（Save）]をクリックします。

次のタスク

ヒント [アラーム設定（Alarm Configuration）] ウィンドウで特定の宛先に対して設定されたアラーム イベント レベルが、アラーム定義に設定されている重大度以下の場合、アラームが送信されます。 たとえば、アラーム定義の重大度が WARNING_ALARM で、[アラーム設定（Alarm Configuration）] ウィンドウで特定の宛先のアラーム イベント レベルをそれよりも低い「警告」、「通知」、「情報」、または「デバッグ」として設定した場合、アラームは対応する宛先に送られます。 アラーム イベント レベルを、重大度がより高い「緊急」、「警報」、「重大」、または「エラー」として設定した場合、アラームは対応する場所に送られません。

Cisco エクステンション モビリティ アプリケーション サービス、Cisco Unified Communications Manager Assistant サービス、Cisco エクステンション モビリティ サービス、および Cisco Web Dialer サービスのアラーム定義にアクセスするには、「アラーム定義」で説明されている [アラームメッセージ定義（Alarm Messages Definitions）] ウィンドウの [JavaApplications]カタログを選択します。

Cisco Tomcat を使用するアラーム サービスのセットアップ

次のサービスは、アラームの生成に Cisco Tomcat を使用します。

- Cisco Extension Mobility アプリケーション
- Cisco IP Manager Assistant
- Cisco Extension Mobility
- Cisco Web Dialer

システム ログイン アラーム AuthenticationFailed も Cisco Tomcat を使用します。 これらのサービスに対してアラームを生成するには、次の手順を実行します。

手順

ステップ 1 Cisco Unified サービスアビリティで、**[アラーム（Alarm）] > [設定（Configuration）]** 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、アラームを設定するサーバーを選択し、**[移動（Go）]** をクリックします。

ステップ 3 [サービスグループ（Services Group）] ドロップダウン リストから、[プラットフォームサービス（Platform Services）]を選択し、[移動（Go）]をクリックします。

ステップ 4 [サービス（Services）] ドロップダウン リストから、**[CiscoTomcat]** を選択し、**[移動（Go）]** をクリックします。

ステップ 5 Unified Commuications Manager のみ：クラスタをサポートしている設定の場合は、必要に応じて [すべてのノードに適用（Apply to All Nodes）]チェックボックスをオンにして、クラスタ内のすべてのノードにサービスのアラーム設定を適用できます。

ステップ 6 「アラーム設定」の説明に従って設定を行います。この項ではモニタおよびイベント レベルについても説明されています。

ステップ 7 設定を保存するには、[保存（Save）]ボタンをクリックします。

サービス グループ

次の表に、[アラーム設定（Alarm Configuration）] ウィンドウの [サービス グループ（Service Group）] ドロップダウン リスト ボックスに表示されるオプションに対応するサービスの一覧を示します。

（注） 一覧されているすべてのサービス グループとサービスが、すべてのシステム設定に適用されるわけではありません。

表 7: アラーム設定のサービス グループ

サービス グループ	サービス
CM サービス	Cisco CTIManager、Cisco CallManager、Cisco DHCP Monitor サービス、Cisco Dialed Number Analyzer、Cisco Dialed Number Analyzer Server、Cisco Extended Functions、Cisco IP Voice Media Streaming App、Cisco Messaging Interface、シスコ ヘッドセット サービス、および Cisco TFTP
CTI サービス	Cisco IP Manager Assistant および Cisco WebDialer Web サービス
CDR サービス	Cisco CAR Scheduler、Cisco CDR Agent、および Cisco CDR Repository Manager
データベースおよび管理者サービス	Cisco Bulk Provisioning サービスと Cisco Database Layer Monitor
パフォーマンスおよびモニタリング サービス	Cisco AMC サービスおよび Cisco RIS Data Collector
セキュリティ サービス	Cisco Certificate Authority Proxy Function と Cisco Certificate Expiry Monitor

サービス グループ	サービス
ディレクトリ サービス	Cisco DirSync
バックアップおよび復元サービス	Cisco DRF Local および Cisco DRF Master
システム サービス	Cisco Trace Collection サービス
プラットフォーム サービス	Cisco Tomcat と Cisco Smart License Manager
ロケーションベースのトラッキング サービス	Cisco Wireless Controller Synchronization サービス

アラーム設定

次の表で、すべてのアラームの構成時の設定について説明します。サービスでこれらの設定をサポートしていない場合もあります。

表 *8:* アラーム設定

名前	説明
サーバ（Server）	ドロップダウン リストから、アラームを設定するサーバ（ノード）を選択し、[移動（Go）]をクリックします。
サービス グループ	Cisco Unity Connection がサポートしているサービス グループは、[データベースおよび管理サービス（Database and Admin Services）]、[パフォーマンスおよびモニタリング サービス（Performance and Monitoring Services）]、[バックアップおよび復元サービス（Backup and Restore Services）]、[システム サービス（System Services）]、[プラットフォーム サービス（Platform Services）] だけです。 ドロップダウン リストからアラームを設定するサービスのカテゴリ（[データベースおよび管理サービス（Database and Admin Services）] など）を選択し、[移動（Go）] をクリックします。

名前	説明
サービス	[サービス（Service）] ドロップダウン リストからアラームを設定するサービスを選択し、[移動（Go）]をクリックします。 サービス グループと設定をサポートするサービスだけが表示されます。 **ヒント** ドロップダウン リストには、実行中のサービスと実行されていないサービスの両方が表示されます。
Unified Communications Manager および Cisco Unified Communications Manager IM and Presence Serviceのみ： すべてのノードに適用（Apply to All Nodes）	クラスタ内のすべてのノードにサービスのアラーム設定を適用するには、このチェックボックスをオンにします。
ローカル Syslog のアラームのイネーブル化（Enable Alarm for Local Syslogs）	SysLog ビューアがアラームの宛先として機能します。プログラムはエラーを Syslog ビューアの [アプリケーション ログ（Application Logs）] に記録して、アラームの説明と推奨処置を提供します。 Syslog ビューアには Cisco Unified Real-Time Monitoring Tool からアクセスできます。 Syslog ビューアでのログの表示については、『*Cisco Unified Real-Time Monitoring Tool Administration Guide*』を参照してください。

名前	説明
リモート Syslog のアラームのイネーブル化（Enable Alarm for Remote Syslogs）	SysLog ファイルがアラームの宛先として機能します。 このチェックボックスをオンにすると、Syslog メッセージを Syslog サーバーに保存して、その Syslog サーバーの名前を指定することができます。この通知先が有効になっているときにサーバー名が指定されていないと、Cisco Unified Serviceability は Syslog メッセージを送信しません。 設定されている AMC プライマリとフェールオーバー コレクタは、リモート Syslog 設定を使用します。 コレクタが使用するリモート Syslog 設定は、個々のノードでそれぞれ設定されている設定です。 リモート Syslog が AMC プライマリ コレクタでのみ設定されていて、AMC フェールオーバー コレクタでリモート Syslog が設定されていないときに、AMC プライマリ コレクタでフェールオーバーが発生すると、リモート Syslog は生成されません。 すべてのノードで同じ設定を正確に行い、リモート Syslog アラームが同じリモート Syslog サーバーに送信されるようにする必要があります。 フェールオーバーが AMC コントローラで発生した場合、またはコレクタの設定が別のノードに変更される場合は、バックアップ ノードまたは新たに設定されたノードのリモート Syslog の設定が使用されます。 システムで非常に多くのアラームがフラッディングするのを防ぐには、[エンドポイントアラームを除外（Exclude End Point Alarms）] チェックボックスをオンにします。 これにより、エンドポイントの電話関連のイベントが別のファイルに記録されるようになります。 [エンドポイントアラームを除外（Exclude End Point Alarms）] チェックボックスは Call Manager サービスの場合にのみ表示され、デフォルトでは選択されていません。 このチェックボックスをオンにする場合は、[すべてのノードに適用（Apply to All Nodes）]もオンにする必要があります。 エンドポイントアラームの設定オプションは、アラームの構成時の設定に表示されます。 **ヒント** ノードは他のノードからの Syslog メッセージを受け付けないため、Unified Communications Manager あるいは Cisco Unified Communications Manager IM and Presence Service ノードを通知先として指定しないでください。

名前	説明
リモート Syslog サーバ（Remote Syslog Server）	[サーバー名 1（Server Name 1）]、[サーバー名 2（Server Name 2）]、[サーバー名 3（Server Name 3）]、[サーバー名 4（Server Name 4）]、[サーバー名 5（Server Name 5）] の各フィールドに、Syslog メッセージを受け入れるために使用するリモート Syslog サーバーの名前または IP アドレスを入力します。 たとえば、アラームを Cisco Unified Operations Manager に送信する場合は、Cisco Unified Operations Manager をサーバ名として指定します。 **ヒント** ノードは他のノードからの Syslog メッセージを受け付けないため、Unified Communications Manager あるいは Cisco Unified Communications Manager IM and Presence Service ノードを通知先として指定しないでください。
SDI トレースのアラームのイネーブル化（Enable Alarm for SDI Trace）	SDI トレース ライブラリがアラームの宛先として機能します。 アラームを記録するには、このチェックボックスをオンにして、選択されたサービスの [トレース設定（Trace Configuration）] ウィンドウで [トレース オン（Trace On）] チェックボックスをオンにします。 Cisco Unified Serviceability の [トレース設定（Trace Configuration）] ウィンドウの構成時の設定の詳細については、トレース パラメータのセットアップを確認します。
Unified Communications Manager および Unified Communications Manager BE のみ： SDL トレースのアラームのイネーブル化（Enable Alarm for SDL Trace）	SDL トレース ライブラリがアラームの宛先として機能します。 この宛先は Cisco CallManager サービスと CTIManager サービスの場合にのみ使用できます。 このアラームの宛先を設定するには、Trace SDL の設定を使用します。 SDL トレース ログ ファイルにアラームのログを記録するには、このチェックボックスをオンにして、選択したサービスの [トレース設定（Trace Configuration）] ウィンドウで [トレース オン（Trace On）] チェックボックスをオンにします。 Cisco Unified Serviceability の [トレース設定（Trace Configuration）]ウィンドウの構成時の設定の詳細については、トレース パラメータのセットアップを確認します。

名前	説明
アラーム イベント レベル（Alarm Event Level）	ドロップダウン リストから、次のオプションのいずれかを選択します。 **緊急（Emergency）** このレベルは、システムを使用不能と指定します。 **アラート（Alert）** このレベルは、ただちに対処が必要であることを示します。 **クリティカル（Critical）** システムがクリティカルな状態を検出します。 **エラー（Error）** このレベルは、エラーがあることを示します。 **警告** このレベルは、警告状態が検出されたことを示します。 **通知（Notice）** このレベルは、正常ではあるものの重要な状態を示します。 **情報（Informational）** このレベルは、情報メッセージだけを示します。 **デバッグ（Debug）** このレベルは、Cisco Technical Assistance Center のエンジニアがデバッグに使用する詳細イベント情報を示します。

次の表に、デフォルトのアラームの構成時の設定について説明します。

	ローカル syslog	リモート syslog	SDI トレース	SDL トレース
アラームのイネーブル化（Enable Alarm）	オン	オフ	オン	オン
アラーム イベント レベル（Alarm Event Level）	エラー（Error）	無効	エラー（Error）	エラー（Error）

エンド ポイント アラームを除外	ローカル Syslog	代替 syslog	リモート Syslog	Syslog の重大度とアラートの絞り込み	Syslog トラップ

オン	不可	可	不可	不可	不可
オフ	不可	可	可	可	可

アラーム定義およびユーザ定義の説明の追加

ここでは、Serviceability のインターフェイスに表示されるアラーム定義のユーザ情報を検索、表示、作成する手順について説明します。

アラーム定義の表示とユーザ定義の説明の追加

ここでは、アラーム定義の検索方法と表示方法について説明します。

ヒント Unified Communications Manager および Cisco Unity Connection のみ：Cisco Unity Connection Serviceability で Cisco Unity Connection アラーム定義を表示することができます。 Cisco Unity Connection Serviceability ではアラーム定義にユーザ定義の説明を追加できません。

Cisco Unity Connection は、Cisco Unified Serviceability で特定のアラーム定義を使用します。それらのアラーム定義は、Cisco Unified Serviceability で表示する必要があります。 システム カタログ内のカタログに関連したアラームは表示用であることに注意してください。

始める前に

アラーム定義カタログの記述を確認してください。

手順

ステップ 1 **[アラーム（Alarm）]** > **[定義（Definitions）]** を選択します。

ステップ 2 次のいずれかの操作を実行します。

- 次のようにアラームを選択します。
  - [アラームの検索場所（Find alarms where）]ドロップダウン リストからアラーム カタログを選択します。たとえば、システム アラーム カタログまたは IM and Presence アラーム カタログを選択します。
  - [等しい（Equals）]ドロップダウン リストから特定のカタログ名を選択します。
- [アラーム名を入力（Enter Alarm Name）]フィールドにアラーム名を入力します。

ステップ 3 [検索（Find）]を選択します。

ステップ 4 複数のアラーム定義ページが存在する場合は、次のいずれかの操作を実行します。

- 別のページを選択するには、[アラームメッセージ定義（Alarm Message Definitions）]ウィンドウで適切なナビゲーション ボタンを選択します。
- ウィンドウに表示されるアラームの数を変更するには、[ページあたりの行数（Rows Per Page）]ドロップダウン リストから別の値を選択します。

ステップ 5 アラームの詳細を設定するアラーム定義を選択します。

ステップ 6 アラームに情報を追加する場合は、[ユーザ定義テキスト（User Defined Text）]フィールドにテキストを入力し、[保存（Save）]を選択します。

ヒント [ユーザ定義テキスト（User Defined Text）] フィールドにテキストを追加する場合、いつでも [すべてクリア（Clear All）]を選択して入力した情報を削除できます。

ステップ 7 **保存**を選択します。

ステップ 8 **[アラームメッセージ定義（Alarm Message Definitions）]** ウィンドウに戻るには、[関連リンク（Related Links）] ドロップダウン リストから **[アラームの検索/リストに戻る（Back to Find/List Alarms）]** を選択します。

ステップ 9 [移動（Go）]を選択します。

システム アラーム カタログの説明

次の表に、システム アラーム カタログのアラームの説明を示します。システム アラーム カタログでは、Cisco Unified Communications Manager および Cisco Unity Connectionをサポートしています。

表 *9:* システム カタログ

名前	説明
ClusterManagerAlarmCatalog	クラスタ内のサーバー間のセキュリティ アソシエーションの確立すべての Cluster Manager アラーム定義。
DBAlarmCatalog	すべてのシスコ データベース アラーム定義
DRFAlarmCatalog	すべてのディザスタ リカバリ システム アラーム定義
GenericAlarmCatalog	すべてのアプリケーションで共有されるすべての汎用アラーム定

名前	説明
JavaApplications	すべての Java アプリケーション アラーム定義。 ヒント アラーム設定 GUI を使用して JavaApplications アラーム とはできません。 Unified Communications Manager およ Connection の場合は、通常はこれらのアラームをイベン よう設定します。Unified Communications Manager の場合 アラームは SNMP トラップを生成して CiscoWorks LAN Solution と統合するように設定します。 アラーム定義と 表示および変更するには、オペレーティング システムに レジストリ エディタを使用してください。
EMAlarmCatalog	エクステンション モビリティのアラーム
LoginAlarmCatalog	すべてのログイン関連のアラーム定義
LpmTctCatalog	すべてのログパーティションモニタリングおよびトレース収
RTMTAlarmCatalog	すべての Cisco Unified Real-Time Monitoring Tool アラーム定義
SystemAccessCatalog	SystemAccess がすべてのプロセス統計カウンタと共にすべての カウンタを提供するかどうかのトラッキングに使用されるす 定義。
ServiceManagerAlarmCatalogs	サービスのアクティブ化、非アクティブ化、開始、リスター に関連するすべての Service Manager アラーム定義。
TFTPAlarmCatalog	すべての Cisco TFTP アラーム定義
TVSAlarmCatalog	信頼検証サービスのアラーム
TestAlarmCatalog	コマンドライン インターフェイス（CLI）から SNMP トラッ ト アラームを送信するために使用されるすべてのアラーム定 については、『*Command Line Interface Reference Guide for Cisc* *Solutions*』を参照してください。 ヒント Cisco Unity Connection SNMP では、Unified Communicat よび Cisco Unity Connection システムのトラップをサポー ん。
CertMonitorAlarmCatalog	すべての証明書の有効期限の定義。
CTLproviderAlarmCatalog	Certificate Trust List（CTL）Provider サービスのアラーム
CDPAlarmCatalog	Cisco Discovery Protocol（CDP）サービスのアラーム
IMSAlarmCatalog	すべてのユーザ認証とクレデンシャルの定義。
SLMAlarmCatalog	Cisco Smart Licensing のアラーム

CallManager アラーム カタログの説明

ここで説明する内容は、Cisco Unity Connection には適用されません。

次の表に、CallManager アラーム カタログの説明を示します。

表 *10 : CallManager* アラーム カタログ

名前	説明
CallManager	すべての Cisco CallManager サービスのアラーム定義
CDRRepAlarmCatalog	すべての CDRRep アラーム定義
CARAlarmCatalog	すべての CDR 分析とレポート アラーム定義
CEFAlarmCatalog	すべての Cisco Extended Functions のアラーム定義
CMIAlarmCatalog	すべての Cisco Messaging Interface のアラーム定義
CtiManagerAlarmCatalog	すべての Cisco Computer Telephony Integration（CTI）マネージャの義
IpVmsAlarmCatalog	すべての IP Voice Media Streaming Application のアラーム定義
TCDSRVAlarmCatalog	すべての Cisco Telephony Call Dispatcher サービスのアラーム定義
電話（Phone）	ダウンロードなどの電話関連タスクに対するアラーム
CAPFAlarmCatalog	Certificate Authority Proxy Function（CAPF）サービスに対するア
SAMLSSOAlarmCatalog	SAML シングル サインオン機能に対するアラーム

IM and Presence アラーム カタログの説明

次の表に、IM and Presence Service アラーム カタログの説明を示します。

表 *11 : IM and Presence Service* アラーム カタログ

名前	説明
CiscoUPSConfigAgent	IM and Presence Service IDS データベースの構成変更を IM and Presence Service SIP プロキシに通知する、すべての構成エージェント アラーム。
CiscoUPInterclusterSyncAgent	クラスタ間ルーティングのために IM and Presence Service クラスタ間でエンド ユーザ情報を同期化する、すべてのクラスタ間同期エージェント アラーム。

名前	説明
CiscoUPSPresenceEngine	可用性ステータスとユーザーの通信機能に関する情報を収集する、すべてのプレゼンスエンジンアラーム。
CiscoUPSSIPProxy	ルーティング、要求者識別、およびトランスポートの相互接続に関するすべての SIP プロキシ アラーム。
CiscoUPSSOAP	HTTPS を使用して外部クライアントとの間での安全な SOAP インターフェイスを提供する、すべての Simple Object Access Protocol（SOAP）アラーム。
CiscoUPSSyncAgent	Unified Communications Manager との IM and Presence Service データの同期を保つすべての Sync Agent アラーム。
CiscoUPXCP	IM and Presence Service 上の XCP コンポーネントとサービスのステータスに関する情報を収集するすべての XCP アラーム。
CiscoUPServerRecoveryManager	プレゼンス冗長グループ内のノード間のフェールオーバーおよびフォールバック プロセスに関するすべての Server Recovery Manager アラーム。
CiscoUPReplWatcher	IDS 複製状態をモニタするすべての ReplWatcher アラーム。
CiscoUPXCPConfigManager	XCP コンポーネントに関係するすべての Cisco XCP Config Manager アラーム定義。

アラーム情報には、説明と推奨されるアクションが含まれているのに加えて、ローカル IM and Presence Service ノード以外の問題についてもトラブルシューティングを行うのに役立つ、アプリケーション名、サーバ名などが含まれています。

IM and Presence Service に固有のアラームの詳細については、『*System Error Messages for IM and Presence on Cisco Unified Communications Manager*』を参照してください。

CiscoSyslog ファイル内のデフォルトのアラーム

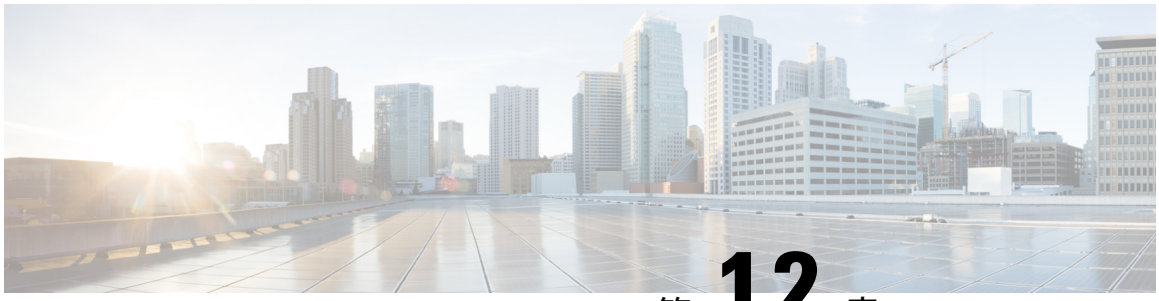
次の表に、アラーム設定なしで CiscoSyslog ファイルでトリガーされるデフォルト アラームの説明を示します。

表 *12 : CiscoSyslog* ファイル内のデフォルトのアラーム

名前	説明
CLM_IPSecCertUpdated	変更が発生したため、クラスタ内のピア ノードから IPSec 自己署名証明書がインポートされました。
CLM_IPAddressChange	クラスタ内のピア ノードの IP アドレスが変更されました。
CLM_PeerState	クラスタ内の別のノードとの ClusterMgr のセッション状態が、現在の状態に変更されました。
CLM_MsgIntChkError	ClusterMgr は、メッセージの整合性チェックに失敗したメッセージを受信しました。 これは、クラスタ内の別のノードが誤ったセキュリティ パスワードで設定されていることを示す場合があります。
CLM_UnrecognizedHost	ClusterMgr は、このクラスタ内でノードとして設定されていない IP アドレスからメッセージを受信しました。
CLM_ConnectivityTest	Cluster Manager により、ネットワーク エラーが検出されました。
ServiceActivated	このサービスはアクティブになっています。
ServiceDeactivated	このサービスは現在非アクティブになっています。
ServiceActivationFailed	このサービスをアクティブにできませんでした。
ServiceDeactivationFailed	このサービスを非アクティブにできませんでした。
ServiceFailed	サービスが突然終了しました。 サービス マネージャが再起動を試みます。
ServiceStartFailed	このサービスを開始できませんでした。 サービス マネージャがサービスの開始を再度試みます。
ServiceStopFailed	数回の再試行後に指定されたサービスを停止できません。 サービスは停止済みとマークされます。

名前	説明
ServiceRestartFailed	指定されたサービスを再起動できません。
ServiceExceededMaxRestarts	再起動の試行を最大数行っても、サービスを開始できませんでした。
FailedToReadConfig	設定ファイルの読み込みに失敗しました。 設定ファイルが壊れている可能性があります。
MemAllocFailed	メモリの割り当てに失敗しました。
SystemResourceError	システム コールに失敗しました。
ServiceManagerUnexpectedShutdown	予期しない終了後にサービス マネージャが正常に再起動されました。
OutOfMemory	プロセスからオペレーティングシステムに対してメモリがリクエストされていますが、使用可能なメモリが不足しています。
CREATE-DST-RULE-FILE-CLI	新しい DST ルール ファイルが cli から生成されます。電話機を再起動する必要があります。電話機を再起動しないと、DSTの開始日/終了日が間違った日付になります。
CREATE-DST-RULE-FILE-BOOTUP	新しいDSTルール ファイルがブートアップ中に生成されます。 電話機を再起動する必要があります。電話機を再起動しないと、DST の開始日/終了日が間違った日付になります。
CREATE-DST-RULE-FILE-CRON	新しい DST ルール ファイルが cron から生成されます。 電話機を再起動する必要があります。電話機を再起動しないと、DSTの開始日/終了日が間違った日付になります。
PermissionDenied	このプロセスにはこの操作を実行する権限がないため、この操作を完了できませんでした。
ServiceNotInstalled	実行可能ファイルの開始が試行されていますが、サービス制御マネージャでサービスとして設定されていないため、開始できません。サービス名は %s です。
ServiceStopped	サービスが停止しました。
ServiceStarted	サービスが開始されました。
ServiceStartupFailed	サービスが開始されました。

名前	説明
FileWriteError	プライマリ ファイルパスに書き込めませんでした。



第 12 章

監査ログ

監査ログ

監査ログを使用すると、監査用の別のログ ファイルにシステムの設定変更が記録されます。

監査ロギング（標準）

監査ロギングは有効になっているが、詳細監査ロギング オプションは選択されていない場合は、システムが標準監査ロギング用に設定されます。

標準監査ロギングを使用すると、監査用の別のログ ファイルにシステムの設定変更が記録されます。 Serviceability GUI の [コントロール センター - ネットワーク サービス（Control Center - Network Services）] の下に表示される Cisco Audit Event Service により、ユーザーが行った、またはユーザーの操作によって発生したシステムへの設定変更がモニタされ、ログに記録されます。

監査ログの設定を行うには、Serviceability GUI の [監査ログの設定（Audit Log Configuration）] ウィンドウにアクセスします。

標準監査ロギングの構成は次のとおりです。

- 監査ロギング フレームワーク：このフレームワークは、監査ログに監査イベントを書き込むためにアラーム ライブラリを使用する API で構成されます。 GenericAlarmCatalog.xml として定義されたアラーム カタログがこれらのアラームに適用されます。 各種システム コンポーネントで独自のロギングが提供されます。

  以下に、アラームを送信するために Unified Communications Manager のコンポーネントを使用することが API の例を示します。

```
User ID: CCMAdministratorClient IP Address: 172.19.240.207 Severity: 3
EventType: ServiceStatusUpdated ResourceAccessed: CCMService EventStatus:
Successful Description: CallManager Service status is stopped
```

- 監査イベントロギング：監査イベントとは、記録する必要があるあらゆるイベントを指します。 次に、監査イベントの例を示します。

```
CCM_TOMCAT-GENERIC-3-AuditEventGenerated: Audit Event Generated
UserID:CCMAdministrator Client IP Address:172.19.240.207 Severity:3
EventType:ServiceStatusUpdated ResourceAccessed: CCMService
EventStatus:Successful Description: Call Manager Service status is stopped
 App ID:Cisco Tomcat Cluster ID:StandAloneCluster Node ID:sa-cm1-3
```

ヒント　監査イベントのロギングは、デフォルトでは一元的に管理され、有効化されることに注意してください。 Syslog Audit と呼ばれるアラーム モニタによってログが書き込まれます。 デフォルトでは、ログはローテーションされるように設定されています。 AuditLogAlarmMonitor が監査イベントを書き込むことができない場合、AuditLogAlarmMonitor はこのエラーを重大なエラーとして syslog ファイルに記録します。 Alert Manager は、SeverityMatchFound アラートの一部としてこのエラーを報告します。 イベント ロギングが失敗した場合も実際の動作は継続されます。 監査ログはすべて、Cisco Unified Real-Time Monitoring Tool の Trace and Log Central から収集、表示、および削除されます。

Cisco Unified Serviceability の標準イベント ロギング

Cisco Unified Serviceability では次のイベントがログに記録されます。

- サービスのアクティブ化、非アクティブ化、起動、または停止。
- トレース設定およびアラーム設定の変更。
- SNMP 設定の変更。
- CDR 管理の変更 （Cisco Unified Communications Manager のみ）。
- サービスアビリティ レポートのアーカイブのレポートの参照。 このログは、レポート用ノードで表示されます。 （Unified Communications Manager のみ）

Cisco Unified Real-Time Monitoring Tool の標準イベント ロギング

Cisco Unified Real-Time Monitoring Tool では、監査イベント アラームを含む次のイベントがログに記録されます。

- アラートの設定
- アラートの一時停止
- 電子メールの設定
- ノード アラート ステータスの設定
- アラートの追加
- アラートの追加アクション

- アラートのクリア
- アラートのイネーブル化
- アラートの削除アクション
- アラートの削除

Unified Communications Manager 標準イベント ロギング

Cisco CDR Analysis and Reporting（CAR）では、次のイベントに関する監査ログが作成されます。

- ローダのスケジューリング
- 日次、週次、月次レポートのスケジューリング
- メール パラメータの設定
- ダイヤル プラン設定
- ゲートウェイの設定
- システム プリファレンスの設定
- 自動消去の設定
- 接続時間、時刻、および音声品質の評価エンジンの設定
- QoS の設定
- 事前生成レポートの自動生成/アラートの設定
- 通知限度の設定

Cisco Unified CM Administration の標準イベント ロギング

次のイベントは、Cisco Unified Communications Manager の管理 のさまざまなコンポーネントに対して記録されます。

- ユーザーのログイン/ログアウト
- ユーザーのロールメンバーシップの更新（ユーザーの追加、ユーザーの削除、またはユーザーのロールの更新）
- ロールの更新（新しいロールの追加、削除、または更新）
- デバイスの更新（電話機およびゲートウェイ）
- サーバ設定の更新（アラームまたはトレースの設定、サービスパラメータ、エンタープライズパラメータ、IP アドレス、ホスト名、イーサネット設定の変更、および Unified Communications Manager サーバーの追加または削除）。

Cisco Unified Communications セルフ ケア ポータルの標準イベント ロギング

Cisco Unified Communications セルフ ケア ポータルに対するユーザ ロギング（ユーザ ログインとユーザ ログアウト）イベントが記録されます。

コマンドライン インターフェイスの標準イベント ロギング

コマンドラインインターフェイスで実行されたすべてのコマンドがログに記録されます（Unified Communications Manager と Cisco Unity Connection の両方）。

Cisco Unity Connection Administration の標準イベント ロギング

Cisco Unity Connection Administration では次のイベントがログに記録されます。

- ユーザーのログイン/ログアウト
- すべての設定変更（ユーザ、連絡先、コール管理オブジェクト、ネットワーク、システム設定、テレフォニーなど）
- タスク管理（タスクの有効化/無効化）
- 一括管理ツール（一括作成、一括削除）
- カスタム キーパッド マップ（マップの更新）

Cisco Personal Communications Assistant（Cisco PCA）の標準イベント ロギング

Cisco Personal Communications Assistant クライアントでは次のイベントがログに記録されます。

- ユーザーのログイン/ログアウト
- Messaging Assistant で行われたすべての設定変更

Cisco Unity Connection Serviceability の標準イベント ロギング

Cisco Unity Connection Serviceability では次のイベントがログに記録されます。

- ユーザーのログイン/ログアウト。
- すべての設定変更。
- サービスのアクティブ化、非アクティブ化、開始、または停止。

Representational State Transfer API を使用する Cisco Unity Connection クライアントのイベント ロギング

Representational State Transfer（REST）API を使用する Cisco Unity Connection クライアントでは次のイベントがログに記録されます。

- ユーザーのログイン（ユーザーの API 認証）。
- Cisco Unity Connection プロビジョニング インターフェイスを使用する API 呼び出し。

Cisco Unified IM and Presence Serviceability の標準イベント ロギング

Cisco Unified IM and Presence Serviceability では次のイベントがログに記録されます。

- サービスのアクティブ化、非アクティブ化、起動、または停止
- トレース設定およびアラーム設定の変更
- SNMP 設定の変更
- サービスアビリティ レポートのアーカイブ内のレポートの参照（このログは、レポート用ノードで表示されます）

Cisco Unified IM and Presence Real-Time Monitoring Tool の標準イベント ロギング

Cisco Unified IM and Presence Real-Time Monitoring Tool では、監査イベント アラームを含む次のイベントがログに記録されます。

- アラートの設定
- アラートの一時停止
- 電子メールの設定
- ノード アラート ステータスの設定
- アラートの追加
- アラートの追加アクション
- アラートのクリア
- アラートのイネーブル化
- アラートの削除アクション
- アラートの削除

Cisco IM and Presence Administration の標準イベント ロギング

以下のイベントは、Cisco Unified Communications Manager 管理のさまざまなコンポーネントに対して記録されます。

- 管理者のロギング（Administration、OS Administration、Disaster Recovery System、Reporting などの IM and Presence のインターフェイスへのログインおよびログアウト）
- ユーザーのロールメンバーシップの更新（ユーザーの追加、ユーザーの削除、またはユーザーのロールの更新）
- ロールの更新（新しいロールの追加、削除、または更新）
- デバイスの更新（電話機およびゲートウェイ）

- サーバー設定の更新（アラームまたはトレースの設定、サービスパラメータ、エンタープライズパラメータ、IP アドレス、ホスト名、イーサネット設定の変更、および IM and Presence サーバーの追加または削除）

IM and Presence アプリケーションの標準イベント ロギング

IM and Presence アプリケーションのさまざまなコンポーネントでは、次のイベントがログに記録されます。

- IM クライアントへのエンドユーザーのログイン（ユーザーのログイン/ログアウト、およびログイン試行の失敗）
- IM チャットルームへのユーザーの入室および退室
- IM チャット ルームの作成と破棄

コマンドライン インターフェイスの標準イベント ロギング

コマンドライン インターフェイスで実行されたすべてのコマンドがログに記録されます。

監査ロギング（詳細）

詳細監査ロギングは、標準（デフォルト）監査ログに保存されない追加の設定変更を記録するオプション機能です。 標準監査ログに保存されるすべての情報に加えて、詳細監査ロギングには、変更された値も含め、追加、更新、または削除された設定項目も保存されます。 詳細監査ロギングはデフォルトで無効になっていますが、[監査ログ設定（Audit Log Configuration）]ウィンドウで有効にすることができます。

Audit Log Types

システム監査ログ

システム監査ログでは、Linux OS ユーザーの作成、変更、削除、ログの改ざん、およびファイルまたはディレクトリの権限に対するあらゆる変更をトレースします。 このタイプの監査ログは、収集されるデータが大量になるためにデフォルトでディセーブルになっています。 この機能を有効にするには、CLI を使用して手動で utils auditd を有効にします。 システム監査ログ機能をイネーブルにすると、Real-Time Monitoring Tool の [Trace & Log Central] を使用して、選択したログの収集、表示、ダウンロード、削除を実行できます。 システム監査ログは `vos-audit.log` という形式になります。

この機能をイネーブルにする方法については、『*Command Line Interface Reference Guide for Cisco Unified Communications Solutions*』を参照してください。 Real-Time Monitoring Tool から収集したログを操作する方法については、『*Cisco Unified Real-Time Monitoring Tool Administration Guide*』を参照してください。

アプリケーション監査ログ

アプリケーション監査ログは、ユーザーによる、またはユーザー操作の結果発生したシステムへの設定変更をモニタし、記録します。

（注） アプリケーションの監査ログ（Linux auditd）は、CLIからのみイネーブルまたはディセーブルにすることができます。 このタイプの監査ログの設定は、Real-Time Monitoring Tool による vos-audit.log の収集以外は変更できません。

データベース監査ログ

データベース監査ログは、ログインなど、Informix データベースへのアクセスに関連するすべてのアクティビティを追跡します。

監査ログ設定タスク フロー

監査ロギングを設定するには、次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	監査ロギングのセットアップ（144 ページ）	[監査ログ設定（Audit Log Configuration）] ウィンドウで監査ログ設定をセットアップします。 リモート監査ロギングを使用するかどうかと、[詳細監査ロギング（Detailed Audit Logging）] オプションが必要かどうかを設定できます。
ステップ 2	リモート監査ログの転送プロトコルの設定 （145 ページ）	これはオプションです。 リモート監査ロギングを設定した場合は、転送プロトコルを設定します。 通常の動作モードのシステム デフォルトは UDP ですが、TCP または TLS を設定することもできます。
ステップ 3	アラート通知用の電子メールサーバーの設定 （147 ページ）	これはオプションです。 RTMT で、電子メールアラート用の電子メールサーバーをセットアップします。
ステップ 4	電子メールアラートの有効化（147 ページ）	これはオプションです。 次の電子メール アラートのいずれかをセットアップします。

	コマンドまたはアクション	目的
		• リモート監査ロギングが TCP で設定されている場合は、**TCPRemoteSyslogDeliveryFailed** アラート用の電子メール通知をセットアップします。 • リモート監査ロギングが TLS で設定されている場合は、**TLSRemoteSyslogDeliveryFailed** アラート用の電子メール通知をセットアップします。
ステップ 5	プラットフォーム ログ用のリモート監査ロギングの設定 （148 ページ）	プラットフォーム監査ログとリモート サーバ ログ用のリモート監査ロギングをセットアップします。 この種の監査ログでは、FileBeat クライアントと外部 logstash サーバーを設定する必要があります。

監査ロギングのセットアップ

始める前に

リモート監査ロギングでは、事前に、リモート syslog サーバーをセットアップし、間にあるゲートウェイへの接続も含め、各クラスタノードとリモート syslog サーバー間で IPSec を設定しておく必要があります。 IPSec 設定については、『*Cisco IOS Security Configuration Guide*』を参照してください。

手順

ステップ 1 Cisco Unified Serviceability で、**[ツール（Tools）]** > **[監査ログ設定（Audit Log Configuration）]** を選択します。

ステップ 2 **[サーバ（Server）]** ドロップダウンメニューから、クラスタ内のサーバーを選択し、**[実行（Go）]** をクリックします。

ステップ 3 すべてのクラスタ ノードを記録するには、[すべてのノードに適用（Apply to All Nodes）]チェックボックスをオンにします。

ステップ 4 **[サーバー名（Server Name）]** フィールドに、リモート syslog サーバーの IP アドレスまたは完全修飾ドメイン名を入力します。

ステップ 5 これはオプションです。 変更された項目と変更された値も含め、設定更新を記録するには、[詳細監査ロギング（Detailed Audit Logging）]チェックボックスをオンにします。

ステップ 6 [監査ログ設定（Audit Log Configuration）]ウィンドウの残りのフィールドに値を入力します。フィールドとその説明を含むヘルプについては、オンライン ヘルプを参照してください。

ステップ 7 **[保存（Save）]** をクリックします。

次のタスク

リモート監査ログの転送プロトコルの設定 （145 ページ）

リモート監査ログの転送プロトコルの設定

リモート監査ログ用の転送プロトコルを変更するには、次の手順を使用します。 システムデフォルトは UDP ですが、 に設定し直すこともできます。 TCP または TLS に設定し直すこともできます。

手順

ステップ 1 コマンドライン インターフェイスにログインします。

ステップ 2 **utils remotesyslog show protocol** コマンドを実行して、どのプロトコルが設定されているかを確認します。

ステップ 3 このノード上でプロトコルを変更する必要がある場合は、次の手順を実行します。

- TCP を設定するには、**utils remotesyslog set protocol tcp** コマンドを実行します。
- UDP を設定するには、**utils remotesyslog set protocol udp** コマンドを実行します。
- TLS を設定するには、**utils remotesyslog set protocol tls** コマンドを実行します。

（注） コモンクライテリアモードでは、厳密なホスト名検証が使用されます。そのため、証明書と一致する完全修飾ドメイン名（FQDN）でサーバーを設定する必要があります。

ステップ 4 プロトコルを変更した場合は、ノードを再起動します。

ステップ 5 すべての Unified Communications Manager と IM and Presence Service のクラスタノードでこの手順を繰り返します。

次のタスク

アラート通知用の電子メールサーバーの設定 （147 ページ）

Syslog サーバーとの TLS 接続を確立する

この手順を使用して、Unified Communications Manager と Syslog サーバーの間に自己署名または CA 署名の証明書を使用して安全な TLS 接続を設定します。 以下の認証モードがサポートされています。

- 単方向 x.509 認証 - Syslog サーバーのみが Unified CM に対して認証します。
- 双方向 x.509 認証 - Unified CM と Syslog サーバーの両方が相互に認証します。

手順

ステップ 1 自己署名証明書の場合：

a) 単方向認証の場合、自己署名証明書を使用して TLS 接続を確立するには、syslog サーバーからのセキュリティ証明書が Unified Communications Manager パブリッシャノードの tomcat トラストストアにアップロードされている必要があります。

b) 双方向 x.509 認証の場合：

1. 自己署名証明書を使用して TLS 接続を確立するには、syslog サーバーからのセキュリティ証明書が Unified Communications Manager パブリッシャノードの tomcat トラストストアにアップロードされている必要があります。
2. Cisco Unified OS Administration から、**[セキュリティ（Security）] > [証明書の管理（Certificate Management）]** に移動します。そして、Unified Communications Manager および IM and Presence Service から Tomcat 証明書をダウンロードします。
3. Tomcat 証明書を Syslog サーバーの証明書ディレクトリにアップロードします。

   （注） Tomcat 証明書が再生成された場合、syslog サーバーに再アップロードする必要があります。
4. 必要に応じて Syslog サーバーを再起動します。

ステップ 2 CA 署名証明書の場合：

a) 単方向認証の場合、認証局（CA）証明書を Unified Communications Manager パブリッシャノード上の tomcat トラストストアにアップロードします。

b) 双方向 x.509 認証の場合：

1. TLS 接続を確立するには、Unified Communications Manager パブリッシャノードの tomcat トラストストアに認証局（CA）の証明書をアップロードする必要があります。
2. Cisco Unified OS Administration から、**[セキュリティ（Security）] > [証明書の管理（Certificate Management）]** に移動します。そして、Unified Communications Manager および IM and Presence Service から Tomcat 証明書をダウンロードします。
3. この証明書が同じ CA によって署名されていることを確認してください。
4. CA 署名付き Tomcat 証明書を Unified Communications Manager パブリッシャノードの tomcat ストアにアップロードします。
5. CA 証明書を Syslog サーバーの証明書ディレクトリにアップロードします。
6. 必要に応じて Syslog サーバーを再起動します。

（注） TLS およびそれらのサポートされている形式（PEM、DER など）に関連する設定の詳細については、Syslog サーバーのドキュメントを参照してください。

アラート通知用の電子メールサーバーの設定

アラート通知用の電子メールサーバーをセットアップするには、次の手順を使用します。

手順

ステップ 1 Real-Time Monitoring Tool のシステム ウィンドウで、[アラート セントラル（Alert Central）]をクリックします。

ステップ 2 **[システム（System）]** > **[ツール（Tools）]** > **[アラート（Alert）]** > **[電子メールサーバーの設定（Config Email Server）]** の順に選択します。

ステップ 3 **[メールサーバー設定（Mail Server Configuration）]** ポップアップで、メールサーバーの詳細を入力します。

ステップ 4 **OK**をクリックします。

次のタスク

電子メール アラートの有効化 （147 ページ）

電子メール アラートの有効化

リモート監査ロギングを TCP または TLS で設定した場合は、次の手順を使用して、送信障害を通知する電子メール アラートを設定します。

手順

ステップ 1 Real-Time Monitoring Tool の **[システム（System）]** 領域で、**[アラート セントラル（Alert Central）]** をクリックします。

ステップ 2 **[アラートセントラル（Alert Central）]** ウィンドウで、します

- TCP でリモート監査ロギングを使用する場合は、**TCPRemoteSyslogDeliveryFailed** を選択します。
- TLS でリモート監査ロギングを使用する場合は、**TLSRemoteSyslogDeliveryFailed** を選択します。

ステップ 3 **[システム（System）]** > **[ツール（Tools）]** > **[アラート（Alert）]** > **[アラート アクションの設定（Config Alert Action）]** の順に選択します。

ステップ 4 [アラート アクション（Alert Action）]ポップアップで、[デフォルト（Default）]を選択して、[編集（Edit）]をクリックします。

ステップ 5 [アラート アクション（Alert Action）]ポップアップで、受信者を追加します。

ステップ 6 ポップアップ ウィンドウで、電子メール アラートを送信するアドレスを入力して、[OK]をクリックします。

ステップ 7 [アラート アクション（Alert Action）]ポップアップで、アドレスが[受信者（Recipients）]に表示されていることと、[有効（Enable）]チェックボックスがオンになっていることを確認します。

ステップ 8 **OK**をクリックします。

プラットフォーム ログ用のリモート監査ロギングの設定

プラットフォーム監査ログ、リモート サポート ログ、および一括管理 CSV ファイルに対するリモート監査ロギング サポートを追加するには、次のタスクを実行します。 この種のログでは、FileBeat クライアントと logstash サーバーが使用されます。

始める前に

外部 logstash サーバーがセットアップされていることを確認します。

手順

	コマンドまたはアクション	目的
ステップ 1	Logstash サーバ情報の設定 （148 ページ）	IP アドレス、ポート、ファイル タイプなどの外部 logstash サーバ詳細で FileBeat クライアントを設定します。
ステップ 2	FileBeat クライアントの設定 （149 ページ）	リモート監査ロギング用の FileBeat クライアントを有効にします。

Logstash サーバ情報の設定

次の手順を使用して、IP アドレス、ポート番号、ダウンロード可能なファイル タイプなどの外部 Logstash サーバ情報で FileBeat クライアントを設定します。

始める前に

外部 Logstash サーバーがセットアップされていることを確認します。

手順

ステップ 1 コマンドライン インターフェイスにログインします。

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

ステップ 3 画面上の指示に従って、Logstash サーバーの詳細を設定します。

FileBeat クライアントの設定

プラットフォーム監査ログ、リモート サポート ログ、および一括管理 CSV ファイルのアップロード用の FileBeat クライアントを有効または無効にするには、次の手順を使用します。

手順

ステップ 1 コマンドライン インターフェイスにログインします。

ステップ 2 **utils FileBeat status** コマンドを実行し、Filebeat クライアントが有効になっているかどうかを確認します。

ステップ 3 次のコマンドの 1 つを実行します。

- クライアントを有効にするには、**utils FileBeat enable** コマンドを実行します。
- クライアントを無効にするには、**utils FileBeat disable** コマンドを実行します。

（注） TCP はデフォルトの転送プロトコルです。

ステップ 4 これはオプションです。転送プロトコルとして TLS を使用するには、次の手順を実行します。

- 転送プロトコルとして TLS を有効にするには、**utils FileBeat tls enable** コマンドを実行します。
- 転送プロトコルとして TLS を無効にするには、**utils FileBeat tls disable** コマンドを実行します。

（注） TLS を使用するには、セキュリティ証明書を logstash サーバから Unified Communications Manager と IM and Presence Service 上の tomcat 信頼ストアにアップロードする必要があります。

ステップ 5 各ノードでこの手順を繰り返します。

これらのコマンドをすべてのノードで同時に実行しないでください。

監査ログの構成時の設定

事前準備

監査ロールを割り当てられたユーザだけが監査ログの設定を変更できることに注意してください。デフォルトでは、Unified Communications Manager の新規インストールおよびアップグレード後、CCMAdministrator が監査ロールを所有します。 CCMAdministrator は、Cisco Unified Communications Manager の管理 の [User Group Configuration] ウィンドウで標準監査ユーザーグループに監査権限を持つユーザーを割り当てることができます。その後必要であれば、標準監査ユーザ グループから CCMAdministrator を削除できます。

IM and Presence Serviceの場合、新規インストールまたはアップグレードの後で管理者に監査ロールが与えられ、監査権限を持つ任意のユーザーを標準監査ユーザーグループに割り当てることができます。

Cisco Unity Connection の場合、インストール時に作成されたアプリケーション管理アカウントが Audit Administrator ロールに割り当てられます。このアカウントは、他の管理者ユーザーをこのロールに割り当てることができます。 このアカウントから Audit Administrator ロールを削除することもできます。

Standard Audit Log Configuration ロールには、監査ログを削除する権限と、Cisco Unified Real-Time Monitoring Tool、IM and Presence Real-Time Monitoring Tool、Trace Collection Tool、Real-Time Monitoring Tool（RTMT）アラート設定、Serviceability ユーザ インターフェイスのコントロール センター - ネットワーク サービス、RTMT プロファイルの保存、Serviceability ユーザ インターフェイスの監査設定、監査トレースというリソースへの読み取り/更新権限が与えられます。

Standard Audit Log Configuration ロールには、監査ログを削除する権限と、Cisco Unified RTMT、Trace Collection Tool、RTMT アラート設定、Cisco Unified Serviceability のコントロール センター - ネットワーク サービス、RTMT プロファイルの保存、Cisco Unified Serviceability の監査設定、監査トレースというリソースへの読み取り/更新権限が与えられます。

Cisco Unity Connection の Audit Administrator ロールに割り当てられたユーザーは、Cisco Unified RTMT で監査ログを表示、ダウンロード、および削除できます。

Cisco Unified Communications Manager のロール、ユーザ、およびユーザ グループの詳細については、*Cisco Unified Communications Manager* 管理ガイドを参照してください。

Cisco Unity Connection のロールとユーザーの詳細については、『*User Moves, Adds, and Changes Guide for Cisco Unity Connection*』を参照してください。

IM and Presenceのロール、ユーザ、ユーザ グループの詳細は、*Unified Communications Manager* の *Configuration and Administration of IM and Presence Service* の設定および管理を参照してください。

次の表に、Cisco Unified Serviceability の [監査ログの設定（Audit Log Configuration）] ウィンドウで設定できる設定について説明します。

表 *13*：監査ログの構成時の設定

フィールド	説明
サーバーの選択	
サーバ（Server）	監査ログを設定するサーバ（ノード）を選択し、[移動（Go）]をクリックします。
すべてのノードに適用（Apply to All Nodes）	クラスタのすべてのノードに監査ログ設定を適用する場合は、[すべてのノードに適用（Apply to All Nodes）]チェックボックスをオンにします。
アプリケーション監査ログの設定	

フィールド	説明
監査ログを有効にする（Enable Audit Log）	このチェックボックスをオンにすると、監査ログがアプリケーション監査ログに対して作成されます。 Unified Communications Managerの場合、アプリケーション監査ログは、Cisco Unified Communications Manager 管理、Cisco Unified RTMT、Cisco Unified Communications Manager CDR Analysis and Reporting および Cisco Unified Serviceabilityなどの Unified Communications Manager ユーザ インターフェイスの設定の更新をサポートします。 IM and Presence Service の場合、アプリケーション監査ログは Cisco Unified Communications Manager IM and Presence 管理、Cisco Unified IM and Presence Real-Time Monitoring Tool、Cisco Unified IM and Presence Serviceability などの IM and Presence ユーザーインターフェイスの設定更新をサポートします。 Cisco Unity Connection の場合、アプリケーション監査ログは Cisco Unity Connection Administration、Cisco Unity Connection Serviceability、Cisco Personal Communications Assistant、接続 REST API を使用するクライアントなどの Cisco Unity Connection ユーザーインターフェイスの設定更新をサポートします。 この設定は、デフォルトで有効と表示されます。 （注） ネットワーク サービス Audit Event Service が動作している必要があります。
消去を有効にする（Enable Purging）	Log Partition Monitor（LPM）は、[消去を有効にする（Enable Purging）] オプションを確認して監査ログを消去する必要があるかどうかを判断します。 このチェックボックスをオンにすると、共通パーティションのディスク使用率が上限を超えるたびに LPM によって RTMT のすべての監査ログファイルが消去されます。ただし、このチェックボックスをオフにして消去を無効にすることができます。 消去が無効の場合、監査ログの数は、ディスクがいっぱいになるまで増加し続けます。 このアクションは、システムの中断を引き起こす可能性があります。 [消去を有効にする（Enable Purging）] チェックボックスをオフにすると、消去の無効化のリスクを説明するメッセージが表示されます。 このオプションは、アクティブ パーティションの監査ログに使用可能なことに注意してください。監査ログが非アクティブパーティションにある場合、ディスク使用率が上限を上回ると消去されます。 監査ログにアクセスするには、RTMT の **[Trace & Log Central]** > **[監査ログ（Audit Logs）]** を選択します。 （注） ネットワーク サービス Cisco Log Partition Monitoring Tool が動作している必要があります。

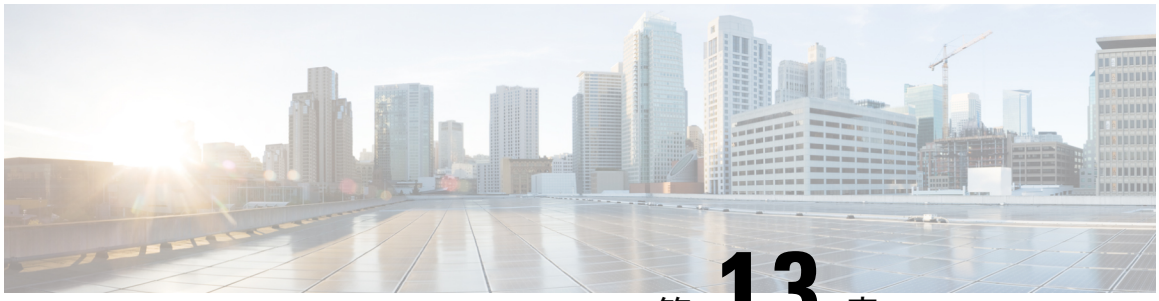
フィールド	説明
ログ ローテーションを有効にする（Enable Log Rotation）	システムは、このオプションを読み取り、監査ログ ファイルをローテーションする必要があるか、または新しいファイルの作成を続行するかを判断します。 ファイルの最大数は 5000 を超えることはできません。[ログローテーションを有効にする（Enable Log Rotation）] チェックボックスをオンにすると、監査ログファイルの最大数に達すると最も古いファイルが上書きされます。 **ヒント** ログ ローテーションを無効（オフ）にすると、監査ログは [最大ファイル数（Maximum No. of Files）] 設定を無視します。
詳細監査ロギング（Detailed Audit Logging）	このチェックボックスをオンにすると、システムは詳細監査ログに対して有効にされます。 詳細監査ログは、標準監査ログと同じ項目を提供しますが、設定の変更も含まれています。 たとえば、監査ログには、変更された値も含め、追加、更新、または削除された項目が保存されます。
サーバ名（Server Name）	Syslog メッセージ受信のために使用する、リモート Syslog サーバーの名前または IP アドレスを入力します。 サーバ名が指定されていない場合、Cisco Unified IM and Presence Serviceability は Syslog メッセージを送信しません。 ノードは他のサーバからの Syslog メッセージを受け付けないため、Unified Communications Manager ノードを通知先として指定しないでください。 これは、IM and Presence Service にのみ適用されます。
リモート Syslog 監査イベントレベル（Remote Syslog Audit Event Level）	リモート Syslog サーバーの、対象となる Syslog メッセージの重大度を選択します。 選択した重大度以上のすべての Syslog メッセージが、リモート Syslog に送信されます。 これは、IM and Presence Service にのみ適用されます。
最大ファイル数（Maximum No. of Files）	ログに含めるファイルの最大数を入力します。 デフォルト設定は 250 です。最大数は 5000 です。
最大ファイル サイズ（Maximum File Size）	監査ログの最大ファイル サイズを入力します。 ファイル サイズの値は 1 MB〜10 MBの範囲内にする必要があります。 1 ～ 10 の間の数を指定します。

フィールド	説明
ログ ローテーション オーバーライドに到達する際の警告しきい値（%）（Warning Threshold for Approaching Log Rotation Overwrite (%)）	監査ログが上書きされるレベルに達すると、警告が送信されます。警告を送信するしきい値を設定するには、このフィールドを使用します。 たとえば、2 MB のファイルが 250 個あり、警告しきい値を 80% にデフォルト設定とすると、監査ログが 200 個（80%）収集されると、警告が送信されます。監査履歴を保持する場合は、システムがログを上書きする前に、RTMT を使用してログを取得します。 RTMT には、ファイルの収集後にそのファイルを削除するオプションがあります。 1 ～ 99% の範囲で値を入力します。デフォルトは 80% です。 このフィールドを設定する場合は、[ログ ローテーションを有効にする（Enable Log Rotation）]オプションもオンにする必要があります。 （注） 監査ログに割り当てられたディスク容量合計は、最大ファイル数を最大ファイル サイズで乗算したものです。 ディスク上の監査ログのサイズが割り当てられたディスク容量合計のこの割合を超える場合は、Alert Central に警告が表示されます。
データベース監査ログ フィルタ設定	
監査ログを有効にする（Enable Audit Log）	このチェック ボックスをオンにすると、監査ログが Unified Communications Manager および Cisco Unity Connection データベースに作成されます。 [デバッグ監査レベル（Debug Audit Level）] の設定とともにこの設定を使用します。これにより、データベースの特定の側面に対してログを作成できます。

フィールド	説明
デバッグ監査レベル（Debug Audit Level）	この設定では、ログで監査するデータベースの側面を選択できます。 ドロップダウン リスト ボックスから、次のオプションのいずれかを選択します。 各監査ログ フィルタ レベルは累積的であることに注意してください。 • [スキーマ（Schema）]：監査ログデータベースの設定の変更（たとえば、データベース テーブルのカラムや行）を追跡します。 • **管理タスク**：Unified Communications Managerシステムに対するすべての管理上の変更（たとえば、システム保全のためのあらゆる変更など）およびすべての**スキーマ**を追跡します。 **ヒント** ほとんどの管理者は [管理タスク（Administrative Tasks）] 設定を無効にしたままにします。 監査が必要なユーザーに対しては、[データベースの更新（Database Updates）] レベルを使用します。 • [データベースの更新（Database Updates）]：データベースのすべての変更、および[スキーマ（Schema）]のすべての変更と [管理タスク（Administrative Tasks）]のすべての変更を追跡します。 • **データベースの読み取り**：システムへのすべての読み取りと、すべてのスキーマ変更、管理タスク変更、データベース更新のすべての変更を追跡します。 **ヒント** Unified Communications Manager または Cisco Unity Connection システムを簡単に確認する場合にのみ、データベースの読み取りレベルを選択します。 このレベルでは、大量のシステム リソースを消費するため、短時間だけ使用してください。
監査ログローテーションを有効にする（Enable Audit Log Rotation）	システムはこのオプションを読み取り、データベースの監査ログ ファイルをローテーションする必要があるか、または新しいファイルの作成を続行するかどうかを判断します。 [監査ログローテーションを有効にする（Enable Audit Log Rotation）] オプションのチェックボックスをオンにすると、監査ログ ファイルが最大数に達すると最も古いファイルが上書きされます。 この設定のチェックボックスがオフの場合、監査ログでは [最大ファイル数（Maximum No. of Files）] 設定は無視されます。
最大ファイル数（Maximum No. of Files）	ログに含めるファイルの最大数を入力します。 [最大ファイル数（Maximum No. of Files）] 設定に入力した値が、[ログローテーション時に削除されるファイル数（No. of Files Deleted on Log Rotation）] 設定に入力した値を上回っていることを確認します。 4（最小）～ 40（最大）の値を入力できます。

フィールド	説明
ログローテーション時に削除されるファイル数（No. of Files Deleted on Log Rotation）	データベース監査ログのローテーションが発生したときにシステムが削除できるファイルの最大数を入力します。 このフィールドに入力できる最小値は 1 です。最大値は [最大ファイル数（Max No. of Files）] 設定に入力した値よりも 2 低い数値です。たとえば、[最大ファイル数（Max No. of Files）] フィールドに 40 を入力した場合、[ログローテーション時に削除されるファイル数（No. of Files Deleted on Log Rotation）] フィールドに入力できる最大数は 38 です。
デフォルトに設定（Set to Default）	[デフォルトに設定（Set to Default）]ボタンは、デフォルト値を指定します。監査ログは、詳細なトラブルシューティング用の別のレベルに設定する必要がなければ、デフォルト モードに設定することをお勧めします。 [デフォルトに設定（Set to Default）]オプションは、ログ ファイルに使用されるディスク容量を最小限に抑えます。

注意 有効になっている場合、特にデバッグ監査レベルが [データベースの更新（Database Updates）] または [データベースの読み取り（Database Reads）]に設定されていると、データベース ロギングが短時間で大量のデータを生成する可能性があります。 これにより、多用期間中に、パフォーマンスに重大な影響が発生する可能性があります。 通常、データベース ロギングは無効のままにすることを推奨します。データベースの変更を追跡するためにロギングを有効にする必要がある場合には、[データベースの更新（Database Updates）]レベルを使用して短時間のみ有効にすることを推奨します。 同様に、特にデータベース エントリをポーリングする場合（データベースから 250 台のデバイスを引き出す場合など）、管理ロギングは Web ユーザ インターフェイスの全体的なパフォーマンスに影響を与えます。



第 13 章

Call Home

Call Home

この章では、Unified Communications Manager Call Home サービスの概要と Unified Communications Manager Call Home 機能を設定する方法について説明します。 Call Home 機能を使用すると、Smart Call Home バックエンドサーバーと通信し、診断アラート、インベントリなどのメッセージを送信できます。

Smart Call Home

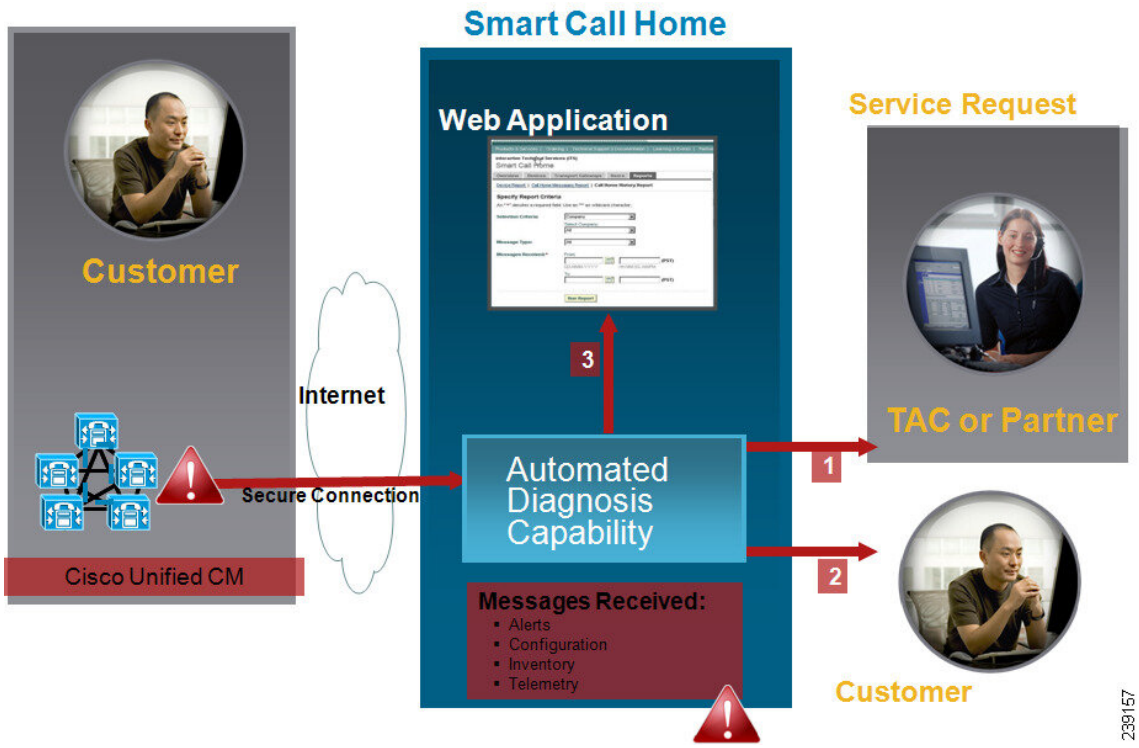
Smart Call Home は、さまざまなシスコデバイスを対象として予防的診断、リアルタイム アラート、および修復を実行し、ネットワークの可用性と運用効率を向上させます。 Smart Call Home が有効化された Unified Communications Manager から診断アラート、インベントリ、その他のメッセージを受け取り、分析することでも、同様の結果が得られます。 Unified Communications Manager のこの機能は、Unified Communications Manager Call Home と呼ばれます。

Smart Call Home の機能は次のとおりです。

- 次の機能によって予防的で迅速な問題解決を行い、ネットワークの可用性を向上させます。
  - 継続的モニタリング、リアルタイムの予防的なアラート、および詳細な診断により、問題を迅速に識別できるようにします。
  - ネットワーク内のデバイスのタイプに特有のアラートを発生させ、潜在的な問題を認識できるようにします。 Cisco Technical Assistance Center（TAC）のエキスパートに直接かつ自動的にアクセスして、重大な問題を迅速に解決します。
- ユーザーに次の機能を提供して、運用効率を向上させます。
  - トラブルシューティングに必要な時間を短縮することにより、スタッフリソースを効率よく活用できます。

- 必要な情報に迅速に Web ベースでアクセスでき、ユーザーが次のことを実行できるようにします。
  - すべての Call Home メッセージ、診断、および推奨事項を一箇所で確認できます。
  - サービス リクエスト ステータスを迅速に確認できます。
  - すべての Call Home デバイスに関する最新のインベントリおよび設定情報を参照できます。

図 *2 : Cisco Smart Call Home* の概要



Smart Call Home には、次のタスクを実行するモジュールが含まれています。

- ユーザーへの Call Home メッセージの通知。
- 影響分析と修正手順の提供。

Smart Call Home の詳細については、次の URL の Smart Call Home のページを参照してください。

http://www.cisco.com/en/US/products/ps7334/serv_home.html

Smart Call Home 証明書の更新に関する情報

Cisco リリース 10.5(2) 以降では、Smart Call Home 機能のサポートを継続するには、更新リクエストの都度、管理者が新しい証明書を手動でアップロードすることになります。 証明書のアップロードは、Cisco Unified Operating System（OS）管理 Web GUI を使用して行うことができま

す。 **セキュリティ > 証明書管理 > 証明書または証明書チェーンのアップロード**を開きます。証明書として **tomcat-trust** を選択して、保存した接続先から証明書をアップロードします。

以下の「 .PEM 」拡張子の証明書を tomcat-trust にアップロードする必要があります。

（注） 管理者は、文字列全体をコピーして、「-----BEGIN CERTIFICATE----- and -----END CERTIFICATE-----」を含めてテキストファイルにペーストして、「.PEM」の拡張子で保存します。

-----BEGIN CERTIFICATE-----
MIIFtzCCA5+gAwIBAgICBQkwDQYJKoZIhvcNAQEFBQAwRTELMAkGA1UEBhMCQk0x
GTAXBgNVBAoTEFF1b1ZhZGlzIExpbWl0ZWQxGzAZBgNVBAMTElF1b1ZhZGlzIFJv
b3QgQ0EgMjAeFw0wNjExMjQxODI3MDBaFw0zMTExMjQxODIzMzNaMEUxCzAJBgNV
BAYTAkJNMRkwFwYDVQQKExBRdW9WYWRpcyBMaW1pdGVkMRswGQYDVQQDExJRdW9
WYWRpcyBSb290IENBIDIwggIiMA0GCSqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQCa
GMpLlA0ALa8DKYrwD4HIrkwZhR0In6spRIXzL4GtMh6QRr+jhiYaHv5+HBg6XJxg
Fyo6dIMzMH1hVBHL7avg5tKifvVrbxi3Cgst/ek+7wrGsxDp3MJGF/hd/aTa/55J
WpzmM+Yklvc/ulsrHHo1wtZn/qtmUIttKGAr79dgw8eTvI02kfN/+NsRE8Scd3bB
rrcCaoF6qUWD4gXmuVbBlDePSHFjIuwXZQeVikvfj8ZaCuWw419eaxGrDPmF60Tp
+ARz8un+XJiM9XOva7R+zdRcAitMOeGylZUtQofX1bOQQ7dsE/He3fbE+Ik/0XX1
ksOR1YqI0JDs3G3eicJlcZaLDQP9nL9bFqyS2+r+eXyt66/3FsvbzSUr5R/7mp/i
Ucw6UwxI5g69ybR2BlLmEROFcmMDBOAENisgGQLodKcftslWZvB1JdxnwQ5hYIiz
PtGo/KPaHbDRsSNU30R2be1B2MGyIrZTHN81Hdyhdyox5C315eXbyOD/5YDXC2Og
/zOhD7osFRXql7PSorW+8oyWHhqPHWykYTe5hnMz15eWniN9gqRMgeKh0bpnX5UH
oycR7hYQe7xFSkyyBNKr79X9DFHOUGoIMfmR2gyPZFwDwzqLID9ujWc9Otb+fVuI
yV77zGHcizN300QyNQliBJIWENieJ0f7OyHj+OsdWwIDAQABo4GwMIGtMA8GA1Ud
EwEB/wQFMAMBAf8wCwYDVR0PBAQDAgEGMB0GA1UdDgQWBBQahGK8SEwzJQTU7tD2
A8QZRtGUazBuBgNVHSMEZzBlgBQahGK8SEwzJQTU7tD2A8QZRtGUa6FJpEcwRTEL
MAkGA1UEBhMCQk0xGTAXBgNVBAoTEFF1b1ZhZGlzIExpbWl0ZWQxGzAZBgNVBAMT
ElF1b1ZhZGlzIFJvb3QgQ0EgMoICBQkwDQYJKoZIhvcNAQEFBQADggIBAD4KFk2f
BluornFdLwUvZ+YTRYPENvbzwCYMDbVHZF34tHLJRqUDGCdViXh9duqWNIAXINzn
g/iN/Ae42l9NLmeyhP3ZRPx3UIHmfLTJDQtyU/h2BwdBR5YM++CCJpNVjP4iH2Bl
fF/nJrP3MpCYUNQ3cVX2kiF495V5+vgtJodmVjB3pjd4M1IQWK4/YY7yarHvGH5K
WWPKjaJW1acvvFYfzznB4vsKqBUsfU16Y8Zsl0Q80m/DShcK+JDSV6IZUaUtl0Ha
B0+pUNqQjZRG4T7wlP0QADj1O+hA4bRuVhogzG9Yje0uRY/W6ZM/57Es3zrWIozc
hLsib9D45MY56QSIPMO661V6bYCZJPVsAfv4l7CUW+v90m/xd2gNNWQjrLhVoQPR

TUIZ3Ph1WVaj+ahJefivDrkRoHy3au000LYmYjgahwz46P0u05B/B5EqHdZ+XIWD
mbA4CD/pXvk1B+TJYm5Xf6dQlfe6yJvmjqIBxdZmv3lh8zwc4bmCXF2gw+nYSL0Z
ohEUGW6yhhtoPkg3Goi3XZZenMfvJ2II4pEZXNLxId26F0KCl3GBUzGpn/Z9Yr9y
4aOTHcyKJloJONDO1w2AFrR4pTqHTI2KpdVGl/IsELm8VCLAAVBpQ570su9t+Oza
8eOx79+Rj1QqCyXBJhnEUhAFZdWCEOrCMc0u
-----END CERTIFICATE-----

匿名 Call Home

匿名 Call Home 機能は、Cisco が匿名でインベントリおよびテレメトリ メッセージを受けられるようにする、Smart Call Home 機能のサブ機能です。 ID の匿名性を保つには、この機能を有効にします。

匿名 Call Home の特徴は、次のとおりです。

- Unified Communications Manager は Smart Call Home バックエンドにインベントリおよびテレメトリ メッセージのみを送信し、診断および設定情報は送信しません。
- また、ユーザーに関する情報を送信しません（登録デバイスやアップグレード履歴など）。
- 匿名 Call Home オプションは、Cisco の Smart Call Home 機能への登録または権限付与を必要としません。
- インベントリおよびテレメトリ メッセージは Call Home バックエンドに定期的に送信されます（各月の最初の日）。
- Cisco Unified Communications Manager が匿名 Call Home を使用するように設定されている場合、**トレースログと診断情報を含める** オプションは無効になります。

インベントリ メッセージには、クラスタ、ノード、ライセンスに関する情報が含まれます。

次の表に、Smart Call Home と匿名 Call Home のインベントリ メッセージを示します。

表 *14 : Smart Call Home* と匿名 *Call Home* のインベントリ メッセージ

インベントリ メッセージ	Smart Call Home	匿名 Call Home
連絡先の電子メール（Contact Email）	適用可能	該当なし
連絡先電話番号（Contact Phone Number）	適用可能	該当なし
住所（Street Address）	適用可能	該当なし
サーバ名（Server Name）	適用可能	該当なし
サーバーの IP アドレス（Server IP Address）	適用可能	該当なし

インベントリ メッセージ	Smart Call Home	匿名 Call Home
ライセンス サーバ（Licence Server）	適用可能	該当なし
OS バージョン（OS Version）	適用可能	適用可能
モデル（Model）	適用可能	適用可能
シリアル番号（Serial Number）	適用可能	適用可能
CPU 速度（CPU Speed）	適用可能	適用可能
RAM	適用可能	適用可能
ストレージのパーティション（Storage Partition）	適用可能	適用可能
ファームウェアのバージョン（Firmware version）	適用可能	適用可能
BIOS のバージョン（BIOS Version）	適用可能	適用可能
BIOS 情報（BIOS Information）	適用可能	適用可能
RAID 設定（Raid Configuration）	適用可能	適用可能
アクティブ サービス（Active Services）	適用可能	適用可能
パブリッシャ名（Publisher Name）	適用可能	該当なし
パブリッシャ IP（Publisher IP）	適用可能	該当なし
製品 ID（Product IDl）	適用可能	適用可能
アクティブなバージョン（Active Version）	適用可能	適用可能
アクティブでないバージョン（Inactive Version）	適用可能	適用可能
製品の略称（Product Short name）	適用可能	適用可能

テレメトリ メッセージには、Unified Communications Manager クラスタで使用できる各デバイス タイプのデバイス数（IP 電話、ゲートウェイ、会議ブリッジなど）に関する情報が含まれます。 テレメトリ データには、クラスタ全体のデバイスの数が含まれます。

次の表に、Smart Call Home と匿名 Call Home のテレメトリ メッセージを示します。

表 *15 : Smart Call Home* と匿名 *Call Home* のテレメトリ メッセージ

テレメトリ メッセージ	Smart Call Home	匿名 Call Home
連絡先の電子メール（Contact Email）	適用可能	該当なし
連絡先電話番号（Contact Phone Number）	適用可能	該当なし
住所（Street Address）	適用可能	該当なし
サーバ名（Server name）	適用可能	該当なし
CM ユーザ数（CM User Count）	適用可能	該当なし
シリアル番号（Serial Number）	適用可能	適用可能
パブリッシャ名（Publisher name）	適用可能	該当なし
デバイス数およびモデル（Device count and Model）	適用可能	適用可能
電話ユーザーの数（Phone User Count）	適用可能	適用可能
CM のコール アクティビティ（CM Call Activity）	適用可能	適用可能
登録されたデバイスの数（Registered Device count）	適用可能	該当なし
アップグレードの履歴（Upgrade history）	適用可能	該当なし
システム ステータス（System Status）	ホスト名、日付、ロケール、製品バージョン、OS のバージョン、ライセンス MAC、アップ タイム、MPの状態、使用メモリ、ディスク使用率、使用アクティブおよび非アクティブ パーティション、DNS に適用可能	日付、ロケール、製品バージョン、OS のバージョン、ライセンス MAC、アップ タイム、使用メモリ、ディスク使用率、使用アクティブおよび非アクティブ パーティションに適用可能

設定メッセージには、設定に関連する各データベーステーブルの行数に関する情報が含まれます。 この設定データはクラスタ全体の各テーブルのテーブル名と行数で構成されます。

Smart Call Home による処理

Cisco Systems と直接サービス契約を結んでいる場合は、Cisco Smart Call Home サービスに Unified Communications Manager を登録することができます。 Smart Call Home は、Unified Communications Manager から送信された Call Home メッセージを分析し、背景情報および推奨事項を提供して、システムの問題を迅速に解決します。

Cisco Unified CM Call Home 機能は、Smart Call Home バックエンドサーバーに次のメッセージを送信します。

- アラート：環境、ハードウェア障害、システムパフォーマンスに関連するさまざまな状況のアラート情報が含まれています。 アラートは、Unified Communications Manager クラスタ内の任意のノードから生成される場合があります。 アラートの詳細には、アラートのタイプに応じて、トラブルシューティングに必要なノードなどの情報が含まれています。 Smart Call Home バックエンドサーバーに送信されるアラートについては、Smart Call Home による処理に関するトピックを参照してください。

Smart Call Home のアラートは、次のとおりです。

デフォルトでは、Smart Call Home は 24 時間に 1 回アラートを処理します。 混在クラスタ（Unified Communication Manager および Cisco Unified Presence）で 24 時間以内に同じアラートが繰り返し発生した場合は、Smart Call Home は処理を行いません。

重要 収集された情報は、48 年後にプライマリ AMC サーバから削除されます。 デフォルトでは、Unified Communications Manager パブリッシャがプライマリ AMC サーバーとなります。

- **パフォーマンスに関連するアラート**
  - CallProcessingNodeCPUPegging
  - CodeYellow
  - CPUPegging
  - LowActivePartitionAvailableDiskSpace
  - LowAvailableVirtualMemory
  - LowSwapPartitionAvailableDiskSpace
- **データベースに関連するアラート**
  - DBReplicationFailure
- **失敗したコールに関連するアラート**
  - MediaListExhausted
  - RouteListExhausted
- **クラッシュに関連するアラート**

- Coredumpfilefound
- CriticalServiceDown

設定、インベントリ、テレメトリ メッセージはCall Homeバックエンドに定期的に送信されます（各月の最初の日）。 これらのメッセージの情報を活用することで、TAC はお客様がネットワークを維持管理する上で役立つサービスをタイムリーかつ予防的に提供します。

Call Home の前提条件

Unified Communications Manager Call Home サービスをサポートするには、以下が必要となります。

- 対応する Unified Communications Manager サービス契約に関連付けられた Cisco.com ユーザー ID。
- ドメインネームシステム（DNS）と Simple Mail Transfer Protocol（SMTP）の両サーバーを Unified Communications Manager Call Home 機能用に設定することを推奨します。
  - DNS 設定は、セキュア Web（HTTPS）を使用して Call Home メッセージを送信するために必要です。
  - SMTP 設定は、Call Home メッセージを Cisco TAC に送信したり、電子メールを介して受信者のリストにメッセージのコピーを送信するために必要です。

Call Home へのアクセス

Unified CM Call Home にアクセスするには、Cisco Unified Serviceability 管理を開き、**CallHome**（**Cisco Unified Serviceability** > **CallHome** > **Call Home の設定**）を選択します。

Call Home の設定

以下の表は、Unified Communications Manager Call Home のデフォルト設定の一覧です。

表 *16 : Call Home* のデフォルト設定

パラメータ	デフォルト
Call Home	[有効（Enabled）]
次を使用して Cisco Technical Assistance Center（TAC）にデータを送信（Send Data to Cisco Technical Assistance Center（TAC）using）	セキュア Web（HTTPS）

デフォルト Smart Call Home 設定がインストール中に変更された場合、同じ設定が Call Home のユーザ インターフェイスに反映されます。

（注） 転送方式に [電子メール（Email）]を選択し、[セキュア Web（HTTPS）（Secure Web（HTTPS））]オプションでSMTP設定が必要でない場合、SMTP設定を行う必要があります。

Call Home の設定

Cisco Unified Serviceability で、**[Call Home]** > **[Call Home の設定（Call Home Configuration）]** を選択します。

[Call Homeの設定（Call Home Configuration）] ウィンドウが表示されます。

（注） Unified Communications Manager のインストール時に Cisco Smart Call Home を設定することもできます。

Smart Call Home 機能は、インストール時に Smart Call Home オプションを設定すると有効になります。 **なし** を選択すると、通知メッセージは Cisco Unified Communications Manager 管理 にログインする際に表示されます。 Smart Call Home を設定するか、Cisco Unified Serviceability を使用してリマインダを無効にする手順が表示されます。

次の表では、Cisco Unified Communications Manager Call Home の設定について説明しています。

表 *17 : Unified Communications Manager Call Home*の設定の構成

フィールド名	説明
Call Homeメッセージスケジュール（Call Home Message Schedule）	最後に送信された Call Home メッセージと、スケジュール設定されている次のメッセージの日付と時刻を表示します。

フィールド名	説明
Call Home*	ドロップダウン リストから、次のいずれかのオプションを選択します。 • **なし**： Call Home を有効または無効にする場合は、このオプションを選択します。 `Smart Call Home` が設定されていません、という再通知が表示されます。 `Smart Call Home` の設定、あるいは 再通知を無効にするには、`[Cisco Unified Serviceability > Call Home]` を開くか、管理者ページで、ここ をクリックします。 • **無効**： Call Home を無効にする場合に、このオプションを選択します。 • **有効（Smart Call Home）**：インストール中に Smart Call Home を選択した場合は、このオプションが有効となります。 このオプションを選択すると、[カスタマーの連絡先詳細（Customer Contact Details）]の下のすべてのフィールドが有効になります。 同じ設定で、[送信データ（Send Data）]のオプションも有効になります。 • **有効（匿名 Call Home）**：匿名モードで Call Home を使用する場合には、このオプションを選択します。 このオプションを選択すると、[カスタマーの連絡先詳細（Customer Contact Details）]の下のすべてのフィールドが無効になります。 同じ設定で、[送信データ（Send Data）]の [次の電子メールアドレスにコピーを送信します(複数のアドレスはカンマで区切ります)（Send a copy to the following email addresses (separate multiple addresses with comma)）] フィールドが有効になり、[Call Home] ページで [トレースログと診断情報を含める（Include Trace logs and Diagnostics Information）] が無効になります。 （注） 匿名 Call Home を有効にすると、サーバからシスコに使用状況の統計情報を送信します。 この情報は、シスコが製品のユーザエクスペリエンスを理解し、製品の方向性を推進するために役立ちます。
カスタマーの連絡先詳細	
電子メール アドレス（Email Address）*	顧客の連絡先の電子メールアドレスを入力します。 これは必須フィールドです。
会社（Company）	（任意）会社名を入力します。 入力できるのは最大 255 文字です。

フィールド名	説明
連絡先名（Contact Name）	（任意）顧客の担当者名を入力します。 入力できるのは最大128 文字です。 担当者には、英数字とドット（.）、下線（_）、ハイフン（-）などの一部の特殊文字を使用できます。
アドレス（Address）	（任意）顧客の住所を入力します。 入力できるのは最大1024文字です。
電話（Phone）	（任意）顧客の電話番号を入力します。
送信データ	
次を使用して Cisco Technical Assistance Center（TAC）にデータを送信（Send Data to Cisco Technical Assistance Center（TAC）using）	これは必須フィールドです。 ドロップダウンリストから、次のいずれかのオプションを選択して Call Home メッセージを Cisco TAC に送信します。 • **セキュア Web（HTTPS）**：セキュア Web を使用して Cisco TAC にデータを送信する場合は、このオプションを選択します。 • **電子メール**：電子メールを使用して Cisco TAC にデータを送信する場合は、このオプションを選択します。 電子メールの場合は、SMTP サーバーを設定する必要があります。 設定された SMTP サーバーのホスト名または IP アドレスを表示することができます。 （注） SMTP サーバーを設定していない場合は、警告メッセージが表示されます。 • [プロキシ経由のセキュアWeb (HTTPS)（Secure Web (HTTPS) through Proxy）]：プロキシ経由でCisco TAC にデータを送信する場合には、このオプションを選択します。 現在、プロキシレベルでの認証はサポートしていません。 次のフィールドがこのオプションの設定時に表示されます。 • **HTTPS プロキシ IP または ホスト名***: プロキシの IP あるいはホスト名を入力します。 • [HTTPSプロキシポート（HTTPS Proxy Port）]*：通信のためのプロキシポート番号を入力します。
次の電子メール アドレスにコピーを送信します(複数のアドレスはカンマで区切ります)（Send a copy to the following email addresses (separate multiple addresses with comma)）	指定した電子メールアドレスにCall Home メッセージのコピーを送信するには、このチェックボックスをオンにします。 最大 1024 文字まで入力できます。

フィールド名	説明
トレースログと診断情報を含める（Include Trace logs and Diagnostics Information）	Cisco Unified CM のログおよび診断情報の収集を有効にするには、このチェック ボックスをオンにします。 （注） このオプションは、Smart Call Home を有効にした場合にのみアクティブになります。 メッセージには、アラート時に収集された診断情報とトレース メッセージが含まれます。 トレースのサイズが 3 MB 未満の場合は、トレースがエンコードされてアラート メッセージの一部として送信され、トレースが 3 MB を超える場合には、トレースの場所のパスがアラート メッセージに表示されます。
保存（Save）	Call Home 設定を保存します。 （注） Call Home 設定を保存すると、エンド ユーザ ライセンス契約（EULA）のメッセージが表示されます。 初めて設定する場合は、ライセンス契約に同意する必要があります。 ヒント アクティブ化した Call Home サービスを非アクティブ化するには、ドロップダウン リストから [無効（Disabled）] オプションを選択して [保存（Save）]をクリックします。
リセット（Reset）	最後に保存された設定にリセットします。
保存して今すぐ Call Home を送信（Save and Call Home Now）	Call Home メッセージを保存し、送信します。 （注） メッセージが正常に送信されると、「Call Home設定が保存され、すべてのCall Homeメッセージが正常に送信されました（Call Home Configuration saved and all Call Home Messages sent successfully）」というメッセージが表示されます。

制約事項

Unified Communications Manager サーバーあるいは Cisco Unified Presence サーバーがダウンしている場合、または接続不能である場合には、以下の制限事項が適用されます。

- Smart Call Home は、サーバーが到達可能になるまで、送信された最後の Call Home メッセージおよびスケジュール設定されている次のメッセージの日時をキャプチャできません。

- Smart Call Home は、サーバーが到達可能になるまで、Call Home メッセージを送信しません。
- Smart Call Home は、パブリッシャがダウンしていると、インベントリのメールでライセンス情報を取得できません。

次の制限事項は、Alert Manager and Collector（AMC）に起因します。

- ノード A でアラートが発生してプライマリ AMC サーバ（デフォルトではパブリッシャ）を再起動する場合、同じノードで 24 時間以内に同じアラートが発生すると、Smart Call Home はノード A からアラート データを再送信します。プライマリ AMC が再行動されたため、Smart Call Home はすでに発生していたアラートを認識できません。
- ノード A でアラートが発生し、プライマリ AMC サーバーを別のノードに変更する場合、同じノードで 24 時間以内に同じアラートが発生すると、Smart Call Home はノード A を新しいアラートとして認識し、アラートデータを送信します。
- プライマリ AMC サーバーで収集したトレースは、シナリオによっては最大 60 時間、プライマリ AMC サーバー上に存在する可能性があります。

混在クラスタ（Cisco Unified Communications Manager および IM and Presence）シナリオにおける制限事項は以下の通りです。

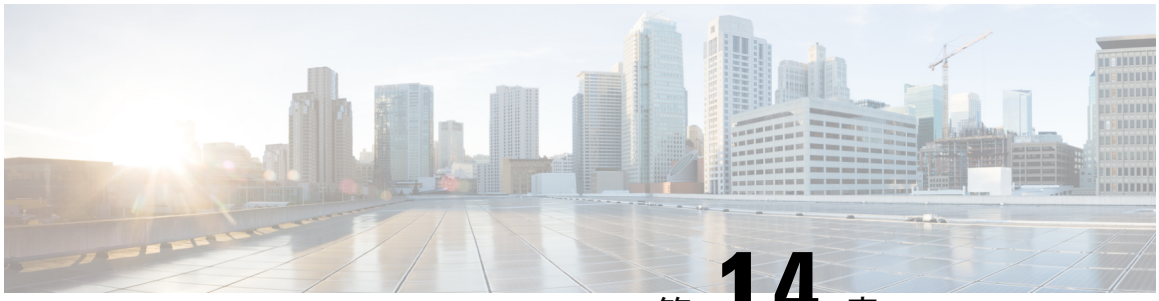
- **CallProcessingNodeCpuPegging**、**Media List Exhausted**、**Route List Exhausted** などのアラートは、IM and Presence には適用されません。
- ユーザーがプライマリ AMC サーバーを IM and Presence に変更した場合、Smart Call Home は **Media List Exhausted** および **Route List Exhausted** のクラスタ概要レポートを生成できません。
- ユーザがプライマリ AMC サーバを IM and Presence に変更した場合、Smart Call Home は **DB Replication** アラートの概要レポートを生成できません。

Call Home の参照先

Smart Call Home の詳細については、次の URL を参照してください。

- Smart Call Home サービスの概要

  http://www.cisco.com/en/US/products/ps7334/serv_home.html



第 14 章

サービスアビリティコネクタ

サービスアビリティコネクタ の概要

Webex Serviceability サービスを使用すると、ログの収集を容易にすることができます。 このサービスでは、診断ログや情報を検索、取得、保管するタスクを自動化します。

この機能は、お客様の社内に導入された サービスアビリティコネクタ を使用します。 サービスアビリティコネクタ は、ネットワーク内の専用ホスト（「コネクタ ホスト」）で実行されます。 次のいずれかのコンポーネントにコネクタを取り付けできます。

- Enterprise Platform (ECP) の利用: 推奨

  ECP は、Docker コンテナを使用してサービスを分離、保護、管理します。 ホストとサービスアビリティ コネクタ アプリケーションがクラウドからインストールされます。 最新の状態で安全な状態を確保するために、手動でアップグレードする必要はありません。

重要 ECP の使用を推奨します。 私たちの将来の開発は、このプラットフォームに焦点を当てます。 Expressway に有用性コネクタをインストールすると、一部の新機能が使用できなくなります。

- Cisco Expressway

Serviceability コネクタは、次の目的で使用できます。

- サービス要求のログおよびシステム情報の自動取得
- クラウド接続型 UC 導入内の Unified CM クラスタのログ収集

どちらの使用例にも同じ Serviceability コネクタを使用できます。

Serviceability サービスを使用する利点

サービスには次の利点があります。

- ログの収集速度を上がります。 TAC エンジニアは、問題の診断を実行する際に関連するログを取得できます。 追加のログ リクエストや手動による収集と配送の待機の遅延を回避できます。 この自動化により、問題解決に要する時間を数日短縮できる可能性があります。
- TAC のコラボレーション ソリューション 解析ツールおよび診断署名データベースと連携します。 システムは、ログを自動的に分析し、既知の問題を特定し、既知の修正または回避策を推奨します。

他のハイブリッド サービスとの違い

サービスアビリティコネクタ の導入と管理は、Hybrid Calendar Service やハイブリッド コール サービスなどの他の Expressway ベースのハイブリッド カレンダー サービスと同様に Control Hub を介して行います。 ただし、重要な違いがいくつかあります。

このサービスには、ユーザ向けの機能がありません。 TAC は、このサービスの主要なユーザです。 他のハイブリッド サービスを使用する組織にはメリットがあります。一方、他のハイブリッド サービスを使用しない組織は共通のユーザです。

組織がすでに Control Hub で設定済みである場合は、既存の組織の管理者アカウントを使用してサービスを有効化できます。

サービスアビリティコネクタ は、ユーザに直接機能を提供するコネクタとは異なる負荷プロファイルがあります。 コネクタは常に使用可能なので、TAC は必要に応じてデータを収集できます。 ただし、時間が経過すると負荷は安定しません。 TAC の担当者は、データ収集を手動で開始します。 同じインフラストラクチャで提供される他のサービスへの影響を最小限に抑えるため、収集の適切な実行時間を調整します。

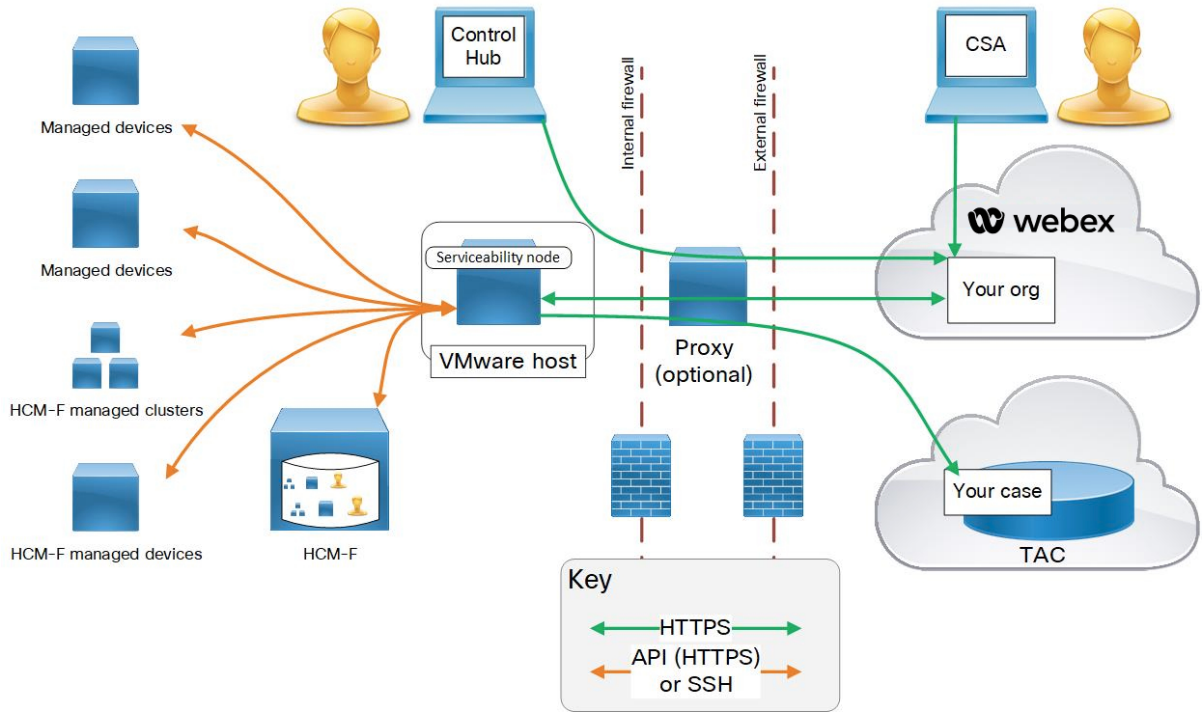
仕組みの概略説明

1. 管理者がシスコ TAC と協力して Serviceability サービスを導入します。 TAC ケースの展開アーキテクチャ （173 ページ）を参照してください。
2. TAC が、ご使用のいずれかのシスコ デバイスに問題があることを確認します（お客様がケースをオープンした場合）。
3. TAC の担当者が Collaborations Solution Analyzer（CSA）のWeb インターフェイスを使用して、関連デバイスからデータを収集するように サービスアビリティコネクタ に要求します。

4. サービスアビリティコネクタは、リクエストを API コマンドに変換して、管理対象デバイスからリクエストされたデータを収集します。
5. サービスアビリティコネクタが、データを収集して暗号化し、暗号化されたリンクを介してカスタマー エクスペリエンス ドライブ (CXD) にアップロードして、サービス リクエストにデータを関連付けます。
6. このデータは、1,000 種類を超える診断シグネチャを含む TAC データベースと照合して分析します。
7. TAC 担当者が結果を確認し、必要に応じてオリジナルのログを確認します。

TAC ケースの展開アーキテクチャ

図 *3 : Expressway* でのサービス コネクタを使用した展開

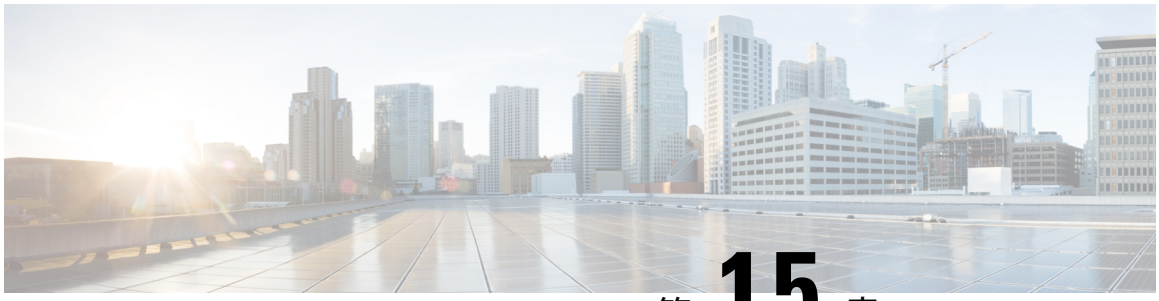


要素	説明
管理対象デバイス	Serviceability サービスにログを提供するすべてのデバイスが含まれます。 Serviceability コネクタ 1 つあたり最大 150 台のローカル管理対象デバイスを追加できます。 HCS の顧客の管理下のデバイスとクラスタ (デバイス数が多い場合は、https://help.webex.com/en-us/142g9e/Limits-and-Bounds-of-Serviceability-Serviceを参照のこと) に関する情報を HCM-F (Hosted Collaboration Mediation Fulfillment) からインポートできます。 このサービスは現在、次のデバイスで動作します。 • Hosted Collaboration Mediation Fulfillment（HCM-F） • Cisco Unified Communications Manager • Cisco Unified CM IM and Presence Service • Cisco Expressway シリーズ • Cisco TelePresence Video Communication Server（VCS） • Cisco Unified Contact Center Express（UCCX） • Cisco Unified Border Element（CUBE） • Cisco BroadWorks Application Server（AS） • Cisco BroadWorks Profile Server（PS） • Cisco BroadWorks Messaging Server（UMS） • Cisco BroadWorks Execution Server（XS） • Cisco Broadworks Xtended Services プラットフォーム (XSP)
管理者	Control Hub を使用してコネクタ ホストを登録し、Serviceability サービスを有効化します。 URL は https://admin.webex.com で、「組織の管理者」としての資格情報が必要です。
コネクタ ホスト	管理コネクタおよび Serviceability Connector をホストする Enterprise Compute Platform (ECP) または Expressway です。 • **管理コネクタ** (ECP または Expressway 上) と対応管理サービス (Webex) が登録を管理します。 接続が保持されて、必要に応じてコネクタが更新され、ステータスとアラームがレポートされます。 • **Serviceability Connector**: お客様の組織で Serviceability サービスが有効化された後にコネクタのホスト (ECP または Expressway) が Webex からダウンロードする、小サイズのアプリケーションです。

要素	説明
[プロキシ（Proxy）]	（オプション）Serviceability Connector の起動後にプロキシ設定を変更した場合は、Serviceability Connector を再起動する必要があります。
Webex クラウド	Webex、Webex Calling、Webex Meetings、Webex ハイブリッド サービスをホストします。
DTP: Delete [Technical Assistance Center] Section.	内容： • CSA を使用して Webex クラウド経由で Serviceability Connector と通信する TAC 担当者。 • Serviceability Connector が収集し、カスタマー エクスペリエンス ドライブにアップロードしたケースと関連ログを含むTACケース管理システム。

サービスアビリティコネクタ の TAC サポート

サービスアビリティコネクタ の詳細については、https://www.cisco.com/go/serviceability を参照するか、TAC の担当者に問い合わせてください。



第 15 章

簡易ネットワーク管理プロトコル

簡易ネットワーク管理プロトコル（SNMP）のサポート

アプリケーション層プロトコルである SNMP を使用すると、ノードやルータなどのネットワーク デバイス間の管理情報を簡単に交換できます。 TCP/IP プロトコル スイートの一部である SNMP を使用すると、管理者はリモートでネットワークのパフォーマンスを管理し、ネットワークの問題を検出および解決し、ネットワークの拡張計画を立てることができます。

Serviceability GUI を使用して、V1、V2c、および V3 のコミュニティ ストリング、ユーザ、通知先など、SNMP 関連の設定を行います。 ユーザーが設定した SNMP 設定は、ローカルノードに適用されます。ただし、システム構成でクラスタをサポートしている場合、SNMP の設定ウィンドウで、「[すべてのノードに適用（Apply to All Nodes）]」オプションを使用して、クラスタ内のすべてのサーバーに設定を適用することもできます。

ヒント Unified Communications Manager のみ：Cisco Unified CallManager または Unified Communications Manager 4.X で指定した SNMP 設定パラメータは、Unified Communications Manager 6.0 以降のアップグレード時に移行されません。 Cisco Unified Serviceability で SNMP 設定手順を繰り返す必要があります。

SNMP は IPv4 と IPv6 をサポートし、CISCO-CCM-MIB には IPv4 と IPv6 の両方のアドレスやプリファレンスなどの列とストレージが含まれています。

SNMP の基礎

SNMP 管理のネットワークは、管理対象デバイス、エージェント、およびネットワーク管理システムという 3 つの主要コンポーネントで構成されています。

- 管理対象デバイス：SNMP エージェントを含み、管理対象ネットワークに存在するネットワーク ノード。 管理対象デバイスには管理情報が収集および格納され、その情報は SNMP を使用することによって利用可能になります。

