Cisco Unified Serviceability リリース 11.5(1) アドミニストレーション ガイド

初版：2016 年 04 月 21 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

はじめに

目的

『*Cisco Unified Serviceability Administration Guide*』では、次の Cisco Unified Serviceability を通じてアラーム、トレース、SNMP を設定するための説明と手順を示します。

- Cisco Unified Communications Manager
- Cisco Unified Communications Manager IM and Presence Service
- Cisco Unity Connection

ヒント

Cisco Unity Connection の場合、Cisco Unified Serviceability と Cisco Unity Connection Serviceability の両方でサービスアビリティ関連タスクを実行する必要があります。たとえば、問題を解決するために、両方のアプリケーションでサービスの起動や停止、アラームの表示、トレースの設定が必要な場合があります。

Cisco Unified Serviceability は、『*Cisco Unified Serviceability Administration Guide*』に記載されている機能をサポートしています。Cisco Unity Connection Serviceability 固有のタスクについては、『*Cisco Unity Connection Serviceability Administration Guide*』を参照してください。

対象読者

『*Cisco Unified Serviceability Administration Guide*』は、Cisco Unified Communications Manager、Cisco Unified Communications Manager IM and Presence Service、または Cisco Unity Connection の設定、トラブルシューティング、およびサポートを行う管理者を支援することを目的としています。このマニュアルを使用するには、テレフォニーおよびIPネットワーキングテクノロジーに関する知識が必要です。

関連資料

このガイドは、設定に関するマニュアルと併せて使用してください。

製品	資料
Cisco Unified Communications Manager	『*Cisco Unified Real-Time Monitoring Tool Administration Guide*』、『*Cisco Unified Communications ManagerCDR Analysis and Reporting Administration Guide*』、および『*Cisco Unified Communications Manager Call Detail Records Administration Guide*』
Cisco Unified Communications Manager IM and Presence Service	『*Cisco Unified Real-Time Monitoring Tool Administration Guide*』
Cisco Unity Connection	『*Cisco Unity Connection Serviceability Administration Guide*』および『*Cisco Unified Real-Time Monitoring Tool Administration Guide*』

これらのマニュアルは、次の情報が含まれます。

- 『*Cisco Unified Communications Manager CDR Analysis and Reporting Administration Guide*』：このマニュアルでは、ユーザ、システム、デバイス、および課金レポートの作成に使用するツールである Cisco Unified Communications Manager CDR Analysis and Reporting を設定および使用する方法について説明します。
- 『*Cisco Unified Communications Manager Call Detail Records Administration Guide*』：このマニュアルには呼詳細レコード（CDR）定義が含まれます。
- 『*Cisco Unified Real-Time Monitoring Tool Administration Guide*』：このマニュアルでは、システムのさまざまな面（重要なサービス、アラート、パフォーマンスカウンタなど）をモニタするためのツールである Unified RTMT の使用方法について説明します。
- 『*Cisco Unity Connection Serviceability Administration Guide*』：このマニュアルでは、Cisco Unity Connection Serviceability でアラーム、トレース、クラスタ、レポートを使用する方法と、その手順について説明します。

表記法

このマニュアルでは、次の表記法を使用しています。

表記法	説明
太字 フォント	コマンドおよびキーワードは**太字**で示しています。
イタリック体フォント	ユーザが値を指定する引数は、イタリック体で示しています。
[ ]	角カッコの中の要素は、省略可能です。
{ x | y | z }	必ずどれか1つを選択しなければならない必須キーワードは、波カッコで囲み、縦棒で区切って示しています。
[x | y | z]	どれか1つを選択できる省略可能なキーワードは、角カッコで囲み、縦棒で区切って示しています。
string	引用符を付けない一組の文字。string の前後には引用符を使用しません。引用符を使用すると、その引用符も含めて string とみなされます。
screen フォント	システムが表示する端末セッションおよび情報は、screen フォントで示しています。
太字の screen フォント	ユーザが入力しなければならない情報は、**太字の screen** フォントで示しています。
イタリック体の screen フォント	ユーザが値を指定する引数は、イタリック体の screen フォントで示しています。
^	^ 記号は、Ctrl キーを表します。たとえば、画面に表示される ^D というキーの組み合わせは、Ctrl キーを押しながら D キーを押すことを意味します。
< >	パスワードのように出力されない文字は、山カッコ（< >）で囲んで示しています。

（注）は、次のように表しています。

（注） 「注釈」です。役立つ情報や、このマニュアル以外の参照資料などを紹介しています。

ワンポイント アドバイスは、次のように表しています。

ワンポイント アドバイス 「時間の節約に役立つ操作」です。記述されている操作を実行すると時間を節約できます。

ヒントは、次のように表しています。

ヒント 役立つ「ヒント」の意味です。

注意は、次のように表しています。

注意 「要注意」の意味です。機器の損傷またはデータ損失を予防するための注意事項が記述されています。

警告は、次のように表しています。

警告 「危険」の意味です。人身事故を予防するための注意事項が記述されています。機器の取り扱い作業を行うときは、電気回路の危険性に注意し、一般的な事故防止対策に留意してください。

マニュアルの入手、サポート、およびセキュリティのガイドライン

マニュアルの入手方法、テクニカル サポート、マニュアルに関するフィードバックの提供、セキュリティ ガイドライン、および推奨エイリアスや一般的なシスコのマニュアルについては、次の URL で、毎月更新される『What's New in Cisco Product Documentation』を参照してください。シスコの新規および改訂版の技術マニュアルの一覧も示されています。
`http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html`

シスコ製品のセキュリティの概要

本製品には暗号化機能が備わっており、輸入、輸出、配布および使用に適用される米国および他の国での法律を順守するものとします。シスコの暗号化製品を譲渡された第三者は、その暗号化技術の輸入、輸出、配布、および使用を許可されたわけではありません。輸入業者、輸出業者、販売業者、およびユーザは、米国および他の国での法律を順守する責任があります。本製品を使用するにあたっては、関係法令の順守に同意する必要があります。米国および他の国の法律を順守できない場合は、本製品を至急送り返してください。

米国の輸出規制の詳細については、`http://www.access.gpo.gov/bis/ear/ear_data.html` で参照できます。

マニュアルの構成

Unified Communications Manager の Cisco Unified Serviceability および IM and Presence Serviceability の設定手順についての情報を提供します。

- Cisco Unified Serviceability：ブラウザのサポートを含む Serviceability の概要です。
- はじめに：Serviceability GUI のアクセス方法と使用方法について説明します。
- アラーム：Serviceability GUI アラームとアラーム定義、アラームの設定の手順、アラーム定義の検索と編集の手順の概要です。
- トレース：トレース パラメータ設定の概要、および Cisco Unified Real-Time Monitoring Tool のトレース収集の概要です。ネットワーク サービスおよび機能サービスのトレース パラメータを設定する手順およびサービスのトラブルシューティング トレース設定を行う手順について説明します。
- ツールおよびレポート：表示される各ネットワーク サービスおよび機能サービスの説明です。機能サービスおよびネットワーク サービスのアクティブ化、非アクティブ化、起動、および停止の手順と推奨事項について説明します。Cisco Serviceability Reporter サービスによって生成されるレポートの概要です。Cisco Serviceability Reporter サービスによって生成されるレポートを表示する手順を示します。
  - Unified Communications Manager のみ：[CDRの管理設定（CDR Management Configuration）] ウィンドウを使用して呼詳細レコード（CDR）ファイルと呼管理レコード（CMR）ファイルに割り当てるディスク スペースの容量の設定、ファイルを削除するまでの保存日数の設定、および CDR の送信先となる課金アプリケーション サーバの設定を行う際の情報について説明します。
- シンプル ネットワーク管理プロトコル：シンプル ネットワーク管理プロトコル（SNMP）バージョン 1、2c、3 のサポートと設定手順の概要です。
- Call Home：Call Home サービスの概要です。Call Home 機能の設定方法について説明します。

第 1 章

Serviceability の管理の概要

概要

Web ベースのトラブルシューティング ツールである Cisco Unified Serviceability は次の機能を提供します。

- トラブルシューティング用に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する。
- トレース情報を、トラブルシューティング用にログ ファイル保存します。
- Cisco Unified Real-Time Monitoring Tool（Unified RTMT）を使用して、コンポーネントの動作をリアルタイムで監視します。
- ユーザによる、またはユーザ処理の結果としてのシステムの設定変更を記録することによって、監査機能を提供します。この機能は、Cisco Unified Communications Manager および Cisco Unity Connection の情報保証機能をサポートします。
- [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。
- 日次レポート（警告サマリーやサーバ統計レポートなど）の生成とアーカイブ。
- Cisco Unified Communications Manager、IM and Presence Service、Cisco Unity Connection が、シンプル ネットワーク管理プロトコル（SNMP）の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機能できるようにします。
- 1 つのノード（またはクラスタ内のすべてのノード）のログ パーティションのディスク使用をモニタします。

- システム内のスレッドとプロセスの数をモニタする。キャッシュを使用してパフォーマンスを向上させる。
- Cisco Unified Communications Manager のみ：Cisco Unified Communications Manager CDR Analysis and Reporting を使用して、サービス品質、トラフィック、請求情報の Cisco Unified Communications Manager レポートを生成します。

（注） IM and Presence Service は他とは異なる Serviceability インターフェイスを使用するため、必要なときに個別に言及されます。

ヒント Cisco RIS Data Collector は、Cisco Unified Real-Time Monitoring Tool におけるプロセスとスレッドの統計カウンタを提供します。許可されるプロセスとスレッドの最大数を設定し、Cisco RIS Data Collector がこれらの関連カウンタを提供できるようにするには、設定の管理インターフェイスで Cisco RIS Data Collector サービスの Maximum Number of Threads and Process サービス パラメータにアクセスします。

Cisco Unified Communications Manager：サービス パラメータの設定については、『*System Configuration Guide for Cisco Unified Communications Manager*』を参照してください。

Cisco Unity Connection：サービス パラメータの設定については、『*System Administration Guide for Cisco Unity Connection*』を参照してください。

ヒント Cisco Unity Connection のみ：Cisco Unity Connection の場合、Cisco Unified Serviceability と Cisco Unity Connection Serviceability の両方でサービスアビリティ関連タスクを実行する必要があります。たとえば、問題を解決するために、両方のアプリケーションでサービスの起動や停止、アラームの表示、トレースの設定が必要な場合があります。

Cisco Unified Serviceability は、『Cisco Unified Serviceability Administration Guide』に記載されている機能をサポートしています。Cisco Unity Connection Serviceability 固有のタスクについては、『*Cisco Unity Connection Serviceability Administration Guide*』を参照してください。

レポート ツール

Cisco Unified Serviceability は、次のレポート ツールを提供します。

- Cisco Unified Communications Manager のみ：
  - Cisco Unified Communications Manager のみ：Cisco Unified Communications Manager CDR Analysis and Reporting：Cisco Unified Communications Manager CDR Analysis and Reporting を使用して、サービス品質、トラフィック、請求情報の Cisco Unified Communications Manager レポートを生成します。詳細については、『*CDR Analysis and Reporting Administration Guide*』を参照してください。

- Cisco Unified Communications Manager のみ：Cisco Unified Communications Manager Dialed Number Analyzer：展開された Cisco Unified Communications Manager ダイヤル プランの設定をテストおよび診断し、テスト結果を分析し、その結果を使用してダイヤルプランを改善できます。Dialed Number Analyzer のアクセス方法と使用方法の詳細については、『*Cisco Unified Communications Manager Dialed Number Analyzer Guide*』を参照してください。
- Cisco Unified Communications Manager のみ：Cisco Unified Reporting Web Application：スタンドアロンサーバまたはクラスタのデータの検査やトラブルシューティングを行えるようにします。このアプリケーションは、Cisco Unified Serviceability とは別になっており、クラスタ内のアクセス可能なすべての Cisco Unified Communications Manager サーバからカテゴリ別のデータを 1 つの出力ビューに統合します。一部のレポートは、ヘルスチェックを実行して、サーバまたはクラスタの動作に影響を与える可能性がある状態を特定します。許可されたユーザは、Cisco Unified Communications Manager Administration のメインナビゲーションメニュー、または Unified RTMT メニューの [ファイル（File）] > [Cisco Unified Reporting] リンクを使用して Cisco Unified Reporting にアクセスします。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：Cisco Serviceability Reporter サービスが生成するレポートをアーカイブします。

- Cisco Unified Real-Time Monitoring Tool（Unified RTMT）：Unified RTMTを使用してコンポーネントのリアルタイムな動作をモニタします。サービスアビリティ レポートのアーカイブからアクセスできる日次レポートを作成します。詳細については、『*Cisco Unified Real-Time Monitoring Tool Administration Guide*』を参照してください。
- Cisco Unified Communications IM and Presence Service のメイン ナビゲーション メニューで Cisco Unified IM and Presence Reporting にアクセスできます。

遠隔サービスアビリティ ツール

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

Cisco Unified Communications Manager システムの管理を補うために、遠隔サービスアビリティ ツールを使用できます。これらのツールを使用して、診断の支援またはリモート トラブルシューティング用にシステムおよびデバッグ情報を収集できます。これらのツールでは、ローカルまたはリモートの Unified Communications Manager の設定情報の収集を処理し、レポートを生成できます。テクニカル サポート エンジニアは、お客様の許可を得たうえで、Unified Communications Manager サーバにログインし、ローカルログインセッションから実行可能な機能をすべて実行できるデスクトップまたはシェルを取得します。

Unified Communications Manager は次の遠隔サービスアビリティの機能をサポートします。

- シンプル ネットワーク管理プロトコル（SNMP）：Unified Communications Manager などの管理対象デバイスのリモート管理機能を提供します。

- コマンドライン インターフェイスの表示：Unified Communications Manager システムのデータを表示します。

カスタマイズされたログイン メッセージ

最初の Serviceability ウィンドウに表示されるカスタマイズされたログイン メッセージを含むテキスト ファイルをアップロードできます。

カスタマイズされたログイン メッセージのアップロードの詳細および手順については、『*Administration Guide for Cisco Unified Communications Manager*』を参照してください。

第 2 章

使用する前に

アクセス

複数の方法で Serviceability アプリケーションにアクセスできます。

- ブラウザのウィンドウに `https://<サーバ名または IP アドレス>:8443/ccmservice/` と入力し、続いて有効なユーザ名とパスワードを入力します。
- Cisco Unified Communications Manager Administration のコンソールの [ナビゲーション（Navigation）] メニューで、[Cisco Unified Serviceability] を選択します。
- Cisco Unified Real-Time Monitoring Tool（Unified RTMT）メニューで [アプリケーション（Application）] > [Serviceability Web ページ（Serviceability Webpage）] を選択し、続いて有効なユーザ名とパスワードを入力します。
- Cisco Unity Connection の [ナビゲーション（Navigation）] メニューで [Cisco Unified Serviceability] を選択します。
- Cisco IM and Presence Administration の [ナビゲーション（Navigation）] メニューで [Cisco Unified Serviceability] を選択します。

ヒント Cisco Unified Serviceability にログインした後は、[ナビゲーション（Navigation）] メニューに表示されるすべての管理アプリケーションに再度ログインせずにアクセスできます。ただし Cisco Unified OS Administration と Disaster Recovery System は除きます。Cisco Unified Serviceability からアクセスできる Web ページは、割り当てられているロールと権限によって異なります。Cisco Unified OS Administration と Disaster Recovery System には、別の認証手順が必要になります。

このシステムは、Web アプリケーションへのアクセスをユーザに許可する前に、Cisco Tomcat サービスを使用してユーザを認証します。

ヒント　Cisco Unified Communications Manager のみ：“Standard CCM Admin Users” ロールが割り当てられているユーザは、Cisco Unified Serviceability にアクセスできます。このロールをユーザに割り当てる方法については、『*Administration Guide for Cisco Unified Communications Manager*』を参照してください。

ヒント　Cisco Unity Connection のみ：System Administrator のロールまたは Technician のロールが割り当てられているユーザが、Cisco Unified Serviceability にアクセスできます。このロールをユーザに割り当てる方法については、『*User Moves, Adds, and Changes Guide for Cisco Unity Connection*』を参照してください。

サイトが信頼されていないというセキュリティの警告が表示された場合、これはサーバ証明書がまだダウンロードされていないことを示しています。

Cisco Unified Serviceability にアクセスするには、次の手順を実行します。

手順

ステップ 1　サポートされているブラウザで、Cisco Unified Serviceability サービスが実行されているサーバを参照します。

ヒント　サポートされているブラウザで、`https://<サーバ名または IP アドレス>:8443/ccmservice/` と入力します。ここでサーバ名または IP アドレスは、Cisco Unified Serviceability サービスが実行されているサーバのもので、8443 は HTTPS のポート番号です。