  Unified Communications Manager および IM and Presence Service のみ：クラスタをサポートする設定では、クラスタ内の最初のノードが管理対象デバイスとして機能します。

- エージェント：管理対象デバイスに存在するネットワーク管理対象ソフトウェア モジュール。 エージェントには、管理情報のローカルな知識が蓄積され、SNMP と互換性のある形式に変換されます。

  SNMP をサポートするため、マスター エージェントとサブエージェントのコンポーネントが使用されます。 マスター エージェントはエージェント プロトコル エンジンとして機能し、SNMP リクエストに関連する認証、許可、アクセスコントロール、およびプライバシーの機能を実行します。 同様に、マスター エージェントには、MIB-II に関係するいくつかの管理情報ベース（MIB）変数が含まれています。 また、マスター エージェントは、サブエージェントへの接続も行います。サブエージェントでの必要なタスクが完了すると、その接続を解除します。 SNMP マスター エージェントはポート 161 で待ち受けし、ベンダー MIB の SNMP パケットを転送します。

  Unified Communications Manager サブ エージェントは、ローカルの Unified Communications Manager のみと通信します。 Unified Communications Manager サブエージェントは SNMP マスター エージェントにトラップと情報メッセージを送信し、SNMP マスター エージェントは SNMP トラップ レシーバ（通知の宛先）と通信します。

  IM and Presence Service サブエージェントは、ローカルの IM and Presence Service とのみ対話します。 IM and Presence Service サブエージェントは SNMP マスター エージェントにトラップと情報メッセージを送信し、SNMP マスター エージェントは SNMP トラップ レシーバ（通知の宛先）と通信します。

- ネットワーク管理システム（NMS）：SNMP 管理アプリケーション（および動作する PC）。ネットワーク管理に必要な処理リソースとメモリ リソースのほとんどを提供します。 NMS では、管理対象デバイスをモニタおよび制御するアプリケーションが実行されます。 次の NMS がサポートされます。

  - CiscoWorks LAN Management Solution
  - HP OpenView
  - SNMP および Unified Communications Manager SNMP インターフェイスをサポートするサードパーティ製アプリケーション

SNMP 管理情報ベース

SNMP では、階層的に編成された情報のコレクションである管理情報ベース（MIB）にアクセスできます。 MIB は、オブジェクト ID で識別される管理対象オブジェクトで構成されます。MIB オブジェクトには、管理対象デバイスの特定の特性が格納され、1 つ以上のオブジェクトインスタンス（変数）で構成されます。

SNMP インターフェイスでは、次のシスコ標準 MIB が提供されます。

- CISCO-CDP-MIB
- CISCO-CCM-MIB
- CISCO-SYSLOG-MIB
- CISCO-UNITY-MIB

次の制限事項があります。

- Unified Communications Manager は、CISCO-UNITY-MIB をサポートしていません。
- Cisco Unity Connection では CISCO-CCM-MIB はサポートされません。
- IM and Presence Service では CISCO-CCM-MIB および CISCO-UNITY-MIB はサポートされません。

SNMP 拡張エージェントはサーバーに常駐し、サーバーが認識しているデバイスに関する詳細情報を提供する CISCO-CCM-MIB を公開します。 クラスタ構成の場合、SNMP 拡張エージェントはクラスタ内の各サーバーに常駐します。 CISCO-CCM-MIB は、サーバ（クラスタでなく、クラスタをサポートする構成内のサーバ）にデバイスの登録状態、IP アドレス、説明、およびモデル タイプなどのデバイス情報を提供します。

SNMP インターフェイスでは、次の業界標準 MIB も提供されます。

- SYSAPPL-MIB
- MIB-II（RFC 1213）
- HOST-RESOURCES-MIB

CISCO-CDP-MIB

Cisco Discovery Protocol MIB（CISCO-CDP-MIB）を読み取るには、CDP サブエージェントを使用します。 この MIB を使用すると、SNMP 管理対象デバイスが自身をネットワーク上の他のシスコ デバイスにアドバタイズできるようになります。

CDP サブエージェントは CDP-MIB を実装します。 CDP-MIB には、次のオブジェクトが含まれています。

- cdpInterfaceIfIndex
- cdpInterfaceMessageInterval
- cdpInterfaceEnable

- cdpInterfaceGroup
- cdpInterfacePort
- cdpGlobalRun
- cdpGlobalMessageInterval
- cdpGlobalHoldTime
- cdpGlobalLastChange
- cdpGobalDeviceId
- cdpGlobalDeviceIdFormat
- cdpGlobalDeviceIdFormatCpd

（注） CISCO-CDP-MIB は、次の MIB の存在に依存しています。CISCO-SMI、CISCO-TC、CISCO-VTP-MIB。

SYSAPPL-MIB

インストールされているアプリケーション、アプリケーション コンポーネント、システム動作しているプロセスなど、SYSAPPL-MIB から情報を取得するには、System Application Agent を使用します。

System Application Agent は、SYSAPPL-MIB の次のオブジェクト グループをサポートしています。

- sysApplInstallPkg
- sysApplRun
- sysApplMap
- sysApplInstallElmt
- sysApplElmtRun

表 *18 : SYSAPPL-MIB* のコマンド

コマンド	説明
デバイスに関連するクエリー	
sysApplInstallPkgVersion	ソフトウェアの製造元によってアプリケーション パッケージに割り当てられたバージョン番号を提供します。
sysApplElmPastRunUser	プロセス所有者のログイン名（root など）を提供します。

メモリ、ストレージ、CPU に関連するクエリー	
sysApplElmPastRunMemory	このプロセスが終了するまでに割り当てられた実システム メモリの合計（KB 単位）の最新の既知の値を提供します。
sysApplElmtPastRunCPU	このプロセスによって消費されたシステム CPU リソースの合計（1/100 秒単位）の最新の既知の値を提供します。 （注） マルチプロセッサ システムでは、この値は実際の時間（実時間）の 1/100 秒よりも大きい単位で増加する可能性があります。
sysApplInstallElmtCurSizeLow	現在のファイル サイズ（modulo 2^32 バイト）を提供します。 たとえば、合計サイズが 4,294,967,296 バイトのファイルの場合、この値は、0 になり、合計サイズが 4,294,967,295 バイトのファイルの場合、この値は、4,294,967,295 になります。
sysApplInstallElmtSizeLow	インストールされたファイル サイズ（modulo 2^32 バイト）を提供します。 これは、インストール直後のディスク上のファイル サイズです。 たとえば、合計サイズが 4,294,967,296 バイトのファイルの場合、この値は、0 になり、合計サイズが 4,294,967,295 バイトのファイルの場合、この値は、4,294,967,295 になります。
sysApplElmRunMemory	このプロセスに現在割り当てられている実システム メモリの合計値（KB 単位）を提供します。
sysApplElmRunCPU	このプロセスによって消費されたシステム CPU リソースの合計値（1/100 秒単位）を提供します。 （注） マルチプロセッサ システムでは、この値は実際の時間（実時間）の 1/100 秒よりも大きい単位で増加する可能性があります。

プロセスに関連するクエリー	
sysApplElmtRunState	実行中のプロセスの現在の状態を提供します。 値は次のとおりです。実行中 (1)、実行可能 (2)、実行可能であるが、CPU などのリソースを待機中 (3)、終了 (4)、その他 (5)。
sysApplElmtRunNumFiles	プロセスによって現在開かれている通常ファイルの数を提供します。 この値の計算には、転送接続（ソケット）や、オペレーティング システム固有の特殊なファイル タイプは含まれません。
sysApplElmtRunTimeStarted	プロセスが開始された時刻を提供します。
sysApplElmtRunMemory	このプロセスに現在割り当てられている実システム メモリの合計値（KB 単位）を提供します。
sysApplElmtPastRunInstallID	インストール済み要素テーブルのインデックスを提供します。 このオブジェクトの値は、このエントリが以前実行されたプロセスを表しているアプリケーション要素の sysApplInstallElmtIndex の値と同じです。
sysApplElmtPastRunUser	プロセス所有者のログイン名（root など）を提供します。
sysApplElmtPastRunTimeEnded	プロセスが終了した時刻を提供します。
sysApplElmtRunUser	プロセス所有者のログイン名（root など）を提供します。
sysApplRunStarted	アプリケーションが起動された日時を提供します。
sysApplElmtRunCPU	このプロセスによって消費されたシステム CPU リソースの合計値（1/100 秒単位）を提供します。 （注） マルチプロセッサ システムでは、この値は実際の時間（実時間）の 1/100 秒よりも大きい単位で増加する可能性があります。

ソフトウェア コンポーネントに関連するクエリー	
sysApplInstallPkgProductName	製造元によってソフトウェア アプリケーション パッケージに割り当てられた名前を提供します。
sysApplElmtRunParameters	プロセスの起動パラメータを提供します。
sysApplElmtRunName	プロセスのフル パスとファイル名を提供します。 たとえば、実行パスが「opt/MYYpkg/bin/myyproc」のプロセス「myyproc」の場合は「/opt/MYYpkg/bin/myyproc」が返されます。
sysApplInstallElmtName	アプリケーションに含まれるこの要素の名前を提供します。
sysApplElmtRunUser	プロセス所有者のログイン名（root など）を提供します。
sysApplInstallElmtPath	この要素がインストールされているディレクトリのフル パスを提供します。 たとえば、「/opt/EMPuma/bin」ディレクトリにインストールされている要素の場合、値は「/opt/EMPuma/bin」になります。 ほとんどのアプリケーション パッケージには、パッケージ内の要素に関する情報が含まれています。 また、要素は通常、パッケージのインストール ディレクトリのサブディレクトリにインストールされます。 パッケージの情報自体に要素のパス名が含まれていない場合、通常はサブディレクトリの簡易検索でパスを特定することができます。 要素がその場所にインストールされておらず、エージェント実装のために別の情報も参照できない場合には、パスは不明となり、null が返されます。

sysApplMapInstallPkgIndex	このオブジェクトの値を提供し、このプロセスが含まれているアプリケーションのインストール済みソフトウェア パッケージを特定します。 プロセスの親アプリケーションを特定できる場合、このオブジェクトの値は、このプロセスが含まれているインストール済みアプリケーションに対応するsysApplInstallPkgTable のエントリのsysApplInstallPkgIndex と同じになります。 ただし、親アプリケーションを特定できない場合には（プロセスが特定のインストール済みアプリケーションに含まれない場合など）、このオブジェクトの値は「0」になります。これは、このプロセスをアプリケーションやインストール済みソフトウェアパッケージと関連付けることができないことを示します。
sysApplElmtRunInstallID	sysApplInstallElmtTable のインデックスを提供します。 このオブジェクトの値は、このエントリが実行中のインスタンスを表すアプリケーション要素のsysApplInstallElmtIndex の値と同じです。 このプロセスが、インストール済みの実行可能ファイルと関連付けられない場合、値は「0」になります。

sysApplRunCurrentState	実行中のアプリケーション インスタンスの現在の状態を提供します。 値は次のとおりです。実行中 (1)、 実行可能 (2)、実行可能であるが、CPU などのリソースを待機中 (3)、終了 (4)、その他 (5)。 This value is based on an evaluation of the running elements of this application instance (see sysApplElmRunState) and their Roles as defined by sysApplInstallElmtRole. エージェント実装は、その REQUIRED 要素の 1 つ以上がもはや実行されない場合アプリケーション インスタンスが終了のプロセスにある事を検出する可能性があります。 エージェント実装のほとんどは、システム時刻を提供して REQUIRED 要素を開始するために、2 番目の内部ポーリングが完了するまで待機してからアプリケーション インスタンスを終了としてマークします。
sysApplInstallPkgDate	このソフトウェア アプリケーションがホストにインストールされた日時を提供します。
sysApplInstallPkgVersion	ソフトウェアの製造元によってアプリケーション パッケージに割り当てられたバージョン番号を提供します。
sysApplInstallElmtType	インストール済みアプリケーションに含まれている要素のタイプを提供します。
日付または時刻に関連するクエリー	
sysApplElmtRunCPU	このプロセスによって消費されたシステム CPU リソースの合計値（1/100 秒単位）です。 （注） マルチプロセッサ システムでは、この値は実際の時間（実時間）の 1/100 秒よりも大きい単位で増加する可能性があります。
sysApplInstallPkgDate	このソフトウェア アプリケーションがホストにインストールされた日時を提供します。

sysApplElmtPastRunTimeEnded	プロセスが終了した時刻を提供します。
sysApplRunStarted	アプリケーションが起動された日時を提供します。

MIB-II

MIB-II から情報を取得するには、MIB2 エージェントを使用します。 MIB2 エージェントは、インターフェイスや IP など、RFC 1213 で定義されている変数へのアクセスを提供し、次のオブジェクト グループをサポートしています。

- システム
- interfaces
- at
- ip
- icmp
- tcp
- udp
- snmp

表 *19 : MIB-II* コマンド

コマンド	説明
デバイスに関連するクエリー	
sysName	この管理対象ノードに管理上割り当てられた名前を提供します。慣例として、この名前はノードの完全修飾ドメイン名になります。名前が不明な場合、この値は長さがゼロの文字列になります。
sysDescr	エンティティの説明テキストを提供します。この値には、システムのハードウェア タイプ、ソフトウェア オペレーティング システム、ネットワーク ソフトウェアの完全な名前とバージョン識別番号が含まれます。
SNMP 診断クエリー	
sysName	この管理対象ノードに管理上割り当てられた名前を提供します。慣例として、この名前はノードの完全修飾ドメイン名になります。名前が不明な場合、この値は長さがゼロの文字列になります。

sysUpTime	システムのネットワーク管理部分が最後に再初期化されてからの時間（1/100 秒単位）を提供します。
snmpInTotalReqVars	有効な SNMP Get-Request と Get-Next PDU を受信した結果として、SNMP プロトコル エンティティによって正常に取得された MIB オブジェクトの合計数を提供します。
snmpOutPkts	SNMP エンティティから転送サービスに渡された SNMP メッセージの合計数を提供します。
sysServices	このエンティティが提供する可能性があるサービスのセットを示す値を提供します。 値は合計値です。 この合計は最初は 0 の値を取りますが、このノードがトランザクションを実行する各レイヤ（L）について 1 ～ 7 の範囲を取り、この合計に（L - 1）の 2 乗が加算されます。 たとえば、アプリケーション サービスを提供するホストであるノードの値が 4（2^（3-1））になる場合や、 逆に、アプリケーション サービスを提供するホストであるノードの値が、72 (2^(4-1) + 2^(7-1)) になる場合があります。 （注） プロトコルのインターネット スイートの場合には、レイヤ 1 の物理（リピータなど）、レイヤ 2 のデータリンクまたはサブネットワーク（ブリッジなど）、レイヤ 3 のインターネット（IP をサポート）、レイヤ 4 のエンドツーエンド（TCP をサポート）、レイヤ 7 のアプリケーション（SMTP をサポート）を計算します。 OSI プロトコルを含むシステムでは、レイヤ 5 および 6 も計算できます。

snmpEnableAuthenTraps	SNMP エンティティが authenticationFailure トラップの生成を許可されているかどうかを示します。 このオブジェクトの値は、すべての設定情報を上書きします。そのため、すべての authenticationFailure トラップを無効化できる手段が提供されます。 （注） シスコでは、このオブジェクトを不揮発性メモリに保存して、ネットワーク管理システムの再初期化後にも維持されるようにすることを強く推奨します。
Syslog に関連するクエリー	
snmpEnabledAuthenTraps	SNMP エンティティが authenticationFailure トラップの生成を許可されているかどうかを示します。 このオブジェクトの値は、すべての設定情報を上書きします。そのため、すべての authenticationFailure トラップを無効化できる手段が提供されます。 （注） シスコでは、このオブジェクトを不揮発性メモリに保存して、ネットワーク管理システムの再初期化後にも維持されるようにすることを強く推奨します。
日付または時刻に関連するクエリー	
sysUpTime	システムのネットワーク管理部分が最後に再初期化されてからの時間（1/100秒単位）を提供します。

HOST-RESOURCES MIB

HOST-RESOURCES-MIB から値を取得するには、Host Resources Agent を使用します。 Host Resources Agent は、ストレージ リソース、プロセス テーブル、デバイス情報、およびインストールされたソフトウェア ベースなど、ホスト情報に対する SNMP アクセスを提供します。 Host Resources Agent は次のオブジェクト グループをサポートしています。

- hrSystem
- hrStorage
- hrDevice
- hrSWRun
- hrSWRunPerf

- hrSWInstalled

表 *20 : HOST-RESOURCES MIB* のコマンド

コマンド	説明
デバイスに関連するクエリー	
hrFSMountPoint	このファイル システムのルートのパス名を提供します。
hrDeviceDescr	デバイスの製造元やリビジョン、シリアル番号（オプション）など、このデバイスの説明テキストを提供します。
hrStorageDescr	ストレージのタイプおよびインスタンスの説明を提供します。
メモリ、ストレージ、CPU に関連するクエリー	
hrMemorySize	ホストに搭載されている物理的な読み取り/書き込みメイン メモリ（通常は RAM）の容量を提供します。
hrStorageSize	ストレージのサイズを hrStorageAllocationUnits の単位で提供します。このオブジェクトは書き込み可能であるため、操作が理に適っており、基盤となるシステムで実行可能な場合には、ストレージエリアのサイズのリモート設定が可能です。 たとえば、バッファ プールに割り当てるメモリの量や、仮想メモリに割り当てるディスク容量を変更できます。
プロセスに関連するクエリー	
hrSWRunName	製造元、リビジョン、一般に知られている名前など、この実行中のソフトウェアの説明テキストを提供します。このソフトウェアがローカルにインストールされている場合は、対応する hrSWInstalledName で使用されているものと同じ文字列である必要があります。
hrSystemProcesses	このシステムに現在ロードされているか、実行中のプロセス コンテキストの数を提供します。
hrSWRunIndex	ホストで実行中の各ソフトウェアに固有の値を提供します。 可能な限り、ネイティブかつ一意のシステム識別番号を使用します。
ソフトウェア コンポーネントに関連するクエリー	

hrSWInstalledName	製造元、リビジョン、一般に知られている名前、およびシリアル番号（オプション）など、このインストールされているソフトウェアの説明テキストを提供します。
hrSWRunPath	このソフトウェアのロード元である長期ストレージの場所（ディスク ドライブなど）の説明を提供します。
日付または時刻に関連するクエリー	
hrSystemDate	ホストのローカルの日時を提供します。
hrFSLastPartialBackupDate	このファイル システムの一部が、バックアップのために別のストレージデバイスにコピーされた最後の日付を提供します。この情報は、バックアップが定期的に実行されていることを確認するのに役立ちます。この情報が不明な場合、この変数は 0000 年 1 月 1 日 00:00:00.0 に対応する値となり、「00 00 01 01 00 00 00 00」（16 進数）と符号化されます。

CISCO-SYSLOG-MIB

Syslog は、情報レベルから重大なものまでのすべてのシステム メッセージを追跡し、ログに記録します。 この MIB を使用すると、ネットワーク管理アプリケーションでは Syslog メッセージを SNMP トラップとして受信できるようになります。

Cisco Syslog Agent では、次の MIB オブジェクトによるトラップ機能をサポートしています。

- clogNotificationsSent
- clogNotificationsEnabled
- clogMaxSeverity
- clogMsgIgnores
- clogMsgDrops

（注） CISCO-SYSLOG-MIB は、CISCO-SMI MIB の存在に依存します。

表 *21 : CISCO-SYSLOG-MIB* のコマンド

コマンド	説明
Syslog に関連するクエリー	

clogNotificationEnabled	デバイスが Syslog メッセージを生成するときに、clogMessageGenerated 通知が送信されるかどうかを示します。 通知を無効化しても、syslog メッセージは、clogHistoryTable に追加されます。
clogMaxSeverity	Indicates which syslog severity levels will be processed. エージェントは、重大度がこの値より大きい Syslog メッセージを無視します。 （注） 重大度は数値が大きくなるほど低くなります。 たとえば、エラー（4）は、デバッグ（8）より重大度が高いです。

CISCO-CCM-MIB および CISCO-CCM-CAPABILITY MIB

CISCO-CCM-MIB には、Unified Communications Manager と、Unified Communications Manager ノードで確認できる、電話やゲートウェイなどのそれに関連するデバイスについての動的な（リアルタイム）情報と設定された（静的）情報の両方が含まれています。 簡易ネットワーク管理プロトコル（SNMP）テーブルには、IP アドレス、登録ステータス、およびモデルタイプなどの情報が格納されています。

SNMP は IPv4 と IPv6 をサポートし、CISCO-CCM-MIB には IPv4 と IPv6 の両方のアドレスやプリファレンスなどの列とストレージが含まれています。

（注） Unified Communications Manager は、Unified Communications Manager システム内のこの MIB をサポートしています。 IM and Presence Service と Cisco Unity Connection はこの MIB をサポートしていません。

CISCO-CCM-MIB および MIB 定義のサポート リストを参照するには、次のリンクにアクセスしてください。

ftp://ftp.cisco.com/pub/mibs/supportlists/callmanager/callmanager-supportlist.html

廃止オブジェクトを含め、Unified Communications Manage リリース全体での MIB の依存関係と MIB コンテンツを表示するには、次のリンクにアクセスしてください。 http://tools.cisco.com/Support/SNMP/do/BrowseMIB.do?local=en&step=2&mibName=CISCO-CCM-CAPABILITY

動的テーブルは、Cisco CallManager サービスが起動され、実行中の場合のみ入力されます（またはUnified Communications Manage クラスタ設定の場合は、ローカルの Cisco CallManager サービス）。静的テーブルは、Cisco CallManager SNMP サービスが実行中の場合に入力されます。

表 *22 : Cisco-CCM-MIB* の動的テーブル

テーブル	コンテンツ
ccmTable	このテーブルには、ローカル Unified Communications Manager のバージョンおよびインストール ID が保存されます。 また、このテーブルには、ローカルの Unified Communications Manager が認識するクラスタ内のすべての Unified Communications Manager についての情報も保存されますが、バージョンの詳細は、「「unknown」」と示されます。 ローカルの Unified Communications Manager がダウンした場合、バージョンおよびインストール ID の値を除き、テーブルは空のままになります。
ccmPhoneFailed、ccmPhoneStatusUpdate、ccmPhoneExtn、ccmPhone、ccmPhoneExtension	Cisco Unified IP 電話 の場合、ccmPhoneTable の登録済み電話機の数は、Unified Communications Manager/RegisteredHardware Phones perfmon カウンタと一致する必要があります。 ccmPhoneTable には、登録済み、未登録、および拒否された Cisco Unified IP 電話 ごとに 1 つのエントリがあります。 ccmPhoneExtnTable では、インデックス ccmPhoneIndex と ccmPhoneExtnIndex を組み合わせて、ccmPhoneTable と ccmPhoneExtnTable のエントリが関連付けられます。
ccmCTIDevice、ccmCTIDeviceDirNum	ccmCTIDeviceTable には、各 CTI デバイスが 1 つのデバイスとして保存されます。 CTI ルートポイントまたは CTI ポートの登録ステータスに基づいて、Unified Communications Manager MIB 内の ccmRegisteredCTIDevices、ccmUnregisteredCTIDevices、ccmRejectedCTIDevices カウンタが更新されます。
ccmSIPDevice	CCMSIPDeviceTable には、各 SIP トランクが 1 つのデバイスとして保存されます。
ccmH323Device	ccmH323DeviceTable には、Unified Communications Manager（または、クラスタ設定の場合は、ローカルの Unified Communications Manager）に情報が含まれる H.323 デバイスのリストが含まれます。 H.323 電話機または H.323 ゲートウェイの場合、ccmH.323DeviceTable には H.323 デバイスごとに 1 つのエントリが作成されます。 (H.323 電話機およびゲートウェイは、Unified Communications Manager で登録されません。 指定された H.323 電話機およびゲートウェイのコールを処理する準備ができると、Unified Communications Manager によって H.323Started アラームが生成されます。) システムにより、H.323 トランク情報の一部としてゲートキーパー情報が提供されます。
ccmVoiceMailDevice、ccmVoiceMailDirNum	Cisco uOne、ActiveVoice の場合、ccmVoiceMailDeviceTable には音声メッセージングデバイスごとに 1 つのエントリが作成されます。 登録ステータスに基づいて、Cisc MIB 内の ccmRegisteredVoiceMailDevices、ccmUnregisteredVoiceMailDevices、ccmRejectedVoiceMailDevices カウンタが更新されます。

テーブル	コンテンツ
ccmGateway	ccmRegisteredGateways、ccmUnregisteredGateways、および ccmRejectedGateways は、それぞれ、登録されたゲートウェイ デバイスまたはポートの数、登録されていないゲートウェイ デバイスまたはポートの数、および拒否されたゲートウェイ デバイスまたはポートの数を追跡します。 Unified Communications Manager は、デバイスまたはポート レベルでアラームを生成します。 ccmGatewayTable には、CallManager アラームに基づいて、デバイスレベルまたはポートレベルの情報が格納されます。 登録済み、未登録、または拒否されたデバイスまたはポートごとに、1 つのエントリが ccmGatewayTable に存在します。2 つの FXS ポートと 1 つの T1 ポートを備えた VG200 の場合、ccmGatewayTable には 3 つのエントリが作成されます。ccmActiveGateway および ccmInActiveGateway のカウンタは、アクティブな（登録済みの）ゲートウェイ デバイスまたはポート、および接続されていない（未登録または拒否）ゲートウェイ デバイスまたはポートの数を追跡します。 登録ステータスに基づき、ccmRegisteredGateways、ccmUnregisteredGateways、ccmRejectedGateways の各カウンタが更新されます。
ccmMediaDeviceInfo	このテーブルには、少なくとも 1 回はローカルの Unified Communications Manager での登録を試みたすべてのメディア デバイスのリストが格納されます。
ccmGroup	このテーブルには、Unified Communications Manager クラスタ内の Unified Communications Manager グループが格納されます。
ccmGroupMapping	このテーブルは、クラスタ内のすべての Unified Communications Manager を Unified Communications Manager グループにマッピングします。 ローカルの Unified Communications Manager ノードがダウンしても、このテーブルは空のままです。

表 *23 : CISCO-CCM-MIB* の静的テーブル

テーブル	コンテンツ
ccmProductType	このテーブルには、Unified Communications Manager（Unified Communications Manager クラスタ設定の場合はクラスタ）でサポートされる製品タイプのリストが格納されます。タイプには、電話機タイプ、ゲートウェイ タイプ、メディア デバイス タイプ、H.323 デバイス タイプ、CTI デバイス タイプ、音声メッセージング デバイス タイプ、SIP デバイス タイプなどがあります。
ccmRegion、ccmRegionPair	ccmRegionTable には、Cisco Communications Network（CCN）システムの地理的に離れた場所にあるすべてのリージョンのリストが格納されます。 ccmRegionPairTable には、Unified Communications Manager クラスタの地理的リージョンペアのリストが含まれます。 地理的リージョンペアは、接続元リージョンと接続先リージョンで定義されます。
ccmTimeZone	このテーブルには、Unified Communications Manager のクラスタ内のすべてのタイム ゾーン グループのリストが含まれます。
ccmDevicePool	このテーブルには、Unified Communications Manager のクラスタ内のすべてのデバイス プールのリストが含まれます。デバイス プールは、リージョン、日付/時刻グループ、および Unified Communications Manager グループによって定義されます。

（注） CISCO-CCM-MIB の 「ccmAlarmConfigInfo」 グループおよび 「ccmQualityReportAlarmConfigInfo」 グループでは、通知に関する設定パラメータを定義します。

CISCO-UNITY-MIB

CISCO-UNITY-MIB では、Cisco Unity Connection に関する情報を入手するために Connection SNMP エージェントを使用します。

CISCO-UNITY-MIB の定義を確認するには、次のリンクにアクセスして [SNMP v2 MIB（SNMP v2 MIBs）]をクリックしてください。

http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml [英語]

（注） Cisco Unity Connection ではこの MIB をサポートしています。 Unified Communications Manager と IM and Presence Service は、この MIB をサポートしていません。

Connection SNMP エージェントでは次のオブジェクトをサポートしています。

表 *24 : CISCO-UNITY-MIB* のオブジェクト

オブジェクト	説明
ciscoUnityTable	このテーブルには、ホスト名やバージョン番号など、Cisco Unity Connection サーバーに関する一般的な情報が格納されます。
ciscoUnityPortTable	このテーブルには、Cisco Unity Connection のボイス メッセージング ポートに関する一般的な情報が格納されます。
General Unity Usage Info オブジェクト	このグループには、Cisco Unity Connection のボイス メッセージング ポートの容量と使用率に関する情報が格納されます。

SNMP の設定要件

システムにはデフォルトの SNMP 設定はありません。 MIB 情報にアクセスするには、インストール後に SNMP の設定を行う必要があります。 シスコでは、SNMP V1、V2c、および V3 バージョンをサポートしています。

SNMP エージェントは、コミュニティ名と認証トラップによるセキュリティを提供します。 MIB 情報にアクセスするには、コミュニティ名を設定する必要があります。 次の表に、必要な SNMP 構成時の設定を提供します。

表 *25 : SNMP* の設定要件

設定	**[Cisco Unified Serviceability] ページ**
V1/V2c コミュニティ ストリング	**SNMP** > **V1/V2c** > **コミュニティ ストリング**
V3 コミュニティ ストリング	**SNMP** > **V3** > **ユーザ**
MIB2 のシステム コンタクトおよびロケーション	**SNMP** > **SystemGroup** > **MIB2 システム グループ**
トラップ通知先（V1/V2c）	**SNMP** > **V1/V2c** > **Notification Destination**
トラップ通知先（V3）	**SNMP** > **V3** > **Notification Destination**

SNMP バージョン 1 のサポート

SNMP バージョン 1（SNMPv1）は、管理情報構造（SMI）の仕様の範囲内で機能する SNMP の初期実装で、User Datagram Protocol（UDP）や Internet Protocol（IP）などのプロトコル上で動作します。

SNMPv1 SMI では、高度な構造を持つテーブル（MIB）が定義されます。このテーブルは、表形式のオブジェクト（つまり、複数の変数を含むオブジェクト）のインスタンスのグループ化に使用されます。 テーブルにはインデックスが付けられた 0 個以上の行が格納されるため、SNMP では、サポートされているコマンドを使用して、行全体を取得したり変更したりできます。

SNMPv1 では、NMS がリクエストを発行し、管理対象デバイスからレスポンスが返されます。エージェントは、トラップ オペレーションを使用して、NMS に重要なイベントを非同期的に通知します。

Serviceability GUI では、SNMPv1 サポートを [V1/V2c の設定（V1/V2c Configuration）]ウィンドウで設定します。

SNMP バージョン 2c のサポート

SNMPv2c は、SNMPv1 と同様に、Structure of Management Information（SMI）の仕様の範囲内で機能します。 MIB モジュールには、相互に関係のある管理対象オブジェクトの定義が格納されます。 SNMPv1 で使用されるオペレーションと SNMPv2 で使用されるオペレーションは、ほぼ同じです。 たとえば、SNMPv2 トラップ オペレーションは、SNMPv1 で使用する機能と同じですが、異なるメッセージ形式を使用する、SNMPv1 トラップに代わる機能です。

SNMPv2c のインフォームオペレーションでは、ある NMS から別の NMS にトラップ情報を送信して、その NMS からレスポンスを受信することができます。

Serviceability GUI では、SNMPv2c サポートを [V1/V2c の設定（V1/V2c Configuration）] ウィンドウで設定します。

SNMP バージョン 3 のサポート

SNMP バージョン 3 は、認証（リクエストが正規の送信元から送信されたものかどうかの確認）、プライバシー（データの暗号化）、認可（リクエストされた操作がユーザーに許可されているかどうかの確認）、およびアクセスコントロール（リクエストされたオブジェクトにユーザーがアクセスできるかどうかの確認）などのセキュリティ機能を提供します。 SNMP パケットがネットワーク上で公開されないように、SNMPv3 では暗号化を設定できます。

（注） リリース 12.5(1)SU1 以降の MD5 または DES の暗号化方式は、ユニファイドコミュニケーションマネージャではサポートされません。 SNMPv3 ユーザーを追加する場合は、認証プロトコルとして SHA または AES のいずれかを選択することができます。

SNMPv3 では、SNMPv1 や SNMPv2 のようにコミュニティ ストリングを使用するのではなく、SNMP ユーザーを使用します。

有用性 GUI で、**[V3 設定 (V3 Configuration)]** ウィンドウで SNMPv3 サポートを設定します。

SNMP サービス

次の表のサービスでは、SNMP の操作をサポートしています。

（注） SNMP マスター エージェントは、MIB インターフェイスのプライマリ サービスとして機能します。 Cisco CallManager SNMP サービスは手動でアクティブ化する必要があります。他のすべての SNMP サービスは、インストール後に実行する必要があります。

表 *26 : SNMP* サービス

MIB	サービス	ウィンドウ
CISCO-CCM-MIB	Cisco CallManager SNMP サービス	**[Cisco Unified Serviceability]** > **[ツール（Tools）]** > **[コントロール センター - 機能サービス（Control Center - Feature Services）]**。 サーバーを選択した後、[パフォーマンスおよびモニタリング（Performance and Monitoring）] カテゴリを選択します。
SNMP エージェント	SNMP Master Agent	**[Cisco Unified Serviceability]** > **[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）]** サーバーを選択した後、[プラットフォームサービス（Platform Services）] カテゴリを選択します。 **[CiscoUnifiedIM and Presence Serviceability]** > **[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）]** サーバーを選択した後、[プラットフォームサービス（Platform Services）] カテゴリを選択します。
CISCO-CDP-MIB	Cisco CDP Agent	
SYSAPPL-MIB	System Application Agent	
MIB-II	MIB2 Agent	
HOST-RESOURCES-MIB	Host Resources Agent	
CISCO-SYSLOG-MIB	Cisco Syslog Agent	
ハードウェア MIB	Native Agent Adaptor	
CISCO-UNITY-MIB	Connection SNMP Agent	**[Cisco Unity Connection Serviceability]** > **[ツール（Tools）]** > **[サービス管理（Service Management）]** サーバーを選択した後、[基本サービス（Base Services）] カテゴリを選択します。

⚠

注意 SNMP サービスを停止すると、ネットワーク管理システムが Unified Communications Manager または Cisco Unity Connection ネットワークをモニタしなくなるため、データが失われます。テクニカル サポート チームの指示がない限り、サービスを停止しないでください。

SNMP のコミュニティ ストリングとユーザ

SNMP コミュニティ ストリングでは、セキュリティは確保されませんが、MIB オブジェクトへのアクセスを認証し、組み込みパスワードとして機能します。 SNMP コミュニティ ストリングは、SNMP v1 および v2c の場合にのみ設定します。

SNMPv3 では、コミュニティ ストリングを使用しません。バージョン 3 では、代わりに SNMP ユーザーを使用します。 SNMP ユーザーを使用する目的はコミュニティストリングと同じですが、ユーザーの暗号化や認証を設定できるため、セキュリティが確保されます。

Serviceability GUI では、デフォルトのコミュニティストリングやユーザーは存在しません。

SNMP のトラップとインフォーム

SNMP エージェントは、重要なシステム イベントを識別するために、トラップ形式またはインフォーム形式で NMS に通知を送信します。 トラップ形式の場合は宛先からの確認応答を受信しませんが、インフォーム形式の場合は確認応答を受信します。 通知先を設定するには、Serviceability GUI の [SNMP 通知先設定（Notification Destination Configuration）] ウィンドウを使用します。

（注） Unified Communications Manager は、Unified Communications Manager および IM and Presence Service システムの SNMP トラップをサポートします。

SNMP 通知では、対応するトラップ フラグが有効な場合、トラップが即座に送信されます。Syslog エージェントの場合、アラームとシステム レベルのログ メッセージが Syslog デーモンに送信され、ログに記録されます。また、一部の標準的なサードパーティ製アプリケーションでもログ メッセージが syslog デーモンに送信され、ログに記録されます。 これらのログ メッセージはローカルの syslog ファイルに記録され、SNMP トラップまたは通知への変換も行われます。

以下に、設定済みのトラップ通知先に送信される、Unified Communications Manager の SNMP のトラップおよびインフォーム メッセージの一覧を示します。

- Unified Communications Manager で障害が発生しました
- 電話機で障害が発生しました（Phone failed）
- 電話機ステータスの更新（Phones status update）
- ゲートウェイで障害が発生しました（Gateway failed）
- メディア リソース リストが使い果たされました（Media resource list exhausted）
- ルート リストが使い果たされました（Route list exhausted）
- ゲートウェイ レイヤ 2 の変更（Gateway layer 2 change）
- 品質レポート（Quality report）
- 悪質なコール（Malicious call）

• syslog メッセージが生成されました（Syslog message generated）

ヒント 通知先を設定する前に、必要なSNMPサービスがアクティブ化され、動作していることを確認します。 また、コミュニティストリング/ユーザーに対する特権が正しく設定されていることを確認します。

Serviceability GUI の **[SNMP]** > **[V1/V2]** > **[通知先（Notification Destination）]** または **[SNMP]** > **[V3]** > **[通知先（Notification Destination）]** を選択して SNMP トラップの宛先を設定します。

次の表では、ネットワーク管理システム（NMS）で設定するトラップとインフォームのパラメータについて説明します。 この表の値を設定するには、その NMS をサポートする SNMP 製品のドキュメントの説明に従って、NMS 上で適切なコマンドを実行します。

（注） この表に一覧されているパラメータは、最後の 2 つのパラメータを除き、すべて CISCO-CCM-MIB の一部です。 最後の 2 つの clogNotificationsEnabled と clogMaxSeverity は、CISCO-SYSLOG-MIB の一部です。

IM and Presence Service の場合、NMS で clogNotificationsEnabled パラメータと clogMaxSeverity trap/inform パラメータのみを設定します。

表 *27 : Cisco Unified Communications Manager* のトラップおよびインフォーム設定パラメータ

パラメータ名	デフォルト値	生成されるトラップ	推奨設定
ccmCallManagerAlarmEnable	True	ccmCallManagerFailed ccmMediaResourceListExhausted ccmRouteListExhausted ccmTLSConnectionFailure	デフォルトの仕様を維持します。
ccmGatewayAlarmEnable	True	ccmGatewayFailed ccmGatewayLayer2Change Cisco Unified Communications Manager 管理では、CiscoATA 186 デバイスを電話機として設定することができますが、Unified Communications Manager が SNMP トラップを CiscoATA デバイスに送信する際には、ゲートウェイ タイプのトラップが送信されます（たとえば、ccmGatewayFailed など）。	なし。 デフォルトではこのトラップは有効に設定されています。

パラメータ名	デフォルト値	生成されるトラップ	推奨設定
ccmPhoneStatusUpdateStorePeriod ccmPhoneStatusUpdateAlarmInterval	1800 0	ccmPhoneStatusUpdate	ccmPhoneStatusUpdateAlarmInterval は 30 ～ 3600 の範囲の値に設定します。
ccmPhoneFailedStorePeriod ccmPhoneFailedAlarmInterval	1800 0	ccmPhoneFailed	ccmPhoneFailedAlarmInterval は 30 ～ 3600 の範囲の値に設定します。
ccmMaliciousCallAlarmEnable	True	ccmMaliciousCall	なし。 デフォルトではこのトラップは有効に設定されています。
ccmQualityReportAlarmEnable	True	このトラップは、CiscoExtended Functions サービスがサーバー上、または、クラスタ設定の場合には（Unified Communications Manager のみ）ローカル Unified Communications Manager サーバー上でアクティブ化されて実行されている場合にのみ生成されます。 ccmQualityReport	なし。 デフォルトではこのトラップは有効に設定されています。
clogNotificationsEnabled	False	clogMessageGenerated	トラップ生成をイネーブルにするには、clogNotificationsEnable を True に設定します。
clogMaxSeverity	警告	clogMessageGenerated	clogMaxSeverity を warning に設定すると、アプリケーションが、重大度が警告以上の Syslog メッセージを生成したときに SNMP トラップが生成されます。

SFTP サーバーのサポート

内部テストでは、Cisco が提供し、Cisco TAC がサポートする Cisco Prime Collaboration Deployment（PCD）上で SFTP サーバーを使用します。 SFTP サーバオプションの概要については、次の表を参照してください。

表 *28 : SFTP* サーバーのサポート

SFTP サーバ	サポートの説明
Cisco Prime Collaboration Deployment の SFTP サーバ	このサーバーはシスコが提供およびテストした唯一の SFTP サーバーであり、Cisco TAC が完全にサポートします。 バージョンの互換性は、使用している Emergency Responder および Cisco Prime Collaboration Deployment のバージョンに依存します。 バージョン（SFTP）または Emergency Responder をアップグレードする前に、『Cisco Prime Collaboration Deployment Administration Guide』を参照して、互換性のあるバージョンであることを確認してください。
テクノロジー パートナーの SFTP サーバ	これらのサーバーはサードパーティが提供およびテストしたものです。 バージョンの互換性は、サードパーティによるテストに依存します。 テクノロジーパートナーの SFTP 製品または Unified Communications Manager をアップグレードする場合、テクノロジーパートナーのページを参照してください。
他のサードパーティの SFTP サーバ	これらのサーバーはサードパーティが提供するものであり、Cisco TAC はこれらのサーバーを正式にサポートしていません。 バージョンの互換性は、SFTP バージョンと Emergency Responder バージョンの互換性を確立するためのベスト エフォートに基づきます。 （注） これらの製品はシスコによってテストされていないため、機能を保証することはできません。 Cisco TAC はこれらの製品をサポートしていません。 完全にテストされてサポートされる SFTP ソリューションとしては、Cisco Prime Collaboration Deployment またはテクノロジーパートナーの SFTP サーバーを利用してください。

SNMP 設定タスク フロー

簡易ネットワーク管理プロトコルの設定を行うには、以下のタスクを実行します。タスクが異なる場合があるため、どの SNMP バージョンを設定するかを必ず確認してください。 SNMP V1、V2c、または V3 から選択することができます。

始める前に

SNMP ネットワーク管理システムをインストールして、設定します。

手順

	コマンドまたはアクション	目的
ステップ 1	SNMP サービスの有効化 （202 ページ）	重要な SNMP サービスが稼働中であることを確認します。
ステップ 2	使用する SNMP のバージョンに応じて、以下のいずれかのタスクを実行します。 • SNMP コミュニティ ストリングの設定 （203 ページ） • SNMP ユーザの設定 （206 ページ）	SNMP V1 あるいは V2 の場合、SNMP コミュニティ ストリングを設定します。 SNMP V3 の場合は、SNMP ユーザーを設定します。
ステップ 3	Remote SNMP Engine ID の取得 （210 ページ）	SNMP V3 の場合は、通知先の設定に必要なリモート SNMP エンジンのアドレスを取得します。 （注） Snmp V3 の場合は、この手順は必須ですが、SNMP V1 または V2c の場合は省略できます。
ステップ 4	SNMP 通知先の設定 （210 ページ）	すべての SNMP に、SNMP トラップおよび通知を送信する通知先を設定します。
ステップ 5	MIB2 システム グループの設定 （215 ページ）	MIB-II システム グループのシステム コンタクトおよびシステム ロケーションを設定します。
ステップ 6	CISCO-SYSLOG-MIB トラップ パラメータ （217 ページ）	CISCO-SYSLOG-MIB のトラップ設定を設定します。
ステップ 7	CISCO-CCM-MIB トラップ パラメータ （218 ページ）	Unified Communications Manager のみ：CISCO-CCM-MIB のトラップ設定を行います。
ステップ 8	SNMP Master Agent の再起動 （218 ページ）	SNMP の設定が完了したら、SNMP マスター エージェントを再起動します。
ステップ 9	SNMP ネットワークk管理システムで、Unified Communications Manager のトラップ パラメータを設定します。	

SNMP サービスの有効化

SNMP サービスが動作していることを確認するには、以下の手順を使用します。

手順

ステップ 1 [Cisco Unified Serviceability] にログインします。

ステップ 2 **Cisco SNMP Master Agent** ネットワーク サービスが実行中であることを確認します。 サービスはデフォルトでオンになっています。

a) **[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。
b) パブリッシャ ノードを選択し、**移動**をクリックします。
c) **Cisco SNMP Master Agent** サービスが稼働していることを確認します。

ステップ 3 **Cisco Call Manager SNMP Service**を起動します。

a) **コントロール センター** > **サービスの有効化**を選択します。
b) **サーバ** ドロップダウンから、パブリッシャ ノードを選択して、**移動**をクリックします。
c) **Cisco Call Manager SNMP サービス** が稼働していることを確認します。 稼働していない場合は、対応するチェック ボックスをオンにして、**[保存]** をクリックします。

次のタスク

SNMP V1 または V2c を設定する場合は、SNMP コミュニティ ストリングの設定 （203 ページ）。

SNMP V3 を設定する場合は、SNMP ユーザの設定 （206 ページ）。

SNMP コミュニティ ストリングの設定

SNMP V1 または V2c を導入している場合は、以下の手順を使用して SNMP コミュニティ ストリングを設定します。

（注） この手順は、SNMP V1 または V2c の場合、必須となります。 SNMP V3 では、コミュニティ ストリングではなく SNMP ユーザーを設定します。

手順

ステップ 1 Cisco Unified Serviceabilityから、**SNMP** > **V1/V2c** > **コミュニティ ストリング**を選択します。

ステップ 2 **サーバ** を選択し、**検索** をクリックして、既存のコミュニティ ストリングを検索します。 必要に応じて、検索パラメータを入力して特定のコミュニティ文字列を検索することができます。

ステップ 3 次のいずれかを実行します。

- 既存の SNMP コミュニティ ストリングを編集するには、そのストリングを選択します。

- 新しいコミュニティ ストリングを追加するには、[新規追加（Add New）]をクリックします。

（注） 既存のコミュニティストリングを削除するには、そのストリングを選択して、**選択したものを削除する** をクリックします。 ユーザーを削除したら、Cisco SNMP マスターエージェントを再起動します。

ステップ 4 **コミュニティ ストリング名**を入力します。

ステップ 5 **SNMP コミュニティ ストリングの設定** ウィンドウの各フィールドに入力します。 フィールドおよびフィールドの設定の詳細は、コミュニティ ストリングの構成時の設定 （204 ページ）を参照してください。

ステップ 6 **アクセス権限** ドロップダウンで、そのコミュニティ ストリングの権限を設定します。

ステップ 7 この設定をすべてのクラスタ ノードに適用する場合、**すべてのノードに適用する** チェック ボックスをオンにします。

ステップ 8 **[保存]** をクリックします。

ステップ 9 **OK** をクリックして、SNMP マスター エージェントのサービスを再起動して、変更を反映させます。

次のタスク

SNMP 通知先の設定 （210 ページ）

コミュニティ ストリングの構成時の設定

次の表で、コミュニティ ストリングの構成時の設定について説明します。

表 *29*：コミュニティ ストリングの構成時の設定

フィールド	説明
サーバ（Server）	コミュニティストリングを検索する際に手順を実行してサーバーの選択を指定しているため、[コミュニティ ストリング設定（Community String configuration）] ウィンドウの設定は読み取り専用として表示されます。 コミュニティストリングのサーバーを変更するには、コミュニティストリングの検索手順を実行します。

フィールド	説明
コミュニティ ストリング（Community String）	コミュニティ ストリングの名前を入力します。 この名前には、最長 32 文字を指定でき、英数字、ハイフン（-）、および下線文字（_）を任意に組み合わせることが可能です。 **ヒント** 部外者が推測しにくいコミュニティ ストリング名を選択してください。 コミュニティ ストリングを編集するとき、コミュニティ ストリングの名前は変更できません。
任意のホストからの SNMP パケットを受け入れる（Accept SNMP Packets from any host）	任意のホストから SNMP パケットを受け入れるには、このボタンをクリックします。
指定したホストからの SNMP パケットのみ受け入れる（Accept SNMP Packets only from these hosts）	特定のホストからの SNMP パケットを受け入れるには、このオプション ボタンをクリックします。 [ホスト名/IPv4/IPv6 アドレス（Hostname/IPv4/IPv6 Address）] フィールドに、SNMP パケットを受け取る IPv4 または IPv6 アドレスを入力し、[挿入（Insert）]をクリックします。 IPv4 アドレスはドット付き 10 進表記です。 たとえば、10.66.34.23 と指定します。 IPv6 アドレスはコロンで区切られた 16 進表記です。 たとえば、2001:0db8:85a3:0000:0000:8a2e:0370:7334 または 2001:0db8:85a3::8a2e:0370:7334 と指定します。 SNMP パケットを受け取るアドレスごとにこのプロセスを繰り返します。 アドレスを削除するには、それを [ホスト IPv4/IPv6 アドレス（Host IPv4/IPv6 Addresses）] リスト ボックスから選択し、[削除（Remove）]をクリックします。

フィールド	説明
アクセス権限（Access Privileges）	ドロップダウン リスト ボックスで、適切なアクセス レベルを次のリストの中から選択します。 **ReadOnly** コミュニティ ストリングは、MIB オブジェクトの値の読み取りのみが可能です。 **ReadWrite** コミュニティ ストリングは、MIB オブジェクトの値を読み書きできます。 **ReadWriteNotify** コミュニティ ストリングは、MIB オブジェクト値の読み取りおよび書き込みと、トラップおよびインフォーム メッセージでの MIB オブジェクト値の送信が可能です。 **NotifyOnly** コミュニティ ストリングは、トラップおよびインフォーム メッセージでの MIB オブジェクト値の送信のみ可能です。 **ReadNotifyOnly** コミュニティ ストリングは、MIB オブジェクト値の読み取りと、トラップおよびインフォーム メッセージでの値の送信が可能です。 **None** コミュニティ ストリングはトラップ情報の読み取り、書き込み、送信を行えません。 **ヒント** トラップ設定パラメータを変更するには、NotifyOnly、ReadNotifyOnly、または ReadWriteNotify 権限でコミュニティ ストリングを設定します。 IM and Presence Service は ReadNoticyOnly をサポートしていません。
すべてのノードに適用（Apply to All Nodes）	クラスタ内のすべてのノードにコミュニティ ストリングを適用する場合は、このチェックボックスをオンにします。 このフィールドは、Unified Communications Manager および IM and Presence Service のクラスタにのみ適用されます。

SNMP ユーザの設定

SNMP V3 を導入している場合は、以下の手順を使用して SNMP ユーザーを設定します。

（注） この手順は、SNMP V3 の場合にのみ必要です。 SNMP V1 または V2c の場合は、コミュニティストリングを設定します。

手順

ステップ 1 Cisco Unified Serviceability で、**SNMP** > **V3** > **ユーザ**を選択します。

ステップ 2 **[サーバー（Server）]** を選択して、**[検索（Find）]** をクリックして、既存の SNMP ユーザーを検索します。 必要に応じて、検索パラメータを入力して特定のユーザーを検索することができます。

ステップ 3 次のいずれかを実行します。

- 既存の SNMP ユーザーを編集するには、ユーザーを選択します。
- 新しい SNMP ユーザーを追加するには、**[新規追加（Add New）]** をクリックします。

（注） 既存のユーザーを削除するには、ユーザーを選択して **[選択したものを削除する（Delete Selected）]** をクリックします。 ユーザーを削除したら、Cisco SNMP マスターエージェントを再起動します。

ステップ 4 [SNMP User Name]を入力します。

ステップ 5 SNMP ユーザーの設定を入力します。 フィールドおよびフィールドの設定の詳細は、SNMP V3 のユーザ構成時の設定 （208 ページ）を参照してください。

ヒント 設定を保存する前であれば、[すべてクリア（Clear All）]ボタンをクリックしてウィンドウ内の設定に入力した情報をすべて消去することができます。

ステップ 6 **アクセス権限** ドロップダウンで、このユーザーに割り当てるアクセス権限を設定します。

ステップ 7 この設定をすべてのクラスタ ノードに適用する場合、**すべてのノードに適用する**チェックボックスをオンにします。

ステップ 8 **[保存]** をクリックします。

ステップ 9 **OK** をクリックして、SNMP マスター エージェントを再起動します。

（注） 設定したユーザーが存在するこのサーバーにアクセスするには必ず NMS で適切な認証およびプライバシー設定を使用して、このユーザーを設定します。

次のタスク

Remote SNMP Engine ID の取得 （210 ページ）

SNMP V3 のユーザ構成時の設定

次の表に、SNMP V3 のユーザ構成時の設定について説明します。

表 *30 : SNMP V3* のユーザ構成時の設定

フィールド	説明
サーバ（Server）	通知先の検索の手順を実行したときにサーバーを指定済みのため、この設定は読み取り専用として表示されます。 アクセスを提供するサーバーを変更するには、SNMPユーザーの検索手順を実行します。
ユーザー名	このフィールドには、アクセスを提供するユーザーの名前を入力します。 この名前には、最長32文字を指定でき、英数字、ハイフン（-）、および下線文字（_）を任意に組み合わせることが可能です。 **ヒント** ネットワーク管理システム（NMS）に設定済みのユーザーを入力します。 既存の SNMP ユーザーの場合、この設定は読み取り専用として表示されます。
認証を要求（Authentication Required）	認証を義務付けるには、このチェックボックスをオンにして、[パスワード（Password）] フィールドと [パスワードを再入力（Reenter Password）] フィールドにパスワードを入力し、適切なプロトコルを選択します。 パスワードには 8 文字以上が必要です。 （注） FIPS モードまたは拡張セキュリティ モードが有効になっている場合は、プロトコルとして [SHA]を選択します。
プライバシーを要求（Privacy Required）	[認証を要求（Authentication Required）] チェックボックスをオンにした場合は、プライバシー情報を指定できます。 プライバシーを義務付けるには、このチェックボックスをオンにして、[パスワード（Password）] フィールドと [パスワードを再入力（Reenter Password）] フィールドにパスワードを入力し、プロトコルのチェックボックスをオンにします。 パスワードには 8 文字以上が必要です。 （注） FIPS モードまたは拡張セキュリティ モードが有効になっている場合は、プロトコルとして [AES128]を選択します。
任意のホストからのSNMPパケットを受け入れる（Accept SNMP Packets from any host）	任意のホストからのSNMPパケットを受け入れるには、このオプション ボタンをクリックします。

フィールド	説明
指定したホストからのSNMPパケットのみ受け入れる（Accept SNMP Packets only from these hosts）	特定のホストからのSNMPパケットを受け入れるには、このオプション ボタンをクリックします。 [ホスト名/IPv4/IPv6 アドレス（Hostname/IPv4/IPv6 Address）] フィールドに、SNMP パケットを受け取る IPv4 または IPv6 アドレスを入力し、[挿入（Insert）]をクリックします。 IPv4 アドレスはドット付き 10 進表記です。 たとえば、10.66.34.23 と指定します。 IPv6 アドレスはコロンで区切られた 16 進表記です。 たとえば、2001:0db8:85a3:0000:0000:8a2e:0370:7334 または 2001:0db8:85a3::8a2e:0370:7334 と指定します。 SNMPパケットを受け取るアドレスごとにこのプロセスを繰り返します。 アドレスを削除するには、それを [ホスト IPv4/IPv6 アドレス（Host IPv4/IPv6 Addresses）] リスト ボックスから選択し、[削除（Remove）]をクリックします。
アクセス権限（Access Privileges）	ドロップダウン リスト ボックスから、アクセス レベルとして次のいずれかのオプションを選択します。 **ReadOnly** MIB オブジェクトの値の読み取りのみが可能です。 **ReadWrite** MIB オブジェクトの値の読み取りおよび書き込みが可能です。 **ReadWriteNotify** MIBオブジェクトの値の読み取りおよび書き込みと、トラップおよびインフォーム メッセージの MIB オブジェクト値の送信が可能です。 **NotifyOnly** トラップおよびインフォーム メッセージの MIB オブジェクト値の送信のみ可能です。 **ReadNotifyOnly** MIBオブジェクトの値の読み取りと、トラップおよびインフォーム メッセージの値の送信も可能です。 **None** トラップ情報の読み取り、書き込み、送信を行えません。 **ヒント** トラップ設定パラメータを変更するには、NotifyOnly、ReadNotifyOnly、または ReadWriteNotify 権限でユーザーを設定します。

フィールド	説明
すべてのノードに適用（Apply to All Nodes）	クラスタ内のすべてのノードにユーザ設定を適用する場合は、このチェックボックスをオンにします。 これは、Unified Communications Manager と IM and Presence Service クラスタにのみ適用されます。

Remote SNMP Engine ID の取得

SNMP V3 を導入している場合は、次の手順を使用して、通知先の設定に必要なリモート SNMP エンジン ID を取得します。

（注） Snmp V3 の場合は、この手順は必須ですが、SNMP V1 または 2C の場合は省略できます。

手順

ステップ 1 コマンドライン インターフェイスにログインします。

ステップ 2 `utils snmp walk 1` CLI コマンドを実行します。

ステップ 3 設定されているコミュニティ文字列 (SNMP V1/V2) または設定されたユーザ (SNMP V3) を入力します。

ステップ 4 サーバーの IP アドレスを入力します。 たとえば、localhost の場合は `127.0.0.1` を入力します。

ステップ 5 オブジェクト ID (OID) として `1.3.6.1.6.3.10.2.1.1.0` を入力します。

ステップ 6 ファイルの場合は、`file` を入力します。

ステップ 7 `y` と入力します。
システム出力である 16 進数文字列は、リモート SNMP エンジン ID を表します。

ステップ 8 SNMP が実行されている各ノードでこの手順を繰り返します。

次のタスク

SNMP 通知先の設定 （210 ページ）

SNMP 通知先の設定

この手順を使用して、SNMP トラップおよび通知を送信する通知先を設定します。 この手順は、SNMP V1、V2c、または V3 のいずれかでも使用することができます。

始める前に

SNMP コミュニティ ストリングあるいは SNMP ユーザーが未設定の場合、以下のいずれかのタスクを実行します。

- SNMP V1/V2 については、以下を参照してください。 SNMP コミュニティ ストリングの設定 （203 ページ）
- SNMP V3 については、以下を参照してください。 SNMP ユーザの設定 （206 ページ）

手順

ステップ 1 Cisco Unifeid Serviceability で、以下のいずれかを選択します。

- SNMP V1 または V2の場合、**SNMP** > **V1 または V2** > **通知先**を選択します
- SNMP V3 の場合、**SNMP** > **V3** > **通知先**を選択します

ステップ 2 **サーバ** を選択して、**検索** をクリックして、既存の SNMP 通知先を検索します。 必要に応じて、検索パラメータを入力して特定の通知先を検索することができます。

ステップ 3 次のいずれかを実行します。

- 既存の SNMP 通知先を編集するには、通知先を選択します。
- 新しい SNMP 通知先を追加するには、[新規追加（Add New）]をクリックします。

（注） 既存の SNMP 通知先を削除するには、通知先を選択して、**選択したものを削除する**をクリックします。 ユーザーを削除したら、**Cisco SNMP マスターエージェント**を再起動します。

ステップ 4 **ホスト IP アドレス** ドロップダウンで、既存のアドレスを選択するか、**新規追加** をクリックして、新しいホスト IP アドレスを入力します。

ステップ 5 SNMP V1、V2 のみ。 SNMP V1 あるいは V2c を設定する場合、いずれかに応じて、**SNMP バージョン** フィールドで、V1 あるいは V2C オプション ボタンをオンにします。

ステップ 6 SNMP V1 または V2 の場合は、以下の手順を実行します。

a) SNMP V2 のみ。 **通知タイプ** ドロップダウンで、**通知** あるいは **トラップ**を選択します。
b) 設定した**コミュニティ ストリング** を選択します。

ステップ 7 SNMP V3 の場合は、以下の手順を実行します。

a) **通知タイプ** ドロップダウンで、**通知** あるいは **トラップ**を選択します。
b) **リモート SNMP エンジン ID** ドロップダウンで、既存のエンジン ID を選択するか、**新規追加** を選択して、新しい ID を入力します。
c) **セキュリティ レベル** ドロップダウンで、適切なセキュリティ レベルを割り当てます。

ステップ 8 この設定をすべてのクラスタ ノードに適用する場合、**すべてのノードに適用する** チェック ボックスをオンにします。

ステップ 9 [挿入（Insert）]をクリックします。

ステップ 10　**OK** をクリックして、SNMP マスター エージェントを再起動します。

例

（注）　[通知先の設定] ウィンドウのフィールドの説明については、以下のトピックのいずれかを参照してください。

- SNMP V1 および V2c の通知先の設定 （212 ページ）
- SNMP V3 の通知先の設定 （214 ページ）

次のタスク

MIB2 システム グループの設定 （215 ページ）

SNMP V1 および V2c の通知先の設定

次の表では、SNMP V1/V2c の通知先の構成時の設定について説明します。

表 *31 : SNMP V1/V2c* の通知先の構成時の設定

フィールド	説明
サーバ（Server）	通知先を検索するための操作ですでにサーバーを指定済みのため、この設定は読み取り専用として表示されます。 通知先のサーバーを変更するには、コミュニティストリングを検索するための手順を実行します。
ホスト IPv4/IPv6 アドレス（Host IPv4/IPv6 Addresses）	ドロップダウン リスト ボックスから、トラップ宛先のホストの IPv4/IPv6 アドレスを選択するか、[新規追加（Add New）]をクリックします。 [新規追加（Add New）]をクリックした場合は、[ホスト IPv4/IPv6 アドレス（Host IPv4/IPv6 Address）] フィールドにトラップ宛先の IPv4/IPv6 アドレスを入力します。 既存の通知先の場合、ホストの IP アドレスの設定は変更できません。
ホスト IPv4/IPv6 アドレス（Host IPv4/IPv6 Address）	このフィールドに、SNMP パケットを受け取る IPv4 または IPv6 アドレスを入力します。 IPv4 アドレスはドット付き 10 進表記です。 たとえば、10.66.34.23 と指定します。 IPv6 アドレスはコロンで区切られた 16 進表記です。 たとえば、2001:0db8:85a3:0000:0000:8a2e:0370:7334 または 2001:0db8:85a3::8a2e:0370:7334 と指定します。

フィールド	説明
ポート番号（Port Number）	フィールドに、SNMPパケットを受信する宛先サーバー上の通知を受け取るポート番号を入力します。
V1 または V2c（V1 or V2c）	[SNMPバージョン情報（SNMP Version Information）] ペインで、適切な SNMP バージョンのオプション ボタン（[V1] または [V2c]）をクリックします。これは使用しているSNMPのバージョンによります。 • [V1]を選択した場合は、コミュニティ ストリングを設定します。 • [V2c]を選択した場合は、通知タイプを設定してからコミュニティ ストリングを設定します。
コミュニティ ストリング（Community String）	ドロップダウン リスト ボックスから、このホストで生成される通知メッセージに使用するコミュニティ ストリング名を選択します。 最小限の通知権限（ReadWriteNotify または Notify Only）を持つコミュニティ ストリングのみが表示されます。 これらの権限を持つコミュニティ ストリングを設定していない場合、ドロップダウン リスト ボックスに選択肢が表示されません。 必要に応じて、[新規コミュニティ ストリングの作成（Create New uiCommunity String）]をクリックしてコミュニティ ストリングを作成します。 IM and Presence のみ：最小限の通知権限（ReadWriteNotify、ReadNotifyOnly、または Notify Only）を持つコミュニティ ストリングのみが表示されます。 これらの権限を持つコミュニティ ストリングを設定していない場合、ドロップダウン リスト ボックスに選択肢が表示されません。 必要に応じて、[新規コミュニティ ストリングの作成（Create New Community String）]をクリックしてコミュニティ ストリングを作成します。
通知の種類（Notification Type）	ドロップダウン リスト ボックスから適切な通知タイプを選択します。
すべてのノードに適用（Apply to All Nodes）	クラスタ内のすべてのノードに通知先の設定を適用する場合は、このチェックボックスをオンにします。 これは、Cisco Unified Communications Manager および IM and Presence Service クラスタにのみ適用されます。

SNMP V3 の通知先の設定

次の表では、SNMP V3 の通知先の構成時の設定について説明します。

表 *32 : SNMP V3* の通知先の構成時の設定

フィールド	説明
サーバ（Server）	SNMP V3 の通知先を検索するための操作ですでにサーバーを指定済みのため、この設定は読み取り専用として表示されます。 通知先のサーバーを変更するには、SNMP V3 の通知先を検索するための手順を実行し、別のサーバーを選択します。
ホスト IPv4/IPv6 アドレス（Host IPv4/IPv6 Addresses）	ドロップダウン リスト ボックスから、トラップ宛先のホストの IPv4/IPv6 アドレスを選択するか、[新規追加（Add New）]をクリックします。 [新規追加（Add New）]をクリックした場合は、[ホスト IPv4/IPv6 アドレス（Host IPv4/IPv6 Address）] フィールドにトラップ宛先の IPv4/IPv6 アドレスを入力します。 既存の通知先の場合、ホストの IP アドレスの設定は変更できません。
ホスト IPv4/IPv6 アドレス（Host IPv4/IPv6 Address）	このフィールドに、SNMP パケットを受け取る IPv4 または IPv6 アドレスを入力します。 IPv4 アドレスはドット付き 10 進表記です。 たとえば、10.66.34.23 と指定します。 IPv6 アドレスはコロンで区切られた 16 進表記です。 たとえば、2001:0db8:85a3:0000:0000:8a2e:0370:7334 または 2001:0db8:85a3::8a2e:0370:7334 と指定します。
ポート番号（Port Number）	フィールドに、宛先サーバー上の通知を受け取るポート番号を入力します。
通知の種類（Notification Type）	ドロップダウン リスト ボックスから [インフォーム（Inform）]または [トラップ（Trap）] を選択します。 **ヒント** [インフォーム（Inform）] オプションを選択することを推奨します。 通知機能では、受信確認されるまでメッセージが再送されるため、トラップよりも信頼性が高くなります。
リモート SNMP エンジン ID（Remote SNMP Engine Id）	この設定は、[通知の種類（Notification Type）] ドロップダウン リスト ボックスから [インフォーム（Inform）] を選択した場合に表示されます。 ドロップダウン リスト ボックスからエンジン ID を選択するか、[新規追加（Add New）]を選択します。 [新規追加（Add New）] を選択した場合は、[リモート SNMP エンジン ID（Remote SNMP Engine Id）] フィールドに 16 進数値で ID を入力します。

フィールド	説明
セキュリティ レベル（Security Level）	ドロップダウン リスト ボックスからユーザーに対する適切なセキュリティレベルを選択します。 **noAuthNoPriv** 認証もプライバシーも設定しません。 **authNoPriv** 認証を設定しますが、プライバシーは設定しません。 **authPriv** 認証とプライバシーを設定します。
[ユーザ情報（User Information）] ペイン	ペインから、次のいずれかのタスクを実行し、通信先とユーザーの間の関連付けを設定または解除します。 1. 新しいユーザーを作成するには、**[新規ユーザーの作成（Create New User）]** をクリックします。 2. 既存のユーザーを変更するには、ユーザーのオプションボタンをクリックしてから、**[選択したユーザーの更新（Update Selected User）]** をクリックします。 3. ユーザーを削除するには、ユーザーのオプションボタンをクリックしてから、**[選択したユーザーの削除（Delete Selected User）]** をクリックします。 表示されるユーザーは、通知先に設定したセキュリティレベルに応じて変化します。
すべてのノードに適用（Apply to All Nodes）	クラスタ内のすべてのノードに通知先の設定を適用する場合は、このチェックボックスをオンにします。 これは、Cisco Unified Communications Manager および IM and Presence Service クラスタにのみ適用されます。

MIB2 システム グループの設定

以下の手順で、MIB-II システム グループのシステム コンタクトおよびシステム ロケーションを設定します。 たとえば、システムの連絡先として「管理者、 555-121-6633」と入力し、システム ロケーションとして「San Jose, Bldg 23, 2nd floor」と入力することができます。 この手順は、SNMP V1、V2、および V3 に対して使用できます。

手順

ステップ 1 Cisco Unified Serviceabilityで、**SNMP** > **SystemGroup** > **MIB2 システム グループ**を選択します。
ステップ 2 **サーバ** ドロップダウンで、ノードを 1 つ選択して、**移動**をクリックします。

ステップ 3 **システムの連絡先** および **システム ロケーション** フィールドの設定を完了します。

ステップ 4 この設定をすべてのクラスタ ノードに適用する場合、**すべてのノードに適用する** チェック ボックスをオンにします。

ステップ 5 **[保存]** をクリックします。

ステップ 6 **OK** をクリックして、SNMP マスター エージェント サービスを再起動します。

例

（注） フィールドの説明のヘルプは、以下を参照してください MIB2 システム グループの設定 （216 ページ）

（注） フィールドをクリアするには、**すべてクリア** をクリックします。 **すべてクリア** をクリックした後、**保存**をクリックすると、該当の記録が削除されます。

MIB2 システム グループの設定

次の表で、MIB2 システム グループの構成時の設定について説明します。

表 *33 : MIB2* システム グループの構成時の設定

フィールド	説明
サーバ（Server）	ドロップダウン リスト ボックスからコンタクトを設定するサーバーを選択し、**[移動（Go）]** をクリックします。
システム管理者（System Contact）	問題が発生したときに知らせる人を入力します。
システムの場所（System Location）	システム コンタクトとして識別される人の場所を入力します。
すべてのノードに適用（Apply to All Nodes）	システム設定をクラスタ内のすべてのノードに適用するには、このチェック ボックスをオンにします。 これは、Unified Communications Manager と IM and Presence Service クラスタにのみ適用されます。

CISCO-SYSLOG-MIB トラップ パラメータ

システムの CISCO-SYSLOG-MIB トラップ設定を行う場合は次のガイドラインを使用してください。

- SNMP Set 操作を使用して、clogsNotificationEnabled（1.3.6.1.4.1.9.9.41.1.1.2）を True に設定します。たとえば、次のように Linux コマンドラインから net-snmp set ユーティリティを使用してこの OID を True に設定します。

```
snmpset -c <community string>-v2c <transmitter ipaddress>
1.3.6.1.4.1.9.9.41.1.1.2.0 i 1
```

  SNMP Set 操作にはその他の SNMP 管理アプリケーションを使用することもできます。

- SNMP Set 操作を使用して clogMaxSeverity（1.3.6.1.4.1.9.9.41.1.1.3）値を設定します。たとえば、次のように Linux コマンドラインから net-snmp set ユーティリティを使用してこの OID 値を設定します。

```
snmpset-c public-v2c <transmitter ipaddress> 1.3.6.1.4.1.9.9.41.1.1.3.0 i
<value>
```

  <value> 設定には重大度の数値を入力します。 値が大きくなるほど、重大度は低くなります。 値 1（緊急）は最も高い重大度を表し、値 8（デバッグ）は最も低い重大度を表します。 Syslog Agent では、指定した値よりも大きいメッセージは無視されます。たとえば、すべての Syslog メッセージをトラップする場合は値 8 を使用します。

  重大度の値は次のとおりです。

  - 1：緊急
  - 2：アラート
  - 3：重大
  - 4：エラー
  - 5：警告
  - 6：通知
  - 7：情報
  - 8：デバッグ

  SNMP Set 操作にはその他の SNMP 管理アプリケーションを使用することもできます。

（注） 指定されている Syslog バッファ サイズよりも大きいトラップ メッセージ データは、ロギング前に Syslog によって切り捨てられます。 Syslog トラップ メッセージの長さの制限は 255 バイトです。

CISCO-CCM-MIB トラップ パラメータ

- SNMP Set 操作を使用して、ccmPhoneFailedAlarmInterval（1.3.6.1.4.1.9.9.156.1.9.2）を 30 ～ 3600 の範囲の値に設定します。たとえば、次のように Linux コマンドラインから net-snmp set ユーティリティを使用してこの OID 値を設定します。

```
snmpset -c <community string> -v2c <transmitter ipaddress>
1.3.6.1.4.1.9.9.156.1.9.2 .0 i <value>
```

  SNMP Set 操作にはその他の SNMP 管理アプリケーションを使用することもできます。

- SNMP Set 操作を使用して、ccmPhoneStatusUpdateAlarmInterval（1.3.6.1.4.1.9.9.156.1.9.4）を 30 ～ 3600 の範囲の値に設定します。たとえば、次のように Linux コマンドラインから net-snmp set ユーティリティを使用してこの OID 値を設定します。

```
snmpset -c <community string> -v2c <transmitter ipaddress>
1.3.6.1.4.1.9.9.156.1.9.4.0 i <value>
```

  SNMP Set 操作にはその他の SNMP 管理アプリケーションを使用することもできます。

CISCO-UNITY-MIB トラップ パラメータ

Cisco Unity Connection のみ：Cisco Unity Connection SNMP エージェントはトラップ通知を有効化しませんが、トラップは Cisco Unity Connection アラームによってトリガーできます。 Cisco Unity Connection のアラーム定義は、Cisco Unity Connection Serviceability の **[アラーム（Alarm）]** > **[定義（Definitions）]** 画面で確認できます。

CISCO-SYSLOG-MIB を使用してトラップ パラメータを設定できます。

関連トピック

CISCO-SYSLOG-MIB トラップ パラメータ （217 ページ）

SNMP Master Agent の再起動

すべての SNMP 設定を完了したら、SNMP Master Agent 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）]** > **[コントロールセンター-ネットワークサービス（Control Center - Network Services）]** の順に選択します。

ステップ 2 **サーバ** を選択して、**移動**をクリックします。

ステップ 3 **SNMP Master Agent** を選択します。

ステップ 4 **再起動（Restart）**をクリックします。

SNMP トラップの設定

設定可能な SNMP トラップ設定を行うには、CLI コマンドを使用します。 SNMP トラップの設定パラメータと推奨される設定のヒントは、CISCO-SYSLOG-MIB、CISCO-CCM-MIB、および CISCO-UNITY-MIB で提供されています。

SNMP トラップの設定

SNMP トラップを設定するには、以下の手順を実行します。

始める前に

SNMP用のシステム設定詳細については、SNMP設定タスク フロー （201ページ）を参照してください。

SNMP コミュニティ ストリング（SNMP V1 または V2 の場合）あるいは SNMP ユーザ（SNMP V3 の場合）の **アクセス権限** が以下のいずれかに設定されていることを確認します。**ReadWriteNotify**、**ReadNotify**、**NotifyOnly**。

手順

ステップ 1 CLI にログインし、`utils snmp test` CLI コマンドを実行して、SNMP が実行されていることを確認します。

ステップ 2 SNMP トラップの生成 （219 ページ） に従って、SNMP トラップ を生成します（たとえば、ccmPhoneFailed または MediaResourceListExhausted トラップなど）。

ステップ 3 トラップが生成されない場合は、次の手順を実行します。

- Cisco Unified Serviceability で、**[アラーム（Alarm）] > [設定（Configuration）]** を選択し、[CM サービス（CM Services）]および [Cisco CallManager]を選択します。
- [すべてのノードに適用（Apply to All Nodes）] チェックボックスをオンにします。
- [ローカル Syslog（Local Syslogs）] で、[アラーム イベント レベル（Alarm Event Level）] ドロップダウン リスト ボックスを [情報（Informational）]に設定します。

ステップ 4 トラップを再現し、対応するアラームが CiscoSyslog ファイルに記録されるかどうかを確認します。

SNMP トラップの生成

ここでは、特定のタイプの SNMP トラップを生成するためのプロセスについて説明します。個別のトラップを生成するために、SNMP をサーバー上でセットアップし、実行する必要があります。 SNMP トラップを生成するためのシステムのセットアップ方法については、SNMP トラップの設定 （219 ページ） の指示に従ってください。

（注） 個々の SNMP トラップの処理時間は、生成しようとしているトラップによって異なります。一部の SNMP トラップは、生成するために最大で数分がかかる場合があります。

表 *34 : SNMP* トラップの生成

SNMP トラップ	プロセス
ccmPhoneStatusUpdate	ccmPhoneStatusUpdate トラップをトリガーするには： **1.** ccmAlarmConfig Info mib テーブルで、ccmPhoneStatusUpdateAlarmInterv (1.3.6.1.4.1.9.9.156.1.9.4) = 30 以上に設定します。 **2.** Cisco Unified Communications Manager の管理 にログインします。 **3.** Unified Communications Manager に登録され、稼働中の電話機の場合は、電話機をリセットします。 電話の登録が解除されるので、再登録すると ccmPhoneStatusUpdate トラップが生成されます。
ccmPhoneFailed	ccmPhoneFailed トラップをトリガーするには： **1.** ccmAlarmConfigInfo mib テーブルで、ccmPhoneFailedAlarmInterval (1.3.6.1.4.1.9.9.156.1.9.2) =30 以上に設定します。 **2.** Cisco Unified Communications Manager の管理 で、電話の MAC アドレスを無効な値に変更します。 **3.** Cisco Unified Communications Manager の管理 で、電話機の再登録を行います。 **4.** TFTP サーバー A を指すように電話を設定し、別のサーバーに電話を差し込みます。
ccmGatewayFailed	ccmGatewayFailed SNMP トラップをトリガーするには： **1.** ccmGatewayAlarmEnable (1.3.6.1.4.1.9.9.156.1.9.6) が true に設定されていることを確認します。 **2.** Cisco Unified Communications Manager の管理 で、ゲートウェイの MAC アドレスを無効な値に変更します。 **3.** ゲートウェイをリブートします。

SNMP トラップ	プロセス
ccmGatewayLayer2Change	レイヤ2がモニタされている動作中のゲートウェイ（MGCPバックホール ロードなど）で ccmGatewayLayer2Change トラップをトリガーするには： 1. ccmAlarmConfig Info mib テーブルで、ccmGatewayAlarmEnable (1.3.6.1.4.1.9.9.156.1.9.6.0) = true に設定します。 2. Cisco Unified Communications Manager の管理 で、ゲートウェイの MAC アドレスを無効な値に変更します。 3. ゲートウェイをリセットします。
MediaResourceListExhausted	MediaResourceListExhausted トラップをトリガーするには： 1. Cisco Unified Communications Manager の管理 で、標準会議ブリッジリソース（CFB-2）のいずれかを含むメディア リソース グループを作成します。 2. 作成したメディア リソース グループを含むメディア リソース グループ リストを作成します。 3. [電話の設定] ウィンドウで、作成したメディア リソース グループ リストを、メディア リソース グループ リストに設定します。 4. IP Voice Media Streaming サービスを停止します。 このアクションにより、ConferenceBridge リソース（CFB-2）が動作を停止します。 5. メディア リソース グループ リストを使用する電話で電話会議を行います。 「使用可能な会議ブリッジがありません（No Conference Bridge available）」というメッセージが電話画面に表示されます。
RouteListExhausted	RouteListExhausted トラップをトリガーするには： 1. ゲートウェイを 1 つ含むルート グループを作成します。 2. 作成したルート グループを含むルート グループ リストを作成します。 3. ルート グループ リストを使用してコールをルーティングする固有のルート パターンを作成します。 4. ゲートウェイの登録を解除します。 5. いずれかの電話から、ルート パターンに一致する番号に電話をかけます。

SNMP トラップ	プロセス
MaliciousCallFailed	MaliciousCallFailed トラップをトリガーするには： **1.** すべての使用可能な「MaliciousCall」ソフトキーを含むソフトキー テンプレートを作成します。 **2.** 新しいソフトキーテンプレートをネットワークの電話に割り当てて、電話をリセットします。 **3.** 電話間で電話をかけます。 **4.** コール中に、「MaliciousCall」ソフトキーを選択します。
ccmCallManagerFailed	**1.** `show process list` CLI コマンドを実行して、CallManager アプリケーション ccm のプロセス ID（PID）を取得します。 このコマンドは、多くのプロセスとその PID を返します。 具体的には、ccm の PID を取得する必要があります。アラームを生成するにはこの PID を停止する必要があるためです。 **2.** `delete process<pid>` crash の CLI コマンドを実行します **3.** CLI コマンドを実行します。 CallManager 障害アラームは、内部エラーが発生すると生成されます。 内部エラーには、CPU の不足による内部スレッドの終了、16 秒を超える CallManager サーバーの停止、タイマーの問題などがあります。 このアラームを手動で生成することはできません。 （注） ccmCallManagerFailed アラームまたはトラップを生成して CallManager サービスをシャット ダウンし、コア ファイルを生成します。 混乱を避けるために、コア ファイルはすぐに削除することを推奨します。

SNMP トラップ	プロセス
トラップとしての syslog メッセージ	特定の重大度を超える syslog メッセージをトラップとして受信するには、clogBasic テーブルで次の 2 つの MIB オブジェクトを設定します。 1. clogNotificationsEnabled (1.3.6.1.4.1.9.9.41.1.1.2) を true（1）に設定します。デフォルト値は false（2）です。たとえば、snmpset -c <Community String> -v 2c <transmitter ip address> 1.3.6.1.4.1.9.9.41.1.1.2.0 i 1 2. clogMaxSeverity (1.3.6.1.4.1.9.9.41.1.1.3) を、トラップを生成するレベルよりも大きいレベルに設定します。デフォルト値は警告（5）です。 設定された重大度レベル以下のアラーム重大度を持つすべての syslog メッセージがトラップとして送信されます。 たとえば、snmpset -c <Community String> -v 2c <transmitter ip address> 1.3.6.1.4.1.9.9.41.1.1.3.0 i <value>

SNMP トレースの設定

Unified Communications Manager の場合、Cisco CallManager SNMP エージェントのトレースを設定するには、Cisco Unified Serviceability の [トレース設定] ウィンドウで、[パフォーマンスおよびモニタリング サービス] サービス グループの [Cisco CallManager SNMP サービス] を選択します。 デフォルトの設定は、すべてのエージェントに対して存在します。 Cisco CDP Agent および Cisco Syslog Agent の場合、『*Command Line Interface Reference Guide for Cisco Unified Solutions*』に従って、CLI を使用してトレース設定を変更します。

Cisco Unity Connection の場合、Cisco Unity Connection SNMP エージェントのトレースを設定するには、Cisco Unity Connection Serviceability の [トレース設定（Trace Configuration）] ウィンドウで Connection SNMP エージェントのコンポーネントを選択します。

SNMP のトラブルシューティング

トラブルシューティングのヒントについては、この項を参照してください。 すべての機能サービスとネットワーク サービスが動作していることを確認してください。

問題

システムから MIB をポーリングできない

この状態は、コミュニティストリングまたはSNMPユーザーがシステム上に設定されていないか、システム上に設定されているものと一致しないことを意味します。 デフォルトでは、コミュニティストリングまたはユーザーはシステムに設定されていません。

ソリューション

SNMPの設定ウィンドウを使用して、コミュニティストリングまたはSNMPユーザーがシステム上に適切に設定されているかどうかを確認します。

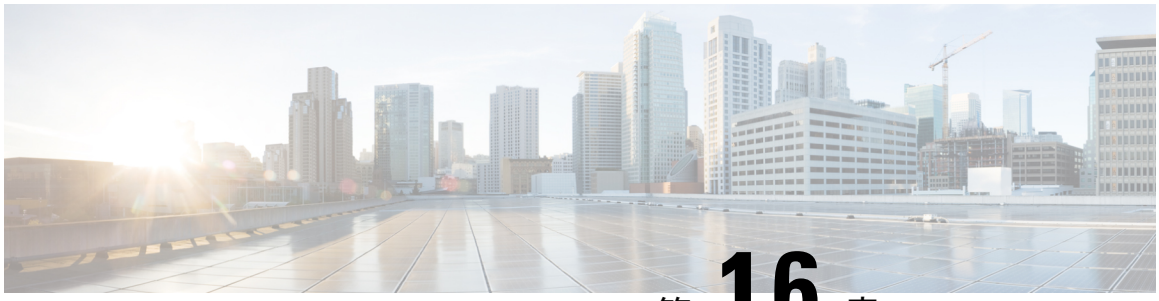
問題

システムから通知を受信できない。

この状態は、通知の宛先がシステム上に正しく設定されていないことを意味します。

ソリューション

[通知先（Notification Destination）]（V1/V2cまたはV3）設定ウィンドウで、通知の宛先を正しく設定したことを確認します。



第 16 章

サービス

機能サービス

Cisco Unified Communications Manager および IM and Presence Service のアクティブ化、開始、停止を行うには、Serviceability GUI を使用します。 アクティブ化すると、サービスが有効になり、開始されます。 使用するすべての機能について、手動で機能サービスをアクティブ化する必要があります。 サービスのアクティブ化に関する推奨事項については、サービスのアクティブ化に関するトピックを参照してください。

（注） IM and Presence ノードから Unified Communications Manager サーバーにアクセスしようとした場合、またはその逆を行おうとした場合、以下のエラーが発生することがあります：「サーバーへの接続が確立できません（リモートノードにアクセスできません）」。 このエラーメッセージが表示された場合は、『*Administration Guide for Cisco Unified Communications Manager*』を参照してください。

（注） IM and Presence を使用したデバイスは、常設チャット、コンプライアンス、およびファイル転送をサポートするために Postgres 外部データベースを使用するように設定されます。 ただし、IM and Presence サーバーと Postgres 間の接続は保護されず、データはチェックなしで通過します。 TLS をサポートしないサービスまたはデバイスの場合は、IP Sec を設定することによってセキュア通信を提供する別の方法があります。この方法は、通信セッションの IP パケットごとに認証と暗号化を行うことによるセキュア通信用の標準プロトコルです。

[サービスの開始（Service Activation）]ウィンドウでサービスをアクティブ化した後、[コントロール センター - 機能サービス（Control Center - Feature Services）]ウィンドウでサービスを起

動する必要はありません。 サービスが何らかの理由で起動しなければ、[コントロール センター - 機能サービス（Control Center - Feature Services）]ウィンドウで起動する必要があります。

システムがインストールされた後、機能サービスは自動的にアクティブ化されません。サービスアビリティ レポートのアーカイブ機能などの設定機能を使用するには、機能サービスをアクティブ化する必要があります。

Unified Communications Manager および Cisco Unified IM and Presence Service のみ：Unified Communications Manager をアップグレードする場合、アップグレード前にシステムで有効化されているていたこれらのサービスは、アップグレード後に自動的に起動します。

機能サービスをアクティブ化した後、製品の管理 GUI を使用してサービス パラメータ設定を変更できます。

- Cisco Unified Communications Manager Administration
- Cisco Unity Connection Administration

機能サービスのカテゴリ

Cisco Unified Serviceability では、**[サービスの開始（Service Activation）]** ウィンドウと **[コントロール センター - 機能サービス（Control Center - Feature Services）]** ウィンドウは機能サービスを次のグループに分類しています。

- データベースおよび管理サービス
- パフォーマンスおよびモニタリング サービス
- CM サービス
- CTI サービス
- CDR サービス
- セキュリティ サービス
- ディレクトリ サービス
- Voice Quality Reporter サービス

Cisco Unified IM and Presence Serviceability では、**[サービスの開始（Service Activation）]** ウィンドウと **[コントロール センター - 機能サービス（Control Center - Feature Services）]** ウィンドウは機能サービスを次のグループに分類しています。

- データベースおよび管理サービス
- パフォーマンスおよびモニタリング サービス
- IM and Presence Service サービス

データベースおよび管理サービス

Locations Bandwidth Manager

このサービスは、IM and Presence Service ではサポートされません。

Locations Bandwidth Manager サービスは、1 つ以上のクラスタで設定されているロケーションとリンク データからネットワーク モデルを組み立て、2つのロケーション間の有効なパスを決定し、コールのタイプごとの帯域幅の可用性に基づいて2つのロケーション間のコールを許可するかどうかを決定し、許可された各コールの実行期間の帯域幅を差し引きます（予約します）。

Cisco AXL Web Service

Cisco AXL Web Service を使用すると、データベース エントリを変更し、AXL を使用するクライアント ベースのアプリケーションからストアド プロシージャを実行することができます。

IM and Presence Service システムでは、このサービスは Unified Communications Managerと Cisco Unity Connection の両方をサポートします。

Cisco UXL Web サービス

このサービスは、IM and Presence Service ではサポートされません。

Cisco IP 電話Address Book Synchronizer の TabSync クライアントは、Unified Communications Manager データベースに対するクエリーに Cisco UXL Web サービスを使用します。これにより、Cisco IP 電話Address Book Synchronizer ユーザーは自身に関連するエンドユーザーデータのみにアクセスすることになります。 Cisco UXL Web サービスは、次の機能を実行します。

- エンドユーザーが Cisco IP 電話 Address Book Synchronizer にログインするときにエンドユーザー名とパスワードを確認することにより、認証チェックを行います。
- コンタクトの一覧表示、取得、更新、削除、追加などの機能を実行するために現在 Cisco IP 電話Address Book Synchronizer にログインしているユーザだけを許可することにより、ユーザ許可チェックを行います。

Cisco Bulk Provisioning サービス

このサービスは、Cisco Unity Connection をサポートしていません。

設定でクラスタをサポートしている場合（Unified Communications Manager のみ）、Cisco Bulk Provisioning Service は 1 台目のサーバーでのみ有効化することができます。 Unified Communications Manager Bulk Administration Tool を使用して電話とユーザーを管理する場合は、このサービスを有効にする必要があります。

Cisco TAPS サービス

このサービスは、Cisco Unity Connection または IM and Presence Service をサポートしていません。

Auto-Registered Phones Support（TAPS）サービス用の Cisco ツールは Cisco Unified Communications Manager Auto-Register Phone Tool をサポートしているため、音声自動レスポンス装置（IVR）プロンプトにユーザーが応答した後、カスタマイズされた設定を自動登録済みの電話にアップロードできます。

クラスタをサポートする設定にした場合（Unified Communications Manager のみ）、最初のサーバーでこのサービスを有効にします。 ツール用にダミーの MAC アドレスを作成する場合、Cisco Bulk Provisioning サービスが同じサーバー上でアクティブ化されていることを確認します。

ヒント　Cisco Unified Communications Manager Auto-Register Phone Tool は Cisco Customer Response Solutions（CRS）に依存します。 ツールが設計どおりに動作できるようにするには、CRS マニュアルで説明されているように CRS サーバーを設定し、実行していることを確認します。

Platform Administrative Web サービス

Platform Administrative Web サービスとは、Unified Communications Manager、IM and Presence Service、Cisco Unity Connection システムでアクティブ化され PAWS-M サーバーがシステムをアップグレードできるようにすることが可能な Simple Object Access Protocol（SOAP）API です。

重要　PAWS-M サーバーで Platform Administrative Web サービスをアクティブ化しないでください。

Performance and monitoring services

Cisco Serviceability Reporter

Cisco Serviceability Reporter サービスは、日次レポートを生成します。 詳細については、Serviceability レポートのアーカイブに関連するトピックを参照してください。

クラスタをサポートする設定の場合（Unified Communications Manager のみ）、このサービスはクラスタ内のすべての Unified Communications Manager サーバーにインストールされます。 Reporter は、ログに記録された情報に基づいてレポートを 1 日 1 回生成します。 Reporter が生成したレポートには、Cisco Unified Serviceability の [ツール（Tools）] メニューからアクセスできます。 各要約レポートは、特定のレポートの統計を示すさまざまなチャートで構成されます。 サービスをアクティブ化した後、レポートの生成に最大 24 時間かかる場合があります。

関連トピック

サービスアビリティ レポートのアーカイブ （331 ページ）

Cisco CallManager SNMP サービス

このサービスは、IM and Presence Service および Cisco Unity Connection をサポートしていません。

このサービスは、CISCO-CCM-MIB を実装し、Unified Communications Manager が使用できるプロビジョニングおよび統計情報に対する SNMP アクセスを提供します。

クラスタをサポートする設定にした場合（Unified Communications Manager のみ）、クラスタ内のすべてのサーバーでこのサービスを有効にします。

CM サービス

ここでは、CM サービスについて説明します。IM and Presence Service および Cisco Unity Connection には適用されません。

Cisco CallManager

Cisco CallManager Service は、ソフトウェアのみのコール処理、また、Unified Communications Manager のシグナリングおよびコール制御機能を提供します。

ヒント

Unified Communications Manager クラスタのみ：このサービスを有効化する前に、Cisco Unified Communications Manager 管理で、[Cisco Unified Communications Manager 検索および一覧表示] ウィンドウに Unified Communications Manager サーバーが表示されていることを確認してください。 サーバーが表示されていない場合、このサービスをアクティブ化する前に Unified Communications Manager サーバーを追加します。 サーバーを検索して追加する方法については、『*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。

Unified Communications Manager クラスタのみ：[Service Activation] で Cisco CallManager または CTIManager サービスを無効にした場合、サービスを無効にした Unified Communications Manager サーバーはデータベースに存在しなくなります。これは、グラフィカルユーザーインターフェイス（GUI）に表示されないため、[Cisco Unified Communications Manager の管理] で設定操作で、該当する Unified Communications Manager サーバーを選択できないことを意味します。 その後、同じ Unified Communications Manager サーバーのサービスを再度有効にすると、データベースに Unified Communications Manager のエントリが再作成され、サーバー名または IP アドレスに 「CM_」 プレフィックスが追加されます。たとえば、IP アドレスが 172.19.140.180 のサーバーで Cisco CallManager または CTIManager サービスを再度有効化した場合は、Cisco Unified Communications Manager の管理 に CM_172.19.140.180 と表示されます。 これで、新しく 「CM_」 プレフィックスが追加されたサーバーを Cisco Unified Communications Manager の管理 で選択できるようになりました。

次のサービスには、Cisco CallManager サービスのアクティブ化が必要です。

- CM サービス
- CDR サービス

Cisco TFTP

Cisco Trivial File Transfer Protocol（TFTP）は、トリビアル ファイル転送プロトコル（FTP の簡易バージョン）と整合性のあるファイルを構築し、提供します。 Cisco TFTP は、埋め込みコンポーネント実行ファイル、リンガー ファイル、デバイス コンフィギュレーション ファイルを提供します。

Unified Communications Manager のみ：設定ファイルには、デバイス（電話およびゲートウェイ）が接続する Unified Communications Manager のリストが含まれます。 デバイスをブートすると、コンポーネントは、Dynamic Host Configuration Protocol（DHCP）サーバーにそのネットワーク設定情報を照会します。 DHCP サーバーはデバイスの IP アドレス、サブネットマスク、デフォルトゲートウェイ、ドメインネームシステム（DNS）サーバーアドレスと TFTP サーバー名またはアドレスを返します。 デバイスが TFTP サーバーに設定ファイルをリクエストします。 設定ファイルには、Unified Communications Manager およびデバイスが Unified Communications Manager に接続する際に使用する TCP ポートのリストが含まれます。 設定ファイルには、Unified Communications Manager およびデバイスが Unified Communications Manager に接続する際に使用する TCP ポートのリストが含まれます。

Cisco Unified Mobile Voice Access Service

Cisco Unified Voice Access Service は、Cisco Unified Mobility 内のモバイル ボイスアクセス機能を起動します。モバイルボイスアクセスは自動音声レスポンス（IVR）システムで、この機能により Cisco Unified Mobility ユーザーは次のタスクを実行できます。

- コールがデスクの電話から発信されたかのように、携帯電話からコールを発信します。
- Cisco Unified Mobility を有効にします。
- Cisco Unified Mobility を無効にします。

Cisco IP Voice Media Streaming App

Cisco IP Voice Media Streaming Application サービスは、メディア ターミネーション ポイント（MTP）、会議、保留音（MoH）、およびアナンシエータに使用する音声メディア ストリーミング機能を Unified Communications Manager に提供します。 Cisco IP Voice Media Streaming Application は、Unified Communications Manager から、リアルタイム プロトコル（RTP）ストリーミングを処理する IP 音声メディア ストリーミング ドライバにメッセージをリレーします。

Cisco IP Voice Media Streaming Application サービスは、会議、MOH、アナンシエータ、MTP などの IP Voice Media Streaming Application コンポーネントを含むコール レッグの呼管理レコード（CMR）ファイルは生成しません。

Cisco CTIManager

Cisco CTI Manager には、アプリケーションと対話する CTI コンポーネントが含まれます。 このサービスは、アプリケーションのコール制御機能を実行するために電話および仮想デバイスをモニタまたは制御することもできます。

Unified Communications Manager クラスタのみ：CTI Manager を使用すると、アプリケーションはクラスタのすべての Unified Communications Manager のリソースおよび機能にアクセスすることができ、フェールオーバー機能が向上します。 1 つのクラスタでは 1 つまたは複数の CTI Manager をアクティブにできますが、個々のサーバーに置くことのできる CTI Manager は 1 つだけです。 1 つのアプリケーション（JTAPI/TAPI）を複数の CTI Manager に同時に接続できますが、1 つのアプリケーションがメディア ターミネーションを持つデバイスを開くために使用できる接続は、一度に 1 つだけです。

Cisco Extension Mobility

このサービスは エクステンション モビリティ 機能をサポートし、この機能に対するログインと自動ログアウト機能を実行します。

Cisco Dialed Number Analyzer

Dialed Number Analyzer サービスは、Unified Communications Manager Dialed Number Analyzer をサポートしています。アクティブ化すると、このアプリケーションによって大量のリソースが消費されるため、このサービスはコール処理の中断が最小限になるオフピーク時にのみ実行してください。

Cisco Unified Communications Manager クラスタの場合のみ：このサービスをクラスタ内のすべてのサーバーで有効化することは推奨されません。 このサービスは、コール処理作業が最も少ないクラスタのサーバーの 1 つでのみアクティブにすることを推奨します。

Cisco Dialed Number Analyzer Server

Cisco Dialed Number Analyzer Server サービスは Cisco Dialed Number Analyzer サービスとともに、Cisco Unified Communications Manager Dialed Number Analyzer をサポートします。 このサービスは、Cisco Dialed Number Analyzer サービス専用のノードでのみアクティブ化する必要があります。

Cisco Unified Communications Manager クラスタの場合のみ：このサービスをクラスタ内のすべてのサーバーで有効化することは推奨されません。 このサービスは、コール処理作業が最も少ないクラスタのサーバーの 1 つでのみアクティブにすることを推奨します。

Cisco DHCP Monitor サービス

Cisco DHCP Monitor サービスは、データベース テーブルで、IP 電話の IP アドレスの変更をモニタします。 変更が検出されると、/etc./dhcpd.conf ファイルを変更し、DHCPD デーモンを再起動します。

シスコ クラスタ間検索サービス

Intercluster Lookup Service（ILS）は、クラスタ全体をベースとして実行されます。 ILS を使用すると、リモートの Unified Communications Manager クラスタのネットワークを作成することができます。 ILS クラスタ検出機能を使用すると、管理者が各クラスタ間の接続を手動で設定しなくても、Cisco Unified Communications Manager からリモート クラスタに接続できるようになります。 ILS グローバル ダイヤル プラン レプリケーション機能は、ILS ネットワーク内の

クラスタがグローバル ダイヤル プラン データを ILS ネットワーク内の他のクラスタと交換できるようにします。

ILS の有効化は、Cisco Unified Communications Manager 管理で、**高度な機能** > **ILS 設定**を選択して、[ILS 設定]ウィンドウで行うことができます。

Cisco UserSync サービス

Cisco UserSync サービスは、Unified Communications Manager のエンド ユーザ テーブルのデータを LDAP データベースに同期します。

Cisco UserLookup Web Service

Cisco UserLookup Web Service は、商用コール（外部ゲートウェイ経由のコール）を着信側の内線の代替番号に転送して、外線番号に電話する際の商用コストがかからないようにします。

Unified Communications Manager ネットワーク内の発信者が外線番号にコールを発信する場合、Unified Communications Manager は内部番号が LDAP データベースの着信側に存在するかどうかを確認します。 内線番号がある場合、そのコールはその内線番号に転送されます。 LDAP データベースに内線番号がない場合は、そのコールは元の（外線の）番号に転送されます。

シスコ ヘッドセット サービス

互換性のある Cisco IP 電話、Cisco Jabber、またはその他の Cisco デバイスを使用している場合、Cisco Headset Service で、シスコ ヘッドセットのインベントリ、設定の更新、および診断データを管理することができます。