ヒント　ブラウザに `http://<サーバ名または IP アドレス>:8080` と入力すると、HTTP が使用されます。HTTP ではポート番号 8080 を使用します。

（注）　システムから証明書についてのプロンプトが表示された場合は、サーバ証明書のインストールに関するトピックを参照してください。

ステップ 2　有効なユーザ名とパスワードを入力し、[ログイン（Login）] をクリックします。
ユーザ名とパスワードをクリアするには、[リセット（Reset）] をクリックします。

Cisco Unified Serviceability にログインすると、各ユーザ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 ID、日時、IP アドレスとともに、メイン [Cisco Unified Serviceability] ウィンドウに表示されます。

関連トピック

サーバ証明書のインストール，（7 ページ）

Cisco Unified IM and Presence Serviceability へのアクセス

Cisco Unified IM and Presence Serviceability にサインインすると、[Navigation（ナビゲーション）] リスト ボックスに表示される各アプリケーションにサインインしなくても、すべてのアプリケーションにアクセスできるようになります。リスト ボックスから必要なアプリケーションを選択し、[移動（Go）]を選択します。

はじめる前に

[ナビゲーション（Navigation）] リスト ボックスに表示されるいずれかのアプリケーション（Cisco Unified IM and Presence OS Administration または IM and Presence Disaster Recovery System 以外）にサインイン済みである場合は、サインインしなくても Cisco Unified IM and Presence Serviceability にアクセスできます。[ナビゲーション（Navigation）] リスト ボックスから Cisco Unified IM and Presence Serviceability を選択し、[移動（Go）]を選択します。

手順

ステップ 1 `https://`<サーバ名または `IP` アドレス> と入力します。<サーバ名または IP アドレス> は、Cisco Unified IM and Presence Serviceability サービスが動作しているサーバです。

ステップ 2 Unified Communications Manager IM and Presence Administration にサインインします。

ステップ 3 証明書の入力を求められたら、HTTPS を有効にして、ブラウザ クライアントと Web サーバ間の通信を保護する必要があります。

ステップ 4 ユーザとパスワードの入力を求められる場合は、インストール時に指定したアプリケーション ユーザ名とアプリケーション ユーザ パスワードを入力します。

ステップ 5 Unified Communications Manager IM and Presence Administration が表示されたら、メイン ウィンドウの右上隅にあるメニューから [ナビゲーション（Navigation）] > [Cisco Unified IM and Presence Serviceability] を選択します。

Cisco Unified IM and Presence Serviceability にログインすると、各ユーザ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 ID、日時、IP アドレスとともに、[Cisco Unified IM and Presence Serviceability]ウィンドウに表示されます。

サーバ証明書のインストール

（注） Cisco Unified Communications Manager での HTTPS の使用に関する詳細については、『Cisco Unified Communications Manager Security Guide』を参照してください。

Hypertext Transfer Protocol over Secure Sockets Layer（SSL）は、ブラウザ クライアントと Tomcat Web サーバとの間の通信を安全に保護し、証明書および公開キーを使用してインターネット経由で転送されるデータを暗号化します。HTTPS は、サーバが正しいものであることを保障し、Cisco

Unified Serviceability などのアプリケーションをサポートします。また、ユーザのログイン パスワードも HTTPS によって Web 経由で安全に転送されるようになります。

（注） ブラウザの証明書とサーバ証明書は完全に一致する必要があります。

（注） Internet Explorer 7 では、証明書の処理方法が原因で、サーバ証明書をインポートするとブラウザにエラー ステータスが表示されます。このステータスは、URL の再入力、ブラウザの更新または再起動を行った場合にも残りますが、エラーは表示されなくなります。詳細については、Internet Explorer 7 の証明書のインストール，（9 ページ）を参照してください。

HTTPS

Cisco Unified Serviceability に初めてアクセスしようとすると、[セキュリティの警告（Security Alert）] ダイアログボックスが表示されます。これは、サーバ証明書が信頼できるフォルダにないため、サーバが信頼されていないことを示しています。ダイアログボックスが表示されたら、次のいずれかのタスクを実行します。

- [はい（Yes）] をクリックすると、現在の Web セッションの間だけ証明書を信頼することになります。現在のセッションの間だけ証明書を信頼する場合は、アプリケーションにアクセスするごとに [セキュリティの警告（Security Alert）] ダイアログ ボックスが表示されます。つまり、信頼できるフォルダに証明書をインストールするまでこのダイアログボックスが表示されることになります。
- [証明書の表示（View Certificate）] > [証明書のインストール（Install Certificate）] をクリックして、証明書のインストールのタスクを実行し、証明書を常に信頼することを示します。証明書を信頼できるフォルダにインストールすると、Web アプリケーションにアクセスするごとに [セキュリティの警告（Security Alert）] ダイアログボックスが表示されることはなくなります。
- [いいえ（No）] をクリックすると、操作がキャンセルされます。認証が行われないため、Web アプリケーションにアクセスできません。

（注） 証明書はホスト名を使用して発行されます。IP アドレスを使用して Web アプリケーションにアクセスしようとすると、証明書がインストールされていても、[セキュリティの警告（Security Alert）] ダイアログボックスが表示されます。

Internet Explorer 7 の証明書のインストール

Internet Explorer 7 では、Web サイト アクセスのための Cisco 証明書のブラウザによる処理方法を変更するセキュリティ機能が追加されています。シスコは Cisco Unified Communications Manager または Cisco Unity Connection サーバ用の自己署名証明書を提供するため、Internet Explorer 7 では信頼ストアにサーバの証明書が含まれている場合でも Cisco Unified Communications Manager Administration または Cisco Unity Connection Web の Web サイトに信頼できないというフラグを立て、証明書エラーとします。

（注） Internet Explorer 7 は Windows Vista の機能ですが、Windows XP Service Pack 2（SP2）、Windows XP Professional x64 Edition、Windows Server 2003 Service Pack 1（SP1）でも動作します。IE で Java 関連のブラウザをサポートできるよう、Java Runtime Environment（JRE）が必要です。

ブラウザを再起動するたびに証明書をリロードしなくても安全なアクセスが行えるよう、Cisco Unified Communications Manager または Cisco Unity Connection の証明書を Internet Explorer 7 にインポートしてください。Web サイトで証明書に対する警告が表示され、証明書が信頼ストアにない場合、Internet Explorer 7 は現在のセッションの間だけ証明書を記憶します。

サーバ証明書をダウンロードした後も、Internet Explorer 7 ではその Web サイトに対する証明書エラーが引き続き表示されます。このセキュリティの警告は、ブラウザの信頼ルート認証局の信頼できるストアにインポートされた証明書が含まれている場合には無視できます。

次の手順では、Internet Explorer 7 のルート証明書の信頼ストアに Cisco Unified Communications Manager または Cisco Unity Connection の証明書をインポートする方法について説明します。

手順

ステップ 1 ブラウザにホスト名（サーバ名）またはIPアドレスを入力して、Tomcatサーバのアプリケーションにアクセスします。
ブラウザに「証明書エラー: ナビゲーションはブロックされました（Certificate Error: Navigation Blocked）」というメッセージが表示されます。これはこの Web サイトは信頼できないことを示しています。

ステップ 2 サーバにアクセスするには、[このサイトの閲覧を続行する（推奨されません）（Continue to this website (not recommended)）] をクリックします。
管理ウィンドウが表示され、ブラウザにアドレス バーと証明書のエラーのステータスが赤色で表示されます。

ステップ 3 サーバ証明書をインポートするには、[証明書のエラー（Certificate Error）] ステータス ボックスをクリックして、ステータス レポートを表示します。レポートの [証明書の表示（View Certificates）] リンクをクリックします。

ステップ 4 証明書の詳細を確認します。

[証明のパス（Certification Path）] タブに、「信頼されたルート証明機関のストアに存在しないためこの CA ルート証明書は信頼されていません。（This CA Root certificate is not trusted because it is not in the Trusted Root Certification Authorities store.）」と表示されます。

ステップ 5 [証明書（Certificate）] ウィンドウで [全般（General）] タブを選択し、[証明書のインストール（Install Certificate）] をクリックします。
証明書のインポート ウィザードが起動します。

ステップ 6 ウィザードを起動するには、[次へ（Next）] をクリックします。
[証明書ストア（Certificate Store）] ウィンドウが表示されます。

ステップ 7 [自動（Automatic）]オプションが選択されていることを確認します。これを選択すると、ウィザードでこの証明書タイプの証明書ストアを選択できるようになります。[次へ（Next）] をクリックしてください。

ステップ 8 設定を確認し、[完了（Finish）] をクリックします。
インポート操作に対してセキュリティ警告が表示されます。

ステップ 9 証明書をインストールするには、[はい（Yes）] をクリックします。
インポート ウィザードに「正しくインポートされました。（The import was successful.）」と表示されます。

ステップ 10 [OK] をクリックします。[証明書の表示（View certificates）] リンクを次にクリックしたときには、[証明書（Certificate）] ウィンドウの [証明のパス（Certification Path）] タブに「この証明書は問題ありません。（This certificate is OK.）」と表示されます。

ステップ 11 信頼ストアにインポートした証明書が含まれていることを確認するには、Internet Explorer のツールバーの [ツール（Tools）] > [インターネット オプション（Internet Options）] をクリックして、[コンテンツ（Content）] タブを選択します。[証明書（Certificates）] をクリックして、[信頼されたルート証明機関（Trusted Root Certifications Authorities）] タブを選択します。インポートした証明書が見つかるまでリストをスクロールします。
証明書のインポート後、ブラウザには引き続きアドレス バーと証明書エラーのステータスが赤色で表示されます。このステータスは、ホスト名または IP アドレスを入力したり、ブラウザを更新または再起動した場合でも表示されます。

Serviceability のインターフェイス

Cisco Unified Serviceability でトラブルシューティングとサービス関連のタスクを実行するのに加えて、次のタスクを実行できます。

- Cisco Unified Communications Manager のみ：展開した Unified Communications Manager ダイヤル プラン設定のテストと診断を行い、テスト結果を分析し、ダイヤル プランの調整のために結果を使用するために Dialed Number Analyzer にアクセスするには、[ツール（Tools）] > [サービスの開始（Service Activation）] を選択し、[ツール（Tools）] > [Dialed Number Analyzer] を選択して Cisco Dialed Number Analyzer サービスをアクティブ化します。

- [ツール（Tools）] > [サービスの開始（Service Activation）] を選択し、[ツール（Tools）] > [Dialed Number Analyzerサーバ（Dialed Number Analyzer server）] を選択して Cisco Dialed Number Analyzer サービスとともに Cisco Dialed Number Analyzer Server サービスをアクティブ化する必要があります。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にする必要があります。

  Dialed Number Analyzer の使用方法の詳細については、『*Cisco Unified Communications Manager Dialed Number Analyzer Guide*』を参照してください。

- Unified Communications Manager のみ：[ツール（Tools）] > [CDR Analysis and Reporting] から Cisco Unified Communications Manager CDR Analysis and Reporting にアクセスするには、『*CDR Analysis and Reporting Administration Guide*』に説明されている必要な手順を実行する必要があります。

（注） Cisco CAR 管理者ユーザ グループのメンバーでなければ、Cisco Unified Communications Manager CDR Analysis and Reporting ツールにアクセスできません。Cisco CAR 管理者ユーザ グループのメンバーになる方法については、『*CDR Analysis and Reporting Administration Guide*』の「Configuring the CDR Analysis and Reporting Tool」の章を参照してください。

- 単一のウィンドウでドキュメントを表示するには、Cisco Unified Serviceability の [ヘルプ（Help）] > [このページ（This Page）] を選択します。
- このリリースで利用可能なドキュメントのリストを表示するには（またはオンライン ヘルプのインデックスにアクセスするには）、Cisco Unified Serviceability の [ヘルプ（Help）] > [目次（Contents）] を選択します。
- サーバ上で実行されている Cisco Unified Serviceability のバージョンを確認するには、[ヘルプ（Help）] > [概要（About）] を選択するか、ウィンドウの右上隅にある [概要（About）] リンクをクリックします。
- 設定ウィンドウから Cisco Unified Serviceability のホームページに直接移動するには、ウィンドウの右上隅にある [ナビゲーション（Navigation）] ドロップダウン リスト ボックスから [Cisco Unified Serviceability] を選択します。

（注） 状況によっては、Cisco Unified OS Administration から Cisco Unified Serviceability にアクセスできない場合があります。「ロード中です、お待ちください（Loading, please wait）」というメッセージがいつまでも表示されます。リダイレクトが失敗した場合は、Cisco Unified OS Administration からログアウトして、[ナビゲーション（Navigation）] ドロップダウン リスト ボックスから [Cisco Unified Serviceability] を選択し、Cisco Unified Serviceability にログインします。

- 設定ウィンドウから Cisco Unified IM and Presence Serviceability のホームページに直接移動するには、ウィンドウの右上にある [ナビゲーション（Navigation）] ドロップダウン リスト ボックスから [Cisco Unified IM and Presence Serviceability] を選択します。

- 他のアプリケーションの GUI にアクセスするには、ウィンドウの右上にある [ナビゲーション（Navigation）] ドロップダウン リスト ボックスからアプリケーションを選択し、[移動（Go）] をクリックします。
- Cisco Unified Serviceability からログアウトするには、[Cisco Unified Serviceability] ウィンドウの右上の [ログアウト（Logout）] リンクをクリックします。
- 各 Cisco Unified Serviceability 設定ウィンドウには、ウィンドウの下部にある設定ボタンに対応する設定アイコンが表示されます。たとえば、[保存（Save）]アイコンまたは[保存（Save）] ボタンをクリックして作業を完了することができます。

ヒント　Cisco Unified Serviceability はブラウザのボタンをサポートしていません。設定作業を行うときは、[戻る（Back）] ボタンなどのブラウザ ボタンを使用しないでください。

ヒント　Cisco Unified Serviceability のユーザ インターフェイスでは、セッションのアイドル状態が 30 分を超えた場合、セッションがタイム アウトしたことを示すメッセージが表示されてログイン ウィンドウにリダイレクトされる前に、変更を行うことができます。ここで行った変更は、場合によっては、再度ログインした後で再び実行する必要があります。この現象は、アラーム、トレース、サービスの開始、コントロール センター、および SNMP の各ウィンドウで発生します。セッションのアイドル状態が 30 分を超えたことがわかっている場合は、ユーザ インターフェイス内で変更を行う前に、[ログアウト（Logout）]ボタンを使用してログアウトしてください。

Cisco Unified Serviceability のアイコン

表 *1*：*Cisco Unified Serviceability* のアイコン

アイコン	目的
	新しい設定を追加します
	操作をキャンセルします
	指定した設定をクリアします
	選択した設定を削除します
	設定のオンライン ヘルプを表示します
	ウィンドウを更新して最新の設定を表示します

アイコン	目的
	選択したサービスをリスタートします
	入力した情報を保存します
	デフォルト設定に設定します
	選択したサービスを開始します
	選択したサービスを停止します

第 3 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 サーバの場合は、Cisco Unified Communications Manager サーバを指定しないでください。このサーバは他のサーバからの Syslog メッセージを受け入れることができません。

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に異なるリモート syslog サーバを設定する
- 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 Administration 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。

Cisco Unified Communications Manager	Cisco Unified Communications Manager 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。
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る。

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 サーバにアラームが送信される。

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 サーバにアラームを転送します。このため、リモート syslog サーバにアラームが 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, （17 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）] ウィンドウで参照します。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 サーバのサーバ名または 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、システムはアラームを送信します。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（Cisco 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 Administration、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。
- Cisco 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 サーバ名を設定していない場合、Cisco Unified Serviceability はリモート Syslog サーバに Syslog メッセージを送信しません。

  ヒント Cisco Unified Communications Manager サーバをリモート Syslog サーバ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。

Cisco Unified Communications Manager	Cisco Unified Communications Manager 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。
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 Cisco Unified Communications Manager でリモート syslog サーバを設定するときには、リモート syslog サーバ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 サーバに送信するときに重複したエントリを無視します。

（注） Cisco Unified Communications Manager をリモート syslog サーバとして設定しないでください。Cisco 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（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 Cisco 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（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。

（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。

次の作業

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 エクステンション モビリティ
- 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、[Cisco Tomcat] 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 *2*：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、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、Cisco Database Layer Monitor、および Cisco License Manager