（注） Cisco CallManager サービスが既に実行されている場合は、すべてのユニファイド コミュニケーション マネージャ ノードでシスコ ヘッドセット サービスをアクティブにする必要があります。 Cisco Unified CM の管理インターフェイスを使用してヘッドセットを管理するには、ユニファイド コミュニケーション マネージャ ノード上でシスコ ヘッドセット サービスをアクティブにしてください。 Cisco CallManager サービスは、シスコ ヘッドセット サービスを有効にすると自動的にアクティブになります。 必要でない場合は、Cisco CallManager サービスを非アクティブにします。

IM and Presence Services

IM and Presence Service は IM and Presence Serviceだけに適用されます。

Cisco SIP Proxy

Cisco SIP Proxy サービスは、SIP レジストラとプロキシ機能を提供します。 これには、リクエストのルーティング、要求者の識別、および伝送の相互接続が含まれます。

Cisco Presence Engine

Cisco Presence Engine は標準ベースの SIP および SIMPLE インターフェイスを使用して、ユーザーの機能と属性を収集、集約、および配布します。 また、可用性ステータスとユーザの通信機能に関する情報を収集します。

Cisco XCP Text Conference Manager

Cisco XCP Text Conference Manager はチャット機能をサポートします。 チャット機能を使用すると、ユーザーは、オンラインチャットルームで互いにコミュニケートできます。アドホック（一時的）なチャットルームと、削除されるまでシスコがサポートしている外部データベースに保持される常設チャット ルームを使用したチャット機能がサポートされています。

Cisco XCP Web Connection Manager

Cisco XCP Web Connection Manager サービスでは、ブラウザベースのクライアントを IM and Presence Serviceに接続できます。

Cisco XCP Connection Manager

Cisco Unified Presence XCP Connection Manager は、Cisco Unified Presence サーバーに接続するために XMPP クライアントを有効にします。

Cisco XCP SIP Federation Connection Manager

Cisco XCP SIP Federation Connection Manager は、SIP プロトコル経由で Microsoft OCS を使用したドメイン間フェデレーションをサポートします。 展開に IM and Presence Service Release 9.0 クラスタと Cisco Unified Presence Release 8.6 クラスタとの間のクラスタ間接続が含まれる場合、このサービスもオンにする必要があります。

Cisco XCP XMPP Federation Connection Manager

Cisco XCP XMPP Federation Connection Manager は XMPP プロトコル経由での IBM Lotus Sametime、Cisco Webex Meetings Center、GoogleTalk などのサードパーティ エンタープライズとのドメイン間フェデレーション、および XMPP プロトコル経由での別の IM and Presence Service エンタープライズとのドメイン間フェデレーションをサポートします。

Cisco XCP Message Archiver

Cisco XCP Message Archiver サービスは、IM コンプライアンス機能をサポートします。 IM コンプライアンス機能は、ポイントツーポイントメッセージ、チャット機能のアドホック（一時的）なチャットルームと常設チャットルームからのメッセージなど、IM and Presence Service サーバーとの間で送受信したすべてのメッセージを記録します。 メッセージは、シスコによってサポートされる外部データベースに記録されます。

Cisco XCP Directory Service

Cisco XCP Directory サービスは XMPP クライアントと LDAP ディレクトリの統合をサポートし、ユーザが LDAP ディレクトリの連絡先を検索および追加できるようにします。

Cisco XCP Authentication Service

Cisco XCP Authentication Service は、IM and Presence Serviceに接続する XMPP クライアントからのすべての認証リクエストを処理します。

CTI サービス

ここでは、CTI サービスについて説明します。Cisco Unity Connection または IM and Presence Service には適用されません。

Cisco IP Manager Assistant

このサービスは、Cisco Unified Communications Manager Assistant をサポートしています。 サービスをアクティブ化すると、Cisco Unified Communications Manager Assistant によってマネージャとアシスタントがより効率的に連携できるようなります。 Cisco Unified Communications Manager Assistant は、プロキシ回線サポートと共有回線サポートという 2 種類の動作モードをサポートしています。

この機能は、コール ルーティング サービス、マネージャに対する電話機能の機能拡張、そして主にアシスタントによって使用されるデスクトップ インターフェイスで構成されています。

このサービスは、マネージャ宛てのコールを代行受信し、これを事前に設定されたコール フィルタに基づいて選択したアシスタント、マネージャ、または他の宛先にルーティングします。マネージャはコール ルーティングを動的に変更することができます。たとえば、電話機のソフトキーを押すと、すべてのコールをアシスタントにルーティングするようサービスに指示したり、それらのコールの状態を受信したりすることができます。

Unified Communications Manager のユーザーは、マネージャとアシスタントで構成されます。ルーティング サービスはマネージャのコールを代行受信し、それを適切にルーティングします。 アシスタントユーザーはマネージャに代わってコールを処理します。

Cisco WebDialer Web Service

Cisco Unified Communications Manager システム用の Cisco WebDialer Web サービス

Cisco Web Dialer にはクリックツーダイヤル機能があります。 この機能を使用すると、Unified Communications Manager のクラスタ内のユーザーが、Web ページやデスクトップ アプリケーションを使用して、クラスタ内およびクラスタ外の他のユーザーに対してコールを発信することができるようになります。 Cisco Web Dialer には、ユーザーがクラスタ内で相互に通話するための Web ページが用意されています。 Cisco WebDialer は、WebDialer Servlet と Redirector Servlet という 2 つのコンポーネントで構成されています。

Redirector Servlet は、サードパーティ製アプリケーションに Cisco Web Dialer を使用する機能を提供します。 Redirector Servlet は Cisco Web Dialer ユーザーのための適切な Unified Communications Manager のクラスタを検出し、そのクラスタの Cisco Web Dialer にリクエストをリダイレクトします。 Redirector 機能は Simple Object Access Protocol（SOAP）ベースの Web Dialer アプリケーションでは使用できないため、HTTP または HTML ベースの Web Dialer クライアント アプリケーションでのみ使用できます。

セルフプロビジョニング IVR

セルフプロビジョニング IVR サービスの導入により、Unified Communications Manager に自動登録された IP フォンをより少ない作業量で、より早くユーザーに割り当てることができます。IVR サービスを使用するユーザーの内線番号から、[セルフプロビジョニング（Self-Provisioning）] ページで設定された CTI RP DN にダイヤルすると、電話がセルフプロビジョニング IVR アプリケーションに繋がり、セルフサービス クレデンシャルの提供が求められます。 入力したセルフサービス クレデンシャルの検証に基づいて、IVR サービスが自動登録された IP フォンをユーザーに割り当てます。

サービスが非アクティブ化されている場合でもセルフプロビジョニングを設定することはできますが、管理者が IVR サービスを使用して IP フォンをユーザーに割り当てることはできません。 デフォルトでは、このサービスは非アクティブ化されています。

セルフプロビジョニング IVR サービスを有効にするには、Cisco CTI Manager サービスも有効にする必要があります。

セルフプロビジョニングの設定方法の詳細については、『*Administration Guide for Cisco Unified Communications Manager*』を参照してください。

CDR サービス

ここでは、CDR サービスについて説明します。IM and Presence Service および Cisco Unity Connection には適用されません。

CAR Web サービス

Cisco CAR Web サービスは CAR のユーザ インターフェイスをロードします。CAR は CDR データを使用して CSV 形式または PDF 形式のレポートを生成する Web ベースのレポート アプリケーションです。

Cisco SOAP - CDROnDemand サービス

SOAP または HTTPS ベースのサービスである Cisco SOAP - CDROnDemand サービスは、CDR Repository サーバーで実行されます。 ユーザーが指定した間隔（最大 1 時間）に基づく CDR ファイル名のリストに対する SOAP リクエストを受信し、リクエストで指定された時間内に収まるファイル名のリストを返します。 また、このサービスはリクエストで指定されたファイル名と転送方式（SFTP または FTP、サーバー名、ログイン情報、ディレクトリ）を持つ特定の CDR/CMR ファイルの配信に対するリクエストも受信します。

HTTPS または SOAP インターフェイスを通じて CDR データにアクセスするサードパーティ製の課金アプリケーションを使用している場合は、このサービスをアクティブにします。

Unified Communications Manager リリース 12.x と以降のリリースの場合、CDR onDemand Service は、デフォルトで有効になっていません。 CDR onDemand Service を有効にする場合、このサービスを手動でアクティブにする必要があります。 CDR onDemand Service をアクティブにするに

は、/usr/local/cm/bin/soapservicecontrol2.shCDRonDemandServiceCDRonDemanddeploy8443 コマンドを実行します。

セキュリティ サービス

この項では、セキュリティサービスについて説明します。IM and Presence Service および Cisco Unity Connection には適用されません。

Cisco CTL Provider

Unified Communications Manager のみ：ローカル システム アカウント権限で実行される Cisco CTL Provider サービスは、クライアント側のプラグインである Cisco CTL Provider Utility と連携し、クラスタのセキュリティ モードを非セキュア モードから混合モードに変更します。 このプラグインをインストールすると、Cisco CTL Provider サービスは、CTL ファイルのクラスタ内のすべての Unified Communications Manager および Cisco TFTP サーバーのリストを取得します。ここには、クラスタ内のセキュリティトークンおよびサーバーのリストが含まれます。

Cisco CTL Client または CLI コマンド セット **utils ctl** をインストールおよび設定してから、このサービスをアクティブ化してクラスタ全体のセキュリティ モードを非セキュアからセキュアに変更することができます。

サービスをアクティブ化すると、Cisco CTL Provider サービスはデフォルト CTL ポート（2444）に戻ります。 ポートを変更する場合の詳細については、『*Cisco Unified Communications Manager Security Guide*』を参照してください。

Cisco Certificate Authority Proxy Function（CAPF）

Certificate Authority Proxy Function （CAPF）アプリケーションと連携することで、CAPF サービスは設定に応じて次のタスクを実行できます。

- サポートされている Cisco Unified IP 電話 モデルにローカルで有効な証明書を発行します。
- 電話の既存の証明書をアップグレードします。
- トラブルシューティング用に電話の証明書を取得します。
- 電話のローカルで有効な証明書を削除します。

（注） Unified Communications Manager のみ：Real-Time Monitoring Tool（RTMT）でリアルタイム情報を表示する場合、CAPF サービスは最初のサーバーにのみ表示されます。

ディレクトリ サービス

ここでは、ディレクトリ サービスについて説明します。IM and Presence Service および Cisco Unity Connection には適用されません。

Cisco DirSync

Unified Communications Manager：Cisco DirSync サービスを使用すると、Unified Communications Manager のデータベースにすべてのユーザ情報が保存されます。 たとえば、Microsoft Active Directory や Netscape/iPlanet Directory などの統合された社内ディレクトリを Unified Communications Manager に使用している場合、Cisco DirSync サービスはユーザ データを Unified Communications Manager データベースに移行します。 Cisco DirSync サービスは社内ディレクトリのパスワードを同期しません。

（注） 重複した電子メール ID を持つユーザーは同期されず、管理者は同期されていないユーザーのリストに関する通知を受信しません。 これらの ID は Unified RTMT の DirSync エラー ログに表示されます。

Cisco Unity Connection：Cisco Unity Connection が LDAP ディレクトリと統合されている場合、Cisco DirSync サービスは LDAP ディレクトリ内の対応するデータと Cisco Unity Connection サーバー上の Unified Communications Manager のデータベース内のユーザーデータ（氏名、エイリアス、電話番号など）の小規模なサブセットを同期します。 別のサービス（CuCmDbEventListener）では、Unified Communications Manager のデータベースのデータと Cisco Unity Connection ユーザ データベースのデータを同期します。 Cisco Unity Connection クラスタが設定されている場合、Cisco DirSync サービスはパブリッシャ サーバだけで実行されます。

ロケーション ベースのトラッキング サービス

ここでは、ロケーション ベースのトラッキング サービスについて説明します。

Cisco Wireless Controller Synchronization サービス

このサービスは、ネットワークのワイヤレス アクセス ポイントと関連モバイル デバイスのステータスを提供するロケーション認識機能をサポートします。

このサービスは、Unified Communications Manager とシスコのワイヤレス アクセス ポイント コントローラを同期するためにも実行する必要があります。 サービスが動作し、同期が設定されると、Unified Communications Manager は、データベースとシスコのワイヤレス アクセス ポイント コントローラを同期し、コントローラが管理するワイヤレス アクセス ポイントのステータス情報を保存します。 最新の情報となるように、一定の間隔で同期が実行されるようにスケジュール設定できます。

（注） 新しいシスコ ワイヤレス アクセス ポイント コントローラを追加するときに、このサービスが動作していることを確認します。

Voice Quality Reporter サービス

この項では、Voice Quality Reporter サービスについて説明します。IM and Presence Service および Cisco Unity Connection には適用されません。

Cisco Extended Functions

Cisco Extended Functions サービスは、Quality Report Tool（QRT）など、Unified Communications Manager の音声品質機能のサポートを提供します。 個々の機能の詳細については、『*System Configuration Guide for Cisco Unified Communications Manager*』および『*Cisco Unified IP PhoneAdministrationGuide for Cisco Unified Communications Manager*』を参照してください。

ネットワーク サービス

ネットワーク サービスは自動的にインストールされ、データベース サービスやプラットフォーム サービスなど、システムが動作するために必要なサービスが含まれます。 これらのサービスは、基本機能に必要なため [サービスのアクティブ化（Service Activation）] ウィンドウで有効にできません。 トラブルシューティングのためなど、必要に応じて [コントロール センター - ネットワーク サービス（Control Center - Network Services）] ウィンドウで、ネットワーク サービスを停止してから起動（または再起動）する必要があります。

アプリケーションのインストール後、ネットワーク サービスは [コントロール センター - ネットワーク サービス（Control Center - Network Services）] ウィンドウで指定されたとおりに自動的に起動します。 Serviceability GUI は論理グループにサービスを分類します。

パフォーマンスおよびモニタリング サービス

Cisco CallManager のサービスアビリティ RTMT

Cisco CallManager Serviceability RTMT サーブレットは、トレースの収集と表示、パフォーマンス モニタリング オブジェクトの表示、アラートの処理、システム パフォーマンスとパフォーマンス カウンタのモニタなどを実行できる IM and Presence Real-Time Monitoring Tool（RTMT）をサポートします。

Cisco RTMT Reporter Servlet

Cisco RTMT Reporter サーブレットを使用すると、RTMT にレポートをパブリッシュできます。

Cisco Log Partition Monitoring Tool

Cisco Log Partition Monitoring Tool サービスは、設定済みのしきい値とポーリング間隔を使用して、ノード（またはクラスタ内のすべてのノード）上のログ パーティションのディスク使用率をモニタするログ パーティション モニタリング機能をサポートします。

Cisco Tomcat Stats Servlet

Cisco Tomcat Stats Servlet は RTMT または CLI を使用して Tomcat perfmon カウンタをモニタすることができます。 このサービスが CPU 時間などのリソースを大量に使用していることが疑われる場合を除き、このサービスを停止しないでください。

Cisco RIS Data Collector

Real-time Information Server（RIS）は、デバイス登録ステータス、パフォーマンス カウンタ統計、生成された重大アラームなどのリアルタイム情報を保持します。 Cisco RIS Data Collector サービスは、IM and Presence Real-Time Monitoring Tool（RTMT）、SOAP アプリケーションなどのアプリケーションに、クラスタ内のすべてのRISノードに格納された情報を取得するためのインターフェイスを提供します。

Cisco AMC サービス

このサービス、Alert Manager、Collector サービスを Real-Time Monitoring Tool（RTMT）に使用することで、RTMTはサーバ（またはクラスタ内のすべてのサーバ）に存在するリアルタイム情報を取得できるようになります。

Cisco Audit Event Service

Cisco Audit Event Service は、ユーザーによる、またはユーザー処理の結果による Unified Communications Manager または IM and Presence システムへの管理設定のすべての変更をモニタし、記録します。 Cisco Audit Event Service は、ログイン、ログアウト、IM チャット ルームの入退場などのエンド ユーザ イベントもモニタし、記録します。

バックアップおよび復元サービス

Cisco DRF Master

これは、IM and Presence Service には適用されません。

CiscoDRF Master Agent サービスは、Disaster Recovery System GUI または CLI と連携して必要に応じてバックアップのスケジューリング、復元の実行、依存関係の表示、ジョブ ステータスの確認、ジョブの取り消しを行う DRF Master Agent をサポートします。 Cisco DRF Master Agent は、バックアップおよび復元プロセス用のストレージ メディアも提供します。

Cisco DRF Local

Cisco DRF Local サービスは、DRF Master Agent の主要部分である Cisco DRF Local Agent をサポートします。 コンポーネントは、ディザスタ リカバリ フレームワークを使用するために Cisco DRF Local Agent に登録されます。 Cisco DRF Local Agent は、Cisco DRF Master Agent から受信したコマンドを実行します。 Cisco DRF Local Agent は、ステータス、ログ、およびコマンド結果を Cisco DRF Master Agent に送信します。

システム サービス

Cisco CallManager のサービスアビリティ

Cisco CallManager Serviceability サービスは、問題をトラブルシューティングし、サービスを管理するために使用する Web アプリケーション/インターフェイスである Cisco Unified Serviceability および IM and Presence Service Serviceability GUI をサポートしています。 自動的にインストールされるこのサービスは Serviceability GUI にアクセスできます。 サーバーでこのサービスを停止すると、そのサーバーを参照するときに Serviceability GUI にアクセスできません。

Cisco CDP

Cisco Discovery Protocol（CDP）は音声アプリケーションを他のネットワーク管理アプリケーションにアドバタイズするため、ネットワーク管理アプリケーション（SNMP や Cisco Unified Operations Manager など）が、音声アプリケーション用のネットワーク管理タスクを実行できるようになります。

Cisco Trace Collection Servlet

Cisco Trace Collection Servlet は、Cisco Trace Collection サービスとともにトレース収集をサポートし、ユーザーが RTMT を使用してトレースを表示できるようにします。 サーバー上でこのサービスを停止すると、そのサーバー上のトレースは収集または表示ができなくなります。

SysLog ビューアと Trace and Log Central が RTMT で動作するためには、Cisco Trace Collection Servlet と Cisco Trace Collection Service がサーバーで動作している必要があります。

Cisco Trace Collection サービス

Cisco Trace Collection サービスは、Cisco Trace Collection Servlet とともにトレース収集をサポートし、ユーザーが RTMT クライアントを使用してトレースを表示できるようにします。 サーバー上でこのサービスを停止すると、そのサーバー上のトレースは収集または表示ができなくなります。

SysLog ビューアと Trace and Log Central が RTMT で動作するためには、Cisco Trace Collection Servlet と Cisco Trace Collection Service がサーバーで動作している必要があります。

ヒント　必要に応じて初期化時間を短くし、Cisco Trace Collection Servlet を再起動する前に Cisco Trace Collection サービスを再起動することを推奨します。

プラットフォーム サービス

Cisco DB

Cisco DB サービスは、Unified Communications Manager 上での Progres データベース エンジンをサポートしています。 IM and Presence Serviceでは、A Cisco DB サービスは IDS データベース エンジンをサポートします。

Cisco DB Replicator

Unified Communications Manager および IM and Presence のみ：Cisco DB Replicator サービスは、データベース設定と、クラスタ内の最初のサーバーとその他サーバーの間でデータ同期を確認します。

Cisco Tomcat

Cisco Tomcat サービスは Web サーバーをサポートします。

SNMP Master Agent

このサービスはエージェント プロトコル エンジンとして機能し、SNMP リクエストに関連する認証、許可、アクセスコントロール、およびプライバシーの機能を提供します。

ヒント　Serviceability GUI で SNMP の設定を完了した後、[コントロール センター—ネットワーク機能（Control Center—Network Features）]ウィンドウで SNMP Master Agent サービスを再起動する必要があります。

MIB2 Agent

このサービスは、システム、インターフェイス、IP など、変数の読み取りおよび書き込みを行う、RFC 1213 で定義されている変数に対する SNMP アクセスを提供します。

Host Resources Agent

このサービスは、ストレージ リソース、プロセステーブル、デバイス情報、およびインストールされたソフトウェア ベースなど、ホスト情報に対する SNMP アクセスを提供します。 このサービスは HOST-RESOURCES-MIB を実装します。

Native Agent Adaptor

このサービスは、ベンダーの Management Information Bases（MIB）をサポートしており、SNMP リクエストを、システム上で実行されている別の SNMP エージェントに転送できます。

IM and Presence Serviceおよび Unified Communications Manager では、仮想マシンにインストールされた場合、このサービスは提供されません。

System Application Agent

このサービスは、システム上にインストールされ、実行されているアプリケーションに対する SNMP アクセスを提供します。 これは SYSAPPL-MIB を実装します。

Cisco CDP Agent

このサービスは、ノードのネットワーク接続情報に対する SNMP アクセスを提供するために Cisco Discovery Protocol を使用します。 このサービスは CISCO-CDP-MIB を実装します。

Cisco Syslog Agent

このサービスでは、さまざまな Unified Communications Manager コンポーネントが生成する syslog メッセージの収集をサポートします。 このサービスは CISCO-SYSLOG-MIB を実装します。

注意 SNMP サービスを停止すると、ネットワーク管理システムがネットワークをモニタしなくなるため、データが失われる場合があります。テクニカルサポートチームの指示がない限り、サービスを停止しないでください。

Cisco Certificate Change Notification

このサービスによって、Tomcat、CallManager、XMPP などのコンポーネントの証明書がクラスタ内のすべてのノードで自動的に同期されます。 サービスが停止し、証明書を再生成した場合には、他のノードの証明書信頼に証明書を手動でアップロードする必要があります。

Platform Administrative Web サービス

Platform Administrative Web サービスとは、Unified Communications Manager、IM and Presence Service、Cisco Unity Connection システムでアクティブ化され PAWS-M サーバーがシステムをアップグレードできるようにすることが可能な Simple Object Access Protocol（SOAP）API です。

重要 PAWS-M サーバーで Platform Administrative Web サービスをアクティブ化しないでください。

Platform Communication Web Service

Platform Communication Web Service は、Unified Communications Manager、Unified Communications Manager、IM and Presence Service、および Cisco Unity Connection システム上で実行される、Representational State Transfer Protocol（REST）API です。

（注） **Platform Communication Web Service** を手動で起動あるいは停止することはできません。

Cisco UDS Tomcat

このサービスは、他の Web アプリケーションの速度を低下させたり、GUI を遅くしたりアクセスできなくなったりする、UDS での大量のリソース使用を回避します。

Cisco AXL Tomcat

このサービスは、他の Web アプリケーションの速度を低下させたり、GUI を遅くしたりアクセスできなくなったりする、AXL での大量のリソース使用を回避します。

Cisco SSOSP Tomcat

このサービスは、他の Web アプリケーションの速度を低下させたり、GUI を遅くしたりアクセスできなくなったりする、SSOSP での大量のリソース使用を回避します。

Cisco Certificate Expiry Monitor

このサービスは、システムが生成する証明書の有効期限切れのステータスを定期的に確認し、証明書の有効期限に近づくと、通知を送信します。 Unified Communications Manager では、Cisco Unified Operating System Administration で、このサービスを使用する証明書を管理します。 IM and Presence Serviceでは、Cisco Unified IM and Presence Operating System Administration でこのサービスを使用する証明書を管理します。

Cisco Smart License Manager

Cisco Smart License Managerは、パブリッシャ上でしか動作しないネットワーク サービスです。 Unified Communications Manager パブリッシャ上のすべての Cisco Smart Licensing 処理を管理します。 Cisco Smart License Manager サービスは、Cisco Smart Software Manager または Cisco Smart Software Manager サテライトに対する製品のライセンスまたは権限付与の使用状況をレポートし、Cisco Smart Software Manager または Cisco Smart Software Manager サテライトから承認ステータスを取得します。

セキュリティ サービス

Cisco Certificate Enrollment Service

このサービスは、オンラインのサードパーティ CA および認証局のプロキシ機能の間にオンライン接続を構築します。 LSC 証明書に署名するために認証局のプロキシ機能を備えたオンライン CA を使用するには、このサービスをアクティブにする必要があります。

シスコ信頼検証サービス

このサービスは、IM and Presence Service ではサポートされません。

Cisco信頼検証サービスはCallManagerサーバまたは専用サーバーで実行されるサービスで、電話およびその他のエンドポイントに代わって証明書を認証します。 これは、証明書の所有者のロールのリストを関連付けます。 証明書または所有者を1つまたは複数のロールに関連付けることができます。

電話と信頼検証サービス間のプロトコルにより、電話は検証をリクエストできます。信頼検証サービスは証明書を検証し、それに関連付けられたロールのリストを返します。 プロトコルは、信頼検証サービスがリクエストを認証できるようにし、逆に電話は信頼検証サービスからのレスポンスを認証できるようにします。プロトコルは、リクエストとレスポンスの整合性を保護します。 リクエストとレスポンスの機密性は必要ではありません。

スケーラビリティを提供するために、クラスタ内の異なるサーバーで Cisco 信頼検証サービスの複数のインスタンスが実行されます。 これらのサーバーは、Cisco Unified CallManager をホストするサーバーと同じであっても、同じでなくてもかまいません。 電話はネットワーク内の信頼検証サービスのリストを取得し、選択アルゴリズム（ラウンドロビンなど）を使用してそ

のいずれかに接続します。連絡された信頼検証サービスが応答しない場合、電話はリスト内の次の信頼検証サービスに切替えます。

データベース サービス

Cisco Database Layer Monitor

Cisco Database Layer Monitor サービスは、データベース層の局面をモニタします。 このサービスは、変更通知とモニタリングを扱います。

（注） Unified Communications Manager で使用される Automatic Update Statistics は、データベース テーブルに加えられた変更をモニタし、統計の更新を必要とするテーブルのみを更新する、インテリジェントな統計更新機能です。 この機能により、とりわけ Unified Communications Manager の VMware 導入で、帯域幅が大幅に節約されます。 インデックスは、デフォルトで Automatic Update Statistics によって作成されます。

SOAP サービス

Cisco SOAP-Real-Time Service APIs

IM and Presence Serviceのみ：Cisco SOAP-Real-Time Service API は、プレゼンス データのためのクライアント ログインおよびサードパーティ API をサポートします。

Unified Communications Manager および Cisco Unity Connection のみ：Cisco SOAP-Real-Time Service API により、デバイスと CTI アプリケーションのリアルタイム情報を収集することができます。 このサービスは、サービスのアクティブ化、起動、停止のための API も提供します。

Cisco SOAP-Performance Monitoring APIs

Cisco SOAP-Performance Monitoring API サービスは、さまざまなアプリケーションで SOAP API を通じてパフォーマンス モニタリング カウンタを使用できるようにします。たとえば、サービスごとのメモリ情報、CPU 使用率、パフォーマンス モニタリング カウンタなどをモニタできます。

Cisco SOAP-Log Collection APIs

Cisco SOAP-Log Collection API サービスは、ログファイルを収集し、リモート SFTP サーバーのログ ファイルの収集スケジュールを設定できるようにします。 収集するログ ファイルの例としては、syslog、コア ダンプ ファイル、シスコ アプリケーション トレース ファイルなどがあります。

SOAP-Diagnostic Portal Database サービス

Cisco Unified Real-Time Monitoring Tool（RTMT）は、SOAP-Diagnostic Portal Database サービスを使用して RTMT Analysis Manager がホストするデータベースにアクセスします。 RTMT はオ

ペレータの定義したフィルタ選択に基づいて通話レコードを収集します。 このサービスを停止すると、RTMT はデータベースから通話レコードを収集できません。

CM サービス

ここでは、Unified Communications Manager CM サービスについて説明します。Cisco Unity Connection および Cisco Unity Connection には適用されません。

Cisco Extension Mobility アプリケーション

Cisco のエクステンション モビリティ アプリケーション サービスでは、Cisco エクステンション モビリティ機能の電話機設定の接続時間制限などのログイン設定を定義することができます。

Unified Communications Manager のみ：Cisco Extension Mobility 機能により、Unified Communications Manager クラスタ内のユーザーは、クラスタ内の別の電話機にログインして、その電話機を一時的に自分自身の電話機として設定できます。 ユーザーがログインすると、電話機にユーザーの個人の電話番号、スピードダイヤル、サービスリンク、その他のユーザー固有のプロパティが反映されます。 ログアウト後、電話機には元のユーザ プロファイルが反映されます。

Cisco User Data Services

Cisco User Data Services により、Cisco Unified IP 電話は Cisco Unified Communications Manager データベースのユーザ データにアクセスできます。 Cisco User Data Services は Cisco Personal Directory のサポートを提供します。

シスコ プッシュ通知サービス

シスコ プッシュ通知サービスは、着信コールに関するプッシュ通知を Cisco Unified Communications Manager から Apple iOS デバイスに送信するための機能を提供します。 このサービスは、Cisco CallManager サービスから Cisco Collaboration Cloud にプッシュ通知メッセージを中継します。 また、このサービスは、プッシュ通知の送信に使用されるアクセス トークンを管理します。

シスコ ヘッドセット サービス

互換性のある Cisco IP 電話、Cisco Jabber、またはその他の Cisco デバイスを使用している場合、Cisco Headset Service で、シスコ ヘッドセットのインベントリ、設定の更新、および診断データを管理することができます。

（注） Cisco CallManager サービスが既に実行されている場合は、すべてのユニファイド コミュニケーション マネージャ ノードでシスコ ヘッドセット サービスをアクティブにする必要があります。Cisco Unified CM の管理インターフェイスを使用してヘッドセットを管理するには、ユニファイド コミュニケーション マネージャ ノード上でシスコ ヘッドセット サービスをアクティブにしてください。 Cisco CallManager サービスは、シスコ ヘッドセット サービスを有効にすると自動的にアクティブになります。 必要でない場合は、Cisco CallManager サービスを非アクティブにします。

IM and Presence Service サービス

IM and Presence Service サービスは IM and Presence Service だけに適用されます。

Cisco Login Datastore

Cisco Login Datastore は、Cisco Client Profile Agent にクライアント セッションを保存するためのリアルタイム データベースです。

Cisco Route Datastore

Cisco Route Datastore は、Cisco SIP Proxy と Cisco Client Profile Agent のルート情報と割り当て済みユーザーのキャッシュを保存するためのリアルタイムデータベースです。

Cisco Config Agent

Cisco Configuration Agent は、IM and Presence Service IDS データベースの設定変更を Cisco SIP プロキシに通知する変更通知サービスです。

Cisco Sync Agent

Cisco Sync Agent は、IM and Presence データと Unified Communications Manager データの同期を維持します。 IM and Presence に重要なデータについて Unified Communications Manager に SOAP リクエストを送信し、Unified Communications Manager からの変更通知にサブスクライブして IM and Presence IDS データベースを更新します。

Cisco OAM Agent

Cisco OAM Agent サービスは、プレゼンス エンジンに関係する IM and Presence Service IDS データベースの設定パラメータを監視します。 データベースに変更が発生すると、OAM Agent はコンフィギュレーション ファイルを書き込み、プレゼンス エンジンに RPC 通知を送信します。

Cisco Client Profile Agent

Cisco Client Profile Agent サービスは、HTTPS を使用した外部クライアントとの間の安全な SOAP インターフェイスを提供します。

Cisco Intercluster Sync Agent

Cisco Intercluster Sync Agent サービスは、Unified Communications Manager への DND の伝播を可能にし、クラスタ間 SIP ルーティングのために IM and Presence Service クラスタの間でエンドユーザ情報を同期します。

Cisco XCP Router

XCP ルータは IM and Presence Service サーバーのコアコミュニケーション機能です。 IM and Presence Service で XMPP ベースのルーティング機能を提供します。XMPP データを IM and Presence Service 上の他のアクティブな XCP サービスにルーティングしたり、SDNS にアクセスして、システムが XMPP データを IM and Presence Service ユーザーにルーティングできるようにします。 XCP ルータはユーザーの XMPP セッションを管理し、これらのセッションとの間で XMPP メッセージをルーティングします。

IM and Presence Service のインストール後に、システムは Cisco XCP Router をデフォルトでオンにします。

（注） Cisco XCP ルータを再起動すると、IM and Presence Service によりすべてのアクティブな XCP サービスが自動的に再起動されます。 Cisco XCP Router を再起動するには、[再起動（Restart）] オプションを選択する必要があることに注意してください。これは、Cisco XCP Router を停止して起動するのとは違います。 Cisco XCP Router を再起動するのではなく停止した場合、IM and Presence Service により他のすべての XCP サービスが停止されます。 その後 XCP ルータを起動しても、IM and Presence Service により他の XCP サービスは自動的に起動しません。手動で他の XCP サービスを起動する必要があります。

Cisco XCP Config Manager

Cisco XCP Config Manager サービスは、他の XCP コンポーネント（ルータや Message Archiver など）に影響がある、管理 GUI による設定とシステム トポロジの変更（およびクラスタ間ピアから同期されたトポロジ変更）をモニタし、必要に応じてこれらのコンポーネントを更新します。 Cisco XCP Config Manager サービスは、これらの変更により XCP コンポーネントの再起動が必要な場合、管理者向けの通知を作成し、再起動が完了すると自動的に通知をクリアします。

Cisco Server Recovery Manager

Cisco Server Recovery Manager（SRM）サービスは、プレゼンス冗長グループ内のノード間のフェイルオーバーを管理します。 SRM は、ノード内のすべての状態変化を管理します。状態変化には、自動的なものと管理者により実行されるもの（手動）があります。プレゼンス冗長グループでハイ アベイラビリティを有効にすると、各ノードの SRM がピア ノードとのハートビート接続を確立し、重要なプロセスのモニタを開始します。

Cisco IM and Presence Data Monitor

Cisco IM and Presence Data Monitor は IM and Presence Service の IDS 複製状態をモニタします。他の IM and Presence Service は、Cisco IM and Presence Data Monitor に依存します。 これらの依

存サービスは、シスコのサービスを使用して、IDS の複製が安定した状態になるまで起動を遅らせます。

また、Cisco IM and Presence Data Monitor は、Unified Communications Manager から Cisco Sync Agent の同期のステータスを確認します。 IDS の複製が設定され、IM and Presence データベース パブリッシャ ノードの Sync Agent が Unified Communications Manager からの同期を完了させた後にのみ、依存するサービスを起動することができます。 タイムアウトになると、IDS の複製と Sync Agent が完了していなくても、パブリッシャ ノードの Cisco IM and Presence Data Monitor は依存サービスの起動を許可します。

サブスクライバ ノードで、IDS の複製が正常に確立されるまで、Cisco IM and PresenceData Monitor は機能サービスの起動を遅らせます。 Cisco IM and Presence Data Monitor は、クラスタ内の問題のあるサブスクライバ ノードのみで機能サービスの開始を遅らせます。問題があるノードが 1 台あるからといって、すべてのサブスクライバ ノードで機能サービスの開始を遅らせることはありません。 たとえば、IDS の複製が node1 および node2 で正常に確立されたが、node3 では確立されない場合、Cisco IM and Presence Data Monitor により、機能サービスは node1 および node2 で開始できますが、node3 では機能サービスの開始が遅れます。

Cisco Presence Datastore

Cisco Presence Datastore は、一時的なプレゼンス データとサブスクリプションを保存するためのリアルタイム データベースです。

Cisco SIP Registration Datastore

Cisco Presence SIP Registration Datastore は、SIP 登録データを保存するためのリアルタイム データベースです。

CDR サービス

ここでは、CDR サービスについて説明します。IM and Presence Service および Cisco Unity Connection には適用されません。

Cisco CDR Repository Manager

このサービスは、Cisco CDR Agent サービスから取得された、生成されたコール詳細レコード（CDR）を維持し、移動します。 クラスタがサポートされているシステム（Unified Communications Manager のみ）では、このサービスは最初のサーバーにあります。

Cisco CDR Agent

（注） Unified Communications Manager は、Cisco Unified Communications Managerシステムの Cisco CDR Agent をサポートします。

このサービスは、IM and Presence Service および Cisco Unity Connection をサポートしていません。

Cisco CDR Agent サービスは、Unified Communications Manager によって生成される CDR ファイルおよび CMR ファイルを、ローカルホストから CDR リポジトリサーバーに転送します。このサーバーでは、CDR Repository Manager サービスが SFTP 接続を使用して実行されます。

このサービスは、ローカルホストからクラスタ内の CDR リポジトリサーバーに生成された CDR ファイルおよび CMR ファイルを転送します。 CDR Repository Node スタンドアロンサーバーの CDR Agent が SFTP 接続で Cisco CDR Repository Manager へのスタンドアロンサーバーで生成したファイルを転送します。 CDR Agent がファイルを維持し、移動します。

このサービスを機能させるには、サーバーで Cisco CallManager サービスをアクティブにし、サービスが実行されていることを確認します。 設定でクラスタがサポートされている場合（Unified Communications Manager のみ）、最初のサーバー上で Cisco CallManager サービスをアクティブ化します。

Cisco CAR Scheduler

Cisco CDR Analysis and Reporting（CAR）Scheduler サービスは、IM and Presence Service および Cisco Unity Connection をサポートしていません。

Cisco CAR Scheduler サービスを使用すると、レポートの生成や、CDR 分析とレポート（CAR）データベースへの CDR ファイルのロードなど、CAR に関連するタスクをスケジュールできます。

Cisco SOAP-CallRecord Service

Cisco SOAP-CallRecord サービスはデフォルトではパブリッシャで SOAP サーバーとして実行され、クライアントが SOAP API を通じて CAR データベースに接続できるようにします。 この接続は、（別の CAR IDS インスタンスにより）CAR コネクタを使用して行われます。

Cisco CAR DB

Cisco CAR DB は CAR データベースの Informix インスタンスを管理し、Service Manager がこのサービスを開始または停止できるようにして、CAR IDS インスタンスを個々に起動またはシャットダウンできるようにします。 これは、CCM IDS インスタンスを維持するために使用される Unified Communications Manager データベースと似ています。

Cisco CAR DB サービスは、デフォルトではパブリッシャでアクティブ化されます。 CAR DB インスタンスがインストールされてパブリッシャでアクティブに実行され、CAR データベースを維持します。 このネットワーク サービスはパブリッシャでのみ使用され、サブスクライバでは使用できません。

管理サービス

ここでは、管理サービスについて説明します。Cisco Unity Connection には適用されません。

Cisco CallManager Admin

Cisco CallManager Admin サービスは、IM and Presence Service および Cisco Unity Connection ではサポートされていません。

Cisco CallManager Admin サービスは、Unified Communications Manager Administration（Cisco Unified Communications Manager 設定を構成するために使用する Web アプリケーション/インターフェイス）をサポートします。 Unified Communications Manager のインストール後に、このサービスは自動的に起動し、グラフィカル ユーザ インターフェイス（GUI）にアクセスすることができるようになります。 このサービスを停止すると、そのサーバーをブラウズしたときに、Cisco Unified Communications Manager の管理 のグラフィカル ユーザー インターフェイスにアクセスできません。

Cisco IM and Presence Admin

Cisco IM and Presence 管理サービスは、Unified Communications Manager および Cisco Unity Connectionではサポートされません。

Cisco IM and Presence Admin サービスは、Cisco Unified Communications Manager IM and Presence 管理、つまりIM and Presence Service 設定を行うために使用する Web アプリケーション/インターフェイス）をサポートします。 IM and Presence Serviceをインストールした後、このサービスが自動的に起動し、GUI にアクセスできるようになります。 このサービスを停止すると、そのサーバーをブラウズする際に、Cisco Unified Communications Manager IM and Presence 管理 GUI にアクセスできなくなります。

Services setup

コントロール センター

Serviceability GUI のコントロール センターでは、ステータスを表示したり、一度に 1 つのサービスを起動および停止したりすることができます。 ネットワーク サービスを起動、停止、および再起動するには、[コントロール センター - ネットワーク サービス（Control Center - Network Services）] ウィンドウにアクセスします。 機能サービスを起動、停止、再起動するには、[コントロール センター - 機能サービス（Control Center - Feature Services）] ウィンドウにアクセスします。

ヒント [関連リンク（Related Links）] リストボックスと [移動（Go）] ボタンを使用して、[コントロール センター（Control Center）] ウィンドウと [サービスの開始（Service Activation）] ウィンドウにナビゲートします。

Unified Communications Manager および IM and Presence のみ：クラスタ設定では、ステータスを表示したり、クラスタ内の 1 台のサーバーのサービスを一度に開始および停止することができます。

Unified Communications Manager のみ：機能サービスを起動および停止すると、そのサービスに現在登録されているすべての Cisco Unified IP 電話 およびゲートウェイがセカンダリ サービスにフェールオーバーされます。 セカンダリ サービスに登録できない場合だけデバイスと電話機を再起動する必要があります。 サービスを起動および停止すると、Unified Communications

Manager をホームとするその他のインストール済みアプリケーション（会議ブリッジまたは Cisco Messaging Interface など）も起動および停止します。

注意 Unified Communications Manager のみ：サービスを停止すると、そのサービスによって制御されるすべてのデバイスの呼処理も停止します。 サービスが停止すると、IP フォンから別の IP フォンへのコールは停止せず、IP フォンから Media Gateway Control Protocol（MGCP）ゲートウェイへの実行中のコールも停止しませんが、他の種類のコールはドロップします。

サービスのセットアップ

サービスを使用する場合は、次のタスクを実行できます。

手順

ステップ 1 実行する機能サービスをアクティブ化します。

ステップ 2 適切なサービス パラメータを設定します。

ステップ 3 必要に応じて、Serviceability GUI のトレース ツールを使って問題のトラブルシューティングを行います。

サービスのアクティブ化

（注） Serviceability GUI の [サービスの開始（Service Activation）] ウィンドウでは、複数の機能サービスをアクティブ化または非アクティブ化したり、アクティブ化するデフォルトのサービスを選択できます。 IM and Presence のノードから Unified Communications Manager サービスの表示、起動、停止を行ったり、その逆を行うことができます。 次のエラーが発生することがあります。「サーバへの接続が確立できません(リモート ノードにアクセスできません)（Connection to the Server cannot be established (unable to access Remote Node)）」。 このエラー メッセージが表示された場合は、『*Administration Guide for Cisco Unified Communications Manager*』を参照してください。

（注） Unified Communications Manager Release 6.1.1 以降、エンドユーザーはサービスの起動および停止に Cisco Unified Serviceability を利用することができません。

機能サービスは自動モードでアクティブ化され、Serviceability GUI により、単一ノード構成に基づいてサービスの依存関係がチェックされます。機能サービスをアクティブ化することを選択すると、動作するためにそのサービスに依存するサービスが他にある場合は、そのすべてを

選択することが求められます。 **[デフォルトの設定（Set Default）]** をクリックすると、サーバーで実行するために必要なサービスが Serviceability GUI によって選択されます。

Cisco Unified Communications Manager および IM and Presence Service のみ：クラスタをサポートする設定であっても、このプロセスは単一サーバ設定に基づきます。

サービスをアクティブ化すると、自動的にサービスが起動します。 サービスはコントロールセンターから開始および停止します。

Cisco Unified Communications Manager のクラスタ サービス アクティベーションに関する推奨事項

クラスタでサービスを有効化する前に、マルチサーバ Unified Communications Manager 設定用のサービスの推奨事項を示す、次の表を確認してください。

表 *35 : Cisco Unified Communications Manager* のサービス アクティベーションに関する推奨事項

サービス/サーブレット	アクティブ化の推奨事項
CM サービス	
Cisco CallManager	このサービスは、Unified Communications Manager をサポートしています。 [Control Center - Network Services] で、Cisco RIS Data Collector サービスと Databas Monitor サービスがノードで実行されていることを確認します。 **ヒント** このサービスをアクティブ化する前に、Cisco Unified Communications Ma Administration 内の [Unified Communications Manager の検索/リスト（Unif Communications Manager Find/List）] ウィンドウの Unified Communications M サーバーの表示内容を確認します。 サーバーが表示されていない場合、 サービスをアクティブ化する前に Unified Communications Manager サー 追加します。 サーバーを追加する方法については、『*Cisco Unified Communications Ma* システム設定ガイド』を参照してください。
Cisco Messaging Interface	サーバーに接続された USB/シリアルアダプタを使用してサードパーティ製ボイ ルシステムとの SMDI 統合を使用している場合にだけアクティブ化します。
Cisco Unified Mobile Voice Access Service	モバイル ボイス アクセスが機能するには、最初の VXML ページを指すように ゲートウェイを設定した後でクラスタ内の最初のノードでこのサービスをアク 化する必要があります。 また、Cisco CallManager および Cisco TFTP サービスは タ内の 1 つのサーバー上で実行するようにしてください。Cisco Unified Mobile Access Service が実行されているサーバーと同じサーバーである必要はありませ

サービス/サーブレット	アクティブ化の推奨事項
Cisco IP Voice Media Streaming App	クラスタ内に複数のノードがある場合は、クラスタごとに 1 つまたは 2 つの でアクティブ化します。 保留音専用のノードでアクティブ化することができ のサービスでは、クラスタ内の 1 つのノードで Cisco TFTP をアクティブ化 あります。 最初のノードおよび Cisco CallManager サービスを実行するノー のサービスをアクティブ化しないでください。
Cisco CTIManager	JTAPI/TAPI アプリケーションが接続する各ノードでアクティブ化します。 C をアクティブ化するには、Cisco CallManager サービスもノードでアクティブ 要があります。 CTIManager および Cisco CallManager サービスの相互作用の いては、CM サービスに関連するトピックを参照してください。
Cisco Extension Mobility	クラスタ内のすべてのノードでアクティブ化します。
Cisco Extended Functions	Quality Report Tool（QRT）をサポートするこのサービスは、Cisco RIS Data C 実行する 1 つまたは複数のサーバーでアクティブ化します。 クラスタ内の Cisco CTIManager サービスがアクティブなことを確認します。
Cisco DHCP Monitor サービス	DHCP Monitor Service が有効になると、IP フォンの IP アドレスに影響するネ スの変更を検出し、/etc/dhcpd.conf ファイルを変更し、DHCPD を停止し、更 コンフィギュレーション ファイルで再起動します。 このサービスは、DHCP されているノード上でアクティブ化してください。
シスコ ロケーション帯域幅マネージャ	音声コールとビデオ コールの帯域幅割り当てを管理するために Cisco のロケ コール アドミッション制御メカニズムを使用する場合は、このサービスをア 化する必要があります。 このサービスは、Cisco CallManager サービスとと ます。 Cisco CallManager サービスを実行するサーバーで Cisco Location Band Manager を実行することを推奨します。 CallManager サービスと同じサーバー Bandwidth Manager が実行されていない場合は、Location Bandwidth Manager 正しく設定されていることを確認します。
シスコ クラスタ間検索サービス	複数の Unified Communications Manager クラスタ間で URI と数字ルーティング 播する場合、この交換に参加するクラスタのパブリッシャでこのサービスを ブ化する必要があります。
Cisco Dialed Number Analyzer Server	クラスタ内に複数のノードがある場合は、Cisco Dialed Number Analyzer サー の 1 つのノードでこのサービスをアクティブにしてください。
Cisco Dialed Number Analyzer	Unified Communications Manage の Dialed Number Analyzer を使用する場合は、 ビスをアクティブ化します。 このサービスはリソースを大量に消費するこ め、コール処理アクティビティが最も少ないノードかオフピーク時にアクテ ます。
Cisco TFTP	クラスタ内に複数のノードがある場合は、Cisco TFTP サービス専用の 1 つの このサービスをアクティブ化します。 クラスタ内の複数のノードでこのサー クティブ化する場合は、オプション 150 を設定します。

サービス/サーブレット	アクティブ化の推奨事項
シスコ ヘッドセット サービス	Unified Communications Manager からシスコ ヘッドセットを管理する場合は、こ ビスを有効化します。 （注） Cisco CallManager サービスが既に実行されている場合は、すべてのユニ ド コミュニケーション マネージャノードでシスコ ヘッドセットサービ クティブにする必要があります。 Cisco Unified CM の管理インターフェ 使用してヘッドセットを管理するには、ユニファイド コミュニケーショ ネージャノード上でシスコ ヘッドセットサービスをアクティブにしてく い。 Cisco CallManager サービスは、シスコ ヘッドセットサービスを有効 ると自動的にアクティブになります。 必要でない場合は、Cisco CallMan サービスを非アクティブにします。
CTI サービス	
Cisco IP Manager Assistant	Cisco Unified Communications Manager Assistant を使用する場合は、クラスタ内の 2 台のサーバ（プライマリおよびバックアップ）でこのサービスをアクティブ化 す。 Cisco CTI Manager サービスがクラスタ内でアクティブ化されていることを ます。 Cisco IP Manager Assistant の詳細については、『 *Feature Configuration Guide for* *Unified Communications Manager* 』を参照してください。
Cisco WebDialer Web Service	クラスタごとに 1 つのノードでアクティブ化します。
セルフプロビジョニング IVR	セルフプロビジョニング IVR サービスを有効にするには、Cisco CTI Manager サ も有効にする必要があります。 サービスが非アクティブ化されている場合でもセルフプロビジョニングを設定 とはできますが、管理者が IVR サービスを使用して IP フォンをユーザーに割り ことはできません。 デフォルトでは、このサービスは非アクティブ化されてい
CDR サービス	
Cisco SOAP-CDROnDemand サービス	Cisco SOAP-CDROnDemand サービスは、最初のサーバー上だけでアクティブ化 とができ、Cisco CDR Repository Manager および Cisco CDR Agent サービスが同 バー上で実行されている必要があります。 Unified Communications Manager リリース 12.x と以降のリリースの場合、CDR onl Service は、デフォルトで有効になっていません。 CDR onDemand Service を有効 る場合、このサービスを手動でアクティブにする必要があります。 CDR onDem Service をアクティブにするに は、`/usr/local/cm/bin/soapservicecontrol2.shCDRonDemandServiceCDRonDemanddep` コマンドを実行します。

サービス/サーブレット	アクティブ化の推奨事項
Cisco CAR Web Service	Cisco CAR Web サービスは、最初のサーバー上だけでアクティブ化すること Cisco CAR Scheduler サービスが同じサーバー上でアクティブにされ、実行さ CDR Repository Manager サービスも同じサーバー上で実行されている必要が
データベースおよび管理者サービス	
Cisco AXL Web Service	インストール後は、すべてのクラスタ ノードで Cisco AXL Web サービスが で有効になります。パブリッシャ ノードではこのサービスを常にアクティ することを推奨します。 これにより、Unified Provisioning Manager などの A する製品を設定できるようになります。 必要に応じて、機能サービス下の Cisco Unified Serviceability の特定のサブス ノードのサービスをアクティブ化/非アクティブ化することができます。
Cisco Bulk Provisioning サービス	Cisco Bulk Provisioning サービスは、最初のノードだけでアクティブにでき Administration Tool（BAT）を使用して電話とユーザーを管理している場合は サービスをアクティブ化する必要があります。
Cisco UXL Web サービス	このサービスは、認証およびユーザ許可のチェックを実行します。 Cisco IP 電 Book Synchronizer の TabSync クライアントは、Cisco Unified Communications データベースの照会用に Cisco UXL Web サービスを使用します。 Cisco IP 電話Address Book Synchronizer を使用する場合は、このサービスを ド（パブリッシャ ノードを推奨）でこのサービスをアクティブ化する必要が す。 Cisco IP 電話Address Book Synchronizer を使用しない場合、このサービス ティブ化することを推奨します。 デフォルトでは、このサービスは非アク れています。
Cisco Platform Administrative Web サービス	アップグレードの管理、バージョンの切り替え、操作の再開または再対処の Cisco Prime Collaboration Deployment（PCD）サーバーを使用する場合は、こ スをアクティブ化する必要があります。 Platform Administrative Web サービス により、Call Manager と Prime Collaboration Deployment（PCD）の間で通信を ができます。 クラスタ内に複数のノードがある場合は、クラスタ内の各サー のサービスをアクティブ化する必要があります。
Cisco TAPS サービス	Cisco Unified Communications Manager Auto-Register Phone Tool を使用する前に ノードでこのサービスをアクティブ化する必要があります。 Cisco Unified Com Manager Auto-Register Phone Tool のダミー MAC アドレスを作成する場合、C Provisioning サービスが同じノードでアクティブ化されていることを確認し
パフォーマンスおよびモニタリング サービス	
Cisco Serviceability Reporter	最初のノードだけでアクティブ化します。 （注） このサービスは、他のノードでアクティブ化されていても、最初のノ でレポートを生成します。

サービス/サーブレット	アクティブ化の推奨事項
Cisco CallManager SNMP サービス	SNMP を使用する場合は、このサービスをクラスタ内のすべてのサーバーでアブ化します。
セキュリティ サービス	
Cisco CTL Provider	クラスタ内のすべてのサーバーでアクティブ化します。
Cisco Certificate Authority Proxy Function（CAPF）	最初のノードだけでアクティブ化します。
ディレクトリ サービス	
Cisco DirSync	最初のノードだけでアクティブ化します。

IM and Presence Service のクラスタ サービス アクティベーションに関する推奨事項

注意 ある機能のいずれかのサービスを有効にする前に、その機能についてIM and Presenceで必要なすべての設定を行う必要があります。 各 IM and Presence 機能については、関連マニュアルを参照してください。

クラスタ内でサービスを有効にする前に、マルチノード構成でのIM and Presence構成の推奨事項を示した次の表を確認してください。

表 *36 : IM and Presence Service* アクティベーションに関する推奨事項

サービス/サーブレット	推奨事項
データベースおよび管理者サービス	

サービス/サーブレット	推奨事項
Cisco AXL Web Service	インストール後は、すべてのクラスタ ノードで Cisco AXL Web サービスがデフォルトで有効になります。 IM and Presence Service データベース パブリッシャ ノードでサービスを常にアクティベートしたままにしておくことを推奨します。 これにより、AXL に依存している製品を構成できるようになります。クラスタ間通信が構成されている場合、リモート ピアからの同期元として構成されたサブクラスタ内の両方のノードで、このサービスを有効にする必要があります。このサービスが両方のノードでイネーブルになっていない場合、プレゼンス機能およびIM機能はフェールオーバー時に失われます。 必要に応じて、[Cisco Unified Serviceability] で [機能サービス（Feature Services）] の下にある特定の IM and Presence サブスクライバ ノードで、このサービスをアクティベートまたは非アクティベートできます。
Cisco Bulk Provisioning サービス	• Cisco Bulk Provisioning サービスは、最初のノードだけで有効にします。 • Bulk Administration Tool（BAT）を使用してユーザーを管理している場合は、このサービスを有効にする必要があります。
パフォーマンスおよびモニタリング サービス	
Cisco Serviceability Reporter	このサービスは、パブリッシャ ノードのみで有効にします。 （注） このサービスは、他のノードでサービスを有効にした場合でも、必ずパブリッシャ ノードでレポートを生成します。
IM and Presence サービス	
Cisco SIP Proxy	このサービスは、クラスタ内のすべてのノードで有効にします。
Cisco Presence Engine	このサービスは、クラスタ内のすべてのノードで有効にします。
Cisco Sync Agent	このサービスは、クラスタ内のすべてのノードで有効にします。

サービス/サーブレット	推奨事項
Cisco XCP Text Conference Manager	• IM and Presence でチャット機能を展開する場合はこのサービスを有効にします。 • このサービスは、チャット機能を実行する各ノードで有効にします。 （注） 常設チャット機能は、外部データベースを必要とします。 常設チャット機能を有効にする場合、Text Conference Manager サービスを起動する前に、外部データベースも設定する必要があります。 Text Conference Manager サービスは、常設チャット機能が有効でも外部データベースが設定されていない場合は起動しません。 については、『*Database Setup Guide for IM and Presence*』*Unified Communications Manager*を参照してください。
Cisco XCP Web Connection Manager	• Web クライアントを IM and Presence と統合する場合はこのサービスを有効にします。 • このサービスは、クラスタ内のすべてのノードで有効にします。
Cisco XCP Connection Manager	• XMPP クライアントを IM and Presence と統合する場合はこのサービスを有効にします。 • このサービスは、クラスタ内のすべてのノードで有効にします。
Cisco XCP SIP Federation Connection Manager	次のいずれかの構成を展開する場合はこのサービスを有効にします。 • IM and Presence 上で SIP プロトコルを介したドメイン間フェデレーション。 このサービスは、SIP フェデレーションを実行する各ノードで有効にします。 • IM and Presence Release 9.x クラスタと Cisco Unified Presence Release 8.6(x) クラスタ間のクラスタ間導入。 このサービスは、Release 9.x クラスタ内のすべてのノードで有効にします。

サービス/サーブレット	推奨事項
Cisco XCP XMPP Federation Connection Manager	• このサービスは、IM and Presence 上で XMPP プロトコルを介したドメイン間フェデレーションを展開する場合にのみ有効にします。 • このサービスは、XMPP フェデレーションを実行する各ノードで有効にします。 （注） ノードで XMPP Federation Connection Manager サービスを有効にする前に、そのノードの Cisco Unified Communications Manager IM and Presence Administration で XMPP フェデレーションを有効にする必要があります。 については、『*Interdomain Federation for IM and Presence*』*Unified Communications Manager*を参照してください。
Cisco XCP Message Archiver	• IM and Presence でコンプライアンス機能を展開する場合はこのサービスを有効にします。 • このサービスは、IM コンプライアンス機能を実行するすべてのノードで有効にします。 （注） 外部データベースを設定する前に Message Archiver を有効にしても、サービスは開始されません。また、外部データベースに到達できない場合もサービスは開始されません。 については、『*Database Setup Guide for IM and Presence*』*Unified Communications Manager*を参照してください。

サービス/サーブレット	推奨事項
Cisco XCP Directory Service	• IM and Presence 上の XMPP クライアントを LDAP ディレクトリと統合する場合はこのサービスを有効にします。 • このサービスは、クラスタ内のすべてのノードで有効にします。 （注） サードパーティ XMPP クライアント用の連絡先検索設定を行う前に Directory Service を有効にしても、サービスは開始されますが、再度停止されます。Unified Communications Manager については、『*Configuration and Administration of IM and Presence Service*』を参照してください。
Cisco XCP Authentication Service	• XMPP クライアントを IM and Presence と統合する場合はこのサービスを有効にします。 • このサービスは、クラスタ内のすべてのノードで有効にします。

機能サービスのアクティブ化

Serviceability GUI の [サービスの開始（Service Activation）] ウィンドウで、機能サービスをアクティブ化および非アクティブ化します。 [サービスの開始（Service Activation）] ウィンドウに表示されるサービスは、アクティブ化されるまで起動しません。

（ネットワーク サービスではなく）機能サービスのみをアクティブ化および非アクティブ化することができます。 必要な数のサービスを同時にアクティブ化または非アクティブ化できます。 一部の機能サービスは他のサービスに依存しているため、その依存しているサービスがアクティブ化してから、該当の機能サービスがアクティブ化します。

ヒント Unified Communications Manager と IM and Presence Service のみ：[サービスの開始（Service Activation）] ウィンドウでサービスをアクティブ化する前に、クラスタサービスをアクティブ化する際の推奨事項に関連するトピックを確認してください。

手順

ステップ 1 **[ツール（Tools）] > [サービス アクティベーション（Service Activation）]** を選択します。

[Service Activation]ウィンドウが表示されます。

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

IM and Presence Service ノードから Unified Communications Manager サービスにアクセスしたり、その逆を行うことができます。 リモート ノードにアクセスしようとすると、次のエラーが発生する場合があります。「サーバへの接続が確立できません(リモートノードに接続できません)（Connection to the Server cannot be established (unable to connect to Remote Node)）」。 このエラー メッセージが表示された場合は、『*Administration Guide for Cisco Unified Communications Manager*』を参照してください。

ステップ 3 次のいずれかの操作を実行してサービスを有効または無効にします。

a) 単一サーバーで実行する必要があるデフォルトサービスをオンにするには、**[デフォルトに設定（Set to Default）]** を選択します。

（注） このオプションを選択すると、単一サーバーの構成に基づいてデフォルトのサービスが選択され、サービスの依存関係が確認されます。

b) すべてのサービスを有効にするには、[すべてのサービスをチェック（Check All Services）] をオンにします。

c) 特定のサービスを有効にするには、有効にするサービスのチェックボックスをオンにします。

d) サービスを無効にするには、無効にするサービスのチェックボックスをオフにします。

ステップ 4 Unified Communications Manager と IM and Presence Service のみ：クラスタ構成の場合は、クラスタ サービスのアクティブ化に関する推奨事項を確認してから、アクティブ化するサービスの隣にあるチェックボックスをオンにします。

ステップ 5 アクティブ化するサービスのチェックボックスをオンにした後、[保存（Save）] をクリックします。

ヒント アクティブ化したサービスを非アクティブ化するには、非アクティブ化するサービスの隣にあるチェックボックスをオフにして、[保存（Save）] をクリックします。

ヒント サービスの最新の状態を取得するには、[更新（Refresh）] ボタンをクリックします。

関連トピック

Cisco Unified Communications Manager のクラスタ サービス アクティベーションに関する推奨事項 （252 ページ）
IM and Presence Service のクラスタ サービス アクティベーションに関する推奨事項 （256 ページ）

コントロール センターまたは CLI でのサービスの開始、停止、再起動

これらのタスクを実行するために、Serviceability GUI には 2 つのコントロール センター ウィンドウがあります。 ネットワーク サービスを起動、停止、および再起動するには、[コントロール センター—ネットワークサービス（Control Center—Network Services）]ウィンドウにア

クセスします。 機能サービスを起動、停止、再起動するには、[コントロール センター - 機能サービス（Control Center—Feature Services）]ウィンドウにアクセスします。

ヒント [関連リンク（Related Links）] リスト ボックスと [移動（Go）] ボタンを使用して、[コントロール センター（Control Center）] ウィンドウと [サービスの開始（Service Activation）] ウィンドウにナビゲートします。

コントロール センターでのサービスの開始、停止、再起動

Serviceability GUI のコントロール センターでは次のことができます。

- ステータスの表示
- ステータスの更新
- 特定のサーバー、またはクラスタ設定のクラスタ内のサーバーにおける機能およびネットワークサービスの起動、停止、および再起動

サービスが停止中の場合、サービスが停止するまで起動できないことに注意してください。

注意 Unified Communications Manager のみ：サービスを停止すると、そのサービスによって制御されるすべてのデバイスの呼処理も停止します。 サービスを停止しても、IP フォンから別の IP フォンへのコールは接続されたまま、IP フォンから Media Gateway Control Protocol（MGCP）ゲートウェイへの進行中のコールも接続されたままになります。他の種類のコールはドロップされます。

手順

ステップ 1 起動/停止/再起動/更新するサービスのタイプに応じて、次のいずれかのタスクを実行します。

- **[ツール（Tool）]** > > **[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。

  ヒント 機能サービスは、起動/停止/再起動する前にアクティブ化する必要があります。

- **[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 [サーバー（Server）] ドロップダウン リストからサーバーを選択し、**[移動（Go）]** をクリックします。

ウィンドウに次の項目が表示されます。

- 選択したサーバーのサービス名。
- サービス グループ。

- サービス ステータス。[起動済み（Started）]、[実行中（Running）]、[停止中（Not Running）] など （[ステータス（Status）] カラム）。
- サービスが実行を開始した正確な時刻 （[開始時間（Start Time）] カラム）。
- サービスを実行している時間 （[アップタイム（Up Time）] カラム）。

ステップ 3 次のいずれかの作業を実行します。

- 起動するサービスの横にあるオプション ボタンをクリックし、[開始（Start）]をクリックします。 [ステータス（Status）] が変化し、更新されたステータスが反映されます。
- 停止するサービスの横にあるオプション ボタンをクリックし、[停止（Stop）]をクリックします。 [ステータス（Status）] が変化し、更新されたステータスが反映されます。
- 再起動するサービスの横にあるオプション ボタンをクリックし、[再起動（Restart）]をクリックします。 再起動に時間がかかることを示すメッセージが表示されます。 **OK**をクリックします。
- サービスの最新の状態を表示するには、[更新（Refresh）]をクリックします。
- [サービスの開始（Service Activation）]ウィンドウまたは他のコントロール センター ウィンドウを表示するには、[関連リンク（Related Links）] ドロップダウン リストからオプションを選択し、[移動（Go）]をクリックします。

コマンドライン インターフェイスを使用したサービスの開始、停止、再起動

CLI を使用してサービスを開始および停止することができます。 CLI から開始および停止できるサービスのリストとその実行方法については、『*Command Line Interface Reference Guide for Cisco Unified Solutions*』を参照してください。

ヒント ほとんどのサービスは、Serviceability GUI のコントロール センターから開始または停止する必要があります。

第 17 章

トレース

トレース

Cisco Unified Serviceability では、音声アプリケーションの問題のトラブルシューティングで使用できるトレース ツールを提供しています。 Cisco Unified Serviceability は、SDI（System Diagnostic Interface）トレース、Cisco CallManager サービスおよび Cisco CTIManager サービス用の SDL（Signaling Distribution Layer）トレース（Unified Communications Manager に適用可能）、および Java アプリケーション用の Log4J トレースをサポートしています。

トレースする情報のレベルや、各トレース ファイルに含める情報の種類は、[Trace Configuration] ウィンドウを使用して指定します。

Unified Communications Manager のみ：サービスが、Cisco CallManager や Cisco CTIManager などのコール処理アプリケーションの場合、電話機やゲートウェイなどのデバイスに対してトレースを設定することができます。

Unified Communications Manager のみ：[アラーム設定] ウィンドウで、SDL トレース ログ ファイルなど、さまざまな場所にアラームを送ることができます。 必要に応じて、Cisco Unified Real-Time Monitoring Tool（Unified RTMT）での警告用にトレースを設定することもできます。

さまざまなサービスに対しトレース ファイルに含める情報を設定したら、Cisco Unified Real-Time Monitoring Tool の Trace and Log Central オプションを使用して、トレース ファイルを収集および表示できます。

Cisco Unified IM and Presence Serviceability には、インスタント メッセージングおよびプレゼンス アプリケーションの問題のトラブルシューティングに使用できるトレース ツールが用意されています。 Cisco Unified IM and Presence Serviceability では、次のトレースをサポートしています。

- SDI トレース
- Log4J トレース（Java アプリケーション用）

トレースする情報のレベル（デバッグ レベル）、トレースする情報（トレース フィールド）、およびトレース ファイルに関する情報（サービスごとのファイル数、ファイル サイズ、トレース ファイルにデータが保存された時間など）を設定できます。1 つのサービスに対してトレースを設定することも、クラスタ内のすべてのサーバーに対してサービスのトレース設定を適用することもできます。

[アラーム設定（Alarm Configuration）]ウィンドウでは、さまざまな場所にアラームを送ることができます。 必要に応じて、IM and Presence Unified RTMT での警告用にトレースを設定することもできます。

さまざまなサービスに対しトレース ファイルに含める情報を設定したら、Unified RTMT の Trace and Log Central オプションを使用して、トレース ファイルを収集および表示できます。クラスタ内の任意の IM and Presence ノードで使用できる任意の機能またはネットワーク サービスのトレース パラメータを設定できます。 [トレース設定（Trace Configuration）]ウィンドウを使用して、問題をトラブルシューティングするためにトレースするパラメータを指定します。 独自のトレース フィールドを選択する代わりに、あらかじめ決められたトラブルシューティング トレース設定を使用するには、[トラブルシューティング トレース設定（Troubleshooting Trace Settings）]ウィンドウを使用します。

（注） トレースをイネーブルにすると、システムのパフォーマンスが低下します。そのため、トレースは、トラブルシューティング目的でのみイネーブルにします。トレースの使用について支援が必要な場合は、Cisco Technical Assistance Center（TAC）にお問い合わせください。

トレース設定

トレース パラメータは、Serviceability のインターフェイスに表示される任意の機能またはネットワーク サービスに対して設定できます。 クラスタがある場合は、クラスタ内の任意のサーバーで使用できる機能またはネットワークサービスに対してトレースパラメータを設定できます。[トレース設定（Trace Configuration）] ウィンドウを使用して、問題をトラブルシューティングするためにトレースするパラメータを指定します。

トレースする情報のレベル（デバッグ レベル）、トレースする情報（トレース フィールド）、およびトレース ファイルに関する情報（サービスごとのファイル数、ファイル サイズ、トレース ファイルにデータが保存された時間など）を設定できます。 クラスタがある場合、1 つのサービスに対してトレースを設定することも、クラスタ内のすべてのサーバーに対してサービスのトレース設定を適用することもできます。

独自のトレース フィールドを選択する代わりに、あらかじめ決められたトラブルシューティング トレース設定を使用するには、[トラブルシューティング トレース（Troubleshooting Trace）] ウィンドウを使用します。 トラブルシューティング トレースの詳細については、「トレースの設定」を参照してください。

さまざまなサービスに対しトレース ファイルに含める情報を設定したら、Unified RTMT の Trace and Log Central オプションを使用して、トレース ファイルを収集できます。 トレースの収集に関連する詳細情報については、「トレース収集」を参照してください。

トレース設定

[トラブルシューティング トレース設定（Troubleshooting Trace Settings）] ウィンドウでは、事前に設定されたトラブルシューティング トレース設定に設定するサービスを選択できます。このウィンドウでは、1 つ以上のサービスを選択し、これらのサービスの設定を、事前に設定されたトレース設定に変更できます。クラスタがある場合、クラスタ内の異なるサーバー上のサービスを選択して、そのサービスのトレース設定を事前に設定されたトレース設定に変更することができます。1 台のサーバーの特定のアクティブ化されたサービス、サーバーのすべてのアクティブ化されたサービス、クラスタ内のすべてのサーバーの特定のアクティブ化されたサービス、クラスタ内のすべてのサーバーのすべてのアクティブ化されたサービスを選択できます。 このウィンドウでは、非アクティブなサーバーの横に [N/A] と表示されます。

（注） 機能またはネットワーク サービスの事前に決定されたトラブルシューティング トレース設定には、SDL、SDI、および Log4j トレース設定があります。 トラブルシューティング トレース設定が適用される前に、元のトレース設定がバックアップされます。 トラブルシューティング トレース設定をリセットすると、元のトレース設定が復元されます。

トラブルシューティング トレース設定をサービスに適用した後で [トラブルシューティング トレース設定（Troubleshooting Trace Settings）] ウィンドウを開くと、トラブルシューティング用に設定したサービスがチェック付きで表示されます。 [トラブルシューティング トレース設定（Troubleshooting Trace Settings）] ウィンドウでは、トレース設定を元の設定にリセットできます。

トラブルシューティング トレース設定をサービスに適用すると、トラブルシューティング トレースがそのサービスに設定されたことを示すメッセージが [トレース設定（Trace Configuration）] ウィンドウに表示されます。 サービスの設定をリセットする場合は、[関連リンク（Related Links）] ドロップダウン リスト ボックスから、[トラブルシューティング トレース設定（Troubleshooting Trace Settings）] オプションを選択できます。 指定したサービスの [トレース設定（Trace Configuration）] ウィンドウでは、すべての設定が読み取り専用として表示されます。ただし、最大ファイル数など、トレース出力設定の一部のパラメータを除きます。これらのパラメータは、トラブルシューティング トレース設定を適用した後でも変更できます。

トレース収集

各種サービス トレースやその他のログ ファイルを収集、表示、および zip 圧縮するには、Trace and Log Central（Cisco Unified Real-Time Monitoring Tool のオプション）を使用します。 Trace and Log Central オプションを使用すると、SDL/SDI トレース、アプリケーション ログ、システム ログ（イベント ビューア アプリケーション ログ、セキュリティ ログ、システム ログなど）、クラッシュ ダンプ ファイルを収集できます。

ヒント　収集したトレース ファイルの表示には Windows のメモ帳は使用しないでください。Windows のメモ帳では改行が正しく表示されません。

（注）　Unified Communications Manager のみ：暗号化をサポートするデバイスでは、Secure Real-time Transport Protocol（SRTP）のセキュア キー関連情報はトレース ファイルに表示されません。

トレース収集の詳細情報については、『*Cisco Unified Real-Time Monitoring Tool Administration Guide*』を参照してください。

着信側トレース

着信側トレースでは、トレースする電話番号または電話番号のリストを設定できます。 セッショントレースツールを使用してコールのオンデマンドトレースをリクエストできます。

詳細については、『*Cisco Unified Real-Time Monitoring Tool Administration Guide*』を参照してください。

トレース設定のセットアップ

次の手順では、Serviceabilityインターフェイスの機能およびネットワーク サービスのトレースを設定および収集する手順の概要を示します。

手順

ステップ 1　次のいずれかの手順を実行して、TLC Throttling CPU Goal および TLC Throttling IOWait Goal サービス パラメータ（Cisco RIS Data Collector サービス）の値を設定します。

- Cisco Unified Communications Manager の管理および Cisco Unified IM and Presence：**システム** > **サービス パラメータ** を選択し、TLC Throttling CPU Goal および TLC Throttling IOWait Goal サービス パラメータ（Cisco RIS Data Collector サービス）の値を設定します。
- Cisco Unity Connection のみ：Cisco Unity Connection Administrationで **[システム設定（System Settings）]** > [サービス パラメータ（Service Parameters）]を選択し、TLC Throttling CPU Goal および TLC Throttling IOWait Goal サービス パラメータ（Cisco RIS Data Collector サービス）の値を設定します。

ステップ 2　トレースを収集するサービスのトレース設定を行います。 クラスタがある場合、1 台のサーバー、またはクラスタ内のすべてのサーバーに対してサービスのトレースを設定できます。

トレース設定を行う場合、デバッグ レベルとトレース フィールドを選択してトレース ログに含める情報を選択します。

サービスで事前に設定されているトレースを実行する場合は、これらのサービスのトラブルシューティング トレースを設定します。

ステップ 3 ローカル PC に Cisco Unified Real-Time Monitoring Tool をインストールします。

ステップ 4 監視されているトレース ファイル内に指定された検索文字列が存在するときにアラームを生成する場合は、Unified RTMT の LogFileSearchStringFound アラートを有効にします。

LogFileSearchStringFound アラームは LpmTctCatalog にあります。 **[アラーム（Alarms）]** > **[定義（Definitions）]** を選択します。 [アラームの検索場所（Find alarms where）] ドロップダウン リスト ボックスで [システムアラームカタログ（System Alarm Catalog）]を選択し、[等しい（Equals）] ドロップダウン リスト ボックスで [LpmTctCatalog]を選択します）。

ステップ 5 CriticalServiceDownand CodeYellow など、アラートのトレースを自動的にキャプチャする場合は、Unified RTMT の特定のアラートの [アラート/プロパティの設定（Set Alert/Properties）] ダイアログボックスで [トレースダウンロードのイネーブル化（Enable Trace Download）]チェックボックスをオンにし、ダウンロードを実行する頻度を設定します。

ステップ 6 トレースを収集します。

ステップ 7 適切なビューアでログ ファイルを表示します。

ステップ 8 トラブルシューティング トレースをイネーブルにすると、トレース設定サービスがリセットされて、元の設定に戻ります。

（注） トラブルシューティング トレースを長時間イネーブルのままにすると、トレース ファイルのサイズが大きくなり、サービスのパフォーマンスに影響が生じるおそれがあります。

トレースの設定

ここでは、トレースの設定について説明します。

（注） トレースをイネーブルにすると、システムのパフォーマンスが低下します。そのため、トレースは、トラブルシューティング目的でのみイネーブルにします。 トレースの使用について支援が必要な場合は、テクニカル サポート チームにお問い合わせください。

トレース パラメータの設定

ここでは、Serviceability GUI で管理する機能サービスとネットワーク サービスのトレース パラメータを設定する方法について説明します。

ヒント Cisco Unity Connection では、Cisco Unified Serviceability および Cisco Unity Connection Serviceability でトレースを実行して Cisco Unity Connection の問題をトラブルシューティングする必要がある場合があります。 Cisco Unity Connection Serviceability でトレースを実行する方法については、『*Cisco Unity Connection Serviceability Administration Guide*』を参照してください。

手順

ステップ 1 **[トレース（Trace）] > [設定（Configuration）]** の順に選択します。

[トレース設定（Trace Configuration）] ウィンドウが表示されます。

ステップ 2 [サーバー（Server）] ドロップダウン リスト ボックスから、トレースを設定するサービスを実行しているサーバーを選択し、**[移動（Go）]** をクリックします。

ステップ 3 [サービス グループ（Service Group）] ドロップダウン リスト ボックスから、トレースを設定するサービスのサービス グループを選択し、[移動（Go）]をクリックします。

ヒント 「トレース設定のサービス グループ」の表に、[サービス グループ（Service Group）] ドロップダウン リスト ボックスに表示されるオプションに対応するサービスとトレース ライブラリの一覧を示します。

ステップ 4 [サービス（Service）] ドロップダウン リスト ボックスからトレースを設定するサービスを選択し、[移動（Go）]をクリックします。

ドロップダウン リスト ボックスには、アクティブなサービスと非アクティブのサービスが表示されます。

ヒント Cisco Unity Connection のみ：Cisco CallManager サービスおよび CTIManager サービスでは、SDL トレース パラメータを設定できます。 設定を行うには、いずれかのサービスの [トレース設定（Trace Configuration）] ウィンドウを開き、[関連リンク（Related Links）] ドロップダウン リスト ボックスの横にある [移動（Go）]ボタンをクリックします。

サービスのトラブルシューティング トレースを設定すると、トラブルシューティング トレース機能が設定されていることを示すメッセージがウィンドウの上部に表示されます。これは、[トレース設定（Trace Configuration）] ウィンドウのフィールドが、[トレース出力設定（Trace Output Settings）] 以外すべて無効になることを意味します。 [トレース出力設定（Trace Output Settings）] を設定するには、ステップ 11 に進みます。トラブルシューティング トレースをリセットするには、トラブルシューティング トレース設定のセットアップを参照してください。

選択したサービスのトレース パラメータが表示されます。また、[すべてのノードに適用する] チェックボックスが表示されます（Cisco Unified Communications Manager のみ）。

ステップ 5 Unified Communications Manager および IM and Presence のみ：クラスタをサポートしている設定の場合は、必要に応じて **[すべてのノードに適用（Apply to All Nodes）]** チェックボックスをオンにして、クラスタ内のすべてのサーバーにサービスのトレース設定またはトレース ライブラリを適用できます。

ステップ 6 **トレースオン**チェックボックスをオンにします。

ステップ 7 Cisco Unity Connection のみ：SDL トレース パラメータを設定している場合は、ステップ 10 に進みます。

ステップ 8 「デバッグ トレース レベルの設定」の記述に従って、トレースする情報のレベルを [デバッグ トレース レベル（Debug Trace Level）]リスト ボックスから選択します。

ステップ 9 選択したサービスの [トレースフィールド（Trace Fields）]チェックボックス（たとえば、[Cisco Log Partition Monitoring Toolトレースフィールド（Cisco Log Partition Monitoring Tool Trace Fields）]）をオンにします。

ステップ 10 アクティブ化するトレースを指定できるトレース設定がサービスに複数存在しない場合は、[すべてのトレースをイネーブル化（Enable All Trace）]チェックボックスをオンにします。 選択したサービスに複数のトレース設定がある場合は、「トレース フィールドの説明」の記述に従って、イネーブル化するトレースのチェックボックスの横にあるチェックボックスをオンにします。

ステップ 11 トレース ファイルの数とサイズを制限するには、トレース出力設定を指定します。 詳細については、トレース出力設定を参照してください。

ステップ 12 トレース パラメータの設定を保存するには、[保存（Save）]ボタンをクリックします。

トレース設定に加えた変更は、Cisco Messaging Interface 以外のすべてのサービスに即座に反映されます（Unified Communications Manager のみ）。 Cisco Messaging Interface のトレースの設定変更は、3 ～ 5 分で有効になります。

（注） デフォルトを設定するには、[デフォルトの設定（Set Default）]ボタンをクリックします。

トレース設定のサービス グループ

次の表に、[トレース設定（Trace Configuration）] ウィンドウの [サービス グループ（Service Group）] ドロップダウン リスト ボックスに表示されるオプションに対応するサービスとトレース ライブラリの一覧を示します。

表 *37:* トレース設定のサービス グループ

サービス グループ	サービスおよびトレース ライブラリ	注記
Unified Communications Manager CM サービス	• Cisco CTIManager • Cisco CallManager • Cisco CallManager Cisco IP 電話Service • Cisco DHCP Monitor サービス • Cisco Dialed Number Analyzer • Cisco Dialed Number Analyzer Server • Cisco Extended Functions、Cisco エクステンション モビリティ • Cisco Extension Mobility アプリケーション • Cisco IP Voice Media Streaming App • Cisco Messaging Interface • Cisco TFTP • Cisco Unified Mobile Voice Access Service	CM サービス グループのほとんどのサービスでは、サービスのすべてのトレースを有効化する代わりに、特定のコンポーネントのトレースを実行することができます。 [トレース（Trace）] フィールドの説明は、特定のコンポーネントのトレースを実行できるサービスを示します。
Unified Communications Manager CTI サービス	• Cisco IP Manager Assistant • Cisco Web Dialer Web Service	これらのサービスでは、サービスに対してすべてのトレースを有効化する代わりに、特定のコンポーネントのトレースを実行できます。トレース フィールドの説明を参照してください。

サービス グループ	サービスおよびトレースライブラリ	注記
Unified Communications Manager CDR サービス	• Cisco Unified Communications Manager CDR Analysis and Reporting Scheduler • Cisco Unified Communications Manager CDR Analysis and Reporting Web Service • Cisco CDR Agent • Cisco CDR Repository Manager	特定のコンポーネントのトレースを実行する代わりに、各サービスのすべてのトレースをイネーブルにします。 Cisco Unified Communications Manager CDR Analysis and Reporting では、ストアド プロシージャを呼び出すレポートが実行されると、ストアド プロシージャのロギングが開始される前に、Cisco Unified Communications Manager CDR Analysis and Reporting が [トレース設定] ウィンドウの Cisco Unified Communications Manager CDR Analysis and Reporting Scheduler サービスおよび Cisco Unified Communications Manager CDR Analysis and Reporting Web サービスの設定されたデバッグ トレース レベルを確認します。 事前生成レポートの場合は、Cisco Unified Communications Manager CDR Analysis and Reportingg が Cisco Unified Communications Manager CDR Analysis and Reporting Scheduler サービスのレベルをチェックします。オンデマンド レポートの場合は、Cisco Unified Communications Manager CDR Analysis and Reporting が Cisco Unified Communications Manager CDR Analysis and Reporting Web Service のレベルをチェックします。 [Debug Trace Level] ドロップダウン リスト ボックスから [Debug] を選択した場合、ストアドプロシージャのロギングがイネーブルにされ、ドロップダウン リスト ボックスで別のオプションを選択するまで続行されます。 以下の Cisco Unified Communications Manager CDR Analysis and Reporting レポートでは、ストアド プロシージャのロギングが使用されます。ゲートウェイ使用状況レポート、ルートおよび回線グループ使用状況レポート、ルートまたはハントリスト使用状況レポート、ルート パターンまたはハント パイロット使用状況レポート、会議コール詳細レポート、会議コール要約レポート、会議ブリッジ使用状況レポート、ボイス メッセージ使用状況レポート、CDR 検索レポート。

サービス グループ	サービスおよびトレース ライブラリ	注記
IM and Presence サービス	• Cisco Client Profile Agent • Cisco Config Agent • Cisco Intercluster Sync Agent • Cisco Login Datastore • Cisco OAM Agent • Cisco Presence Datastore • Cisco Presence Engine • Cisco IM and Presence Data Monitor • Cisco Route Datastore • Cisco SIP Proxy • Cisco SIP Registration Datastore • Cisco Server Recovery Manager • Cisco Sync Agent • Cisco XCP Authentication Service • Cisco XCP Config Manager • Cisco XCP Connection Manager • Cisco XCP Directory Service • Cisco XCP Message Archiver • Cisco XCP Router • Cisco XCP SIP Federation Connection Manager • Cisco XCP Text Conference Manager • Cisco XCP Web Connection Manager • Cisco XCP XMPP Federation Connection Manager	これらのサービスの説明については、Cisco Unified IM and Presence Serviceability の機能とネットワークサービスに関連するトピックを参照してください。 • これらのサービスでは、特定のコンポーネントのトレースを実行する代わりに、このサービスのすべてのトレースをイネーブルにする必要があります。

サービス グループ	サービスおよびトレース ライブラリ	注記
データベースおよび管理者サービス	Unified Communications Manager および Cisco Unity Connection: • Cisco AXL Web Service • Cisco CCM DBL Web Library • Cisco CCMAdmin Web Service • Cisco CCMUser Web サービス • Cisco Database Layer Monitor • Cisco UXL Web サービス Unified Communications Manager • Cisco Bulk Provisioning サービス • Cisco GRT Communications Web サービス • Cisco Role-based Security • Cisco TAPS サービス • Cisco Unified Reporting Web サービス IM and Presence Services： • Cisco AXL Web Service • Cisco Bulk Provisioning サービス • Cisco CCMUser Web サービス • Cisco Database Layer Monitor • Cisco GRT Communications Web サービス • Cisco IM and Presence Admin • Cisco Unified Reporting Web サービス • Platform Administrative Web サービス	Cisco CCM DBL Web Library オプションを選択すると、Javaアプリケーションのデータベース アクセスのトレースがアクティブ化されます。 C++ アプリケーションのデータベース アクセスの場合は、Cisco Extended Functions トレース フィールドで説明するように、Cisco Database Layer Monitor のトレースをアクティブ化します。 Unified Communications Manager をサポートする Cisco Role-based Security オプションを選択すると、ユーザ ロールの許可に対するトレースが有効となります。 データベースおよび管理者サービス グループのほとんどのサービスでは、特定のコンポーネントのトレースをイネーブルにするのではなく、サービスまたはライブラリのすべてのトレースをイネーブルにします。 Cisco Database Layer Monitor の場合、特定のコンポーネントのトレースを実行できます。 （注） サービスのロギングの制御は、Cisco Unified IM and Presence Serviceability の UI で実行できます。 ログ レベルを変更するには、[システムサービス（System Services）] グループと [Cisco CCMService Webサービス（Cisco CCMService Web Service）] を選択します。

サービス グループ	サービスおよびトレース ライブラリ	注記
パフォーマンスおよびモニタリング サービス	Unified Communications Manager および Cisco Unity Connection: • Cisco AMC サービス • Cisco CCM NCS Web Library • CCM PD Web サービス • Cisco CallManager SNMP サービス • Cisco Log Partition Monitoring Tool • Cisco RIS Data Collector • Cisco RTMT Web Service • Cisco Audit Event Service • Cisco RisBean Library Unified Communications Manager： • Cisco CCM PD Web サービス IM and Presence Services： • Cisco AMC サービス • Cisco Audit Event Service • Cisco Log Partition Monitoring Tool • Cisco RIS Data Collector • Cisco RTMT Web Service • Cisco RisBean Library	Cisco CCM NCS Web Library オプションを選択すると、Java クライアントのデータベース変更通知のトレースがアクティブ化されます。 Cisco Unity RTMT Web サービス オプションを選択すると、Unity RTMT サーブレットのトレースがアクティブ化されます。このトレースを実行すると、Unity RTMT クライアント クエリーのサーバ側のログが作成されます。
Unified Communications Manager セキュリティ サービス	• Cisco CTL Provider • Cisco Certificate Authority Proxy Function • シスコ信頼検証サービス	特定のコンポーネントのトレースを実行する代わりに、各サービスのすべてのトレースをイネーブルにします。
Unified Communications Manager ディレクトリ サービス	Cisco DirSync	特定のコンポーネントのトレースを実行する代わりに、このサービスのすべてのトレースをイネーブルにします。

サービス グループ	サービスおよびトレースライブラリ	注記
バックアップおよび復元サービス	• Cisco DRF Local • Unified Communications Manager および Cisco Unity Connection のみ： Cisco DRF Master	特定のコンポーネントのトレースを実行する代わりに、各サービスのすべてのトレースをイネーブルにします。
システム サービス	Unified Communications Manager： • Cisco CCMRealm Web Service • Cisco CCMService Web Service • Cisco Common User Interface • Cisco Trace Collection サービス IM and Presence Services： • Cisco CCMService Web Service • Cisco Trace Collection サービス	Cisco CCMRealm Web Service オプションを選択すると、ログイン認証のトレースがアクティブ化されます。 Cisco Common User Interface オプションを選択すると、複数のアプリケーションが使用する共通コードのトレースがアクティブ化されます。たとえば、Cisco Unified Operating System Administration や Cisco Unified Serviceability などが該当します。 Cisco CCMService Web Service オプションを選択すると、Cisco Unified Serviceability の Web アプリケーション（GUI）のトレースがアクティブ化されます。 特定のコンポーネントのトレースを実行する代わりに、各オプションまたはサービスのすべてのトレースを有効化します。
SOAP サービス	• CiscoSOAP Web サービス • CiscoSOAPMessage サービス	Cisco SOAP Web Service オプションを選択すると、AXL Serviceability API のトレースがアクティブ化されます。 特定のコンポーネントのトレースを実行する代わりに、このサービスのすべてのトレースをイネーブルにします。
プラットフォーム サービス	Cisco Unified OS Admin Web Service	Cisco Unified OS Admin Web Service は Cisco Unified Operating System Administration をサポートしています。これは、証明書管理、バージョンの設定、およびインストールやアップグレードなどのプラットフォーム関連の機能を管理する Web アプリケーションです。 特定のコンポーネントのトレースを実行する代わりに、このサービスのすべてのトレースをイネーブルにします。

デバッグ トレース レベルの設定

次の表に、サービスのデバッグ トレース レベル設定について説明します。

表 *38 :* サービスのデバッグ トレース レベル

レベル	説明
エラー（Error）	アラームの状態とイベントをトレースします。 異常なパスで生成されるすべてのトレースに使用します。 CPU サイクルの最小数を使用します。
特殊（Special）	すべてのエラー状態と、プロセスおよびデバイスの初期化メッセージをトレースします。
状態遷移（State Transition）	すべての特殊条件と、通常運用中に発生するサブシステムの状態遷移をトレースします。 コール処理イベントをトレースします。
重大（Significant）	通常運用時に発生するすべての状態遷移条件とメディア レイヤ イベントをトレースします。
開始/終了（Entry/Exit）	（注） すべてのサービスがこのトレース レベルを使用するわけではありません。 重要なすべての状態と、ルーチンの開始および終了点をトレースします。
任意（Arbitrary）	すべての開始および終了状態と、低レベルのデバッグ情報をトレースします。
詳細（Detailed）	すべての任意の条件と、詳細なデバッグ情報をトレースします。

次の表に、servlet のデバッグ トレース レベル設定について説明します。

表 *39 : servlet* のデバッグ トレース レベル

レベル	説明
重大（Fatal）	アプリケーションの中止を引き起こす可能性がある非常に重大なエラー イベントをトレースします。
エラー（Error）	アラームの状態とイベントをトレースします。 異常なパスで生成されるすべてのトレースに使用します。
警告（Warn）	有害な可能性のある状況をトレースします。

レベル	説明
情報（Info）	多くのサーブレットの問題をトレースします。システムパフォーマンスへの影響は最小です。
デバッグ（Debug）	通常運用時に発生するすべての状態遷移条件とメディア レイヤ イベントをトレースします。 すべてのロギングをオンにするトレース レベルです。 （注） メモリの問題を避けるため、Cisco XCP Router サービスのデバッグログを有効にしないことをお勧めします。 システムの負荷が許容できる場合、メモリ容量に基づいて非常に短い時間、システムをオンにすることができます。

トレース フィールドの説明

一部のサービスでは、サービスのすべてのトレースをイネーブルにする代わりに、特定のコンポーネントのトレースをアクティブ化できます。 次のリストに、特定のコンポーネントのトレースをアクティブにできるサービスを示します。いずれかの相互参照をクリックすると該当するセクションに移動し、サービスの各トレース フィールドの説明が表示されます。 サービスが次のリストにない場合、[トレース設定（Trace Configuration）] ウィンドウにそのサービスの [すべてのトレースをイネーブル化（Enable All Trace）] チェックボックスが表示されます。

以下ののサービスは、Unified Communications Manager および Cisco Unity Connectionで利用することができます。

- Database Layer Monitor のトレース フィールド
- Cisco RIS Data Collector のトレース フィールド

以下ののサービスは、Unified Communications Manager で利用することができます。

- Cisco CallManager SDI のトレース フィールド
- Cisco CallManager SDL のトレース フィールド
- Cisco CTIManager SDL のトレース フィールド
- Cisco Extended Functions のトレース フィールド
- Cisco エクステンション モビリティのトレース フィールド
- Cisco IP Manager Assistant のトレース フィールド
- Cisco IP Voice Media Streaming App のトレース フィールド
- Cisco TFTP のトレース フィールド
- Cisco Web Dialer Web サービスのトレース フィールド

Database Layer Monitor のトレース フィールド

次の表に、Cisco Database Layer Monitor のトレース フィールドを示します。 The Cisco Database Layer Monitor サービスは、Unified Communications Manager および Cisco Unity Connectionをサポートします。

表 *40 : Cisco Database Layer Monitor* のトレース フィールド

フィールド名	説明
DB ライブラリ トレースのイネーブル化（Enable DB Library Trace）	C++アプリケーションのデータベース ライブラリのトレースをアクティブ化します。
サービスのトレースのイネーブル化（Enable Service Trace）	サービスのトレースをアクティブ化します。
DB変更通知のトレースのイネーブル化（Enable DB Change Notification Trace）	C++アプリケーションのデータベース変更通知トレースを有効にします。
単体試験のトレースのイネーブル化（Enable Unit Test Trace）	このチェックボックスはオンにしないでください。デバッグ目的でシスコのエンジニアが使用します。

Cisco RIS Data Collector のトレース フィールド

次の表に、Cisco RIS Data Collector のトレース フィールドを示します。 Cisco RIS Data Collector サービスは、Unified Communications Manager および Cisco Unity Connectionをサポートします。

表 *41 : Cisco RIS Data Collector* のトレース フィールド

フィールド名	説明
RISDC のトレースのイネーブル化（Enable RISDC Trace）	RIS データ コレクタ サービス（RIS）の RISDC スレッドのトレースをアクティブ化します。
システムアクセスのトレースのイネーブル化（Enable System Access Trace）	RIS データ コレクタのシステム アクセス ライブラリのトレースをアクティブ化します。
リンクサービスのトレースのイネーブル化（Enable Link Services Trace）	RIS データ コレクタのリンク サービス ライブラリのトレースをアクティブ化します。
RISDCアクセスのトレースのイネーブル化（Enable RISDC Access Trace）	RIS データ コレクタの RISDC アクセス ライブラリのトレースをアクティブ化します。
RISDB のトレースのイネーブル化（Enable RISDB Trace）	RIS データ コレクタの RISDB ライブラリのトレースを有効にします。
PI のトレースのイネーブル化（Enable PI Trace）	RIS データ コレクタの PI ライブラリのトレースを有効にします。

フィールド名	説明
XML のトレースのイネーブル化（Enable XML Trace）	RIS データ コレクタ サービスの入出力 XML メッセージのトレースを有効にします。
Perfmon ロガーのトレースのイネーブル化（Enable Perfmon Logger Trace）	RIS データ コレクタの perfmon データ ロギングをトラブルシューティングするためのトレースを有効にします。 ログ ファイル、記録されたカウンタの総数、アプリケーションおよびシステム カウンタとインスタンスの名前、プロセスとスレッドの CPU パーセンテージの計算、ログ ファイルのロールオーバーと削除の発生をトレースするために使用します。

Cisco CallManager SDI のトレース フィールド

次の表に、Cisco CallManager SDI のトレース フィールドを示します。 Cisco CallManager サービスは、Unified Communications Manager をサポートします。

表 *42 : Cisco CallManager SDI* のトレース フィールド

フィールド名	説明
H245メッセージのトレースのイネーブル化（Enable H245 Message Trace）	H245 メッセージのトレースをアクティブ化します。
DT-24+/DE-30+のトレースのイネーブル化（Enable DT-24+/DE-30+ Trace）	DT-24+/DE-30+ デバイス トレースの ISDN タイプのロギングをアクティブ化します。
PRIのトレースのイネーブル化（Enable PRI Trace）	一次群速度インターフェイス（PRI）デバイスのトレースをアクティブ化します。
ISDN変換のトレースのイネーブル化（Enable ISDN Translation Trace）	ISDN メッセージ トレースをアクティブ化します。 通常のデバッグに使用します。
H225とゲートキーパーのトレースのイネーブル化（Enable H225 & Gatekeeper Trace）	H.225 デバイスのトレースをアクティブ化します。 通常のデバッグに使用します。
各種のトレースのイネーブル化（Enable Miscellaneous Trace）	各種デバイスのトレースをアクティブ化します。 （注） 通常のシステム動作中はこのチェック ボックスをオンにしないでください。
会議ブリッジのトレースのイネーブル化（Enable Conference Bridge Trace）	会議ブリッジのトレースをアクティブ化します。 通常のデバッグに使用します。

フィールド名	説明
保留音のトレースのイネーブル化（Enable Music on Hold Trace）	保留音（MOH）デバイスのトレースをアクティブ化します。 Unified Communications Managerへの登録、Unified Communications Managerへの登録解除、リソース割り当ての成功または失敗など、MOH デバイスのステータスのトレースのために使用されます。
Unified CM リアルタイム情報サーバーのトレースのイネーブル化（Enable Unified CM Real-Time Information Server Trace）	Real-time Information Server が使用する Unified Communications Manager のリアルタイム情報トレースを有効化します。
SIPスタックのトレースのイネーブル化（Enable SIP Stack Trace）	SIP スタックのトレースをアクティブ化します。デフォルトではイネーブルになっています。
アナンシエータのトレースのイネーブル化（Enable Annunciator Trace）	Unified Communications Manager が、Cisco Unified IP Phone、ゲートウェイ、およびその他の設定可能なデバイスへ、録音済みの音声案内（.wav ファイル）とトーンを再生できるようにするために、Cisco IP Voice Media Streaming Application サービスを使用する SCCP デバイスである Annunciator のトレースを有効化します。
CDR のトレースのイネーブル化（Enable CDR Trace）	CDR のトレースをアクティブ化します。
アナログ トランクのトレースのイネーブル化（Enable Analog Trunk Trace）	すべてのアナログ トランク（AT）ゲートウェイのトレースをアクティブ化します。
すべての電話機のトレースのイネーブル化（Enable All Phone Device Trace）	電話機のトレースをアクティブ化します。 トレース情報にはソフトフォンデバイスが含まれます。 通常のデバッグに使用します。
MTPのトレースのイネーブル化（Enable MTP Trace）	メディア ターミネーション ポイント（MTP）デバイスのトレースをアクティブ化します。 通常のデバッグに使用します。
すべてのゲートウェイトレースのイネーブル化（Enable All Gateway Trace）	すべてのアナログおよびデジタル ゲートウェイのトレースをアクティブ化します。
転送と各種のトレースのイネーブル化（Enable Forward and Miscellaneous Trace）	別のチェックボックスで対象にされていないコール転送およびすべてのサブシステムのトレースをアクティブ化します。 通常のデバッグに使用します。

フィールド名	説明
MGCPのトレースのイネーブル化（Enable MGCP Trace）	メディア ゲートウェイ コントロール プロトコル（MGCP）デバイスのトレースをアクティブ化します。 通常のデバッグに使用します。
メディアリソースマネージャのトレースのイネーブル化（Enable Media Resource Manager Trace）	メディア リソース マネージャ（MRM）のアクティビティのトレースをアクティブ化します。
SIP呼処理のトレースのイネーブル化（Enable SIP Call Processing Trace）	SIP 呼処理のトレースをアクティブ化します。
SCCPキープアライブのトレースのイネーブル化（Enable SCCP Keep Alive Trace）	Cisco CallManager トレースの SCCP キープアライブ トレース情報のトレースをアクティブ化します。 各 SCCP デバイスは 30 秒ごとにキープアライブ メッセージをレポートし、各キープアライブ メッセージは 3 行のトレース データを作成するため、このチェックボックスがオンの場合大量のトレース データが生成されます。
SIPキープアライブ(REGISTER Refresh)のトレースのイネーブル化（Enable SIP Keep Alive (REGISTER Refresh) Trace）	Cisco CallManager トレースの SIP キープアライブ（REGISTER Refresh）トレース情報のトレースをアクティブ化します。 各 SIP デバイスは 2 秒ごとにキープアライブ メッセージをレポートし、各キープアライブ メッセージは複数行のトレース データを作成するため、このチェックボックスがオンの場合大量のトレース データが生成されます。