サービス グループ	サービス
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
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

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 *3*：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（Service Group）	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（Service）	[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。
Cisco Unified Communications Manager と Cisco 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 サーバに保存して、その Syslog サーバの名前を指定することができます。この宛先が有効になっているときに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。 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** ノードが他のノードからの syslog メッセージを受け入れないため、Cisco Cisco Unified Communications Manager または Cisco Cisco Unified Communications Manager IM and Presence Service ノードを宛先に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）	[サーバ名 1（Server Name 1）]、[サーバ名 2（Server Name 2）]、[サーバ名 3（Server Name 3）]、[サーバ名 4（Server Name 4）]、[サーバ名 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** ノードが他のノードからの syslog メッセージを受け入れないため、Cisco Cisco Unified Communications Manager または Cisco Cisco Unified Communications Manager IM and Presence Service ノードを宛先に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。
Cisco Unified Communications Manager および Cisco 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（Warning）** 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	無効	エラー	エラー

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	なし	あり	なし	なし	なし
オフ	なし	あり	あり	あり	あり

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

Cisco 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。

はじめる前に

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（Save）] 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 と Cisco Unity Connection をサポートしています。

表 *4*：システム カタログ

名前	説明
ClusterManagerAlarmCatalog	クラスタ内のサーバ間のセキュリティ アソシエーションの確立に関連するすべての 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義

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　Cisco Unified Communications Manager をサポートしている Cisco License Manager がこのカタログを使用します。 ヒント　アラーム設定 GUI を使用して JavaApplications アラームを設定することはできません。Cisco Unified Communications Manager および Cisco Unity Connection の場合、通常はこれらのアラームをイベント ログに送るよう設定します。Cisco Unified Communications Manager の場合は、SNMP トラップを生成して CiscoWorks LAN Management Solution と統合するようにこれらのアラームを設定することができます。アラーム定義とパラメータを表示および変更するには、オペレーティング システムに付属しているレジストリ 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集アラーム定義
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スレッド統計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べてのアラーム定義。
ServiceManagerAlarmCatalogs	サービスのアクティブ化、非アクティブ化、開始、リスタート、および停止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 トラップによってテス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義。CLI 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。 ヒント　Cisco Unity Connection SNMP では、Unified Communications Manager および Cisco Unity Connection システムのトラップをサポートしていません。

名前	説明
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。

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 5 : *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）マネージャのアラーム定義
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
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ラーム
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 *6*：*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。
CiscoUPSPresenceEngine	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	Cisco 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。

名前	説明
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。

第 4 章

Trace

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（Cisco 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、[トレース設定（Trace Configuration）] ウィンドウを使用して指定します。

Cisco 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できます。

Cisco Unified Communications Manager のみ：[アラーム設定（Alarm Configuration）] 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（Trace Settings）

[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 台のサーバの特定のアクティブ化されたサービス、サーバ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、トレ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） Cisco 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することができます。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 トレースを要求できます。

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 Administration および Cisco Unified IM and Presence：[システム（System）] > [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。
- 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、またはクラスタ内のすべてのサーバ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（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（Apply to All Nodes）] 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（Trace On）] 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（Cisco Unified Communications Manager のみ）。Cisco Messaging Interface については 3 ～ 5 分で反映されます。

（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 7：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
Cisco Cisco Unified Communications Manager CM サービス	• Cisco CTIManager • Cisco CallManager • Cisco CallManager Cisco IP Phone 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。
Cisco Cisco 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
Cisco Cisco Unified Communications Manager CDR サービス	• Cisco Cisco Unified Communications Manager CDR Analysis and Reporting Scheduler • Cisco Cisco Unified Communications Manager CDR Analysis and Reporting Web サービス • Cisco CDR Agent • Cisco CDR Repository Manager	

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
		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 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（Trace Configuration）] ウィンドウの Cisco Unified Communications Manager CDR Analysis and Reporting Scheduler サービスと 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 レベルをチェックします。事前生成レポートの場合は、Cisco Unified Communications Manager CDR Analysis and Reporting が Cisco Unified Communications Manager CDR Analysis and Reporting 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 サービスのレベルをチェックします。[デバッグ トレース レベル（Debug Trace Level）] ドロップダウン リスト ボックスから [デバッグ（Debug）] を選択した場合、ストアドプロシージャのロギングが有効化され、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。次の 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

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
		検索レポート。
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		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。 Cisco Unified Communications Manager をサポートしている 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アクティブ化されます。 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
	Cisco Cisco Unified Communications Manager と 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 Cisco Cisco 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 サービス： • 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	

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
	• Platform Administrative Web サービス	
パフォーマンスおよびモニタリングサービス	Cisco Cisco Unified Communications Manager と 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 Cisco Cisco Unified Communications Manager： • Cisco CCM PD Web サービス IM and Presence サービス： • 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。

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
Cisco Cisco 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。
Cisco Cisco 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。
バックアップおよび復元サービス	• Cisco DRF Local • Cisco Cisco Unified Communications Manager と 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	Cisco Cisco 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 サービス： • 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。

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
SOAP サービス	• Cisco SOAP Web Service • Cisco SOAPMessage Service	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 *8*：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）	アラーム状態およびイベントをトレースします。異常なパスで生成されたすべてのトレースに使用します。最小の CPU サイクル数を使用します。
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。

レベル	説明
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 *9*：*servlet* のデバッグ トレース レベル

レベル	説明
重大（Fatal）	アプリケーションが中断する可能性がある重大なエラーイベントをトレースします。
エラー（Error）	アラーム状態およびイベントをトレースします。異常なパスで生成されたすべてのトレースに使用します。
警告（Warn）	損害が発生する可能性がある状況をトレースします。
情報（Info）	servlet の問題の多数をトレースし、システム パフォーマンスに最小限の影響を与えます。
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有効にするトレース レベル。

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。

次のサービスは、Cisco Unified Communications Manager および Cisco Unity Connection に適用可能です。

- 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

次のサービスは、Cisco Unified Communications Manager に適用可能です。

- 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。Cisco Database Layer Monitor サービスは、Cisco Unified Communications Manager と Cisco Unity Connection をサポートしています。

表 *10*：*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、Cisco Unified Communications Manager と Cisco Unity Connection をサポートしています。

表 *11*：***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。
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、Cisco Unified Communications Manager をサポートしています。

表 *12*：*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。
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。MOHデバイスのステータス（Cisco Unified Communications Manager に登録済み、Cisco Unified Communications Manager から登録解除済み、正常に処理されたリソース割り当て、処理に失敗したリソース割り当てなど）のトレースに使用します。
Unified CMリアルタイム情報サーバのトレースのイネーブル化（Enable Unified CMReal-Time Information Server Trace）	リアルタイム情報サーバが使用する Cisco Unified Communications Manager のリアルタイム情報トレースをアクティブ化します。
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。

フィールド名	説明
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（Cisco IP Voice Media Streaming Application サービスを使用して Cisco 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に録音済み音声案内（.wav ファイル）およびトーンを再生できるようにする SCCP デバイス）のトレースをアクティブ化します。
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。
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。

フィールド名	説明
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、Cisco Unified Communications Manager をサポートしています。

（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 *13*：***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。
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。

設定名	説明
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。
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 *14*：***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、Cisco Unified Communications Manager をサポートしています。

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 *15*：*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 *16*：*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。
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 サービスでは、Cisco Unified Communications Manager をサポートしています。

表 *17*：*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。

フィールド名	説明
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。
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 エクステンション モビリティ サービスでは、Cisco Unified Communications Manager をサポートしています。

表 *18*：*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 *19*：*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 App サービスでは、Cisco Unified Communications Manager をサポートしています。

表 *20*：*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。
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、Cisco Unified Communications Manager をサポートしています。

表 *21*：*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 サービスでは、Cisco Unified Communications Manager をサポートしています。

表 *22*：*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 *23*：*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。
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）	プライバシー要求に関する 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。

パラメータ	説明
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。
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 *24*：***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 *25*：***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 *26*：***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 *27*：*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 *28*：*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 *29*：*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 *30*：***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 *31*：***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 *32*：***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 *33*：*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 *34*：*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 *35*：*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 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 *36*：***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 *37*：***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 *38*：*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 *39*：*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 *40*：*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 *41*：*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 *42* : ***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 *43* : 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

はじめる前に

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（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) 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すべてのサービスをモニタするには、[すべてのノードですべてのサービスをチェック（Check All Services on All Nodes）] をチェックします。

ステップ 5 [保存（Save）] 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 5 章

サービス

機能サービス

Cisco Unified Communications Manager および IM and Presence サービスのアクティブ化、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 Cisco Unified Communications Manager サーバ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、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） 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。

Cisco Unified Communications Manager および Cisco Unified IM and Presence Service のみ：Cisco 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アクティブ化し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されます。

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 Cisco 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 Phone Address Book Synchronizer の TabSync クライアントは、Cisco 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 Phone Address Book Synchronizer ユーザは自身に関連するエンドユーザ データだけにアクセスするようになります。Cisco UXL Web サービスは、次の機能を実行します。

- エンド ユーザが Cisco IP Phone Address Book Synchronizer にログインするときにエンド ユーザ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 Phone 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（Cisco Unified Communications Manager のみ）、Cisco Bulk Provisioning サービスは最初のサーバでのみアクティブ化できます。Cisco Unified Communications Manager Bulk Administration Tool を使用して電話とユーザを管理している場合は、こ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

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、音声自動応答装置（IVR）プロンプトにユーザが応答した後、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。

設定でクラスタをサポートしている場合（Cisco Unified Communications Manager のみ）、最初のサーバでこのサービスをアクティブ化します。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 サービスは、Cisco Unified Communications Manager、IM and Presence Service、Cisco Unity Connection システムでアクティブ化して PAWS-M サーバがそのシステムをアップグレードできるようにすることができる、Simple Object Access Protocol（SOAP）API です。

重要　PAWS-M サーバで Platform Administrative Web サービスをアクティブ化しないでください。

パフォーマンスおよびモニタリング サービス

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。

設定でクラスタをサポートしている場合（Cisco Unified Communications Manager リリースのみ）、このサービスはクラスタ内のすべての Cisco Unified Communications Manager サーバ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，（117 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 を実装しており、Cisco Unified Communications Manager で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。

設定でクラスタをサポートしている場合（Cisco Unified Communications Manager のみ）、クラスタ内のすべてのサーバでこのサービスをアクティブ化します。

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 サービスは、ソフトウェア限定の呼処理に加えて、Cisco 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

Cisco Unified Communications Manager クラスタのみ：このサービスをアクティブ化する前に、Cisco Unified Communications Manager Administration の [Cisco Unified Communications Managers の検索と一覧表示（Find and List Cisco Unified Communications Managers）] ウィンドウに Cisco Unified Communications Manager サーバが表示されていることを確認します。サーバ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 Cisco Unified Communications Manager サーバを追加します。サーバを検索して追加する方法については、『*Administration Guide for Cisco Unified Communications Manager*』を参照してください。

Cisco Cisco Unified Communications Manager クラスタのみ：[サービスの開始（Service Activation）] で Cisco CallManager または CTIManager サービスを非アクティブ化すると、このサービスを非アクティブ化した Cisco Unified Communications Manager サーバはデータベースに存在しなくなります。したがってグラフィカルユーザインターフェイス（GUI）に表示されなくなるため、Cisco Unified Communications Manager Administration での設定操作で Cisco Unified Communications Manager サーバを選択できなくなります。その後、同じ Cisco Unified Communications Manager サーバのサービスを再度アクティブ化すると、データベースに Cisco Unified Communications Manager のエントリが再作成され、サーバ名または 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 のサーバで Cisco CallManager または CTIManager サービスを再度アクティブ化した場合は、Cisco Unified Communications Manager Administration 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を Cisco Unified Communications Manager Administration 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。

Cisco 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 Cisco 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）サーバにそのネットワーク設定情報を照会します。DHCP サーバはデバイスの 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 アドレスと TFTP サーバ名またはアドレスを返します。デバイスが TFTP サーバに設定ファイルを要求します。設定ファイルには、Cisco Unified Communications Manager およびデバイスがその Cisco Unified Communications Manager に接続するときに使用する TCP ポートのリストが含まれます。設定ファイルには、Cisco Unified Communications Manager およびデバイスがその Cisco Unified Communications Manager に接続するときに使用する 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応答（IVR）システムで、この機能により Cisco Unified Mobility ユーザ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 Cisco Unified Communications Manager に提供します。Cisco IP Voice Media Streaming Application は、Cisco 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。

Cisco 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 Cisco Unified Communications Manager のリソースおよび機能にアクセスでき、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 エクステンション モビリティ

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

Cisco Dialed Number Analyzer サービスは、Cisco 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：クラスタ内のすべてのサーバでサービスをアクティブ化することは推奨しません。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にする必要があります。

Cisco Unified Communications Manager クラスタの場合のみ：クラスタ内のすべてのサーバでサービスをアクティブ化することは推奨しません。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 Phone 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 Cisco 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 は、Cisco Cisco Unified Communications Manager Administration で [高度な機能（Advanced Features）] > [ILS設定（ILS Configuration）] を選択してアクセスできる [ILS設定（ILS Configuration）] ウィンドウからアクティブ化できます。

Cisco UserSync サービス

Cisco UserSync サービスは、Cisco 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。

Cisco 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、Cisco 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。

IM and Presence サービス

IM and Presence サービスは 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、要求のルーティング、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永続的なチャット 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 Meeting 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 ルームと永続的なチャット ルームからのメッセージなど、IM and Presence Service サーバとの間で送受信され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要求を処理します。

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。

Cisco Unified Communications Manager のユーザ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、Cisco Unified Communications Manager のクラスタ内のユーザが、Web ページやデスクトップ アプリケーションを使用して、クラスタの内側または外側の他のユーザに対してコールを開始できるようになります。Cisco Web Dialer には、ユーザ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、Web Dialer 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 ユーザのための適切な Cisco Unified Communications Manager のクラスタを検出し、そのクラスタの Cisco Web Dialer に要求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、Cisco Unified Communications Manager に自動登録された IP フォンを少ない労力ですぐにユーザ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。提供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 サービスは自動登録された IP フォンをユーザに割り当てます。

サービスが非アクティブ化されていて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 フォンをユーザに割り当てることができません。このサービスはデフォルトで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 サーバで実行されます。ユーザが指定した間隔（最大 1 時間）に基づく CDR ファイル名のリストに対する SOAP 要求を受信し、要求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、このサービスは要求で指定されたファイル名と転送方式（SFTP または FTP、サーバ名、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要求も受信します。

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。

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

Cisco 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 Cisco Unified Communications Manager および Cisco TFTP サーバ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 トークンとサーバ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 Phone 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） Cisco 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

Cisco Unified Communications Manager：Cisco DirSync サービスを使用すると、Cisco 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るようになります。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 Cisco 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 Cisco 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 を持つユーザは同期されず、管理者は同期されていないユーザ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 サーバ上の Cisco Unified Communications Manager のデータベース内のユーザ 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）は、Cisco 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、Cisco 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、Cisco 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、Cisco 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 Phone Administration Guide 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 Serviceability 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、ユーザによる、またはユーザ処理の結果による Cisco Unified Communications Manager または IM and Presence システムへのすべての管理設定の変更をモニタし、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 Serviceability

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。サーバでこのサービスを停止すると、そのサーバを参照するときに 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。サーバ上でこのサービスを停止すると、そのサーバ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。サーバ上でこのサービスを停止すると、そのサーバ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

A Cisco DB サービスは Cisco Unified Communications Manager の Progres データベース エンジンをサポートします。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

Cisco Unified Communications Manager および IM and Presence のみ：A 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と以降のサーバの間のデータ同期を確認します。

Cisco Tomcat

Cisco Tomcat サービスは Web サーバをサポートします。

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 要求に関連する認証、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 要求を、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 Cisco Cisco 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ありません。

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

このサービスは、さまざまな Cisco Cisco 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

このサービスは、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るようにします。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します。

Platform Administrative Web サービス

Platform Administrative Web サービスは、Cisco Unified Communications Manager、IM and Presence Service、Cisco Unity Connection システムでアクティブ化して PAWS-M サーバがそのシステムをアップグレードできるようにすることができる、Simple Object Access Protocol（SOAP）API です。

重要 PAWS-M サーバで Platform Administrative Web サービスをアクティブ化しないでください。

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。Cisco Cisco 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 License Manager