Cisco CallManager SDL のトレース フィールド

次の表で、Cisco CallManager SDL のトレース フィールド設定について説明します。 Cisco CallManager サービスは、Unified Communications Manager をサポートします。

（注） シスコのエンジニアから指示された場合を除き、デフォルト設定を使用することを推奨します。

表 *43 : Cisco CallManager SDL* の設定に対するトレース フィルタの設定

設定名	説明
すべてのレイヤ1トレースのイネーブル化。（Enable all Layer 1 traces.）	レイヤ 1 のトレースをアクティブ化します。

設定名	説明
詳細なレイヤ1のトレースのイネーブル化。（Enable detailed Layer 1 traces.）	詳細なレイヤ 1 のトレースをアクティブ化します。
すべてのレイヤ2トレースのイネーブル化。（Enable all Layer 2 traces.）	レイヤ 2 のトレースをアクティブ化します。
レイヤ2インターフェイスのトレースのイネーブル化。（Enable Layer 2 interface trace.）	レイヤ 2 インターフェイスのトレースをアクティブ化します。
レイヤ2TCPのトレースのイネーブル化。（Enable Layer 2 TCP trace.）	レイヤ 2 伝送制御プログラム（TCP）のトレースをアクティブ化します。
詳細なダンプレイヤ2のトレースのイネーブル化。（Enable detailed dump Layer 2 trace.）	ダンプ レイヤ 2 の詳細なトレースをアクティブ化します。
すべてのレイヤ3トレースのイネーブル化。（Enable all Layer 1 traces.）	レイヤ 3 のトレースをアクティブ化します。
すべてのコール制御のトレースのイネーブル化。（Enable all call control traces.）	コール制御のトレースをアクティブ化します。
各種のポーリングのトレースのイネーブル化。（Enable miscellaneous polls trace.）	さまざまなポーリングに対するトレースをアクティブ化します。
各種のトレース(データベース信号)のイネーブル化。（Enable miscellaneous trace (database signals).）	データベースの信号のようなさまざまなトレースをアクティブ化します。
メッセージ変換信号のトレースのイネーブル化。（Enable message translation signals trace.）	メッセージ変換信号のトレースをアクティブ化します。
UUIEの出力のトレースのイネーブル化。（Enable UUIE output trace.）	ユーザ間情報要素（UUIE）の出力のトレースをアクティブ化します。
ゲートウェイ信号のトレースのイネーブル化。（Enable gateway signals trace.）	ゲートウェイ信号のトレースをアクティブ化します。
CTIのトレースのイネーブル化。（Enable CTI trace.）	CTI のトレースをアクティブ化します。
ネットワークサービスのデータのトレースのイネーブル化（Enable network service data trace）	ネットワーク サービスのデータのトレースをアクティブ化します。
ネットワークサービスのイベントのトレースのイネーブル化（Enable network service event trace）	ネットワーク サービスのイベントのトレースをアクティブ化します。
ICCP管理のトレースのイネーブル化（Enable ICCP admin trace）	ICCP 管理のトレースをアクティブ化します。

設定名	説明
デフォルトのトレースのイネーブル化（Enable default trace）	デフォルトのトレースをアクティブ化します。

次の表で、Cisco CallManager SDL 設定の特性について説明します。

表 *44 : Cisco CallManager SDL* の設定に対するトレースの特性

特性	説明
SDLリンクステートのトレースのイネーブル化。（Enable SDL link states trace.）	クラスタ内通信プロトコル（ICCP）リンク ステートのトレースをアクティブ化します。
低レベルのSDLのトレースのイネーブル化。（Enable low-level SDL trace.）	低レベルの SDL のトレースをアクティブ化します。
SDLリンクのポーリングのトレースのイネーブル化。（Enable SDL link poll trace.）	ICCP リンクのポーリングのトレースをアクティブ化します。
SDLリンクメッセージのトレースのイネーブル化。（Enable SDL link messages trace.）	ICCP 未処理メッセージのトレースをアクティブ化します。
信号データのダンプのトレースのイネーブル化。（Enable signal data dump trace.）	信号データのダンプに対するトレースをアクティブ化します。
相関タグのマッピングのトレースのイネーブル化。（Enable correlation tag mapping trace.）	相関タグのマッピングに対するトレースをアクティブ化します。
SDLプロセスの状態のトレースのイネーブル化。（Enable SDL process states trace.）	SDL プロセスの状態に対するトレースをアクティブ化します。
SDLのprettyプリントのトレースの無効化。（Disable pretty print of SDL trace.）	SDL の pretty プリントに対するトレースを無効化します。 pretty プリントでは、後処理を実行しないでトレース ファイルにタブとスペースを追加します。
SDL TCPイベントのトレースのイネーブル化。（Enable SDL TCP event trace.）	SDL TCP イベントのトレースをアクティブ化します。

Cisco CTIManager SDL のトレース フィールド

次の表で、Cisco CTIManager SDL 設定のトレース フィルタの設定について説明します。 Cisco CTIManager サービスは Unified Communications Manager をサポートします。

ヒント シスコのエンジニアから指示された場合を除き、デフォルト設定を使用することを推奨します。

ヒント [サービスグループ（Service Groups）] ドロップダウン リスト ボックスから CTIManager サービスを選択すると、[トレース設定（Trace Configuration）] ウィンドウにこのサービスの SDI トレースが表示されます。 Cisco CTI Manager サービスに対する SDI トレースをアクティブ化するには、[トレース設定（Trace Configuration）] ウィンドウで Cisco CTIManager サービスに対して [すべてのトレースをイネーブル化（Enable All Trace）]をオンにします。 [SDL設定（SDL Configuration）] ウィンドウにアクセスするには、[関連リンク（Related Links）] ドロップダウン リスト ボックスから [SDL設定（SDL Configuration）]を選択します。Cisco CTIManager の SDL 設定に対するトレース フィルタ設定テーブルと Cisco CTIManager SDL の設定に対するトレースの特性テーブルに示されている設定が表示されます。

表 *45 : Cisco CTIManager* の *SDL* 設定に対するトレース フィルタ設定

設定名	説明
各種のポーリングのトレースのイネーブル化。（Enable miscellaneous polls trace.）	さまざまなポーリングに対するトレースをアクティブ化します。
各種のトレース(データベース信号)のイネーブル化。（Enable miscellaneous trace (database signals).）	データベースの信号のようなさまざまなトレースをアクティブ化します。
CTIのトレースのイネーブル化。（Enable CTI trace.）	CTI のトレースをアクティブ化します。
ネットワークサービスのデータのトレースのイネーブル化（Enable network service data trace）	ネットワーク サービスのデータのトレースをアクティブ化します。
ネットワークサービスのイベントのトレースのイネーブル化（Enable network service event trace）	ネットワーク サービスのイベントのトレースをアクティブ化します。
ICCP管理のトレースのイネーブル化（Enable ICCP admin trace）	ICCP 管理のトレースをアクティブ化します。
デフォルトのトレースのイネーブル化（Enable Default Trace）	デフォルトのトレースをアクティブ化します。

次の表で、Cisco CTIManager SDL 設定のトレースの特性について説明します。

表 *46 : Cisco CTIManager SDL* の設定に対するトレースの特性

特性	説明
SDLリンクステートのトレースのイネーブル化。（Enable SDL link states trace.）	ICCP リンク ステートのトレースをアクティブ化します。

特性	説明
低レベルのSDLのトレースのイネーブル化。（Enable low-level SDL trace.）	低レベルの SDL のトレースをアクティブ化します。
SDLリンクのポーリングのトレースのイネーブル化。（Enable SDL link poll trace.）	ICCP リンクのポーリングのトレースをアクティブ化します。
SDLリンクメッセージのトレースのイネーブル化。（Enable SDL link messages trace.）	ICCP 未処理メッセージのトレースをアクティブ化します。
信号データのダンプのトレースのイネーブル化。（Enable signal data dump trace.）	信号データのダンプに対するトレースをアクティブ化します。
相関タグのマッピングのトレースのイネーブル化。（Enable correlation tag mapping trace.）	相関タグのマッピングに対するトレースをアクティブ化します。
SDLプロセスの状態のトレースのイネーブル化。（Enable SDL process states trace.）	SDL プロセスの状態に対するトレースをアクティブ化します。
SDLのprettyプリントのトレースの無効化。（Disable pretty print of SDL trace.）	SDL の pretty プリントに対するトレースを無効化します。 pretty プリントでは、後処理を実行しないでトレース ファイルにタブとスペースを追加します。
SDL TCPイベントのトレースのイネーブル化（Enable SDL TCP Event trace）	SDL TCP イベントのトレースをアクティブ化します。

Cisco Extended Functions のトレース フィールド

次の表に、Cisco Extended Functions のトレース フィールドについて説明します。 Cisco Extended Functions サービスは Unified Communications Manager をサポートします。

表 *47 : Cisco Extended Functions* のトレース フィールド

フィールド名	説明
QBEヘルパーCTIのトレースのイネーブル化（Enable QBE Helper TSP Trace）	テレフォニー サービス プロバイダーのトレースをアクティブ化します。
QBEヘルパーTSPIのトレースのイネーブル化（Enable QBE Helper TSPI Trace）	QBE ヘルパー TSP インターフェイスのトレースをアクティブ化します。
QRTディクショナリのトレースのイネーブル化（Enable QRT Dictionary Trace）	品質レポート ツールのサービスのディクショナリのトレースをアクティブ化します。
DOMヘルパーのトレースのイネーブル化（Enable DOM Helper Traces）	DOM ヘルパーのトレースをアクティブ化します。

フィールド名	説明
冗長性および変更通知のトレースのイネーブル化（Enable Redundancy and Change Notification Trace）	データベース変更通知のトレースをアクティブ化します。
QRTレポートハンドラのトレースのイネーブル化（Enable QRT Report Handler Trace）	品質レポート ツールのレポート ハンドラのトレースをアクティブ化します。
QBEヘルパーCTIのトレースのイネーブル化（Enable QBE Helper CTI Trace）	QBE ヘルパー CTI のトレースをアクティブ化します。
QRTサービスのトレースのイネーブル化（Enable QRT Service Trace）	品質レポート ツールのサービスに関連するトレースをアクティブ化します。
QRT DBのトレースのイネーブル化（Enable QRT DB Traces）	QRT DB アクセスのトレースをアクティブ化します。
テンプレートマップのトレースのイネーブル化（Enable Template Map Traces）	標準テンプレートマップおよびマルチマップのトレースをアクティブ化します。
QRTイベントハンドラのトレースのイネーブル化（Enable QRT Event Handler Trace）	品質レポート ツールのイベント ハンドラのトレースをアクティブ化します。
QRTリアルタイム情報サーバーのトレースのイネーブル化（Enable QRT Real-Time Information Server Trace）	品質レポートツールのリアルタイム情報サーバーのトレースをアクティブ化します。

Cisco エクステンション モビリティのトレース フィールド

次の表に、Cisco エクステンション モビリティのトレース フィールドを示します。 Cisco Extension Mobility サービスは Unified Communications Manager をサポートします。

表 *48 : Cisco* エクステンション モビリティのトレース フィールド

フィールド名	説明
EMサービスのトレースのイネーブル化（Enable EM Service Trace）	Cisco エクステンション モビリティ サービスのトレースをアクティブ化します。

ヒント Cisco エクステンション モビリティ アプリケーション サービスのトレースをアクティブ化する場合は、Cisco エクステンション モビリティ アプリケーション サービスの [トレースの設定（Trace Configuration）] ウィンドウで [すべてのトレースのイネーブル化（Enable All Trace）] チェックボックスをオンにします。

Cisco IP Manager Assistant のトレース フィールド

次の表に、Cisco IP Manager Assistant のトレース フィールドを示します。 Cisco IP Manager Assistant サービスは、Cisco Unified Communications Manager Assistant をサポートしています。

表 *49 : Cisco IP Manager Assistant* のトレース フィールド

フィールド名	説明
IPMAサービスのトレースのイネーブル化（Enable IPMA Service Trace）	Cisco IP Manager Assistant サービスのトレースをアクティブ化します。
IPMA Managerの設定変更ログのイネーブル化（Enable IPMA Manager Configuration Change Log）	マネージャとアシスタントの設定に加えた変更のトレースをアクティブ化します。
IPMA CTIのトレースのイネーブル化（Enable IPMA CTI Trace）	CTI Managerの接続に対するトレースをアクティブ化します。
IPMA CTIセキュリティのトレースのイネーブル化（Enable IPMA CTI Security Trace）	CTIManagerのセキュアな接続に対するトレースをアクティブ化します。

Cisco IP Voice Media Streaming App のトレース フィールド

ここで説明する内容は、Cisco Unity Connection には適用されません。

次の表で、Cisco IP Voice Media Streaming App のトレース フィールドについて説明します。 Cisco IP Voice Media Streaming アプリ サービスは、Unified Communications Manager をサポートします。

表 *50 : Cisco IP Voice Media Streaming Application* のトレース フィールド

フィールド名	説明
サービス初期化のトレースのイネーブル化（Enable Service Initialization Trace）	初期化情報のトレースをアクティブ化します。
MTPデバイスのトレースのイネーブル化（Enable MTP Device Trace）	メディア ターミネーション ポイント（MTP）用に処理されたメッセージをモニタするトレースをアクティブ化します。
デバイスリカバリのトレースのイネーブル化（Enable Device Recovery Trace）	MTP、会議ブリッジ、MOH に対するデバイスリカバリ情報のトレースをアクティブ化します。
Skinny Stationメッセージのトレースのイネーブル化（Enable Skinny Station Messages Trace）	Skinny Station Protocol のトレースをアクティブ化します。

フィールド名	説明
WinSockレベル2のトレースのイネーブル化（Enable WinSock Level 2 Trace）	高レベルで詳細なWinSock関連情報のトレースをアクティブ化します。
保留音マネージャのトレースのイネーブル化（Enable Music On Hold Manager Trace）	MOH オーディオ ソース マネージャをモニタするトレースをアクティブ化します。
アナンシエータのトレースのイネーブル化（Enable Annunciator Trace）	アナンシエータをモニタするトレースをアクティブ化します。
DB設定マネージャのトレースのイネーブル化（Enable DB Setup Manager Trace）	MTP、会議ブリッジ、MOHに対するデータベース設定や変更をモニタするトレースをアクティブ化します。
会議ブリッジデバイスのトレースのイネーブル化（Enable Conference Bridge Device Trace）	会議ブリッジ用に処理されたメッセージをモニタするトレースをアクティブ化します。
デバイスドライバのトレースのイネーブル化（Enable Device Driver Trace）	デバイス ドライバのトレースをアクティブ化します。
WinSockレベル1のトレースのイネーブル化（Enable WinSock Level 1 Trace）	低レベルで一般的なWinSock関連情報のトレースをアクティブ化します。
保留音デバイスのトレースのイネーブル化（Enable Music on Hold Device Trace）	MOH 用に処理されたメッセージをモニタするトレースをアクティブ化します。
TFTPダウンロードのトレースのイネーブル化（Enable TFTP Downloads Trace）	MOH オーディオ ソース ファイルのダウンロードをモニタするトレースをアクティブ化します。

Cisco TFTP のトレース フィールド

次の表に、Cisco TFTP のトレース フィールドを示します。 Cisco TFTP サービスは、Unified Communications Manager をサポートします。

表 *51 : Cisco TFTP* のトレース フィールド

フィールド名	説明
サービスシステムのトレースのイネーブル化（Enable Service System Trace）	サービス システムのトレースをアクティブ化します。
ビルドファイルのトレースのイネーブル化（Enable Build File Trace）	ビルドファイルのトレースをアクティブ化します。
サーブファイルのトレースのイネーブル化（Enable Serve File Trace）	サーブ ファイルのトレースをアクティブ化します。

Cisco Web Dialer Web サービスのトレース フィールド

次の表に、Cisco Web Dialer Web サービスのトレース フィールドについて説明します。 Cisco Web Dialer Web Service は Unified Communications Manager をサポートします。

表 *52 : Cisco Web Dialer Web* サービスのトレース フィールド

フィールド名	説明
Web Dialer Servletのトレースのイネーブル化（Enable Web Dialer Servlet Trace）	Cisco Web Dialer Servlet のトレースをアクティブ化します。
Redirector Servletのトレースのイネーブル化（Enable Redirector Servlet Trace）	Redirector Servlet のトレースをアクティブ化します。

IM and Presence SIP Proxy サービスのトレース フィルタの設定

次の表では、IM and Presence SIP Proxy のトレース フィルタの設定について説明します。

表 *53 : IM and Presence SIP Proxy* サービスのトレース フィルタの設定

パラメータ	説明
Access Log のトレースのイネーブル化（Enable Access Log Trace）	プロキシ アクセス ログ トレースをイネーブルにします。プロキシが受信した各 SIP メッセージの先頭行がログに記録されます。
Authentication のトレースのイネーブル化（Enable Authentication Trace）	認証モジュールのトレースをイネーブルにします。
Calendar のトレースのイネーブル化（Enable CALENDAR Trace）	カレンダー モジュールのトレースをイネーブルにします。
CTI ゲートウェイのトレースのイネーブル化（Enable CTI Gateway Trace）	CTI ゲートウェイのトレースをイネーブルにします。
Enum のトレースのイネーブル化（Enable Enum Trace）	Enum モジュールのトレースをイネーブルにします。

パラメータ	説明
Method/Event ルーティングのトレースのイネーブル化（Enable Method/Event Routing Trace）	メソッド/イベント ルーティング モジュールのトレースをイネーブルにします。
Number Expansion のトレースのイネーブル化（Enable Number Expansion Trace）	Number Expansion モジュールのトレースをイネーブルにします。
Parser のトレースのイネーブル化（Enable Parser Trace）	sipd の子 SIP パーサーの動作に関係するパーサー情報のトレースをイネーブルにします。
Privacy のトレースのイネーブル化（Enable Privacy Trace）	プライバシーリクエストに関する PAI、RPID、および Diversion ヘッダーの処理に関する情報のトレースをイネーブルにします。
Registry のトレースのイネーブル化（Enable Registry Trace）	Registry モジュールのトレースをイネーブルにします。
Routing のトレースのイネーブル化（Enable Routing Trace）	Routing モジュールのトレースをイネーブルにします。
SIPUA トレースのイネーブル化（Enable SIPUA Trace）	SIP UA アプリケーション モジュールのトレースをイネーブルにします。
Server のトレースのイネーブル化（Enable Server Trace）	Server のトレースをイネーブルにします。
SIP メッセージとステート マシンのトレースのイネーブル化（Enable SIP Message and State Machine Trace）	sipd ごとの SIP マシンの動作に関係する情報のトレースをイネーブルにします。
SIP TCP のトレースのイネーブル化（Enable SIP TCP Trace）	TCP サービスによる SIP メッセージの TCP トランスポートのトレースをイネーブルにします。

パラメータ	説明
SIP TLS のトレースのイネーブル化（Enable SIP TLS Trace）	TCP サービスによる SIP メッセージの TLS トランスポートのトレースをイネーブルにします。
SIP XMPP IM ゲートウェイ トレースのイネーブル化（Enable SIP XMPP IM Gateway Trace）	SIP XMPP IM ゲートウェイのトレースをイネーブルにします。
Presence Web Service のトレースのイネーブル化（Enable Presence Web Service Trace）	Presence Web Service のトレースをイネーブルにします。

IM and Presence のトレース フィールドの説明

次の表では、特定のコンポーネントに対するトレースのアクティブ化をサポートしているサービスのフィールドについて説明します。一部のサービスでは、サービスのすべてのトレースをイネーブルにする代わりに、特定のコンポーネントのトレースをアクティブ化できます。この章にないサービスの場合は、[トレース設定（Trace Configuration）] ウィンドウで、そのサービスに [すべてのトレースをイネーブル化（Enable All Trace）] が表示されます。

Cisco Access Log のトレース フィールド

次の表に、Cisco Access Log のトレース フィールドを示します。

表 *54 : Access Log* のトレース フィールド

フィールド名	説明
Access Log のトレースのイネーブル化（Enable Access Log Trace）	Access Log のトレースを有効にします。

Cisco Authentication のトレース フィールド

次の表に、Cisco Authentication のトレース フィールドを示します。

表 *55 : Authentication* のトレース フィールド

フィールド名	説明
Authentication のトレースのイネーブル化（Enable Authentication Trace）	認証トレースを有効にします。

Cisco Calendar のトレース フィールド

次の表に、Cisco Calendar のトレース フィールドを示します。

表 *56 : Calendar* のトレース フィールド

フィールド名	説明
Calendar のトレースのイネーブル化（Enable CALENDAR Trace）	Calendar のトレースを有効にします。

Cisco CTI ゲートウェイのトレース フィールド

次の表に、Cisco CTI ゲートウェイのトレース フィールドを示します。

表 *57 : CTI* ゲートウェイのトレース フィールド

フィールド名	説明
CTI ゲートウェイのトレースのイネーブル化（Enable CTI Gateway Trace）	CTI ゲートウェイのトレースを有効にします。

Cisco Database Layer Monitor のトレース フィールド

次の表に、Cisco Database Layer Monitor のトレース フィールドを示します。

表 *58 : Cisco Database Layer Monitor* のトレース フィールド

フィールド名	説明
DB ライブラリ トレースのイネーブル化（Enable DB Library Trace）	C++アプリケーションのデータベース ライブラリのトレースをイネーブルにします。
サービスのトレースのイネーブル化（Enable Service Trace）	サービスのトレースをイネーブルにします。
DB変更通知のトレースのイネーブル化（Enable DB Change Notification Trace）	C++アプリケーションのデータベース変更通知トレースを有効にします。
単体試験のトレースのイネーブル化（Enable Unit Test Trace）	オンにしないでください。デバッグ目的でシスコのエンジニアが使用します。

Cisco Enum のトレース フィールド

次の表に、Cisco Enum のトレース フィールドを示します。

表 *59 : Enum* のトレース フィールド

フィールド名	説明
Enum のトレースのイネーブル化（Enable Enum Trace）	Enum のトレースをアクティブ化します。

Cisco Method/Event のトレース フィールド

次の表に、Cisco Method/Event のトレース フィールドを示します。

表 *60 : Method/Event* のトレース フィールド

フィールド名	説明
Method/Event のトレースのイネーブル化（Enable Method/Event Trace）	Method/Event のトレースをイネーブルにします。

Cisco Number Expansion のトレース フィールド

次の表に、Cisco Number Expansion のトレース フィールドを示します。

表 *61 : Number Expansion* のトレース フィールド

フィールド名	説明
Number Expansion のトレースのイネーブル化（Enable Number Expansion Trace）	Number Expansion のトレースを有効にします。

Cisco Parser のトレース フィールド

次の表に、Cisco Parser のトレース フィールドを示します。

表 *62 : Parser* のトレース フィールド

フィールド名	説明
Parser のトレースのイネーブル化（Enable Parser Trace）	Parser のトレースを有効にします。

Cisco Privacy のトレース フィールド

次の表に、Cisco Privacy のトレース フィールドを示します。

表 *63 : Privacy* のトレース フィールド

フィールド名	説明
Privacy のトレースのイネーブル化（Enable Privacy Trace）	Privacy のトレースをアクティブ化します。

Cisco Proxy のトレース フィールド

次の表に、Cisco Proxy のトレース フィールドを示します。

表 *64 : Proxy* のトレース フィールド

フィールド名	説明
プロキシの追加（Add Proxy）	Proxy のトレースをアクティブ化します。

Cisco RIS Data Collector のトレース フィールド

次の表に、Cisco RIS Data Collector のトレース フィールドを示します。

表 *65 : Cisco RIS Data Collector* のトレース フィールド

フィールド名	説明
RISDC のトレースのイネーブル化（Enable RISDC Trace）	RIS データ コレクタ サービス（RIS）の RISDC スレッドのトレースをアクティブ化します。
システムアクセスのトレースのイネーブル化（Enable System Access Trace）	RIS データ コレクタのシステム アクセス ライブラリのトレースをアクティブ化します。
リンクサービスのトレースのイネーブル化（Enable Link Services Trace）	RIS データ コレクタのリンク サービス ライブラリのトレースをアクティブ化します。
RISDCアクセスのトレースのイネーブル化（Enable RISDC Access Trace）	RIS データ コレクタの RISDC アクセス ライブラリのトレースをアクティブ化します。
RISDB のトレースのイネーブル化（Enable RISDB Trace）	RIS データ コレクタの RISDB ライブラリのトレースを有効にします。
PI のトレースのイネーブル化（Enable PI Trace）	RIS データ コレクタの PI ライブラリのトレースを有効にします。
XML のトレースのイネーブル化（Enable XML Trace）	RIS データ コレクタ サービスの入出力 XML メッセージのトレースを有効にします。

フィールド名	説明
Perfmon ロガーのトレースのイネーブル化（Enable Perfmon Logger Trace）	RIS データ コレクタの perfmon データ ロギングをトラブルシューティングするためのトレースを有効にします。 ログ ファイル、記録されたカウンタの総数、アプリケーションおよびシステム カウンタとインスタンスの名前、プロセスとスレッドの CPU パーセンテージの計算、ログ ファイルのロールオーバーと削除の発生をトレースするために使用します。

Cisco Registry のトレース フィールド

次の表に、Cisco Registry のトレース フィールドを示します。

表 *66 : Registry* のトレース フィールド

フィールド名	説明
Registry のトレースのイネーブル化（Enable Registry Trace）	Registry のトレースを有効にします。

Cisco Routing のトレース フィールド

次の表に、Cisco Routing のトレース フィールドを示します。

表 *67 : Routing* のトレース フィールド

フィールド名	説明
Routing のトレースのイネーブル化（Enable Routing Trace）	ルーティング トレースを有効にします。

Cisco Server のトレース フィールド

次の表に、Cisco Server のトレース フィールドを示します。

表 *68 : Server* のトレース フィールド

フィールド名	説明
Server のトレースのイネーブル化（Enable Server Trace）	Server のトレースをアクティブ化します。

Cisco SIP Message と State Machine のトレース フィールド

次の表に、Cisco SIP Message と State Machine のトレース フィールドを示します。

表 *69 : SIP Message* と *State Machine* のトレース フィールド

フィールド名	説明
SIP メッセージとステート マシンのトレースのイネーブル化（Enable SIP Message and State Machine Trace）	SIP メッセージとステート マシンのトレースを有効にします。

Cisco SIP TCP のトレース フィールド

次の表に、Cisco SIP TCP のトレース フィールドを示します。

表 *70 : SIP TCP* のトレース フィールド

フィールド名	説明
SIP TCP のトレースのイネーブル化（Enable SIP TCP Trace）	SIP TCP のトレースを有効にします。

Cisco SIP TLS のトレース フィールド

次の表に、Cisco SIP TLS のトレース フィールドを示します。

表 *71 : SIP TLS* のトレース フィールド

フィールド名	説明
SIP TLS のトレースのイネーブル化（Enable SIP TLS Trace）	SIP TLS のトレースを有効にします。

Cisco Web Service のトレース フィールド

次の表に、Cisco Web Service のトレース フィールドを示します。

表 *72 : Web Service* のトレース フィールド

フィールド名	説明
Presence Web Service のトレースのイネーブル化（Enable Presence Web Service Trace）	Presence Web Service のトレースを有効にします。

トレース出力設定

次の表に、トレース ログ ファイルの説明を示します。

注意 [トレース設定（Trace Configuration）] ウィンドウで [最大ファイル数（Maximum No. of Files）] または [最大ファイル サイズ（Maximum File Size）] を変更すると、サービスが実行中の場合は現在のファイル以外のすべてのサービス ログ ファイルが削除されます。サービスがアクティブ化されていない場合は、サービスをアクティブ化したときにただちにファイルが削除されます。 ログファイルの記録を保持する必要がある場合は、[最大ファイル数（Maximum No. of Files）] または [最大ファイルサイズ（Maximum File Size）] の設定を変更する前に、サービス ログファイルをダウンロードして別のサーバーに保存してください。そのためには、Unity RTMT の Trace and Log Central を使用します。

表 *73*：トレース出力設定

フィールド	説明
最大ファイル数（Maximum number of files）	指定したサービスのトレース ファイルの総数を指定します。 Cisco Unified Serviceability では、ファイルを識別するために、cus299.txt のようにファイル名にシーケンス番号が自動的に追加されます。 シーケンス中の最後のファイルが一杯になると、最初のファイルのトレースデータが上書きされます。 デフォルトはサービスによって異なります。
最大ファイル サイズ(MB)（Maximum file size (MB)）	トレース ファイルの最大サイズ（MB 単位）を指定します。 デフォルトはサービスによって異なります。

トレース設定のトラブルシューティング

トラブルシューティング トレース設定ウィンドウ

[トラブルシューティング トレース設定（Troubleshooting Trace Settings）]ウィンドウでは、事前に設定されたトラブルシューティング トレース設定を行う Serviceability GUI のサービスを選択できます。 このウィンドウでは、クラスタ内の異なるノードに対してサービスを選択できます。 これにより、選択したすべてのサービスのトレース設定の変更が行われます。 1 台のノードの特定のアクティブなサービスの選択、そのノードのすべてのアクティブなサービスの選択、クラスタ内のすべてのノードの特定のアクティブなサービスの選択、クラスタ内のすべてのノードのすべてのアクティブなサービスの選択が可能です。 このウィンドウでは、非アクティブなサーバーの横に [N/A] と表示されます。

（注） IM and Presence の場合、IM and Presence 機能またはネットワーク サービスの事前に決定されたトラブルシューティング トレース設定には、SDI および Log4j トレースの設定があります。 トラブルシューティング トレース設定が適用される前に、元のトレース設定がバックアップされます。 トラブルシューティング トレース設定をリセットすると、元のトレース設定が復元されます。

トラブルシューティング トレース設定をサービスに適用した後で [トラブルシューティング トレース設定（Troubleshooting Trace Settings）]ウィンドウを開くと、トラブルシューティング用に設定したサービスがチェック付きで表示されます。 [トラブルシューティング トレース設定（Troubleshooting Trace Settings）]ウィンドウでは、トレース設定を元の設定にリセットできます。

トラブルシューティング トレース設定をサービスに適用すると、トラブルシューティング トレースがそのサービスに設定されたことを示すメッセージが [トレース設定（Trace Configuration）]ウィンドウに表示されます。 サービスの設定をリセットする場合は、[関連リンク（Related Links）] リスト ボックスから、[トラブルシューティング トレース設定（Troubleshooting Trace Settings）] オプションを選択できます。 指定したサービスの [トレース設定（Trace Configuration）]ウィンドウでは、すべての設定が読み取り専用として表示されます。ただし、最大ファイル数など、トレース出力設定の一部のパラメータを除きます。

トラブルシューティング トレース設定

始める前に

トレース設定の設定タスクとトレース パラメータの設定タスクを確認します。

手順

ステップ 1 **[トレース（Trace）]**>**[トラブルシューティング トレース設定（Troubleshooting Trace Settings）]** を選択します。

ステップ 2 **[サーバー（Server）]** リストボックスから、トレース設定をトラブルシューティングするサーバーを選択します。

ステップ 3 [移動（Go）]を選択します。

サービスの一覧が表示されます。 アクティブ化されていないサービスは、[該当なし（N/A）] と表示されます。

ステップ 4 次のいずれかの操作を実行します。

a) [サーバ（Server）]リストボックスで選択したノードの特定のサービスをモニタするには、[サービス（Services）]ペインでそのサービスをオンにします。

たとえば、[データベースおよび管理サービス（Database and Admin Services）]、[パフォーマンスおよびモニタリング サービス（Performance and Monitoring Services）]、[バックアップおよび復元サービス（Backup and Restore Services）] ペインなどがあります。

この作業は、[サーバ（Server）]リスト ボックスで選択したノードのみに影響します。

b) [サーバ（Server）] リスト ボックスで選択したノードのすべてのサービスをモニタするには、[すべてのサービスをチェック（Check All Services）]をオンにします。

c) Cisco Unified Communications Manager および IM and Presence クラスタのみ：クラスタ内のすべてのノードで特定のサービスをモニタするには、[すべてのノードで選択されたサービスをチェック（Check Selected Services on All Nodes）]をチェックします。

この設定は、クラスタ内のサービスがアクティブなすべてのノードに適用されます。

d) Unified Communications Manager and IM and Presence クラスタのみ：クラスタのすべてのサービスをモニタするには、**すべてのノードのすべてのサービスをチェックする**をオンにします。

ステップ 5 **保存**を選択します。

ステップ 6 元のトレース設定に戻すには、次のいずれかのボタンをクリックします。

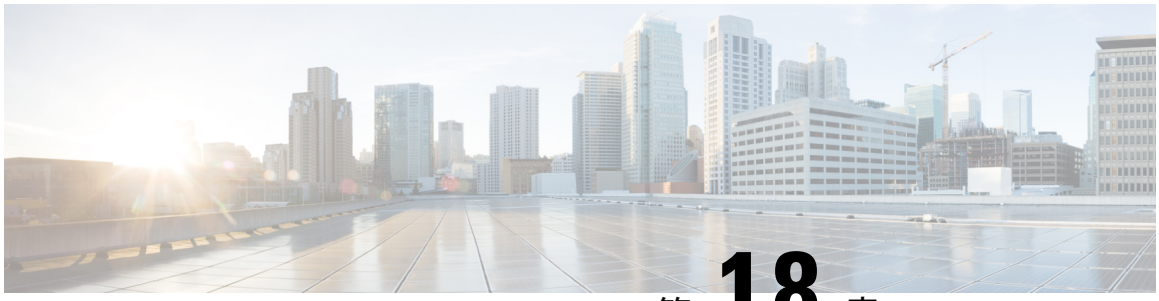
a) [トラブルシューティングトレースをリセット（Reset Troubleshooting Traces）] : [サーバ（Server）]リストボックスで選択したノードで元のトレース設定を復元します。また、選択可能なアイコンも表示されます。

b) Cisco Unified Communications Manager および IM and Presence クラスタのみ：[すべてのノードでトラブルシューティングトレースをリセット（Reset Troubleshooting Traces On All Nodes）] : クラスタ内のすべてのノードでサービスの元のトレース設定を復元します。

[トラブルシューティングトレースをリセット（Reset Troubleshooting Traces）] ボタンは、1 つ以上のサービスのトラブルシューティング トレースを設定してある場合にのみ表示されます。

（注） トラブルシューティング トレースを長時間イネーブルのままにすると、トレース ファイルのサイズが大きくなり、サービスのパフォーマンスに影響が生じるおそれがあります。

[リセット（Reset）]ボタンをクリックすると、ウィンドウが更新され、サービスのチェックボックスがオフになります。



第 18 章

使用状況レコードの表示

使用状況レコードの概要

Cisco Unified Communications Manager が提供するレコードを使用して、設定済みの項目がシステム内でどのように使用されているのかを確認することができます。 設定済みの項目には、デバイスだけでなく、デバイス プール、日時グループ、ルート プランなどのシステム レベルの設定も含まれます。

依存関係レコード

依存関係レコードは、次の目的で使用します。

- システム レベルの設定（サーバ、デバイス プール、日時グループなど）に関する情報を調べる。
- 他のレコードを使用しているデータベース内のレコードを確認する。 たとえば、特定のコーリング サーチ スペースを使用しているデバイス（CTI ルート ポイントや電話機など）を確認できます。
- レコードを削除する前に、レコード間の依存関係を明らかにする。 たとえば、パーティションを削除する前に、依存関係レコードを使用して、そのパーティションにどのコーリング サーチ スペース（CSS）とデバイスが関連付けられているかを確認します。 こうすることで、その依存関係を削除するように設定を再構成できます。

ルート プラン レポート

ルート プラン レポートでは、システム内で設定されている番号、ルート、パターンの一部またはすべてを確認できます。 レポートを生成する際は、レポートの [パターン/電話番号（Pattern/Directory Number）] 列、[パーティション（Partition）] 列、または [ルート詳細（Route

Detail）]列のエントリをクリックすることで、該当する項目の設定ウィンドウにアクセスできます。

さらに、ルート プラン レポートを使用してレポート データを .CSV ファイルに保存し、そのファイルを他のアプリケーションにインポートすることもできます。 保存される .CSV ファイルには、ウェブ ページより詳細な情報（電話機の電話番号、ルート パターン、パターン使用法、デバイス名、デバイスの説明など）が含まれます。

Cisco Unified Communications Manager は、ルート プランを使用して、内部コールと外部公衆電話交換網（PSTN）コールの両方をルート指定します。 ネットワークには複数のレコードが存在する可能性があるため、Cisco Unified Communications Manager Administration では、特定の基準に基づいて特定のルート プラン レコードを見つけることができます。

使用状況レポートのタスク

手順

	コマンドまたはアクション	目的
ステップ 1	ルート プラン レコードを表示し、これらのレコードを使用して未割り当ての電話番号を管理するには、次の手順を参照してください。 • ルート プラン レコードの表示（305 ページ） • ルート プラン レコードの保存（306 ページ） • 未定義の電話番号の削除（306 ページ） • 未割り当ての電話番号の更新（307 ページ）	特定のルート プラン レコードを検索し、レコードを CSV ファイルに保存し、未割り当ての電話番号を管理するには、これらの手順を使用してください。
ステップ 2	依存関係レコードを使用するには、次の手順を参照してください。 • 依存関係レコードの表示（309 ページ）	システムレベルの設定に関する情報を見つけ、データベース内のレコード間の依存関係を表示するには、これらの手順を使用してください。

ルート プラン レポートのタスク フロー

手順

	コマンドまたはアクション	目的
ステップ 1	ルート プラン レコードの表示（305 ページ）.	ルート プラン レコードを表示し、カスタマイズされたルート プラン レポートを生成します。
ステップ 2	ルート プラン レコードの保存（306 ページ）.	.csv ファイル形式でルート プラン レポートを表示します。
ステップ 3	未定義の電話番号の削除（306 ページ）.	ルート プラン レポートから未割り当ての電話番号を削除します。
ステップ 4	未割り当ての電話番号の更新（307 ページ）.	ルート プラン レポートから未割り当ての電話番号の設定を更新します。

ルート プラン レコードの表示

ここでは、ルート プラン レコードを表示する方法について説明します。 ネットワークには複数のレコードが存在する可能性があるため、Cisco Unified Communications Manager Administration では、特定の基準に基づいて特定のルート プラン レコードを見つけることができます。 カスタマイズされたルート プラン レポートを生成するには、次の手順を実行します。

手順

ステップ 1 **[コール ルーティング（Call Routing）]** > **[ルート プラン レポート（Route Plan Report）]** の順に選択します。

ステップ 2 データベースのすべてのレコードを検索するには、ダイアログボックスが空であることを確認して、ステップ 3 に進みます。

レコードをフィルタまたは検索する手順は、次のとおりです。

a) 最初のドロップダウン リスト ボックスで、検索パラメータを選択します。
b) 2 番目のドロップダウン リスト ボックスで、検索パターンを選択します。
c) 必要に応じて、適切な検索テキストを指定します。

ステップ 3 **[検索(Find)]** をクリックします。

すべてのレコードまたは一致するレコードが表示されます。 [ページあたりの行数(Rows per Page)] ドロップダウン リスト ボックスで別の値を選択すると、各ページに表示される項目数を変更できます。

ステップ 4 表示されたレコード リストから、目的のレコードのリンクをクリックします。

選択した項目がウィンドウに表示されます。

ルート プラン レコードの保存

このセクションでは、.csv ファイルでルート プラン レポートを表示する方法について説明します。

手順

ステップ 1 **[コール ルーティング（Call Routing）]** > **[ルート プラン レポート（Route Plan Report）]** の順に選択します。

ステップ 2 [ルート プラン レポート（Route Plan Report）]ウィンドウの [関連リンク（Related Links）] ドロップダウンリストから [ファイルで表示（View In File）]を選択し、[移動（Go）]をクリックします。

表示されたダイアログボックスで、ファイルを保存するか、別のアプリケーションにファイルをインポートすることができます。

ステップ 3 **[保存]** をクリックします。

別のウィンドウが表示され、任意の場所にこのファイルを保存できます。

（注） 別のファイル名での保存も可能ですが、ファイル名には .CSV 拡張子を含める必要があります。

ステップ 4 ファイルを保存する場所を選択し、[保存（Save）]をクリックします。 この操作により、指定した場所にファイルが保存されます。

ステップ 5 保存した .CSV ファイルを探し、アイコンをダブルクリックして表示します。

未定義の電話番号の削除

このセクションでは、ルート プラン レポートから未割り当ての電話番号を削除する方法について説明します。 電話番号は、Cisco Unified Communications Manager Administration の [電話番号の設定（Directory Number Configuration）] ウィンドウで設定または削除します。 電話番号がデバイスから削除されたり、電話機が削除されたりしても、電話番号はそのまま Cisco Unified Communications Manager データベース内に残ります。 データベースから電話番号を削除するには、[ルート プラン レポート（Route Plan Report）] ウィンドウを使用します。

手順

ステップ 1 **[コール ルーティング（Call Routing）]** > **[ルート プラン レポート（Route Plan Report）]** を選択します。

ステップ 2 [ルート プラン レポート（Route Plan Report）] ウィンドウで、3 つのドロップダウン リストを使用して、すべての未割り当て DN を列挙するルート プラン レポートを指定します。

ステップ 3 電話番号を削除する 3 つの方法があります。

a) 削除する電話番号をクリックします。 [電話番号の設定（Directory Number Configuration）] ウィンドウが表示されたら、[削除（Delete）] をクリックします。

b) 削除する電話番号の横にあるチェック ボックスをオンにします。 [選択項目の削除（Delete Selected）] をクリックします。

c) 見つかった未割り当ての電話番号をすべて削除するには、[見つかった項目をすべて削除（Delete All Found Items）] をクリックします。

電話番号を削除するかどうかを確認する警告メッセージが表示されます。

ステップ 4 電話番号を削除する場合は、[OK] をクリックします。 削除要求をキャンセルする場合は、[キャンセル（Cancel）] をクリックします。

未割り当ての電話番号の更新

この項では、ルート プラン レポートから未割り当ての電話番号の設定を更新する方法について説明します。 電話番号は、Cisco Unified Communications Manager Administration の [電話番号の設定（Directory Number Configuration）] ウィンドウで設定または削除します。 デバイスから電話番号が削除されても、電話番号は Cisco Unified Communications Manager データベースに残っています。 電話番号の設定を更新するには、[ルート プラン レポート（Route Plan Report）] ウィンドウを使用します。

手順

ステップ 1 **[コール ルーティング（Call Routing）]** > **[ルート プラン レポート（Route Plan Report）]** の順に選択します。

ステップ 2 **[ルート プラン レポート（Route Plan Report）]** ウィンドウで、3 つのドロップダウン リストを使用して、すべての未割り当て DN を列挙するルート プラン レポートを指定します。

ステップ 3 更新する電話番号をクリックします。

（注） 電話番号およびパーティションを除く、電話番号のすべての設定を更新できます。

ステップ 4 コーリング サーチ スペースや転送オプションなどの必要な更新を行います。

ステップ 5 **[保存]** をクリックします。

[電話番号の設定（Directory Number Configuration）] ウィンドウが再度表示され、電話番号フィールドが空になります。

依存関係レコード タスク フロー

手順

	コマンドまたはアクション	目的
ステップ 1	依存関係レコードの設定 （308 ページ）.	この手順を使用して、依存関係レコードを有効または無効にします。 この手順は、通常よりも低い優先順位で実行され、ダイヤル プランの規模と複雑さ、CPU 速度、およびその他のアプリケーションの CPU 要件によっては完了までに時間がかかることがあります。
ステップ 2	依存関係レコードの表示 （309 ページ）.	依存関係レコードを有効にすると、インターフェイスの設定ウィンドウからそれらにアクセスできます。

依存関係レコードの設定

依存レコードを使用して、Cisco Unified Communications Manager データベース内のレコード間の関係を表示します。 たとえば、パーティションを削除する前に、依存関係レコードを使用して、そのパーティションにどのコーリング サーチ スペース（CSS）とデバイスが関連付けられているかを確認します。

⚠

注意 依存関係レコードを使用すると、CPU 使用率が高くなります。 この手順は、通常よりも低い優先順位で実行され、ダイヤルプランの規模と複雑さ、CPU速度、およびその他のアプリケーションの CPU 要件によっては完了までに時間がかかることがあります。

依存関係レコードを有効にしたために、システムでCPU使用率の問題が発生している場合は、依存関係レコードを無効にすることができます。

手順

ステップ 1 Cisco Unified CM Administrationから、**[システム（System）]** > **[エンタープライズ パラメータ（Enterprise Parameters）]** を選択します。

ステップ 2 [CCMAdmin パラメータ（CCMAdmin Parameters）]セクションにスクロールし、[依存関係レコードの有効化（Enable Dependency Records）]ドロップダウン リストで、次のオプションのいずれかを選択します。

- [True]：依存関係レコードを有効にします。
- [False]：依存関係レコードを無効にします。

選択したオプションに基づいて、依存関係レコードを有効または無効にした結果に関するメッセージを含むダイアログボックスが表示されます。 このダイアログボックスで、[OK]をクリックする前に、メッセージをお読みください。

ステップ 3 **OK**をクリックします。

ステップ 4 **[保存]** をクリックします。
変更を確認する「更新に成功しました（Update Successful）」メッセージが表示されます。

依存関係レコードの表示

依存関係レコードを有効にすると、インターフェイスの設定ウィンドウからそれらにアクセスできます。

始める前に

依存関係レコードの設定 （308 ページ）

手順

ステップ 1 Cisco Unified CM の管理から、表示するレコードの設定ウィンドウに移動します。

例：

デバイス プールの依存関係レコードを表示するには、**[システム（System）]** > **[デバイス プール（Device Pool）]** を選択します。

（注） [デバイスのデフォルト（Device Defaults）]ウィンドウと [エンタープライズ パラメータ設定（Enterprise Parameters Configuration）]ウィンドウで依存関係レコードを表示することはできません。

ステップ 2 **[検索(Find)]** をクリックします。

ステップ 3 レコードのいずれかをクリックします。
設定ウィンドウが表示されます。

ステップ 4 [関連リンク（Related Links）] リスト ボックスで、[依存関係レコード（Dependency Records）] を選択し、[移動（Go）] をクリックします。

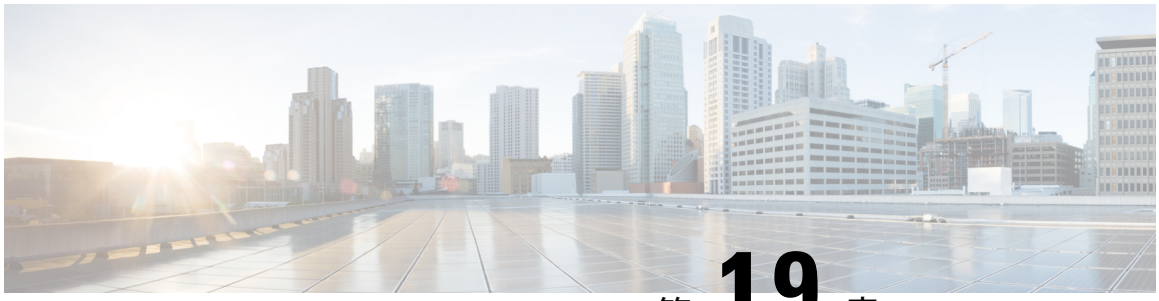
（注） 依存関係レコードを有効にしていない場合は、[依存関係レコード要約（Dependency Records Summary）]ウィンドウに、レコードに関する情報ではなくメッセージが表示されます。

[依存関係レコード要約（Dependency Records Summary）]ウィンドウには、データベース内の他のレコードによって使用されるレコードが表示されます。

ステップ 5 このウィンドウで、次の依存関係レコード ボタンのいずれかを選択します。

- [更新（Refresh）]：最新の情報でウィンドウを更新します。

- [閉じる（Close）]：[依存関係レコード（Dependency Records）] リンクをクリックした設定ウィンドウに戻らずにウィンドウを閉じます。
- [閉じて戻る（Close and Go Back）]：ウィンドウを閉じて、[依存関係レコード（Dependency Records）] リンクをクリックした設定ウィンドウに戻ります。



第 19 章

エンタープライズ パラメータの管理

エンタープライズ パラメータの概要

エンタープライズパラメータは、クラスタ全体ですべてのデバイスやサービスに適用されるデフォルト設定を提供します。 たとえば、システムではエンタープライズ パラメータを使用してデバイスのデフォルトの初期値を設定します。

ユーザはエンタープライズパラメータを追加または削除できませんが、既存のエンタープライズ パラメータを更新することはできます。 エンタープライズ パラメータの設定ウィンドウには、カテゴリ（CCMAdmin パラメータ、CCMUser パラメータ、CDR パラメータなど）ごとにエンタープライズ パラメータが一覧表示されます。

エンタープライズ パラメータの詳細な説明は、[エンタープライズパラメータ設定（Enterprise Parameters Configuration）] ウィンドウで確認できます。

注意 エンタープライズ パラメータの多くは、変更する必要がありません。 変更しようとしている機能を完全に理解している場合、または Cisco Technical Assistance Center（TAC）から変更を指示された場合を除き、エンタープライズ パラメータを変更しないでください。

エンタープライズ パラメータ情報の表示

[エンタープライズパラメータ設定（Enterprise Parameter Configuration）]ウィンドウで、埋め込まれたコンテンツを通してエンタープライズ パラメータに関する情報にアクセスします。

手順

ステップ 1 Cisco Unified CM Administrationから、**[システム]** > **[企業パラメータ]** を選択します。

ステップ 2 次のいずれかの作業を実行します。

- 特定のエンタープライズパラメータの説明を表示するには、そのパラメータ名をクリックします。
- エンタープライズ パラメータの説明をすべて表示するには、[?]をクリックします。

エンタープライズ パラメータの更新

次の手順を使用して、[エンタープライズパラメータ設定（Enterprise Parameter Configuration）] ウィンドウを開き、システム レベル設定を構成します。

注意 エンタープライズ パラメータの多くは、変更する必要がありません。 変更しようとしている機能を完全に理解している場合、またはCisco Technical Assistance Center（TAC）から変更を指示された場合を除き、エンタープライズ パラメータを変更しないでください。

手順

ステップ 1 Cisco Unified CM Administrationから、**[システム]** > **[企業パラメータ]** を選択します。
ステップ 2 変更するエンタープライズ パラメータに必要な値を選択します。
ステップ 3 **[保存（Save）]** をクリックします。

次のタスク

デバイスへの設定の適用 （312 ページ）

デバイスへの設定の適用

次の手順を使用して、構成した設定でクラスタ内のすべての影響を受けるデバイスを更新します。

始める前に

エンタープライズ パラメータの更新 （312 ページ）

手順

ステップ 1 Cisco Unified CM Administrationから、**[システム]** > **[企業パラメータ]** を選択します。
ステップ 2 変更を確認してから、[保存（Save）]をクリックします。
ステップ 3 次のいずれかのオプションを選択します。

- システムでリブートするデバイスを判断するには、[設定の適用（Apply Config）]をクリックします。 リブートする必要がないデバイスもあります。 進行中のコールはドロップされる可能性がありますが、接続されたコールは、デバイス プールにSIP トランクが含まれていない限り、保持されます。
- クラスタ内のすべてのデバイスをリブートするには、[リセット（Reset）]をクリックします。 この手順はオフピーク時間帯に実行することをお勧めします。

ステップ 4 確認ダイアログを読んでから、[OK]をクリックします。

デフォルト エンタープライズ パラメータの復元

エンタープライズ パラメータをデフォルト設定にリセットする場合は、次の手順を使用します。 一部のエンタープライズ パラメータには、設定ウィンドウの列に示すように、推奨値が含まれています、この手順では、これらの値をデフォルト設定として使用します。

手順

ステップ 1 Cisco Unified CM Administrationから、**[システム]** > **[企業パラメータ]** を選択します。
ステップ 2 [デフォルトに設定（Set to Default）]をクリックします。
ステップ 3 確認プロンプトを読み、[OK]をクリックします。

第 20 章

サーバの管理

サーバの管理の概要

この章では、Cisco Unified Communications Manager ノードのプロパティを管理する方法、プレゼンス サーバのステータスを表示する方法、および Unified Communications Manager サーバのホスト名を設定する方法を説明します。

サーバの削除

この項では、Cisco Unified Communications Manager データベースからサーバを削除する方法、および削除したサーバを再び Cisco Unified Communications Manager クラスタに追加する方法について説明します。

Cisco Unified Communications Manager の管理ページでは、クラスタの最初のノードは削除できませんが、2 番目以降のノードは削除できます。 [サーバの検索/一覧表示 (Find and List Servers)] ウィンドウで後続のノードを削除する前に、Cisco ユニファイド CM Administration に次のメッセージが表示されます。「1つ以上のサーバを完全に削除しようとしています。 この操作を取り消すことはできません。 続行しますか？」」というメッセージが表示されます。 [OK] をクリックすると、サーバは Cisco UnifiedCM データベースから削除され、使用できなくなります。

ヒント [サーバの設定 (Server Configuration)] ウィンドウからサーバを削除しようとすると、前のパラグラフのメッセージが表示されます。[OK] をクリックすると、サーバは Cisco UnifiedCM データベースから削除され、使用できなくなります。

サーバを削除する前に、次の点を考慮してください。

- Cisco Unified Communications Manager の管理ページでは、クラスタ内の最初のノードを削除できませんが、2 番目以降のノードは削除できます。
- Cisco Unified Communications Manager が動作しているノード、特に、電話機などのデバイスが登録されているノードは削除しないことをお勧めします。
- 2 番目以降のノードに関する依存関係レコードが存在する場合でも、そのレコードが原因でノードが削除できなくなることはありません。
- 削除するノードの Cisco Unified Communications Manager にコール パーク番号が設定されている場合は、削除できません。 ノードを削除するには、Cisco Unified Communications Manager Administrationでコール パーク番号を削除する必要があります。
- Cisco Unified Communications Manager の管理ページの設定フィールドに削除するサーバの IP アドレスまたはホスト名が含まれている場合は、サーバを削除する前に設定を更新してください。 この作業を行わないと、サーバの削除後、その設定に依存する機能が動作しなくなる場合があります。たとえば、サービスパラメータ、エンタープライズパラメータ、サービス URL、ディレクトリ URL、IP Phone サービスなどに IP アドレスまたはホスト名を入力した場合は、サーバを削除する前に、この設定を更新してください。
- たとえば Cisco Unity、Cisco Unity Connection などのアプリケーションの GUI に削除するサーバの IP アドレスまたはホスト名が含まれている場合は、サーバを削除する前に、対応する GUI の設定を更新してください。 この作業を行わないと、サーバの削除後、その設定に依存する機能が動作しなくなる場合があります。
- サーバを削除すると、MOH サーバなどのデバイスも自動的に削除される場合があります。
- ノードを削除する前に、2 番目以降のノードでアクティブになっているサービスを非アクティブにしておくことをお勧めします。 この作業を実行しておくと、ノードの削除後にサービスが動作することが保証されます。
- サーバ設定の変更を有効にするには、Cisco Unified Communications Manager を再起動します。 Cisco CallManager 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。
- データベース ファイルが正しく更新されるようにするには、サーバ、プレゼンス、またはアプリケーション サーバの削除後にクラスタをリブートする必要があります。
- ノードの削除後、Cisco Unified Reporting にアクセスして、Cisco Unified Communications Manager でクラスタからノードが削除されたことを確認してください。 さらに、Cisco Unified Reporting、RTMT、または CLI にアクセスして既存のノード間でデータベース レ

プリケーションが行われていることを確認し、必要であれば、CLI を使用してノード間のデータベース レプリケーションを修復してください。

（注） サブスクライバ ノードをクラスタから削除すると、その証明書は引き続き発行元とその他のノードに存在します。 管理者は以下を手動で削除する必要があります。

- 個々のクラスタ メンバーの信頼ストアから削除されたサブスクライバ ノードの証明書。
- 削除されたサブスクライバ ノードの信頼ストアからの他の各クラスタ メンバーの証明書。

クラスタからの Unified Communications Manager ノードの削除

次の手順に従って、クラスタから Cisco Unified Communications Manager ノードを削除します。

手順

ステップ 1 Cisco Unified CM Administration から、**[システム（System）] > [サーバ（Server）]** を選択します。

ステップ 2 **[検索（Find）]** をクリックして、削除するノードを選択します。

ステップ 3 [削除（Delete）]をクリックします。

ステップ 4 この操作は取り消せないことを示す警告ダイアログ ボックスが表示されたら、[OK] をクリックします。

ステップ 5 割り当てを解除したノードのホスト VM をシャットダウンします。

クラスタからの IM and Presence ノードの削除

プレゼンス冗長グループおよびクラスタから IM and Presence Service ノードを安全に削除する必要がある場合は、この手順に従います。

注意 ノードを削除すると、そのプレゼンス冗長グループの残りのノードで、ユーザに対するサービスが中断されます。 この手順は、メンテナンス時間中にのみ実行してください。

手順

ステップ 1 **[Cisco Unified CM の管理（Cisco Unified CM Administration）] > [システム（System）] > [プレゼンス冗長グループ（Presence Redundancy Groups）]**ページで、高可用性が有効な場合は無効にします。

ステップ 2 **[Cisco Unified CM の管理（Cisco Unified CM Administration）] > [ユーザ管理（User Management）] > [プレゼンスユーザの割り当て（Assign Presence Users）]**ページで、削除するノードからすべてのユーザの割り当てを解除するか、移動します。

ステップ 3 プレゼンス冗長グループからノードを削除するには、プレゼンス冗長グループの **[プレゼンス冗長グループの設定（Presence Redundancy Group Configuration）]** ページの [プレゼンスサーバ（Presence Server）] ドロップダウンリストから、**[未選択（Not-Selected）]** を選択します。ノードの割り当て解除の結果として、プレゼンス冗長グループ内のサービスが再起動されることを示す警告ダイアログボックスが表示されたら、**[OK]** を選択します。

（注） プレゼンス冗長グループからパブリッシャ ノードを直接削除することはできません。パブリッシャ ノードを削除するには、まずパブリッシャ ノードからユーザの割り当てを解除し、プレゼンス冗長グループを完全に削除します。

ただし、削除した IM and Presence ノードをクラスタに再び追加することもできます。削除されたノードを追加する方法の詳細については、「削除したサーバをクラスタに戻す（318 ページ）」を参照してください。 この場合、削除されたパブリッシャノードが Cisco Unified CM 管理コンソールの **[システム（System）] > [サーバ（Server）]** 画面でサーバーに再び追加されると、**DefaultCUPSubcluster** が自動的に作成されます。

ステップ 4 Cisco Unified CM Administration で、**[システム（System）] > [サーバ（Server）]** から未割り当てのノードを削除します。 この操作は取り消せないことを示す警告ダイアログ ボックスが表示されたら、[OK] をクリックします。

ステップ 5 割り当てを解除したノードのホスト VM またはサーバをシャットダウンします。

ステップ 6 すべてのノードの **Cisco XCP Router** を再起動します。

削除したサーバをクラスタに戻す

Cisco Unified Communications Manager Administration から後続のノード（サブスクライバ）を削除してそれをクラスタに戻す場合に、次の手順を実行します。

手順

ステップ 1 Cisco Unified Communications Manager Administration で、**[システム（System）] > [サーバ（Server）]** を選択してサーバを追加します。

ステップ 2 後続のノードを Cisco Unified Communications Manager Administration に追加したら、シスコが提供しているお使いのバージョンのソフトウェア キットに付属しているディスクを使用して、サーバ上でインストールを実行します。

ヒント インストールするバージョンが、パブリッシャノードで動作しているバージョンと一致することを確認します。パブリッシャで実行されているバージョンがインストールファイルと一致しない場合は、インストールプロセス中に [Upgrade While Install] オプションを選択します。 詳細は、*Cisco Unified Communications Manager* および *IM and Presence Service* リリース *11.5(1)* インストール ガイドを参照してください。

ステップ 3 Cisco UnifiedCM をインストールしたら、その Cisco UnifiedCM のバージョンをサポートしているインストール マニュアルの説明に従って、後続のノードを設定します。

ステップ 4 Cisco Unified Reporting、RTMT、または CLI にアクセスして、データベース レプリケーションが既存のノード間で発生していることを確認します。必要に応じて、ノード間のデータベース レプリケーションを修復します。

インストール前のクラスタへのノードの追加

ノードをインストールする前に、Cisco Unified Communications Manager Administration を使用して、新しいノードをクラスタに追加します。 ノードの追加時に選択するサーバ タイプは、インストールしたサーバ タイプと一致する必要があります。

新しいノードをインストールする前に、Cisco Unified Communications Manager Administration を使用して、最初のノードで新しいノードを設定する必要があります。クラスタにノードをインストールする方法については、『*Cisco Unified Communications Manager Installation Guide*』を参照してください。

Cisco Unified Communications Manager のビデオ/音声サーバでは、Cisco Unified Communications Manager ソフトウェアの初期インストール中に追加した最初のサーバがパブリッシャ ノードに指定されます。 後続のすべてのサーバ インストールまたは追加は、サブスクライバ ノードに指定されます。 クラスタに追加した最初の Cisco Unified Communications Manager IM and Presence ノードが、IM and Presence Service データベース パブリッシャ ノードに指定されます。

（注） サーバの追加後は、Cisco Unified Communications Manager Administration を使用して、サーバ タイプを変更できなくなります。既存のサーバインスタンスを削除してから、再度、新しいサーバを追加して、正しいサーバ タイプ設定を選択する必要があります。

手順

ステップ 1 **[システム（System）]** > **[サーバ（Server）]** を選択します。

[サーバの検索/一覧表示（Find and List Servers）]ウィンドウが表示されます。

ステップ 2 [新規追加] をクリックします。

[サーバの設定 - サーバを追加（Server Configuration - Add a Server）]ウィンドウが表示されます。

ステップ 3 [サーバ タイプ（Server Type）]ドロップダウン リスト ボックスで、追加するサーバ タイプを選択してから、[次へ（Next）]をクリックします。

- CUCM ビデオ/音声
- CUCM IM and Presence

ステップ 4 [サーバの設定（Server Configuration）]ウィンドウで、適切なサーバ設定を入力します。

サーバ設定フィールドの説明については、「Server Settings」を参照してください。

ステップ 5 **[保存（Save）]** をクリックします。

プレゼンス サーバのステータスの表示

IM and Presence サービスノードの重要なサービスのステータスと自己診断テスト結果を確認するには、Cisco Unified Communications Manager の管理を使用します。

手順

ステップ 1 **[システム（System）]** > **[サーバ（Server）]** を選択します。

[サーバの検索/一覧表示（Find and List Servers）]ウィンドウが表示されます。

ステップ 2 サーバの検索パラメータを選択し、[検索（Find）]をクリックします。

一致するレコードが表示されます。

ステップ 3 [サーバの検索/一覧表示（Find and List Servers）]ウィンドウに表示される IM and Presence サーバを選択します。

[サーバの設定（Server Configuration）]ウィンドウが表示されます。

ステップ 4 [サーバの設定（Server Configuration）]ウィンドウの IM and Presence サーバ情報のセクションで、プレゼンス サーバ ステータスのリンクをクリックします。

サーバの [ノードの詳細（Node Details）]ウィンドウが表示されます。

ポートの設定

SCCPデバイス登録、SIPデバイス登録、MGCPゲートウェイ接続などの接続に使用されるポートの設定を変更するには、この手順を使用します。

（注） 通常、デフォルトのポート設定を変更する必要はありません。この手順は、デフォルトを変更する場合にのみ使用します。

手順

ステップ 1 Cisco Unified Communications Manager Administration で、**[システム（System）]** > **[Cisco Unified CM]** を選択します。
[Cisco Unified CM の検索と一覧表示（Find and List Cisco Unified CMs）]ウィンドウが表示されます。

ステップ 2 適切な検索条件を入力し、[検索（Find）]をクリックします。
一致するすべての Cisco Unified Communications Manager が表示されます。

ステップ 3 表示する Cisco Unified CMを選択します。
[Cisco Unified CM の設定（Cisco Unified CM Configuration）]ウィンドウが表示されます。

ステップ 4 [このサーバの Cisco Unified Communications Manager TCP ポートの設定（Cisco Unified Communications Manager TCP Port Settings for this Server）]セクションに移動します。

ステップ 5 Cisco Unified Communications Manager のポートを設定します。

フィールドとその設定オプションの詳細については、「ポート設定（322ページ）」を参照してください。

ステップ 6 **[保存（Save）]** をクリックします。

ステップ 7 **[設定の適用（Apply Config）]** をクリックします。

ステップ 8 **OK**をクリックします。

ポート設定

フィールド	説明
[イーサネット電話ポート（Ethernet Phone Port）]	システムは、このTCPポートを使用してネットワークのCisco Unified IP Phone（SCCP専用）と通信します。 • デフォルトのポート値2000がシステム上ですでに使用中の場合以外は、このデフォルト ポートを受け入れてください。 2000を選択すると、このポートは非セキュアとして識別されます。 • すべてのポート入力値は固有のものでなければなりません。 • 有効なポート番号の範囲は、1024 ～ 49151です。
[MGCPリッスンポート（MGCP Listen Port）]	システムは、TCPポートを使用して、その関連するMGCPゲートウェイからのメッセージを検出する。 • デフォルトのポート番号2427がシステム上ですでに使用中の場合以外は、このデフォルト ポートを受け入れてください。 • すべてのポート入力値は固有のものでなければなりません。 • 有効なポート番号の範囲は、1024 ～ 49151です。
[MGCPキープアライブポート(MGCP Keep-alive Port)]	システムは、このTCPポートを使用して、その関連するMGCPゲートウェイとアクティブメッセージを交換する。 • デフォルトのポート番号2428がシステム上ですでに使用中の場合以外は、このデフォルト ポートを受け入れてください。 • すべてのポート入力値は固有のものでなければなりません。 • 有効なポート番号の範囲は、1024 ～ 49151です。
[SIP電話ポート(SIP Phone Port)]	このフィールドでは、Unified Communications ManagerがTCPとUDPを介してSIP回線登録をリッスンするのに使用するポート番号を指定します。
[SIP電話セキュアポート（SIP Phone Secure Port）]	このフィールドでは、システムがTLSを介してSIP回線登録をリッスンするのに使用するポート番号を指定します。
SIP電話OAuthポート（SIP Phone OAuth Port）	このフィールドは、Cisco Unified Communications ManagerがTLS（Transport Layer Security）を介して、オンプレミスのJabberデバイスによるSIP回線への登録をリッスンするために使用するポート番号を指定します。 デフォルト値は5090です。範囲は1024 ～ 49151です。

フィールド	説明
[SIPモバイルおよびリモートアクセスOAuthポート（SIP Mobile and Remote Access OAuth Port）]	このフィールドは、Cisco Unified Communications ManagerがMTLS（Mutual Transport Layer Security）を介してExpressway上のJabberからのSIP回線登録を受信するために使用するポート番号を指定します。デフォルト値は 5091 です。範囲は 1024 ～ 49151 です。

ホスト名の設定

次の表に、Unified Communications Manager サーバーのホスト名を設定できる場所、ホスト名に使用できる文字数、ホスト名に推奨される最初と最後の文字を示します。ホスト名を正しく設定しないと、Unified Communications Manager の一部のコンポーネント（オペレーティングシステム、データベース、インストールなど）が期待通りに動作しない可能性があります。

表 *74 : Cisco Unified Communications Manager* におけるホスト名の設定

ホスト名の場所	可能な設定	指定できる文字数	推奨されるホスト名の先頭文字	推奨されるホスト名の最終文字
[ホスト名/IPアドレス（Host Name/IP Address）] フィールド Cisco Unified Communications Manager Administration の **[システム（System）]** > **[サーバ（Server）]**	クラスタ内のサーバのホスト名を追加または変更できます。	2-63	英字	英数字
[ホスト名（Hostname）] フィールド Cisco Unified Communications Manager インストール ウィザード	クラスタ内のサーバのホスト名を追加できます。	1-63	英字	英数字
[ホスト名（Hostname）] フィールド Cisco Unified Communications オペレーティング システムの **[設定（Settings）]** > **[IP]** > **[イーサネット（Ethernet）]**	クラスタ内のサーバのホスト名を変更できますが、追加はできません。	1-63	英字	英数字
set network hostname hostname コマンドライン インターフェイス	クラスタ内のサーバのホスト名を変更できますが、追加はできません。	1-63	英字	英数字

ヒント　このホスト名は、ARPANETホスト名の規則に従う必要があります。 ホスト名の先頭文字と最終文字の間には、英数文字とハイフンを入力できます。

いずれかの場所でホスト名を設定する前に、次の情報を確認してください。

- [サーバの設定（Server Configuration）] ウィンドウの [ホスト名/IP アドレス（Host Name/IP Address）] フィールドは、デバイスとサーバ間、アプリケーションとサーバ間、および異なるサーバ間の通信をサポートします。このフィールドには、ドット区切り形式の IPv4 アドレスまたはホスト名を入力できます。

  Unified Communications Manager パブリッシャ ノードをインストールした後は、パブリッシャのホスト名がこのフィールドに自動的に表示されます。 Unified Communications Manager サブスクライバ ノードをインストールする前に、Unified Communications Manager パブリッシャ ノードでこのフィールドにサブスクライバ ノードの IP アドレスまたはホスト名を入力してください。

  このフィールドにホスト名を設定できるのは、Unified Communications Manager が DNS サーバにアクセスしてホスト名を IP アドレスに解決できる場合のみです。DNS サーバに Cisco Unified Communications Manager の名前とアドレスの情報が設定されていることを確認してください。

ヒント　DNS サーバに Unified Communications Manager の情報を設定するのに加えて、Cisco Unified Communications Manager のインストール時に DNS 情報を入力します。

- Unified Communications Manager パブリッシャ ノードのインストール時に、ネットワーク情報を設定するために（つまり、スタティック ネットワークを使用する場合に）パブリッシャ サーバのホスト名（必須）と IP アドレスを入力します。

  Unified Communications Manager サブスクライバ ノードのインストール時には、Unified Communications Manager パブリッシャ ノードのホスト名と IP アドレスを入力して、Unified Communications Manager がネットワークの接続性およびパブリッシャとサブスクライバ間の検証を確認できるようにしてください。 さらに、サブスクライバ ノードのホスト名と IP アドレスも入力する必要があります。 Unified Communications Manager のインストール時にサブスクライバ サーバのホスト名の入力を求められた場合は、Cisco Unified Communications Manager Administration の（[ホスト名/IP アドレス（Host Name/IP Address）] フィールドでサブスクライバ サーバのホスト名を設定した場合に）[サーバの設定（Server Configuration）] ウィンドウに表示される値を入力します。

Kerneldump ユーティリティ

Kerneldump ユーティリティにより、セカンダリ サーバを要求することなしに、該当するマシンでクラッシュ ダンプ ログをローカルに収集できます。

Unified Communications Managerクラスタでは、Kerneldumpユーティリティがサーバで有効であることを確認するだけで、クラッシュ ダンプ情報を収集できます。

（注） シスコでは、より効果的なトラブルシューティングを実現するため、Unified Communications Managerのインストール後に、Kerneldump ユーティリティが有効であることを確認するよう推奨しています。 Kerneldump ユーティリティの設定をまだ行っていない場合は、Unified Communications Managerをサポート対象のアプライアンス リリースからアップグレードする前に行ってください。

重要 Kerneldumpユーティリティをイネーブル化またはディセーブル化を行うには、ノードのリブートが必要です。 リブートが許容されるウィンドウ以外では、enable コマンドを実行しないでください。

Cisco Unified Communications オペレーティング システムのコマンドライン インターフェイス（*CLI*）を使用すると、Kerneldump ユーティリティのイネーブル化、ディセーブル化、ステータス確認を実行できます。

次の手順を利用して Kerneldump ユーティリティをイネーブル化します。

ユーティリティによって収集されるファイルの処理

Kerneldump ユーティリティから送信されたクラッシュ情報を表示するには、*Cisco Unified Real-Time Monitoring Tool* またはコマンドライン インターフェイス（*CLI*）を使用します。 *Cisco Unified Real-Time Monitoring Tool* を使用して netdump ログを収集するには、[トレースおよびログ セントラル（Trace & Log Central）] の [ファイルの収集（Collect Files）] オプションを選択します。 [システム サービス/アプリケーションの選択（Select System Services/Applications）] タブで、[Kerneldump ログ（Kerneldump logs）] チェックボックスをオンにします。 *Cisco Unified Real-Time Monitoring Tool* を使用したファイルの収集の詳細については、『*Cisco Unified Real-Time Monitoring Tool Administration Guide*』を参照してください。

CLI を使用して kerneldump ログを収集するには、クラッシュ ディレクトリのファイルに対して「「file」」CLI コマンドを使用します。 これらは 「activelog」 のパーティションの下にあります。 ログ ファイル名は、kerneldump クライアントの IP アドレスで始まり、ファイルが作成された日付で終わります。 ファイル コマンドの詳細については、『*Command Line Interface Reference Guide for Cisco Unified Solutions*』を参照してください。

Kerneldump ユーティリティの有効化

次の手順を利用して Kerneldump ユーティリティをイネーブル化します。 カーネル クラッシュが発生した場合、ユーティリティは、クラッシュの収集とダンプのメカニズムを提供します。 ローカル サーバまたは外部サーバにログをダンプするユーティリティを設定できます。

手順

ステップ 1 コマンドライン インターフェイスにログインします。

ステップ 2 次のいずれかを実行します。

- ローカルサーバー上のカーネルクラッシュを破棄するには、`utils os kerneldump enable` CLI コマンドを実行します。
- 外部サーバにカーネルクラッシュをダンプするには、外部サーバの IP アドレスを指定して `utils os kerneldump ssh enable <ip_address>` CLI コマンドを実行します。

ステップ 3 サーバをリブートします。

例

（注） kerneldump ユーティリティを無効にする必要がある場合、`utils os kernelcrash disable` コマンドを実行してローカルサーバのコアダンプを無効にし、`utils os kerneldump ssh disable <ip_address>` CLI コマンドを実行して外部サーバ上のユーティリティを無効にします。

次のタスク

コア ダンプの指示に従ってリアルタイム モニタリング ツールで電子メール アラートを設定します。 詳細は、コア ダンプの電子メール アラートの有効化 （326 ページ）を参照してください。

kerneldump ユーティリティおよびトラブルシューティングについては、『*Troubleshooting Guide for Cisco Unified Communications Manager*』を参照してください。

コア ダンプの電子メール アラートの有効化

コア ダンプが発生するたびに管理者に電子メールを送信するようにリアルタイム モニタリング ツールを設定するには、次の手順を使用します。

手順

ステップ 1 **[システム（System）]**>**[ツール（Tools）]**>**[アラート（Alert）]**>**[アラートセントラル（Alert Central）]**の順に選択します。

ステップ 2 [CoreDumpFileFound]アラートを右クリックし、[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 ウィザードの指示に従って優先条件を設定します。

a) [アラート プロパティ：電子メール通知（Alert Properties: Email Notification）] ポップアップで、[電子メールの有効化（電子メールの有効化(Enable Email)）] がオンになっていることを確認し、[設定（Configure）]をクリックしてデフォルトのアラートアクションを設定します。これにより管理者に電子メールが送信されます。
b) プロンプトに従って、受信者電子メールアドレスを**[追加（Add）]**します。 このアラートがトリガーされると、デフォルトのアクションは、このアドレスへの電子メールの送信になります。
c) **[保存]** をクリックします。

ステップ 4 デフォルトの電子メールサーバーを設定します。

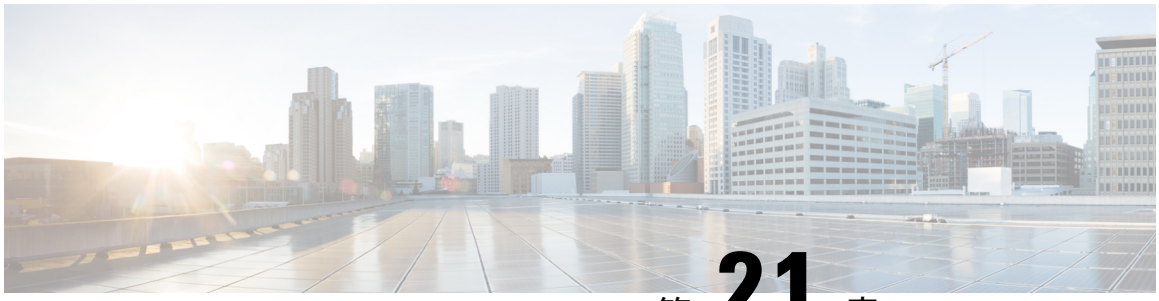
a) **[システム（System）]** > **[ツール（Tools）]** > **[アラート（Alert）]** > **[電子メールサーバーの設定（Config Email Server）]** の順に選択します。
b) 電子メールサーバーとポート情報を入力して、電子メールアラートを送信します。
c) （任意）暗号化された通信チャネルをSMTPサーバーに対して有効にするには、**[TLSモードを有効にする（Enable TLS mode）]** チェックボックスをオンにします。
d) （任意）受信者のメールアドレスを 認証する必要がある場合は、**[認証モードを有効にする（Enable Authentication mode）]** チェックボックスをオンにします。

（注） **[ユーザー名]** と **[パスワード]** のフィールドにアクセスできるのは、**[認証モードを有効にする（Enable Authentication mode）]** チェックボックスが有効になっている場合のみです。

e) **[ユーザー名]** フィールドに、ユーザーの名前を入力します。
f) **[パスワード]** フィールドに、パスワードを入力します。
g) **[送信するユーザー ID（Send User Id）]** を入力します。
h) **OK**をクリックします。

第 V 部

レポートの管理



第 21 章

Cisco Serviceability Reporter

サービスアビリティ レポートのアーカイブ

Cisco Serviceability Reporter サービスは、特定のレポートについて統計情報のサマリーを表示するグラフを含む、日報を生成します。 Reporter は、ログに記録された情報に基づいてレポートを 1 日 1 回生成します。

Serviceability GUI を使用して、**[ツール（Tools）] > [サービスアビリティ レポートのアーカイブ（Serviceability Reports Archive）]** からレポートを表示します。 レポートを表示する前に、Cisco Serviceability Reporter サービスをアクティブ化する必要があります。 サービスをアクティブ化した後、レポートの生成に最大 24 時間かかる場合があります。

レポートには、前日の 24 時間のデータが含まれます。 レポート名に追加されるサフィックスは、Reporter がレポートを生成した日付を表します。たとえば、AlertRep_mm_dd_yyyy.pdf です。 [サービスアビリティ レポートのアーカイブ（Serviceability Reports Archive）] ウィンドウでは、この日付を使用して該当する日付だけのレポートを表示します。 レポートは、前日のタイムスタンプを持つログ ファイルにあるデータから生成されます。 システムは、現在の日付と過去 2 日間のログ ファイルを対象にデータを収集します。

レポートに表示される時刻は、サーバーの 「システム時刻」 が反映されます。

レポートの生成中にサーバからログ ファイルを取得できます。

（注） Cisco Unified Reporting Web アプリケーションは、1 つの出力にデータのスナップショット ビューを提供し、データ チェックを実行します。 また、生成されたレポートをアーカイブすることもできます。 詳細については、『*Cisco Unified Reporting Administration Guide*』を参照してください。

サービスアビリティ レポートのアーカイブのクラスタ構成に関する考慮事項

この項では、Unified Communications Manager および IM and Presence Service のみに適用されます。

- Cisco Serviceability Reporter は最初のサーバーでのみアクティブなため、Reporter は常に、他のサーバーではなく、最初のサーバーでのみレポートを生成します。
- レポートに表示される時刻には、最初のサーバーの 「システム時刻」が反映されます。最初のサーバーとそれに続くサーバーが異なる時間帯に設置されている場合は、最初のサーバーの 「システム時刻」 がレポートに表示されます。
- クラスタ内のサーバ ロケーション間のタイム ゾーンの差は、レポート用にデータが収集されるときに考慮されます。
- レポートの生成時に、個々のサーバまたはクラスタ内のすべてのサーバからログ ファイルを選択できます。
- Cisco Unified Reporting Web アプリケーションの出力やデータ チェックには、アクセス可能なすべてのサーバからのクラスタ データが含まれます。

Cisco Serviceability Reporter 設定タスク フロー

Cisco Serviceability Reporter による日次システム レポートを設定するには、次のタスクをすべて行います。

手順

	コマンドまたはアクション	目的
ステップ 1	Cisco Serviceability Reporter のアクティブ化 （332 ページ）	日次レポートを生成するためには、**Cisco Serviceability Reporter** サービスが実行されている必要があります。
ステップ 2	Cisco Serviceability Reporter の設定 （333 ページ）	Cisco Serviceability Reporter のスケジュール設定を行います。
ステップ 3	日次レポート アーカイブの表示 （334 ページ）	システムによる日次レポートの生成後、このタスクを使用して PDF ファイル形式で日次レポートを表示します。

Cisco Serviceability Reporter のアクティブ化

次の手順を使用して、**Cisco Serviceability Reporter** による日次システム レポートを有効にします。 レポートを生成するには、サービスを**アクティブ化**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**を選択し、[**Go（移動）**] をクリックします。

ステップ 3 [**パフォーマンスおよびモニタリング サービス（Performance and Monitoring Services）**] の下で、**Cisco Serviceability Reporterr** サービスのステータスを確認します。

ステップ 4 サービスが非アクティブ化されている場合は、隣接するオプション ボタンにチェックを入れ、[**保存（Save）**] をクリックします。

（注） レポートは毎日生成されます。 最初のレポートが生成されるまで最大 24 時間かかる場合があります。

Cisco Serviceability Reporter の設定

Cisco Serviceability Reporter が生成する日次レポートのスケジュール設定を行います。

手順

ステップ 1 Cisco Unified CM Administration 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 2 Cisco Serviceability Reporter を実行している**サーバ**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 Serviceability Reporter] を選択します。

ステップ 4 次のサービス パラメータを設定します。

- **RTMT Reporter Designated Node**：RTMT Reporter が動作する指定ノードを指定します。Cisco では、コール処理を行わないノードを割り当てることを推奨しています。
- **Report Generation Time**：レポートが生成される時刻を、午前 0 時からの時間（分単位）で指定します。 指定範囲は 0 ～ 1439 で、デフォルト設定は 30 分です。
- **Report Deletion Age**：レポートをディスクに保存する日数。 指定範囲は 0 ～ 30 で、デフォルト設定は 7 日間です。

ステップ 5 **[保存（Save）]** をクリックします。

日次レポート アーカイブの表示

Cisco Serviceability Reporter による日次レポートの生成後、次の手順を使用して PDF ファイル形式のレポートを表示します。

手順

ステップ 1 **[ツール（Tools）] > [サービスアビリティ レポートのアーカイブ（Serviceability Reports Archive）]** を選択します。

ステップ 2 レポートを表示したい月と年を選択します。
選択した月に対応する日の一覧が表示されます。

ステップ 3 生成されたレポートを表示したい日付をクリックします。

ステップ 4 表示したいレポートをクリックします。

（注） PDF 形式でレポートを表示するには、Acrobat Reader をインストールしてください。Acrobat Reader をダウンロードするには、[**Serviceability Reports Archive**] ウィンドウの下部にあるリンクをクリックします。

日次レポートの要約

Cisco Serviceability Reporter によって、次のシステム レポートが毎日生成されます。

- デバイス統計レポート
- サーバ統計レポート
- サービス統計レポート
- コール アクティビティ レポート
- アラート サマリー レポート
- パフォーマンス保護レポート

デバイス統計レポート

デバイス統計レポートは、IM and Presence Service および Cisco Unity Connection には適用されません。

デバイス統計レポートでは、次の折れ線グラフが表示されます。

- サーバごとの登録済み電話機の数
- クラスタ内の H.323 ゲートウェイの数

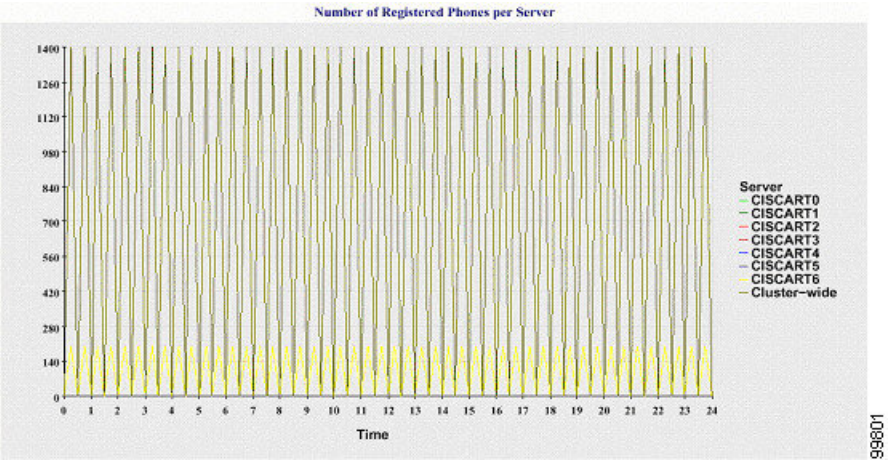
- クラスタ内のトランクの数

サーバごとの登録済み電話機の数

折れ線グラフには、Unified Communications Manager の各サーバ（および Unified Communications Manager クラスタ構成のクラスタ）に登録された電話機の数が表示されます。 グラフの各線はデータが利用できるサーバーのデータを表し、もう 1 本はクラスタ全体のデータを示します（Unified Communications Manager クラスタのみ）。 グラフ内の各データ値は、15 分の間に登録された電話機の平均数を表します。 サーバーにデータが表示されない場合、そのサーバーを表す線は生成されません。 データがサーバ（または Unified Communications Manager クラスタ構成のすべてのサーバ）に存在しない場合、Reporter はグラフを生成しません。「利用可能なデバイス統計レポートのデータがありません」 のメッセージが表示されます。

図 *4:* サーバごとの登録済み電話機の数を示す折れ線グラフ

以下の図では、Unified Communications Manager のクラスタ構成内の Unified Communications Manager サーバごとの登録済み電話機の数を表す折れ線グラフの例を示しています。

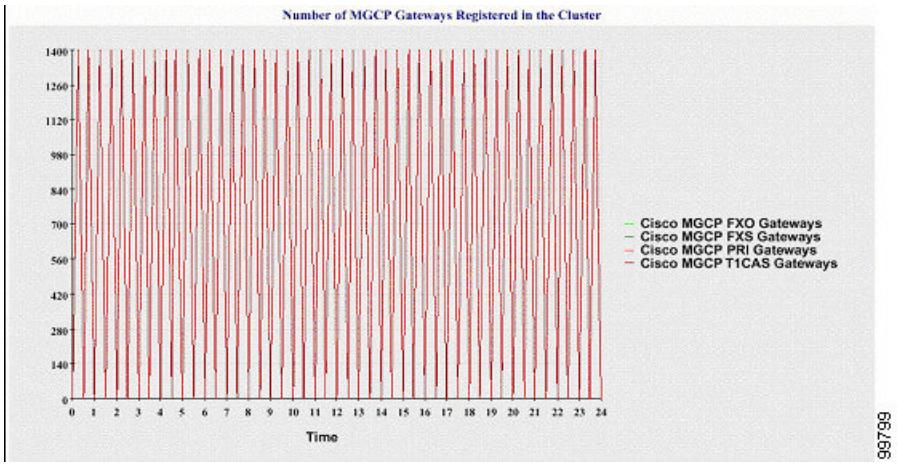


クラスタ内の登録済み MGCP ゲートウェイの数

折れ線グラフには、登録済み MGCP FXO、FXS、PRI、T1CAS ゲートウェイの数が表示されます。 各線は、Unified Communications Manager サーバ（または Unified Communications Manager クラスタ構成のクラスタ）のデータだけを表します。つまり、4 本の線は各ゲートウェイ タイプのサーバ（またはクラスタ全体）の詳細を示します。 グラフ内の各データ値は、15 分の間に登録された MGCP ゲートウェイの平均数を表します。 あるゲートウェイに関するデータがサーバ（またはクラスタ内のすべてのサーバ）に存在しない場合、そのゲートウェイのデータを表す線は生成されません。すべてのゲートウェイに関するデータがサーバ（またはクラスタ内のすべてのサーバ）に存在しない場合、グラフは生成されません。

図 *5:* クラスタごとの登録済みゲートウェイの数を示す折れ線グラフ

次の図は、Unified Communications Manager クラスタ構成におけるクラスタごとの登録済みゲートウェイの数を表す折れ線グラフの例を示しています。

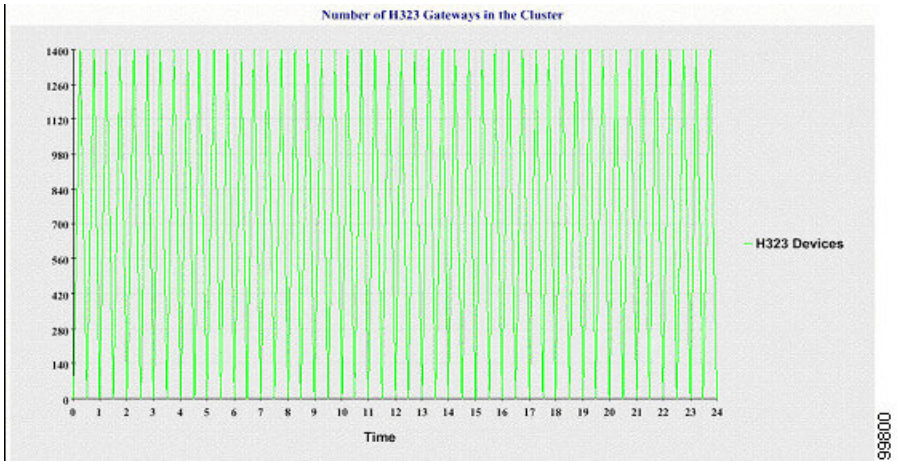


クラスタ内の H.323 ゲートウェイの数

折れ線グラフには、H.323 ゲートウェイの数が表示されます。 1 本の線は、H.323 ゲートウェイの詳細（あるいは Unified Communications Manager のクラスタ構成のクラスタ全体の詳細）を示しています。 グラフ内の各データ値は、15 分間での H.323 ゲートウェイの平均数を表します。 サーバ（またはクラスタ内のすべてのサーバ）の H.323 ゲートウェイに関するデータが存在しない場合、グラフは生成されません。

図 *6:* クラスタごとの登録済み *H.323* ゲートウェイの数を示す折れ線グラフ

次の図は、Unified Communications Manager クラスタ構成のクラスタごとの H.323 ゲートウェイの数を表す折れ線グラフの例を示しています。



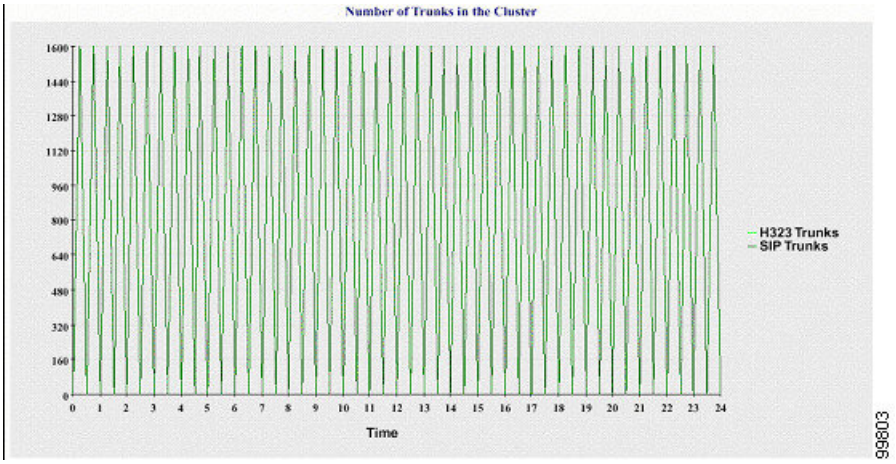
クラスタ内のトランクの数

折れ線グラフには、H.323 および SIP トランクの数が表示されます。 2 本の線が、H.323 トランクおよび SIP トランクの詳細（または Unified Communications Manager のクラスタ構成のクラスタ全体の詳細）を示します。 グラフ内の各データ値は、15 分間での H.323 および SIP トランクの平均数を表します。 サーバ（またはクラスタ内のすべてのサーバ）の H.323 トランクに関するデータが存在しない場合、H.323 トランクのデータを表す線は生成されません。 サー

バ（またはクラスタ内のすべてのサーバ）の SIP トランクに関するデータが存在しない場合、SIP トランクのデータを表す線は生成されません。 トランクに関するデータがまったく存在しない場合、グラフは生成されません。

図 7: クラスタごとのトランクの数を示す折れ線グラフ

次の図は、Unified Communications Manager クラスタ構成のクラスタごとのトランクの数を表す折れ線グラフの例を示します。



サーバ（またはクラスタ内の各サーバ）には、ファイル名パターン DeviceLog_mm_dd_yyyy_hh_mm.csv に一致するログ ファイルが格納されています。 ログ ファイルには次の情報が格納されています。

- サーバ（または Unified Communications Manager クラスタ内の各サーバ）上の登録済み電話機の数
- サーバ（または Unified Communications Manager クラスタ内の各サーバ）上の登録済み MGCP FXO、FXS、PRI、および T1CAS ゲートウェイの数
- サーバ（または Unified Communications Manager クラスタ内の各サーバ）上の登録済み H.323 ゲートウェイの数
- SIP トランクと H.323 トランクの数

サーバ統計レポート

サーバ統計レポートでは、次の折れ線グラフが表示されます。

- サーバごとの CPU のパーセンテージ
- サーバごとのメモリ使用率のパーセンテージ
- サーバごとの最大パーティションのハード ディスク使用率のパーセンテージ

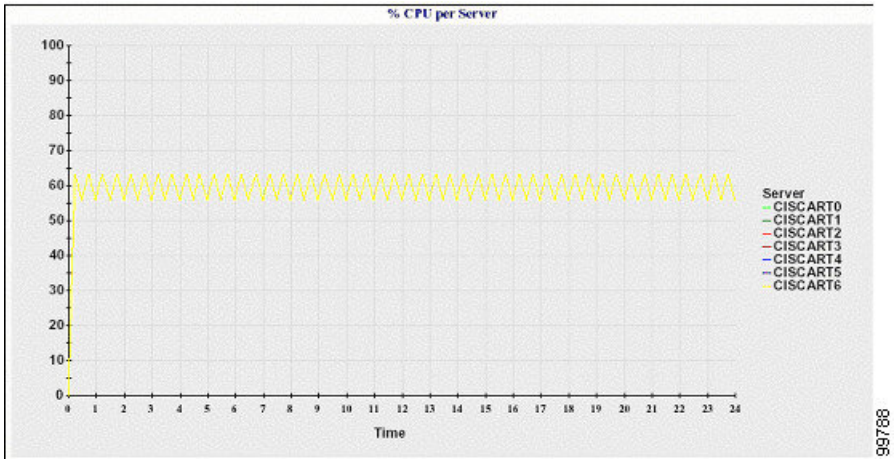
クラスタ固有の統計情報は、Unified Communications Manager および IM and Presence Service でのみサポートされます。

サーバごとの CPU のパーセンテージ

折れ線グラフには、サーバ（またはクラスタ内の各サーバ）の CPU 使用率のパーセンテージが表示されます。 グラフの折れ線は、データが利用できるサーバーのデータを表します（または、クラスタ内のサーバーごとに 1 本の折れ線）。 グラフ内の各データ値は、15 分間の平均 CPU 使用率を表します。 サーバー（またはクラスタ内のいずれかのサーバー）のデータが存在しない場合、そのサーバーを表す線は生成されません。 生成する線がない場合は、Reporter はグラフを作成しません。 「利用可能なサーバ統計レポートのデータがありません」 のメッセージが表示されます。

図 *8*：サーバごとの *CPU* のパーセンテージを示す折れ線グラフ

次の図は、Unified Communications Manager のクラスタ構成でサーバごとの CPU 使用率のパーセンテージを表す折れ線グラフの例を示します。

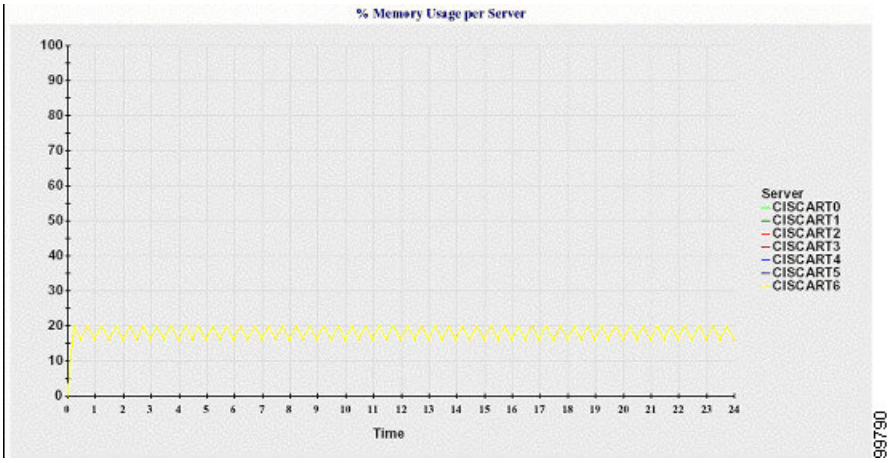


サーバごとのメモリ使用率のパーセンテージ

折れ線グラフには、Unified Communications Manager サーバーのメモリ使用率のパーセンテージ（%MemoryInUse）が表示されます。 Unified Communications Manager クラスタ構成では、データが利用できるクラスタ内のサーバごとに 1 本の線があります。 グラフ内の各データ値は、15 分間の平均メモリ使用率を表します。 データが存在しない場合はグラフが生成されません。 クラスタ構成でいずれかのサーバーのデータが存在しない場合、Reporter はそのサーバーを表す線を生成しません。

図 *9*：サーバごとのメモリ使用率のパーセンテージを示す折れ線グラフ

次の図は、クラスタ構成で Unified Communications Manager サーバあたりのメモリ消費率を示す線グラフの例を示します。

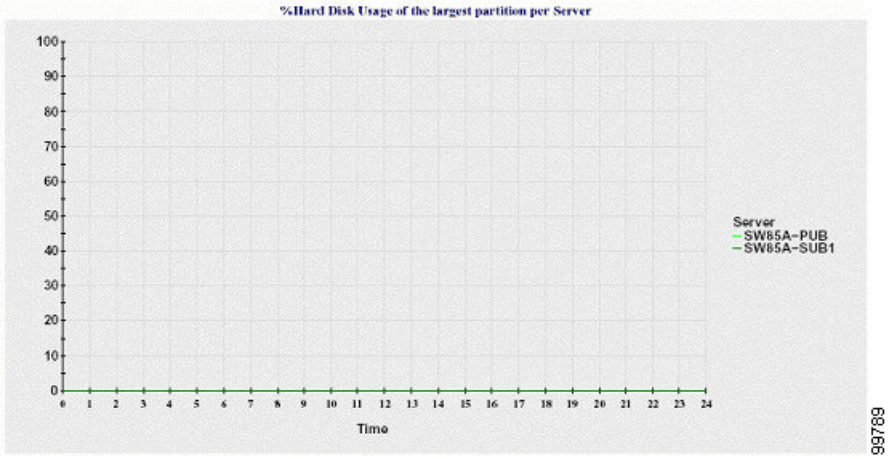


サーバごとの最大パーティションのハード ディスク使用率のパーセンテージ

折れ線グラフには、サーバまたはクラスタ構成の各サーバー上の最大パーティションのディスク領域使用率のパーセンテージ（%DiskSpaceInUse）が表示されます。 グラフ内の各データ値は、15 分間の平均ディスク使用率を表します。 データが存在しない場合はグラフが生成されません。 クラスタ構成でいずれかのサーバーのデータが存在しない場合、Reporter はそのサーバーを表す線を生成しません。

図 *10*：サーバごとの最大パーティションのハード ディスク使用率のパーセンテージを示す折れ線グラフ

次の図は、Unified Communications Manager のクラスタ構成でサーバごとの最大パーティションのハード ディスク使用率のパーセンテージを表す折れ線グラフの例を示します。



サーバ（またはクラスタ構成内の各サーバ）には、ファイル名パターン ServerLog_mm_dd_yyyy_hh_mm.csv に一致するログ ファイルが格納されています。 ログ ファイルには次の情報が格納されています。

- サーバ（またはクラスタ内の各サーバ）での CPU 使用率
- サーバ（またはクラスタ内の各サーバ）でのメモリ使用率（%MemoryInUse）

- サーバ（またはクラスタの各サーバ）の最大パーティションのハードディスク使用率（%DiskSpaceInUse）

サービス統計レポート

サービス統計レポートは、IM and Presence Service および Cisco Unity Connection をサポートしていません。

サービス統計レポートでは、次の折れ線グラフが表示されます。

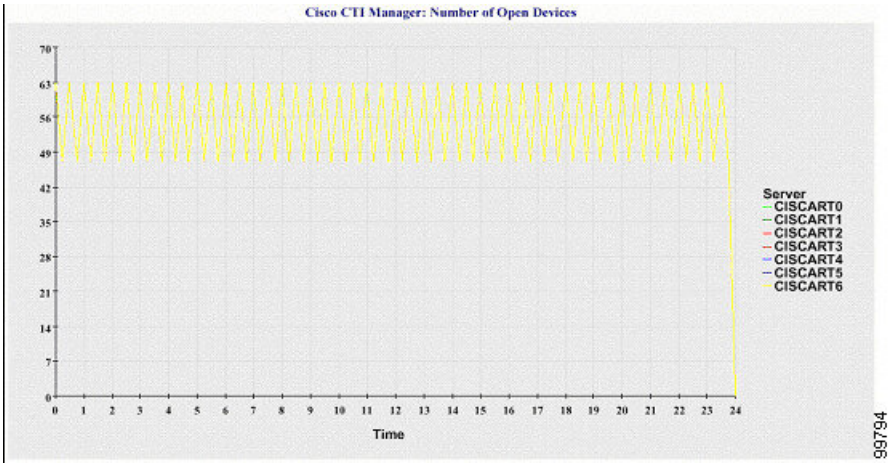
- Cisco CTI Manager：オープン デバイスの数
- Cisco CTI Manager：オープン回線の数
- Cisco TFTP：リクエストの数
- Cisco TFTP：中断されたリクエストの数

Cisco CTI Manager：オープン デバイスの数

折れ線グラフには、CTI Manager（または Unified Communications Manager クラスタ構成内の各 CTI Manager）の CTI オープン デバイスの数が表示されます。 各折れ線グラフは、サービスがアクティブなサーバ（または Unified Communications Manager のクラスタ内の各サーバ）のデータを表します。 グラフ内の各データ値は、15 分間の CTI オープン デバイスの平均数を表します。 データが存在しない場合はグラフが生成されません。 Unified Communications Manager クラスタ構成でいずれかのサーバーのデータが存在しない場合、Reporter はそのサーバーを表す線を生成しません。 「利用可能なサービス統計レポートのデータがありません」 のメッセージが表示されます。

図 *11 : Cisco CTI Manager*：オープン デバイスの数を示す折れ線グラフ

次の図は、Unified Communications Manager のクラスタ構成で Cisco CTI Manager あたりのオープン デバイスを表す折れ線グラフの例を示します。

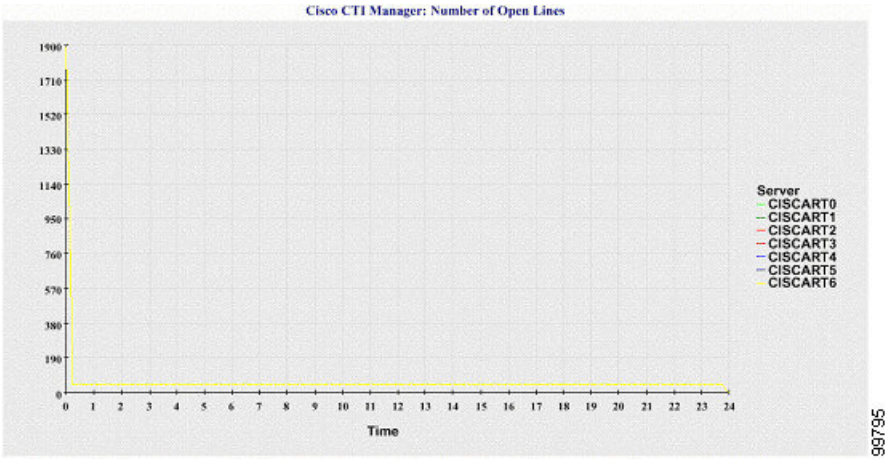


Cisco CTI Manager：オープン回線の数

折れ線グラフには、CTI Manager（または Unified Communications Manager クラスタ構成内の CTI Manager ごと）の CTI オープン回線の数が表示されます。 グラフの折れ線は、Cisco CTI Manager サービスがアクティブなサーバーのデータを表します（または Unified Communications Manager クラスタ構成内のサーバーごとに 1 本の線）。 グラフ内の各データ値は、15 分間の CTI オープン回線の平均数を表します。 データが存在しない場合はグラフが生成されません。 Unified Communications Manager クラスタ構成でいずれかのサーバーのデータが存在しない場合、Reporter はそのサーバーを表す線を生成しません。

図 *12 : Cisco CTI Manager*：オープン回線の数を示す折れ線グラフ

次の図は、Unified Communications Manager のクラスタ構成内の Cisco CTI Manager ごとのオープン回線の数を表す折れ線グラフの例を示します。

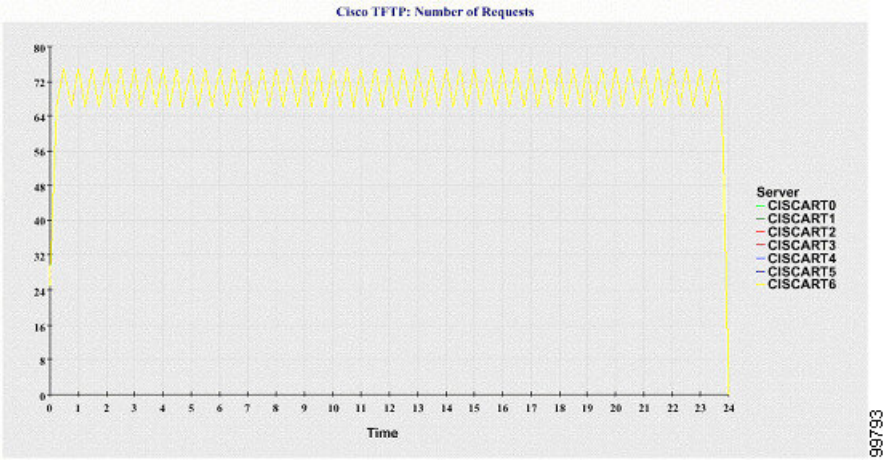


Cisco TFTP：リクエストの数

折れ線グラフには、TFTP サーバー（または Unified Communications Manager クラスタ構成内の TFTP サーバーごと）の Cisco TFTP リクエストの数が表示されます。 グラフの折れ線は、Cisco TFTP サービスがアクティブなサーバーのデータを示します（または Unified Communications Manager クラスタ内のサーバーごとに 1 本の線）。 グラフ内の各データ値は、15 分間の TFTP リクエストの平均数を表します。 データが存在しない場合はグラフが生成されません。 Unified Communications Manager クラスタ構成でいずれかのサーバーのデータが存在しない場合、Reporter はそのサーバーを表す線を生成しません。

図 *13 : Cisco TFTP*：リクエストの数を示す折れ線グラフ

次の図は、TFTP サーバーごとの Cisco TFTP リクエストの数を表す折れ線グラフの例を示します。

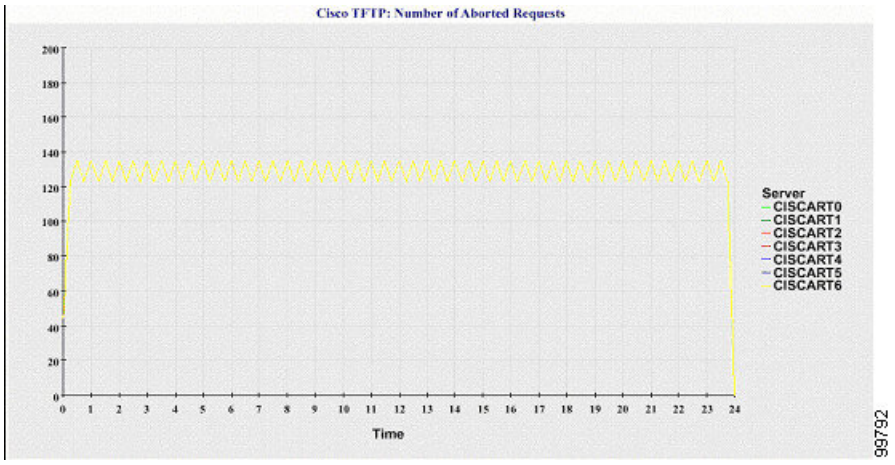


Cisco TFTP：中断されたリクエストの数

折れ線グラフには、TFTP サーバー（または Unified Communications Manager クラスタ構成内の TFTP サーバーごと）の中断された Cisco TFTP リクエストの数が表示されます。 グラフの折れ線は、Cisco TFTP サービスがアクティブなサーバーのデータを示します（または Unified Communications Manager クラスタ内のサーバーごとに 1 本の線）。 グラフ内の各データ値は、15 分間の中断された TFTP リクエストの平均を表します。 データが存在しない場合はグラフが生成されません。 Unified Communications Manager クラスタ構成でいずれかのサーバーのデータが存在しない場合、Reporter はそのサーバーを表す線を生成しません。

図 *14 : Cisco TFTP*：中断されたリクエストの数を示す折れ線グラフ

次の図は、TFTP サーバーごとに中断された Cisco TFTP リクエストの数を表す折れ線グラフの例を示します。



サーバ（または Unified Communications Manager クラスタ内の各サーバ）には、ファイル名パターン ServiceLog_mm_dd_yyyy_hh_mm.csv に一致するログ ファイルが格納されています。 ログ ファイルには次の情報が格納されています。

- 各 CTI Manager：オープン デバイスの数

- 各 CTI Manager：オープン回線の数
- 各 Cisco TFTP サーバ：TotalTftpRequests
- 各 Cisco TFTP サーバ：TotalTftpRequestsAborted

コール アクティビティ レポート

コール アクティビティ レポートは、IM and Presence Service および Cisco Unity Connection をサポートしていません。

コール アクティビティ レポートでは、次の折れ線グラフが表示されます。

- クラスタの Unified Communications Manager コール アクティビティ
- クラスタの H.323 ゲートウェイ コール アクティビティ
- クラスタの MGCP ゲートウェイ コール アクティビティ
- MGCP ゲートウェイ
- クラスタのトランク コール アクティビティ

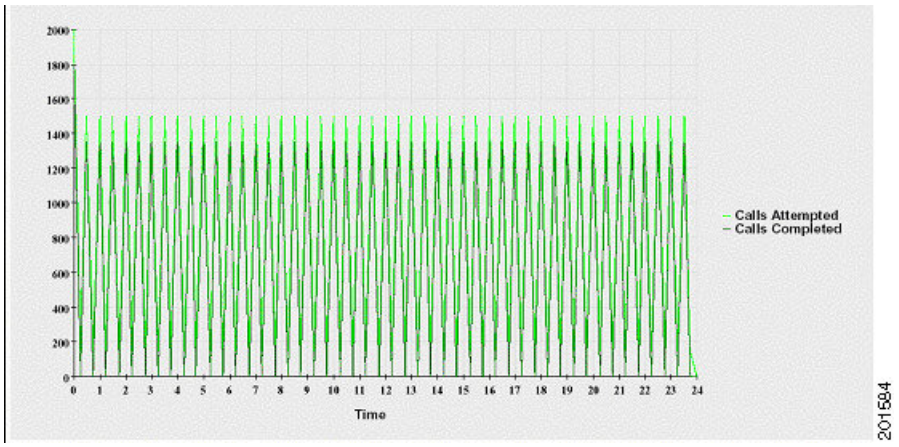
クラスタの Cisco Unified Communications Manager コール アクティビティ

折れ線グラフには、Unified Communications Manager の試行されたコールと完了したコールの数が表示されます。 Unified Communications Manager のクラスタ構成では、折れ線グラフはクラスタ全体の試行されたコールと完了したコールの数を表示します。グラフは2本の線で構成されます。1 本は試行されたコールの数、もう 1 本は完了したコールの数を示します。 Unified Communications Manager のクラスタ構成では、各線はクラスタ値を表します。これは（データが利用できる）クラスタ内のすべてのサーバーの値の合計です。グラフ内の各データ値は、15 分の間に試行されたコールと完了したコールの総数を表します。

完了した Unified Communications Manager のコールのデータがない場合、Reporter は完了したコールのデータを表す線を生成しません。 試行された Unified Communications Manager コールのデータが存在しない場合、試行されたコールのデータを表す線は生成されません。 Unified Communications Manager のクラスタ構成では、クラスタ内のサーバーのデータがない場合、Reporter はそのサーバーで試行されたコールまたは完了したコールを表す線を生成しません。Unified Communications Manager コール アクティビティのデータがまったく存在しない場合、グラフは生成されません。「利用可能なコール アクティビティ レポートのデータがありません」 のメッセージが表示されます。

図 *15 :* クラスタの *Cisco Unified Communications Manager* コール アクティビティを示す折れ線グラフ

次の図は、Unified Communications Manager クラスタの試行されたコールと完了したコールを表す折れ線グラフを示しています。

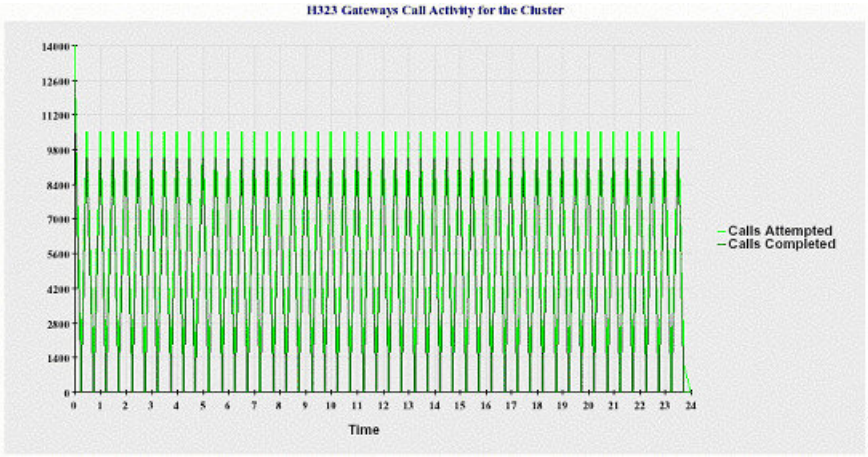


クラスタの H.323 ゲートウェイ コール アクティビティ

折れ線グラフには、H.323 ゲートウェイの試行されたコールと完了したコールの数が表示されます。 Unified Communications Manager のクラスタ構成では、折れ線グラフはクラスタ全体の試行されたコールと完了したコールの数を表示します。 グラフは 2 本の線で構成されます。1 本は試行されたコールの数、もう 1 本は完了したコールの数を示します。 Unified Communications Manager のクラスタ構成では、各線はクラスタ値を表します。これは（データが利用できる）クラスタ内のすべてのサーバーの値の合計と等しくなります。 グラフ内の各データ値は、15 分の間に試行されたコールと完了したコールの総数を表します。 完了した H.323 ゲートウェイ コールのデータが存在しない場合、完了したコールのデータを表す線は生成されません。 試行された H.323 ゲートウェイ コールのデータが存在しない場合、試行されたコールのデータを表す線は生成されません。 Unified Communications Manager のクラスタ構成では、クラスタ内のサーバーのデータがない場合、Reporter はそのサーバーで試行されたコールまたは完了したコールを表す線を生成しません。 H.323 ゲートウェイ コール アクティビティのデータがまったく存在しない場合、グラフは生成されません。

図 *16 : クラスタの H.323 ゲートウェイ コール アクティビティを示す折れ線グラフ*

次の図は、Unified Communications Manager クラスタの H.323 ゲートウェイ コール アクティビティを表す折れ線グラフを示しています。

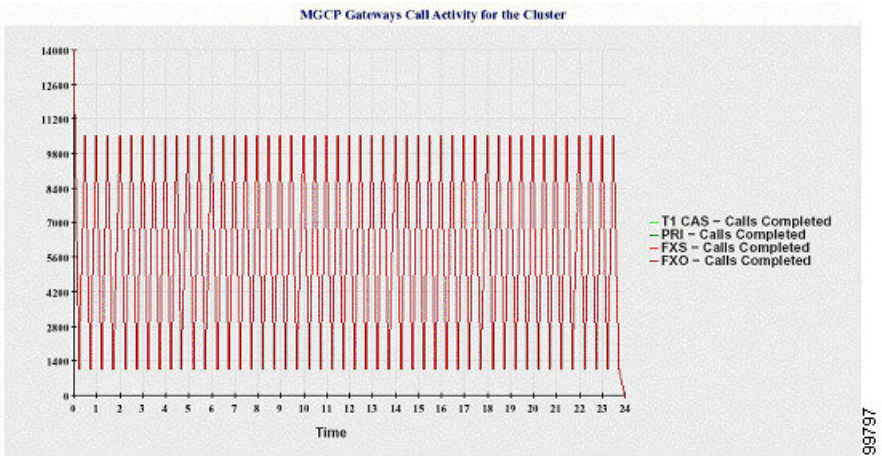


クラスタの MGCP ゲートウェイ コール アクティビティ

折れ線グラフには、MGCP FXO、FXS、PRI、および T1CAS ゲートウェイの 1 時間に完了したコールの数が表示されます。 Unified Communications Manager クラスタ構成では、グラフには Unified Communications Manager クラスタ全体の完了したコールの数が表示されます。 グラフは最大 4 本の線で構成され、完了したコールの数が（データが利用できる）ゲートウェイ タイプごとに示されます。 グラフ内の各データ値は、15 分の間に完了したコールの総数を表します。 ゲートウェイのデータが存在しない場合、その特定のゲートウェイについて完了したコールのデータを表す線は生成されません。すべてのゲートウェイに関してデータが存在しない場合、グラフは生成されません。

図 *17*：クラスタの *MGCP* ゲートウェイ コール アクティビティを示す折れ線グラフ

次の図は、Unified Communications Manager クラスタの MGCP ゲートウェイ コール アクティビティを表す折れ線グラフを示しています。

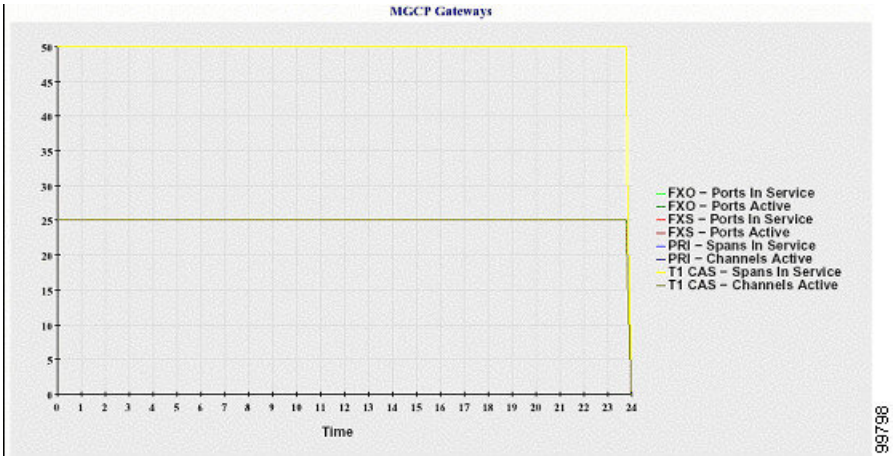


MGCP ゲートウェイ

折れ線グラフには、MGCP FXO ゲートウェイと FXS ゲートウェイの稼働中のポートおよびアクティブ ポートの数、および PRI ゲートウェイと T1CAS ゲートウェイの稼働中のスパンまたはアクティブ チャネルの数が表示されます。 Unified Communications Manager クラスタ構成の場合、グラフには Unified Communications Manager クラスタ全体のデータが表示されます。 グラフは 8 本の線で構成され、MGCP FXO および FXS の稼働中のポートの数に 2 本、MGCP FXO および FXS のアクティブ ポートの数に 2 本割り当てられています。 残りの 4 本は、PRI および T1CAS ゲートウェイの稼働中のスパンとアクティブ チャネルの数を示しています。 Unified Communications Manager のクラスタ構成では、各線はクラスタ値を表します。これは（データが利用できる）クラスタ内のすべてのサーバーの値の合計です。 グラフ内の各データ値は、15 分間での稼働中のポートの総数、アクティブ ポートの数、稼働中のスパンの数、またはアクティブ チャネルの数を表します。 すべてのサーバーについて、ゲートウェイ（MGCP PRI、T1CAS）の稼働中のスパンまたはアクティブチャネルの数に関するデータが存在しない場合、そのゲートウェイのデータを表す線は生成されません。

図 *18*：*MGCP* ゲートウェイを示す折れ線グラフ

次の図は、MGCP ゲートウェイを表す折れ線グラフを示しています。

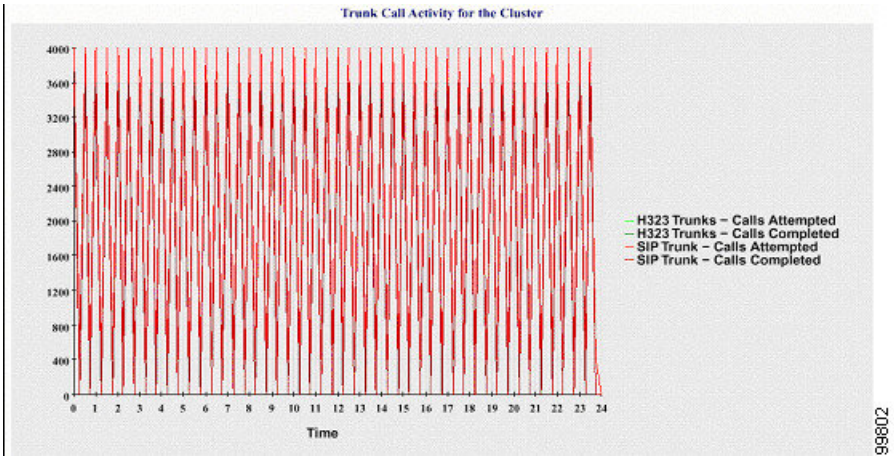


クラスタのトランク コール アクティビティ

折れ線グラフには、SIP トランクと H.323 トランクの 1 時間に完了したコールと試行されたコールの数が表示されます。 Unified Communications Manager クラスタ構成の場合、グラフには Unified Communications Manager クラスタ全体の完了したコールと試行されたコールの数が表示されます。 グラフは 4 本の線で構成されます。2 本は（データが利用できる）各 SIP および H.323 トランクの完了したコールの数、もう 2 本は試行されたコールの数を示します。 Unified Communications Manager のクラスタ構成では、各線はクラスタ値を表します。これは（データが利用できる）クラスタ内のすべてのノードの値の合計です。 グラフ内の各データ値は、15 分の間に完了したコールの総数または試行されたコールの数を表します。 トランクのデータが存在しない場合、その特定のトランクについて完了したコールまたは試行されたコールを表す線は生成されません。 両方のトランク タイプに関してデータが存在しない場合、グラフは生成されません。

図 *19*：クラスタのトランク コール アクティビティを示す折れ線グラフ

下の図は、Unified Communications Manager クラスタのトランク コール アクティビティを表す折れ線グラフを示しています。



サーバ（または Unified Communications Manager クラスタ構成内の各サーバ）には、ファイル名パターン CallLog_mm_dd_yyyy_hh_mm.csv に一致するログ ファイルが格納されています。ログ ファイルには次の情報が格納されています。

- Unified Communications Manager（または Unified Communications Manager クラスタ内の各サーバ）の試行されたコールおよび完了したコール
- H.323 ゲートウェイ（または Unified Communications Manager クラスタ内の各サーバーのゲートウェイ）の試行されたコールおよび完了したコール
- MGCP FXO、FXS、PRI、T1CAS ゲートウェイ（または Unified Communications Manager クラスタ内の各サーバーのゲートウェイ）の完了したコール
- （Unified Communications Manager クラスタ内の各サーバーの）MGCP FXO ゲートウェイと FXS ゲートウェイの稼働中のポートおよびアクティブ ポート、および PRI ゲートウェイと T1CAS ゲートウェイの稼働中のスパンおよびアクティブチャネル
- H.323 トランクと SIP トランクの試行されたコールおよび完了したコール

アラート サマリー レポート

アラート サマリー レポートには、その日に生成されたアラートの詳細が表示されます。

クラスタ固有の統計情報は、Unified Communications Manager および IM and Presence Serviceでのみサポートされます。

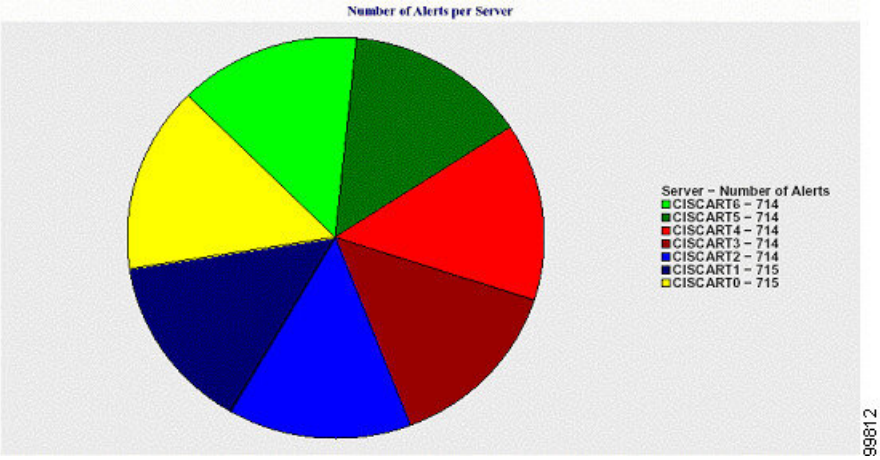
サーバごとのアラートの数

クラスタ内のノードごとのアラートの数が円グラフに表示されます。グラフには、生成されたアラートのサーバ全体の詳細が表示されます。 円グラフの各領域は、クラスタの特定のサーバーに対して生成されたアラートの数を表しています。 グラフには、クラスタ内のサーバ（Reporterによってその日にアラートが生成されたサーバ）と同じ数の領域が含まれます。 あるサーバーのデータがない場合、そのサーバーを表すチャートの領域はありません。すべてのサーバーのデータが存在しない場合はグラフが生成されません。「「指定された日に生成されたアラートはありません」」というメッセージが表示されます。

Cisco Unity Connection のみ：円グラフには、サーバーのアラート数が示されます。 グラフには、生成されたアラートのサーバ全体の詳細が表示されます。サーバーのデータが存在しない場合はグラフが生成されません。「指定された日に生成されたアラートはありません」というメッセージが表示されます。

下のグラフは、Unified Communications Managerクラスタ内のサーバごとのアラートの数を表す円グラフの例を示します。

図 *20* : サーバごとのアラート数を示す円グラフ

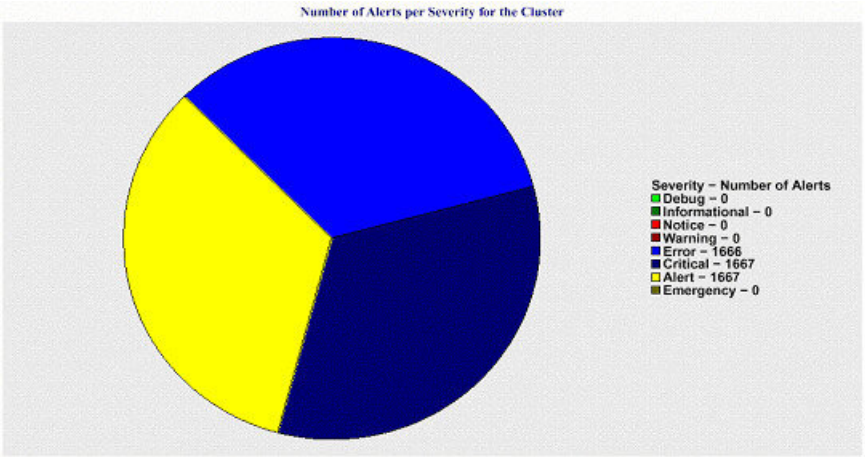


クラスタの重大度ごとのアラート数

アラートの重大度ごとのアラート数が円グラフに表示されます。 グラフには、生成されたアラートの重大度の詳細が表示されます。 円グラフの各領域は、生成された特定の重大度タイプのアラートの数を表します。 グラフには、（Reporter によってその日に生成されたアラートの）重大度と同じ数の領域が含まれます。 ある重大度のデータがない場合、その重大度を表すチャートの領域はありません。 データが存在しない場合はグラフが生成されません。

下のグラフは、Unified Communications Manager クラスタの重大度ごとのアラートの数を表す円グラフの例を示します。

図 *21* : クラスタの重大度ごとのアラート数を示す円グラフ



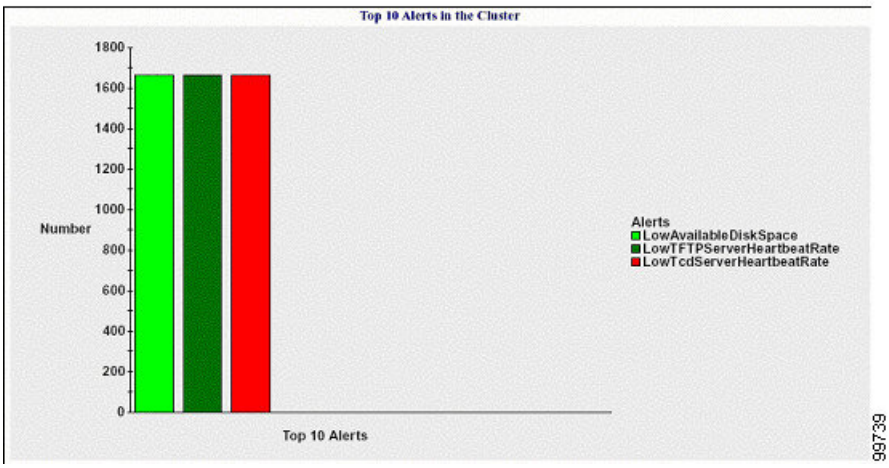
クラスタ内の上位 10 のアラート

特定のアラート タイプのアラート数が棒グラフに表示されます。 グラフには、アラート タイプに基づいて生成されたアラートの詳細が表示されます。 それぞれの折れ線は、そのアラートタイプのアラートの数を表します。 グラフには、アラート数が多いものから順に、最初の 10

個のアラートの詳細のみが表示されます。 特定のアラート タイプのデータがない場合、そのアラートを表す折れ線はありません。 アラート タイプのデータがない場合はグラフが生成されません。

下のグラフは、Unified Communications Manager クラスタ内の上位 10 のアラートを表す棒グラフの例を示しています。

図 *22* : クラスタ内の上位 *10* のアラートを示す棒グラフ



サーバ（またはクラスタ内の各サーバ）には、ファイル名パターン AlertLog_mm_dd_yyyy_hh_mm.csv に一致するログ ファイルが格納されています。 ログ ファイルには次の情報が格納されています。

- 時刻：アラートが発生した時刻
- アラート名：わかりやすい名前
- ノード名：アラートが発生したサーバ
- モニタ対象オブジェクト：モニタされるオブジェクト
- 重大度：アラートの重大度

パフォーマンス保護レポート

パフォーマンス保護レポートは、IM and Presence Service および Cisco Unity Connection をサポートしていません。

パフォーマンス保護レポートには、特定のレポートの統計情報を表示するさまざまなグラフで構成される要約が表示されます。 Reporter は、ログに記録された情報に基づいてレポートを 1 日 1 回生成します。

パフォーマンス保護レポートは、過去 7 日間のデフォルト モニタリング オブジェクトに関する傾向分析情報を提供します。この情報により、Cisco Intercompany Media Engine に関する情報を追跡できます。 レポートには、Cisco IME クライアントの総コール数およびフォールバック コール率を示す Cisco IME クライアント コール アクティビティ グラフが表示されます。

パフォーマンス保護レポートは、次のグラフで構成されます。

- Cisco Unified Communications Manager コール アクティビティ
- 登録済み電話機および MGCP ゲートウェイの数
- システム リソースの使用率
- デバイスとダイヤル プランの数量

Cisco Unified Communications Manager コール アクティビティ

折れ線グラフには、試行されたコールと完了したコールの数の 1 時間ごとの増減率がアクティブ コール数として表示されます。 Unified Communications Manager のクラスタ構成では、クラスタ内の各サーバーのデータのグラフが作成されます。 グラフは 3 本の線で構成され、それぞれ試行されたコールの数、完了したコールの数、およびアクティブ コールを示します。 コール アクティビティのデータが存在しない場合、Reporter はグラフを生成しません。

登録済み電話機および MGCP ゲートウェイの数

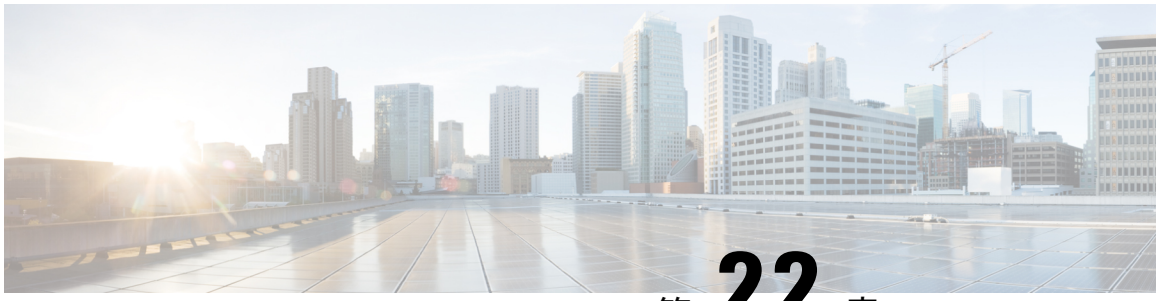
折れ線グラフには、登録済み電話機および MGCP ゲートウェイの数が表示されます。 Unified Communications Manager のクラスタ構成の場合、グラフにはクラスタ内の各サーバーのデータが表示されます。グラフは 2 本の線で構成され、1 本は登録済み電話機の数、もう 1 本は MGCP ゲートウェイの数を示します。 電話機または MGCP ゲートウェイのデータがない場合、Reporter はグラフを生成しません。

システム リソースの使用率

折れ線グラフには、サーバ（または Unified Communications Manager クラスタ構成のクラスタ全体）の CPU 負荷率とメモリ使用率（バイト）が表示されます。 グラフは 2 本の線で構成され、1 本は CPU 負荷、もう 1 本はメモリ使用率を示します。 Unified Communications Manager のクラスタでは、各線はクラスタ値を表します。これは（データが利用できる）クラスタ内のすべてのサーバーの値の平均です。 電話機または MGCP ゲートウェイのデータがない場合、Reporter はグラフを生成しません。

デバイスとダイヤル プランの数量

2 つのテーブルに、デバイスの数およびダイヤル プラン コンポーネントの数に関する Unified Communications Manager データベースの情報が表示されます。 デバイス テーブルは、IP フォン、Cisco Unity Connection ポート、H.323 クライアント、H.323 ゲートウェイ、MGCP ゲートウェイ、MOH リソース、および MTP リソースの数を示します。 ダイヤル プラン テーブルは、電話番号と回線、ルート パターン、およびトランスレーション パターンの数を示します。



第 22 章

Cisco Unified のレポート

統合されたデータのレポート

Cisco Unified Communications Manager および Cisco Unified Communications Manager IM and Presence Service コンソールからアクセスする Cisco Unified Reporting Web アプリケーションは、トラブルシューティングまたはクラスタデータの調査のための統合レポートを生成します。

（注） 特に指定のない限り、このマニュアルの情報、注記、手順は Unified Communications Manager と IM and Presence Service に適用されます。

このツールは、クラスタ データのスナップショットを簡単に作成する方法を提供します。 このツールは、既存のソースからのデータの収集、データの比較、および異常の報告を行います。 Cisco Unified Reporting でレポートを生成すると、レポートでは、1 台以上のサーバーにある 1 つ以上のソースからのデータを結合して、1 つの出力ビューを作成します。 たとえば、クラスタ内の全サーバーの *hosts* ファイルを表示するレポートを参照できます。

Cisco Unified Reporting Web アプリケーションは、インストール時にクラスタ内のすべてのサーバーに展開されます。 レポートは、データベース レコードから生成されます。

レポートの生成に使用するデータ ソース

このアプリケーションでは、パブリッシャサーバーと各サブスクライバサーバーに格納されている次のいずれかのソースから情報を取り込みます。

- RTMT カウンタ
- CDR_CAR （Unified Communications Managerのみ）

- Unified Communications ManagerDB（Unified Communications Manager のみ）
- IM and Presence DB（IM and Presence Service のみ）
- ディスク ファイル
- OS API 呼び出し
- ネットワーク API 呼び出し
- prefs
- CLI
- RIS

レポートには、レポートの生成時点でアクセスできるすべてのアクティブなクラスタ ノードのデータが取り込まれます。パブリッシャサーバーのデータベースが停止している場合は、アクティブなノードのレポートを生成できます。 System Reports リストにある Report Descriptions レポートは、レポートの情報ソースを提供します。

サポートされている出力形式

このリリースでは、レポートの HTML/CSV 出力をサポートしています。 Cisco Unified Reporting では、レポート名と日付と時刻のスタンプによってレポートを識別できます。 このアプリケーションでは、ユーザーが表示できるように最近のレポートのローカルコピーが保管されます。「「新しいレポートのダウンロード」」で説明しているように、最近のレポートのローカルコピーまたは新しいレポートをハード ディスクにダウンロードすることができます。 レポートをダウンロードするときは、区別するためにダウンロードするファイルの名前を変更するか、別のフォルダに保存できます。

システム要件

Cisco Tomcat サービス

Cisco Unified Reporting は、Cisco Tomcat サービス上でアプリケーションとして実行されます。このアプリケーションは、Unified CM および IM and Presence Service のインストールUnified Communications Manager時にアクティブになります。 これらの製品がクラスタ内のすべてのサーバーで稼働していることを確認します。

HTTPS

レポート サブシステムでは、HTTPS 経由で RPC メカニズムを使用して他のサーバから情報を収集します。 レポートが正常に生成されるように、サーバーで HTTPS ポートが開いていて、Cisco Tomcat サービスを実行していることを確認します。

HTTPS を有効にするには、接続プロセス中にサーバ識別用の証明書をダウンロードする必要があります。 現在のセッションだけにサーバー証明書を使用するか、サーバーでの現在のセッ

ションと将来のセッションのセキュリティを確保するために信頼フォルダ（ファイル）に証明書をダウンロードすることができます。信頼フォルダには、すべての信頼済みサイトの証明書を保存します。 HTTPS の詳細については、『*Cisco Unified Communications Manager* 管理ガイド』の「「はじめに」」の章を参照してください。

アプリケーションにアクセスするには、ブラウザウィンドウの管理インターフェイスにアクセスします。 Cisco Unified Reporting では、HTTPS を使用してブラウザとのセキュアな接続を確立します。

必要なアクセス権限

Cisco Unified Reporting アプリケーションでは、Cisco Tomcat サービスを使用してユーザーを認証してから、Web アプリケーションへのアクセスを許可します。 権限のあるユーザだけが Cisco Unified Reporting アプリケーションにアクセスできます。 Unified Communications Manager の場合、デフォルトでは、Standard CCM Super Users グループの管理者ユーザだけが Cisco Unified Reporting にアクセスして、レポートを表示、作成できます。

Cisco Unified Communications Manager および IM and Presence Service の場合は、Standard CUReporting 認証ロールのユーザーが Cisco Unified Reporting にアクセスできます。

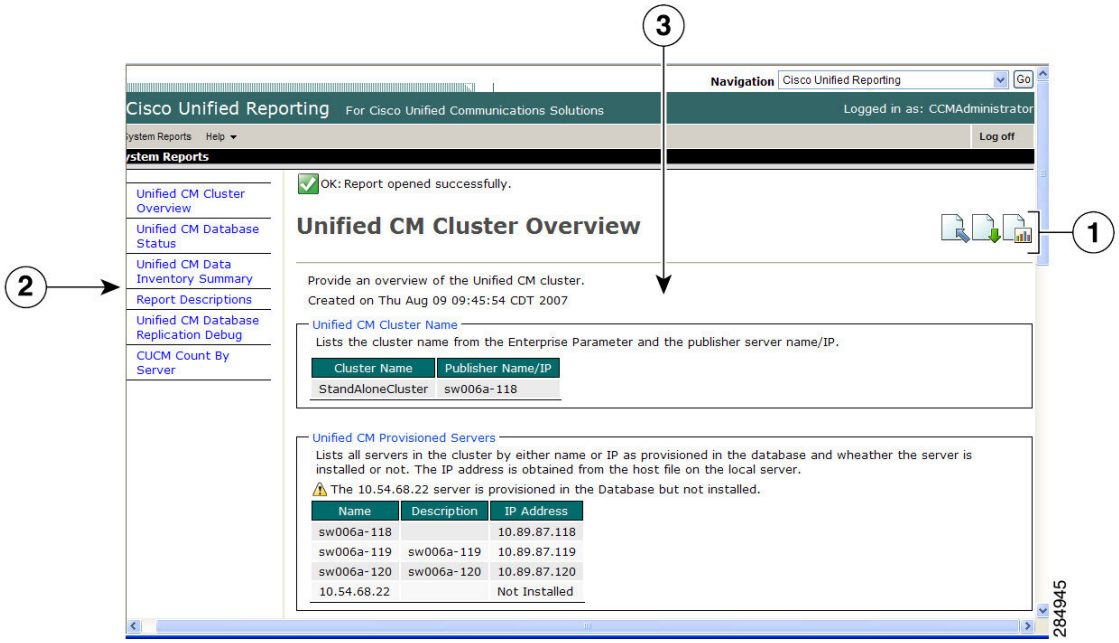
権限のあるユーザーは、Cisco Unified Reporting ユーザーインターフェイスを使用して、レポートの表示、新しいレポートの生成、およびレポートのダウンロードを実行できます。

（注） にUnified Communications Manager、 Standard CCM Super Users グループの管理者ユーザーはアプリケーションの 1 個に管理のUnified Communications Managerナビゲーションメニューの管理アプリケーションに、SSO を備えた Cisco Unified Reporting など、アクセスできます。

UI のコンポーネント

次の図に、Cisco Unified Reporting の UI のコンポーネントを示します。

図 *23 : UI* のコンポーネント



1. [アップロード（Upload）]、[ダウンロード（Download）]、[生成（Generate）] アイコン
2. レポート リスト
3. レポートの詳細

（注） レポートのカテゴリ、使用できるレポート、およびレポートのデータは、リリースによって異なります。

管理インターフェイスからのログイン

次のいずれかの手順を実行し、管理インターフェイスから Cisco Unified Reporting にログインします。

- Unified Communications Managerの場合は、Cisco Unified CM Administration インターフェイスのナビゲーション メニューから**[Cisco Unified Reporting]**を選択します。
- IM and Presence Service の場合は、IM and Presence 管理インターフェイスのナビゲーション メニューから **[Cisco Unified IM and Presence Reporting]** を選択します。

始める前に

Cisco Unified Reporting アプリケーションへのアクセスが許可されていることを確認します。

Cisco Unified Reporting にログインすると、各ユーザーの最後に成功したシステムログインと最後に失敗したシステムログインが、ユーザー ID、日時、IP アドレスとともに、[Cisco Unified Reporting] ウィンドウに表示されます。

サポートされているレポート

このセクションでは、Cisco Unified Communications Manager および Cisco Unified Communications Manager IM and Presence Service でサポートされているレポートの詳細について説明します。Cisco Unified Reporting では、レポート名と日付と時刻のスタンプによってレポートを識別できます。 Cisco Unified Reporting では、ユーザが表示できるように最近のレポートのローカル コピーが保管されます。

Unified Communications Managerのレポート

次の表に、Unified Communications Manager をインストールした後に Cisco Unified Reporting に表示されるシステムレポートの種類を示します。

表 *75 : Unified Communications Manager Cisco Unified Reporting* で表示されるレポート

レポート	説明
期限切れのクレデンシャルアルゴリズムを使用したUCMユーザ（UCM Users with Out-Of-Date Credential Algorithm）	SHA1 を使用してパスワードまたは Pin が保存され、ハッシュされているエンドユーザーのリストを提供しています。
レポートの説明（Report Descriptions）	表示しているレポートに関するトラブルシューティング情報と詳細情報を提供します。
セキュリティ診断ツール（Security Diagnostic Tool）	セキュリティ コンポーネントに関する情報の要約を提供します。
Unified CM クラスタの概要（Unified CM Cluster Overview）	Unified Communications Manager クラスタの概要を提供します。このレポートには、次の詳細情報が含まれています。 • Unified Communications Managerまたは IM およびプレゼンス クラスタにインストールしたバージョンを保守します。 • クラスタ内のすべてのサーバーのホスト名または IP アドレス • ハードウェア詳細情報の要約

レポート	説明
Unified CM データ サマリ（Unified CM Data Summary）	データベースUnified Communications Managerにある場合にUnified Communications Managerメニュー構造に従ってデータの要約が示されます。 たとえば、3 つのクレデンシャル ポリシー、5 つの会議ブリッジ、10 のシェアドライン アピアランスを設定した場合、このレポートに含まれる情報のタイプを確認できます。
Unified CM データベース複製のデバッグ（Unified CM Database Replication Debug）	データベース複製のためのデバッグ情報を提供します。 **ヒント** このレポートを生成すると、CPU の使用率が急増し、生成するのにクラスタ内のサーバごとに最大 10 秒かかる可能性があります。
Unified CM データベース ステータス（Unified CM Database Status）	Unified Communications Manager データベースのヘルス スナップショットを提供します。アップグレードする前にこのレポートを生成して、データベースが正常であることを確認します。
Unified CM デバイス カウント サマリ（Unified CM Device Counts Summary）	存在Unified Communications Managerするデバイスの数を、モデルおよびプロトコル別に示します。
Unified CM デバイス配信サマリ（Unified CM Device Distribution Summary）	クラスタに分散されたデバイスの要約を提供します。たとえば、このレポートは、プライマリ ノード、セカンダリ ノード、ターシャリ ノードなどに関連付けられているデバイスを示します。
Unified CM ディレクトリ URI および GDPR 重複（Unified CM Directory URI and GDPR Duplicates）	システムで重複ユーザディレクトリ URI、学習された Directories URI、学習された数と学習されたパターンの詳細が記載されています。
Unified CM Extension Mobility	Cisco Extension Mobility の使用状況の要約を提供します。たとえば、Cisco Extension Mobility ユーザーがログインしている電話機の数、Cisco Extension Mobility に関連付けられたユーザーなどです。
Unified CM GeoLocation ポリシー（Unified CM GeoLocation Policy）	GeoLocation 論理パーティション ポリシー マトリクスのレコードの一覧を提供します。
Unified CM GeoLocation ポリシーとフィルタ（Unified CM GeoLocation Policy with Filter）	選択した GeoLocation ポリシーに対する、GeoLocation 論理パーティション ポリシー マトリクスのレコードの一覧を提供します。

レポート	説明
電話機に関連付けられていない Unified CM 回線（Unified CM Lines Without Phones）	電話機に関連付けられていない回線の一覧を提供します。
Unified CM 複数回線デバイス（Unified CM Multi-Line Devices）	複数ライン アピアランスを使用する電話機の一覧を提供します。
Unified CM 電話機カテゴリ（Unified CM Phone Category）	ユニバーサル デバイス テンプレートを使用して特定のカテゴリの電話機モデルの一覧を示します。社員のセルフプロビジョニングをイネーブルにすると、各カテゴリのテンプレートを提供することによって、電話機のこれらのカテゴリのいずれか、またはすべてを許可することを選択できます。
Unified CM 電話機能リスト（Unified CM Phone Feature List）	Unified Communications Manager のデバイス タイプごとにサポートされる機能の一覧を提供します。
Unified CM 電話機ロケール インストーラ（Unified CM Phone Locale Installers）	インストールされている電話ロケール パッケージでサポートされる Cisco Unified IP 電話ファームウェア バージョンのリストを提供します。
ロードに不整合が発生した Unified CM 電話機（Unified CM Phones With Mismatched Load）	ファームウェア ロードに不整合が発生したすべての電話機の一覧を提供します。
回線が関連付けられていない Unified CM 電話機（Unified CM Phones Without Lines）	Unified Communications Managerデータベース内の、関連付けられた回線を持たないすべての電話機の一覧を提供します。
Unified CM シェアドライン（Unified CM Shared Lines）	Unified Communications Managerデータベース内の、少なくとも 1 つのシェアドライン アピアランスを使用しているすべての電話機の一覧を提供します。
Unified CM テーブル カウント サマリ（Unified CM Table Count Summary）	データベースを中心にデータを表示します。このレポートは、データベース スキーマを理解している管理者または AXL API 開発者の役に立ちます。
Unified CM ユーザ デバイス カウント（Unified CM User Device Count）	関連するデバイスに関する情報を提供します。たとえば、このレポートは、ユーザーのいない電話機の数、1 つの電話機を持つユーザーの数、複数の電話機を持つユーザーの数を一覧表示します。
プライマリ内線番号を共有している Unified CM ユーザ（Unified CM Users Sharing Primary Extensions）	システムのプライマリ内線番号を共有するユーザーのリストを提供します。

レポート	説明
Unified CM VG2XX ゲートウェイ（Unified CM VG2XX Gateway）	ゲートウェイ エンドポイントのセキュリティ プロファイルの概要を示します。
Unified CM ボイスメール（Unified CM Voice Mail）	Unified Communications Manager Administration のボイスメッセージング関連の設定の要約を提供します。たとえば、このレポートは、設定されたボイスメール ポートの数、メッセージ待機インジケータの数、設定されたボイス メッセージ プロファイルの数、ボイスメッセージプロファイルに関連付けられたディレクトリ番号の数、などを示します。
Unified 内部アクセス レベル マトリックス（Unified Confidential Access Level Matrix）	内部アクセス レベル マトリックスに関するすべての情報が提供されます。

IM and Presence Service レポート

次の表に、Unified Communications Manager で IM and Presence Service をインストールした後に Cisco Unified Reporting に表示されるシステムレポートの種類を示します。

（注） リリース 10.0(1) 以降では、Cisco Unified Communications Manager ノードから IM and Presence クラスタ情報を入手できます。 Cisco Unified Communications Manager から、**[Cisco Unified Reporting]** > **[システムレポート（System Reports）]** > **[Unified CMクラスタの概要（Unified CM Cluster Overview）]** を選択します。

次の表にあるレポートの種類を表示および生成できます。

表 *76 : Cisco Unified Reporting* に表示される *IM and Presence Service* レポート

レポート	説明
IM and Presence データベース複製のデバッグ（IM and Presence Database Replication Debug）	データベース複製のためのデバッグ情報を提供します。 ヒント このレポートを生成すると、CPU の使用率が急増し、生成するのにクラスタ内のサーバごとに最大 10 秒かかる可能性があります。
IM and Presence データベース ステータス（IM and Presence Database Status）	IM and Presence Service データベースのヘルススナップショットを提供します。 アップグレードする前にこのレポートを生成して、データベースが正常であることを確認します。
IM and Presence テーブル カウント サマリ（IM and Presence Table Count Summary）	データベースを中心にデータを表示します。 このレポートは、データベース スキーマを理解している管理者または AXL API 開発者の役に立ちます。

レポート	説明
IM and Presence ユーザセッションレポート（IM and Presence User Sessions Report）	1つまたは複数のデバイスとともにサインインしているアクティブユーザーの一覧を示します。
プレゼンス設定レポート（Presence Configuration Report）	IM and Presence Service ユーザーに関する設定情報を提供します。 • Cisco Unified Communications Manager から同期されたユーザ • IM and Presence Service が有効なユーザー • IM and Presence Service の予定表情報が有効なユーザー ソート可能なカラムのユーザーのリストを表示するには、**[詳細表示（View Details）]** をクリックします。
IM and Presence クラスタの概要（IM and Presence Cluster Overview）	IM and Presence Service クラスタの概要を提供します。 このレポートでは、クラスタにインストールされている IM and Presence Service のバージョン、クラスタ内のすべてのサーバーのホスト名または IP アドレス、ハードウェア詳細情報の要約などを確認できます。
プレゼンス制限警告レポート（Presence Limits Warning Report）	接続またはウォッチャの設定の制限値の最大数を満たしているか、超えてしまったユーザーに関する情報を提供します。 ソート可能なカラムのユーザーのリストを表示するには、**[詳細表示（View Details）]** をクリックします。
プレゼンス使用レポート（Presence Usage Report）	ログインした XMPP クライアントとサードパーティ API の使用情報を提供します。 ソート可能なカラムの XMPP クライアントとサードパーティ API のリストを表示するには、[詳細表示（View Details）]をクリックします。
レポートの説明（Report Descriptions）	表示しているレポートに関するトラブルシューティング情報と詳細情報を提供します。 このレポートでは、レポート、各情報グループ、各データ項目、データ ソース、関連する問題の現象、および対処方法を説明します。

レポートの説明の表示

Cisco Unified Reporting では、レポートのヘルプが用意されています。[レポートの説明（Report Descriptions）] リンクでは、レポート、各情報グループ、各データ項目、データ ソース、関連する問題の現象、および対処方法を説明します。

（注） その他のレポートの問題については、TAC にお問い合わせください。

手順

ステップ 1 [システム レポート（System Reports）]を選択します。

ステップ 2 レポートのリストで [レポートの説明（Report Descriptions）]リンクを選択します。

（注） IM and Presence Service レポートを選択したときに再ログインを要求された場合は、Cisco Unified Communications Manager の管理者ログインクレデンシャルを再入力します。

ステップ 3 [レポートの生成（Generate Report）]アイコンを選択します。

レポートが生成され、表示されます。

新規レポートの作成

新しいレポートを生成して、表示できます。

始める前に

1 台以上のサーバーで Cisco Tomcat サービスが実行されていて、レポートの表示に関してサポートされている Web ブラウザを使用していることを確認します。

レポートを生成するのに非常に時間がかかる場合、またはCPU時間が非常に多くなる場合は、アプリケーションによって通知されます。 レポートの生成中は経過表示バーが表示されます。新しいレポートが表示され、日付と時刻が更新されます。

手順

ステップ 1 メニュー バーから [システム レポート（System Reports）]を選択します。

ステップ 2 レポートを選択します。

（注） IM and Presence Service レポートを選択したときに再ログインを要求された場合は、Cisco Unified Communications Manager の管理者ログインクレデンシャルを再入力します。

ステップ 3 **[レポート（Reports）]** ウィンドウで **[レポートの生成]**（棒グラフ）アイコンを選択します。

ステップ 4 [詳細の表示（View Details）]リンクを選択して、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。

次のタスク

レポートで、項目に対するデータ チェックが失敗したことが示された場合は、[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。 レポートの説明レポートはデータベースから動的に生成されるので、新たに、新規のレポートの説明レポートを生成することもできます。

保存済みレポートの表示

既存のレポートのコピーを表示できます。

（注） Cisco Unified Reporting アプリケーションでは、フレッシュ インストールまたはアップグレード時に最近のレポートのローカル コピーが保存されません。

始める前に

1 台以上のサーバーで Cisco Tomcat サービスが実行されていて、レポートの表示に関してサポートされている Web ブラウザを使用していることを確認します。

手順

ステップ 1 メニュー バーから [システム レポート（System Reports）]を選択します。

ステップ 2 レポート リストから表示するレポートを選択します。

ステップ 3 レポート名のリンクを選択します（日付と時刻が記録されています）。

ステップ 4 [詳細の表示（View Details）]リンクを選択して、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。

次のタスク

新しいレポートまたは保存済みレポートをダウンロードします。

レポートで、項目に対するデータ チェックが失敗したことが示された場合は、[レポートの説明（Report Descriptions）]レポートを選択して、対処方法に関するトラブルシューティング情報を確認します。

新しいレポートのダウンロード

新しいレポートをダウンロードする場合、レポートはローカル ハード ドライブに保存されます。 レポートをダウンロードすると、raw XML データ ファイルがハード ドライブにダウンロードされます。

手順

ステップ 1 新しいレポートを生成します。

ステップ 2 新しいレポートが表示されたら、**[レポート（Reports）]** ウィンドウで **[レポートのダウンロード]**（緑色の矢印）アイコンを選択します。

（注） ドキュメントをダウンロードする前に、[詳細の表示（View Details）]リンクをクリックしてレポートの詳細情報を表示する必要はありません。 データは、ダウンロードしたファイルで検出されます。

ステップ 3 [保存（Save）]を選択して、指定したディスク上の場所にファイルを保存します。

ファイル名またはハードディスク上のファイルの保存場所を変更するには、新しい場所を入力するか、ファイルの名前を変更します（任意）。 ダウンロード中は経過表示バーが表示されます。

ハード ディスクにファイルがダウンロードされます。

ステップ 4 ダウンロードが完了したら、[開く（Open）]を選択して XML レポートを開きます。

（注） XML ファイルの内容を変更しない場合、レポートは画面で正しく表示されない場合があります。

次のタスク

ダウンロードされたレポートファイルをブラウザで表示するには、ファイルをサーバーにアップロードします。

（注） テクニカルサポートを受けるときに、ダウンロードしたファイルを電子メールに添付するか、ファイルを別のサーバーにアップロードできます。

保存済みレポートのダウンロード

保存済みレポートをダウンロードする場合、ダウンロードされたレポートはローカル ハード ドライブに保存されます。 レポートをダウンロードすると、raw XML データ ファイルがハード ディスクにダウンロードされます。

手順

ステップ 1 既存のレポートの詳細情報を開いて、表示します。

ステップ 2 **[レポート（Reports）]**ウィンドウで**[レポートのダウンロード]**（緑色の矢印）アイコンを選択します。

ステップ 3 [保存（Save）]を選択して、指定したディスク上の場所にファイルを保存します。

ファイル名またはハードディスク上のファイルの保存場所を変更するには、新しい場所を入力するか、ファイルの名前を変更します（任意）。ダウンロード中は経過表示バーが表示されます。

ハード ディスクにファイルがダウンロードされます。

ステップ 4 ダウンロードが完了したら、[開く（Open）]を選択して XML レポートを開きます。

（注） XML ファイルの内容を変更しない場合、レポートは正しく表示されない場合があります。

次のタスク

ダウンロードされたレポートファイルをブラウザで表示するには、ファイルをサーバーにアップロードします。

（注） テクニカルサポートを受けるときに、ダウンロードしたファイルを電子メールに添付するか、ファイルを別のサーバーにアップロードできます。

レポートのアップロード

ダウンロードされたレポートをブラウザウィンドウで表示するには、レポートをサーバーにアップロードする必要があります。

始める前に

ハード ドライブにレポートをダウンロードします。

手順

ステップ 1 メニュー バーから [システム レポート（System Reports）]を選択します。

ステップ 2 レポートにアクセスすると、**[レポート（Reports）]** ウィンドウに **[レポートのアップロード]** アイコン（青色の矢印）が表示されます。

ステップ 3 [レポートのアップロード（Upload Report）]アイコンを選択します。

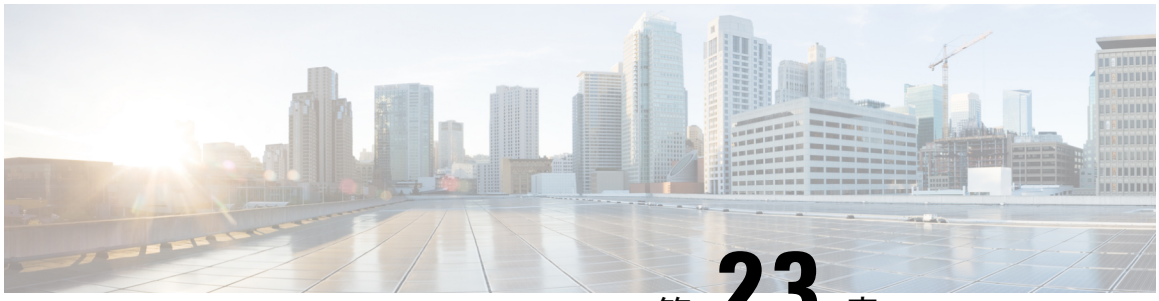
ステップ 4 .xml ファイルの場所を指定するには、[参照（Browse）]を選択して、ハード ドライブ上のファイルの場所に移動します。

ステップ 5 [アップロード（Upload）]を選択します。

ステップ 6 [続行（Continue）]を選択して、アップロードしたファイルをブラウザ ウィンドウに表示します。

次のタスク

アップグレードするときにアップロードしたレポートと新しく生成したレポートを並べて比較できます。



第 23 章

Cisco IP 電話の通話診断と品質レポートを設置する

診断およびレポートの概要

Cisco Unified Communications Manager には、Cisco IP Phone の通話品質を保証するためのオプションが 2 つあります。

- コール診断: コールの診断には、コール管理レコード (CMR) と音声品質メトリックの生成が含まれています。
- 品質報告ツールQRT-QRTはCisco Unified IP電話の音声品質と一般的な問題報告ツールです。 このツールを使用すると、ユーザはIP電話に音声やその他の一般的な問題を簡単に、かつ正確にレポートできます。

コール診断の概要

コール診断を収集するために、SCCP と SIP を実行している Cisco IP 電話を設定することができます。 通話診断には、診断記録とも呼ばれる通話管理記録(CMR)と音声品質指標が含まれる。

音声品質メトリックは、デフォルトで有効になっており、ほとんどの Cisco IP 電話でサポートされています。 Cisco IP 電話は、MOS (平均意見四つ角) 値に基づいて音声品質メトリックを計算します。 音声品質メトリックでは、ノイズや歪みは考慮されません。フレーム損失だけが考慮されます。

CMR レコードには、コールの音声ストリームの品質に関する情報が格納されます。 CMR を生成するように Unified Communications Manager を設定できます。 この情報は、請求レコードの生成やネットワーク分析などの後処理活動に使用できます。

品質レポート ツールの概要

品質レポート ツール（QRT）は、Cisco IP 電話の音声品質と一般的な問題をレポートするツールです。 このツールを使用すると、ユーザはIP電話に音声やその他の一般的な問題を簡単に、かつ正確にレポートできます。

システム管理者は、ユーザの IP 電話に QRT ソフトキーを表示するソフトキー テンプレートを設定して割り当てることで、QRT 機能を有効化できます。 QRT を使用して行うユーザ インタラクションのレベルに応じて、2 つの異なるユーザ モードを選択できます。 次に、システムにおける機能の動作を定義するため、システム パラメータを設定し、Cisco Unified Serviceability ツールを設定します。 QRT Viewer アプリケーションを使用して、電話の問題レポートを作成、カスタマイズ、および表示できます。

ユーザーの IP 電話で問題が発生した場合、ユーザーは、コールの状態がオンフックまたは接続済みのときに Cisco IP 電話の QRT ソフトキーを押すことで、問題のタイプとその他の関連統計をレポートできます。 ユーザは IP 電話で報告されている問題を最もよく表している理由コードを選択できます。 カスタマイズされた電話の問題レポートには、具体的な情報が表示されます。

ユーザが QRT ソフトキーを押して問題の種類を選択すると、QRT はストリーミングの統計情報を収集しようとします。 ストリーミングの統計情報を収集するには、QRT でコールを 5 秒以上アクティブにする必要があります。

詳細なコール レポートおよび課金情報

Cisco CDR Analysis and Reporting（CAR）ツールは、サービス品質、トラフィック、ユーザ コール量、課金情報、ゲートウェイに関する詳細なレポートを生成します。 CAR は、コール詳細レコード（CDR）、コール管理レコード（CMR）、および Unified Communications Manager データベースのデータを使用してレポートを生成します。 CAR インターフェイスには、Cisco Unified Serviceability の [ツール (Tools)]メニューからアクセスできます。

CAR は、サードパーティが提供するコール アカウンティング/課金ソリューションに代わるものではありません。 Cisco Developer Community のホームページで、これらのソリューションを提供する、Cisco Technology Developer Program のメンバ企業を検索できます。

CAR でレポートを設定する方法の詳細については、『*Cisco Unified Communications Manager* のコールレポートおよび課金管理ガイド』を参照してください。

Prerequisites

コール診断の要件

Cisco Unified IP Phone がコール診断をサポートしているかどうかを確認します。

次の表を使用して、電話機がコール診断をサポートしているかどうかを確認します。 コール診断の凡例は、次のようにサポートされています。

- X：SCCP と SIP の両方を実行している電話機によるサポート
- S：SCCP 機能のみ

表 *77*：コール診断のデバイスサポート

Device	コール診断のサポート
Cisco Unified IP Phone 7906	X
Cisco Unified IP 電話 7911	X
Cisco Unified IP Phone 7931	X
Cisco Unified IP 電話 7940	S
Cisco Unified IP 電話 7941	X
Cisco Unified IP Phone 7942-G	X
Cisco Unified IP Phone 7942-G/GE	X
Cisco Unified IP Phone 7945	X
Cisco Unified IP 電話 7960	S
Cisco Unified IP 電話 7961	X
Cisco Unified IP Phone 7962-G	X
Cisco Unified IP Phone 7962-G/GE	X
Cisco Unified IP Phone 7965	X
Cisco Unified IP Phone 7972-G/GE	X
Cisco Unified IP Phone 7975	X

品質レポート ツールの前提条件

Cisco IP 電話の機能：

- ソフトキー テンプレートのサポート
- IP Phone サービスのサポート
- CTI による制御が可能
- 内部 HTTP サーバを含む

詳細については、お使いの電話モデルのガイドを参照してください。

診断とレポートの設定タスク フロー

手順

	コマンドまたはアクション	目的
ステップ 1	コール診断の設定 （369 ページ）	このタスクを実行すると、CMR を生成するように Cisco Unified Communications Manager を設定できます。 CMR レコードには、コールの音声ストリームの品質に関する情報が格納されます。 CDRへのアクセスの詳細については、『*Cisco Unified Communications Manager Call Detail Records* アドミニストレーション ガイド』を参照してください。 音声品質メトリックは、Cisco IP 電話で自動的に有効になります。 音声品質メトリックへのアクセス方法の詳細については、ご使用の電話機モデルの『Cisco Unified IP Phone 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 2	品質レポート ツールの設定 （369 ページ）を行うには、次のサブタスクを実行します。 • QRT ソフトキーのソフトキー テンプレートの設定 （370 ページ） • 共通デバイス設定と QRT ソフトキーテンプレートの関連付け （372 ページ） • 電話機への QRT ソフトキー テンプレートの追加 （373 ページ） • Cisco Unified Serviceability での QRT の設定 （374 ページ） • 品質レポート ツールのサービス パラメータの設定 （377 ページ）	品質レポートツール(QRT) を設定して、IP phone で問題が発生したユーザが、QRT ソフトキーを押すことによって、問題のタイプやその他の関連統計情報をレポートできるようにします。

コール診断の設定

手順

ステップ 1 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 2 [サーバ（Server）]ドロップダウン リストから、Cisco CallManager サービスを実行しているサーバを選択します。

ステップ 3 [サービス（Service）] ドロップダウン リストから、[Cisco CallManager] を選択します。
[サービスパラメータ設定（Service Parameter Configuration）]ウィンドウが表示されます。

ステップ 4 [クラスタ全体のパラメータ（デバイス - 全般）（Clusterwide Parameters (Device - General)）]エリアで、[コール診断有効（Call Diagnostics Enabled）]サービス パラメータを設定します。 次のオプションを使用できます。

- [無効（Disabled）]：CMR は生成されません。
- [CDR有効フラグが True の場合のみ有効化（Enabled Only When CDR Enabled Flag is True）]：[呼詳細レコード（CDR）有効化フラグ（Call Detail Records (CDR) Enabled Flag）] サービス パラメータが True に設定されている場合のみ、CMR が生成されます。
- [CDR 有効化フラグに関係なく有効化（Enabled Regardless of CDR Enabled Flag）]：[CDR 有効化フラグ（CDR Enabled Flag）] サービス パラメータの値に関係なく、CMR が生成されます。

（注） [CDR有効化フラグ（CDR Enabled Flag）] サービス パラメータを有効にせずに CMR を生成すると、制御されずにディスク容量が消費される場合があります。 CMR を有効にする場合は、CDR を有効にすることをお勧めします。

ステップ 5 **[保存（Save）]** をクリックします。

品質レポート ツールの設定

品質レポートツール (QRT) を設定して、IP phone で問題が発生したユーザが、QRT ソフトキーを押すことによって、問題のタイプやその他の関連統計情報をレポートできるようにします。

手順

	コマンドまたはアクション	目的
ステップ 1	QRT ソフトキーのソフトキー テンプレートの設定 （370 ページ）	QRTソフトキーのオンフック状態と接続済みコール状態を設定する必要があります。 次のコール状態も利用できます。 • 接続された会議

	コマンドまたはアクション	目的
		• 接続転送（Connected Transfer）
ステップ 2	（任意） 共通デバイス設定と QRT ソフトキー テンプレートの関連付け （372 ページ）を行うには、次のサブタスクを実行します。 • 共通デバイス設定への QRT ソフトキーテンプレートの追加 （372 ページ） • 電話機と共通デバイス設定の関連付け （373 ページ）	ソフトキー テンプレートを電話で使用できるようにするには、この手順か次の手順のいずれかを実行する必要があります。 システムが [共通デバイス設定（Common Device Configuration）]を使用して設定オプションを電話機に適用する場合は、この手順に従います。 これは、電話機でソフトキー テンプレートを使用できるようにする際に、最も一般的に使用されている方法です。
ステップ 3	（任意） 電話機への QRT ソフトキー テンプレートの追加 （373 ページ）	次の手順は、ソフトキー テンプレートと共通デバイス設定を関連付けるための代替手段として、または共通デバイス設定と共に使用します。 ソフトキー テンプレートを適用して、共通デバイス設定での割り当てや、他のデフォルトのソフトキーの割り当てを上書きする必要がある場合は、次の手順を共通デバイス設定と共に使用します。
ステップ 4	Cisco Unified Serviceability での QRT の設定 （374 ページ）を行うには、次のサブタスクを実行します。 • Cisco Extended Functions サービスの有効化 （375 ページ） • アラームの設定 （375 ページ） • トレースの設定 （376 ページ）	
ステップ 5	（任意） 品質レポート ツールのサービス パラメータの設定 （377 ページ）	

QRT ソフトキーのソフトキー テンプレートの設定

QRTソフトキーのオンフック状態と接続済みコール状態を設定する必要があります。 次のコール状態も利用できます。

- 接続された会議
- 接続転送（Connected Transfer）

手順

ステップ 1 [Cisco Unified CM 管理（Cisco Unified CM Administration）] から、以下を選択します。**[デバイス（Device）] > [デバイスの設定（Device Settings）] > [ソフトキー テンプレート（Softkey Template）]**。

ステップ 2 新しいソフトキーテンプレートを作成するには、この手順を実行します。それ以外の場合は、次のステップに進みます。

a) [新規追加] をクリックします。
b) デフォルトのテンプレートを選択して、[コピー（Copy）]をクリックします。
c) [ソフトキーテンプレート名（Softkey Template Name）]フィールドに、テンプレートの新しい名前を入力します。
d) **[保存]** をクリックします。

ステップ 3 既存のテンプレートにソフトキーを追加するには、次の手順を実行します。

a) [検索（Find）]をクリックして、検索条件を入力します。
b) 必要な既存のテンプレートを選択します。

ステップ 4 [デフォルト ソフトキー テンプレート（Default Softkey Template）]チェックボックスをオンにし、このソフトキーテンプレートをデフォルトのソフトキーテンプレートとして指定します。

（注） あるソフトキー テンプレートをデフォルトのソフトキー テンプレートとして指定した場合、先にデフォルトの指定を解除してからでないと、そのテンプレートは削除することができません。

ステップ 5 右上隅にある **[関連リンク（Related Links）]** ドロップダウンリストから **[ソフトキーレイアウトの設定（Configure Softkey Layout）]** を選択し、**[移動（Go）]** をクリックします。

ステップ 6 [設定するコール状態の選択（Select a Call State to Configure）]ドロップダウン リストから、ソフトキーに表示するコール状態を選択します。

ステップ 7 [選択されていないソフトキー（Unselected Softkeys）]リストから追加するソフトキーを選択し、右矢印をクリックして [選択されたソフトキー（Selected Softkeys）]リストにそのソフトキーを移動します。新しいソフトキーの位置を変更するには、上矢印と下矢印を使用します。

ステップ 8 追加のコール状態でのソフトキーを表示するには、前述のステップを繰り返します。

ステップ 9 **[保存]** をクリックします。

ステップ 10 次のいずれかの作業を実行します。

- すでにデバイスに関連付けられているテンプレートを変更した場合は、[設定の適用（Apply Config）] をクリックしてデバイスを再起動します。
- 新しいソフトキーテンプレートを作成した場合は、そのテンプレートをデバイスに関連付けた後にデバイスを再起動します。詳細については、「共通デバイス設定へのソフトキーテンプレートの追加」と「電話機のセクションとソフトキーテンプレートの関連付け」を参照してください。

次のタスク

次のいずれかの手順を実行します。

- 共通デバイス設定への QRT ソフトキー テンプレートの追加 （372 ページ）
- 電話機への QRT ソフトキー テンプレートの追加 （373 ページ）

共通デバイス設定と QRT ソフトキー テンプレートの関連付け

これはオプションです。 ソフトキーテンプレートを電話機に関連付ける方法は2つあります。

- ソフトキー テンプレートを電話機設定に追加する。
- ソフトキー テンプレートを共通デバイス設定に追加する。

ここに示す手順では、ソフトキーテンプレートを共通デバイス設定に関連付ける方法について説明します。 システムが共通デバイス設定を使用して設定オプションを電話機に適用する場合は、この手順に従ってください。 これは、電話機でソフトキー テンプレートを使用できるようにする際に、最も一般的に使用されている方法です。

別の方法を使用するには、「電話機への QRT ソフトキーテンプレートの追加 （373 ページ）」を参照してください。

手順

	コマンドまたはアクション	目的
ステップ 1	共通デバイス設定への QRT ソフトキー テンプレートの追加 （372 ページ）	
ステップ 2	電話機と共通デバイス設定の関連付け （373 ページ）	

共通デバイス設定への QRT ソフトキー テンプレートの追加

始める前に

QRT ソフトキーのソフトキー テンプレートの設定 （370 ページ）

手順

ステップ 1 [Cisco Unified CM 管理（Cisco Unified CM Administration）] から、以下を選択します。**[デバイス（Device）] > [デバイスの設定（Device Settings）] > [共通デバイス設定（Common Device Configuration）]** を選択します。

ステップ 2 新しい共通デバイス設定を作成し、それにソフトキーテンプレートを関連付けるには、この手順を実行します。それ以外の場合は、次のステップに進みます。

a) [新規追加] をクリックします。

b) [名前（Name）]フィールドに、共通デバイス設定の名前を入力します。

c) **[保存]** をクリックします。

ステップ 3 既存の共通デバイス設定にソフトキーテンプレートを追加するには、次の手順を実行します。

a) [検索（Find）]をクリックして、検索条件を入力します。

b) 既存の共通デバイス設定をクリックします。

ステップ 4 [ソフトキー テンプレート（Softkey Template）]ドロップダウン リストで、使用可能にするソフトキーが含まれているソフトキー テンプレートを選択します。

ステップ 5 **[保存]** をクリックします。

ステップ 6 次のいずれかの作業を実行します。

- すでにデバイスに関連付けられている共通デバイス設定を変更した場合は、[設定の適用（Apply Config）]をクリックしてデバイスを再起動します。
- 新しい共通デバイス設定を作成してその設定をデバイスに関連付けた後に、デバイスを再起動します。

次のタスク

電話機と共通デバイス設定の関連付け （373 ページ）

電話機と共通デバイス設定の関連付け

始める前に

共通デバイス設定への QRT ソフトキー テンプレートの追加 （372 ページ）

手順

ステップ 1 [Cisco Unified CM 管理（Cisco Unified CM Administration）] から、以下を選択します。**[デバイス（Device）] > [電話（Phone）]**。

ステップ 2 **[検索 (Find)]** をクリックし、ソフトキーテンプレートを追加する電話デバイスを選択します。

ステップ 3 [共通デバイス設定（Common Device Configuration）]ドロップダウン リストから、新しいソフトキー テンプレートが含まれている共通デバイス設定を選択します。

ステップ 4 **[保存（Save）]** をクリックします。

ステップ 5 [リセット（Reset）]をクリックして、電話機の設定を更新します。

電話機への QRT ソフトキー テンプレートの追加

始める前に

QRT ソフトキーのソフトキー テンプレートの設定 （370 ページ）

手順

ステップ 1 [Cisco Unified CM 管理（Cisco Unified CM Administration）] から、以下を選択します。**[デバイス（Device）] > [電話（Phone）]**。

ステップ 2 [検索（Find）]をクリックして、設定済みの電話のリストを表示します。

ステップ 3 電話ボタン テンプレートを追加する電話を選択します。

ステップ 4 [電話ボタン テンプレート（Phone Button Template）]ドロップダウン リストで、新しい機能ボタンが含まれる電話ボタン テンプレートを選択します。

ステップ 5 **[保存]** をクリックします。
電話の設定を更新するには[リセット（Reset）]を押すというメッセージ付きのダイアログ ボックスが表示されます。

Cisco Unified Serviceability での QRT の設定

手順

	コマンドまたはアクション	目的
ステップ 1	Cisco Extended Functions サービスの有効化 （375 ページ）	Cisco 拡張ファンクションサービスをアクティブにすると、品質レポートツールなどの音声品質機能がサポートされます。
ステップ 2	アラームの設定 （375 ページ）	QRT のアラームを設定して、SysLog ビュアー内のアプリケーションログのエラーをログに記録します。 この機能は、アラームをログに記録し、アラームの説明と推奨される操作を提供します。 Syslog ビューアにはCisco Unified Real-Time Monitoring Toolからアクセスできます。
ステップ 3	トレースの設定 （376 ページ）	音声アプリケーションのトレース情報をログに記録するように、QRT のトレースを設定します。 QRTのトレースファイルに含める情報を構成したら、Cisco Unifie Rreal-Time監視ツールのトレースとログセンターオプションを使用して、トレースファイルを収集して表示できます。

Cisco Extended Functions サービスの有効化

Cisco 拡張ファンクションサービスをアクティブにすると、品質レポートツールなどの音声品質機能がサポートされます。

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**ドロップダウンリストから、Cisco Extended Functionsサービスを有効にするノードを選択します。

ステップ 3 **Cisco Extended Functions**チェックボックスをオンにします。

ステップ 4 **[保存（Save）]** をクリックします。

次のタスク

アラームの設定 （375 ページ）

アラームの設定

QRT のアラームを設定して、SysLog ビュアー内のアプリケーションログのエラーをログに記録します。 この機能は、アラームをログに記録し、アラームの説明と推奨される操作を提供します。 Syslog ビューアにはCisco Unified Real-Time Monitoring Toolからアクセスできます。

始める前に

Cisco Extended Functions サービスの有効化 （375 ページ）

手順

ステップ 1 Cisco Unified Serviceability で、**アラーム** > **設定** を選択します。

ステップ 2 **サーバ**ドロップダウンリストから、ノードを設定する サーバを選択します。

ステップ 3 **サービスグループ**ドロップダウンリストから、**CMサービス**を選択します。

ステップ 4 **[サービス（Service）]** ドロップダウンリストから、**[Cisco Extended Functions]** を選択します。

ステップ 5 ローカルSyslogsとSDIトレースの両方について**アラームの有効化**チェックボックスをオンにします。

ステップ 6 このドロップダウンリストから、次のいずれかのオプションを選択し、ローカルSyslogsとSDIトレースの両方に アラームイベントレベルを設定します。

- **緊急**：このレベルは、システムが使用不可であることを示します。
- **アラート**：このレベルは、ただちに処置が必要であることを示します。
- **重要**：システムが重要な状態を検出したことを示します。
- **エラー**: エラー条件が検出されたことを示します。

- **警告**：このレベルは、警告状態が検出されたことを示します。
- **注意**: 通常の重要な条件が検出されていることを示します。
- **情報**：情報メッセージのみを示す。
- **デバッグ**：Cisco技術サポートセンター(TAC)エンジニアにデバッグ用の詳細なイベント情報を指示します。

デフォルト値は **エラー（Error）** です。

ステップ 7 **[保存（Save）]** をクリックします。

次のタスク

トレースの設定 （376 ページ）

トレースの設定

音声アプリケーションのトレース情報をログに記録するように、QRT のトレースを設定します。 QRTのトレースファイルに含める情報を構成したら、Cisco Unifie Rreal-Time監視ツールのトレースとログセンターオプションを使用して、トレースファイルを収集して表示できます。

始める前に

アラームの設定 （375 ページ）

手順

ステップ 1 Cisco Unified Serviceability から **トレース** > **設定**を選択します。
ステップ 2 **サーバ**ドロップダウンリストから、トレースを構成するノードを選択します。
ステップ 3 **サービスグループ**ドロップダウンリストから、**CMサービス**を選択します。
ステップ 4 **[サービス（Service）]** ドロップダウンリストから、**[Cisco Extended Functions]** を選択します。
ステップ 5 **トレースオン**チェックボックスをオンにします。
ステップ 6 このドロップダウンリストから、次のいずれかのオプションを選択し、**デバッグトレースレベル**を設定します。

- **エラー**：すべてのエラー状態、およびプロセスとデバイス初期化メッセージを追跡します。
- **特殊**：通常運転中に発生したすべての特殊な条件とサブシステムの状態遷移を追跡します。 コール処理イベントをトレースします。
- **状態遷移**通常の操作中に発生したすべての状態遷移条件とメディア層イベントを追跡します。
- **重要**：すべての重要条件とルーチンの入り口と出口を追跡します。 すべてのサービスがこのトレース レベルを使用するわけではありません。
- **Entry_exit**：すべての入力条件と終了条件、および基礎となるデバッグ情報を追跡します。
- **任意**：すべての条件と詳細なデバッグ情報を追跡します。

- **詳細**：アラート状態とイベントを追跡します。 異常なパスで生成されるすべてのトレースに使用します。 CPU サイクルの最小数を使用します。

デフォルト値は **エラー（Error）** です。

ヒント トラブルシューティングのためには、このセクションにあるすべてのチェックボックスをオンにするようにしてください。

ステップ 7 **[保存（Save）]** をクリックします。

次のタスク

（任意） 品質レポート ツールのサービス パラメータの設定 （377 ページ）

品質レポート ツールのサービス パラメータの設定

注意 Cisco Technical Assistance Center（TAC）の指示があった場合を除き、デフォルトのサービスパラメータ設定の使用をお勧めします。

手順

ステップ 1 Cisco Unified Communications Managerの管理ページで、**システム** > **サービスパラメータ** を選択します。

ステップ 2 QRT アプリケーションが存在するサーバを選択します。

ステップ 3 **Cisco Extended Functions**サービスを選択します。

ステップ 4 サービスパラメータを設定します。 サービス パラメータとその設定オプションの詳細については、「関連項目」セクションを参照してください。

ステップ 5 **[保存（Save）]** をクリックします。

関連トピック

品質レポート ツールのサービス パラメータ （378 ページ）

品質レポート ツールのサービス パラメータ

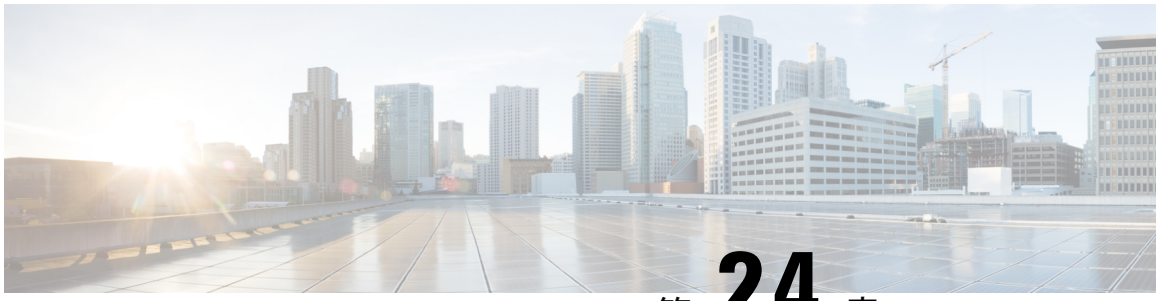
表 *78 :* 品質レポート ツールのサービス パラメータ

パラメータ	説明
拡張 QRT メニューの選択肢を表示する（Display Extended QRT Menu Choices）	拡張メニュー選択項目をユーザに表示するかどうかを決定します。 次のいずれかの設定オプションを選択できます。 • このフィールドを [True] に設定すると、拡張メニュー選択項目が表示されます（対話モード）。 • このフィールドを [False] に設定すると、拡張メニュー選択項目が表示されません（サイレント モード）。 • 推奨するデフォルト値としてFalse（サイレント モード）が設定されています。
ストリーミング統計のポーリング期間（Streaming Statistics Polling Duration）	ストリーミング統計情報のポーリングに使用する間隔を決定します。 次のいずれかの設定オプションを選択できます。 • このフィールドを[-1]に設定すると、コールが終了するまでポーリングが行われます。 • このフィールドを[0]に設定すると、ポーリングはまったく行われません。 • このフィールドを任意の正の値に設定すると、その秒数の間、ポーリングが行われます。 コールが終了すると、ポーリングは停止します。 • 推奨するデフォルトの値として、-1（コールが終了するまでポーリングを行う）が設定されています。
ストリーミング統計のポーリング頻度（秒）（Streaming Statistics Polling Frequency (seconds)）	ポーリング間に待機する秒数を入力します。 この値の範囲は 30 ～ 3600 です。推奨されるデフォルト値は 30 です。

パラメータ	説明
最大ファイル数（Maximum No. of Files）	ファイルカウントを再起動し、古いファイルを上書きする前に、最大ファイル数を入力します。 有効値は 1 ～ 10000 です。推奨されるデフォルト値は 250 です。
1 ファイルあたりの最大回線数（Maximum No. of Lines per File）	各ファイルでの行の最大数を入力します。この数を超えると、次のファイルが始まります。 • 値の範囲は、100 ～ 2000 です。 • 推奨するデフォルトの値として 2000 が設定されています。
CTI Managerに安全に接続するためのCAPFプロファイルインスタンスID（CAPF Profile Instance Id for Secure Connection to CTI Manager）	CTI マネージャへのセキュアな接続を開くために Cisco Extended Function サービスが使用する、アプリケーションユーザ CCMQRTSysUser の CAPF アプリケーション プロファイルのインスタンス ID を入力します。 CTI Manager Connection Security Flag パラメータが有効な場合、このパラメータを設定する必要があります。 （注） CTI Manager Connection Security Flag サービスパラメータを有効にすることで、セキュリティをオンにします。変更を有効にするためには、Cisco Extended Functions サービスを再起動する必要があります。
CTI Manager接続セキュリティフラグ（CTI Manager Connection Security Flag）	Cisco Extended Functions サービスの CTI Manager接続のセキュリティを有効にするか、または無効にするかを選択します。 有効にすると、Cisco Extended Functions はアプリケーション ユーザ CCMQRTSysUser のインスタンス ID に設定された CAPF アプリケーション プロファイルを使用して、CTI マネージャへのセキュアな接続を開きます。 値は True または False を選択します。 CTI へのセキュアな接続を有効にするには、True を選択する必要があります。

第 VI 部

セキュリティの管理



第 24 章

SAML シングル サインオンの管理

SAML シングル サインオンの概要

定義された一連の Cisco アプリケーションのうちの 1 つにサインインした後は、SAML シングル サインオン（SSO）を使用して、それらすべてのアプリケーションにアクセスできます。SAML では、信頼できるビジネス パートナー間で、セキュリティに関連した情報交換を記述します。 これは、ユーザを認証するために、サービス プロバイダー（Cisco Unified Communications Manager など）が使用する認証プロトコルです。 SAML では、ID プロバイダー（IdP）とサービス プロバイダーとの間でセキュリティ認証情報が交換されます。 この機能は、さまざまなアプリケーションにわたり、共通の資格情報と関連情報を使用するための安全な機構を提供します。

SAML SSO は、IdP とサービス プロバイダーの間でのプロビジョニング プロセスの一部として、メタデータと証明書を交換することで、信頼の輪（CoT）を確立します。 サービス プロバイダーは IdP のユーザ情報を信頼して、さまざまなサービスやアプリケーションへのアクセスを許可します。

クライアントは IdP に対する認証を行い、IdP はクライアントにアサーションを与えます。 クライアントはサービス プロバイダーにアサーションを提示します。 CoT が確立されているため、サービス プロバイダーはアサーションを信頼し、クライアントにアクセス権を与えます。

iOS 上での Cisco Jabber の証明書ベースの SSO 認証のオプトイン制御

このリリースの Cisco Unified Communications Manager には、iOS での Cisco Jabber の SSO ログイン動作を ID プロバイダー（IdP）によって制御するためのオプトイン設定オプションが導入

されています。このオプションを使用すると、制御されたモバイルデバイス管理（MDM）環境内で、Cisco Jabber が IdP による証明書ベースの認証を実行できるようになります。

オプトイン制御を設定するには、Cisco Unified Communications Manager で [iOS の SSO ログイン動作（SSO Login Behavior for iOS）] エンタープライズ パラメータを使用します。

（注） このパラメータのデフォルト値を変更する前に、http://www.cisco.com/c/en/us/support/unified-communications/jabber-windows/tsd-products-support-series-home.html で Cisco Jabber 機能のサポートおよびドキュメントを参照して、SSO ログイン動作と証明書ベースの認証に対する iOS 上での Cisco Jabber のサポートを確認してください。

この機能を有効にするには、iOS Cisco Jabber の SSO ログインの動作設定 （386 ページ）の手順を参照してください。

SAML シングル サインオンの前提条件

- Cisco Unified Communications Manager クラスタに DNS が設定されていること
- ID プロバイダー（IdP）サーバ
- IdP サーバによって信頼され、システムでサポートされる LDAP サーバ

SAML SSO 機能のテストは、SAML 2.0 を使用した以下の IdP で行われています。

- OpenAM 10.0.1
- Microsoft® Active Directory® Federation Services 2.0 (AD FS 2.0)
- PingFederate® 6.10.0.4
- F5 BIP-IP 11.6.0

サードパーティ アプリケーションは、次の設定要件を満たす必要があります。

- 必須属性の「uid」が IdP で設定されていること。この属性は、Cisco Unified Communications Manager の LDAP と同期されたユーザ ID に使用されている属性と一致している必要があります。
- SAML SSO に参加するすべてのエンティティのクロックを同期させる必要があります。クロックの同期の詳細については、『*Cisco Unified Communications Manager* システム設定ガイド』（http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html）の「NTP 設定」を参照してください。

SAML シングル サインオンの管理

SAML シングル サインオンの有効化

（注） 同期エージェントの確認テストに合格するまで、SAML SSO を有効にすることができません。

始める前に

- ユーザ データが Unified Communications Manager データベースに同期されていることを確認します。 詳細については、http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html で、『*System Configuration Guide for Cisco Unified Communications Manager*』を参照してください。
- Cisco Unified CM IM and Presence サービスと Cisco Sync Agent サービスのデータ同期が完了していることを確認します。 このテストのステータスをチェックするには、**[Cisco Unified CM IM and Presence Administration]** > **[診断（Diagnostics）]** > **[システム トラブルシュータ（System Troubleshooter）]** を選択します。 「[Sync Agent が関連データ（デバイス、ユーザ、ライセンス情報など）を使用して同期したことを確認する（Verify Sync Agent has sync'ed over relevant data (e.g. devices, users, licensing information）]」 テストは、データ同期が正常に完了した場合にテスト合格の結果が示されています。
- Cisco Unified CM の管理へのアクセスを有効にするには、少なくとも 1 人の LDAP 同期ユーザが Standard CCM Super Users グループに追加されていることを確認します。 詳細については、http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html で、『*System Configuration Guide for Cisco Unified Communications Manager*』を参照してください。
- IdP とサーバ間の信頼関係を設定するには、IdP から信頼メタデータ ファイルを取得し、それをすべてのサーバにインポートする必要があります。

手順

ステップ 1 Cisco Unified CM の管理で、**[システム（System）]** > **[SAML シングル サインオン（SAML Single Sign-On）]** を選択します。

ステップ 2 [SAML SSO の有効化（Enable SAML SSO）]をクリックします。

ステップ 3 すべてのサーバ接続が再起動されることを通知する警告メッセージが表示されたら、[続行（Continue）]をクリックします。

ステップ 4 [参照(Browse)]をクリックし、IdP メタデータ ファイルを探してアップロードします。

ステップ 5 [IdP メタデータのインポート(Import IdP Metadata)]をクリックします。

ステップ 6 [次へ（Next）]をクリックします。

ステップ 7 [信頼メタデータ ファイルセットをダウンロード(Download Trust Metadata Fileset)]をクリックして、サーバのメタデータをシステムにダウンロードします。

ステップ 8 サーバのメタデータを IdP サーバにアップロードします。

ステップ 9 [次へ(Next)]をクリックして続行します。

ステップ 10 有効な管理者 ID のリストから、管理者権限を持つ LDAP 同期ユーザを選択します。

ステップ 11 [テスト実行(Run Test)]をクリックします。

ステップ 12 有効なユーザ名およびパスワードを入力します。

ステップ 13 成功メッセージが表示されたら、ブラウザ ウィンドウを閉じます。

ステップ 14 [完了（Finish）]をクリックし、Web アプリケーションが再起動するまで 1～2 分待ちます。

iOS Cisco Jabber の SSO ログインの動作設定

手順

ステップ 1 Cisco Unified CM Administrationから、**[システム]** > **[企業パラメータ]** を選択します。

ステップ 2 オプトイン制御を設定するには、[SSO の設定（SSO Configuration）] セクションの **[iOS 向け SSO ログイン動作（SSO Login Behavior for iOS）]** パラメータで、**[ネイティブブラウザの使用（Use Native Browser）]** オプションを選択します。

（注） [iOS向けSSOログイン動作（SSO Login Behavior for iOS）]パラメータには次のオプションが含まれます。

- [組み込みブラウザの使用（Use Embedded Browser）]：このオプションを有効にすると、Cisco Jabber は SSO の認証に、組み込みブラウザを使用します。 このオプションにより、バージョン 9 より前の iOS デバイスのネイティブ Apple Safari ブラウザで、クロス起動なしの SSO を使用できるようになります。 このオプションは、デフォルトで有効です。
- [ネイティブブラウザの使用（Use Native Browser）]：このオプションを有効にすると、Cisco Jabber は、iOS デバイスで Apple Safari フレームワークを使用し、MDM の導入で、ID プロバイダー（IdP）を利用する証明書ベースの認証を実行します。

  （注） ネイティブ ブラウザの使用は組み込みブラウザの使用ほど安全ではないため、制御された MDM の導入での利用を除いては、このオプションの設定を推奨しません。

ステップ 3 **[保存（Save）]** をクリックします。

アップグレード後の WebDialer 上での SAML シングル サインオンの有効化

次のタスクに従って、アップグレード後に Cisco WebDialer 上で SAML シングル サインオンを再度アクティブ化します。 SAML シングル サインオンを有効化する前に Cisco WebDialer をアクティブ化すると、デフォルトで、Cisco WebDialer 上で SAML シングル サインオンが有効になりません。

手順

	コマンドまたはアクション	目的
ステップ 1	Cisco WebDialer サービスの非アクティブ化 （387 ページ）	Cisco WebDialer Web サービスがすでにアクティブになっている場合は、それを非アクティブにします。
ステップ 2	SAML シングル サインオンの無効化 （388 ページ）	SAML シングル サインオンがすでに有効になっている場合は、それを無効にします。
ステップ 3	Cisco WebDialer サービスのアクティベーション （388 ページ）	
ステップ 4	SAML シングル サインオンの有効化 （385 ページ）	

Cisco WebDialer サービスの非アクティブ化

Cisco WebDialer Web サービスがすでにアクティブになっている場合は、それを非アクティブにします。

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（Servers）]ドロップダウン リストから、リストされている Cisco Unified Communications Manager サーバを選択します。

ステップ 3 [CTI サービス（CTI Services）]で、[Cisco WebDialer Web サービス（Cisco WebDialer Web Service）]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。

次のタスク

SAML シングル サインオンの無効化 （388 ページ）

SAML シングル サインオンの無効化

SAML シングル サインオンがすでに有効になっている場合は、それを無効にします。

始める前に

Cisco WebDialer サービスの非アクティブ化 （387 ページ）

手順

CLI から、**utils sso disable** コマンドを実行します。

次のタスク

Cisco WebDialer サービスのアクティベーション （388 ページ）

Cisco WebDialer サービスのアクティベーション

始める前に

SAML シングル サインオンの無効化 （388 ページ）

手順

ステップ 1 [Cisco Unified Serviceability] から、以下を選択します。**[ツール（Tools）] > [サービス アクティベーション（Service Activation）]** 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、リストされている Unified Communications Manager サーバを選択します。

ステップ 3 [CTI サービス（CTI Services）]から、[Cisco Webダイヤラー Web サービス（Cisco Webダイヤラー Web Service）]チェック ボックスをオンにします。

ステップ 4 **[保存]** をクリックします。

ステップ 5 [Cisco Unified Serviceability] から、以下を選択します。**[ツール（Tools）] > [コントロール センター - 機能サービス（Control Center - Feature Services）]** を選択して、CTI Manager サービスがアクティブでスタート モードになっていることを確認します。

Webダイヤラー を正しく機能させるには、CTI Manager サービスをアクティブにして、スタート モードにする必要があります。

次のタスク

SAML シングル サインオンの有効化 （385 ページ）

リカバリ URL へのアクセス

トラブルシューティングのために、SAML シングル サインオンをバイパスして、Cisco Unified Communications Manager Administration インターフェイスと Cisco Unified CM IM and Presence サービス インターフェイスにログインする場合に、リカバリ URL を使用します。 たとえば、サーバのドメインまたはホスト名を変更する前に、リカバリ URL を有効にします。 リカバリ URL にログインすると、サーバ メタデータの更新が容易になります。

（注） セルフケアポータルにログインしようとするエンドユーザー（LDAP またはローカル）に対して、復元 URL は機能しません。

始める前に

- 管理権限を持っているアプリケーション ユーザのみがリカバリ URL にアクセスできます。
- SAML SSO が有効になっている場合は、リカバリ URL がデフォルトで有効になります。 CLI からリカバリ URL を有効/無効にすることができます。 リカバリ URL を有効または無効にする CLI コマンドの詳細については、『*Command Line Interface Guide for Cisco Unified Communications Solutions*』を参照してください。

手順

ブラウザで、「`https://hostname:8443/ssosp/local/login`」と入力します。

ドメインまたはホスト名の変更後のサーバ メタデータの更新

ドメインまたはホスト名の変更後は、この手順を実行するまで、SAML シングル サインオンが機能しません。

（注） この手順を実行しても [SAML シングル サインオン（SAML Single Sign-On）]ウィンドウ にログインできない場合は、ブラウザのキャッシュをクリアしてもう一度ログインしてみてください。