このサービスは、IM and Presence Service および Cisco Unity Connection ではサポートされていません。

Cisco License Manager は、お客様が購入し、使用する Cisco Cisco Unified Communications Manager 関連のライセンスを追跡します。ライセンスのチェックインとチェックアウトを制御し、Cisco Cisco Unified Communications Manager 関連のライセンスの発行と回収を管理します。Cisco Cisco Unified Communications Manager では、Cisco License Manager は、Cisco Cisco Unified Communications Manager アプリケーションと、IP フォン ユニットのライセンス数を管理します。電話の数がライセンス数を超えると、アラームが発行されます。

Cisco Cisco Unified Communications Manager クラスタのみ：このサービスは、すべてのサーバ上で実行されますが、最初のサーバ上のサービスがライセンスの発行と回収を担当します。

セキュリティ サービス

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、電話は検証を要求できます。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要求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応答を認証できるようにします。プロトコルは、要求と応答の整合性を保護します。要求と応答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。これらのサーバは、Cisco Unified CallManager をホストするサーバと同じであっても、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） Cisco 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、特に Cisco 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。

Cisco 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 API

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 API

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、Cisco Unified Communications Manager 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 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。

Cisco Unified Communications Manager のみ：Cisco エクステンション モビリティ機能により、Cisco Unified Communications Manager クラスタ内のユーザは、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。ユーザがログインすると、電話機にユーザの個人の電話番号、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 Phone 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。

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 Cisco Unified Communications Manager データの同期を保ちます。IM and Presence に関係するデータについて Cisco Unified Communications Manager に SOAP リクエストを送信し、Cisco 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、Cisco 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 ユーザにルーティングできるようにします。XCP ルータはユーザの 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 サービスは、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。

Cisco IM and Presence Data Monitor は、Cisco Unified Communications Manager から Cisco Sync Agent の同期のステータスをチェックします。依存サービスは、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 Cisco Unified Communications Manager からの同期を完了させた後にのみ、起動できます。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。

シスコ RCC デバイス選択

シスコ RCC デバイス選択サービスはリモート コール制御のための Cisco IM and Presence ユーザのデバイス選択サービスです。

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（Cisco Unified Communications Manager のみ）では、このサービスは 1 番目のサーバにあります。

Cisco CDR Agent

（注） Cisco Unified Communications Manager は、Cisco Unified Communications Manager システムの Cisco CDR Agent をサポートしています。

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、Cisco Unified Communications Manager によって生成された 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 サーバに転送します。このサーバでは、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 サーバの CDR Agent が SFTP 接続で Cisco CDR Repository Manager へのスタンドアロン サーバ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（Cisco Unified Communications Manager のみ）、最初のサーバで 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、Cisco Unified CM Administration（Cisco Unified Communications Manager 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）をサポートしています。Cisco Unified Communications Manager をインストールした後、このサービスが自動的に開始され、グラフィカル ユーザ インターフェイス（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、そのサーバをブラウズしたときに、Cisco Unified Communications Manager Administration のグラフィカル ユーザ 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 Admin サービスは、Cisco Unified Communications Manager および Cisco Unity Connection ではサポートされていません。

Cisco IM and Presence Admin サービスは、Cisco Unified CM IM and Presence Administration（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、そのサーバをブラウズしたときに Cisco Unified IM and Presence Serviceability の GUI にアクセスできなくなります。

サービスのセットアップ

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。

Cisco 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 台のサーバのサービスを一度に開始および停止したりすることができます。

Cisco 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 Phone と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にのみ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、Cisco 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（会議ブリッジや Cisco Messaging Interface など）も起動および停止することがあります。

注意 Cisco 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てい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。

サービスの設定

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 Cisco 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） Cisco Unified Communications Manager Release 6.1.1 以降、エンド ユーザは Cisco Unified Serviceability にアクセスしてサービスを起動および停止することができなくなりました。

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アクティブ化する前に、マルチサーバ Cisco Unified Communications Manager 構成用のサービスの推奨事項を示した次の表を確認してください。

表 44：*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、Cisco Unified Communications Manager をサポートしています。 [コントロール センター - ネットワーク サービス（Control Center - Network Services）] で、Cisco RIS Data Collector サービスと Database Layer 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 Manager Administration の [Cisco Unified Communications Manager検索/リスト（Cisco Unified Communications Manager Find/List）] ウィンドウに Cisco Unified Communications Manager サーバが表示されることを確認します。サーバ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 Cisco Unified Communications Manager サーバを追加します。 サーバを追加する方法については、『*System Configuration Guide for Cisco Unified Communications Manager*』を参照してください。
Cisco Messaging Interface	サーバに接続された USB/シリアル アダプタを使用してサード パーティ製ボイスメール 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。

サービス/サーブレット	アクティブ化の推奨事項
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 H.323 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ティブ化する必要があります。また、Cisco CallManager および Cisco TFTP サービスはクラスタ内の 1 つのサーバ上で実行するようにしてください。Cisco Unified Mobile Voice Access Service が実行されているサーバと同じサーバである必要はありません。
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 つのサーバ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ます。このサービスでは、クラスタ内の 1 つのノードで Cisco TFTP をアクティブ化する必要があります。最初のノードおよび Cisco CallManager サービスを実行するノードでは、こ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。CTIManager 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化する必要があります。CTIManager および Cisco CallManager サービスの相互作用の詳細については、CM サービスに関連するトピックを参照してください。
Cisco エクステンション モビリティ	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 Collector を実行する 1 つまたは複数のサーバでアクティブ化します。クラスタ内のノードで 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データベースの変更を検出し、/etc/dhcpd.conf ファイルを変更し、DHCPD を停止し、更新された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 が有効化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 のロケーション 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、このサービスをアクティブ化する必要があります。このサービスは、Cisco CallManager サービスとともに動作します。Cisco CallManager サービスを実行するサーバで Cisco Location Bandwidth 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で Location Bandwidth Manager が実行されていない場合は、Location Bandwidth Manager グループが正しく設定されていることを確認します。

サービス/サーブレット	アクティブ化の推奨事項
シスコ クラスタ間検索サービス	複数の Cisco Unified Communications Manager クラスタ間で URI と数字ルーティング情報を伝播する場合、それらのクラスタのパブリッシャでこのサービスをアクティ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 サービス専用の 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	Cisco Unified Communications Manager Dialed Number Analyzer を使用する場合は、このサー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とがあるため、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ィブ化します。
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 つのノードで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ビスをアクティブ化する場合は、オプション 150 を設定します。
CTI サービス	
Cisco IP Manager Assistant	Cisco Unified Communications Manager Assistant を使用する場合は、クラスタ内の任意の 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します。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確認します。 Cisco IP Manager Assistant の詳細については、『 *Feature Configuration Guide for Cisco 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 サービス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て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 フォンをユーザに割り当てることができません。このサービスはデフォルトでは非アクティブ化されています。
CDR サービス	
Cisco SOAP-CDRonDemand サービス	Cisco SOAP-CDROnDemand サービスは、最初のサーバ上だけでアクティブ化することができ、Cisco CDR Repository Manager および Cisco CDR Agent サービスが同じサーバ上で実行されている必要があります。

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、最初のサーバ上だけでアクティブ化することができ、Cisco CAR Scheduler サービスが同じサーバ上でアクティブにされ、実行されており、CDR Repository Manager サービスも同じサーバ上で実行されている必要があります。
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 サービスがデフォルトで有効になります。パブリッシャ ノードではこのサービスを常にアクティブなままにすることを推奨します。これにより、Unified Provisioning Manager などの AXL に依存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 の特定のサブスクライバ 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ます。Bulk Administration Tool（BAT）を使用して電話とユーザを管理している場合は、この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 Phone Address Book Synchronizer の TabSync クライアントは、Cisco Unified Communications Manager 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 Phone Address Book Synchronizer を使用する場合は、このサービスを 1 つのノード（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あります。Cisco IP Phone Address Book Synchronizer を使用しない場合、このサービスを非アクティブ化することを推奨します。このサービスはデフォルトでは非アクティブ化されています。
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ために Cisco Prime Collaboration Deployment（PCD）サーバを使用する場合は、このサービスをアクティブ化する必要があります。Platform Administrative Web サービス（PAWS）により、Call Manager と Prime Collaboration Deployment（PCD）の間で通信を行うことができます。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バでこのサービスをアクティブ化する必要があります。