始める前に

リカバリ URL が無効になっている場合、シングル サインオン リンクをバイパスするようには表示されません。 リカバリ URL を有効にするには、CLI にログインして次のコマンドを実行します：**utils sso recovery-url enable**。

手順

ステップ 1 Web ブラウザのアドレス バーに次の URL を入力します。

`https://<Unified CM-server-name>`

`<Unified CM-server-name>` は、サーバのホスト名、または IP アドレスです。

ステップ 2 [シングル サインオンをバイパスするリカバリURL（Recovery URL to bypass Single Sign-On (SSO)）] をクリックします。

ステップ 3 管理者ロールを持つアプリケーションユーザのクレデンシャルを入力し、[ログイン（Login）] をクリックします。

ステップ 4 Cisco Unified CM の管理で、**[システム（System）]** > **[SAML シングル サインオン（SAML Single Sign-On）]** を選択します。

ステップ 5 [メタデータのエクスポート（Export Metadata）] をクリックしてサーバ メタデータをダウンロードします。

ステップ 6 サーバ メタデータ ファイルを IdP にアップロードします。

ステップ 7 [テスト実行(Run Test)]をクリックします。

ステップ 8 有効なユーザ ID とパスワードを入力します。

ステップ 9 成功のメッセージが表示されたら、ブラウザウィンドウを閉じます。

サーバーの削除後のサーバーメタデータの更新

クラスタ全体で SSO を統合している場合は、サーバをクラスタから削除した際に、インデックスが IdP と一致しなくなるのを防ぐために、メタデータを必ずインポートし直す必要があります。

始める前に

（注） リカバリ URL が無効になっている場合、シングル サインオン リンクをバイパスするようには表示されません。 リカバリ URL を有効にするには、CLI にログインして次のコマンドを実行します：**utils sso recovery-url enable**。

手順

ステップ 1 Web ブラウザのアドレス バーに次の URL を入力します。

`https://<Unified CM-server-name>`

`<Unified CM-server-name>` は、サーバのホスト名、または IP アドレスです。

ステップ 2 [シングル サインオンをバイパスするリカバリURL（Recovery URL to bypass Single Sign-On (SSO)）] をクリックします。

ステップ 3 管理者ロールを持つアプリケーションユーザのクレデンシャルを入力し、[ログイン（Login）] をクリックします。

ステップ 4 Cisco Unified CM の管理で、**[システム（System）]** > **[SAML シングルサインオン（SAML Single Sign-On）]** を選択します。

ステップ 5 [メタデータのエクスポート（Export Metadata）] をクリックしてサーバ メタデータをダウンロードします。

ステップ 6 サーバ メタデータ ファイルを IdP にアップロードします。

ステップ 7 [テスト実行(Run Test)]をクリックします。

ステップ 8 有効なユーザ ID とパスワードを入力します。

ステップ 9 成功のメッセージが表示されたら、ブラウザウィンドウを閉じます。

サーバ メタデータの手動プロビジョニング

IDプロバイダーで複数のUCアプリケーション用の単一接続をプロビジョニングするには、IDプロバイダーとサービス プロバイダー間の信頼の輪を設定しながら、サーバ メタデータを手動でプロビジョニングする必要があります。 信頼の輪の設定方法については、IdP 製品のマニュアルを参照してください。

一般的な URL 構文は次のとおりです。

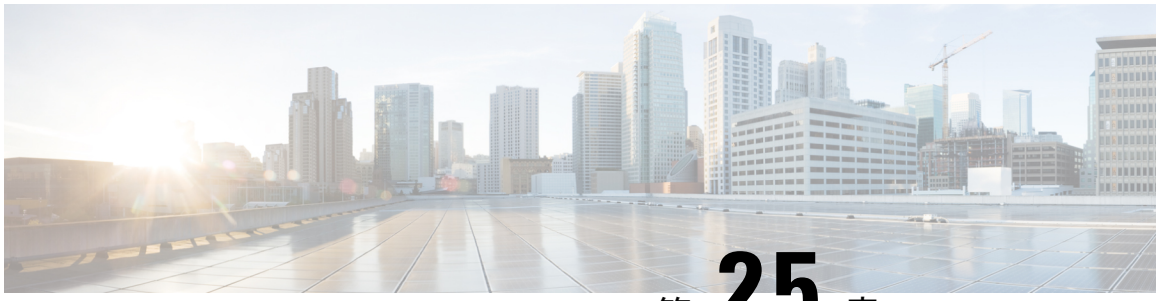
```
https://<SP FQDN>:8443/ssosp/saml/SSO/alias/<SP FQDN>
```

手順

サーバ メタデータを手動でプロビジョニングするには、Assertion Customer Service（ACS）URL を使用します。

例：

ACS URL の例:
```
<md:AssertionConsumerService
Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://cucm.ucsso.cisco.com:8443/ssosp/saml/SSO/alias/cucm.ucsso.cisco.com"
index="0"/>
```



第 25 章

証明書の管理

証明書の概要

システムでは、自己署名証明書とサードパーティの署名付き証明書が使用されます。送信元から宛先までのデータ整合性を確保するために、デバイスのセキュア認証、データの暗号化、データのハッシュを行う際に、システム内のデバイス間で証明書を使用します。証明書を使用することにより、帯域幅、通信、操作のセキュアな転送が可能になります。

証明書を使用する際、意図した Web サイト、電話、FTP サーバなどのエンティティとの間でデータがどのように暗号化され共有されているかを理解し、それを定義することが最も重要な部分です。

システムが証明書を信頼するということは、システムにプレインストールされている証明書によって、適切な接続先と情報を共有していることが完全に確信されているということです。そうでない場合、システムはこれらのポイント間の通信を終了します。

証明書を信頼するには、サードパーティ認証局（CA）によって信頼がすでに確立されている必要があります。

まずデバイスが CA 証明書と中間証明書の両方を信頼できると認識していることが必要であり、そうであるならデバイスはSecure Socket Layer（SSL）ハンドシェイクというメッセージの交換によって提供されるサーバ証明書を信頼することができます。

（注） Tomcat 用の EC ベースの証明書がサポートされています。 この新しい証明書を tomcat-ECDSA といいます。 詳細については、『*Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager*』の「Enhanced TLS Encryption on IM and Presence Service」の章を参照してください。

Tomcat インターフェイスの EC 暗号はデフォルトで無効になっています。 Cisco Unified Communications Manager または IM and Presence Service で [HTTPS 暗号（HTTPS Ciphers）]のエンタープライズ パラメータを使用して、これらを有効にできます。 このパラメータを変更すると、すべてのノードで Cisco Tomcat サービスを再起動する必要があります。

EC ベースの証明書の詳細については、Cisco Unified Communications Manager and IM and Presence Service リリース ノートの「ECDSA Support for Common Criteria for Certified Solutions」を参照してください。

サードパーティの署名付き証明書または証明書チェーン

アプリケーション証明書に署名した認証局の認証局ルート証明書をアップロードします。 下位認証局がアプリケーション証明書に署名した場合は、下位認証局の認証局ルート証明書をアップロードする必要があります。 すべての認証局証明書の PKCS#7 形式の証明書チェーンもアップロードできます。

認証局ルート証明書およびアプリケーション証明書は、同じ [証明書のアップロード（Upload Certificate）] ダイアログボックスを使用してアップロードできます。 認証局ルート証明書または認証局証明書だけが含まれる証明書チェーンをアップロードする場合は、certificate type-trust 形式の証明書名を選択します。 アプリケーション証明書またはアプリケーション証明書と認証局証明書が含まれる証明書チェーンをアップロードする場合は、証明書タイプだけが含まれている証明書名を選択します。

たとえば、Tomcat 認証局証明書または認証局証明書チェーンをアップロードする場合は [tomcat-trust] を選択します。Tomcat アプリケーション証明書またはアプリケーション証明書と認証局証明書が含まれる証明書チェーンをアップロードする場合は、[tomcat] または [tomcat-ECDSA] を選択します。

CAPF 認証局ルート証明書をアップロードすると、CallManager の信頼ストアにコピーされるため、認証局ルート証明書を個別に CallManager にアップロードする必要はありません。

（注） サードパーティの認証局署名付き証明書が正常にアップロードされると、署名付き証明書を取得するために使用された、最近生成した CSR が削除され、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。

（注） tomcat-trust、CallManager-trust、およびPhone-SAST-trust証明書がクラスタの各ノードに自動的にレプリケートされます。

（注） DirSyncサービスをセキュア モードで実行する場合に必要となるディレクトリの信頼証明書は、tomcat-trustにアップロードすることができます。

サードパーティ認証局証明書

サードパーティ認証局が発行するアプリケーション証明書を使用するには、署名付きのアプリケーション証明書と認証局ルート証明書の両方を認証局から取得するか、アプリケーション証明書と認証局証明書の両方が含まれているPKCS#7証明書チェーン（Distinguished Encoding Rules [DER]）から取得する必要があります。 これらの証明書の取得に関する情報は、認証局から入手してください。 証明書を取得するプロセスは、認証局によって異なります。 署名アルゴリズムではRSA暗号化が使用されている必要があります。

Cisco Unified Communicationsオペレーティング システムでは、プライバシー強化メール（PEM）エンコード形式でCSRが作成されます。 システムは、DERおよびPEMエンコード形式の証明書と、PEM形式のPKCS#7証明書チェーンを受け入れます。 認証局プロキシ機能（CAPF）以外のすべての証明書タイプの場合、それぞれのノードについて認証局ルート証明書およびアプリケーション証明書を取得してアップロードする必要があります。

CAPFの場合、最初のノードについてのみ認証局ルート証明書およびアプリケーション証明書を取得してアップロードします。 CAPFおよびUnified Communications ManagerのCSRには、認証局へのアプリケーション証明書要求に含める必要のある拡張情報が含まれています。 認証局が拡張要求メカニズムをサポートしていない場合は、次の手順に従ってX.509拡張を有効にする必要があります。

- CAPF CSRでは、次の拡張情報が使用されます。

```
X509v3 拡張キーの使用： TLS Web サーバ認証、X509v3 キーの使用： デジタル署名、証明書署名
```

- TomcatおよびTomcat-ECDSAのCSRでは、次の拡張情報が使用されます。

（注） TomcatまたはTomcat-ECDSAは、キーアグリーメントやIPsecエンドシステムキーを使用する必要はありません。

```
X509v3 拡張キー使用：TLS Web サーバ認証、TLS Web クライアント認証、IPSec エンド システム X509v3 キー使用：デジタル署名、キー暗号化、データ暗号化、キー同意
```

- IPsec の CSR では、次の拡張情報が使用されます。

```
X509v3 拡張キー使用：TLS Web サーバ認証、TLS Web クライアント認証、IPSec エンド システム X509v3 キー使用：デジタル署名、キー暗号化、データ暗号化、キー同意
```

- Unified Communications Manager の CSR では、次の拡張情報が使用されます。

```
X509v3 拡張キー使用：TLS Web サーバ認証、TLS Web クライアント認証 X509v3 キー使用：デジタル署名、キー暗号化、データ暗号化、キー同意
```

- IM and Presence Service cup および cup-xmpp 証明書の CSR は、次の拡張機能を使用します。

```
X509v3 拡張キー使用：TLS Web サーバ認証、TLS Web クライアント認証、IPSec エンド システム X509v3 キー使用：デジタル署名、キー暗号化、データ暗号化、キー同意
```

（注） 使用する証明書に対してCSRを生成し、SHA256署名を使用してサードパーティ認証局に署名させることもできます。 この署名付き証明書を Unified Communications Manager に再度アップロードすることで、Tomcat および他の証明書が SHA256 をサポートできるようになります。

証明書署名要求のキー用途拡張

次の表に、Unified Communications Manager と IM and Presence Service の CA 証明書の両方に対する証明書署名要求（CSR）の主な使用法の拡張を示します。

表 *79 : Cisco Unified Communications Manager CSR* キー鍵用途拡張

	マルチサーバー	拡張キーの使用状況			キーの使用法				
		サーバ認証 (1.3.6.1.5.5.7.3.1)	クライアント認証 (1.3.6.1.5.5.7.3.2)	IP セキュリティ末端システム (1.3.6.1.5.5.7.3.5)	デジタル署名	鍵の暗号化	データの暗号化	鍵証明書サイン	鍵共有
CallManager CallManager-ECDSA	Y	Y	Y		Y	N	Y		
CAPF（パブリッシャーのみ）	N	Y	N		Y	N		Y	
ipsec	N	Y	Y	Y	Y	Y	Y		
tomcat tomcat-ECDSA	Y	Y	Y		Y	N	Y		
TVS	N	Y	Y		Y	Y	Y		

表 *80 : IM and Presence* サービスの *CSR* キーの用途の拡張

	マルチサーバー	拡張キーの使用状況			キーの使用法				
		サーバ認証 (1.3.6.1.5.5.7.3.1)	クライアント認証 (1.3.6.1.5.5.7.3.2)	IP セキュリティ末端システム (1.3.6.1.5.5.7.3.5)	デジタル署名	鍵の暗号化	データの暗号化	鍵証明書サイン	鍵共有
cup cup-ECDSA	N	Y	Y	Y	Y	Y	Y		
cup-xmpp cup-xmpp-ECDSA	Y	Y	Y	Y	Y	Y	Y		
cup-xmpp-s2s cup-xmpp-s2s-ECDSA	Y	Y	Y	Y	Y	Y	Y		
ipsec	N	Y	Y	Y	Y	Y	Y		
tomcat tomcat-ECDSA	Y	Y	Y		Y	Y	Y		

（注） 「データの暗号化」ビットは、CA 署名証明書の処理中に変更も削除もされません。

証明書の表示

[証明書リスト] ページのフィルタ オプションを使用して、共通名、有効期限日付、キー タイプ、および使用方法に基づいて証明書のリストを並べ替えて表示できます。 このため、フィルタ オプションを使用すると、データの並べ替え、表示、およびデータの効率的な管理を行えます。

Unified Communications Manager リリース 14 から、使用オプションを選択して、ID または信頼証明書のリストを並べ替え、表示できます。

手順

ステップ 1 Cisco Unified OS の管理から、**[セキュリティ（Security）][証明書の管理（Certificate Management）]** を選択します。
[Certificate List] ページが表示されます。

ステップ 2 **[証明書リストの検索場所]** ドロップダウン リストから、必要なフィルタ オプションを選択し、**[検索]** フィールドに検索項目を入力して **[検索]** ボタンをクリックします。

たとえば、アイデンティティ証明書だけを表示するには、**[証明書の一覧の検索条件（Find Certificate List where）]** ドロップダウンリストから **[使用法（Usage）]** を選択し、**[検索（Find）]** フィールドにアイデンティティを入力して、**[検索（Find）]** ボタンをクリックします。

BCFIPS プロバイダーの証明書表示データは、リリース 14SU2 以降で変更されました。

14SU1 までのタグ名	**14SU2 からのタグ名**
発行者名	IssuerDN（発行者 DN）
有効期限	開始日
移行後	最終日
サブジェクト名	SubjectDN（サブジェクト DN）
キー	[パブリックキー(Public Key)]
キー値	モジュラス

（注） x509 拡張機能は、実際のキー使用法名ではなく OID 名で表示されます。

証明書のダウンロード

CSR リクエストを送信する際、ダウンロード証明書タスクを使用して証明書のコピーを作成するか、証明書をアップロードします。

手順

ステップ 1 Cisco Unified OS の管理から、**[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 検索情報を指定し、**[検索（Find）]** をクリックします。

ステップ 3 必要なファイル名を選択し、**[ダウンロード]** をクリックします。

中間証明書のインストール

中間証明書をインストールするには、まずルート証明書をインストールしてから、署名付き証明書をアップロードする必要があります。 この手順は、認証局から 1 つの署名付き証明書と複数の証明書が証明書チェーンで提供されている場合にのみ必要です。

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）]** をクリックします。

ステップ 2 **[証明書/証明書チェーンのアップロード]** をクリックします。

ステップ 3 **[証明書の用途]** ドロップダウンリストで適切な信頼ストアを選択して、ルート証明書をインストールします。

ステップ 4 選択した証明書の説明を入力します。

ステップ 5 次のいずれかの手順を実行して、アップロードするファイルを選択します。

- [ファイルのアップロード（Upload File）]テキスト ボックスに、ファイルへのパスを入力します。
- [参照（Browse）]をクリックしてファイルに移動し、[開く（Open）]をクリックします。

ステップ 6 [アップロード（Upload）]をクリックします。

ステップ 7 顧客証明書をインストールしたら、FQDN を使用して Cisco Unified Intelligence Center の URL にアクセスします。 IP アドレスを使用して Cisco Unified Intelligence Center にアクセスすると、カスタム証明書を正常にインストールした後でも「ここをクリックしてログインを継続します（Click here to continue）」のメッセージが表示されます。

（注） • TFTP Tomcat 証明書をアップロードするときは、TFTP サービスを再起動する必要があります。 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。

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。
- 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

証明書が期限切れになる前に、証明書を再生成することを推奨します。 RTMT（Syslog Viewer）で警告が発行され、証明書の期限が近くなると電子メールで通知が送信されます。

ただし、期限切れの証明書を再生成することもできます。 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、営業時間後にこのタスクを実行します。 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。

⚠

注意 証明書を再生成すると、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） 証明書を再生成した場合、**[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 [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 （401 ページ）を参照してください。

ステップ 5 CAPF、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。

重要 CallManager、CAPF、TVS 証明書の再生成/更新後に、更新された ITL ファイル を受信するために、電話機は自動的にリセットされます。

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 *81* : 証明書の名前と説明

名前	説明	再起動が必要なサービス
tomcat tomcat-ECDSA	この証明書は、SIP Oauth モードが有効になっているときに 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） 以下に記載されている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）ローカルサービスおよびマスターサービス、Cisco UDS Tomcat、および Cisco AXL Tomcat Web 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、ユニファイドコミュニケーション マネージャ、MGCP、H.323、IM およびプレゼンス 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	再起動が必要なサービス
CallManager CallManager-ECDSA	これはSIP、SIP トランク、SCCP、TFTP などに使用されます。	重要　リリース 14 では、次のサービスを再起動します。 • Cisco Call Manager Service およびその他の関連サービス（Cisco CTI Manager、HAProxy Service など）- サーバーがセキュアモードの場合、CTL ファイルを更新します。 重要　以下に記載されている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 - サーバーがセキュアモードの場合、CTL ファイルを更新します。 • CallManager-ECDSA：Cisco CallManager サービスおよび HAProxy サービス。
CAPF	Unified Communications Manager Publisherで実行されている CAPF サービスによって使用されます。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 (オンラインとオフラインの CAPF モードを除く)。	該当なし
TVS	これはTrust検証サービスで使用されます。これは、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）

- TVS、CAPF、またはTFTP証明書のいずれかを更新した場合に、手動または自動で電話機をリセットするには、証明書の更新に関する新しいエンタープライズパラメータの電話機の相互操作を導入します。 このパラメータは、デフォルトで電話機を自動的にリセットするために設定されています。
- 証明書の再生成、削除、更新後に、「再起動するサービス」の列で説明されているサービスを必ず再起動してください。

重要 この注意事項は、リリース 14SU2 以降に適用されます。

CLI 経由の複数 SAN 証明書のアップロードはサポートしていません。 これらの証明書は、常に OS 管理 GUI 経由でアップロードする必要があります。

OAuth 更新ログイン用のキーの再生成

コマンドラインインターフェイスを使用して暗号キーと署名キーの両方を再生成するには、この手順を使用します。 Cisco Jabber が Unified Communications Manager との OAuth 認証に使用する暗号キーまたは署名キーが侵害された場合にのみ、この作業を実行します。 署名キーは非対称で RSA ベースであるのに対し、暗号キーは対称キーです。

このタスクを完了すると、これらのキーを使用する現在のアクセストークンと更新トークンは無効になります。

エンドユーザへの影響を最小限に抑えるために、このタスクは営業時間外に完了することを推奨します。

暗号キーは、以下の CLI を使用してのみ再生成できますが、発行元の Cisco Unified OS の管理 GUI を使用して署名キーを再生成することもできます。 **[セキュリティ]** > **[証明書の管理]** を選択し、**AUTHZ** 証明書を選択して、**[再作成]** をクリックします。

手順

ステップ 1 Unified Communications Manager発行元ノードで**コマンドライン**インターフェイスにログインします。

ステップ 2 暗号キーを再生成するには、次の手順を実行します。

a) `set key regen authz encryption` コマンドを実行します。
b) 「`yes`」と入力します。

ステップ 3 署名キーを再生成するには、次の手順を実行します。

a) `set key regen authz signing` コマンドを実行します。
b) 「`yes`」と入力します。

Unified Communications Manager パブリッシャ ノードがキーを再生成し、IM and Presence サービスのローカル ノードを含めたすべての Unified Communications Manager クラスタ ノードに新しいキーを複製します。

すべての UC クラスタで新しいキーを再生成して同期する必要があります。

- IM and Presence 中央クラスタ：IM and Presence 集中型展開の場合、IM and Presence ノードはテレフォニーとは別のクラスタ上で実行されています。 この場合、IM and Presence Service の中央クラスタの Unified Communications Manager パブリッシャ ノードで、この手順を繰り返します。
- Cisco Expressway または Cisco Unity Connection：これらのクラスタ上でもキーを再生成します。 詳細については、Cisco Expressway および Cisco Unity Connection のマニュアルを参照してください。

（注） 次のシナリオでは、Cisco XCP 認証サービスを再起動する必要があります。

- 認定証明書を再作成する場合
- IM and Presence 管理者コンソールで中央集中型導入に新しくエントリを作成する場合

証明書または証明書チェーンのアップロード

システムで信頼する新しい証明書または証明書チェーンをアップロードします。

手順

ステップ 1 Cisco Unified OS の管理から、**[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/証明書チェーンのアップロード]** をクリックします。

ステップ 3 [証明書の用途（Certificate Purpose）] ドロップダウン リストで、証明書名を選択します。

ステップ 4 次のいずれかの手順を実行して、アップロードするファイルを選択します。

- [ファイルのアップロード（Upload File）]テキスト ボックスに、ファイルへのパスを入力します。
- [参照（Browse）]をクリックしてファイルに移動してから、[開く（Open）]をクリックします。

ステップ 5 ファイルをサーバにアップロードするには、[ファイルのアップロード（Upload File）]をクリックします。

（注） 証明書をアップロードしたら、影響を受けるサービスを再起動します。 サーバが再起動したら、CCMAdmin または CCMUser GUI にアクセスして、新しく追加した証明書が使用されていることを確認できます。

サードパーティ証明書の認証局の管理

このタスク フローでは、サードパーティ証明書プロセスの概要を、各ステップへの参照とともに順番に説明します。 お使いのシステムは、サードパーティ認証局が PKCS＃10 証明書署名要求（CSR）を使用して発行する証明書をサポートしています。

手順

	コマンドまたはアクション	目的
ステップ 1	証明書署名要求の生成 （407 ページ）	証明書署名要求（CSR）を生成します。これは、公開キー、組織名、共通名、地域、および国などの証明書申請情報を含む暗号化されたテキストのブロックです。 認証局はこの CSR を使用して、ご使用のシステムの信頼できる証明書を生成します。
ステップ 2	証明書署名要求のダウンロード （407 ページ）	CSR を作成後、ダウンロードして、認証局に証明書を送信できるようにします。
ステップ 3	認証局のドキュメントを参照してください。	認証局からアプリケーション証明書を取得します。
ステップ 4	認証局のドキュメントを参照してください。	認証局からルート証明書を取得します。
ステップ 5	信頼ストアへの認証局署名済み CAPF ルート証明書の追加 （408 ページ）	ルート証明書を信頼ストアに追加します。 認証局の署名付き CAPF 証明書を使用している場合は、この手順を実行します。
ステップ 6	証明書または証明書チェーンのアップロード （405 ページ）	認証局ルート証明書をノードにアップロードします。
ステップ 7	CAPF または Cisco Unified Communications Manager の証明書を更新した場合は、新しい CTL ファイルを生成します。	『*Cisco Unified Communications Manager Security Guide*』（http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/

	コマンドまたはアクション	目的
		products-maintenance-guides-list.html）を参照してください。 サードパーティの署名付きCAPFまたはCallManager証明書をアップロードしたら、CTLクライアント（設定している場合）を再実行します。
ステップ8	サービスの再起動 （408ページ）	新しい証明書の影響を受けるサービスを再起動します。 すべての証明書タイプで、対応するサービスを再起動します（たとえば、Tomcatまたは Tomcat-ECDSAの証明書を更新した場合はCisco Tomcatサービスを再起動します）。

証明書署名要求の生成

証明書署名要求（CSR）を生成します。これは、公開キー、組織名、共通名、地域、および国などの証明書申請情報を含む暗号化されたテキストのブロックです。 認証局はこのCSRを使用して、ご使用のシステムの信頼できる証明書を生成します。

（注） 新しいCSRを生成すると、既存のCSRは上書きされます。

手順

ステップ1 Cisco Unified OSの管理から、**[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 [CSRの作成（Generate CSR）]をクリックします。

ステップ3 **[証明書署名要求の作成]** 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4 [Generate]をクリックします。

証明書署名要求のダウンロード

CSRを作成後、ダウンロードして、認証局に証明書を送信できるようにします。

手順

ステップ 1 Cisco Unified OS の管理から、**[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 [CSR のダウンロード（Download CSR）]をクリックします。

ステップ 3 [証明書の用途（Certificate Purpose）]ドロップダウン リストで、証明書名を選択します。

ステップ 4 [CSR のダウンロード（Download CSR）]をクリックします。

ステップ 5 （任意） プロンプトが表示されたら、[保存（Save）]をクリックします。

信頼ストアへの認証局署名済み CAPF ルート証明書の追加

認証局が署名した CAPF 証明書を使用する場合は、ルート証明書をUnified Communications Manager信頼ストアに追加します。

手順

ステップ 1 Cisco Unified OS の管理から、**[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/証明書チェーンのアップロード]** をクリックします。

ステップ 3 **[証明書/証明書チェーンのアップロード]** ポップアップ ウィンドウで、**[証明書の用途]** ドロップダウン リストから **[CallManager の信頼性]** を選択し、認証局署名済み CAPF ルート証明書を参照します。

ステップ 4 **[ファイルのアップロード]** フィールドに証明書が表示されたら、**[アップロード]** をクリックします。

サービスの再起動

クラスタ内の特定のノードで機能またはネットワーク サービスを再起動する必要がある場合は、次の手順に従います。

手順

ステップ 1 再起動するサービスのタイプに応じて、次のいずれかのタスクを実行します。

- **[ツール（Tool）] > > [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。
- **[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システム ノードを選択し、[移動（Go）]をクリックします。

ステップ 3 再起動するサービスの横にあるオプション ボタンをクリックし、[再起動（Restart）]をクリックします。

ステップ 4 再起動にはしばらく時間がかかることを示すメッセージが表示されたら、[OK]をクリックします。

オンライン証明書ステータス プロトコル（OCSP）による証明書失効（CRL）

Unified Communications Manager は、証明書失効をモニタリングするための OCSP をプロビジョニングします。 スケジュールされた間隔、および証明書がアップロードされるたびにシステムが証明書のステータスをチェックし、有効性を確認します。

オンライン証明書状態プロトコル（OCSP）は、管理者がシステムの証明書要件を管理するのに役立ちます。 OCSP を設定すると、証明書の有効性を確認したり期限切れの証明書をリアルタイムで無効化するための、シンプルかつ安全な自動メソッドを使用できます。

コモンクライテリア モードが有効になっている FIPS 展開の場合、OCSP はシステムのコモンクライテリア要件への準拠にも役立ちます。

有効性検査

Unified Communications Manager は、証明書のステータスを確認し、有効性を確認します。

証明書の検証は、次のように行われます。

- Unified Communications Manager は代理信頼モデル（DTM）を使用し、OCSP 署名属性のルート CA または中間 CA をチェックします。 ルート CA または中間 CA は、ステータスを確認するために OCSP 証明書に署名する必要があります。 委任された信頼モデルが失敗すると、Unified Communications Manager が応答側の信頼モデル（TRP）にフォールバックし、指定された OCSP 応答の署名証明書を OCSP サーバから使用して証明書を検証します。

（注） 証明書の失効ステータスを確認するために、OCSP レスポンダが実行されている必要があります。

- **[証明書失効（Certificate Revocation）]** ウィンドウで OCSP オプションを有効にすると、最も安全な方法でリアルタイムに証明書失効をチェックすることができます。 オプションから、証明書の OCSP URI を使用するか、または設定済みの OCSP URI を使用するかを選択します。 OCSP の手動設定の詳細については、「OCSP による証明書失効の設定」を参照してください。

（注） リーフ証明書の場合、syslog、FileBeat、SIP、ILS、LBM などの TLS クライアントは、OCSP 要求を OCSP レスポンダに送信し、OCSP レスポンダからリアルタイムで証明書失効応答を受信します。

コモンクライテリアモードを有効にした状態で検証が実行されると、証明書に対して次のいずれかのステータスが返されます。

- **[良好（Good）]**：**良好**な状態とは、ステータスの問い合わせへの肯定的な応答を示します。この肯定的な応答は、少なくとも証明書が失効していないことを示しますが、必ずしもその証明書が発行済みであること、または、その応答が生成された時刻が証明書の有効期間内にあることを意味するものではありません。レスポンダが作成したアサーションに加えて、発行や有効性の肯定的なステートメントなど、レスポンダが作成した証明書のステータスに関する追加情報を伝送するためには、応答拡張を使用できます。
- **[失効（Revoked）]**：**失効** 状態とは、証明書が失効している（恒久的または一時的に保留されている）ことを示します。
- **[不明（Unknown）]**：**不明**状態とは、OCSP レスポンダが要求された証明書を認識していないことを示します。

（注） コモンクライテリアモードでは、**失効**と**不明**の両方の場合において接続に失敗しますが、コモンクライテリアモードが有効になっていない状態では応答が**不明**ステータスである場合、接続に成功します。

証明書モニタリング タスク フロー

次のタスクを行い、証明書ステータスと有効期限を自動的にモニタするようシステムを設定します。

- 証明書の有効期限が近づいているときは、電子メールで通知する
- 有効期限が切れた証明書を失効させる

手順

	コマンドまたはアクション	目的
ステップ 1	証明書モニタ通知の設定（411 ページ）	証明書の自動モニタリングを構成します。システムは定期的に証明書ステータスをチェックし、証明書の有効期限が

	コマンドまたはアクション	目的
		近づいていると電子メールで通知します。
ステップ 2	OCSP による証明書失効の設定 （412 ページ）	期限切れの証明書が自動的に失効するように OCSP を設定します。

証明書モニタ通知の設定

Unified Communications Manager または IM and Presence サービスの自動証明書モニタリングを設定します。 システムは定期的に証明書のステータスをチェックし、証明書の有効期限が近づいていると電子メールで通知します。

（注） [Cisco Certificate Expiry Monitor] ネットワーク サービスを実行している必要があります。 デフォルトでこのサービスは有効化されていますが、**[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、[Cisco Certificate Expiry Monitor サービス（Cisco Certificate Expiry Monitor Service）] の状態が [実行中（Running）] であることを検証して Cisco Unified Serviceability でサービスが実行中であることを確認できます。

手順

ステップ 1 （Unified Communications Manager の証明書モニタリングのために）Cisco Unified OS の管理にログインするか、（IM and Presence サービスの証明書モニタリングのために）Cisco Unified IM and Presence の管理にログインします。

ステップ 2 **[セキュリティ（Security）]** > **[証明書モニタ（Certificate Management）]** を選択します。

ステップ 3 [通知開始時期（Notification Start Time）] フィールドに、数値を入力します。 この値は、近づきつつある有効期限の通知を、有効期限の何日前にシステムが開始するかを表します。

ステップ 4 [通知頻度（Notification Frequency）] フィールドには、通知を行う頻度を入力します。

ステップ 5 これはオプションです。 [電子メール通知を有効にする（Enable E-mail notification）] チェックボックスをオンにして、近づきつつある証明書有効期限に関する電子メールアラートをシステムに送信させます。

ステップ 6 [LSC モニタリングを有効にする（Enable LSC Monitoring）] チェック ボックスをオンにして、LSC 証明書を証明書ステータス チェックに含めます。

ステップ 7 [電子メール ID（E-mail IDs）] フィールドに、システムが通知を送信する電子メール アドレスを入力します。 複数の電子メールアドレスは、セミコロンで区切って入力できます。

ステップ 8 **[保存]** をクリックします。

（注） 証明書モニタ サービスは、デフォルトで 24 時間ごとに 1 回だけ実行します。 証明書モニタ サービスを再起動すると、サービスが開始され、24 時間後に実行する次のスケジュールが計算されます。 証明書の有効期限が 7 日以内に近づいても、この周期は変化しません。 このサービスは、証明書の有効期限が切れる 1 日前から、有効期限が切れた後も 1 時間おきに実行します。

次のタスク

Online Certificate Status Protocol（OCSP）を設定し、期限切れの証明書をシステムが自動的に失効させるようにします。 詳細については、次を参照してください。 OCSP による証明書失効の設定 （412 ページ）

OCSP による証明書失効の設定

オンライン証明書ステータスプロトコル（OCSP）を有効にして、証明書の状態を定期的にチェックし、期限切れの証明書を自動的に失効させます。

始める前に

システムに OCSP チェックに必要な証明書があることを確認します。 OCSP 応答属性を設定されているルート CA 証明書または中間 CA 証明書を使用することができます。または、tomcat-trust へアップロードされている指定された OCSP 署名証明書を使用することができます。

手順

ステップ 1 （Unified Communications Manager の証明書失効のために）Cisco Unified OS の管理にログインするか、（IM and Presence サービスの証明書失効のために）Cisco Unified IM and Presence の管理にログインします。

ステップ 2 **[セキュリティ（Security）] > [証明書失効（Certificate Revocation）]** を選択します。

ステップ 3 [OCSP の有効化（Enable OCSP）]チェック ボックスをオンにして、次のタスクのいずれかを実行します。

- OCSP チェックの OCSP レスポンダを指定する場合は、[設定済み OCSP URI を使用する（Use configured OCSP URI）] ボタンを選択し、[OCSP 設定済み URI（OCSP Configured URI）] フィールドにレスポンダの URI を入力します。
- OCSP レスポンダ URI で証明書を設定する場合、[証明書からの OCSP URI を使用する（Use OCSP URI from Certificate）] ボタンを選択します。

ステップ 4 [失効チェックを有効にする（Enable Revocation Check）] チェック ボックスをオンにします。

ステップ 5 [チェック間隔（Check Every）] フィールドに失効チェックの間隔を入力します。

ステップ 6 **[保存]** をクリックします。

ステップ 7 これはオプションです。 CTI、IPsec または LDAP リンクがある場合は、これらの長期性接続のOCSP失効サポートを有効にするために、上記の手順に加えて次の手順も行う必要があります。

a) Cisco Unified CM Administrationから、**[システム]** > **[企業パラメータ]** を選択します。
b) [証明書の失効や有効期限（Certificate Revocation and Expiry）] で、[証明書有効性チェック（Certificate Validity Check）] パラメーターを [True] に設定します。
c) [有効性チェック頻度（Validity Check Frequency）] パラメーターの値を設定します。

（注） **[証明書失効]** ウィンドウの **[失効チェックを有効にする（Enable Revocation Check）]** パラメータの間隔値は、**[有効チェック頻度（Validity Check Frequency）]** エンタープライズ パラメータの値よりも優先されます。

d) **[保存（Save）]** をクリックします。

証明書エラーのトラブルシュート

始める前に

IM and Presence サービス ノードから Unified Communications Manager サービスに、または、Unified Communications Manager ノードから IM and Presence サービス機能にアクセスしようとしてエラーが発生した場合は、tomcat-trust 証明書に問題があります。 「サーバへの接続を確立できません（リモート ノードに接続できません）（Connection to the Server cannot be established (unable to connect to Remote Node)）」というエラー メッセージが、次の [サービスアビリティ（Serviceability ）] インターフェイス ウィンドウに表示されます。

- **サービスのアクティベーション**
- **コントロール センター - 機能サービス**
- **コントロール センター - ネットワーク サービス**

この手順を使用して、証明書のエラーを解決します。 最初のステップから開始し、必要に応じて進みます。 最初のステップだけでエラーが解決される場合もあれば、すべてのステップを実行することが必要になる場合もあります。

手順

ステップ 1 [Cisco Unified OS の管理（Cisco Unified OS Administration）] の **[セキュリティ（Security）]** > **[証明書の管理（Certificate Management）]** で、必要な tomcat-trust 証明書が存在することを確認します。

必要な証明書がない場合は、再度確認するまで 30 分間待ちます。

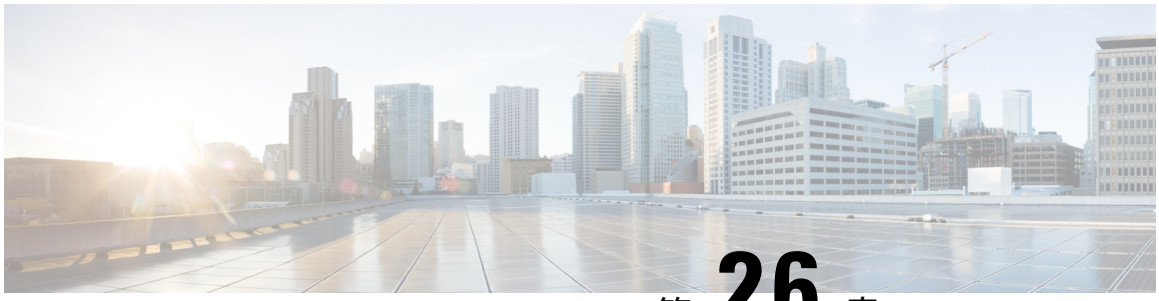
ステップ 2 証明書を選択して情報を表示します。 証明書の内容が、リモート ノード上の対応する証明書の内容と一致することを確認します。

ステップ 3 CLI から、**utils service restart Cisco Intercluster Sync Agent** を実行して Cisco Intercluster Sync Agent サービスを再起動します。

ステップ 4 Cisco Intercluster Sync Agent サービスが再起動したら、**utils service restart Cisco Tomcat** を実行して Cisco Tomcat サービスを再起動します。

ステップ 5 30 分間待機します。 前の手順で証明書のエラーが対処されず、tomcat-trust 証明書が存在する場合は、証明書を削除します。 証明書を削除した後、ノードごとに Tomcat および Tomcat-ECDSA 証明書をダウンロードし、tomcat-trust 証明書としてピアにアップロードして、証明書を手動で交換する必要があります。

ステップ 6 証明書の交換が完了したら、**utils service restart Cisco Tomcat** を実行して、影響を受ける各サーバで Cisco Tomcat を再起動します。



第 26 章

一括証明書の管理

一括証明書の管理

クラスタ間で証明書のセットを共有する場合に、一括証明書管理を使用します。この手順は、Extension Mobility Cross Cluster などのクラスタ間で信頼を確立する必要があるシステム機能に必要です。

手順

	コマンドまたはアクション	目的
ステップ 1	証明書のエクスポート （415 ページ）	この手順では、クラスタ内の全ノードの証明書を含むPKCS12 ファイルを作成します。
ステップ 2	証明書のインポート （416 ページ）	ホーム クラスタとリモート（訪問先）クラスタに証明書をインポートします。

証明書のエクスポート

この手順では、クラスタ内の全ノードの証明書を含む PKCS12 ファイルを作成します。

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）]**> **[証明書の一括管理（Bulk Certificate Management）]** を選択します。

ステップ 2 ホーム クラスタとリモート クラスタの両方で到達可能な TFTP サーバを設定します。 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 **[保存]** をクリックします。

ステップ 4 [エクスポート（Export）]をクリックします。

ステップ 5 [証明書の一括エクスポート（Bulk Certificate Export）]ウィンドウの[証明書のタイプ（Certificate Type）]フィールドで、[すべて（All）]を選択します。

ステップ 6 [エクスポート（Export）]をクリックします。

ステップ 7 **[閉じる（Close）]** をクリックします。

（注） 一括証明書エクスポートを実行すると、証明書は次のようにリモートクラスタにアップロードされます。

- CAPF 証明書は Callmanager-trust としてアップロードされます
- Tomcat 証明書は Tomcat-trust としてアップロードされます
- CallManager 証明書は Callmanager-trust としてアップロードされます
- CallManager 証明書は Phone-SAST-trust としてアップロードされます
- ITLRecovery 証明書は、PhoneSast-trust および CallManager-trust としてアップロードされます。

上記の手順は、証明書が自己署名証明書であり、別のクラスタに共通の信頼がない場合に実行されます。 共通の信頼関係または同じ署名者がいる場合は、すべての証明書のエクスポートは必要ありません。

証明書のインポート

ホーム クラスタとリモート（訪問先）クラスタに証明書をインポートします。

（注） 一括証明書管理機能を使用して証明書をインポートすると、電話機がリセットされます。

始める前に

[インポート（Import）] ボタンが表示されるには、次の操作を完了しておく必要があります。

- 2 つ以上のクラスタから SFTP サーバに証明書をエクスポートします。
- エクスポートした証明書を統合します。

手順

ステップ 1 [Cisco Unified OS 管理（Cisco Unified OS Administration）] から、以下を選択します。**[セキュリティ（Security）]** > **[証明書の一括管理（Bulk Certificate Management）]** > **[インポート（Import）]** > **[証明書の一括インポート（Bulk Certificate Import）]** を選択します。

ステップ 2 [証明書タイプ（Certificate Type）]ドロップダウン リストから、[すべて（All）]を選択します。

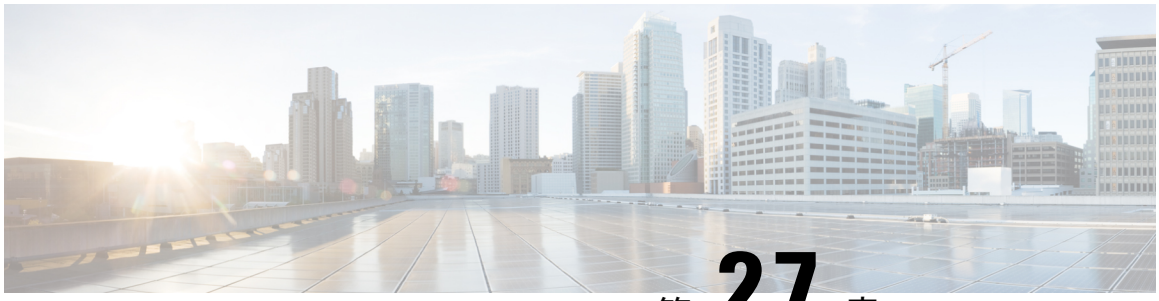
ステップ 3 [Import] を選択します。

（注） 一括証明書インポートを実行すると、証明書は次のようにリモート クラスタにアップロードされます。

- CAPF 証明書は Callmanager-trust としてアップロードされます
- Tomcat 証明書は Tomcat-trust としてアップロードされます
- CallManager 証明書は Callmanager-trust としてアップロードされます
- CallManager 証明書は Phone-SAST-trust としてアップロードされます
- ITLRecovery 証明書は、PhoneSast-trust および CallManager-trust としてアップロードされます。

（注） 次のタイプの証明書により、再起動する電話が決定されます。

- Callmanager：TFTP サービスが、証明書が属するノード上でアクティブになっている場合にのみ、すべての電話。
- TV：Callmanager グループ メンバーシップに基づいて、一部の電話。
- CAPF：CAPF がアクティブになっている場合にのみ、すべての電話。



第 27 章

IPSec ポリシーの管理

IPsec ポリシーの概要

IPsec は、暗号セキュリティ サービスを使用した IP ネットワーク経由の非公開でセキュアな通信を保証するフレームワークです。 IPsec ポリシーが IPsec セキュリティ サービスの設定に使用されます。 このポリシーは、ネットワーク上のほとんどのトラフィック タイプにさまざまなレベルの保護を提供します。 コンピュータ、部門（OU）、ドメイン、サイト、またはグローバル企業のセキュリティ要件を満たすように IPsec ポリシーを設定できます。

IPsec ポリシーの設定

（注）
- システムのアップグレード中、IPsec ポリシーに何らかの変更を行ってもその変更は無効になります。アップグレード中は IPsec ポリシーを作成したり変更したりしないでください。
- IPsec には双方向プロビジョニングが必要です（ホストまたはゲートウェイごとに 1 ピア）。
- 一方の IPsec ポリシープロトコルが 「ANY」、もう一方の IPsec ポリシープロトコルが 「UDP」 または 「TCP」 に設定されている 2 つの Unified Communications Manager ノードに IPsec ポリシーをプロビジョニングする場合、「ANY」 プロトコルを使用するノードでの検証で検出漏れが発生する可能性があります。
- IPsec はシステムのパフォーマンスに影響します（特に暗号化した場合）。
- IPsec ポリシーを現在のバージョンまたはアップグレードされたバージョンに設定し、ベースバージョンに設定していない場合は、バージョンをベースバージョンに切り替える際に、IPSec ポリシーを削除するか、無効にしてください。 これは、IPSec ポリシーが一方のノードにのみ設定され、他方のノードには、バージョンをそちらに切り替えるまで IPSec ポリシーが設定されないためです。 この操作を行わなければ、接続エラーが発生します。
- Unified CM ノードを再起動し、IPsec 接続が確立しない場合は、**utils ipsec restart** のコマンドを使用して IPsec サービスを再起動すると、IPsec 接続が確立します。 この方法で、IPsec サービスの再起動からネットワーク接続の確立までに起こり得る問題を軽減させることができます。

手順

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

ステップ 2 [新規追加] をクリックします。

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

ステップ 4 **[保存]** をクリックします。

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

IPSec 証明書のチェック

IPSec 証明書をチェックするには、次の操作を行います。

手順

ステップ 1 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 検索情報を指定し、**[検索（Find）]** をクリックします。

ステップ 3 IPsec 証明書を検索します（パブリッシャとサブスクライバノードに別々にログインしてください）。

（注） 通常、サブスクライバノードの IPsec 証明書は、パブリッシャノードには表示できませんが、 ただし、パブリッシャノードの IPsec 証明書を IM and Presence Service ノードのサブスクライバノードに表示することはできます。

IPsec 接続を有効にするには、すべての Unified Communications Manager ノードで、他のシステムからの CA 署名付き IPsec 証明書を **IPsec-Trust** 証明書として使用する必要があります。

ipsec-trust で同じ共通名を持つ過去の証明書は、新しい証明書を **ipsec-trust** にアップロードする前に削除してください。

IPsec ポリシーの管理

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 ポリシーを表示、有効、または無効にするには、次の手順を実行します。

a) ポリシー名をクリックします。

b) ポリシーを有効または無効にするには、[ポリシーの有効化（Enable Policy）]チェックボックスをオンまたはオフにします。

c) **[保存]** をクリックします。

（注） IPsec ポリシーを無効にした後、**show network cluster** コマンドを使用してクラスタの認証ステータスを確認します。 作成され無効になっている IPsec ポリシーが接続されているノードが認証されていない場合は、**utils ipsec restart** コマンドを使用して両方のノードで IPsec サービスを再起動してください。

ステップ 3 1 つまたは複数のポリシーを削除するには、次の手順を実行します。

a) 削除するポリシーの横にあるチェックボックスをオンにします。

[すべてを選択（Select All）]をクリックするとすべてのポリシーを選択でき、[すべてをクリア（Clear All）]を選択するとすべてのチェックボックスをクリアできます。

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

第 28 章

クレデンシャル ポリシーの管理

クレデンシャル ポリシーと認証

認証機能は、ユーザの認証、クレデンシャル情報の更新、ユーザイベントとエラーのトラッキングとロギング、クレデンシャル変更履歴の記録、データ ストレージ用のユーザ クレデンシャルの暗号化または復号を行います。

システムは常に、アプリケーション ユーザ パスワードとエンド ユーザ PIN を Unified Communications Manager データベースに照合します。 エンド ユーザ パスワードについては、社内ディレクトリまたはデータベースに照合して認証できます。

システムが社内ディレクトリと同期されていれば、Unified Communications Manager または Lightweight Directory Access Protocol（LDAP）のいずれかの認証機能によってパスワードを認証できます。

- LDAP 認証が有効にされている場合、ユーザ パスワードおよびクレデンシャル ポリシーは適用されません。 これらのデフォルトは、ディレクトリ同期（DirSync サービス）で作成されたユーザに適用されます。
- LDAP 認証を無効にすると、システムはユーザ クレデンシャルをデータベースに照合して認証します。 このオプションを使用する場合、クレデンシャル ポリシーを割り当て、認証イベントおよびパスワードを管理することができます。 エンドユーザは、電話機のユーザ インターフェイスでパスワードと PIN を変更できます。

クレデンシャル ポリシーは、オペレーティング システムのユーザまたは CLI のユーザには適用されません。 オペレーティング システムの管理者は、オペレーティング システムでサポートされている標準のパスワード検証手順を使用します。

データベースにユーザが設定されると、システムはユーザ クレデンシャルの履歴をデータベースに格納して、ユーザがクレデンシャルの変更を要求されたときに以前の情報を入力できないようにします。

クレデンシャル ポリシーの JTAPI および TAPI のサポート

Cisco Unified Communications Manager Java テレフォニー アプリケーション プログラミング インターフェイス（JTAPI）およびテレフォニー アプリケーション プログラミング インターフェイス（TAPI）は、アプリケーション ユーザに割り当てられたクレデンシャル ポリシーをサポートするため、開発者はパスワードの有効期限、PIN の有効期限、およびクレデンシャル ポリシーの適用のためのロックアウト戻りコードに応答するアプリケーションを作成する必要があります。

アプリケーションは、アプリケーションが使用する認証モデルに関係なく、API を使用してデータベースまたは社内ディレクトリで認証します。

開発者向けの JTAPI および TAPI の詳細については、開発者ガイド（http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-programming-reference-guides-list.html）を参照してください。

クレデンシャル ポリシーの設定

クレデンシャル ポリシーは、アプリケーション ユーザとエンド ユーザに適用されます。 パスワード ポリシーをエンド ユーザとアプリケーション ユーザに割り当て、PIN ポリシーをエンド ユーザに割り当てます。 [クレデンシャル ポリシーのデフォルトの設定（Credential Policy Default Configuration）] に、これらのグループのポリシー割り当てが一覧表示されます。 新しいユーザをデータベースに追加すると、システムがデフォルト ポリシーを割り当てます。 割り当てられたポリシーを変更したり、ユーザ認証イベントを管理したりできます。

（注） CTI アプリケーション ユーザーの場合は、[クレデンシャル ポリシーの設定（Credential Policy Settings）] の [許可される非アクティブ日数（Inactive Days Allowed）] が 0（無制限）にセットされていることを確認してください。 0 にセットされていない場合、CTI アプリケーション ユーザーが予期せず非アクティブになり、再起動後に CTI アプリケーションから Unified CM に接続できなくなる可能性があります。

手順

ステップ 1 Cisco Unified CM Administration で、**[ユーザ管理] > [ユーザ設定] > [クレデンシャル ポリシーのデフォルト]** を選択します。

ステップ 2 次のいずれかの手順を実行します。

- [検索（Find）] をクリックし、既存のクレデンシャル ポリシーを選択します。

• [新規追加（Add New）]をクリックして、新しいクレデンシャル ポリシーを作成します。

ステップ 3 [クレデンシャル ポリシーの設定（Credential Policy Configuration）]ウィンドウの各フィールドに入力します。 フィールドとその設定の詳細については、オンライン ヘルプを参照してください。

ステップ 4 **[保存]** をクリックします。

クレデンシャル ポリシーのデフォルトの設定

インストール時に、Cisco Unified Communications Managerがスタティック デフォルト クレデンシャル ポリシーをユーザ グループに割り当てます。 デフォルト クレデンシャルは提供しません。お使いのシステムが、新しいデフォルト ポリシーを割り当てたり、ユーザの新しいデフォルト クレデンシャルとクレデンシャル要件を設定したりするためのオプションを提供します。

手順

ステップ 1 Cisco Unified CM Administration で、**[ユーザ管理]** > **[ユーザ設定]** > **[クレデンシャル ポリシーのデフォルト]** を選択します。

ステップ 2 [クレデンシャル ポリシー（Credential Policy）]ドロップダウン リスト ボックスから、このグループのクレデンシャル ポリシーを選択します。

ステップ 3 [クレデンシャルの変更（Change Credential）]と [クレデンシャルの確認（Confirm Credential）]の両方にパスワードを入力します。

ステップ 4 このクレデンシャルをユーザに変更させない場合は、[ユーザは変更不可（User Cannot Change）]チェックボックスをオンにします。

ステップ 5 ユーザが次のログイン時に変更する必要がある、一時的なクレデンシャルを設定する場合は、[次回ログイン時に変更必要（User Must Change at Next Login）]チェックボックスをオンにします。

（注） このボックスをオンにすると、ユーザはパーソナル ディレクトリ サービスを使用してPIN を変更できなくなることに注意してください。

ステップ 6 クレデンシャルの期限を設定しない場合は、[有効期限なし（Does Not Expire）]チェックボックスをオンにします。

ステップ 7 **[保存]** をクリックします。

認証アクティビティのモニタ

システムは、最後のハッキング試行時刻や失敗したログイン試行のカウントなどの最新の認証結果を表示します。

システムは、次のクレデンシャル ポリシー イベントに関するログ ファイル エントリを生成します。

- 認証成功
- 認証失敗（不正なパスワードまたは不明）
- 次の原因による認証失敗
  - 管理ロック
  - ハッキング ロック（失敗したログオン ロックアウト）
  - 期限切れソフト ロック（期限切れのクレデンシャル）
  - 非アクティブ ロック（一定期間使用されていないクレデンシャル）
  - ユーザによる変更が必要（ユーザが変更するように設定されたクレデンシャル）
  - LDAP 非アクティブ（LDAP 認証へ切り替えたものの LDAP が非アクティブ）
- 成功したユーザ クレデンシャル更新
- 失敗したユーザ クレデンシャル更新

（注） エンド ユーザ パスワードに対して LDAP 認証を使用する場合は、LDAP は認証の成功と失敗だけを追跡します。

すべてのイベント メッセージに、文字列 「ims-auth」 と認証を試みているユーザ ID が含まれています。

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified CM Administration）] で、**[ユーザの管理（User Management）] > [エンド ユーザ（End Users）]** を選択します。

ステップ 2 検索条件を入力し、[検索（Find）]をクリックして、表示された一覧からユーザを選択します。

ステップ 3 [クレデンシャルの編集（Edit Credential）]をクリックし、ユーザの認証アクティビティを表示します。

次のタスク

Cisco Unified Real-Time Monitoring Tool（Unified RTMT）を使用してログ ファイルを表示できます。 キャプチャされたイベントをレポートに収集することもできます。 Unified RTMT の詳細な使用手順については、『*Cisco Unified Real-Time Monitoring Tool Administration Guide*』（http://www.cisco.com/c/en/us/support/unified-communications/

unified-communications-manager-callmanager/products-maintenance-guides-list.html）を参照してください。

クレデンシャル キャッシングの設定

クレデンシャル キャッシングを有効にすると、システム効率が向上します。 システムは、ログイン要求ごとに、データベース ルックアップを実行したり、ストーアド プロシージャを呼び出したりする必要がありません。 キャッシュ期間が経過するまでは、関連付けられているクレデンシャル ポリシーが適用されません。

この設定は、ユーザ認証を呼び出すすべての Java アプリケーションに適用されます。

手順

ステップ 1 Cisco Unified CM Administrationから、**[システム]** > **[企業パラメータ]** を選択します。

ステップ 2 必要に応じて、次のタスクを実行します。

- [キャッシングの有効化（Enable Caching）]エンタープライズパラメータを [True]に設定します。 このパラメータを有効にすると、Cisco Unified Communications Manager は、最大 2 分間、キャッシュされたクレデンシャルを使用します。
- システムがキャッシュされたクレデンシャルを認証に使用しないように、キャッシングを無効にするには、[キャッシングの有効化（Enable Caching）]エンタープライズパラメータを [False]に設定します。 LDAP 認証の場合、この設定は無視されます。 クレデンシャル キャッシングでは、ユーザごとに最小量の追加メモリが必要です。

ステップ 3 **[保存（Save）]** をクリックします。

セッション終了の管理

管理者は、各ノードに固有のユーザのアクティブなサインインセッションを終了するために、次の手順を使用できます。

（注）
- 特権レベル 4 を持つ管理者のみが、セッションを終了できます。
- セッション管理では、特定のノード上のアクティブなサインイン セッションを終了します。 管理者は、異なるノード間ですべてのユーザセッションを終了する場合には、各ノードにサインインしてセッションを終了する必要があります。

これは、次のインターフェイスに適用されます。

- Cisco Unified CM の管理

- Cisco Unified Serviceability
- Cisco Unified のレポート
- Cisco Unified Communications セルフ ケア ポータル
- Cisco Unified CM IM and Presence の管理
- Cisco Unified IM and Presence サービスアビリティ
- Cisco Unified IM and Presence のレポート

手順

ステップ 1 Cisco Unified OS Administration または Cisco Unified IM and Presence OS Administration から、**[セキュリティ（Security）]** > **[セッション管理（Session Management）]** を選択します。
[セッション管理（Session Management）] ウィンドウが表示されます。

ステップ 2 [ユーザ ID（User ID）] フィールドにアクティブなサインイン ユーザのユーザ ID を入力します。

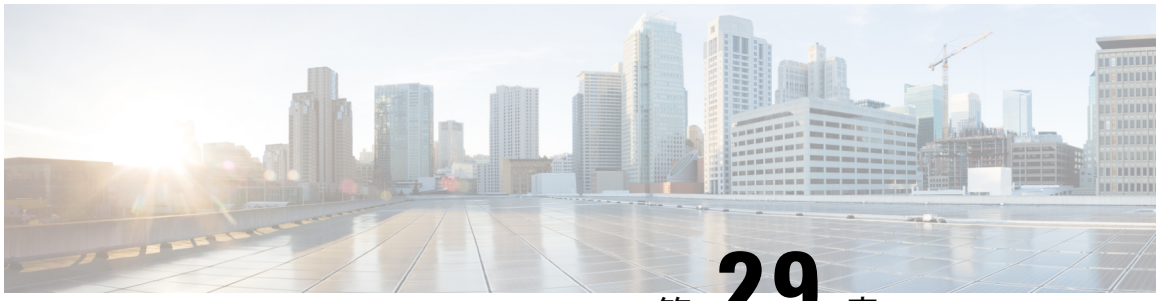
ステップ 3 [セッションの終了（Terminate Session）] をクリックします。

ステップ 4 **OK**をクリックします。

終了したユーザは、サインインしたインターフェイスページを更新にすると、サインアウトします。 監査ログにエントリが作成され、そこに終了した `userID` が表示されます。

第 VII 部

IPアドレス、ホスト名とドメイン名の変更



第 29 章

変更前タスクとシステム ヘルス チェック

変更前のタスク

IP アドレス、ホスト名、およびその他のネットワーク識別子の変更

導入におけるノードのネットワーク レベルの IP アドレスとホスト名をさまざまな理由で変更できます。これには、クラスタ間でノードを移動することや、重複している IP アドレスの問題を解決することが含まれます。 IP アドレスは、ノードに関連付けられたネットワーク レベルの Internet Protocol (IP) ではホスト名は、ノードのネットワーク レベルのホスト名です。

（注） すべての統合コミュニケーション製品（Cisco Unified Communications Manager、Cisco Unity Connections、Cisco IM and Presenceなど）は、1 つのインターフェイスしか持っていません。 したがって、これらの製品ごとにIP アドレスを 1 つづつ割り当てることができます。

ノード名やドメイン名など、その他のネットワーク ID の変更については、次のリソースを参照してください。

- Cisco Unified Communications Manager システム設定ガイド
- *IM and Presence Service*設定および管理ガイド
- *Cisco Unified Communications Manager* および *IM and Presence Service* のインストールガイド

IM and Presence Serviceにおけるノードのノード名およびネットワーク レベル DNS デフォルト ドメイン名を変更する手順については、このドキュメントでも扱われています。

IM and Presence Service ノード名およびデフォルトのドメイン名の変更

ノード名は、Cisco Unified CM Administration GUI を使用して設定され、その他すべての IM and Presence Service ノードとすべてのクライアント マシンから解決可能である必要があります。したがって、推奨されるノード名の値は、ノードのネットワーク FQDN です。 ただし、IP アドレスとホスト名のどちらも、特定の導入ではノード名の値としてサポートされています。ノード名の推奨事項とサポートされている導入タイプの詳細については、ホスト名の設定（323 ページ） を参照してください。

ノードのネットワーク レベルの DNS デフォルト ドメイン名はホスト名と結合され、ノードの完全修飾ドメイン名（FQDN）を形成します。 たとえば、ホスト名が 「imp-server」 で、ドメインが 「example.com」 であるノードの FQDN は 「imp-server.example.com」 になります。

ノードのネットワーク レベル DNS デフォルト ドメインを、IM and Presence Service アプリケーションの企業ドメインと混同しないでください。

- ネットワークレベルの DNS デフォルト ドメインは、ノードのネットワーク ID としてのみ使用されます。
- 企業の IM and Presence Service ドメインは、エンド ユーザの IM アドレスで使用されるアプリケーション レベルのドメインです。

Cisco Unified CM IM and Presence Administration GUI または Cisco Unified Communications Manager Administration を使用して企業全体のドメインを設定できます。 企業ドメインの推奨事項とサポートされる導入タイプの詳細については、『*Deployment Guide for IM and Presence Service on Cisco Unified Communications Manager*』を参照してください。

ホスト名の設定

次の表に、Unified Communications Manager サーバーのホスト名を設定できる場所、ホスト名に使用できる文字数、ホスト名に推奨される最初と最後の文字を示します。ホスト名を正しく設定しないと、Unified Communications Manager の一部のコンポーネント（オペレーティングシステム、データベース、インストールなど）が期待通りに動作しない可能性があります。

表 *82 : Cisco Unified Communications Manager* におけるホスト名の設定

ホスト名の場所	可能な設定	指定できる文字数	推奨されるホスト名の先頭文字	推奨されるホスト名の最終文字
[ホスト名/IP アドレス（Host Name/IP Address）] フィールド Cisco Unified Communications Manager Administration の **[システム（System）]** > **[サーバ（Server）]**	クラスタ内のサーバのホスト名を追加または変更できます。	2-63	英字	英数字
[ホスト名（Hostname）] フィールド Cisco Unified Communications Manager インストール ウィザード	クラスタ内のサーバのホスト名を追加できます。	1-63	英字	英数字
[ホスト名（Hostname）] フィールド Cisco Unified Communications オペレーティング システムの **[設定（Settings）]** > **[IP]** > **[イーサネット（Ethernet）]**	クラスタ内のサーバのホスト名を変更できますが、追加はできません。	1-63	英字	英数字
set network hostname hostname コマンドライン インターフェイス	クラスタ内のサーバのホスト名を変更できますが、追加はできません。	1-63	英字	英数字

ヒント　このホスト名は、ARPANET ホスト名の規則に従う必要があります。ホスト名の先頭文字と最終文字の間には、英数文字とハイフンを入力できます。

いずれかの場所でホスト名を設定する前に、次の情報を確認してください。

- [サーバの設定（Server Configuration）] ウィンドウの [ホスト名/IP アドレス（Host Name/IP Address）] フィールドは、デバイスとサーバ間、アプリケーションとサーバ間、および異なるサーバ間の通信をサポートします。このフィールドには、ドット区切り形式の IPv4 アドレスまたはホスト名を入力できます。

  Unified Communications Manager パブリッシャ ノードをインストールした後は、パブリッシャのホスト名がこのフィールドに自動的に表示されます。Unified Communications Manager サブスクライバ ノードをインストールする前に、Unified Communications Manager パブリッシャ ノードでこのフィールドにサブスクライバ ノードの IP アドレスまたはホスト名を入力してください。

このフィールドにホスト名を設定できるのは、Unified Communications Manager が DNS サーバにアクセスしてホスト名を IP アドレスに解決できる場合のみです。DNS サーバに Cisco Unified Communications Manager の名前とアドレスの情報が設定されていることを確認してください。

ヒント　DNS サーバに Unified Communications Manager の情報を設定するのに加えて、Cisco Unified Communications Manager のインストール時に DNS 情報を入力します。

- Unified Communications Manager パブリッシャ ノードのインストール時に、ネットワーク情報を設定するために（つまり、スタティック ネットワークを使用する場合に）パブリッシャ サーバのホスト名（必須）と IP アドレスを入力します。

  Unified Communications Manager サブスクライバ ノードのインストール時には、Unified Communications Manager パブリッシャ ノードのホスト名と IP アドレスを入力して、Unified Communications Manager がネットワークの接続性およびパブリッシャとサブスクライバ間の検証を確認できるようにしてください。 さらに、サブスクライバ ノードのホスト名と IP アドレスも入力する必要があります。 Unified Communications Manager のインストール時にサブスクライバ サーバのホスト名の入力を求められた場合は、Cisco Unified Communications Manager Administration の（[ホスト名/IP アドレス（Host Name/IP Address）] フィールドでサブスクライバ サーバのホスト名を設定した場合に）[サーバの設定（Server Configuration）] ウィンドウに表示される値を入力します。

Procedure workflows

Cisco Unified Communications Manager ワークフロー

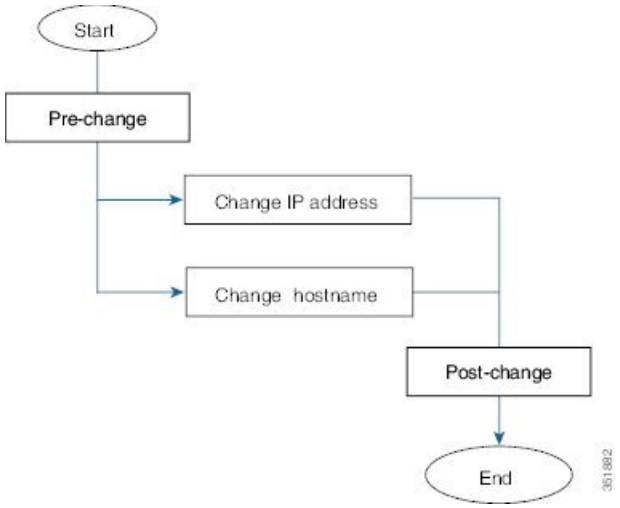
このドキュメントでは、Cisco Unified Communications Manager ノード上における次のタスクの詳細な手順を取り上げます。

- ノードの IP アドレスの変更
- ノードのホスト名の変更

実行するステップを要約したそれぞれの手順に関してタスク リストが示されます。

（注）　こうした変更を行う前に変更前タスクすべてとシステム ヘルス チェックを実行し、変更後には変更後タスクを実行しなければなりません。

図 *24 : Cisco Unified Communications Manager* ワークフロー



IM and Presence Service のワークフロー

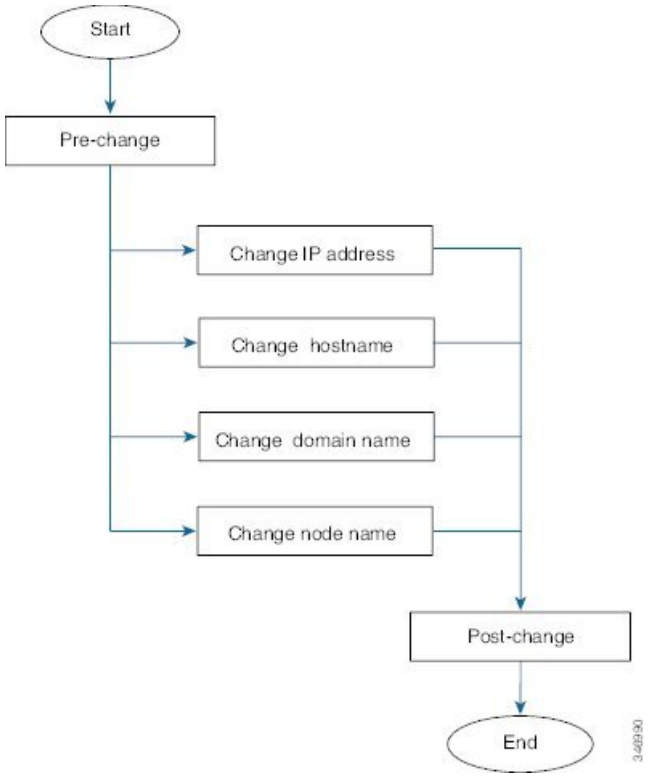
このマニュアルでは、IM and Presence Service ノードに対する以下の作業の詳細な手順を示します。

- ノードの IP アドレスの変更
- ノードのホスト名の変更
- DNS デフォルト ドメイン名の変更
- ノードのノード名の変更

実行するステップを要約したそれぞれの手順に関してタスク リストが示されます。

（注） こうした変更を行う前に変更前タスクすべてとシステム ヘルス チェックを実行し、変更後には変更後タスクを実行しなければなりません。

図 *25 : IM and Presence Service* のワークフロー



Cisco Unified Communications Manager ノードの変更前タスク

次の手順で、Cisco Unified Communications Manager ノードの IP アドレスとホスト名を変更する作業について説明します。これらの手順は、スケジュールしたメンテナンス時間内に実行する必要があります。

注意 これらのタスクを実行しても期待する結果が得られない場合は、問題が解決されるまで続行しないでください。

手順

ステップ 1 Cisco Unified Communications Manager サーバ内で DNS が設定されている場合、正引きおよび逆レコード（A レコードと PTR レコードなど）が設定されていて、DNS が到達可能で作動していることを確認します。

ステップ 2 アクティブな ServerDown 警告が出ていないことを確認し、クラスタ内のすべてのサーバが稼働していて利用可能であることを確かめます。 最初のノードで、Cisco Unified Real-Time Monitoring Tool（RTMT） またはコマンド ライン インターフェイス（CLI）のいずれかを使用します。

a) Unified RTMT を使用して確認するには、Alert Central にアクセスし、ServerDown 警告が発生していないか調べます。

b) 最初のノードで CLI を使用して確認するには、次の CLI コマンドを入力してアプリケーションのイベント ログを調べます。

```
file search activelog syslog/CiscoSyslog ServerDown
```

出力例については、データベース レプリケーションの出力例に関するトピックを参照してください。 詳細な手順およびトラブルシューティングについては、データベース レプリケーションおよびデータベース レプリケーションのトラブルシューティングについてのトピックを参照してください。

ステップ 3 クラスタにあるすべての Cisco Unified Communications Manager ノードでデータベース レプリケーションのステータスを調べ、すべてのサーバがデータベースの変更内容を正常に複製していることを確認します。 IM and Presence Service の場合、導入環境に複数のノードがあるときにはデータベース パブリッシャ ノードでデータベース レプリケーションのステータスを調べます。 Unified RTMT または CLI を使用します。 すべてのノードで 2 のステータスが表示される必要があります。

1. RTMT を使用して確認するには、Database Summary にアクセスしてレプリケーションのステータスを調べます。
2. CLI を使用して確認するには、**utils dbreplication runtimestate** を入力します。

ステップ 4 次の例に示されているように CLI コマンド utils diagnose を入力し、ネットワーク接続と DNS サーバの設定を確認してください。

例：

```
admin: utils diagnose module validate_network
Log file: /var/log/active/platform/log/diag1.log
Starting diagnostic test(s)
===========================
test - validate_network : Passed
Diagnostics Completed
admin:
```

ステップ 5 Cisco Unified レポート ツールで Unified CM Database Status レポートを生成します。 そのレポートにエラーや警告が記録されていないか確認します。

ステップ 6 Cisco Unified レポート ツールで Unified CM Cluster Overview レポートを生成します。 そのレポートにエラーや警告が記録されていないか確認します。

ステップ 7 最初のノードの Cisco Unified Communications Manager Administration から、**[システム（System）]**> **[サーバ（Server）]** の順に選択し、[**検索（Find）**] をクリックします。 クラスタにあるすべてのサーバが一覧表示されます。 後で参照できるように、サーバのこのリストを保持します。

クラスタ内のノードごとに、ホスト名と IP アドレスの両方のインベントリが保存されていることを確認します。

ステップ 8 手動でディザスタ リカバリ システムのバック アップを実行し、すべてのノードとアクティブなサービスが正しくバック アップされていることを確認します。 詳細については、『*Administration Guide for Cisco Unified Communications Manager*』を参照してください。

ステップ 9 ホスト名を変更する場合、SAML シングル サインオン（SSO）を無効にします。 SAML SSO の詳細については、『*Deployment Guide for IM and Presence Service on Cisco Unified Communications Manager*』を参照してください。

ステップ 10 セキュリティが有効なクラスタ（クラスタ セキュリティ モード 1 - 混合）について、証明書信頼リスト（CTL）ファイルを更新します。 既存の CTL ファイルへの新しい TFTP サーバの追加など、CTL ファイルの更新と管理の方法の詳細については、『*Cisco Unified Communications Manager Security Guide*』を参照してください。

（注） 通信不可能な時間が無駄に発生しないように、TFTP サーバの新しい IP アドレスで CTL ファイルを更新してから、TFTP サーバの IP アドレスを変更するようにします。 この手順を実行しない場合は、セキュリティが有効なすべての IP 電話を手動で更新する必要があります。

（注） セキュリティをサポートしているすべての IP 電話では、CTL ファイルが必ずダウンロードされます。このファイルには、その電話からの通信が許可されている TFTP サーバの IP アドレスが記述されています。 TFTP サーバの IP アドレスを変更した場合は、その新しい IP アドレスを CTL ファイルに追加する必要があります。これにより、該当の電話からその TFTP サーバと通信できるようになります。

IM and Presence サービス ノードの変更前セットアップ タスク

該当する変更前セットアップ タスクを実行して IP アドレス、ホスト名、ドメイン、またはノード名が正常に変更されるようにシステムが準備されていることを確認します。 これらのタスクは、スケジュールしたメンテナンス時間内に実行する必要があります。

注意 これらのタスクを実行しても期待する結果が得られない場合は、問題が解決されるまで続行しないでください。

（注） ドメイン名またはノード名を変更するまで、次の手順を実行して Cisco AXL Web サービスと IM and Presence Cisco Sync Agent サービスが開始されたことを確認する必要はありません。実行するタスクの完全な一覧については、変更前のタスクリストを参照してください。

手順

ステップ 1 クラスタにあるすべてのノードでデータベース レプリケーションのステータスを調べ、すべてのサーバがデータベースの変更内容を正常に複製していることを確認します。

IM and Presence Service の場合、導入環境に複数のノードがあるときにはデータベース パブリッシャ ノードでデータベース レプリケーションのステータスを調べます。

Unified RTMT または CLI を使用します。 すべてのノードで **2** のステータスが表示される必要があります。

a) RTMT を使用して確認するには、Database Summary にアクセスしてレプリケーションのステータスを調べます。

b) CLI を使用して確認するには、**utils dbreplication runtimestate** を入力します。

出力例については、データベース レプリケーションの出力例に関するトピックを参照してください。 詳細な手順およびトラブルシューティングについては、データベース レプリケーションおよびデータベース レプリケーションのトラブルシューティングについてのトピックを参照してください。

ステップ 2 次の例に示されているように CLI コマンド **utils diagnose** を入力し、ネットワーク接続と DNS サーバの設定を確認してください。

例：

```
admin: utils diagnose module validate_network Log file:
/var/log/active/platform/log/diag1.log Starting diagnostic test(s)
========================== test - validate_network : Passed Diagnostics
Completed admin:
```

ステップ 3 手動でディザスタ リカバリ システムのバック アップを実行し、すべてのノードとアクティブなサービスが正しくバック アップされていることを確認します。

詳細については、『*Administration Guide for Cisco Unified Communications Manager*』を参照してください。

ステップ 4 すべてのプレゼンス冗長グループでハイ アベイラビリティ（HA）を無効にします。プレゼンス冗長グループの構成情報は、*Cisco Unified Communications Manager* システム設定ガイド の「プレゼンス冗長グループの設定」の章を参考してください。

（注）
- HA を無効にする前に、各ノードとサブクラスタのユーザ数の記録を取ります。 この情報は、[Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）] の **[システム（System）]** > **[プレゼンス トポロジ（Presence Topology）]** ウィンドウで見つけることができます。
- HA を無効にした後、それ以上の変更を加える前に、クラスタ全体にわたって設定が同期されるまで、少なくとも 2 分待機します。

ステップ 5 ホスト名を変更する場合、SAML シングル サインオン（SSO）を無効にします。 SAML SSO の詳細については、『*Deployment Guide for IM and Presence Service on Cisco Unified Communications Manager*』を参照してください。

ステップ 6 現在アクティブなすべてのサービスのリストをまとめます。 後で参照できるように、これらのリストを保持します。

a) Cisco Unified Serviceability を使用してアクティブなネットワーク サービスのリストを表示するには、**[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。

b) Cisco Unified Serviceability を使用してアクティブな機能サービスのリストを表示するには、**[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。

ステップ 7 Cisco Unified Serviceability を使用してすべての機能サービスを停止するには、**[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。 機能サービスを停止する順序は重要ではありません。

ヒント IP アドレス、ホスト名、または IP アドレスとホスト名の両方を変更する場合、この手順を実行する必要はありません。 これらの名前の変更に対して、機能サービスは自動的に停止します。

ステップ 8 **[ツール（Tools）] > [コントロールセンター機能サービス（Control Center - Services）]** を選択するときに、Cisco Unified Serviceability を使用して [IM and Presence サービス（IM and Presence Service）] サービスグループの下にリストされる以下のネットワークサービスを停止します。

次の順序で、これらの IM and Presence Service ネットワーク サービスを停止する必要があります。

1. Cisco Config Agent
2. Cisco Intercluster Sync Agent
3. Cisco Client Profile Agent
4. Cisco OAM Agent
5. Cisco XCP Config Manager
6. Cisco XCP Router
7. Cisco Presence Datastore
8. Cisco SIP Registration Datastore
9. Cisco Login Datastore
10. Cisco Route Datastore
11. Cisco Server Recovery Manager
12. Cisco IM and Presence Data Monitor

ステップ 9 Cisco Unified Serviceability（**[ツール（Tools）]> [コントロールセンターの機能サービス（Control Center - Feature Services）]**）を使用して、Cisco AXL Web Service が Cisco Unified Communications Manager パブリッシャノードで起動していることを確認します。

（注） ドメイン名またはノード名を変更する場合にのみ、この手順を実行します。

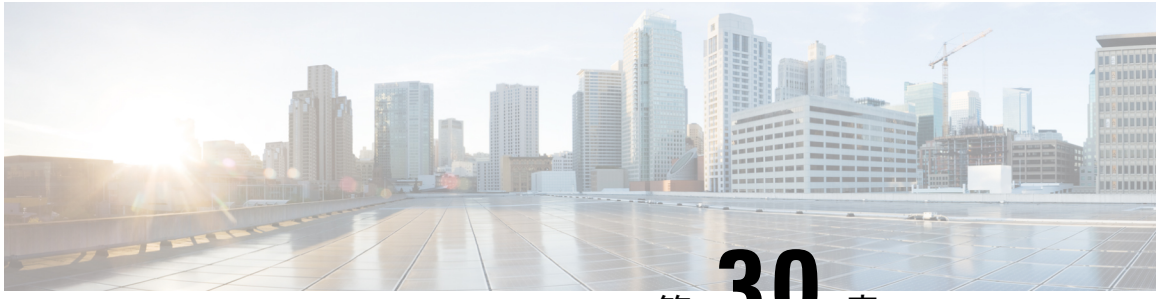
ステップ 10 IM and Presence Cisco Sync Agent サービスが開始し、同期が完了したことを確認します。

（注） ドメイン名またはノード名を変更する場合にのみ、この手順を実行します。

a) Cisco Unified Serviceability を使用して確認するには、以下の手順を実行します。

1. **[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）]** を選択します。
2. IM and Presence データベース パブリッシャ ノードを選択します。
3. [IM and Presence サービス（IM and Presence Service）]サービスを選択します。
4. Cisco Sync Agent サービスが開始していることを確認します。
5. Cisco Unified CM IM and Presence Administration GUI から、**[診断（Diagnostics）] > [システム ダッシュボード（System Dashboard）] > [同期ステータス（Sync Status）]** を選択します。
6. 同期が完了し、同期ステータス領域にエラーが表示されていないことを確認します。

b) IM and Presence データベース パブリッシャ ノードで Cisco Unified CM IM and Presence Administration GUI を使用して確認するには、**[診断（Diagnostics）] > [システム ダッシュボード（System Dashboard）]** を選択します。



第 30 章

IP アドレスおよびホスト名の変更

IP アドレスとホスト名の変更のタスク リスト

次の表に、Cisco Unified Communications Manager と IM and Presence Service ノードの IP アドレスとホスト名を変更するために実行するタスクを示します。

表 *83 : IP* アドレスとホスト名の変更のタスク リスト

項目	タスク
1	変更前タスクおよびシステム ヘルス チェックを行います。
2	コマンド ライン インターフェイス（CLI）または Unified オペレーティング システム GUI を使用してノードの IP アドレスまたはホスト名を変更します。 IM and Presence Service ノードの場合、次の条件に従ってください。 • サブスクライバ ノードを変更する前にデータベース パブリッシャ ノードの IP アドレスとホスト名を変更します。 • すべてのサブスクライバ ノードの IP アドレスとホスト名を同時に変更する、もしくは、一度に 1 つずつ変更することが可能です。 （注） IM and Presence Service ノードの IP アドレスまたはホスト名を変更した後、Cisco Unified Communications Manager の SIP パブリッシュトランクの接続先アドレス値を変更する必要があります。 変更後タスク リストを参照してください。

項目	タスク
3	変更後タスクを実行します。

OS Admin GUI による IP アドレスまたはホスト名の変更

Cisco Unified Operating System Administration を使用して、導入のホスト名で定義されているパブリッシャおよびサブスクライバ ノードの IP アドレスまたはホスト名を変更することができます。 特に明記されていない限り、この手順の各ステップは、Unified Communications Manager および IM and Presence Service クラスター上のパブリッシャーノードとサブスクライバーノードの両方に適用されます。

set network hostname コマンドを使用してホスト名を変更すると、自動的に自己署名証明書の再作成がトリガーされます。 これにより、クラスタ内のすべてのデバイスがリセットされ、更新された ITL ファイルをダウンロードできるようになります。 クラスタが CA 署名付き証明書を使用する場合は、証明書に再署名する必要があります。

set network hostname コマンドを使用して IP アドレスのみを変更すると、クラスタ内のすべてのデバイスがリセットされ、更新された ITL ファイルをダウンロードできます。 証明書は更新されません。

（注） ホスト名を変更しても、ITL リカバリ証明書の再生成はトリガーされません。

注意

- これらの設定を変更する場合は、Cisco Unified Operating System Administration から 1 つずつ行うことを推奨します。 IP アドレスとホスト名を同時に変更するには、CLI コマンドの **set network hostname** を使用します。
- Unified Communications Manager のクラスタセキュリティが混合モードで実行されている場合にホスト名または IP アドレスを変更すると、このノードへのセキュア接続は、CTL クライアントを実行して CTL ファイルを更新しない限り（またはトークンレス CTL 機能を使用している場合は **utils ctl update CTLFile** を実行しない限り）失敗します。

始める前に

導入環境で変更前タスクとシステム ヘルス チェックを実行します。

（注） vcenter から vNIC を変更する必要がある場合は、CLI コマンド **set network hostname** を使用します。

手順

ステップ 1 Cisco Unified Operating System Administration から、**[設定（Settings）]** > **[IP]** > **[イーサネット（Ethernet）]** の順に選択します。

ステップ 2 ホスト名、IP アドレス、また必要に応じてデフォルトのゲートウェイを変更します。

ステップ 3 **[保存]** をクリックします。

ノード サービスが新しい変更内容で自動的に再起動します。 サービスを再起動することで、更新とサービス再起動のシーケンスを適切に実行して、変更を有効にすることができます。

ホスト名を変更すると、自己署名証明書が自動的に再生成されます。また、更新された ITL ファイルをダウンロードできるように、クラスタ内のすべてのデバイスがリセットされます。ホスト名を変更しても、ITL リカバリ証明書の再生成はトリガーされません。

次のタスク

導入の変更が正しく実行されていることを確認するすべての該当する変更後の作業を実行します。

（注） 新しいホスト名が正しいIPアドレスに解決されない場合は、次の手順に進まないでください。

クラスタが CA 署名付き証明書を使用する場合は、証明書に再署名する必要があります。

このプロセスを使用してクラスタを混合モードにした場合は、CTL クライアントを実行して CTL ファイルを更新します。 トークンレス CTL 機能を使用した場合は、CLI コマンドの **utils ctl update CTLFile** を実行します。

Unified CM Administration GUI による IP アドレスまたはホスト名の変更

Cisco Unified CM Administration を使用して、データベースで定義されているパブリッシャおよびサブスクライバノードの IP アドレスまたはホスト名を変更することができます。 これにより、ホスト名のエントリをシステムで定義されているホスト名や IP アドレスの値と一致させることができます。

IP アドレスまたはホスト名を変更すると、自己署名証明書が自動的に再生成されます。 これにより、クラスタ内のすべてのデバイスがリセットされ、更新された ITL ファイルをダウンロードできるようになります。クラスタがCA署名付き証明書を使用する場合は、証明書に再署名する必要があります。

⚠

注意

- ホスト名や IP アドレスを変更するには、システムのサービスを再起動する必要があります。 そのため、通常の就業時間中に行うことは避けなくてはなりません。
- これらの設定を変更する場合は、Cisco Unified CM Administration から 1 つずつ行うことを推奨します。 IP アドレスとホスト名を同時に変更するには、CLI コマンドの **set network hostname** を使用します。
- Unified Communications Manager のクラスタセキュリティが混合モードで実行されている場合にホスト名または IP アドレスを変更すると、このノードへのセキュア接続は、CTL クライアントを実行して CTL ファイルを更新しない限り（またはトークンレス CTL 機能を使用している場合は **utils ctl update CTLFile** を実行しない限り）失敗します。
- Cisco Unified OS Administration と Cisco Unified CM Administration のページに定義されているホスト名または IP アドレスが一致しない場合、アプリケーションは電話機のステータスを正しく取得できません。 また、証明書が一致しなければ TLS ハンドシェイクが失敗します。 Cisco Unified OS Administration と Cisco Unified CM Administration のページには、IP アドレスとホスト名に同じものを定義してください。

始める前に

導入環境で変更前タスクとシステム ヘルス チェックを実行します。

手順

ステップ 1 Cisco Unified CM Administration で、**[システム（System）]** > **[サーバ（Server）]** の順に選択します。

[サーバの検索/一覧表示（Find and List Servers）]ウィンドウが表示されます。

ステップ 2 サーバのリストを取得するには、**[検索（Find）]** をクリックします。

ステップ 3 ホスト名を変更するサーバをリストからクリックします。

ステップ 4 **[ホスト名/IP アドレス（Host name/IP Address）]*** フィールドに、新しいホスト名または IP アドレスを入力して **[保存**（Save）] をクリックします。

ステップ 5 管理 CLI GUI から **utils system restart** の CLI コマンドを使用してノードをリブートします。

CLI による IP アドレスまたはホスト名の変更

導入のホスト名で定義されているパブリッシャおよびサブスクライバ ノードの IP アドレスまたはホスト名を変更するには、CLI を使用できます。 特に明記されていない限り、この手順の各ステップは、Cisco Unified Communications Manager と IM and Presence Service クラスタのパブリッシャ ノードとサブスクライバ ノードの両方に適用されます。

ホスト名を変更すると、自己署名証明書が自動的に再生成されます。これにより、クラスタ内のすべてのデバイスがリセットされ、更新されたITLファイルをダウンロードできるようになります。クラスタがCA署名付き証明書を使用する場合は、証明書に再署名する必要があります。 ホスト名を変更しても、ITL リカバリ証明書の再生成はトリガーされません。

注意 Cisco Unified Communications Manager のクラスタセキュリティが混合モードで実行されている場合にホスト名または IP アドレスを変更すると、このノードへのセキュア接続は、CTL クライアントを実行して CTL ファイルを更新しない限り（またはトークンレス CTL 機能を使用している場合は **utils ctl update CTLFile** を実行しない限り）失敗します。

始める前に

導入環境で変更前タスクとシステム ヘルス チェックを実行します。

手順

ステップ 1 変更するノードの CLI にログインします。

ステップ 2 **set network hostname** と入力します。

ステップ 3 ホスト名、IP アドレス、またはデフォルト ゲートウェイを変更するためのプロンプトに従います。

a) 新しいホスト名を入力し、**Enter** キーを押します。
b) IP アドレスも変更する場合は、**yes** と入力します。その他の場合は、ステップ 4 に進みます。
c) 新しい IP アドレスを入力します。
d) サブネット マスクを入力します。
e) ゲートウェイのアドレスを入力します。

ステップ 4 入力内容がすべて正しいことを確認し、**yes** と入力して、プロセスを開始します。

次のタスク

導入の変更が正しく実行されていることを確認するすべての該当する変更後の作業を実行します。

（注） 新しいホスト名が正しいIPアドレスに解決されない場合は、次の手順に進まないでください。

クラスタが CA 署名付き証明書を使用する場合は、証明書に再署名する必要があります。

このプロセスを使用してクラスタを混合モードにした場合は、CTL クライアントを実行して CTL ファイルを更新します。 トークンレス CTL 機能を使用した場合は、CLI コマンドの **utils ctl update CTLFile** を実行します。

Set Network Hostname の CLI 出力例

（注） vNIC を vcenter から変更する必要がある場合は、次の出力に示すように、ステップ 4/5 のコンポーネント通知スクリプト regenerate_all_certs.sh の後に vNIC を更新します。

```
 admin:set network hostname ctrl-c: To quit the input. *** W A R N I N G ***
Do not close this window without first canceling the command. This command will
 automatically restart system services. The command should not be issued during
 normal operating hours. ======================================================
 Note: Please verify that the new hostname is a unique name across the cluster
 and, if DNS services are utilized, any DNS configuration is completed before
 proceeding. ====================================================== Security
 Warning : This operation will regenerate all CUCM Certificates including any
 third party signed Certificates that have been uploaded. Enter the hostname::
 newHostname Would you like to change the network ip address at this time
[yes]:: Warning: Do not close this window until command finishes. ctrl-c: To
quit the input. *** W A R N I N G ***
====================================================== Note: Please verify
that the new ip address is unique across the cluster.
====================================================== Enter the ip address::
 10.10.10.28 Enter the ip subnet mask:: 255.255.255.0 Enter the ip address of
 the gateway:: 10.10.10.1 Hostname: newHostname IP Address: 10.10.10.28 IP
Subnet Mask: 255.255.255.0 Gateway: 10.10.10.1 Do you want to continue [yes/no]?
 yes calling 1 of 5 component notification script: ahostname_callback.sh Info(0):
 Processnode query returned = name ========== bldr-vcm18 updating server table
 from:'oldHostname', to: 'newHostname' Rows: 1 updating database, please wait
 90 seconds updating database, please wait 60 seconds updating database, please
 wait 30 seconds Going to trigger /usr/local/cm/bin/dbl updatefiles
--remote=newHostname,oldHostname calling 2 of 5 component notification script:
 clm_notify_hostname.sh notification Verifying update across cluster nodes...
 platformConfig.xml is up-to-date: bldr-vcm21 cluster update successfull calling
 3 of 5 component notification script: drf_notify_hostname_change.py calling
4 of 5 component notification script: regenerate_all_certs.sh calling 5 of 5
component notification script: update_idsenv.sh calling 1 of 2 component
notification script: ahostname_callback.sh Info(0): Processnode query returned
 = name ==== Going to trigger /usr/local/cm/bin/dbl updatefiles
--remote=10.10.10.28,10.67.142.24 calling 2 of 2 component notification script:
 clm_notify_hostname.sh Verifying update across cluster nodes... Shutting down
 interface eth0:
```

IP アドレスのみの変更

（注） リリース 14SU3 以降では、CLI を使用して IP アドレスを変更すると、Service Manager サービスが再起動されます。

CLI を使用してノードの IP アドレスを変更できます。

ノードがホスト名または FQDN で定義されている場合、変更を加える前に DNS のみを更新する必要があります（DNS を使用している場合）。

（注） IM and Presence Service の場合：

- 最初に IM and Presence データベース パブリッシャ ノードを変更して確認します。
- IM and Presence Service サブスクライバ ノードは、同時にまたは 1 つずつ変更できます。

始める前に

導入環境で変更前タスクとシステム ヘルス チェックを実行します。

手順

ステップ 1 変更するノードの CLI にログインします。

ステップ 2 **set network ip eth0***new-ip_address new_netmask new_gateway* を入力して、ノードの IP アドレスを変更します。

（注） **set network ip eth0** コマンドのみを使用して IP アドレスを変更した場合、証明書の再生成はトリガーされません。

ここで、*new_ip_address* は新しいサーバ IP アドレスを指定し、*new_netmask* は新しいサーバ ネットワーク マスクを指定します。また、*new_gateway* はゲートウェイ アドレスを指定します。

次の出力が表示されます。

```
admin:set network ip eth0 10.53.57.101 255.255.255.224 10.53.56.1 WARNING:
Changing this setting will invalidate software license on this server. The
license will have to be re-hosted. Continue (y/n)?
```

ステップ 3 CLI コマンドの出力を確認します。 **はい** を入力して、**確定** を押して処理を開始します。

次のタスク

導入の変更が正しく実行されていることを確認するすべての該当する変更後の作業を実行します。

ネットワーク IP アドレスの設定の出力例

（注） vNIC を vcenter から変更する必要がある場合は、次の出力に示すように、ステップ 3/6 のコンポーネント通知スクリプト aetc_hosts_verify.sh の後に vNIC を更新します。

```
admin:set network ip eth0 10.77.30.34 255.255.255.0 10.77.30.1 *** W A R N I
N G *** This command will restart system services
======================================================= Note: Please verify
that the new ip address is unique across the cluster and, if DNS services are
 utilized, any DNS configuration is completed before proceeding.
======================================================= Continue (y/n)?y calling
 1 of 6 component notification script: acluster_healthcheck.sh calling 2 of 6
 component notification script: adns_verify.sh No Primary DNS server defined
No Secondary DNS server defined calling 3 of 6 component notification script:
 aetc_hosts_verify.sh calling 4 of 6 component notification script: afupdateip.sh
 calling 5 of 6 component notification script: ahostname_callback.sh Info(0):
 Processnode query returned using 10.77.30.33: name ==== calling 6 of 6 component
 notification script: clm_notify_hostname.sh
```

CLI による IP アドレスまたはホスト名の変更

CLIを使用して、展開内のパブリッシャ ノードとサブスクライバノードの DNS IP アドレスを変更することができます。 この手順は、Unified Communications Manager のパブリッシャ ノードとサブスクライバ ノード、および IM and Presence Service クラスタの両方に適用されます。

（注） DNS サーバー レコードに何か変更がある場合、または DNS サーバー自体に変更がある場合、ユーザーは nscd サービスを再起動する必要があります。 この再起動によって、キャッシュ レコードがクリアされ、新しいレコードがキャッシュにロードされます。

始める前に

導入環境で変更前タスクとシステム ヘルス チェックを実行します。

手順

ステップ 1 変更するノードの CLI にログインします。

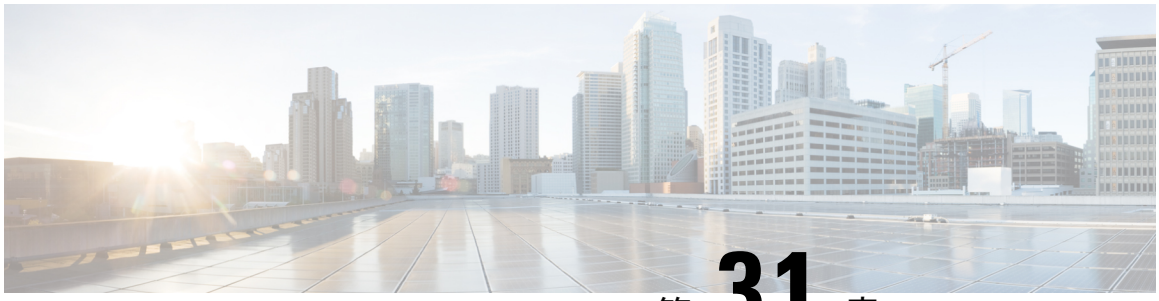
ステップ 2 `set network dns primary/secondary <new IP address of the DNS>` と入力します。

（注） DNS サーバの IP アドレスを変更した場合は、CLI コマンド **utils system restart** を使用してサーバを再起動する必要があります。

以下の出力が表示されます。

```
admin:set network dns primary/secondary <new IP address of DNS> *** W A R N I
 N G *** This will cause the system to temporarily lose network connectivity
```

ステップ 3 CLI コマンドの出力を確認します。 はい を入力して、**確定**を押して処理を開始します。



第 31 章

ドメイン名およびノード名の変更

ドメイン名の変更

管理者は、IM and Presence Service ノードまたはノード グループに関連付けられたネットワーク レベルの DNS デフォルト ドメインを変更できます。

企業全体の IM and Presence Service ドメインは、IM and Presence Service ノードの DNS デフォルト ドメインと対応している必要はありません。導入環境で全社的なドメインを変更するには、『*Deployment Guide for IM and Presence Service on Cisco Unified Communications ManagerIM and Presence Service*の設定および管理ガイド』を参照してください。

注意 IM and Presence Service クラスタ内のノードのデフォルト ドメインを変更すると、ノードが再起動し、プレゼンス サービスやその他のシステム機能が中断されます。 システムにこのような影響があることから、このドメイン変更手順は、スケジュールしたメンテナンス時間の中で実行する必要があります。

ノードのデフォルト ドメイン名を変更すると、すべてのサードパーティの署名済みセキュリティ証明書が新しい自己署名証明書によって自動的に上書きされます。 これらの証明書をサードパーティの認証局によって再署名するには、新しい証明書を手動で要求してアップロードする必要があります。 こうした新しい証明書を有効にするには、サービスの再起動が必要になることがあります。 新しい証明書の要求に要する時間によっては、メンテナンス時間を別途設定して、サービスの再起動スケジュールを設定することが必要になる場合もあります。

（注） ノードのデフォルト ドメイン名を変更する前に、新しい証明書を要求することはできません。証明書署名要求（CSR）の生成は、ノードでドメインを変更し、そのノードを再起動した後にのみ可能です。

IM and Presence サービスのデフォルト ドメイン名の変更作業

次の表に、IM and Presence Service ノードまたはノード グループに関連付けられたネットワーク レベル DNS デフォルト ドメイン名を変更するためのステップごとの手順を示します。 この手順の詳しい説明では、クラスタにある複数のノードに対する変更を実行するステップの正確な順序を指定しています。

複数のクラスタにわたってこの手順を実行する場合は、順番に一度に 1 つのクラスタで変更を完了する必要があります。

（注） この手順の各タスクは、この表に示された順序どおりに実行する必要があります。

手順

ステップ 1 クラスタ内のすべての該当するノードで変更前の作業を完了します。 変更前の作業の一部は IM and Presence データベース パブリッシャ ノードだけに適用し、サブスクライバ ノードを変更する場合はスキップすることができます。

ステップ 2 クラスタ内のすべての該当するノードで、IM and Presence Service ノードの DNS レコードを更新します。 SRV、順方向（A）、および逆方向（PTR）の各レコードも必要に応じて更新し、新しいノード ドメインを取り入れます。

ステップ 3 Cisco Unified Communications Manager Administration を使用して、クラスタ内のすべての該当するノードで、IM and Presence Service ノード名を更新します。

（注） ノード名が FQDN 形式の場合、この手順は必須です。 ノード名が IP アドレスまたはホスト名の場合、この手順は適用されません。

- ノード名が FQDN の場合、古いノードのドメイン名が参照されます。したがって、FQDN 値が新しいドメイン名を反映するようにノード名を更新する必要があります。
- ノード名が IP アドレスまたはホスト名の場合は、ドメインを参照していないので、何の変更も必要ありません。

ステップ 4 コマンドライン インターフェイス（CLI）を使用して、すべての該当するノードで DNS ドメインを更新します。 CLI コマンドは、ノードのオペレーティング システムで必要なドメイン変更を行い、各ノードの自動リブートを実行します。

ステップ 5 ドメイン名の更新後、クラスタ内のすべてのノードの「A Cisco DB」サービスを再起動して、すべてのノードのオペレーティング システムの設定ファイルで、変更されたノードに関連付けられた DNS ドメイン名の変更が確実に有効になるようにします。

（注） システムが正しく機能していることを確認します。 レプリケーションの問題が発生した場合は、クラスタ内のすべてのノードを再起動してください。

ステップ 6 CLI を使用してデータベース レプリケーションを確認します。 詳細については、システム ヘルス チェックの実行およびデータベース レプリケーションのトラブルシューティングに関連

したトピックを参照してください。 クラスタにあるすべてのシステム ファイルが互いに同期した後で、データベースのレプリケーションを確認する必要があります。

ステップ 7 ノードのセキュリティ証明書を再生成します。

- すべての IM and Presence Service のセキュリティ証明書で、件名 CN がノード FQDN に設定されます。 したがって、新しいノード ドメインを取り入れるために、DNS ドメインの変更後は、すべての証明書が自動的に再生成されます。
- 証明書によって以前に署名された証明書。

ステップ 8 クラスタ内の該当するすべてのノードで変更後タスクを実行し、クラスタが正常に動作することを確認します。

DNS レコードの更新

ノードの DNS ドメインを変更するため、そのノードに関連付けられているすべての既存の DNS レコードを更新する必要があります。 この対象となるレコードは、次のタイプのレコードです。

- A レコード
- PTR レコード
- SRV レコード

クラスタにある複数のノードを変更する場合は、それらのノードごとに以下の手順を実行する必要があります。

IM and Presence データベース パブリッシャ ノードを変更する場合、該当する IM and Presence Service サブスクライバ ノードで手順を繰り返す前に、IM and Presence データベース パブリッシャ ノードでこの手順が完了している必要があります。

（注）
- これらの DNS レコードの更新は、ノードでの DNS ノードの変更そのものを実行したメンテナンス時間の中で実行する必要があります。
- スケジュールされているメンテナンス時間の前に DNS レコードを更新すると、IM and Presence Service の機能に影響が及ぶ可能性があります。

始める前に

導入ですべての変更前のタスクと該当するシステム ヘルス チェックを実行します。

手順

ステップ 1 ノードの古い DNS 順方向（A）レコードを、古いドメインから削除します。

ステップ 2 新しいドメインに、このノードの新しい DNS 順方向（A）レコードを作成します。

ステップ 3 このノードの DNS 逆方向（PTR）レコードを更新し、ノードの更新された完全修飾ドメイン名（FQDN）を指すようにします。

ステップ 4 このノードを指している DNS SRV レコードをすべて更新します。

ステップ 5 このノードを指している他の DNS レコードをすべて更新します。

ステップ 6 各ノードでコマンドライン インターフェイス（CLI）コマンドを実行して、クラスタにある他のすべてのノードに上記の DNS の変更がすべて伝播されていることを確認します。

a) 新しい A レコードを検証するには、**utils network host new-fqdn** を入力します。ここで、`new-fqdn` はノードの更新 FQDN です。

例：

```
admin: utils network host server1.new-domain.com Local Resolution:
server1.new-domain.com resolves locally to 10.53.50.219 External Resolution:
 server1.new-domain.com has address 10.53.50.219
```

b) 更新 PTR レコードを検証するには、**utils network host ip-addr** を入力します。ここで、`ip-addr` はノードの IP アドレスです。

```
admin: utils network host 10.53.50.219 Local Resolution: 10.53.50.219
resolves locally to server1.new-domain.com External Resolution:
server1.new-domain.com has address 10.53.50.219 219.50.53.10.in-addr.arpa
domain name pointer server1.new-domain.com.
```

（注） 手順のこの時点では、ノードの DNS ドメインを変更しない限り、IP アドレスの**ローカル解決**は古い FQDN を指したままになっています。

c) 更新された SRV レコードを検証するには、**utils network host srv-name srv** を入力します。ここで、`srv-name` は SRV レコードです。

例：

_xmpp-server SRV レコード検索の例。

```
admin: utils network host _xmpp-server._tcp.galway-imp.com srv Local
Resolution: Nothing found External Resolution: _xmpp-server._tcp.sample.com
 has SRV record 0 0 5269 server1.new-domain.com.
```

次のタスク

IM and Presence Service ノード名を更新します。

FQDN 値での ノード名の更新

Cisco Unified CM IM and Presence 管理 GUI の [プレゼンストポロジ（Presence Topology）] ウィンドウのノード用に定義されたノード名が、ノードの完全修飾ドメイン名（FQDN）に設定されている場合、古いドメイン名が参照されます。したがって、新しいドメイン名を参照するようにノード名を更新する必要があります。

（注） この手順は、このノードのノード名の値がFQDNに設定されている場合にのみ実行する必要があります。 ノード名がノードの IP アドレスまたはホスト名と一致している場合、この手順は不要です。

クラスタにある複数のノードを変更する場合は、それらのノードごとに以下の手順を順番に実行する必要があります。

IM and Presence データベース パブリッシャ ノードを変更する場合、IM and Presence Service サブスクライバ ノードで以下の手順を最初に完了してから、パブリッシャ ノードの手順を完了する必要があります。

始める前に

ノードの DNS レコードを更新します。

手順

ステップ 1 IM and Presence Service ノードのノード名を変更します。

a) Cisco Unified Communications Manager Administration にサイン インします。
b) **[システム（System）]** > **[サーバ（Server）]** を選択します。
c) ノードを検索して選択します。
d) FQDN が新しいドメイン値を参照するように [完全修飾ドメイン名/IP アドレス（Fully Qualified Domain Name/IP Address）]フィールドを更新します。 たとえば、[完全修飾ドメイン名/IP アドレス（Fully Qualified Domain Name/IP Address）]の値を `server1.old-domain.com` から `server1.new-domain.com` に更新します。
e) **保存**を選択します。

ステップ 2 Cisco Unified CM IM and Presence Administration GUI の **[プレゼンス トポロジ（Presence Topology）]** ウィンドウで、このノードのアプリケーション サーバのエントリが、新しいノード名を反映して更新されていることを確認します。

a) Cisco Unified Communications Manager Administration にサインインし、**[システム（System）]** > **[アプリケーション サーバ（Application Server）]** を選択します。
b) **[アプリケーションサーバの検索/一覧表示（Find and List Application Servers）]** ウィンドウで、必要に応じて、**[検索（Find）]** をクリックします。
c) アプリケーション サーバのリストに、更新したノード名に対してエントリが存在することを確認します。

（注） このノードのエントリが存在しない場合、またはそのエントリがあっても、ノードの古いノード名を反映している場合は、以降の手順には進まないでください。

次のタスク

該当するすべてのノードで DNS ドメインを更新します。

DNS ドメインの更新

コマンドライン インターフェイス（CLI）を使用して、IM and Presence Service ノードの DNS ドメインを変更できます。

全社的な IM and Presence Service のドメインは、IM and Presence Service ノードのネットワーク レベルの DNS デフォルト ドメインに対応している必要はありません。 導入環境で企業全体のドメインを変更するには、『*Deployment Guide for IM and Presence Service on Cisco Unified Communications Manager*』を参照してください。

クラスタ内で複数のノードを変更する場合、ノードごとに以下の手順を順番に実行する必要があります。

IM and Presence データベース パブリッシャ ノードを変更する場合、サブスクライバ ノードを変更する前に、まずデータベースパブリッシャ ノードでこの手順を実行する必要があります。

始める前に

IM and Presence Service ノード名を更新します。

手順

ステップ 1 ノードで CLI にサイン インし、**set network domain new-domain** と入力します。new-domain は設定される新しいドメインの値です。

例：

```
admin: set network domain new-domain.com *** W A R N I N G *** Adding/deleting
 or changing domain name on this server will break database replication. Once
 you have completed domain modification on all systems that you intend to
modify, please reboot all the servers in the cluster. This will ensure that
replication keeps working correctly. After the service is rebooted, please
confirm that there are no issues reported on the Cisco Unified Reporting report
 for Database Replication. The server will now be rebooted. Do you wish to
continue. Security Warning : This operation will regenerate all CUP Certificates
 including any third party signed Certificates that have been uploaded. Continue
 (y/n)?
```

ステップ 2 ドメインの変更を確認してノードをリブートする場合は **y** と入力して**リターン** キーを押し、キャンセルする場合は **n** と入力します。

ヒント ノード名の変更が完了すると、すべての証明書がノードで再生成されます。これらの証明書の中に、サードパーティの認証局で署名したものがある場合、この手順の後半で、それらの署名済み証明書を再度要求する必要があります。

ステップ 3 ノードが再起動したら、`show network eth0` と入力して、ドメイン名の変更が有効になっていることを確認します。

例：

次の例での新しいドメインは new-domain.com です。

```
admin: show network eth0 Ethernet 0 DHCP : disabled Status : up IP Address :
10.53.50.219 IP Mask : 255.255.255.000 Link Detected: yes Mode : Auto disabled,
 Full, 1000 Mbits/s Duplicate IP : no DNS Primary : 10.53.51.234 Secondary :
Not Configured Options : timeout:5 attempts:2 Domain : new-domain.com Gateway
 : 10.53.50.1 on Ethernet 0
```

ステップ 4 クラスタ内のすべての該当するノードに対して前の手順を繰り返して行います。

次のタスク

クラスタのすべてのノードをリブートします。

クラスタ ノードに関する考慮事項

コマンドライン インターフェイス（CLI）を使用して、クラスタ内のノードで「A Cisco DB」サービスを再起動できます。

ドメイン名を変更してノードを再起動したら、自動的に再起動したノードを含む、クラスタ内のすべてのノードの「A Cisco DB」サービスを再起動する必要があります。Unified CM Publisher から始めて、公開されたデータベースが表示されると、すべてのサブスクライバに適用されます。 これによって、すべてのノードで、オペレーティング システムのコンフィギュレーション ファイルを、新しいドメインの値に一致したものにすることができます。

システムが正しく機能していることを確認します。 レプリケーションの問題が発生した場合は、クラスタ内のすべてのノードを再起動してください。

最初に IM and Presence データベース パブリッシャ ノードのリブート プロセスを開始します。データベース パブリッシャ ノードが再起動したら、次に残りの IM and Presence Service サブスクライバ ノードのリブートを任意の順序で実行します。

始める前に

ノードの DNS ドメイン名が変更されたことを確認します。

手順

ステップ 1 CLI を使用して IM and Presence データベース パブリッシャ ノードをリブートします。 **utils system restart** を入力します。

例：

```
admin: utils system restart Do you really want to restart ? Enter (yes/no)?
```

ステップ 2 **yes** を入力して、再起動して **Return** キーを押します。

ステップ 3 IM and Presence データベース パブリッシャ ノードが再起動したことを示す次のメッセージが表示されるまで待ちます。

例：

```
Broadcast message from root (Wed Oct 24 16:14:55 2012): The system is going
down for reboot NOW! Waiting . Operation succeeded restart now.
```

ステップ 4 各 IM and Presence Service サブスクライバ ノードの CLI にサインインし、**utils system restart** を入力して各サブスクライバ ノードをリブートます。

（注） サービスの停止を試行してから数分が経過すると、CLI から再起動するよう求められることがあります。 その場合は **yes** を入力します。

次のタスク

データベースのレプリケーションを確認します。 詳細については、システム ヘルス チェックに関するトピックを参照してください。

セキュリティ証明書の再生成

ノードの完全修飾ドメイン名（FQDN）は、すべての IM and Presence Service セキュリティ証明書で件名 CN として使用されます。 したがって、ノードで DNS ドメインを更新すると、すべてのセキュリティ証明書が自動的に再生成されます。

いずれかの証明書にサードパーティの認証局が署名していた場合は、認証局が署名した証明書を新たに手動で生成する必要があります。

クラスタにある複数のノードを変更する場合は、ノードごとに以下の手順を実行する必要があります。

（注） ノードのデフォルト ドメイン名を変更する前に、新しい証明書を要求することはできません。証明書署名要求（CSR）の生成は、ノードでドメインを変更し、そのノードを再起動した後にのみ可能です。

始める前に

データベース レプリケーションがすべてのノードで正常に確立されるように、データベース レプリケーションを確認します。

手順

ステップ 1 証明書にサードパーティの認証局による署名が必要な場合は、Cisco Unified Operating System Administration GUI にサインインし、関連する証明書ごとに必要な手順を実行します。

ステップ 2 署名付き証明書をアップロードしたら、IM and Presence Service ノードでサービスの再起動が必要になることがあります。

再起動が必要になるサービスは次のとおりです。

- Tomcat 証明書：次のコマンドライン インターフェイス（CLI）のコマンドを実行して、Tomcat サービスを再起動します。

  ```
  utils service restart Cisco Tomcat
  ```

- CUP-xmpp 証明書：Cisco Unified Serviceability GUI から Cisco XCP Router サービスを再起動します。
- Cup-xmpp-s2s 証明書：Cisco Unified Serviceability GUI から Cisco XCP Router サービスを再起動します。

（注）
- これらのアクションによって、影響を受けるサービスが再起動します。 したがって、署名済み証明書を入手するまでに要する時間に応じて、再起動をより遅いメンテナンス時間でスケジュールする必要が生じる場合があります。 サービスを再起動するまでの間は、暫定的に自己署名の証明書が関連のインターフェイスに引き続き提示されます。
- 上記のリストで指定されていない証明書では、サービスの再起動は不要です。

次のタスク

クラスタ内のすべての該当するノードで、変更後のタスク リストを実行します。

ノード名の変更

IM and Presence Service ノードまたはノード グループに関連付けられたノード名を変更できます。 更新は、[Cisco Unified Communications Manager Administration]の **[サーバの設定（Server Configuration）]** ウィンドウに表示されます。

次のノード名変更シナリオでこれらの手順を使用します。

- IP アドレスからホスト名へ

- IP アドレスから完全修飾ドメイン名（FQDN）へ
- ホスト名から IP アドレスへ
- ホスト名から FQDN へ
- FQDN からホスト名へ
- FQDN から IP アドレスへ

ノード名の推奨事項について詳しくは、『*Deployment Guide for IM and Presence Service on Cisco Unified Communications Manager*』を参照してください。

注意 ネットワーク レベルの変更が必要とされていない IM and Presence Service ノードでのみノード名を変更するには、以下の手順を使用します。 その場合は、ネットワーク IP アドレス、ホスト名、またはドメイン名の変更に固有の手順を実行します。 このノード名の変更手順は、スケジュールしたメンテナンス時間内に実行する必要があります。 IM and Presence Service クラスタでいずれかのノードのノード名を変更すると、ノードが再起動し、Presence サービスやその他のシステム機能に割り込みます。

IM and Presence Service ノード名の変更作業リスト

次の表に、IM and Presence Service ノードまたはノード グループに関連付けられたノード名を変更するためのステップごとの手順を示します。 この手順の詳しい説明では、変更を実行するステップの正確な順序を指定しています。

複数のクラスタにわたってこの手順を実行する場合は、順番に一度に 1 つのクラスタでノード名を変更する手順を完了します。

表 *84 : IM and Presence Service* ノード名の変更の作業リスト

項目	タスク
1	クラスタ内のすべての該当するノードで変更前の作業を完了します。 変更前の作業の一部は IM and Presence データベース パブリッシャ ノードだけに適用し、サブスクライバ ノードを変更する場合はスキップすることができます。
2	Cisco Unified Communications Manager Administration を使用して、IM and Presence Service ノード名を更新します。
3	ノード名の更新を確認し、ノード名の変更が IM and Presence Service と確実に同期されるようにします。
4	ノード名の更新の完了後に、コマンドライン インターフェイス（CLI）を使用してデータベース レプリケーションを確認します。 新しいノード名がクラスタで複製されていることと、データベース レプリケーションがすべてのノードで動作することを確認します。

項目	タスク
5	更新されたノードで変更後の作業リストを完了し、ノードが正常に動作することを確認します。

ノード名の更新

クラスタにある複数のノードを変更する場合は、それらのノードごとに以下の手順を順番に実行する必要があります。

IM and Presence データベース パブリッシャ ノードを変更する場合、IM and Presence Service サブスクライバ ノードで以下の手順を最初に完了してから、パブリッシャ ノードの手順を完了する必要があります。

（注） IM and Presence ノードの場合、完全修飾ドメイン名を使用することを推奨します。ただし、IP アドレスとホスト名もサポートされています。

始める前に

導入環境で、すべての変更前タスクと該当するシステム ヘルス チェックを実行します。

手順

ステップ 1 [Cisco Unified CM 管理] ページにサインインします。

ステップ 2 **[システム（System）]** > **[サーバ（Server）]** を選択します。

ステップ 3 変更するノードを選択します。

ステップ 4 [**ホスト名/IP アドレス（Host Name/IP Address**）] フィールドを新しいノード名で更新します。

（注） 新しく生成した SP メタデータを IDP サーバに確実にアップロードします。

ステップ 5 クラスタ内の複数のノードを変更する場合は、ノードごとにこの手順を繰り返して行います。

（注） IM and Presence Service ノード名を更新する際に、サードパーティのコンプライアンスも設定されている場合は、ノード名に基づく新しいレルムを使用するようにコンプライアンスサーバを更新する必要があります。この設定の更新は、サードパーティのコンプライアンスサーバで行われます。 新しいレルムは、**[Cisco Unified CM IM and Presence Administration]** > **[メッセージング（Messaging）]** > **[コンプライアンス（Compliance）]** > **[コンプライアンス設定（Compliance Settings）]** ウィンドウに表示されます。

次のタスク

ノード名の変更を確認します。

CLI を使用したノード名の変更の確認

コマンドライン インターフェイス（CLI）を使用して、新しいノード名がクラスタ全体にわたって複製されたことを確認できます。

手順

ステップ 1 新しいノード名がクラスタ内の各ノードで正しく複製されていることを検証するには、**run sql name select from processnode** と入力します。

例：

```
admin:run sql select name from processnode name ====================
EnterpriseWideData server1.example.com server2.example.com server3.example.com
 server4.example.com
```

ステップ 2 クラスタのノードごとに新しいノード名を指定するエントリが存在し、古いノード名が出力に表示されていないことを確認してください。

a) 出力が期待どおりである場合、検証は成功しており、ノードのデータベース レプリケーションを検証する必要はありません。

b) 新しいノード名が欠落しているか、古いノード名への参照が存在する場合は、ステップ 3 に進みます。

ステップ 3 欠落したノード名や、ノードに表示される古いノード名をトラブルシューティングするには、以下の操作を実行します。

a) IM and Presence データベース パブリッシャ ノードの場合は、Cisco Unified CM IM and Presence Administration GUI でダッシュボードを使用して、Sync Agent が正常に実行中であることと、Sync Agent の状態にエラーが発生していないことを確認します。

b) サブスクライバ ノードの場合は、データベース レプリケーションの検証手順を実行します。

Cisco Unified CM IM and Presence Administration を使用したノード名の変更の検証

IM and Presence Service ノードのみに対して、Cisco Unified CM IM and Presence Administration GUI で、このノードのアプリケーション サーバのエントリが新しいノード名を反映して更新されていることを確認します。

始める前に

IM and Presence Service ノード名を更新します。

手順

ステップ 1 Cisco Unified CM IM and Presence Administration GUI にサイン インします。

ステップ 2 **[システム（System）][プレゼンス トポロジ（Presence Topology）]** を選択します。

ステップ 3 新しいノード名が既存の[プレゼンス トポロジ（Presence Topology）] ペインに表示されていることを確認します。

次のタスク

データベースのレプリケーションを確認します。

Cisco Unified Communications Manager のドメイン名の更新

CLI (コマンド ライン インターフェイス) を使用して、Cisco Unified Communications Manager のドメイン名を変更できます。 CLI を使用して、すべての該当するノードで DNS ドメイン名を更新します。 CLI コマンドは、ノードで必要なドメイン名変更を行い、各ノードの自動リブートを実行します。

Unified CM クラスタのセキュリティモードが非セキュアであり、ドメインを更新または変更する場合、ドメイン変更の一環としてすべての証明書が再生成されます。 電話機の ITL を更新するために、ドメイン名を変更する前に次の手順を行ってください。

1. 更新された ITL を処理できるようにすべての電話機が登録され、オンラインであることを確認します。 この手順を実行するときに電話機がオンラインでない場合は、ITL を手動で削除する必要があります。
2. **Prepare Cluster for Rollback to pre-8.0 えんたーぷらいず** パラメータを **True** に設定します。 すべての電話機は自動的にリセットされ、空の信頼検証サービス（TVS）と TFTP 証明書セクションを含む ITL ファイルがダウンロードされます。
3. 電話機で、**[設定（Settings）] > [セキュリティ（Security）] > [信頼リスト（Trust List）] > [ITL ファイル（ITL File）]** の順に選択し、ITL ファイルの TVS および TFTP 証明書セクションが空であることを確認します。
4. サーバのドメインを変更し、クラスタへの登録がロールバックされるように電話機を設定します。
5. すべての電話機がクラスタに正常に登録されたら、エンタープライズパラメータ **Prepare Cluster for Rollback to pre-8.0** を **False** に設定します。

始める前に

- ドメイン名を変更する前に、必ず DNS を有効にします。

- Cisco Unified Communications Manager Administration にサインインし、**[システム（System）] > [サーバーフィールド（Server Fields）]** ページに移動します。 このサーバー構成設定ページに既存のホスト名エントリがある場合は、最初にドメイン名のホスト名エントリを変更する必要があります。
- すべての変更前タスクと該当するシステム ヘルス チェックを実行します。 詳細については、「関連項目」を参照してください。

手順

ステップ 1 コマンド ライン インターフェイスにログインします。

ステップ 2 **run set network domain<new_domain_name>** と入力します。
コマンドからシステム リブートの確認が求められます。

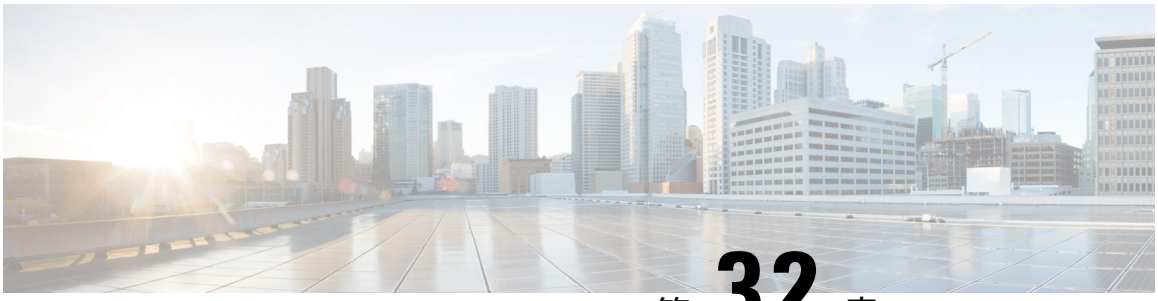
ステップ 3 [はい（Yes）]をクリックしてシステムをリブートします。
システムがリブートした後、新しいドメイン名が更新されます。

ステップ 4 コマンド **show network eth0** を入力して、リブート後に新しいドメイン名に更新されたことを確認します。

ステップ 5 すべてのクラスタ ノードに対してこの手順を繰り返します。

次のタスク

導入の変更が正しく実行されていることを確認するすべての該当する変更後の作業を実行します。



第 32 章

変更後のタスクと検証

Cisco Unified Communications Manager ノードの変更後タスク

変更後タスクすべてを実行し、導入環境に変更が適切に実装されていることを確認してください。

注意 これらのタスクを実行しても期待する結果が得られない場合は、問題が解決されるまで続行しないでください。

手順

ステップ 1 Cisco Unified Communications Manager サーバ内で DNS が設定されている場合、正引きおよび逆引き参照ゾーンが設定され、DNS が到達可能で作動していることを確認します。

ステップ 2 アクティブな ServerDown 警告が出ていないことを確認し、クラスタ内のすべてのサーバが稼働していて利用可能であることを確かめます。 最初のノードで、Cisco Unified Real-Time Monitoring Tool（RTMT） またはコマンド ライン インターフェイス（CLI）のいずれかを使用します。

a) Unified RTMT を使用して確認するには、Alert Central にアクセスし、ServerDown 警告が発生していないか調べます。

b) 最初のノードで CLI を使用して確認するには、次の CLI コマンドを入力してアプリケーションのイベント ログを調べます。

```
file search activelog syslog/CiscoSyslog ServerDown
```

ステップ 3 クラスタにあるすべてのノードでデータベース レプリケーションのステータスを調べ、すべてのサーバがデータベースの変更内容を正常に複製していることを確認します。

IM and Presence Service の場合、導入環境に複数のノードがあるときにはデータベース パブリッシャ ノードでデータベース レプリケーションのステータスを調べます。

Unified RTMT または CLI を使用します。 すべてのノードで **2** のステータスが表示される必要があります。

a) RTMT を使用して確認するには、Database Summary にアクセスしてレプリケーションのステータスを調べます。
b) CLI を使用して確認するには、**utils dbreplication runtimestate** を入力します。

出力例については、データベース レプリケーションの出力例に関するトピックを参照してください。 詳細な手順およびトラブルシューティングについては、データベース レプリケーションおよびデータベース レプリケーションのトラブルシューティングについてのトピックを参照してください。

ステップ 4 次の例に示されているように CLI コマンド **utils diagnose** を入力し、ネットワーク接続と DNS サーバの設定を確認してください。

例：

```
admin: utils diagnose module validate_network Log file:
/var/log/active/platform/log/diag1.log Starting diagnostic test(s)
========================== test - validate_network : Passed Diagnostics
Completed admin:
```

変更前のシステム ヘルス チェックを行っている場合には、これで完了です。そうでない場合には、変更後の確認手順を続行してください。

ステップ 5 Cisco Unified Communications Manager サーバ リストに新しいホスト名または IP アドレスがあることを確認します。 [Cisco Unified CM の管理（Cisco Unified Communications Manager Administration）]で、**[システム（System）]** > **[サーバ（Server）]** を選択します。

（注） このステップは、変更後タスクの一部としてのみ実行します。

ステップ 6 IPアドレス、ホスト名、またはその両方に加えられた変更がネットワーク上で確実に実装されていることを確認します。 クラスタ内の各ノードで CLI コマンド **show network cluster** を入力します。

（注） このステップは、変更後タスクの一部としてのみ実行します。

出力には、ノードの新しい IP アドレスまたはホスト名が含まれている必要があります。

例：

```
admin:show network cluster 10.63.70.125 hippo2.burren.pst hippo2 Subscriber
cups DBPub authenticated 10.63.70.48 aligator.burren.pst aligator Publisher
callmanager DBPub authenticated using TCP since Wed May 29 17:44:48 2013
```

ステップ 7 ホスト名に対する変更内容がネットワークで完全に実装されていることを確認します。クラスタ内の各ノードで CLI コマンド **utils network host<*new_hostname*>** を入力します。

（注） このステップは、変更後タスクの一部としてのみ実行します。

出力で、新しいホスト名が対象 IP アドレスに外部解決されていることを確認してください。

例：

```
admin:utils network host hippo2 Local Resolution: hippo2.burren.pst resolves
locally to 10.63.70.125 External Resolution: hippo2.burren.pst has address
10.63.70.125
```

タスク。

ステップ 8 セキュリティが有効になっているクラスタ（クラスタ セキュリティ モード 1 - 混合）の場合、CTL ファイルを更新し、クラスタ内のすべてのノードを再起動してから、システム ヘルス チェックと他の変更後タスクを実行します。

詳細については、マルチサーバ クラスタ電話機の証明書と ITL の再生成（470 ページ）を参照してください。

ステップ 9 証明書信頼リスト（CTL）ファイルと USB eToken を使用してクラスタ セキュリティを有効にした場合、リリース 8.0 以降のノードの IP アドレスまたはホスト名を変更した際は、Initial Trust List（ITL; 初期信頼リスト）ファイルと ITL の証明書を再生成する必要があります。 クラスタ セキュリティの有効化に証明書信頼リスト（CTL）ファイルと USB eToken を使用していない場合は、このステップをスキップしてください。

ステップ 10 手動で DRS バックアップを実行し、すべてのノードとアクティブなすべてのサービスが正しくバックアップされていることを確認します。

詳細については、『*Administration Guide for Cisco Unified Communications Manager*』を参照してください。

（注） ノードの IP アドレスを変更した後は手動で DRS バックアップを実行する必要があります。これは、DRS ファイルでノードを復元するには、DRS ファイルとノードで IP アドレスとホスト名が一致している必要があるからです。 変更後の DRS ファイルには、新しい IP アドレスや新しいホスト名が記録されています。

ステップ 11 関連する IP フォンの URL パラメータをすべて更新します。

ステップ 12 [Cisco Unified Communications Manager Administration] を使用して、関連するすべての IP フォン サービスを更新します。 **[システム（System）] > [エンタープライズパラメータ（Enterprise Parameters）]** を選択します。

ステップ 13 Unified RTMT カスタム警告と保存済みプロファイルを更新します。

- パフォーマンス カウンタから得られた Unified RTMT カスタム警告には、サーバの IP アドレスがハードコードで記録されています。 これらのカスタム警告を削除し、再設定する必要があります。

- パフォーマンス カウンタを備えた Unified RTMT 保存済みプロファイルには、サーバの IP アドレスがハードコードで記録されています。 これらのカウンタをいったん削除してから追加し直した後、プロファイルを保存して新しい IP アドレスで更新する必要があります。

ステップ 14 Cisco Unified Communications Manager で動作する統合 DHCP サーバを使用している場合は、DHCP サーバを更新します。

ステップ 15 その他の関連する Cisco Unified Communications コンポーネントに対して、必要な設定変更を検査して実行します。

検査対象のコンポーネントの一部を次に示します。

- Cisco Unity
- Cisco Unity Connection
- CiscoUnity Express
- SIP/H.323 トランク
- IOS Gatekeeper
- Cisco Unified MeetingPlace
- Cisco Unified MeetingPlace Express
- Cisco Unified Contact Center Enterprise
- Cisco Unified Contact Center Express
- IP 電話向け DHCP Scopes
- CDR エクスポート用の Cisco Unified Communications Manager のトレース収集、または DRS バックアップの保存先として使用する SFTP サーバ
- Cisco Unified Communications Manager に登録されている IOS ハードウェア リソース（会議ブリッジ、メディア ターミネーション ポイント、トランスコーダ、RSVP エージェント）
- Cisco Unified Communications Manager に登録または統合した IPVC ビデオ MCU
- Cisco Emergency Responder
- Cisco Unified Application Environment
- Cisco Unified Presence
- Cisco Unified Personal Communicator
- 関連するルータおよびゲートウェイ

（注） 必要に応じて設定を変更する方法については、ご使用の製品のマニュアルを参照してください。

Cisco Unified Communications Manager ノードのセキュリティを有効にしたクラスタ タスク

初期信頼リストおよび証明書の再生成

Cisco Unified Communications Manager リリース 8.0 リリース以降のクラスタでサーバの IP アドレスまたはホスト名を変更すると、ITL の初期信頼リスト（ITL）ファイルと証明書が再生成されます。 再生されたファイルは、電話機に保存されたファイルと一致しません。

（注） 証明書信頼リスト（CTL）ファイルと USB eToken を使用してクラスタ セキュリティを有効にする場合は、eToken によって信頼が保持され、eToken は変更されないため、次の手順を実行する必要はありません。

クラスタ セキュリティが有効になっていない場合は、シングルサーバ クラスタまたはマルチサーバ クラスタでこの手順を実行して電話をリセットします。

シングルサーバ クラスタ電話機の証明書と ITL の再生成

Cisco Unified Communications Manager リリース 8.0 以降のシングルサーバ クラスタでサーバの IP アドレスまたはホスト名を変更する際に、ITL ファイルを使用する場合、以下の手順を実行して電話機をリセットします。

サーバの IP アドレスまたはホスト名を変更する前に、ロールバックを有効にします。

手順

ステップ 1 更新された ITL を処理できるようにすべての電話機が登録され、オンラインであることを確認します。 この手順を実行するときに電話機がオンラインでない場合は、ITL を手動で削除する必要があります。

ステップ 2 Prepare Cluster for Rollback to pre-8.0 エンタープライズ パラメータを True に設定します。 すべての電話機は自動的にリセットされ、空の信頼検証サービス（TVS）と TFTP 証明書セクションを含む ITL ファイルがダウンロードされます。

ステップ 3 電話機で、**[設定（Settings）]**>**[セキュリティ（Security）]**>**[信頼リスト（Trust List）]**>**[ITL ファイル（ITL File）]** の順に選択し、ITL ファイルの TVS および TFTP 証明書セクションが空であることを確認します。

ステップ 4 サーバの IP アドレスまたはホスト名を変更し、クラスタへの登録がロールバックされるように電話機を設定します。

ステップ 5 すべての電話機がクラスタに正常に登録されたら、エンタープライズ パラメータ Prepare Cluster for Rollback to pre-8.0 を **False** に設定します。

次のタスク

CTL ファイルまたはトークンを使用する場合は、サーバの IP アドレスまたはホスト名を変更した後、または DNS ドメイン名を変更した後に、CTL クライアントを再実行します。

マルチサーバ クラスタ電話機の証明書と ITL の再生成

マルチサーバ クラスタでは、電話機が、再生成された ITL ファイルおよび証明書を確認するためのプライマリおよびセカンダリ TVS サーバを持つ必要があります。 電話機がプライマリ TVS サーバに（最近の設定変更により）接続できない場合は、セカンダリ サーバにフォールバックされます。 TVS サーバは、電話機に割り当てられた CM グループによって識別されます。

マルチサーバ クラスタでは、一度に 1 つのサーバだけで IP アドレスまたはホスト名を変更するようにしてください。 CTL ファイルまたはトークンを使用する場合は、サーバの IP アドレスまたはホスト名を変更した後、または DNS ドメイン名を変更した後に、CTL クライアントまたは CLI コマンド set **utils ctl** を再実行します。

IM and Presence Service ノードの変更後タスク

変更後タスクすべてを実行し、導入環境に変更が適切に実装されていることを確認してください。

⚠

注意 これらのタスクを実行しても期待する結果が得られない場合は、問題が解決されるまで続行しないでください。

手順

ステップ 1 ホスト名または IP アドレスに対する変更内容が、Cisco Unified Communications Manager サーバ上で更新されていることを確認します。

ステップ 2 変更したノードのネットワーク接続と DNS サーバの設定を確認してください。

（注） 異なるサブネットに IP アドレスを変更した場合は、ネットワーク アダプタが正しい VLAN に接続されていることを確認します。 また、IP アドレスの変更後に IM and Presence Service ノードが別のサブネットに属している場合、Cisco XCP Router サービス パラメータの [ルーティング通信タイプ（Routing Communication Type）] フィールドが [ルータ間（Router to Router）] に設定されていることを確認してください。 その他の場合には、[ルーティング通信タイプ（Routing Communication Type）] フィールドは [マルチキャスト DNS（Multicast DNS）] に設定する必要があります。

ステップ 3 IPアドレス、ホスト名、またはその両方への変更がネットワークで完全に実装されていることを確認してください。

ステップ 4 ホスト名を変更した場合は、ネットワークでホスト名の変更が確実に実装されていることを確認します。

ステップ 5 データベース レプリケーションが正常に確立されたことを確認します。 すべてのノードのステータスが 2 で、[接続済み（Connected）] になっている必要があります。 レプリケーションがセットアップされていない場合、データベース レプリケーションのトラブルシューティングに関するトピックを参照してください。

ステップ 6 SAMLシングルサインオン（SSO）を無効にした場合、ここで有効にできます。 SAML SSOの詳細については、『*Deployment Guide for IM and Presence Service on Cisco Unified Communications Manager*』を参照してください。

ステップ 7 ホスト名を変更した場合、cup、cup-xmpp、およびTomcatの証明書に新しいホスト名が含まれていることを確認する必要があります。

a) Cisco Unified OS Administration GUI から、**[セキュリティ（Security）] > [証明書の管理（Certificate Management）]** を選択します。
b) 信頼証明書の名前に新しいホスト名が含まれていることを確認します。
c) 証明書に新しいホスト名が含まれない場合、証明書を再生成します。

詳細については、『*Administration Guide for Cisco Unified Communications Manager*』を参照してください。

ステップ 8 ノードの IP アドレスを変更したら、Cisco Unified Real-Time Monitoring Tool（RTMT）のカスタム アラートと保存済みプロファイルを更新してください。

- パフォーマンスカウンタから得られたRTMTカスタム警告には、サーバのアドレスがハードコードで記録されています。 これらのカスタム警告を削除し、再設定する必要があります。
- パフォーマンス カウンタを備えた RTMT 保存済みプロファイルには、サーバのアドレスがハードコードで記録されています。 これらのカウンタをいったん削除してから追加し直した後、プロファイルを保存して新しいアドレスで更新する必要があります。

ステップ 9 その他の関連する Cisco Unified Communications のコンポーネント（たとえば Cisco Unified Communications Manager の SIP トランクなど）に必要な設定変更を確認し、変更を行ってください。

ステップ 10 Cisco Unified Serviceability を使用して CUP サービス グループの下にリストされるすべてのネットワーク サービスを開始するには、**[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）]** を選択します。

ヒント IP アドレス、ホスト名、または IP アドレスとホスト名の両方を変更する場合、この手順を実行する必要はありません。 これらの名前を変更した場合、ネットワーク サービスは自動的に開始します。 しかし、変更後に一部のサービスが自動的に開始されない場合には、この手順を実行して、すべてのネットワーク サービスが確実に開始されるようにしてください。

次の順序で CUP サービスのネットワーク サービスを開始する必要があります。

1. Cisco IM and Presence Data Monitor
2. Cisco Server Recovery Manager
3. Cisco Route Datastore
4. Cisco Login Datastore
5. Cisco SIP Registration Datastore
6. Cisco Presence Datastore
7. Cisco XCP Config Manager
8. Cisco XCP Router
9. Cisco OAM Agent
10. Cisco Client Profile Agent
11. Cisco Intercluster Sync Agent
12. Cisco Config Agent

ステップ 11 Cisco Unified Serviceability を使用してすべての機能サービスを開始するには、**[ツール（Tools）]**>**[コントロール センターの機能サービス（Control Center - Feature Services）]** を選択します。機能サービスを開始する順序は重要ではありません。

ヒント IP アドレス、ホスト名、または IP アドレスとホスト名の両方を変更する場合、この手順を実行する必要はありません。これらの名前を変更した場合、機能サービスは自動的に開始します。しかし、変更後に一部のサービスが自動的に開始されない場合には、この手順を実行して、すべての機能サービスが確実に開始されるようにしてください。

ステップ 12 ハイ アベイラビリティを再度有効にする前に Cisco Jabber セッションが再作成されたことを確認します。そうしないと、セッションが作成された Jabber クライアントは接続できなくなります。

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、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。セッションの開始に 30 分以上かかると、システムの問題が大きくなる可能性があります。

ステップ 13 変更前のセットアップ中にハイ アベイラビリティ（HA）を無効にした場合、すべてのプレゼンス冗長グループの HA を有効にします。

ステップ 14 IM and Presence Service が変更後に正しく機能していることを確認します。

a) Cisco Unified Serviceability GUI から、**[システム（System）]**>**[プレゼンス トポロジ（Presence Topology）]** を選択します。

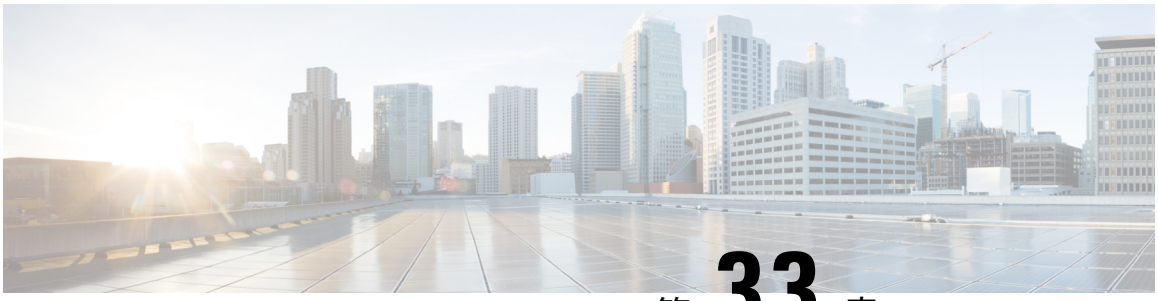
- HA が有効の場合は、すべての HA ノードが [正常（Normal）] 状態であることを確認します。
- すべてのサービスが開始されていることを確認します。

b) Cisco Unified CM IM and Presence Administration GUI からシステム トラブルシュータを実行し、失敗したテストがないことを確認します。**[診断（Diagnostics）]**>**[システム トラブルシュータ（System Troubleshooter）]** を選択します。

ステップ 15 ノードの IP アドレスまたはホスト名を変更した後は、手動でディザスタ リカバリ システム バックアップを実行する必要があります。これは、DRS ファイルでノードを復元するには、

DRS ファイルとノードで IP アドレスとホスト名が一致している必要があるからです。 変更後の DRS ファイルには、新しい IP アドレスや新しいホスト名が記録されています。

詳細については、『*Administration Guide for Cisco Unified Communications Manager*』を参照してください。



第 33 章

アドレス変更に関する問題のトラブルシューティング

クラスタ認証のトラブルシューティング

コマンドライン インターフェイス（CLI）を使用して、サブスクライバ ノードのクラスタ認証問題をトラブルシューティングできます。

手順

ステップ 1 **show network eth0 [detail]** を入力して、ネットワーク設定を確認します。

ステップ 2 **show network cluster** を入力して、ネットワークのクラスタ情報を確認します。

- 誤ったパブリッシャ情報が出力に表示されている場合は、サブスクライバ ノードで **set network cluster publisher [ホスト名/IP アドレス]** CLI コマンドを入力して情報を修正します。
- パブリッシャ ノードで、誤ったサブスクライバ情報が `show network cluster` CLI コマンドに表示される場合、Cisco Unified Communications Manager にログインして、**[システム（System）] > [サーバ（Server）]** を選択し、出力を検査します。
- サブスクライバ ノードで、`show network cluster` の出力に誤ったパブリッシャ情報が表示されている場合は、 `set network cluster publisher [hostname | IP_address]` CLI コマンドを使用して、パブリッシャのホスト名または IP アドレスを変更します。

データベース レプリケーションのトラブルシューティング

コマンドライン インターフェイス（CLI）を使用して、クラスタのノードにおけるデータベース レプリケーションをトラブルシューティングできます。

- データベース レプリケーションがクラスタ内で適切な状態にあることを確認します。
- ノードのデータベース レプリケーションを修復して再確立します。
- データベース レプリケーションをリセットします。

これらのコマンドまたはCLIの使用方法の詳細については、『*Command Line Interface Guide for Cisco Unified Communications Solutions*』を参照してください。

データベース レプリケーションの確認

コマンドライン インターフェイス（CLI）を使用して、クラスタ内のすべてのノードでデータベース レプリケーションのステータスを確認します。 Replication Setup (RTMT) & Details に **2** の値が表示されていることを確認します。 この値が2以外になっている場合は、データベースのレプリケーションに何らかの問題があるので、ノードのレプリケーションをリセットする必要があります。 出力例については、データベース レプリケーションの例に関連したトピックを参照してください。

手順

ステップ 1 クラスタ内のすべてのノードでデータベース レプリケーションを検査するには、最初のノードで **utils dbreplication runtimestate** と入力します。

IM and Presence Service では、導入に複数のノードがある場合、データベース パブリッシャ ノードでこのコマンドを入力します。

ヒント レプリケーションがクラスタ内のノードに設定されていない場合は、CLI を使用してノードのデータベース レプリケーションをリセットできます。 詳細については、CLI を使用したデータベース レプリケーションのリセットに関するトピックを参照してください。

例：

```
admin: utils dbreplication runtimestate DDB and Replication Services: ALL
RUNNING DB CLI Status: No other dbreplication CLI is running... Cluster
Replication State: BROADCAST SYNC Completed on 1 servers at: 2013-09-26-15-18
 Last Sync Result: SYNC COMPLETED 257 tables sync'ed out of 257 Sync Errors:
NO ERRORS DB Version: ccm9_0_1_10000_9000 Number of replicated tables: 257
Repltimeout set to: 300s Cluster Detailed View from PUB (2 Servers): PING
REPLICATION REPL. DBver& REPL. REPLICATION SETUP SERVER-NAME IP ADDRESS (msec)
 RPC? STATUS QUEUE TABLES LOOP? (RTMT) & details ----------- ------------ ------
 ---- ------------ ----- ------ ----- ----------------- server1 100.10.10.17
```

```
0.052 Yes Connected 0 match Yes (2) PUB Setup Completed server2 100.10.10.14
0.166 Yes Connected 0 match Yes (2) Setup Completed
```

ステップ 2 出力を確認します。

出力では、各ノードの REPLICATION STATUS が **Connected**、および REPLICATION SETUP 値が **(2) Setup Complete** として表示される必要があります。 これはクラスタ内のレプリケーション ネットワークが正しく動作していることを意味します。 出力結果が異なる場合は、データベース レプリケーションのトラブルシューティングと修復に進みます。

データベース レプリケーションの CLI 出力例

次のリストは、クラスタの最初のノードで `utils dbreplication runtimestate` コマンドライン インターフェイス（CLI）コマンドを実行した場合に Replicate_State として可能な値を示しています。

IM and Presence Service では、導入に複数のノードがある場合、データベース パブリッシャ ノードでこのコマンドを入力します。

- 0：レプリケーションが開始しません。 これは、サブスクライバが存在していないか、またはサブスクライバをインストールした後に Database Layer Monitor サービスが実行されていないことが原因です。
- 1：レプリケーションは作成されていますが、そのカウントが正しくありません。
- 2：レプリケーションは良好です。
- 3：クラスタ内のレプリケーションは不良です。
- 4：レプリケーションのセットアップに成功しませんでした。

（注） [レプリケーションのセットアップ（RTMT）と詳細（Replication Setup (RTMT) & Details）] に値 2 が示されていることが重要です。 この値が 2 以外になっている場合は、データベースのレプリケーションに何らかの問題があるので、レプリケーションをリセットする必要があります。 データベース レプリケーションの問題の解決方法については、データベース レプリケーションのトラブルシューティングに関するトピックを参照してください。

Cisco Unified Communications Manager ノードの CLI 出力例

この例では、Replication Setup (RTMT) & Details に 2 の値が表示されています。 レプリケーションは良好です。

```
admin: utils dbreplication runtimestate Server Time: Mon Jun 1 12:00:00 EDT 2013
Cluster Replication State: BROADCAST SYNC Completed on 1 servers at:
2013-06-01-12-00 Last Sync Result: SYNC COMPLETED on 672 tables out of 672 Sync
```

```
 Status: NO ERRORS Use CLI to see detail: 'file view activelog
cm/trace/dbl/2013_06_01_12_00_00_dbl_repl_output_Broadcast.log' DB Version:
ccm10_0_1_10000_1 Repltimeout set to: 300s PROCESS option set to: 1 Cluster
Detailed View from uc10-pub (2 Servers): PING Replication REPLICATION SETUP
SERVER-NAME IP ADDRESS (msec) RPC? Group ID (RTMT) & Details -----------
---------- ------ ---- ----------- ------------------- uc10-pub 192.0.2.95
0.040 Yes (g_2) (2) Setup Completed uc10-sub1 192.0.2.96 0.282 Yes (g_3) (2)
Setup Completed
```

IM and Presence Service ノードの CLI 出力例

この例では、Replication Setup (RTMT) & Details に 2 の値が表示されています。 レプリケーションは良好です。

```
admin: utils dbreplication runtimestate Server Time: Mon Jun 1 12:00:00 EDT 2013
DB and Replication Services: ALL RUNNING Cluster Replication State: Replication
 status command started at: 2012-02-26-09-40 Replication status command COMPLETED
 269 tables checked out of 269 No Errors or Mismatches found. Use 'file view
activelog cm/trace/dbl/sdi/ReplicationStatus.2012_02_26_09_40_34.out' to see
the details DB Version: ccm8_6_3_10000_23 Number of replicated tables: 269
Cluster Detailed View from PUB (2 Servers): PING REPLICATION REPL. DBver& REPL.
 REPLICATION SETUP SERVER-NAME IP ADDRESS (msec) RPC? STATUS QUEUE TABLES LOOP?
 (RTMT) & details ----------- ------------ ------ ---- ----------- ----- -------
 ----- ----------------- gwydla020218 10.53.46.130 0.038 Yes Connected 0 match
 Yes (2) PUB Setup Completed gwydla020220 10.53.46.133 0.248 Yes Connected 128
 match Yes (2) Setup Completed
```

データベース レプリケーションの修復

コマンドライン インターフェイス（CLI）を使用して、データベース レプリケーションを修復します。

手順

ステップ 1 最初のノードで **utils dbreplication repair all** と入力し、データベース レプリケーションの修復を試みます。

IM and Presence Service では、導入に複数のノードがある場合、データベース パブリッシャ ノードからデータベース レプリケーションのステータスを修復します。

データベースのサイズによっては、データベース レプリケーションの修復に数分を要することがあります。 次の手順に進み、データベース レプリケーションの修復の進行状況を監視します。

例：

```
admin:utils dbreplication repair all -------------------- utils dbreplication
 repair -------------------- Replication Repair is now running in the background.
 Use command 'utils dbreplication runtimestate' to check its progress Output
will be in file cm/trace/dbl/sdi/ReplicationRepair.2013_05_11_12_33_57.out
Please use "file view activelog
```

```
cm/trace/dbl/sdi/ReplicationRepair.2013_05_11_12_33_57.out " command to see
the output
```

ステップ 2 最初のノードで **utils dbreplication runtimestate** を入力して、レプリケーション修復の進行状況を確認します。

IM and Presence Service では、導入に複数のノードがある場合、データベース パブリッシャ ノードでこのコマンドを入力します。

レプリケーション出力例の太字にされたテキストは、レプリケーション修復の最終ステータスを示しています。

例：

```
admin:utils dbreplication runtimestate DB and Replication Services: ALL RUNNING
 Cluster Replication State: Replication repair command started at:
2013-05-11-12-33 Replication repair command COMPLETED 269 tables processed out
 of 269 No Errors or Mismatches found. Use 'file view activelog
cm/trace/dbl/sdi/ReplicationRepair.2013_05_11_12_33_57.out' to see the details
 DB Version: ccm8_6_4_98000_192 Number of replicated tables: 269 Cluster Detailed
 View from PUB (2 Servers): PING REPLICATION REPL. DBver& REPL. REPLICATION
SETUP SERVER-NAME IP ADDRESS (msec) RPC? STATUS QUEUE TABLES LOOP? (RTMT) &
details ----------- ------------ ------ ---- ----------- ----- ------ -----
----------------- server1 100.10.10.17 0.052 Yes Connected 0 match Yes (2) PUB
 Setup Completed server2 100.10.10.14 0.166 Yes Connected 0 match Yes (2) Setup
 Completed
```

a) レプリケーションの修復がエラーや不一致なしで最後まで実行された場合、ノード名の変更を確認する手順をもう一度実行し、新しいノード名が正常に複製されたことを検証します。

b) エラーまたは不一致が見つかった場合は、ノード間の一時的な不一致が存在する可能性があります。 データベース レプリケーションを修復する手順をもう一度実行します。

（注） レプリケーションの修復を数回試行した後も、不一致またはエラーがレポートされる場合は、シスコのサポート担当者に連絡して問題を解決してください。

ステップ 3 最初のノードで **utils dbreplication reset all** と入力し、データベース レプリケーションの再確立を試みます。

IM and Presence Service では、導入に複数のノードがある場合、データベース パブリッシャ ノードでこのコマンドを入力します。

データベースのサイズによっては、データベース レプリケーションが完全に再確立するのに数分を要することがあります。 次の手順に進み、データベース レプリケーションの再確立の進行状況を監視します。

例：

```
admin:utils dbreplication reset all This command will try to start Replication
 reset and will return in 1-2 minutes. Background repair of replication will
continue after that for 1 hour. Please watch RTMT replication state. It should
 go from 0 to 2. When all subs have an RTMT Replicate State of 2, replication
 is complete. If Sub replication state becomes 4 or 1, there is an error in
replication setup. Monitor the RTMT counters on all subs to determine when
```

```
replication is complete. Error details if found will be listed below OK
[10.53.56.14]
```

ステップ 4 最初のノードで **utils dbreplication runtimestate** を入力して、データベース レプリケーションを再確立する試行の進行状況を監視します。

IM and Presence Service では、導入に複数のノードがある場合、データベース パブリッシャ ノードでこのコマンドを入力します。

すべてのノードで REPLICATION STATUS が **Connected** であり、REPLICATION SETUP 値が **(2) Setup Complete** であれば、レプリケーションは再確立されたと見なされます。

例：

```
admin: utils dbreplication runtimestate DDB and Replication Services: ALL
RUNNING DB CLI Status: No other dbreplication CLI is running... Cluster
Replication State: BROADCAST SYNC Completed on 1 servers at: 2013-09-26-15-18
 Last Sync Result: SYNC COMPLETED 257 tables sync'ed out of 257 Sync Errors:
NO ERRORS DB Version: ccm9_0_1_10000_9000 Number of replicated tables: 257
Repltimeout set to: 300s Cluster Detailed View from newserver100 (2 Servers):
 PING REPLICATION REPL. DBver& REPL. REPLICATION SETUP SERVER-NAME IP ADDRESS
 (msec) RPC? STATUS QUEUE TABLES LOOP? (RTMT) & details -----------
-------------- ------ ---- ----------- ----- ------ ----- -----------------
server1 100.10.10.201 0.038 Yes Connected 0 match Yes (2) PUB Setup Completed
 server2 100.10.10.202 0.248 Yes Connected 0 match Yes (2) Setup Completed
server3 100.10.10.203 0.248 Yes Connected 0 match Yes (2) Setup Completed
server4 100.10.10.204 0.248 Yes Connected 0
```

a) レプリケーションが再確立された場合、ノード名の変更を確認する手順をもう一度実行し、新しいノード名が正常に複製されたことを検証します。

b) レプリケーションが回復しない場合は、シスコのサポート担当者に連絡してこの問題を解決してください。

注意 データベース レプリケーションが切断されている場合は、これより先に進まないでください。

データベース レプリケーションのリセット

レプリケーションがクラスタのノードに設定されていない場合は、データベース レプリケーションをリセットします。コマンドライン インターフェイス（CLI）を使用してデータベース レプリケーションをリセットできます。

始める前に

クラスタにあるすべてのノードでデータベース レプリケーションのステータスを確認します。Replication Setup (RTMT) & Details に 2 の値が表示されていることを確認します。 この値が 2 以外になっている場合は、データベースのレプリケーションに何らかの問題があるので、ノードのレプリケーションをリセットする必要があります。

手順

ステップ 1 クラスタ内のノードでレプリケーションをリセットします。 次のいずれかを実行します。

a) Unified Communications Manager の場合は、**utils db replication reset all** と入力します。

いずれかの Cisco Unified Communications Manager ノードでこの CLI コマンドを実行する前に、まずリセットされているすべてのサブスクライバ ノードで、次にパブリッシャ サーバで **utils dbreplication stop** コマンドを実行します。 詳細については、『*Command Line Interface Guide for Cisco Unified Communications Solutions*』を参照してください。

b) IM and Presence Serviceの場合は、データベース パブリッシャ ノードで **utils db replication reset all** と入力し、クラスタ内のすべての IM and Presence Service ノードをリセットします。

ヒント **all** の代わりに、特定のホスト名を入力して、そのノードだけのデータベース レプリケーションをリセットすることができます。 詳細については、『*Command Line Interface Guide for Cisco Unified Communications Solutions*』を参照してください。

ステップ 2 データベース レプリケーションのステータスを調べるには、**utils dbreplication runtimestate** と入力します。

IM and Presence Service の場合は、IM and Presence データベース パブリッシャ ノードで CLI コマンドを実行します。

ネットワークのトラブルシューティング

コマンドライン インターフェイス（CLI）を使用して、ノードのネットワークの問題をトラブルシューティングできます。

手順

ステップ 1 **show network eth0 [detail]** を入力して、ネットワーク設定を確認します。

ステップ 2 フィールドのいずれかが欠落している場合は、ネットワーク インターフェイスをリセットします。

a) **set network status eth0 down** を入力します。

b) **set network status eth0 up** を入力します。

ステップ 3 IP アドレス、マスク、およびゲートウェイを確認します。

これらの値がネットワーク全体で一意であることを確認します。

Network Time Protocol troubleshooting

サブスクライバ ノードにおける NTP のトラブルシューティング

コマンドライン インターフェイス（CLI）を使用して、サブスクライバ ノードの Network Time Protocol（NTP）の問題をトラブルシューティングできます。

手順

ステップ 1 **show network eth0 [detail]** を入力して、ネットワーク設定を確認します。

ステップ 2 **utils ntp status** を入力して、NTP の状態を確認します。

ステップ 3 **utils ntp restart** を入力して、NTP を再起動します。

ステップ 4 **show network cluster** を入力して、ネットワークのクラスタを確認します。

誤ったパブリッシャ情報が出力に表示される場合は、**set network cluster publisher [hostname/IP_address]** CLI コマンドを使用して、パブリッシャをリセットします。

パブリッシャ ノードにおける NTP のトラブルシューティング

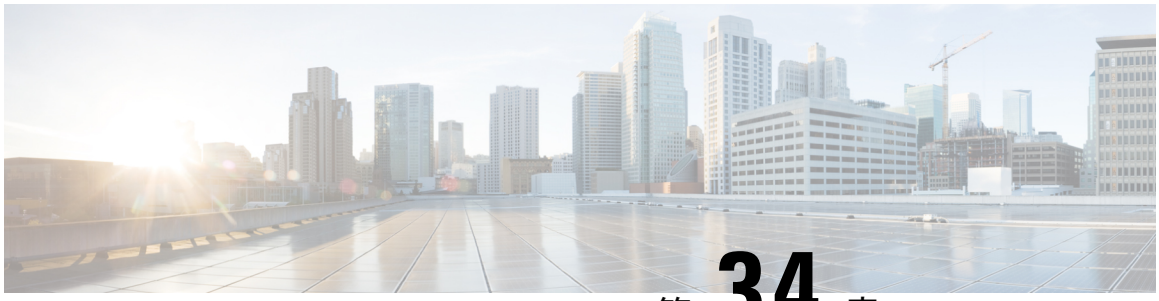
コマンドライン インターフェイス（CLI）を使用して、パブリッシャ ノードのネットワーク タイム プロトコル（NTP）の問題をトラブルシューティングできます。

手順

	コマンドまたはアクション	目的
ステップ 1	**show network eth0 [detail]** を入力して、ネットワーク設定を確認します。	
ステップ 2	**utils ntp status** を入力して、NTP の状態を確認します。	
ステップ 3	**utils ntp restart** を入力して、NTP を再起動します。	
ステップ 4	**utils ntp server list** を入力して、NTP サーバを確認します。	NTP サーバを追加または削除するには、**utils ntp server [add/delete]** CLI コマンドを使用します。

第 VIII 部

ディザスタ リカバリ



第 34 章

システムのバックアップ

バックアップの概要

定期的にバックアップを行うことを推奨します。 ディザスタ リカバリ システム（DRS）を使用して、クラスタ内のすべてのサーバのデータを完全にバックアップできます。 自動バックアップをセットアップすることも、任意の時点でバックアップを起動することもできます。

ディザスタ リカバリ システムで実行するバックアップは、クラスタ レベルであり、Cisco Unified Communications Manager クラスタ内のすべてのサーバのバックアップを 1 箇所に集め、バックアップ データを物理的なストレージ デバイスにアーカイブします。 バックアップ ファイルが暗号化され、システム ソフトウェアによってだけ開くことができます。

DRS は、プラットフォームのバックアップ/復元の一環として、独自の設定（バックアップ デバイス設定およびスケジュール設定）を復元します。 DRS は drfDevice.xml ファイルと drfSchedule.xml ファイルをバックアップおよび復元します。 これらのファイルとともにサーバを復元するときは、DRS バックアップ デバイスおよびスケジュールを再設定する必要がありません。

システムデータを復元するときには、クラスタ内のどのノードを復元するかを選択できます。

ディザスタ リカバリ システムには、次の機能があります。

- バックアップおよび復元タスクを実行するためのユーザ インターフェイス。
- バックアップ機能を実行するための分散システム アーキテクチャ。
- スケジュール バックアップまたは手動（ユーザが起動する）バックアップ。
- リモート SFTP サーバへのバックアップのアーカイブ。

この表では、ディザスタリカバリシステムがバックアップおよび復元できる機能とコンポーネントを示します。 選択した各機能について、すべてのコンポーネントが自動的にバックアップされます。

表 *85 : Cisco Unified CM* の機能とコンポーネント

機能	コンポーネント
CCM - Unified Communications Manager	Unified Communications Manager データベース
	Platform
	Serviceability
	保留音（MOH）
	Cisco Emergency Responder
	一括管理ツール（BAT）
	優先順位
	電話デバイスファイル（TFTP）
	syslogagt（SNMP syslog エージェント）
	cdpagent（SNMP cdp エージェント）
	tct（トレース収集ツール）
	コール詳細レコード（CDR）
	CDR レポートと分析（CAR）

表 *86 : IM and Presence* の機能とコンポーネント

機能	コンポーネント
IM and Presence Service	IM and Presence データベース
	syslogagt（SNMP syslog エージェント）
	cdpagent（SNMP cdp エージェント）
	Platform
	Reporter（Serviceability Reporter）
	CUP SIP Proxy
	XCP
	CLM
	一括管理ツール（BAT）
	優先順位
	tct（トレース収集ツール）

バックアップの前提条件

- バージョンの要件を満たしていることを確認してください。
  - すべての Cisco Unified Communications Manager クラスタ ノードは、同じバージョンの Cisco Unified Communications Manager アプリケーションを実行している必要があります。
  - すべての IM and Presence Service クラスタ ノードは、同じバージョンの IM and Presence Service アプリケーションを実行している必要があります。
  - バックアップ ファイルに保存されているソフトウェア バージョンが、クラスタ ノードで実行されるバージョンと同じでなければなりません。

バージョンの文字列全体が一致している必要があります。 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 であり、バックアップ ファイルに保存されているバージョンも 11.5.1.10000-1 でなければなりません。 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。 バックアップ ファイルに保存されているバージョンが、クラスタ ノードで実行されているバージョンと一致するよう、ソフトウェア バージョンをアップグレードしたら常にシステムをバックアップするようにしてください。

- DRS 暗号化は、クラスタ セキュリティ パスワードに依存することに留意してください。バックアップの実行中に、DRS は暗号化のためにランダム パスワードを生成し、そのランダム パスワードをクラスタ セキュリティ パスワードを使用して暗号化します。バックアップを実行した後、復元を行うまでの間にクラスタ セキュリティ パスワードが変更された場合、そのバックアップ ファイルを使用してシステムを復元するには、バックアップを実行した時点でのパスワードを把握していなければなりません。あるいは、セキュリティ パスワードを変更/リセットした直後にバックアップを作成するようにしてください。
- リモート デバイスをバックアップする必要がある場合は、必ず SFTP サーバを設定する必要があります。利用可能な SFTP サーバの詳細については、次の項を参照してください。リモート バックアップ用 SFTP サーバ （495 ページ）

バックアップ タスク フロー

次のタスクを実行して、バックアップを設定して実行します。バックアップの実行中は OS 管理タスクを実行しないでください。これは、ディザスタ リカバリ システムがプラットフォーム API をロックすることにより、すべての OS 管理要求をブロックするためです。ただし、CLI ベースのアップグレード コマンドしかプラットフォーム API ロッキング パッケージを使用しないため、ディザスタ リカバリ システムはほとんどの CLI コマンドを妨害しません。

手順

	コマンドまたはアクション	目的
ステップ 1	バックアップデバイスの設定（489 ページ）	データをバックアップするデバイスを指定します。
ステップ 2	バックアップ ファイルのサイズの予測（490 ページ）	SFTP デバイス上で作成されるバックアップ ファイルのサイズを見積もります。
ステップ 3	次のいずれかのオプションを選択します。 • スケジュール バックアップの設定（491 ページ） • 手動バックアップの開始（492 ページ）	スケジュールに従ってデータをバックアップするためのバックアップ スケジュールを作成します。 手動バックアップを実行します（任意）。
ステップ 4	現在のバックアップ ステータスの表示（493 ページ）	これはオプションです。バックアップのステータスをチェックします。バックアップの実行中、現在のバックアップ ジョブのステータスを確認できます。
ステップ 5	バックアップ履歴の表示（494 ページ）	これはオプションです。バックアップ履歴の表示

バックアップ デバイスの設定

最大10個のバックアップデバイスを設定できます。 バックアップ ファイルを保存する場所を設定するには、次の手順を実行します。

始める前に

- バックアップ ファイルを保存するために SFTP サーバにディレクトリ パスへの書き込みアクセス権があることを確認します。
- DRS マスターエージェントがバックアップデバイスの設定を検証するときに、ユーザ名、パスワード、サーバ名とディレクトリ パスが有効であることを確認します。

（注） バックアップはネットワーク トラフィックが少なくなる時間帯にスケジューリングしてください。

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）] > [バックアップ デバイス（Backup Device）]** の順に選択します。

ステップ 2 [バックアップ デバイス リスト（Backup Device List）]ウィンドウで、次のいずれかを実行します。

- 新しいデバイスを設定するには、[新規追加（Add New）]をクリックします。
- 既存のバックアップ デバイスを編集するには、検索条件を入力し、[検索（Find）]、次に[選択項目の編集（Edit Selected）]をクリックします。
- バックアップ デバイスを削除するには、[バックアップ デバイス（Backup Device）]リストでバックアップ デバイスを選択してから [選択項目の削除（Delete Selected）]をクリックします。

バックアップ スケジュールにバックアップ デバイスとして設定されているバックアップ デバイスは削除できません。

ステップ 3 [バックアップデバイス名（Backup device name）]フィールドにバックアップ名を入力します。

バックアップ デバイス名には、英数字、スペース（）、ダッシュ（-）、およびアンダースコア（_）だけを使用します。 それ以外の文字は使用しないでください。

ステップ 4 [接続先の選択（Select Destination）]領域の [ネットワーク ディレクトリ（Network Directory）]で、次を実行します。

- [ホスト名/IP アドレス（Host name/IP Address）]フィールドに、ネットワーク サーバのホスト名または IP アドレスを入力します。
- [パス名（Path name）]フィールドに、バックアップ ファイルを格納するディレクトリ パスを入力します。

- [ユーザ名（User name）]フィールドに、有効なユーザ名を入力します。
- [パスワード（Password）]フィールドに、有効なパスワードを入力します。
- [ネットワーク ディレクトリに保存するバックアップ数（Number of backups to store on Network Directory）]ドロップダウン リストから、バックアップの必要数を選択します。

ステップ 5 **[保存（Save）]** をクリックします。

次のタスク

バックアップ ファイルのサイズの予測 （490 ページ）

バックアップ ファイルのサイズの予測

1 つまたは複数の選択した機能のバックアップ履歴が存在する場合に限り、Cisco Unified Communications Manager は、バックアップ tar のサイズを予測します。

計算されたサイズは正確な値ではなく、バックアップ tar の予測サイズです。 サイズは前のバックアップの実際のバックアップ サイズに基づいて計算され、設定が前回のバックアップ以降変更された場合は異なることがあります。

この手順は、前回のバックアップが存在する場合にのみ使用でき、初めてシステムをバックアップする場合は使用できません。

SFTP デバイスに保存されているバックアップ tar のサイズを予測するには、次の手順に従ってください。

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 [機能の選択（Select Features）]領域でバックアップする機能を選択します。

ステップ 3 選択した機能のバックアップの予測サイズを表示するには、[サイズの予測（Estimate Size）]を選択します。

次のタスク

システムをバックアップするには、次のいずれかの手順を実行します。

- スケジュール バックアップの設定 （491 ページ）
- 手動バックアップの開始 （492 ページ）

スケジュール バックアップの設定

最大 10 個のバックアップ スケジュールを作成できます。 各バックアップ スケジュールには、自動バックアップのスケジュール、バックアップする機能セット、保存場所など、独自のプロパティがあります。

バックアップ .tar ファイルはランダムに生成されるパスワードで暗号化されるということに注意してください。 このパスワードは、クラスタ セキュリティ パスワードで暗号化され、バックアップ .tar ファイルとともに保存されます。 このセキュリティ パスワードは忘れないように記憶しておくか、またはセキュリティパスワードを変更またはリセットしたらすぐにバックアップを作成する必要があります。

注意 コール処理が中断してサービスに影響が及ばないように、バックアップはオフピーク時間中にスケジュールしてください。

始める前に

バックアップ デバイスの設定 （489 ページ）

手順

ステップ 1 ディザスタ リカバリ システムで、[バックアップ スケジューラ（Backup Scheduler）] を選択します。

ステップ 2 [スケジュール リスト（Schedule List）]ウィンドウで、新規スケジュールを追加するか、または既存のスケジュールを編集します。

- 新規スケジュールを作成するには、[Add New]をクリックします。
- 既存のスケジュールを設定するには、[スケジュール リスト（Schedule List）] 列でその名前をクリックします。

ステップ 3 [スケジューラ（scheduler）]ウィンドウで、[スケジュール名（Schedule Name）]フィールドにスケジュール名を入力します。

（注） デフォルトのスケジュールの名前は変更できません。

ステップ 4 [バックアップ デバイスの選択（Select Backup Device）]領域でバックアップ デバイスを選択します。

ステップ 5 [機能の選択（Select Features）]領域でバックアップする機能を選択します。 少なくとも 1 つの機能を選択する必要があります。

ステップ 6 [バックアップの開始時刻（Start Backup at）]領域でバックアップを開始する日付と時刻を選択します。

ステップ 7 [頻度（Frequency）]領域でバックアップを行う頻度を選択します。 頻度は、[一度（Once）]、[日次（Daily）]、[週次（Weekly）]、[月次（Monthly）] に設定できます。 [週次（Weekly）]を選択した場合は、バックアップを行う週の曜日も選択できます。

ヒント バックアップ頻度を火曜日から土曜日までの[週次（Weekly）]に設定するには、[デフォルトの設定（Set Default）]をクリックします。

ステップ 8 これらの設定を更新するには、[保存（Save）]をクリックします。

ステップ 9 次のいずれかのオプションを選択します。

- 選択したスケジュールをイネーブルにするには、[選択されたスケジュールの有効化（Enable Selected Schedules）]をクリックします。
- 選択したスケジュールをディセーブルにするには、[選択されたスケジュールの無効化（Disable Selected Schedules）]をクリックします。
- 選択したスケジュールを削除するには、[選択項目の削除（Delete Selected）]をクリックします。

ステップ 10 スケジュールを有効にするには、[スケジュールの有効化（Enable Schedule）]をクリックします。

設定した時刻になると自動的に次のバックアップが実行されます。

（注） クラスタ内のすべてのサーバが、同じバージョンの Cisco Unified Communications Manager または Cisco IM and Presence サービスを実行し、ネットワークから到達可能であることを確認します。スケジュールされたバックアップの時刻にサーバーに到達できないと、そのサーバーはバックアップされません。

次のタスク

次の手順を実行します。

- バックアップ ファイルのサイズの予測 （490 ページ）
- （任意） 現在のバックアップ ステータスの表示 （493 ページ）

手動バックアップの開始

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。
- Cisco Unified Communications Manager または IM and Presence Service のインストールされているバージョンが、すべてのクラスタ ノードで同じであることを確認します。
- 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。

- ネットワークの中断がないことを確認してください。
- バックアップ デバイスの設定 （489 ページ）
- バックアップ ファイルのサイズの予測 （490 ページ）
- 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。

（注） バックアップが実行されている間は、Disaster Recovery System がプラットフォーム API をロックしてすべての要求をブロックするため、Cisco Unified OS の管理または Cisco Unified IM and Presence OS の管理でタスクを実行することはできません。 ただし、CLI ベースのアップグレード コマンドしかプラットフォーム API ロッキング パッケージを使用しないため、ディザスタ リカバリ システムはほとんどの CLI コマンドを妨害しません。

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。

次のタスク

（任意） 現在のバックアップ ステータスの表示 （493 ページ）

現在のバックアップ ステータスの表示

現在のバックアップ ジョブのステータスを確認するには、次の手順を実行します。

注意 リモート サーバへのバックアップが 20 時間以内に完了しないとバックアップ セッションがタイムアウトするため、新規バックアップを開始する必要があります。

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）]**>**[現在のステータス（Current Status）]** の順に選択します。

ステップ 2 バックアップ ログ ファイルを表示するには、ログファイル名リンクをクリックします。

ステップ 3 現在のバックアップをキャンセルするには、[バックアップのキャンセル（Cancel Backup）]をクリックします。

（注） 現在のコンポーネントがバックアップ操作を完了した後、バックアップがキャンセルされます。

次のタスク

バックアップ履歴の表示 （494 ページ）

バックアップ履歴の表示

バックアップ履歴を参照するには、次の手順を実行します。

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）]** > **[履歴（History）]** の順に選択します。

ステップ 2 [バックアップ履歴（Backup History）]ウィンドウで、ファイル名、バックアップ デバイス、完了日、結果、バージョン、バックアップされている機能、失敗した機能など、実行したバックアップを表示できます。

（注） [バックアップ履歴（Backup History）]ウィンドウには、最新の 20 個のバックアップ ジョブだけが表示されます。

バックアップの連携動作と制限事項

• バックアップの制約事項 （495 ページ）

バックアップの制約事項

バックアップには、次の制約事項が適用されます。

表 87 : バックアップの制約事項

制約事項	説明
クラスタ セキュリティ パスワード	クラスタセキュリティパスワードを変更したら、必ずバックアップを実行することを推奨します。 バックアップ暗号化では、バックアップ ファイルのデータを暗号化する際にクラスタセキュリティパスワードを使用します。バックアップファイルの作成後にクラスタセキュリティパスワードを編集すると、古いパスワードを忘れてしまった場合に、そのバックアップ ファイルを使用してデータを復元できなくなります。
証明書の管理	ディザスタリカバリシステム（DRS）は、マスターエージェントとローカルエージェントとの間で SSL ベースの通信を使用して、Unified Communications Manager クラスタノード間のデータの認証および暗号化を行います。 DRS は、リリース 14、14SU1、14SU3 以降のバージョンの公開キー/秘密キーの暗号化に、tomcat RSA 証明書を使用します。証明書管理ページから Tomcat 信頼ストア（hostname.pem）ファイルを削除すると、DRS が想定どおりに機能しなくなることに注意してください。 Tomcat-trust ファイルを手動で削除するときは、tomcat RSA 証明書を Tomcat-trust に必ずアップロードしてください。 （注） リリース 14SU2 について、DRS は Tomcat-ECDSA 証明書を使用して、公開キー/秘密キーの暗号化を行います。 証明書管理ページから Tomcat 信頼ストア（hostname.pem）ファイルを削除すると、DRS が想定どおりに機能しなくなることに注意してください。 Tomcat-trust ファイルを手動で削除するときは、Tomcat-ECDSA 証明書を Tomcat-trust に必ずアップロードしてください。 詳細については、「「証明書管理」」の項を参照してください Cisco Unified Communications Manager セキュリティガイド。

リモート バックアップ用 SFTP サーバ

データをネットワーク上のリモート デバイスにバックアップするには、SFTP サーバーを用意して必要な設定を行う必要があります。 内部テストでは、シスコが提供し、Cisco TAC がサ

ポートしている Cisco Prime Collaboration Deployment（PCD）上の SFTP サーバーを使用します。 SFTP サーバオプションの概要については、次の表を参照してください。

以下の表示に記載されている情報を参考に、システムで使用する SFTP サーバ ソリューションを決定してください。

表 *88 : SFTP* サーバ情報

SFTP サーバ	情報
Cisco Prime Collaboration Deployment の SFTP サーバ	このサーバーはシスコが提供およびテストした唯一の SFTP サーバーであり、Cisco TAC が完全にサポートします。 バージョンの互換性は、使用している Unified Communications Manager および Cisco Prime Collaboration Deployment のバージョンに依存します。 バージョン（SFTP）または Unified Communications Manager をアップグレードする前に、『Cisco Prime Collaboration Deployment Administration Guide』を参照して、互換性のあるバージョンであることを確認してください。
テクノロジー パートナーの SFTP サーバ	これらのサーバーはサードパーティが提供およびテストしたものです。 バージョンの互換性は、サード パーティによるテストに依存します。 テクノロジー パートナーの SFTP サーバまたは Unified Communications Manager をアップグレードする場合、テクノロジー パートナーのページで、互換性のあるバージョンを確認してください。 https://marketplace.cisco.com
他のサードパーティの SFTP サーバ	これらのサーバーはサードパーティが提供するものであり、Cisco TAC はこれらのサーバーを正式にサポートしていません。 バージョンの互換性は、SFTP バージョンと Unified Communications Manager バージョンの互換性を確立するためのベストエフォートに基づきます。 （注） これらの製品はシスコによってテストされていないため、機能を保証することはできません。 Cisco TAC はこれらの製品をサポートしていません。 完全にテストされてサポートされる SFTP ソリューションとしては、Cisco Prime Collaboration Deployment またはテクノロジーパートナーの SFTP サーバーを利用してください。

暗号サポート

Unified Communications Manager 11.5 の場合、Unified Communications Manager は SFTP 接続用に次の CBC および CRT 暗号を通知します。

- aes128-cbc
- 3des-cbc

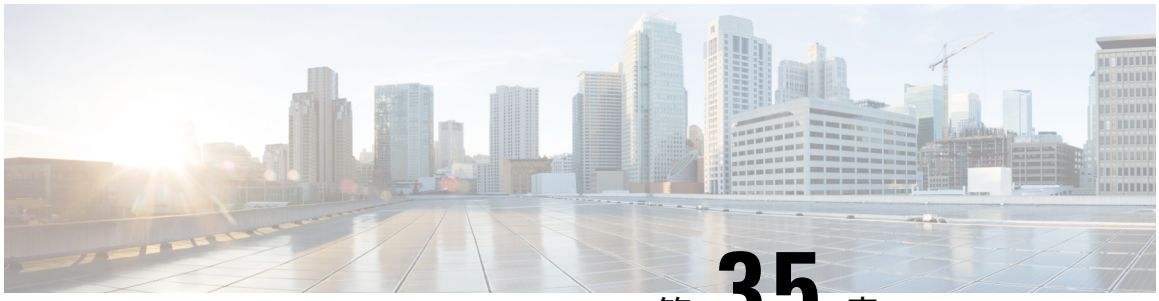
- aes128-ctr
- aes192-ctr
- aes256-ctr

（注） バックアップ SFTP サーバー Unified Communications Manager と通信するためにこれらの暗号のいずれかをサポートしていることを確認してください。

Unified Communications Manager 12.0 以降のリリースでは、CBC 暗号はサポートされていません。 Unified Communications Manager は、次の CTR 暗号だけをサポートおよび通知します。

- aes256-ctr
- aes128-ctr
- aes192-ctr

（注） バックアップ SFTP サーバーが Unified Communications Manager と通信するためにこれらの CTR 暗号のいずれかをサポートしていることを確認してください。



第 35 章

システムの復元

復元の概要

ディザスタ リカバリ システム（DRS）には、システムを復元するプロセスを実行するためのガイドとなるウィザードが用意されています。

バックアップ ファイルは暗号化されており、それらを開いてデータを復元できるのは DRS システムのみです。 ディザスタ リカバリ システムには、次の機能があります。

- 復元タスクを実行するためのユーザ インターフェイス。
- 復元機能を実行するための分散システム アーキテクチャ。

マスター エージェント

クラスタの各ノードで自動的にマスター エージェント サービスが起動されますが、マスター エージェントはパブリッシャ ノード上でのみ機能します。 サブスクライバ ノード上のマスター エージェントは、何の機能も実行しません。

ローカル エージェント

サーバには、バックアップおよび復元機能を実行するローカルエージェントが搭載されています。

マスター エージェントを含むノードをはじめ、Cisco Unified Communications Manager クラスタ内の各ノードには、バックアップおよび復元機能を実行するために独自のローカルエージェントが必要です。

（注） デフォルトでは、ローカル エージェントは IM and Presence ノードをはじめ、クラスタ内の各ノードで自動的に起動されます。

復元の前提条件

- バージョンの要件を満たしていることを確認してください。
  - すべての Cisco Unified Communications Manager クラスタ ノードは、同じバージョンの Cisco Unified Communications Manager アプリケーションを実行している必要があります。
  - すべての IM and Presence Service クラスタ ノードは、同じバージョンの IM and Presence Service アプリケーションを実行している必要があります。
  - バックアップ ファイルに保存されているバージョンが、クラスタ ノードで実行されるバージョンと同じでなければなりません。

  バージョンの文字列全体が一致している必要があります。 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 であり、バックアップ ファイルに保存されているバージョンも 11.5.1.10000-1 でなければなりません。 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。
- サーバの IP アドレス、ホスト名、DNS 設定および導入タイプが、バックアップ ファイルに保存されている IP アドレス、ホスト名、DNS 設定および導入タイプと一致していることを確認します。
- バックアップを実行した後にクラスタ セキュリティ パスワードを変更した場合、元のパスワードのレコードを記録しておきます。元のパスワードが分からなければ、復元は失敗します。
- IPsec ポリシーがクラスタで有効な場合は、復元の処理を開始する前に無効にする必要があります。

復元後の SAML SSO 再有効化

重要　この項は、リリース 12.5（1）SU7 にのみ適用されます。

DRS を使用してシステムを復元した後に、SAML SSO がクラスタ内のいずれかのノードで断続的に無効になる場合があります。影響を受けたノードでSAML SSOを再度有効にするには、次の手順を実行する必要があります。

1. Cisco Unified CM Administration で、**[システム（System）]** > **[SAMLシングルサインオン（SAML Single Sign-On）]** の順に選択します。
2. **[SSOテストの実行（Run SSO Test）]** をクリックします。
3. **「SSO のテストに成功しました（SSO Test Succeeded!）」**メッセージが表示されたら、ブラウザウィンドウを閉じ、**[完了（Finish）]** をクリックします。

（注）　SAML SSO の再有効化中に、Cisco Tomcat が起動されます。 SAML SSO がすでに有効になっているノードには影響がありません。

復元タスク フロー

復元プロセス中、[Cisco Unified CM の管理（Cisco Unified Communications Manager OS Administration）] または [Cisco Unified CM IM and Presence OS の管理（Cisco Unified IM and Presence OS Administration）] に関するタスクを実行しないでください。

手順

	コマンドまたはアクション	目的
ステップ 1	最初のノードのみの復元 （502 ページ）	（オプション）クラスタ内の最初のパブリッシャ ノードだけを復元する場合は、この手順を使用します。
ステップ 2	後続クラスタ ノードの復元 （504 ページ）	（オプション）クラスタ内のサブスクライバ ノードを復元する場合は、この手順を使用します。
ステップ 3	パブリッシャの再構築後の 1 回のステップでのクラスタの復元 （506 ページ）	（オプション）パブリッシャがすでに再構築されている場合、1 回のステップでクラスタ全体を復元するには、次の手順に従ってください。
ステップ 4	クラスタ全体の復元 （508 ページ）	（オプション）パブリッシャ ノードを含む、クラスタ内のすべてのノードを復

	コマンドまたはアクション	目的
		元するには、この手順を使用します。主要なハードドライブで障害またはアップグレードが発生した場合や、ハードドライブを移行する場合には、クラスタ内のすべてのノードの再構築が必要になる場合があります。
ステップ 5	前回正常起動時の設定へのノードまたはクラスタの復元 （509 ページ）	（オプション）前回正常起動時の設定にノードを復元する場合に限り、この手順を使用します。 ハード ドライブ障害やその他のハードウェア障害の後には使用しないでください。
ステップ 6	ノードの再起動 （510 ページ）	ノードを再起動するには、この手順を使用します。
ステップ 7	復元ジョブ ステータスのチェック （511 ページ）	（オプション）復元ジョブ ステータスを確認するには、この手順を使用します。
ステップ 8	復元履歴の表示 （512 ページ）	（オプション）復元履歴を表示するには、この手順を使用します。

最初のノードのみの復元

再構築後に最初のノードを復元する場合は、バックアップ デバイスを設定する必要があります。

この手順は、Cisco Unified Communications Manager の最初のノード（パブリッシャ ノードとも呼ばれます）に対して実行できます。 その他の Cisco Unified Communications Manager ノードおよびすべての IM and Presence サービス ノードは、セカンダリ ノードまたはサブスクライバと見なされます。

始める前に

クラスタ内に IM and Presence サービス ノードがある場合は、最初のノードを復元するときに、ノードが実行されており、アクセス可能であることを確認してください。 これは、この手順の実行中に有効なバックアップ ファイルを見つけるために必須です。

手順

ステップ 1 ディザスタ リカバリ システムから、**[復元（Restore）]** > **[復元ウィザード（Restore Wizard）]** を選択します。

ステップ 2 [復元ウィザード ステップ 1（Restore Wizard Step 1）]ウィンドウの [バックアップ デバイスの選択（Select Backup Device）]領域で、復元する適切なバックアップ デバイスを選択します。

ステップ 3 [次へ（Next）]をクリックします。

ステップ 4 [復元ウィザード ステップ 2（Restore Wizard Step 2）]ウィンドウで、復元するバックアップ ファイルを選択します。

（注） バックアップ ファイル名から、バックアップ ファイルが作成された日付と時刻がわかります。

ステップ 5 [次へ（Next）]をクリックします。

ステップ 6 [復元ウィザード ステップ 3（Restore Wizard Step 3）]ウィンドウで、[次へ（Next）]をクリックします。

ステップ 7 復元する機能を選択します。

（注） バックアップ対象として選択した機能が表示されます。

ステップ 8 [次へ（Next）]をクリックします。 [復元ウィザード ステップ 4（Restore Wizard Step 4）] ウィンドウが表示されます。

ステップ 9 ファイル整合性チェックを実行する場合は、[SHA1 メッセージ ダイジェストを使用してファイル整合性チェックを実行する（Perform file integrity check using SHA1 Message Digest）] チェックボックスをオンにします。

（注） ファイル整合性チェックは任意で、SFTP バックアップの場合にだけ必要です。

ファイル整合性チェックの処理は CPU およびネットワーク帯域幅を大量に消費するため、復元プロセスの処理速度が低下します。

また、FIPS モードでのメッセージ ダイジェストの検証にも SHA-1 を使用できます。 SHA-1 は、デジタル署名には使用されない HMAC やランダム ビット生成など、ハッシュ関数アプリケーションでのすべての非デジタル署名の使用に対して許可されます。 たとえば、SHA-1 をチェックサムの計算に使用することができます。 署名の生成と検証のみの場合には、SHA-1 を使用することはできません。

ステップ 10 復元するノードを選択します。

ステップ 11 [復元（Restore）]をクリックして、データを復元します。

ステップ 12 [次へ（Next）]をクリックします。

ステップ 13 復元するノードの選択を求められたら、最初のノード（パブリッシャ）だけを選択します。

注意 このときに後続（サブスクライバ）ノードは選択しないでください。復元を試みても失敗します。

ステップ 14 （オプション）[サーバ名の選択（Select Server Name）] ドロップダウン リストから、パブリッシャ データベース復元元のサブスクライバ ノードを選択します。 選択したサブスクライバ ノードが稼働しており、クラスタに接続されていることを確認してください。
ディザスタ リカバリ システムでバックアップ ファイルのすべてのデータベース以外の情報が復元され、選択した後続ノードから最新のデータベースが取り出されます。

（注） このオプションは、選択したバックアップ ファイルに CCMDB データベース コンポーネントが含まれている場合にのみ表示されます。 まず、パブリッシャ ノードだけが完全に復元されますが、ステップ 14 を実行し、後続のクラスタ ノードを再起動すると、ディザスタ リカバリ システムはデータベース レプリケーションを実行し、完全にすべてのクラスタ ノードのデータベースが同期されます。 これにより、すべてのクラスタ ノードに最新のデータを使用していることが保障されます。

ステップ 15 [復元（Restore）]をクリックします。

ステップ 16 パブリッシャ ノードにデータが復元されます。 復元するデータベースとコンポーネントのサイズによっては、復元が完了するまでに数時間かかることがあります。

（注） 最初のノードを復元すると、Cisco Unified Communications Manager データベース全体がクラスタに復元されます。そのため、復元しているノードの数とデータベースのサイズによっては、数時間かかることがあります。復元するデータベースとコンポーネントのサイズによっては、復元が完了するまでに数時間かかることがあります。

ステップ 17 [復元ステータス（Restore Status）]ウィンドウの [完了率（Percentage Complete）]フィールドに 100% と表示されたら、サーバを再起動します。 クラスタ内のすべてのノードの再起動は最初のノードのみへの復元の場合に必要となります。 後続ノードを再起動する前に、必ず最初のノードを再起動してください。サーバの再起動方法については、「次の作業」の項を参照してください。

（注） Cisco Unified Communications Manager ノードだけを復元する場合は、Cisco Unified Communications Manager and IM and Presence Service サービス クラスタを再起動する必要があります。

IM and Presence サービスのパブリッシャ ノードのみを復元する場合は、IM and Presence サービス クラスタを再起動する必要があります。

次のタスク

- （オプション）復元のステータスを表示するには、次を参照してください。 復元ジョブステータスのチェック （511 ページ）
- ノードを再起動するには、次を参照してください： ノードの再起動 （510 ページ）

後続クラスタ ノードの復元

この手順は、Cisco Unified Communications Manager のサブスクライバ（後続）ノードにのみ適用されます。 インストールされる最初の Cisco Unified Communications Manager ノードはパブリッシャ ノードです。 その他すべての Cisco Unified Communications Manager ノードおよびすべての IM and Presence サービス ノードはサブスクライバ ノードです。

クラスタ内の 1 つ以上の Cisco Unified Communications Manager サブスクライバ ノードを復元するには、次の手順に従います。

始める前に

復元操作を実行する場合は事前に、復元のホスト名、IP アドレス、DNS 設定、および配置タイプが、復元するバックアップ ファイルのホスト名、IP アドレス、DNS 設定、および配置タイプに一致することを確認します。 ディザスタ リカバリ システムでは、ホスト名、IP アドレス、DNS 設定、および配置タイプが異なると復元が行われません。

サーバにインストールされているソフトウェアのバージョンが復元するバックアップ ファイルのバージョンに一致することを確認します。 ディザスタ リカバリ システムは、一致するソフトウェア バージョンのみを復元操作でサポートします。 再構築後に後続ノードを復元している場合は、バックアップ デバイスを設定する必要があります。

手順

ステップ 1 ディザスタ リカバリ システムから、**[復元（Restore）] > [復元ウィザード（Restore Wizard）]** を選択します。

ステップ 2 [復元ウィザード ステップ 1（Restore Wizard Step 1）]ウィンドウの [バックアップ デバイスの選択（Select Backup Device）]領域で、復元するバックアップ デバイスを選択します。

ステップ 3 [次へ（Next）]をクリックします。

ステップ 4 [復元ウィザード ステップ 2（Restore Wizard Step 2）]ウィンドウで、復元するバックアップ ファイルを選択します。

ステップ 5 [次へ（Next）]をクリックします。

ステップ 6 [復元ウィザード ステップ 3（Restore Wizard Step 3）]ウィンドウで、復元する機能を選択します。

（注） 選択したファイルにバックアップされた機能だけが表示されます。

ステップ 7 [次へ（Next）]をクリックします。 [復元ウィザード ステップ 4（Restore Wizard Step 4）] ウィンドウが表示されます。

ステップ 8 [復元ウィザード ステップ 4（Restore Wizard Step 4）]ウィンドウで、復元するノードを選択するよう求められたら、後続ノードのみを選択します。

ステップ 9 [復元（Restore）]をクリックします。

ステップ 10 後続ノードにデータが復元されます。 復元ステータスの確認方法については、「次の作業」の項を参照してください。

（注） 復元プロセス中、[Cisco Unified CM の管理（Cisco Unified Communications Manager Administration）] または [ユーザ オプション（User Options）] に関するタスクを実行しないでください。

ステップ 11 [復元ステータス（Restore Status）]ウィンドウの [完了率（Percentage Complete）]フィールドに 100% と表示されたら、復元した 2 次サーバを再起動します。 クラスタ内のすべてのノードの再起動は最初のノードのみへの復元の場合に必要となります。後続ノードを再起動する前に、必ず最初のノードを再起動してください。サーバの再起動方法については、「次の作業」の項を参照してください。

（注） 最初の IM and Presence サービス ノードが復元されたら、 IM and Presence サービスの後続ノードを再起動する前に、必ず最初の IM and Presence サービス ノードを再起動してください。

次のタスク

- （オプション）復元のステータスを表示するには、次を参照してください。 復元ジョブステータスのチェック （511 ページ）
- ノードを再起動するには、次を参照してください： ノードの再起動 （510 ページ）

パブリッシャの再構築後の 1 回のステップでのクラスタの復元

復元するデータベースとコンポーネントのサイズによっては、復元が完了するまでに数時間かかることがあります。パブリッシャがすでに再構築されている場合、または新しくインストールされた場合に、1 回のステップでクラスタ全体を復元する場合は、次の手順に従います。

手順

ステップ 1 ディザスタ リカバリ システムから、**[復元（Restore）] > [復元ウィザード（Restore Wizard）]** を選択します。

ステップ 2 [復元ウィザード ステップ 1（Restore Wizard Step 1）]ウィンドウの [バックアップ デバイスの選択（Select Backup Device）]領域で、復元するバックアップ デバイスを選択します。

ステップ 3 [次へ（Next）]をクリックします。

ステップ 4 [復元ウィザード ステップ 2（Restore Wizard Step 2）]ウィンドウで、復元するバックアップ ファイルを選択します。

バックアップ ファイル名から、バックアップ ファイルが作成された日付と時刻がわかります。

クラスタ全体を復元するクラスタのバックアップ ファイルだけを選択します。

ステップ 5 [次へ（Next）]をクリックします。

ステップ 6 [復元ウィザード ステップ 3（Restore Wizard Step 3）]ウィンドウで、復元する機能を選択します。

画面には、復元する機能のうち、バックアップ ファイルに保存された機能のみが表示されます。

ステップ 7 [次へ（Next）]をクリックします。

ステップ 8 [復元ウィザード ステップ 4（Restore Wizard Step 4）]ウィンドウで、[1 ステップでの復元（One-Step Restore）]をクリックします。

このオプションは、復元用に選択されたバックアップ ファイルがクラスタのバックアップ ファイルであり、復元用に選択された機能に、パブリッシャとサブスクライバの両方のノードに登

録された機能が含まれている場合にのみ [復元ウィザード ステップ 4（Restore Wizard Step 4）] ウィンドウに表示されます。詳細については、最初のノードのみの復元 （502 ページ）および後続クラスタ ノードの復元 （504 ページ）を参照してください。

（注） 「パブリッシャがクラスタ対応になりませんでした。*1* ステップでの復元を開始できません（*Publisher has failed to become cluster aware. Cannot start one-step restore*）」というステータス メッセージが表示されたら、パブリッシャ ノードを復元してからサブスクライバ ノードを復元する必要があります。 詳細については、「関連項目」を参照してください。

このオプションでは、パブリッシャがクラスタ対応になり、そのためには 5 分かかります。 このオプションをクリックすると、ステータス メッセージに「「パブリッシャがクラスタ対応になるまで 5 分間待機してください。この期間にバックアップまたは復元処理を開始しないでください。（Please wait for 5 minutes until Publisher becomes cluster aware and do not start any backup or restore activity in this time period.）」」と表示されます。

この待ち時間の経過後に、パブリッシャがクラスタ対応になると、「「パブリッシャがクラスタ対応になりました。 サーバを選択し、[復元（Restore）] をクリックしてクラスタ全体の復元を開始してください（Publisher has become cluster aware. Please select the servers and click on Restore to start the restore of entire cluster）」」というステータス メッセージが表示されます。

この待ち時間の経過後、パブリッシャがクラスタ対応にならない場合、「パブリッシャがクラスタ対応にならなかったため、 1 ステップでの復元を開始できず、 通常の 2 ステップでの復元を実行してください。（Publisher has failed to become cluster aware. Cannot start one-step restore. Please go ahead and do a normal two-step restore.）」というステータス メッセージが表示されます。 クラスタ全体を 2 ステップ（パブリッシャとサブスクライバ）で復元するには、最初のノードのみの復元 （502 ページ） と 後続クラスタ ノードの復元 （504 ページ） で説明する手順を実行してください。

ステップ 9 復元するノードの選択を求められたら、クラスタ内のすべてのノードを選択します。

最初のノードを復元すると、ディザスタ リカバリ システムが自動的に後続ノードに Cisco Unified Communications Manager データベース（CCMDB）を復元します。 そのため、復元しているノードの数とデータベースのサイズによっては、数時間かかることがあります。

ステップ 10 [復元（Restore）] をクリックします。
クラスタ内のすべてのノードでデータが復元されます。

ステップ 11 [復元ステータス（Restore Status）] ウィンドウの [完了率（Percentage Complete）] フィールドに 100% と表示されたら、サーバを再起動します。 クラスタ内のすべてのノードの再起動は最初のノードのみへの復元の場合に必要となります。 後続ノードを再起動する前に、必ず最初のノードを再起動してください。 サーバの再起動方法については、「次の作業」の項を参照してください。

次のタスク

- （オプション）復元のステータスを表示するには、次を参照してください。 復元ジョブステータスのチェック （511 ページ）
- ノードを再起動するには、次を参照してください： ノードの再起動 （510 ページ）

クラスタ全体の復元

主要なハード ドライブで障害またはアップグレードが発生した場合や、ハード ドライブを移行する場合には、クラスタ内のすべてのノードの再構築が必要です。クラスタ全体を復元するには、次の手順を実行します。

ネットワーク カードの交換やメモリの増設など他のほとんどのハードウェア アップグレードでは、次の手順を実行する必要はありません。

手順

ステップ 1 ディザスタ リカバリ システムから、**[復元（Restore）] > [復元ウィザード（Restore Wizard）]** を選択します。

ステップ 2 [バックアップ デバイスの選択（Select Backup Device）]エリアで、復元する適切なバックアップ デバイスを選択します。

ステップ 3 [次へ（Next）]をクリックします。

ステップ 4 [復元ウィザード ステップ 2（Restore Wizard Step 2）]ウィンドウで、復元するバックアップ ファイルを選択します。

（注） バックアップ ファイル名から、バックアップ ファイルが作成された日付と時刻がわかります。

ステップ 5 [次へ（Next）]をクリックします。

ステップ 6 [復元ウィザード ステップ 3（Restore Wizard Step 3）]ウィンドウで、[次へ（Next）]をクリックします。

ステップ 7 [復元ウィザード ステップ 4（Restore Wizard Step 4）]ウィンドウで復元ノードの選択を求められたら、すべてのノードを選択します。

ステップ 8 [復元（Restore）]をクリックして、データを復元します。

第 1 ノードを復元すると、ディザスタ リカバリ システムが自動的に後続ノードに Cisco Unified Communications Manager データベース（CCMDB）を復元します。そのため、ノードの数とデータベースのサイズによっては、最大数時間かかることがあります。

すべてのノードでデータが復元されます。

（注） 復元プロセス中、[Cisco Unified CM の管理（Cisco Unified Communications Manager Administration）] または [ユーザ オプション（User Options）] に関するタスクを実行しないでください。

復元するデータベースとコンポーネントのサイズによっては、復元が完了するまでに数時間かかることがあります。

ステップ 9 復元プロセスが完了したら、サーバを再起動します。 サーバの再起動方法の詳細については、「次の作業」セクションを参照してください。

（注） 必ず最初のノードを再起動してから、後続ノードを再起動してください。

最初のノードが再起動し、Cisco Unified Communications Manager の復元後のバージョンが実行されたら、後続ノードを再起動します。

ステップ 10 レプリケーションはクラスタのリブート後に自動的に設定されます。 『*Cisco Unified Communications* ソリューション コマンドライン インターフェイス リファレンス ガイド』の説明に従って 「utils dbreplication runtimestate」 CLI コマンドを使用して、すべてのノードで [レプリケーションステータス（Replication Status）] の値を確認します。 各ノードの値は 2 になっているはずです。

（注） クラスタのサイズによっては、後続ノードの再起動後に、後続ノードでのデータベースレプリケーションが完了するまでに時間がかかる場合があります。

ヒント レプリケーションが正しくセットアップされない場合は、『*Command Line Interface Reference Guide for Cisco Unifed Communications Solutions*』の説明に従って「utils dbreplication rebuild」CLI コマンドを使用します。

次のタスク

- （オプション）復元のステータスを表示するには、次を参照してください。 復元ジョブステータスのチェック （511 ページ）
- ノードを再起動するには、次を参照してください： ノードの再起動 （510 ページ）

前回正常起動時の設定へのノードまたはクラスタの復元

前回正常起動時の設定にノードまたはクラスタを復元するには、次の手順に従います。

始める前に

- 復元ファイルに、バックアップ ファイルで設定されているホスト名、IP アドレス、DNS 設定、および配置タイプが含まれていることを確認します。
- サーバにインストールされている Cisco Unified Communications Manager のバージョンが復元するバックアップ ファイルのバージョンに一致することを確認します。

- この手順は、前回正常起動時の設定にノードを復元する場合にのみ使用してください。

手順

ステップ 1 ディザスタ リカバリ システムから、**[復元（Restore）]** > **[復元ウィザード（Restore Wizard）]** を選択します。

ステップ 2 [バックアップ デバイスの選択（Select Backup Device）]エリアで、復元する適切なバックアップ デバイスを選択します。

ステップ 3 [次へ（Next）]をクリックします。

ステップ 4 [復元ウィザード ステップ 2（Restore Wizard Step 2）]ウィンドウで、復元するバックアップ ファイルを選択します。

（注） バックアップ ファイル名から、バックアップ ファイルが作成された日付と時刻がわかります。

ステップ 5 [次へ（Next）]をクリックします。

ステップ 6 [復元ウィザード ステップ 3（Restore Wizard Step 3）]ウィンドウで、[次へ（Next）]をクリックします。

ステップ 7 復元ノードを選択するように求められたら、該当するノードを選択します。
選択したノードにデータが復元されます。

ステップ 8 クラスタ内のすべてのノードを再起動します。 後続の Cisco Unified Communications Manager ノードを再起動する前に、最初の Cisco Unified Communications Manager ノードを再起動します。 クラスタに Cisco IM and Presence ノードもある場合は、最初の Cisco IM and Presence ノードを再起動してから、後続の IM and Presence ノードを再起動します。 詳細については、「次の作業」の項を参照してください。

ノードの再起動

データを復元したら、ノードを再起動する必要があります。

パブリッシャ ノード（最初のノード）を復元したら、最初にパブリッシャ ノードを再起動する必要があります。 サブスクライバ ノードは必ず、パブリッシャ ノードが再起動し、ソフトウェアの復元されたバージョンを正常に実行し始めた後で再起動してください。

（注） CUCM パブリッシャ ノードがオフラインの場合は、IM and Presence サブスクライバ ノードを再起動しないでください。 このような場合は、サブスクライバ ノードが CUCM パブリッシャに接続できないため、ノード サービスの開始に失敗します。

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

再起動する必要があるクラスタ内のすべてのノードでこの手順を実行します。

手順

ステップ 1 [Cisco Unified OS の管理（Cisco Unified OS Administration）] から、**[設定（Settings）] > [バージョン（Version）]** を選択します。

ステップ 2 ノードを再起動するには、[再起動（Restart）]をクリックします。

ステップ 3 レプリケーションはクラスタのリブート後に自動的に設定されます。 **utils dbreplication runtimestate** CLI コマンドを使用して、すべてのノードで [レプリケーション ステータス（Replication Status）] 値を確認します。 各ノードの値は 2 になっている必要があります。CLI コマンドの詳細については、「Cisco Unified Communications (CallManager) Command References」を参照してください。

レプリケーションが正しくセットアップされない場合は、『*Command Line Reference Guide for Cisco Unified Communications Solutions*』の説明に従って **utils dbreplication reset** CLI コマンドを使用します。

（注） クラスタのサイズによっては、後続ノードの再起動後に、後続ノードでのデータベース レプリケーションが完了するまでに数時間かかる場合があります。

次のタスク

（オプション）復元のステータスを表示するには、復元ジョブ ステータスのチェック （511 ページ）を参照してください。

復元ジョブ ステータスのチェック

次の手順に従って、復元ジョブ ステータスをチェックします。

手順

ステップ 1 ディザスタ リカバリ システムで、**[復元（Restore）] > [現在のステータス（Current Status）]** を選択します。

ステップ 2 [復元ステータス（Restore Status）]ウィンドウで、ログ ファイル名のリンクをクリックし、復元ステータスを表示します。

復元履歴の表示

復元履歴を参照するには、次の手順を実行します。

手順

ステップ 1 [Disaster Recovery System] で、**[復元（Restore）]** > **[履歴（History）]** を選択します。

ステップ 2 [復元履歴（Restore History）]ウィンドウで、ファイル名、バックアップデバイス、完了日、結果、バージョン、復元された機能、失敗した機能など、実行した復元を表示できます。

[復元履歴（Restore History）]ウィンドウには、最新の 20 個の復元ジョブだけが表示されます。

データ認証

トレース ファイル

トラブルシューティングを行う際、またはログの収集中には、トレース ファイルの保存先として次の場所が使用されます。

マスター エージェント、GUI、各ローカル エージェント、および JSch ライブラリのトレース ファイルは次の場所に書き込まれます。

- マスター エージェントの場合、トレース ファイルは platform/drf/trace/drfMA0* にあります。
- 各ローカル エージェントの場合、トレース ファイルは platform/drf/trace/drfLA0* にあります。
- GUI の場合、トレース ファイルは platform/drf/trace/drfConfLib0* にあります。
- JSch の場合、トレース ファイルは platform/drf/trace/drfJSch* にあります。

詳細については、『*Command Line Interface Reference Guide for Cisco Unified Communications Solutions*』（http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-command-reference-list.html）を参照してください。

コマンドライン インターフェイス

ディザスタ リカバリ システムでは、次の表に示すように、バックアップおよび復元機能のサブセットにコマンドラインからアクセスできます。 これらのコマンドの内容とコマンドライン インターフェイスの使用方法の詳細については、『*Command Line Interface（CLI）Reference Guide for Cisco Unified Presence*』（http://www.cisco.com/c/en/us/support/unified-communications/

unified-communications-manager-callmanager/products-command-reference-list.html）を参照してください。

表 89 : ディザスタ リカバリ システムのコマンドライン インターフェイス

コマンド	説明
utils disaster_recovery estimate_tar_size	SFTP/Local デバイスからのバックアップ tar の概算サイズを表示し、機能リストのパラメータを 1 つ要求します。
utils disaster_recovery backup	ディザスタ リカバリ システムのインターフェイスに設定されている機能を使用して、手動バックアップを開始します。
utils disaster_recovery jschLogs	JSch ライブラリのロギングを有効または無効にします。
utils disaster_recovery restore	復元を開始します。復元するバックアップ場所、ファイル名、機能、およびノードを指定するためのパラメータが必要です。
utils disaster_recovery status	進行中のバックアップ ジョブまたは復元ジョブのステータスを表示します。
utils disaster_recovery show_backupfiles	既存のバックアップ ファイルを表示します。
utils disaster_recovery cancel_backup	進行中のバックアップ ジョブをキャンセルします。
utils disaster_recovery show_registration	現在設定されている登録を表示します。
utils disaster_recovery device add	ネットワーク デバイスを追加します。
utils disaster_recovery device delete	デバイスを削除します。
utils disaster_recovery device list	すべてのデバイスを一覧表示します。
utils disaster_recovery schedule add	スケジュールを追加します。
utils disaster_recovery schedule delete	スケジュールを削除します。
utils disaster_recovery schedule disable	スケジュールを無効にします。
utils disaster_recovery schedule enable	スケジュールを有効にします。
utils disaster_recovery schedule list	すべてのスケジュールを一覧表示します。

コマンド	説明
utils disaster_recovery backup	ディザスタ リカバリ システムのインターフェイスに設定されている機能を使用して、手動バックアップを開始します。
utils disaster_recovery restore	復元を開始します。復元するバックアップ場所、ファイル名、機能、およびノードを指定するためのパラメータが必要です。
utils disaster_recovery status	進行中のバックアップ ジョブまたは復元ジョブのステータスを表示します。
utils disaster_recovery show_backupfiles	既存のバックアップ ファイルを表示します。
utils disaster_recovery cancel_backup	進行中のバックアップ ジョブをキャンセルします。
utils disaster_recovery show_registration	現在設定されている登録を表示します。

アラームおよびメッセージ

アラームおよびメッセージ

ディザスタ リカバリ システムは、バックアップまたは復元手順の実行時に発生するさまざまなエラーのアラームを発行します。 次の表に、ディザスタ リカバリ システムのアラームの一覧を記載します。

表 *90*: ディザスタ リカバリ システムのアラームとメッセージ

アラーム名	説明	説明
DRFBackupDeviceError	DRF バックアップ プロセスでデバイスへのアクセスに関する問題が発生しています。	DRS バックアップ プロセスへのアクセス中にエラーした。
DRFBackupFailure	シスコ DRF バックアップ プロセスが失敗しました。	DRS バックアップ プロセが発生しました。
DRFBackupInProgress	別のバックアップの実行中は、新規バックアップを開始できません。	DRS は、別のバックアップ新規バックアップを開始で
DRFInternalProcessFailure	DRF 内部プロセスでエラーが発生しました。	DRS 内部プロセスでエラーした。
DRFLA2MAFailure	DRF ローカル エージェントが、マスターエージェントに接続できません。	DRS ローカル エージェンターエージェントに接続で

アラーム名	説明	説明
DRFLocalAgentStartFailure	DRF ローカル エージェントが開始されません。	DRS ローカル エージェしている可能性があり
DRFMA2LAFailure	DRF マスター エージェントがローカル エージェントに接続しません。	DRS マスター エージェル エージェントに接続
DRFMABackupComponentFailure	DRF は、少なくとも 1 つのコンポーネントをバックアップできません。	DRS は、コンポーネンバックアップするようましたが、バックアッエラーが発生し、コンバックアップされませ
DRFMABackupNodeDisconnect	バックアップされるノードが、バックアップの完了前にマスターエージェントから切断されました。	DRS マスター エージェUnified Communications でバックアップ操作をきに、そのノードはバが完了する前に切断さ
DRFMARestoreComponentFailure	DRF は、少なくとも 1 つのコンポーネントを復元できません。	DRS は、コンポーネン元するようにリクエス復元プロセス中にエランポーネントは復元さた。
DRFMARestoreNodeDisconnect	復元されるノードが、復元の完了前にマスターエージェントから切断されました。	DRS マスター エージェUnified Communications で復元操作を実行してのノードは復元操作が断されました。
DRFMasterAgentStartFailure	DRF マスター エージェントが開始されませんでした。	DRS マスター エージェしている可能性があり
DRFNoRegisteredComponent	使用可能な登録済みコンポーネントがないため、バックアップが失敗しました。	使用可能な登録済みコないため、DRS バックました。
DRFNoRegisteredFeature	バックアップする機能が選択されませんでした。	バックアップする機能んでした。
DRFRestoreDeviceError	DRF 復元プロセスでデバイスへのアクセスに関する問題が発生しています。	DRS 復元プロセスは、み取ることができませ
DRFRestoreFailure	DRF 復元プロセスが失敗しました。	DRS 復元プロセスでエした。

アラーム名	説明	説明
DRFSftpFailure	DRF SFTP 操作でエラーが発生しています。	DRS SFTP 操作でエラーが ます。
DRFSecurityViolation	DRF システムが、セキュリティ違反となる可能性がある悪意のあるパターンを検出しました。	DRF ネットワーク メッセ コードインジェクションや リトラバーサルなど、セキ 反となる可能性がある悪意 ターンが含まれています。 トワーク メッセージがブロ います。
DRFTruststoreMissing	ノードで IPsec 信頼ストアが見つかりません。	ノードで IPsec 信頼ストア ません。 DRF ローカル エ が、マスターエージェント ません。
DRFUnknownClient	パブリッシャの DRF マスターエージェントが、クラスタ外部の不明なサーバーからクライアント接続リクエストを受け取りました。 リクエストは拒否されました。	パブリッシャの DRF マスタ ントが、クラスタ外部の不 バーからクライアント接続 を受け取りました。 リクエ されました。
DRFBackupCompleted	DRF バックアップが正常に完了しました。	DRF バックアップが正常に た。
DRFRestoreCompleted	DRF 復元が正常に完了しました。	DRF 復元が正常に完了しま
DRFNoBackupTaken	現在のシステムの有効なバックアップが見つかりませんでした。	アップグレード/移行または トール後に、現在のシステ バックアップが見つかりま た。
DRFComponentRegistered	DRF により、リクエストされたコンポーネントが正常に登録されました。	DRF により、リクエストさ ポーネントが正常に登録さ
DRFRegistrationFailure	DRF 登録操作が失敗しました。	内部エラーが原因で、コン に対する DRF 登録操作が た。
DRFComponentDeRegistered	DRF は正常にリクエストされたコンポーネントの登録をキャンセルしました。	DRF は正常にリクエストさ ポーネントの登録をキャン た。
DRFDeRegistrationFailure	コンポーネントの DRF 登録解除リクエストが失敗しました。	コンポーネントの DRF 登 エストが失敗しました。

アラーム名	説明	説明
DRFFailure	DRF バックアップまたは復元プロセスが失敗しました。	DRF バックアップまたでエラーが発生しまし
DRFRestoreInternalError	DRF 復元オペレーションでエラーが発生しました。 復元は内部的にキャンセルされました。	DRF 復元オペレーショ生しました。 復元は内ルされました。
DRFLogDirAccessFailure	DRF は、ログ ディレクトリにアクセスできませんでした。	DRF は、ログ ディレクスできませんでした。
DRFDeRegisteredServer	DRF がサーバーのすべてのコンポーネントを自動的に登録解除しました。	サーバーが Unified Cor Manager クラスタから可能性があります。
DRFSchedulerDisabled	設定された機能がバックアップで使用できないため、DRF スケジューラは無効になっています。	設定された機能がバッできないため、DRF ス効になっています
DRFSchedulerUpdated	機能が登録解除されたため、DRF でスケジュールされたバックアップ設定が自動的に更新されます。	機能が登録解除されたケジュールされたバッ自動的に更新されます

ライセンス予約

ライセンス予約

重要 次のライセンス機能の表は、Unified CM 14SU1 までのリリースに対応しています。

Unified Communication Manager を有効にした特定のライセンス予約または永久ライセンス予約に対して復元操作を実行した後に、次の手順に従います。

表 *91* : ライセンス予約のディザスタ リカバリ システム

復元後の状態	CSSM 上の製品	ソリューション
未登録	可	シスコに連絡して CSSM から製品を削除し、製品から登録してください。
	不可	何もする必要はありません

復元後の状態	CSSM 上の製品	ソリューション
予約を実行中です	可	次のいずれかの手順を実行します。 手順 1： 1. CSSM から製品の承認コードを取得します。 2. 承認コード **ライセンススマート予約の戻り値承認 "<authorization-code>"** を指定して、以下の CLI を実行します。 手順 2： 1. シスコに連絡して CSSM から製品を削除してください。
	不可	製品**ライセンス スマート予約キャンセル**から、CLI を実行します。
登録済み - 特定のライセンス予約または登録済み-ユニバーサル ライセンス予約 （注） スマートエージェントは、ユニバーサルライセンス予約としてステータスを反映する場合がありますが、永久ライセンス予約機能用です。	可	1. 製品から以下の CLI **ライセンス スマート予約戻り**を実行します。 予約戻りコードがコンソールに出力されます。 2. 製品を削除するには、CSSM で予約戻りコードを入力します。
	不可	製品**ライセンス スマート予約戻り**から、CLI を実行します。

ライセンス情報

ライセンス情報

重要 次のライセンス機能の表は、Unified CM 14SU2 以降のリリースに対応しています。

Unified Communications Manager で復元操作を実行してライセンス情報を更新した後、次の手順に従います。

表 *92 :* ライセンスのディザスタリカバリ システム

復元後の状態	バックアップの状態	CSSM またはサテライト上の製品	ソリューション
未登録	特定のライセンス予約または永久ライセンス予約が有効になっている Unified Communications Managerでの復元操作	可	シスコに連絡して CSSM から製品を削除してから、Unified CM からライセンス予約を実行してください。
		不可	処置は不要です。
	CSSM またはサテライトに登録されている Unified Communications Manager の復元操作	可	CSSM またはサテライト上でアクションは不要です。 製品から再登録します。
		不可	処置は不要です。
	CSSM に登録され、輸出制限ライセンスが許可されている Unified Communications Manager の復元操作	可	CSSM またはサテライト上でアクションは不要です。 製品のエクスポート制限付きライセンスを再登録してリクエストします。
		不可	処置は不要です。
	CSSM サテライトに登録され、輸出制限ライセンスが許可されている Unified Communications Manager の復元操作	可	CSSM および Cisco Smart Software Manager サテライトから製品を削除するには、シスコにお問い合わせください。 次に、製品から登録し、製品からのエクスポート制限付きライセンスをリクエストします。
		不可	処置は不要です。

復元の連携動作と制約事項

復元の連携動作と制約事項

ディザスタ リカバリ システムを使用して Cisco Unified Communications Manager または IM and Presence Service を復元する場合、以下の制約事項が適用されます。

表 *93*：復元の制約事項

制約事項	説明
エクスポートの制限	制限されたバージョンにのみ制限済みバージョンの DRS バックアップのリストア、制限されていないバージョンからのバックアップは制限されていないバージョンでのみリストアすることができます。Unified Communications Manager の米国輸出無制限バージョンにアップグレードした場合、その後、このソフトウェアの米国輸出制限バージョンへのアップグレード、または新規インストールを実行できなくなります。
プラットフォームの移行	ディザスタ リカバリ システムを使用してプラットフォーム間で（たとえば、Windows から Linux へ、または Linux から Windows へ）データを移行することはできません。 復元は、バックアップと同じ製品バージョンで実行する必要があります。 Windows ベースのプラットフォームから Linux ベースのプラットフォームへのデータ移行については、『*Data Migration Assistant User Guide*』を参照してください。
HW の交換と移行	DRS 復元を実行してデータを新しいサーバに移行する場合、新しいサーバに古いサーバが使用していたのと同じ IP アドレスとホスト名を割り当てる必要があります。さらに、バックアップの取得時に DNS が設定されている場合、復元を実行する前に、同じ DNS 設定がある必要があります。 サーバの交換の詳細については、『*Replacing a Single Server or Cluster for Cisco Unified Communications Manager*』ガイドを参照してください。 また、ハードウェアの交換後は、証明書信頼リスト（CTL）クライアントを実行する必要もあります。 後続ノード（サブスクライバ）サーバーを復元しない場合には、CTL クライアントを実行する必要があります。 他の場合、DRS は必要な証明書をバックアップします。 詳細については、『*Cisco Unified Communications Manager* セキュリティガイド』の「「CTL クライアントのインストール」」と「「CTL クライアントの設定」」の手順を参照してください。

制約事項	説明
クラスタ間のエクステンション モビリティ	バックアップ時にリモート クラスタにログインしていた Extension Mobility Cross Cluster ユーザは、復元後もログインしたままとなります。

（注） Smart License Manager は、DRS バックアップや復元の一部としてバックアップや復元はされません。

Unified Communications Manager サーバーコンポーネントを正常に復元した後、Unified Communications Manager は未登録状態になります。 次に、Unified Communications Manager を Cisco Smart Software Manager または Cisco Smart Software Manager サテライトに登録します。

バックアップを作成する前に製品がすでに登録されていたとしても、その製品を再登録してライセンス情報を更新する必要があります。

バックアップを取る前に製品がすでに輸出制限ライセンスを承認されており、製品インスタンスが Cisco Smart Software Manager または Cisco Smart Software Manager satellite に存在する場合は、シスコに問い合わせ、CSSM および Smart Software Manager サテライトから製品を削除してから、サテライト導入を使用しながら製品から登録します。 直接導入する場合は、製品とエクスポート制限付きライセンス要求を再登録します。

製品を Cisco Smart Software Manager または Cisco Smart Software Manager サテライトに登録する方法の詳細については、お使いのリリース向けの Cisco Unified Communications Manager システム設定ガイド を参照してください。

トラブルシューティング

小規模な仮想マシンへの DRS 復元の失敗

問題

IM and Presence サービス ノードをディスク容量がより小さい VM に復元すると、データベースの復元が失敗することがあります。

原因

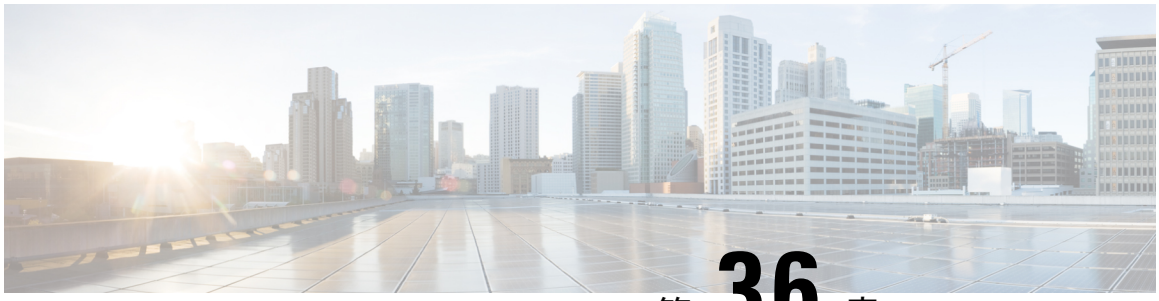
大きいディスク サイズから小さいディスク サイズに移行したときに、この障害が発生します。

ソリューション

2 個の仮想ディスクがある OVA テンプレートから、復元用の VM を展開します。

第 IX 部

トラブルシューティング



第 36 章

トラブルシューティングの概要

ここでは、Unified Communications Managerのトラブルシューティングに必要なバックグラウンド情報と使用できるリソースについて説明します。

Cisco Unified Serviceability

Cisco Unified Serviceability は Unified Communications Manager 用の Web ベースのトラブルシューティング ツールです。このツールには、管理者がシステム問題をトラブルシューティングできるように次の機能が備えられています。

- トラブルシューティング用に Unified Communications Manager サービスのアラームとイベントを保存し、アラーム メッセージの定義を提供します。
- トラブルシューティング用に Unified Communications Manager サービスのトレース情報をさまざまなログ ファイルに保存します。 管理者はトレース情報の設定、収集、および表示を行うことができます。
- Real-Time Monitoring Tool（RTMT）を使用して、Unified Communications Manager クラスタのコンポーネントの動作をリアルタイムで監視します。
- Unified Communications Manager CDR Analysis and Reporting（CAR）を使用して、Quality of Service、トラフィック、課金情報についてのレポートを生成します。
- [サービスの開始（Service Activation）] ウィンドウによりアクティブ化、非アクティブ化、および表示を行うことができる機能サービスを提供します。
- 機能とネットワーク サービスを開始および停止するためのインターフェイスを提供します。
- Cisco Unified Serviceability ツールに関連するレポートをアーカイブします。

- Unified Communications Managerが、SNMPリモート管理およびトラブルシューティングの管理対象デバイスとして動作できるようにします。
- 1つのサーバ（またはクラスタ内のすべてのサーバ）のログパーティションのディスク使用を監視します。

[ナビゲーション] ドロップダウン リスト ボックスからCisco Unified Serviceabilityを選択して、Cisco Unified Communications Manager Administrationウィンドウから Cisco Unified Serviceabilityにアクセスします。 Unified Communications Managerソフトウェアをインストールすると Cisco Unified Serviceabilityが自動的にインストールされ、使用可能になります。

サービスアビリティ ツールの詳細と手順については、『*Cisco Unified Serviceability Administration Guide*』を参照してください。

Cisco Unified Communications Operating System Administration

Cisco Unified Communications Operating System Administration を使用すると、次のタスクを実行して *Cisco Unified Communications Operating System* を設定および管理できます。

- ソフトウェアとハードウェアのステータスを確認する。
- IP アドレスの確認と更新を行う。
- 他のネットワーク デバイスに ping を送信する。
- Network Time Protocol サーバを管理する。
- システム ソフトウェアおよびオプションをアップグレードする。
- システムを再起動する。

サービスアビリティ ツールの詳細と設定手順については、『Administration Guide for Cisco Unified Communications Manager』を参照してください。

一般的な問題解決モデル

テレフォニーまたは IP ネットワーク環境のトラブルシューティングを行う場合は、症状を定義し、その症状の原因と考えられるすべての問題を特定し、考えられる各問題を、症状がなくなるまで可能性の高い順に体系的に取り除いていきます。

次の手順は、問題解決プロセスで使用するガイドラインを示しています。

手順

1. ネットワークの問題を分析し、問題を明確に記述します。 症状と潜在的な原因を定義します。
2. 潜在的な原因を特定するための事実を収集します。

3. 収集した事実を元に、潜在的な原因を検証します。
4. それらの原因に基づいて処置プランを作成します。最も可能性の高い問題から始め、単一の変数だけを操作するプランを考案します。
5. 処置プランを実施し、テストして症状が消えるかどうかを確認しながら、各手順を慎重に実行します。
6. 結果を分析し、問題が解決したかどうかを確認します。問題が解決している場合は、プロセスは完了です。
7. 問題が解決していない場合は、リストで次に可能性の高い原因に基づいて処置プランを作成します。4 （527 ページ） に戻り、問題が解決するまでプロセスを繰り返します。

処置プランの実施中に行った変更は、必ず元に戻してください。変数は一度に1つだけ変更します。

（注） 一般的な原因と処置（このマニュアルで概要を説明しているもの、または環境に応じて特定したもの）をすべて実施しても問題が解決しない場合は、Cisco TAC にお問い合わせください。

ネットワーク障害への事前準備

ネットワーク障害からの回復は、事前準備をしておくと容易に行うことができます。次の質問に答え、ネットワーク障害への事前準備ができているかどうかを確認します。

- ネットワーク上のすべてのデバイスの物理的な場所とそれらの接続方法の概要を示した、相互接続されたネットワークの正確な物理および論理マップがありますか。また、ネットワーク アドレス、ネットワーク番号、サブネットワークを記述した論理マップがありますか。
- ネットワークに実装されているすべてのネットワーク プロトコルのリスト、各プロトコルに関連付けられているネットワーク番号、サブネットワーク、ゾーン、およびエリアの正確なリストがありますか。
- どのプロトコルがルーティングされているか、および各プロトコルについての正確かつ最新の設定情報を把握していますか。
- どのプロトコルがブリッジングされているかを把握していますか。それらのブリッジに設定されているフィルタがありますか。また、その設定のコピーはありますか。そのコピーは Unified Communications Manager に適用できますか。
- インターネットへの接続も含め、外部ネットワークへのすべての接点を知っていますか。各外部ネットワーク接続について、使用されているルーティング プロトコルを知っていますか。
- 現在の問題とベースラインを比較できるように、通常のネットワーク動作とパフォーマンスについて組織で文書化していますか。

これらの質問に「はい」と答えることができれば、障害から迅速に回復できます。

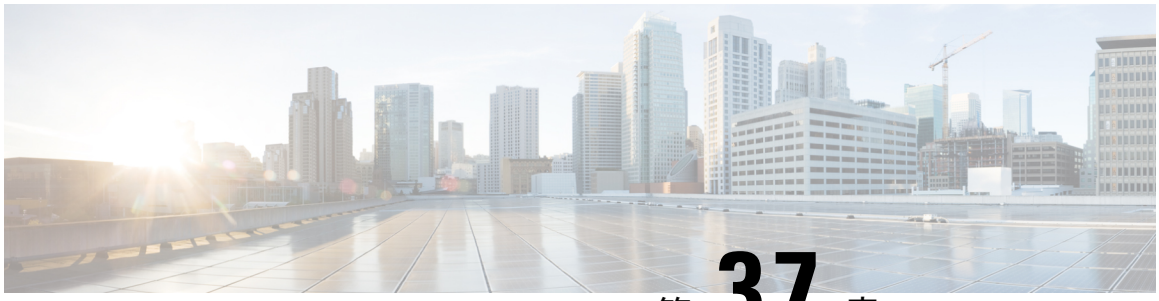
詳細情報の入手先

さまざまな IP テレフォニー トピックに関する情報については、次のリンクを使用してください。

- 関連する Cisco IP テレフォニー アプリケーションおよび製品に関する詳細については、『*Cisco Unified Communications Manager* のドキュメンテーション ガイド』を参照してください。 次の URL は、マニュアルへのパスの例です。

  https://www.cisco.com/en/US/products/sw/voicesw/ps556/products_documentation_roadmaps_list.html

- Cisco Unity に関連するマニュアルについては、次の URL を参照してください。 *https://www.cisco.com/en/US/products/sw/voicesw/ps2237/tsd_products_support_series_home.html*
- Cisco Emergency Responderに関連するマニュアルについては、次の URL を参照してください。 *https://www.cisco.com/en/US/products/sw/voicesw/ps842/tsd_products_support_series_home.html*
- Cisco Unified IP 電話に関連するマニュアルについては、次の URL を参照してください。 *https://www.cisco.com/en/US/products/hw/phones/ps379/tsd_products_support_series_home.html*
- IP テレフォニー ネットワークの設計とトラブルシューティングについては、*https://www.cisco.com/go/srnd*にある『Cisco IP テレフォニー リファレンス ネットワーク設計ガイド』を参照してください。



第 37 章

トラブルシューティング ツール

ここでは、Unified Communications Manager の設定、監視、およびトラブルシューティングを行うために使用するツールやユーティリティについて説明し、テストの繰り返しや同一データの再収集を回避するためのデータ収集に関する一般的なガイドラインを提供します。

（注） このマニュアルにリストされている URL サイトの一部にアクセスするには、登録ユーザとしてログインする必要があります。

Cisco Unified Serviceability トラブルシューティング ツール

Cisco Unified Serviceabilityには、さまざまなUnified Communications Managerシステムを監視および分析するために、次のような各種ツールが用意されています。これらのツールの詳細については、『*Cisco Unified Serviceability* アドミニストレーション ガイド』を参照してください。

表 *94 : Serviceability* ツール

用語	定義
Cisco Unified Real-Time Monitoring Tool（RTMT）	このツールは、Unified Communications Managerのデバイスとパフォーマンス カウンタに関するリアルタイムな情報を提供するとともに、トレースの収集を可能にします。 パフォーマンス カウンタは、システム固有か、またはUnified Communications Manager固有である場合があります。 オブジェクトは、Cisco Unified IP 電話 や Unified Communications Manager などの、特定のデバイスまたは機能に対する同等のカウンタの論理的なグループで構成されています。 カウンタによって、システム パフォーマンスのさまざまな側面が測定されます。 登録済み電話機の数、試行されたコール数、進行中のコール数などの統計が測定されます。
アラーム	管理者は、アラームを使用して、Unified Communications Manager システムの実行時のステータスや状態情報を取得します。アラームには、説明や推奨処置など、システムの問題に関する情報が含まれています。 管理者は、アラーム定義データベースでアラーム情報を検索します。アラーム定義には、アラームの説明と推奨処置が含まれています。
トレース	管理者とシスコのエンジニアは、トレース ファイルを使用して、Unified Communications Managerシステムの問題に関する特定の情報を取得します。Cisco Unified Serviceabilityは設定されたトレース情報をトレース ログファイルに送信します。 トレース ログ ファイルには、SDI と SDL の 2 種類があります。 各サービスには、デフォルトのトレース ログが含まれています。 システムによって、サービスからのシステム診断インターフェイス（SDI）情報がトレースされ、実行時のイベントとトレースがログ ファイルに記録されます。 SDL トレース ログ ファイルには、Cisco CallManager や Cisco CTIManager などのサービスからのコール処理情報が含まれています。システムによって、コールの信号配信レイヤ（SDL）がトレースされ、状態遷移がログ ファイルに記録されます。 （注） .gzo ファイルは圧縮ファイルではなくテキストファイルになりました。 したがって、.gzo ファイルは圧縮解除する必要はなく、プレーンテキストとして読み取る必要があります。 （注） 通常は、Cisco Technical Assistance Center（TAC）の指示に従って、SDL トレースだけを収集することになります。
品質レポート ツール	この用語は、Cisco Unified Serviceability の音声品質と一般的な問題をレポートするユーティリティを示しています。

用語	定義
サービスアビリティコネクタ	Cisco Webex Serviceability サービスは、シスコのテクニカル サポート スタッフがより迅速にインフラストラクチャの問題を診断できます。診断ログや情報を検索、取得、保存するタスクを SR ケースに自動化します。 このサービスは、TAC がオンプレミスの機器の問題を効率的に特定し、解決できるよう、診断署名に対する分析をトリガーします。

コマンドライン インターフェイス

コマンドライン インターフェイス（CLI）を使用すると、Unified Communications Manager システムにアクセスし、基本的なメンテナンスや障害からの回復を行うことができます。ハードワイヤされた端末（システム モニタとキーボード）を使用するか、または SSH セッションを実行することによってシステムにアクセスします。

インストール時に、アカウント名とパスワードが作成されます。パスワードはインストール後に変更できますが、アカウント名は変更できません。

コマンドとは、システムに特定の機能を実行させるテキスト命令を表します。 コマンドは、単独で使用される場合と、必須または任意の引数を伴う場合があります。

レベルは、コマンドの集合で構成されます。たとえば、show はレベルを示し、show status はコマンドを示します。 また、各レベルとコマンドには、特権レベルが関連付けられています。ユーザは、適切な特権レベルを持っている場合にだけ、コマンドを実行できます。

Unified Communications Managerの CLI コマンド セットの詳細については、『*Cisco Unified* ソリューション コマンドライン インターフェイス リファレンス ガイド』を参照してください。

Kerneldump ユーティリティ

Kerneldump ユーティリティにより、セカンダリ サーバを要求することなしに、該当するマシンでクラッシュ ダンプ ログをローカルに収集できます。

Unified Communications Managerクラスタでは、Kerneldump ユーティリティがサーバで有効であることを確認するだけで、クラッシュ ダンプ情報を収集できます。

（注） シスコでは、より効果的なトラブルシューティングを実現するため、Unified Communications Managerのインストール後に、Kerneldump ユーティリティが有効であることを確認するよう推奨しています。 Kerneldump ユーティリティの設定をまだ行っていない場合は、Unified Communications Managerをサポート対象のアプライアンス リリースからアップグレードする前に行ってください。

重要 Kerneldumpユーティリティをイネーブル化またはディセーブル化を行うには、ノードのリブートが必要です。 リブートが許容されるウィンドウ以外では、enableコマンドを実行しないでください。

Cisco Unified Communications オペレーティング システムのコマンドライン インターフェイス（*CLI*）を使用すると、Kerneldumpユーティリティのイネーブル化、ディセーブル化、ステータス確認を実行できます。

次の手順を利用してKerneldumpユーティリティをイネーブル化します。

ユーティリティによって収集されるファイルの処理

Kerneldumpユーティリティから送信されたクラッシュ情報を表示するには、*Cisco Unified Real-Time Monitoring Tool* またはコマンドライン インターフェイス（*CLI*）を使用します。 *Cisco Unified Real-Time Monitoring Tool* を使用してnetdumpログを収集するには、[トレースおよびログ セントラル（Trace & Log Central）] の [ファイルの収集（Collect Files）] オプションを選択します。 [システム サービス/アプリケーションの選択（Select System Services/Applications）] タブで、[Kerneldumpログ（Kerneldump logs）] チェックボックスをオンにします。 *Cisco Unified Real-Time Monitoring Tool* を使用したファイルの収集の詳細については、『*Cisco Unified Real-Time Monitoring Tool Administration Guide*』を参照してください。

CLIを使用してkerneldumpログを収集するには、クラッシュ ディレクトリのファイルに対して「「file」」CLIコマンドを使用します。 これらは「activelog」 のパーティションの下にあります。 ログ ファイル名は、kerneldumpクライアントのIPアドレスで始まり、ファイルが作成された日付で終わります。 ファイル コマンドの詳細については、『*Command Line Interface Reference Guide for Cisco Unified Solutions*』を参照してください。

Kerneldump ユーティリティの有効化

次の手順を利用してKerneldumpユーティリティをイネーブル化します。 カーネル クラッシュが発生した場合、ユーティリティは、クラッシュの収集とダンプのメカニズムを提供します。 ローカル サーバまたは外部サーバにログをダンプするユーティリティを設定できます。

手順

ステップ 1 コマンドライン インターフェイスにログインします。

ステップ 2 次のいずれかを実行します。

- ローカルサーバー上のカーネルクラッシュを破棄するには、`utils os kerneldump enable` CLIコマンドを実行します。
- 外部サーバにカーネルクラッシュをダンプするには、外部サーバのIPアドレスを指定して `utils os kerneldump ssh enable <ip_address>` CLIコマンドを実行します。

ステップ 3 サーバをリブートします。

例

（注） kerneldumpユーティリティを無効にする必要がある場合、`utils os kernelcrash disable` コマンドを実行してローカルサーバのコアダンプを無効にし、`utils os kerneldump ssh disable <ip_address>`CLIコマンドを実行して外部サーバ上のユーティリティを無効にします。

次のタスク

コア ダンプの指示に従ってリアルタイム モニタリング ツールで電子メール アラートを設定します。 詳細は、コア ダンプの電子メール アラートの有効化 （326 ページ）を参照してください。

kerneldumpユーティリティおよびトラブルシューティングについては、『*Troubleshooting Guide for Cisco Unified Communications Manager*』を参照してください。

コア ダンプの電子メール アラートの有効化

コア ダンプが発生するたびに管理者に電子メールを送信するようにリアルタイム モニタリング ツールを設定するには、次の手順を使用します。

手順

ステップ 1 **[システム（System）]**>**[ツール（Tools）]**>**[アラート（Alert）]**>**[アラートセントラル（Alert Central）]**の順に選択します。

ステップ 2 [CoreDumpFileFound]アラートを右クリックし、[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 ウィザードの指示に従って優先条件を設定します。

a) [アラート プロパティ：電子メール通知（Alert Properties: Email Notification）] ポップアップで、[電子メールの有効化（電子メールの有効化(Enable Email)）] がオンになっていることを確認し、[設定（Configure）] をクリックしてデフォルトのアラートアクションを設定します。これにより管理者に電子メールが送信されます。

b) プロンプトに従って、受信者電子メールアドレスを**[追加（Add）]**します。 このアラートがトリガーされると、デフォルトのアクションは、このアドレスへの電子メールの送信になります。

c) **[保存]** をクリックします。

ステップ 4 デフォルトの電子メールサーバーを設定します。

a) **[システム（System）] > [ツール（Tools）] > [アラート（Alert）] > [電子メールサーバーの設定（Config Email Server）]** の順に選択します。
b) 電子メールサーバーとポート情報を入力して、電子メールアラートを送信します。
c) （任意）暗号化された通信チャネルを SMTP サーバーに対して有効にするには、**[TLS モードを有効にする（Enable TLS mode）]** チェックボックスをオンにします。
d) （任意）受信者のメールアドレスを 認証する必要がある場合は、**[認証モードを有効にする（Enable Authentication mode）]** チェックボックスをオンにします。

（注） **[ユーザー名]** と **[パスワード]** のフィールドにアクセスできるのは、**[認証モードを有効にする（Enable Authentication mode）]** チェックボックスが有効になっている場合のみです。

e) **[ユーザー名]** フィールドに、ユーザーの名前を入力します。
f) **[パスワード]** フィールドに、パスワードを入力します。
g) **[送信するユーザー ID（Send User Id）]** を入力します。
h) **OK**をクリックします。

ネットワーク管理

Unified Communications Manager のリモート有用性には、ネットワーク管理ツールを使用します。

- システム ログ管理
- Cisco Discovery Protocol のサポート
- 簡易ネットワーク管理プロトコル（SNMP）のサポート

これらのネットワーク管理ツールの詳細については、それぞれの項に記載された URL にあるマニュアルを参照してください。

システム ログ管理

Resource Manager Essentials（RME）にパッケージされている Cisco Syslog Analysis は、他のネットワーク管理システムにも適応可能ですが、シスコ デバイスから送信される Syslog メッセージの管理に最適な方法を提供します。

Cisco Syslog Analyzer は、複数アプリケーションのシステム ログの共通ストレージを提供し、その分析を行う Cisco Syslog Analysis のコンポーネントとして機能します。 もう 1 つの主要コンポーネントである Syslog Analyzer Collector は、Unified Communications Managerサーバからログ メッセージを収集します。

これら 2 つの Cisco アプリケーションが連動し、Cisco Unified Communication ソリューションの集中型システム ログ サービスを提供します。

RME のマニュアルについては、次の URL を参照してください。
http://www.cisco.com/en/US/products/sw/cscowork/ps2073/products_tech_note09186a00800a7275.shtml

Cisco Discovery Protocol のサポート

Cisco Discovery Protocol がサポートされているため、 Unified Communications Managerサーバの検出および管理が可能です。

RME のマニュアルについては、次の URL を参照してください。
http://www.cisco.com/en/US/products/sw/cscowork/ps2073/products_tech_note09186a00800a7275.shtml

簡易ネットワーク管理プロトコル（SNMP）のサポート

ネットワーク管理システム（NMS）では、業界標準インターフェイスである SNMP を使用して、ネットワーク デバイス間で管理情報が交換されます。 TCP/IP プロトコル スイートの一部である SNMP を使用すると、管理者はリモートでネットワークのパフォーマンスを管理し、ネットワークの問題を検出および解決し、ネットワークの拡張計画を立てることができます。

SNMP管理のネットワークは、管理対象デバイス、エージェント、およびネットワーク管理システムという 3 つの主要コンポーネントで構成されています。

- 管理対象デバイスは、SNMPエージェントを含み、管理対象ネットワークに存在するネットワーク ノードを指します。 管理対象デバイスには管理情報が収集および格納され、その情報は SNMP を使用することによって利用可能になります。
- エージェントは、ネットワーク管理ソフトウェアとして、管理対象デバイスに存在します。エージェントには、管理情報のローカルな知識が蓄積され、SNMP と互換性のある形式に変換されます。
- ネットワーク管理システムは、SNMP管理アプリケーションと、そのアプリケーションが実行されるコンピュータで構成されています。 NMS では、管理対象デバイスをモニタおよび制御するアプリケーションが実行されます。 ネットワーク管理に必要な処理とメモリリソースの大部分は、NMS によって提供されます。 次の NMS は Unified Communications Manager と互換性を持っています。
  - CiscoWorks Common Services Software
  - HP OpenView
  - SNMP および Unified Communications Manager SNMP インターフェイスをサポートしているサードパーティ製アプリケーション

スニファ トレース

通常、スニファ トレースは、VLANまたは問題の情報が含まれるポート（CatOS、Cat6K-IOS、XL-IOS）にまたがるように設定されたCatalystポートに、ラップトップやその他のスニファ搭

載デバイスを接続することによって収集します。利用可能なポートが空いていない場合は、スニファ搭載デバイスを、スイッチとデバイスの間に挿入されるハブに接続します。

ヒント　TAC のエンジニアがトレースを読解しやすいように、TAC で広く使用されている Sniffer Pro ソフトウェアを使用することを推奨します。

IP Phone、ゲートウェイ、Unified Communications Manager など、関連するすべての装置の IP/MAC アドレスを利用可能にしておいてください。

デバッグ

debug 特権 EXEC コマンドの出力は、プロトコルのステータスおよびネットワーク アクティビティ全般に関する、さまざまなネットワーク間イベントについての診断情報を提供します。

端末エミュレータ ソフトウェア（ハイパーターミナルなど）を設定し、デバッグ出力をファイルに取得できるようにしてください。 ハイパーターミナルで、**[転送（Transfer）]**をクリックし、**[テキストのキャプチャ（Capture Text）]**をクリックして、適切なオプションを選択します。

IOS 音声ゲートウェイ デバッグを実行する前に、**servicetimestampsdebugdatetimemsec** がゲートウェイでグローバルに設定されていることを確認してください。

（注）　運用時間中にライブ環境でデバッグを収集することは避けてください。

運用時間外にデバッグを収集することを推奨します。ライブ環境でデバッグを収集する必要がある場合は、**no logging console** oy**loggingbuffered**を設定します。 デバッグを収集するには、**show log** を使用します。

デバッグは長くなることがあるため、コンソール ポート（デフォルトの **logging console**）またはバッファ（**logging buffer**）でデバッグを直接収集します。セッションを介してデバッグを収集すると、デバイスのパフォーマンスが低下して、デバッグが不完全となり、デバッグを再収集する必要が生じることがあります。

デバッグを停止するには、**no debug all** コマンドまたは **undebug all** コマンドを使用します。**show debug** コマンドを使用して、デバッグがオフになっていることを確認してください。

Cisco Secure Telnet

シスコ サービス エンジニア（*CSE*）は、Cisco Secure Telnet を使用して、サイト上のUnified Communications Managerノードに対して透過的にファイアウォール アクセスを実行できます。*Cisco Secure Telnet* は、強力な暗号化を使用して、シスコ内の特別な Telnet クライアントを、ファイアウォールの内側にある Telnetデーモンに接続できます。 このセキュアな接続により、

ファイアウォールを変更せずに、Unified Communications Managerノードの監視およびトラブルシューティングをリモートで行うことができます。

（注） シスコは、お客様の承諾を得た場合にだけこのサービスを提供します。サイトに、このプロセスの開始を支援するネットワーク管理者を配置する必要があります。

パケット キャプチャ

ここでは、パケット キャプチャについて説明します。

関連トピック

パケット キャプチャの概要 （537 ページ）
パケット キャプチャの設定チェックリスト （538 ページ）
Standard Packet Sniffer Users アクセス コントロールグループへのエンドユーザの追加 （539 ページ）
パケット キャプチャのサービス パラメータの設定 （539 ページ）
[電話の設定（Phone Configuration）] ウィンドウでのパケット キャプチャの設定 （540 ページ）
[ゲートウェイの設定（Gateway Configuration）] ウィンドウおよび [トランクの設定（Trunk Configuration）] ウィンドウでのパケット キャプチャの設定 （541 ページ）
パケット キャプチャの構成設定 （543 ページ）
キャプチャしたパケットの分析 （544 ページ）

パケット キャプチャの概要

メディアや TCP パケットをスニフィングするサードパーティ製トラブルシューティング ツールは、暗号化をイネーブルにしたあとは機能しません。このため、問題が発生した場合は、Unified Communications Managerを使用して次のタスクを行う必要があります。

- Unified Communications Manager とデバイスとの間で交換されるメッセージのパケットの分析（Cisco Unified IP 電話[SIP と SCCP]、Cisco IOS MGCP ゲートウェイ、H.323 ゲートウェイ、H.323/H.245/H.225 トランク、または SIP トランク）。
- デバイス間の Secure Real Time Protocol（SRTP）パケットのキャプチャ。
- メッセージからのメディア暗号キー情報の抽出、およびデバイス間のメディアの復号化。

ヒント このタスクを複数のデバイスに対して同時に実行すると、CPU使用率が高くなり、コール処理が中断される可能性があります。このタスクは、コール処理が中断される危険性が最も少ないときに実行することを強く推奨します。

詳細については、Cisco Unified Communications Manager セキュリティガイドを参照してください。

パケット キャプチャの設定チェックリスト

必要なデータを抽出し、分析するには、次の作業を実行します。

手順

1. エンド ユーザを Standard Packet Sniffer Users グループに追加します。
2. Cisco Unified Communications Manager Administrationの [サービス パラメータ設定（Service Parameter Configuration）] ウィンドウで、パケット キャプチャのサービス パラメータを設定します。たとえば、Packet Capture Enable サービス パラメータを設定します。
3. [電話の設定（Phone Configuration）]、[ゲートウェイの設定（Gateway Configuration）]、または [トランクの設定（Trunk Configuration）] の各ウィンドウで、デバイスごとのパケット キャプチャの設定を行います。

（注） パケット キャプチャは、複数のデバイスで同時にはイネーブルにしないことを強く推奨します。このタスクによって、ネットワークで使用されている CPU の使用率が上昇する可能性があるためです。

4. 該当するデバイス間でスニファ トレースを使用して、SRTPパケットをキャプチャします。使用しているスニファ トレースツールに対応したマニュアルを参照してください。
5. パケットをキャプチャしたら、Packet Capture Enable サービス パラメータを False に設定します。
6. パケットの分析に必要なファイルを収集します。
7. Cisco Technical Assistance Center（TAC）がパケットを分析します。 このタスクについては、TAC に直接お問い合わせください。

関連トピック

Standard Packet Sniffer Users アクセス コントロールグループへのエンドユーザの追加 （539 ページ）
キャプチャしたパケットの分析 （544 ページ）
[ゲートウェイの設定（Gateway Configuration）] ウィンドウおよび [トランクの設定（Trunk Configuration）] ウィンドウでのパケット キャプチャの設定 （541 ページ）
[電話の設定（Phone Configuration）] ウィンドウでのパケット キャプチャの設定 （540 ページ）
パケット キャプチャのサービス パラメータの設定 （539 ページ）
パケット キャプチャの構成設定 （543 ページ）

Standard Packet Sniffer Users アクセス コントロールグループへのエンド ユーザの追加

Standard Packet Sniffer Users グループに所属するユーザは、パケット キャプチャをサポートしているデバイスについて、パケット キャプチャ モードとパケット キャプチャ時間を設定できます。 ユーザが Standard Packet Sniffer Users アクセス コントロール グループに含まれていない場合、そのユーザはパケット キャプチャを開始できません。

次の手順では、エンドユーザを Standard Packet Sniffer アクセス制御グループに追加する方法について説明します。この手順では、『Administration Guide for Cisco Unified Communications Manager』の説明に従って、Cisco Unified Communications Manager Administrationでエンド ユーザを設定したことを前提としています。

手順

1. 『Administration Guide for Cisco Unified Communications Manager』の説明に従って、アクセス制御グループを検索します。
2. [検索/リスト（Find/List）] ウィンドウが表示されたら、[標準パケット スニファ ユーザ（Standard Packet Sniffer Users）]リンクをクリックします。
3. [グループにユーザを追加（Add Users to Group）]ボタンをクリックします。
4. 『Administration Guide for Cisco Unified Communications Manager』の説明に従って、エンド ユーザを追加します。
5. ユーザを追加したら、[保存（Save）]をクリックします。

パケット キャプチャのサービス パラメータの設定

パケット キャプチャのパラメータを設定するには、次の手順を実行します。

手順

1. Unified Communications Managerで、**[システム]** > **[サービス パラメータ]** を選択します。
2. [サーバ（Server）] ドロップダウン リスト ボックスで、Cisco CallManager サービスをアクティブにした Active サーバを選択します。
3. [サービス（Service）]ドロップダウン リスト ボックスで、[Cisco CallManager（アクティブ）（Cisco CallManager (Active)）] サービスを選択します。
4. [TLS パケット キャプチャ設定（TLS Packet Capturing Configuration）] ペインまでスクロールして、パケット キャプチャを設定します。

ヒント サービスパラメータについては、ウィンドウに表示されているパラメータ名または疑問符をクリックしてください。

（注） パケット キャプチャを実行するには、Packet Capture Enable サービス パラメータを True に設定する必要があります。

5. 変更内容を有効にするには、[保存（Save）]をクリックします。
6. パケット キャプチャの設定を続行できます。

関連トピック

[ゲートウェイの設定（Gateway Configuration）] ウィンドウおよび[トランクの設定（Trunk Configuration）] ウィンドウでのパケット キャプチャの設定 （541 ページ）
[電話の設定（Phone Configuration）] ウィンドウでのパケット キャプチャの設定 （540 ページ）

[電話の設定（Phone Configuration）] ウィンドウでのパケット キャプチャの設定

[サービス パラメータ（Service Parameter）] ウィンドウでパケット キャプチャをイネーブルにしたら、Cisco Unified Communications Manager Administrationの [電話の設定（Phone Configuration）] ウィンドウで、デバイスごとにパケット キャプチャを設定できます。

電話機ごとに、パケットキャプチャをイネーブルまたはディセーブルにします。パケットキャプチャのデフォルト設定は、None です。

注意 パケットキャプチャは、複数の電話機で同時にはイネーブルにしないことを強く推奨します。このタスクによって、ネットワークで使用されている CPU の使用率が上昇する可能性があるためです。

パケットをキャプチャしない場合、またはタスクを完了した場合は、Packet Capture Enable サービス パラメータを False に設定します。

電話機のパケット キャプチャを設定するには、次の手順を実行します。

手順

1. パケット キャプチャを設定する前に、パケット キャプチャの設定に関するトピックを参照してください。
2. Cisco Unified Communications Manager システム設定ガイドの説明に従って、SIP 電話機または SCCP 電話機を検索します。
3. [電話の設定（Phone Configuration）] ウィンドウが表示されたら、「パケット キャプチャの設定値」の説明に従って、トラブルシューティングの設定を行います。
4. 設定が完了したら、[保存（Save）]をクリックします。

5. [リセット（Reset）] ダイアログボックスで、[OK]をクリックします。

ヒント Cisco Unified Communications Manager Administrationからデバイスをリセットするように求められますが、パケットをキャプチャするためにデバイスをリセットする必要はありません。

この他の手順

該当するデバイス間でスニファ トレースを使用して、SRTP パケットをキャプチャします。

パケットをキャプチャしたら、Packet Capture Enable サービス パラメータを False に設定します。

関連トピック

キャプチャしたパケットの分析 （544 ページ）
パケット キャプチャの設定チェックリスト （538 ページ）

[ゲートウェイの設定（Gateway Configuration）] ウィンドウおよび [トランクの設定（Trunk Configuration）] ウィンドウでのパケット キャプチャの設定

次のゲートウェイおよびトランクは、Unified Communications Managerでのパケット キャプチャをサポートしています。

- Cisco IOS MGCP ゲートウェイ
- H.323 ゲートウェイ
- H.323/H.245/H.225 トランク
- SIP トランク

ヒント パケット キャプチャは、複数のデバイスで同時にはイネーブルにしないことを強く推奨します。このタスクによって、ネットワークで使用されている CPU の使用率が上昇する可能性があるためです。

パケットをキャプチャしない場合、またはタスクを完了した場合は、Packet Capture Enable サービス パラメータを False に設定します。

[ゲートウェイの設定（Gateway Configuration）] ウィンドウまたは [トランクの設定（Trunk Configuration）] ウィンドウでパケット キャプチャの設定を行うには、次の手順を実行します。

手順

1. パケット キャプチャを設定する前に、パケット キャプチャの設定に関するトピックを参照してください。
2. 次のいずれかの作業を実行します。
   - Cisco Unified Communications Manager システム設定ガイドの説明に従って、Cisco IOS MGCP ゲートウェイを検索します。
   - Cisco Unified Communications Manager システム設定ガイドの説明に従って、H.323 ゲートウェイを検索します。
   - Cisco Unified Communications Manager システム設定ガイドの説明に従って、H.323、H.245、または H.225 トランクを検索します。
   - Cisco Unified Communications Manager システム設定ガイドの説明に従って、SIP トランクを検索します。
3. 設定ウィンドウが表示されたら、[パケット キャプチャ モード（Packet Capture Mode）] と [パケット キャプチャ時間（Packet Capture Duration）] の設定値を確認します。

ヒント Cisco IOS MGCP ゲートウェイを見つけたら、Cisco IOS MGCP ゲートウェイ用のポートを『Administration Guide for Cisco Unified Communications Manager』の説明に従って設定してあることを確認します。 Cisco IOS MGCP ゲートウェイのパケット キャプチャ設定値は、エンドポイント識別子の [ゲートウェイの設定（Gateway Configuration）] ウィンドウに表示されます。このウィンドウにアクセスするには、音声インターフェイス カードのエンドポイント識別子をクリックします。

4. 「パケット キャプチャの設定値」の説明に従って、トラブルシューティングを設定します。
5. パケット キャプチャを設定したら、[保存（Save）]をクリックします。
6. [リセット（Reset）] ダイアログボックスで、[OK]をクリックします。

ヒント Cisco Unified Communications Manager Administrationからデバイスをリセットするように求められますが、パケットをキャプチャするためにデバイスをリセットする必要はありません。

この他の手順

該当するデバイス間でスニファ トレースを使用して、SRTP パケットをキャプチャします。

パケットをキャプチャしたら、Packet Capture Enable サービス パラメータを False に設定します。

関連トピック

キャプチャしたパケットの分析 （544 ページ）
パケット キャプチャの設定チェックリスト （538 ページ）

パケット キャプチャの構成設定

次の表に、ゲートウェイ、トランク、および電話機にパケット キャプチャを設定する際の [パケット キャプチャ モード（Packet Capture Mode）] 設定と [パケット キャプチャ時間（Packet Capture Duration）] 設定について説明します。

設定	説明
[パケットキャプチャモード(Packet Capture Mode)]	暗号化のトラブルシューティング専用の設定。パケット キャプチャリングは、高い CPU 使用率およびコール処理中断の原因となります。 ドロップダウン リスト ボックスから、次のオプションのいずれかを選択します。 • [なし（None）]：このオプションは、パケット キャプチャが発生しないことを示します（デフォルト設定）。 パケット キャプチャが完了すると、Unified Communications Manager は [パケット キャプチャ モード（Packet Capture Mode）] を [なし（None）] に設定します。 • **[バッチ処理モード（Batch Processing Mode）]**：Unified Communications Managerが復号化または非暗号化されたメッセージをファイルに書き込み、システムが各ファイルを暗号化します。 システムは毎日、新しい暗号キーを持つ新しいファイルを作成します。 Unified Communications Manager は 7 日間ファイルを保存しますが、ファイルを暗号化するキーも安全な場所に保存します。Unified Communications Manager はファイルを PktCap 仮想ディレクトリに保存します。 単一のファイルには、タイムスタンプ、送信元 IP アドレス、送信元 IP ポート、宛先 IP アドレス、パケット プロトコル、メッセージ長、およびメッセージが含まれます。 TAC デバッグ ツールは、HTTPS、管理者のユーザ名とパスワード、および指定日を使用して、キャプチャされたパケットを含む単一の暗号化されたファイルを要求します。さらにキー情報も要求し、暗号化されたファイルを復号化します。 **ヒント** TAC に連絡する前に、該当するデバイス間でスニファ トレースを使用して、SRTP パケットをキャプチャする必要があります。

設定	説明
[パケットキャプチャ時間(Packet Capture Duration)]	暗号化のトラブルシューティング専用の設定。パケット キャプチャリングは、高い CPU 使用率およびコール処理中断の原因となります。 このフィールドには、パケット キャプチャリングの 1 つのセッションに割り当てる最大分数を指定します。 デフォルト設定は 0 です。ただし、0 ～ 300 分の範囲で指定できます。 パケット キャプチャリングを開始するには、このフィールドに 0 以外の値を入力します。 パケット キャプチャリングの完了後、0 が表示されます。

関連トピック

[ゲートウェイの設定（Gateway Configuration）] ウィンドウおよび[トランクの設定（Trunk Configuration）] ウィンドウでのパケット キャプチャの設定 （541 ページ）
[電話の設定（Phone Configuration）] ウィンドウでのパケット キャプチャの設定 （540 ページ）

キャプチャしたパケットの分析

Cisco Technical Assistance Center（*TAC*）は、デバッグ ツールを使用してパケットを分析します。 TACにお問い合わせいただく前に、該当するデバイス間でスニファ トレースを使用して、SRTP パケットをキャプチャしてください。 次の情報を収集したら、TAC に直接お問い合わせください。

- パケットキャプチャ ファイル—**https://<IP address or server name>/pktCap/pktCap.jsp?file=mm-dd-yyyy.pkt**。サーバを参照し、西暦年と日付（mm-dd-yyyy）別のパケットキャプチャ ファイルを見つけます。
- ファイルのキー—**https://<IP address or server name>/pktCap/pktCap.jsp?key=mm-dd-yyyy.pkt**。サーバを参照し、西暦年と日付（mm-dd-yyyy）別のキーを見つけます。
- Standard Packet Sniffer Users グループに所属しているエンド ユーザのユーザ名とパスワード。

詳細については、Cisco Unified Communications Manager セキュリティガイド を参照してください。

一般的なトラブルシューティングのタスク、ツール、およびコマンド

この項では、ルート アクセスが無効にされた Unified Communications Manager サーバのトラブルシューティングに役立つコマンドやユーティリティのクイック リファレンスを提供します。次の表に、システムのさまざまな問題をトラブルシューティングするための情報収集に使用できる CLI コマンドと GUI をまとめます。

表 *95 : CLI* コマンドと *GUI* 選択のまとめ

情報	Linux コマンド	サービスアビリティの GUI ツール	CLI コマンド
CPU 使用率	top	RTMT [表示（View）] タブに移動し、**[サーバ（Server）] > [CPU とメモリ（CPU and Memory）]** を選択	プロセッサ CPU 使用率： show perf query class Processor すべてのプロセスのプロセス CPU 使用率： show perf query counter Process 「% CPU Time」 個々のプロセス カウンタの詳細（CPU 使用率を含む） show perf query instance <Process task_name>
プロセスの状態	ps	RTMT [表示（View）] タブに移動し、**[サーバ（Server）] > [プロセス（Process）]** を選択	show perf query counter Process 「Process Status」
ディスク使用量	df/du	RTMT [表示（View）] タブに移動し、**[サーバ（Server）] > [ディスク使用量（Disk Usage）]** を選択	show perf query counter Partition「% Used」 または show perf query class Partition
メモリ	free	RTMT [表示（View）] タブに移動し、**[サーバ（Server）] > [CPU とメモリ（CPU and Memory）]** を選択	show perf query class Memory
ネットワーク ステータス	netstats		show network status

情報	Linux コマンド	サービスアビリティの GUI ツール	CLI コマンド
サーバのリブート	リブート（reboot）	サーバの [プラットフォーム（Platform）] Web ページにログイン **[サーバ（Server）] > [現在のバージョン（Current Version）]** に移動	utils system restart
トレース/ログの収集	Sftp、ftp	RTMT [ツール（Tools）] タブに移動し、**[トレース（Trace）] > [トレースおよびログ セントラル（Trace & Log Central）]** を選択	ファイルのリスト：file list ファイルのダウンロード：file get ファイルの表示：file view

次の表に、一般的な問題と、そのトラブルシューティングに使用するツールのリストを示します。

表 *96 : CLI* コマンドおよび *GUI* 選択オプションによる一般的な問題のトラブルシューティング

タスク	GUI ツール	CLI コマンド
データベースにアクセスする	なし	admin としてログインし、次のいずれかの **show** コマンドを使用します。 • show tech database • show tech dbinuse • show tech dbschema • show tech devdefaults • show tech gateway • show tech locales • show tech notify • show tech procedures • show tech routepatterns • show tech routeplan • show tech systables • show tech table • show tech triggers • show tech version • show tech params* SQL コマンドを実行するには、**run** コマンドを使用します。 • run sql <sql command>

タスク	GUI ツール	CLI コマンド
ディスクの空き容量を増やす （注） Log パーティションにあるファイルだけ、削除できます。	RTMT クライアントアプリケーションを使用して、[ツール（Tools）]タブに移動し、**[トレースおよびログセントラル（Trace & Log Central）]** > **[ファイルの収集（Collect Files）]** を選択します。 収集するファイルの選択基準を選択し、[ファイルの削除（Delete Files）]オプションのチェックボックスをオンにします。 この操作を実行すると、ファイルが PC にダウンロードされ、Unified Communications Manager サーバ上のファイルは削除されます。	file delete
コア ファイルを表示する	コアファイルは表示できませんが、RTMT アプリケーションを使用して **[Trace & Log Central]** > **[クラッシュ ダンプの収集（Collect Crash Dump）]** を選択すると、コア ファイルをダウンロードできます。	utils core [options]
Unified Communications Manager サーバをリブートする	サーバの [プラットフォーム（Platform）]ページにログインし、**[リスタート（Restart）]** > **[現在のバージョン（Current Version）]** に移動します。	utils system restart
トレースのデバッグレベルを変更する	*Cisco Unity Connection Serviceability* Administration（`https://<server_ipaddress>:8443/ccmservice/`）にログインして、**[トレース（Trace）]** > **[設定（Configuration）]**を選択します。	set trace enable [Detailed, Significant, Error, Arbitrary, Entry_exit, State_Transition, Special] [syslogmib, cdpmib, dbl, dbnotify]
ネットワークのステータスを表示する	なし	show network status

トラブルシューティングのヒント

次の各ヒントは、Unified Communications Manager のトラブルシューティングに役立ちます。

ヒント　Unified Communications Manager のリリース ノートで既知の問題を確認します。 リリース ノートには、既知の問題の説明と対応策が記載されています。

ヒント　デバイスの登録先を確認します。

各 Unified Communications Manager ログはファイルをローカルでトレースします。 電話機またはゲートウェイが特定の Unified Communications Manager に登録されている場合、その Unified Communications Manager でコールが開始されると、コール処理はそこで実行されます。 問題をデバッグするには、その Unified Communications Manager 上のトレースを取り込む必要があります。

デバイスがサブスクライバ サーバに登録されているにもかかわらず、パブリッシャ サーバ上のトレースを取り込むという間違いがよくあります。 そのトレース ファイルはほとんど空です（そのファイルには目的のコールが含まれていません）。

デバイス 1 を CM1 に登録し、デバイス 2 を CM2 に登録しているために問題が生じることも多くあります。 デバイス 1 がデバイス 2 をコールすると CM1 でコール トレースが実行され、デバイス 2 がデバイス 1 をコールすると CM2 でトレースが実行されます。 双方向のコール問題のトラブルシューティングを行う場合は、トラブルシューティングに必要なすべての情報を得るために、両方の Unified Communications Manager からの両方のトレースが必要となります。

ヒント　問題のおおよその時刻を確認します。

複数のコールが発信された可能性があるため、コールのおおよその時刻を確認していると、TAC が問題を迅速に特定するのに役立ちます。

Cisco Unified IP 電話 79xx の電話機統計情報は、**i** または **?** ボタンをアクティブ コール中に 2 回押すと取得できます。

テストを実行して問題を再現し、情報を生成する場合は、問題を理解するために不可欠な次のデータを確認してください。

- 発信側の番号または着信側の番号
- 特定のシナリオに関係する他の番号
- コールの時刻

（注）　トラブルシューティングには、すべての機器の時刻が同期化されていることが重要であることに注意してください。

問題を再現している場合は、ファイルの変更日付とタイムスタンプを調べて、その時間枠のファイルを選択します。適切なトレースを収集する最良の方法は、問題を再現してからすぐに最新のファイルを見つけ、そのファイルを Unified Communications Manager サーバからコピーすることです。

ヒント ログ ファイルを保存して、上書きされないようにします。

ファイルは、時間が経つと上書きされます。ログが記録されているファイルを調べる唯一の方法は、メニューバーで **[表示（View）]** > **[更新（Refresh）]** を選択し、ファイルの日付と時刻を確認することです。

システム履歴ログ

システム履歴ログを使用すると、システムの初期インストール、システムのアップグレード、Cisco オプションのインストール、DRS バックアップと DRS 復元、バージョン切り替えとリブート履歴などの情報の概要を中央からすばやく把握できます。

関連トピック

システム履歴ログの概要 （550 ページ）
システム履歴ログのフィールド （551 ページ）
システム履歴ログへのアクセス （552 ページ）

システム履歴ログの概要

システム履歴ログは、**system-history.log** という単純な ASCII ファイルとして保管され、そのデータはデータベース内には保持されません。サイズが膨大ではないため、ローテーションされることはありません。

システム履歴ファイルには、次の機能があります。

- サーバ上のソフトウェアの初期インストールを記録します。
- ソフトウェアの各アップデート（Cisco オプション ファイルおよびパッチ）の成功、失敗、またはキャンセルを記録します。
- 実行される各 DRS バックアップと復元を記録します。
- CLI または GUI によって発行されるバージョン切り替えの各呼び出しを記録します。
- CLI または GUI によって発行される再起動およびシャットダウンの各呼び出しを記録します。
- システムの各ブートを記録します。 再起動エントリまたはシャットダウン エントリと関連付けられていない場合のブートは、手動リブート、電源サイクル、またはカーネル パニックの結果として発生したものです。

- 初期インストール以降、または機能が利用可能になって以降のシステム履歴を単一ファイルに保持します。
- インストール フォルダに存在します。 **file** コマンドか、または Real Time Monitoring Tool（RTMT）を使用して、CLI からログにアクセスできます。

システム履歴ログのフィールド

ログには、製品名、製品バージョン、およびカーネルイメージに関する情報を含む、次のような共通のヘッダーが表示されます。

==========

Product Name - Unified Communications Manager

Product Version - 7.1.0.39000-9023

Kernel Image - 2.6.9-67.EL

==========

システム履歴ログの各エントリには、次のようなフィールドがあります。

timestamp userid action description start/result

システム履歴ログのフィールドには、次のような値が含まれます。

- *timestamp*：サーバ上のローカルな日付と時刻が *mm/dd/yyyy hh:mm:ss* の形式で表示されます。
- *userid*：アクションを呼び出したユーザの名前が表示されます。
- *action*：次のいずれかのアクションが表示されます。
  - インストール
  - Windows アップグレード
  - インストール時のアップグレード
  - アップグレード
  - Cisco オプションのインストール
  - バージョン切り替え
  - システム再起動
  - Shutdown
  - Boot
  - DRS バックアップ
  - DRS 復元
- *description*：次のいずれかのメッセージが表示されます。

- *Version*：基本インストール、Windows アップグレード、インストール時のアップグレード、アップグレードの各アクションが表示されます。
- *Cisco Option file name*：Cisco オプションのインストールのアクションが表示されます。
- *Timestamp*：DRS バックアップと DRS 復元の各アクションが表示されます。
- *Active version to inactive version*：バージョン切り替えのアクションが表示されます。
- *Active version*：システム再起動、シャットダウン、およびブートの各アクションが表示されます。

- *result*：次の結果が表示されます。
  - 開始
  - 成功または失敗
  - キャンセル（Cancel）

次に、システム履歴ログの例を示します。

```
admin:file dump install system-history.log=====================================
 Product Name - Cisco Unified Communications Manager Product Version -
6.1.2.9901-117 Kernel Image - 2.4.21-47.EL.cs.3BOOT
===================================== 07/25/2008 14:20:06 | root: Install
6.1.2.9901-117 Start 07/25/2008 15:05:37 | root: Install 6.1.2.9901-117 Success
 07/25/2008 15:05:38 | root: Boot 6.1.2.9901-117 Start 07/30/2008 10:08:56 |
root: Upgrade 6.1.2.9901-126 Start 07/30/2008 10:46:31 | root: Upgrade
6.1.2.9901-126 Success 07/30/2008 10:46:43 | root: Switch Version 6.1.2.9901-117
 to 6.1.2.9901-126 Start 07/30/2008 10:48:39 | root: Switch Version
6.1.2.9901-117 to 6.1.2.9901-126 Success 07/30/2008 10:48:39 | root: Restart
6.1.2.9901-126 Start 07/30/2008 10:51:27 | root: Boot 6.1.2.9901-126 Start
08/01/2008 16:29:31 | root: Restart 6.1.2.9901-126 Start 08/01/2008 16:32:31
| root: Boot 6.1.2.9901-126 Start
```

システム履歴ログへのアクセス

システム履歴ログにアクセスするには、CLI または RTMT を使用できます。

CLI の使用

次のように CLI の **file** コマンドを使用すると、システム履歴ログにアクセスできます。

- **file view install system-history.log**
- **file get install system-history.log**

CLI **ファイル** コマンドの詳細については、『*Command Line Interface Reference Guide for Cisco Unified Communications Solutions*』を参照してください。

RTMT の使用

RTMT を使用してシステム履歴ログにアクセスすることもできます。 [Trace and Log Central] タブで、[インストール ログの収集（Collect Install Logs）]を選択します。

RTMT の使用の詳細については、『*Cisco Unified Real-Time Monitoring Tool Administration Guide*』を参照してください。

監査ロギング

一元化された監査ロギングにより、Unified Communications Manager システムへの設定変更を監査用の別のログ ファイルに記録できます。 監査イベントは、記録する必要があるすべてのイベントを指します。 次の Unified Communications Manager コンポーネントによって監査イベントが生成されます。

- Cisco Unified Communications Manager Administration
- Cisco Unified Serviceability
- *Unified Communications Manager CDR Analysis and Reporting*
- *Cisco Unified Real-Time Monitoring Tool*
- *Cisco Unified Communications Operating System*
- *Disaster Recovery System*
- データベース
- コマンドライン インターフェイス
- Remote Support Account Enabled（テクニカル サポート チームによって発行される CLI コマンド）

Cisco Business Edition 5000 では、次のCisco Unity Connectionコンポーネントによっても監査イベントが生成されます。

- Cisco Unity Connection の管理
- *Cisco Personal Communications Assistant* (Cisco PCA)
- Cisco Unity Connection サービスアビリティ
- Representational State Transfer（REST）API を使用する Cisco Unity Connection クライアント

次に、監査イベントの例を示します。

```
CCM_TOMCAT-GENERIC-3-AuditEventGenerated: Audit Event Generated
UserID:CCMAdministrator Client IP Address:172.19.240.207 Severity:3
EventType:ServiceStatusUpdated ResourceAccessed: CCMService
EventStatus:Successful Description: Call Manager Service status is stopped App
 ID:Cisco Tomcat Cluster ID:StandAloneCluster Node ID:sa-cm1-3
```

監査イベントに関する情報が含まれている監査ログは、共通のパーティションに書き込まれます。 これらの監査ログのページは、トレース ファイルと同様に、Log Partition Monitor（LPM）によって管理されます。 デフォルトでは、LPM によって監査ログがパージされますが、監査ユーザは Cisco Unified Serviceability の [Audit User Configuration] ウィンドウからこの設定を変更できます。 共通パーティションのディスク使用量がしきい値を超えると、LPM によってアラートが送信されますが、アラートには、ディスクが監査ログまたはトレース ファイルによっていっぱいであるかどうかに関する情報は含まれていません。

ヒント　監査ログをサポートするネットワーク サービスである Cisco Audit Event Service は、Cisco Unified Serviceability のコントロール センターのネットワーク サービスに表示されます。 監査ログへの書き込みが行われない場合は、 Cisco Unified Serviceabilityで **[Tools]** > **[Control Center-Network Services]** を選択し、このサービスを停止してから開始します。

監査ログはすべて、*Cisco Unified Real-Time Monitoring Tool* の Trace and Log Central から収集、表示、および削除されます。 RTMT の Trace and Log Central で監査ログにアクセスします。 **[システム]** > **[リアルタイム トレース]** > **[監査ログ]** > **[ノード]** に移動します。 ノードを選択したら、別のウィンドウに **[システム]** > **[Cisco 監査ログ]** が表示されます。

RTMT には、次のタイプの監査ログが表示されます。

- アプリケーション ログ
- データベース ログ
- オペレーティング システム ログ
- リモート SupportAccEnabled ログ

アプリケーション ログ

RTMT の AuditApp フォルダに表示されるアプリケーション監査ログには、Cisco Unified Communications Manager Administration、Cisco Unified Serviceability、*CLI*、*Cisco Unified* リアルタイム監視ツール（*RTMT*）、ディザスタ リカバリ システム、およびCisco Unified CDR Analysis and Reporting（CAR）の設定変更が記録されます。 *Cisco Business Edition 5000* の場合、アプリケーション監査ログにはCisco Unity Connectionの管理、*Cisco Personal Communications Assistant*（Cisco PCA）、Cisco Unity Connectionのサービスアビリティ、および Representational State Transfer（REST）API を使用するクライアントに対する変更も記録されます。

アプリケーション ログはデフォルトでは有効になっていますが、Cisco Unified Serviceabilityで **[Tools]** > **[Audit Log Configuration]** を選択することによって設定を変更できます。 設定可能な監査ログの設定については、『*Cisco Unified Serviceability Administration Guide*』を参照してください。

Cisco Unified Serviceabilityで監査ログが無効になると、監査ログ ファイルは新規で作成されなくなります。

ヒント　監査のロールを割り当てられたユーザだけが監査ログの設定を変更する権限を持っています。新規のインストールまたはアップグレード後には、デフォルトで CCMAdministrator に監査のロールが割り当てられます。 CCMAdministrator は、監査のために作成した新規ユーザを「「Standard Audit Users」」グループに割り当てることができます。 その後、CCMAdministrator を監査ユーザ グループから削除できます。 「「Standard Audit Log Configuration」」ロールには、監査ログを削除する権限と、*Cisco Unified Real-Time Monitoring Tool*、Trace Collection Tool、RTMT Alert Configuration、[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）] ウィンドウ、RTMT Profile Saving、[監査の設定（Audit Configuration）] ウィンドウ、および Audit Traces という新規リソースへの読み取り/更新権限が与えられます。 *Cisco Business Edition 5000* の Cisco Unity Connection の場合、インストール時に作成されたアプリケーション管理アカウントは、Audit Administrator ロールに割り当てられます。このアカウントは、他の管理者ユーザをこのロールに割り当てることができます。

Unified Communications Manager は、設定された最大ファイル サイズに達するまで、1 つのアプリケーション監査ログ ファイルを使用します。最大ファイル サイズに達すると、そのファイルを閉じ、新規アプリケーション監査ログ ファイルを作成します。 システムでログ ファイルのローテーションが指定されている場合、Unified Communications Manager は設定されている数のファイルを保存します。 ログ イベントの一部は、RTMT SyslogViewer を使用して表示できます。

以下の Cisco Unified Communications Manager Administrationのイベントは、ログに記録されます。

- ユーザのログイン/ログアウト。
- ユーザのロール メンバーシップの更新（ユーザの追加、ユーザの削除、またはユーザのロールの更新）。
- ロールの更新（新しいロールの追加、削除、または更新）。
- デバイスの更新（電話機およびゲートウェイ）。
- サーバ設定の更新（アラームまたはトレースの設定、サービス パラメータ、エンタープライズ パラメータ、IP アドレス、ホスト名、イーサネット設定の変更、および Unified Communications Manager サーバの追加または削除）

以下の Cisco Unified Serviceabilityのイベントは、ログに記録されます。

- Serviceability ウィンドウからのサービスのアクティベーション、非アクティブ化、開始、または停止。
- トレース設定およびアラーム設定の変更。
- SNMP 設定の変更。
- CDR 管理の変更。
- サービスアビリティ レポートのアーカイブのレポートの参照。 このログはレポーター ノードで表示します。

RTMT では、次のイベントが監査イベント アラームとともに記録されます。

- アラートの設定。
- アラートの中断。
- 電子メールの設定。
- ノード アラート ステータスの設定。
- アラートの追加。
- アラートの追加アクション。
- アラートのクリア。
- アラートのイネーブル化。
- アラートの削除アクション。
- アラートの削除。

Unified Communications Manager CDR Analysis and Reporting では、次のイベントが記録されます。

- CDR Loader のスケジュール。
- 日次、週次、月次のユーザ レポート、システム レポート、およびデバイス レポートのスケジュール。
- メール パラメータの設定。
- ダイヤル プランの設定。
- ゲートウェイの設定。
- システム プリファレンスの設定。
- 自動消去の設定。
- 接続時間、時刻、および音声品質の評価エンジンの設定。
- QoS の設定。
- 事前生成レポートの自動生成/アラートの設定
- 通知限度の設定。

ディザスタ リカバリ システムでは、次のイベントが記録されます。

- 開始に成功または失敗したバックアップ
- 開始に成功または失敗した復元
- 正しくキャンセルされたバックアップ
- 完了に成功または失敗したバックアップ

- 完了に成功または失敗した復元
- バックアップ スケジュールの保存、更新、削除、イネーブル化、ディセーブル化
- バックアップの宛先デバイスの保存、更新、削除

Cisco Business Edition 5000 の場合、Cisco Unity Connectionの管理では、次のイベントが記録されます。

- ユーザのログイン/ログアウト。
- すべての設定変更（ユーザ、連絡先、コール管理オブジェクト、ネットワーク、システム設定、テレフォニーなど）。
- タスク管理（タスクの有効化/無効化）。
- 一括管理ツール（一括作成、一括削除）。
- カスタム キーパッド マップ（マップの更新）

Cisco Business Edition 5000 の場合、Cisco PCA では、次のイベントが記録されます。

- ユーザのログイン/ログアウト。
- Messaging Assistant で行われたすべての設定変更。

Cisco Business Edition 5000 の場合、Cisco Unity Connectionのサービスアビリティ ログでは、次のイベントが記録されます。

- ユーザのログイン/ログアウト。
- すべての設定変更。
- サービスのアクティブ化、非アクティブ化、開始、または停止。

Cisco Business Edition 5000 の場合、REST API を使用するクライアントでは、次のイベントが記録されます。

- ユーザのログイン（ユーザの API 認証）。
- Cisco Unity Connection プロビジョニング インターフェイス（CUPI）を使用する API 呼び出し。

データベース ログ

RTMT の informix フォルダに表示されるデータベース監査ログでは、データベースの変更がレポートされます。 このログは、デフォルトでは有効になっていませんが、 Cisco Unified Serviceabilityで **[Tools]** > **[Audit Log Configuration]** を選択することによって設定を変更できます。 設定可能な監査ログの設定については、Cisco Unified Serviceabilityを参照してください。

このログは、アプリケーションの設定変更を記録するアプリケーション監査ログとは異なり、データベースの変更を記録します。 Cisco Unified Serviceability でデータベース監査がイネーブルに設定されるまで、informix フォルダは RTMT に表示されません。

オペレーティング システム ログ

RTMT の vos フォルダに表示されるオペレーティング システム監査ログでは、オペレーティング システムによってトリガーされるイベントがレポートされます。 デフォルトでは、イネーブルになっていません。 **utils auditd** CLI コマンドによって、イネーブルまたはディセーブルにしたり、イベントのステータスを提供したりできます。

CLI で監査がイネーブルに設定されるまで、vos フォルダは RTMT に表示されません。

CLI の詳細については、『*Cisco Unified Solutions* コマンドライン インターフェイス リファレンス ガイド』を参照してください。

リモート サポート アカウント イネーブル化ログ

RTMT の vos フォルダに表示されるリモート サポート アカウント イネーブル化ログでは、テクニカル サポート チームによって発行される CLI コマンドがレポートされます。 このログの設定は変更できません。このログは、テクニカル サポート チームによってリモート サポート アカウントがイネーブルに設定された場合にだけ作成されます。

Cisco Unified Communications Manager サービスが稼働しているかどうかの確認

サーバ上で Cisco CallManager サービスがアクティブであることを確認するには、次の手順を実行します。

手順

1. Cisco Unified Communications Manager Administrationの **[ナビゲーション] メニューで、** > **[Cisco Unified Serviceability]** を選択します。
2. **[ツール（Tools）]** > **[サービス アクティベーション（Service Activation）]** を選択します。
3. [サーバ（Server）] カラムから必要なサーバを選択します。

   選択したサーバが [現在のサーバ（Current Server）] というタイトルの隣に表示され、設定済みのサービスを示す一連のボックスが表示されます。

   Cisco CallManager 行の [アクティベーション ステータス（Activation Status）] カラムに、[アクティブ化（Activated）] または [非アクティブ（Deactivated）] と表示されます。

   [アクティブ化（Activated）]というステータスが表示されている場合、選択したサーバ上で、指定した Cisco CallManager サービスがアクティブのままになっています。

   [非アクティブ（Deactivated）]というステータスが表示されている場合は、引き続き次のステップを実行します。
4. 目的の Cisco CallManager サービスのチェックボックスをオンにします。
5. [更新（Update）]ボタンをクリックします。

指定した Cisco CallManager サービス行の [アクティベーション ステータス（Activation Status）] カラムに [アクティブ化（Activated）]と表示されます。

これで、選択したサーバ上の指定したサービスがアクティブになります。

Cisco CallManager サービスがアクティブであるかどうか、およびサービスが現在動作しているかどうかを確認するには、次の手順を実行します。

手順

1. Cisco Unified Communications Manager Administrationの **[ナビゲーション] メニューで、> [Cisco Unified Serviceability]** を選択します。

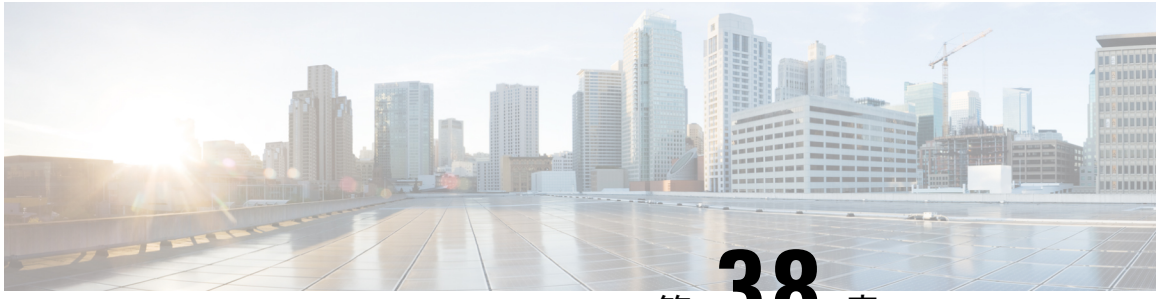
   [Cisco Unified サービスアビリティ（Cisco Unified Serviceability）] ウィンドウが表示されます。

2. **[ツール（Tools）] > [コントロール センター - 機能サービス（Control Center - Feature Services）]** の順に選択します。

3. [サーバ（Server）] カラムからサーバを選択します。

   選択したサーバが Current Server というタイトルの隣に表示され、設定済みのサービスを示すボックスが表示されます。

   [ステータス（Status）] カラムに、選択したサーバでどのサービスが動作しているかが表示されます。



第 38 章

TAC とのケースのオープン

この項では、TAC に問い合わせる場合に必要な情報の詳細、および TAC の担当者と情報を共有する方法について説明します。

シスコテクニカルサポートでは、有効なシスコ サービス契約を保有しているすべてのお客様、パートナー、リセラー、およびディストリビュータ向けに、24時間対応の高い評価を得ているテクニカル サポートを用意しています。 Cisco Technical Support Web サイトでは、シスコ製品やシスコ テクノロジーに関する技術的な問題を解決するためのオンラインのドキュメントやツールをご利用いただけます。 この Web サイトは、24 時間 365 日、いつでも利用可能です。URL は次のとおりです。*http://www.cisco.com/techsupport*

オンラインの TAC Service Request Tool を使用すると、S3 と S4 のサービス リクエストを短時間でオープンできます（S3 と S4 の問題とは、ネットワークの障害が軽微である場合、あるいは製品情報が必要な場合を意味します）。 状況をご説明いただくと、TAC Service Request ツールが自動的に推奨する解決方法を提供します。 これらの推奨手段で問題を解決できない場合は、Cisco TAC のエンジニアが対応します。 次の URL で TAC サービスリクエストツールを検索してください。 *http://www.cisco.com/techsupport/servicerequest*

S1 または S2 に関して、またはインターネット アクセスがない場合は、電話で Cisco TAC にご連絡ください。 （S1 または S2 の問題とは、運用中のネットワークがダウンした場合、あるいは重大な障害が発生した場合を意味します）。 S1 および S2 の問題には Cisco TAC の技術者がただちに対応し、業務を円滑に実行できるよう支援します。

電話でサービス リクエストを開く場合は、次の番号にご連絡ください。

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)

EMEA: +32 2 704 55 55

米国：1 800 553 2447

詳細な Cisco TAC の連絡先については、次の URL を参照してください。
http://www.cisco.com/techsupport/contacts

- Remote Access （566 ページ）
- Cisco Secure Telnet （566 ページ）
- リモート アカウントの設定 （568 ページ）

必要な情報

Cisco TAC に対してサービス リクエストをオープンする場合は、問題を特定し、その内容を把握しやすくするための予備的情報をご提供いただく必要があります。問題の内容によっては、追加の情報をご提供いただく必要があります。次に示す情報をエンジニアから要求されなくても遅滞なく収集してください。サービス リクエストをオープンし、エンジニアから要求されたあとに収集を開始すると、問題の解決が遅くなります。

関連トピック

Cisco Live! （565 ページ）
Cisco Secure Telnet （566 ページ）
全般情報 （563 ページ）
ネットワーク レイアウト （562 ページ）
オンライン ケース （564 ページ）
問題の説明 （563 ページ）
Remote Access （566 ページ）
必要な予備的情報 （562 ページ）

必要な予備的情報

すべての問題において、必ず次の情報を TAC に提供してください。 この情報を収集および保存して TAC サービス リクエストをオープンするときに使用できるようにし、変更があった場合には定期的に更新します。

関連トピック

全般情報 （563 ページ）
ネットワーク レイアウト （562 ページ）
問題の説明 （563 ページ）

ネットワーク レイアウト

物理セットアップおよび論理セットアップの詳細な説明、および音声ネットワークに関連する次のすべてのネットワーク要素をお知らせください（存在する場合）。

- Unified Communications Manager
  - バージョン（Unified Communications Manager Administration で **[詳細]** を選択）
  - Unified Communications Manager の数

- セットアップ（スタンドアロン、クラスタ）
  - Unity
- バージョン（Unified Communications Manager Administration から）
- 統合のタイプ
  - アプリケーション
- インストールされているアプリケーションのリスト
- 各アプリケーションのバージョン番号
  - IP/音声ゲートウェイ
- OS のバージョン
- show tech コマンド（IOS ゲートウェイ）
- Unified Communications Manager の負荷（Skinny ゲートウェイ）
  - スイッチ（Switch）
- OS のバージョン
- VLAN の設定
  - ダイヤル プラン：番号付け方式、コール ルーティング

Visio や JPG などで作成した詳細な図を提出すると理想的です。 ホワイトボードを使用して、Cisco Live! セッションから図を提供することもできます。

問題の説明

問題が発生したときにユーザが実行した処理について、手順ごとの詳細を提供します。 詳細情報には、次の内容を含める必要があります。

- 予想される動作
- 実際に観察された動作の詳細

全般情報

次の情報を準備する必要があります。

- 新しいインストールかどうか

- 以前のバージョンのUnified Communications Managerがインストールされている場合、最初からこの問題が発生していたかどうか（最初から発生していない場合は、最近システムに対して行った変更）
- この問題は再現可能かどうか
  - 再現可能である場合は、通常の環境で発生するか、または特別な環境で発生するか
  - 再現不可能である場合は、問題発生のタイミングが特別であったかどうか
  - 発生の頻度
- 影響のあるデバイス
  - ランダムなデバイスではなく、特定のデバイスが影響を受ける場合、影響を受けるデバイスの共通点は何か
  - 問題に関連するすべてのデバイスの DN または IP アドレス（ゲートウェイの場合）
- コール パス上のデバイス（存在する場合）

オンライン ケース

Cisco.com から TAC Case Open ツールのオンライン サービスを使用すると、他のすべてのサービス リクエスト オープン方法よりも優先的に処理されます。 ただし、高優先度のサービス リクエスト（P1 および P2）は例外です。

サービス リクエストをオープンする場合は、問題についての正確な説明を提供してください。問題の説明を提供すると、すぐに解決策として使用できる可能性がある URL リンクが返されます。

リンクを参照しても問題の解決策が見つからない場合は、プロセスを続行して、サービス リクエストを TAC エンジニアに送信してください。

サービスアビリティコネクタ

サービスアビリティコネクタ の概要

Webex Serviceability サービスを使用すると、ログの収集を容易にすることができます。 このサービスでは、診断ログや情報を検索、取得、保管するタスクを自動化します。

この機能は、お客様の社内に導入された サービスアビリティコネクタ を使用します。 サービスアビリティコネクタ は、ネットワーク内の専用ホスト（「コネクタ ホスト」）で実行されます。 次のいずれかのコンポーネントにコネクタを取り付けできます。

- Enterprise Platform (ECP) の利用: 推奨

ECP は、Docker コンテナを使用してサービスを分離、保護、管理します。 ホストとサービスアビリティ コネクタ アプリケーションがクラウドからインストールされます。 最新の状態で安全な状態を確保するために、手動でアップグレードする必要はありません。

重要 ECP の使用を推奨します。 私たちの将来の開発は、このプラットフォームに焦点を当てます。 Expressway に有用性コネクタをインストールすると、一部の新機能が使用できなくなります。

- Cisco Expressway

Serviceability コネクタは、次の目的で使用できます。

- サービス要求のログおよびシステム情報の自動取得
- クラウド接続型 UC 導入内の Unified CM クラスタのログ収集

どちらの使用例にも同じ Serviceability コネクタを使用できます。

Serviceability サービスを使用する利点

サービスには次の利点があります。

- ログの収集速度を上がります。 TAC エンジニアは、問題の診断を実行する際に関連するログを取得できます。 追加のログ リクエストや手動による収集と配送の待機の遅延を回避できます。 この自動化により、問題解決に要する時間を数日短縮できる可能性があります。
- TAC のコラボレーション ソリューション 解析ツールおよび診断署名データベースと連携します。 システムは、ログを自動的に分析し、既知の問題を特定し、既知の修正または回避策を推奨します。

サービスアビリティコネクタ の TAC サポート

サービスアビリティコネクタ の詳細については、https://www.cisco.com/go/serviceability を参照するか、TAC の担当者に問い合わせてください。

Cisco Live!

安全で暗号化された Java アプレットである Cisco Live! を利用すると、コラボレーティブ Web ブラウジング、URL 共有、ホワイトボード、Telnet、クリップボードツールを使用することによって、Cisco TAC のエンジニアとより効率的に協同して作業できます。

Cisco Live! には次の URL からアクセスできます。

`http://c3.cisco.com/`

Remote Access

リモート アクセスを使用すると、必要なすべての装置に対して Terminal Services セッション（リモート ポート 3389）、HTTP セッション（リモート ポート 80）、および Telnet セッション（リモート ポート 23）を確立できます。

注意 ダイヤルインを設定する場合は、システムに対する脆弱性となるため、**login:cisco** または **password:cisco** は使用しないでください。

TAC エンジニアが次のいずれかの方法を使用してデバイスにリモート アクセスすることを許可すると、多くの問題を非常に迅速に解決できます。

- パブリック IP アドレスが設定された装置
- ダイヤルイン アクセス：（プリファレンスの高い順に）アナログ モデム、統合デジタル通信網（ISDN）モデム、バーチャル プライベート ネットワーク（VPN）
- ネットワーク アドレス変換（NAT）：プライベート IP アドレスが設定された装置へのアクセスを可能にする IOS およびプライベート インターネット エクスチェンジ（PIX）。

エンジニアの介入時にファイアウォールによってIOS トラフィックと PIX トラフィックが遮断されないこと、およびサーバ上で Terminal Services などの必要なすべてのサービスが開始されていることを確認してください。

（注） TAC では、すべてのアクセス情報は厳重に管理されます。また、お客様の同意なしにシステムを変更することはありません。

Cisco Secure Telnet

シスコ サービス エンジニア（CSE）は、Cisco Secure Telnet を使用して、サイト上のUnified Communications Managerサーバに対して透過的にファイアウォール アクセスを実行できます。

Cisco Secure Telnet は、シスコのファイアウォール内部で Telnet クライアントをイネーブル化することによって、ファイアウォールで稼働する Telnet デーモンに接続します。 このセキュアな接続により、ファイアウォールを変更せずに、Unified Communications Managerサーバの監視およびメンテナンスをリモートで行うことができます。

（注） シスコは、許可があった場合にだけお客様のネットワークにアクセスします。 サイトに、このプロセスの開始を支援するネットワーク管理者を配置する必要があります。

ファイアウォールによる保護

ほとんどすべての内部ネットワークでは、外部から内部のホストシステムへのアクセスを制限するためにファイアウォールアプリケーションが使用されています。これらのアプリケーションでは、ネットワークとパブリックインターネットとの間のIP接続を制限することによって、ネットワークが保護されます。

ファイアウォールでは、許可するように明示的に再設定しないかぎり、外部から開始されるTCP/IP 接続が自動的にブロックされます。

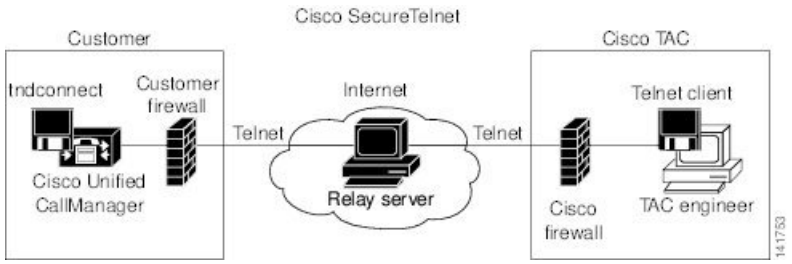
通常、企業ネットワークではパブリックインターネットとの通信が許可されますが、ファイアウォール内部から外部ホストに向けて開始される接続だけが許可されます。

Cisco Secure Telnet の設計

Cisco Secure Telnet では、ファイアウォールの内側から簡単に Telnet 接続を開始できるという技術を活用しています。外部のプロキシ マシンを使用して、ファイアウォールの内側からのTCP/IP 通信が *Cisco Technical Assistance Center* (TAC) にある別のファイアウォールの内側のホストへとリレーされます。

このリレーサーバを使用することによって、両方のファイアウォールの完全性が維持され、また保護されたリモート システム間の安全な通信がサポートされます。

図 *26 : Cisco Secure Telnet* システム



Cisco Secure Telnet の構造

外部のリレー サーバによって、お客様のネットワークとシスコとの間に Telnet トンネルが構築され、接続が確立されます。これにより、Unified Communications Managerサーバの IP アドレスおよびパスワード識別子を CSE に送信できます。

（注） パスワードは、管理者と CSE が相互に同意した文字列です。

管理者は、Telnet トンネルを開始することによって、プロセスを開始します。これにより、ファイアウォールの内部からパブリック インターネット上のリレー サーバへの TCP 接続が確立されます。次に、Telnet トンネルによって、ローカルの Telnet サーバへの別の接続が確立され、エンティティ間の双方向のリンクが作成されます。

（注） Cisco TAC の Telnet クライアントは、Windows NT および Windows 2000 上で動作するシステム、または UNIX オペレーティング システムに準拠して動作します。

ローカル サイトの Cisco Communications Manager がパスワードを受け入れると、Cisco TAC で実行されている Telnet クライアントは、ローカル ファイアウォールの内側で動作する Telnet デーモンに接続します。この結果確立される透過的接続によって、マシンがローカルで使用されている場合と同様にアクセスできるようになります。

安定的な Telnet 接続が確立されると、CSE は、Unified Communications Managerサーバに対してメンテナンス タスク、診断タスク、およびトラブルシューティング タスクを実行するためのあらゆるリモート有用性機能を導入できます。

CSE が送信するコマンドおよびUnified Communications Managerサーバから発行される応答を確認することはできますが、コマンドや応答が常に完全な形式で表示されるとは限りません。

リモート アカウントの設定

シスコ サポートがトラブルシューティングのためにご使用のシステムに一時的にアクセスできるよう、Unified Communications Manager でリモート アカウントを設定します。

手順

ステップ 1 [Cisco Unified オペレーティング システムの管理（Cisco Unified Operating System Administration）]で、**[サービス（Services）]** > **[リモート サポート（Remote Support）]** を選択します。

ステップ 2 [アカウント名（Account Name）]フィールドに、リモート アカウントの名前を入力します。

ステップ 3 [アカウントの有効期限（Account Duration）]フィールドに、アカウントの有効期限を日数で入力します。

ステップ 4 **[保存]** をクリックします。
システムは、暗号化パス フレーズを生成します。

ステップ 5 シスコのサポート担当者に連絡して、リモート サポート アカウント名とパス フレーズを提供します。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。