サービス/サーブレット	アクティブ化の推奨事項
Cisco TAPS サービス	Cisco Unified Communications Manager Auto-Register Phone Tool を使用する前に、最初の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 Communications Manager Auto-Register Phone Tool のダミー MAC アドレスを作成する場合、Cisco Bulk 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	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、最初のノードだけでレポートを生成します。
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でアクティブ化します。
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 *45*：*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	
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。

サービス/サーブレット	推奨事項
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。
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） 永続的なチャット機能は、外部データベースを必要とします。永続的な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、永続的な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。『*Database Setup Guide for IM and Presence on Cisco Cisco 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。

サービス/サーブレット	推奨事項
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。
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 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。『*Interdomain Federation for IM and Presence on Cisco Cisco 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 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。『*Database Setup Guide for IM and Presence on Cisco Cisco Unified Communications Manager*』を参照してください。
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。『*Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager*』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　Cisco Unified Communications Manager および 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。
[サービスの開始（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 Cisco 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 Cisco Unified Communications Manager および 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, （103 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, （107 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 サービスを開始、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。機能サービスを開始、停止、および再起動するには、[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、またはクラスタ設定のクラスタ内のサーバ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 Cisco 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てい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（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。

  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 センタのネットワーク 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 リストからサーバを選択し、[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 6 章

ツールおよびレポート

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にはサーバの「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

この項は、Cisco Unified Communications Manager および IM and Presence Service だけに適用されます。

- Cisco Serviceability Reporter は最初のサーバでのみアクティブなため、Reporter は常に、他のサーバではなく、最初のサーバ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の「システム時刻」が反映されます。最初のサーバとそれに続くサーバが異なるタイムゾーンにある場合は、最初のサーバの「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。

Serviceability Reporter のサービス パラメータ

Cisco Serviceability Reporter は次のサービス パラメータを使用します。

- RTMT Reporter Designated Node：RTMT Reporter が動作する指定ノードを指定します。このデフォルトは、Cisco Serviceability Reporter サービスが最初にアクティブ化されたサーバの IP アドレスです。

  Cisco Unified Communications Manager のみ：Serviceability Reporter サービスは CPU を大量に消費するため、非コール処理ノードを指定することを推奨します。
- Report Generation Time：午前 0 時以降の分数を指定します。レポートは最新日のこの時刻に生成されます。最小値は 0 で、最大値は 1439 です。
- Report Deletion Age：レポートがディスクに保持される日数を指定します。指定した期間を経過したレポートは削除されます。最小値は 0 で、最大値は 30 です。

ヒント　レポートをディセーブルにするには、Report Deletion Age サービス パラメータの値を 0 に設定します。

サービス パラメータ設定に関する詳細については、次のガイドを参照してください。

- Cisco Unified Communications Manager のみ：『*System Configuration Guide for Cisco Unified Communications Manager*』
- Connection のみ：『*System Administration Guide for Cisco Unity Connection*』

（注） Cisco Unified Communications Manager のみ：ノードがネットワークから完全に削除され、Cisco Unified Communications Manager Administration のサーバ リストに表示されない場合、ログ ファイルにそのノードのデータが含まれている場合でも、Reporter はレポートを生成するときにそのノードを含めません。

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。

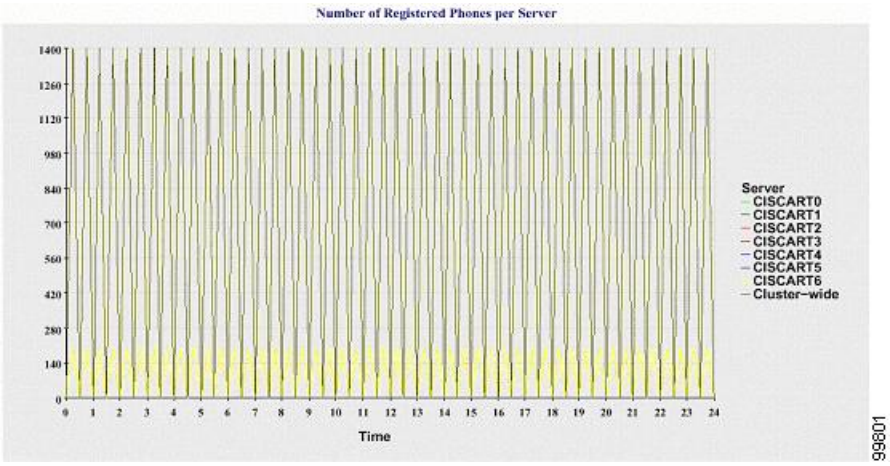
- サーバごとの登録済み電話機の数
- クラスタ内の H.323 ゲートウェイの数
- クラスタ内のトランクの数

サーバごとの登録済み電話機の数

折れ線グラフには、Cisco Unified Communications Manager の各サーバ（および Cisco Unified Communications Manager クラスタ構成内のクラスタ）の登録済み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のデータを表し、クラスタ全体のデータを示す線がさらに 1 本あります（Cisco 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。サーバにデータが表示されない場合、そのサーバを表す線は生成されません。登録済み電話機について、サーバ（または Cisco Unified Communications Manager クラスタ構成内のすべてのサーバ）のデータが存在しない場合、グラフは生成されません。メッセージ「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（No data for Device Statistics report available）」が表示されます。

次の図は、Cisco Unified Communications Manager のクラスタ構成内の Cisco 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。

図 *1*：サーバごとの登録済み電話機の数を示す折れ線グラフ

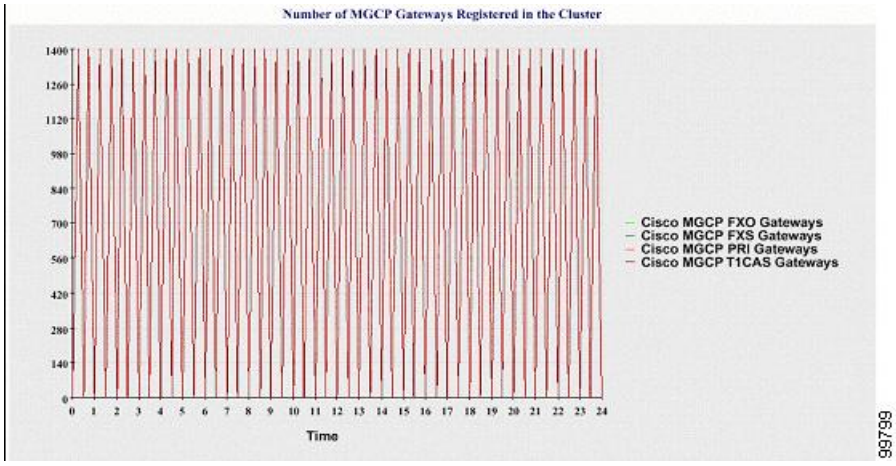


クラスタ内の登録済み MGCP ゲートウェイの数

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、Cisco Unified Communications Manager サーバ（または Cisco Unified Communications Manager クラスタ構成のクラスタ）のデータのみ表しています。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。

次の図は、Cisco 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。

図 *2*：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

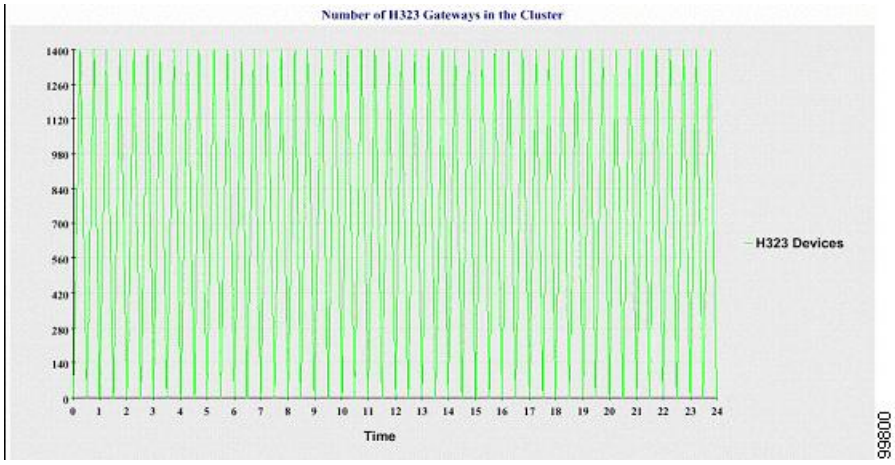


クラスタ内の H.323 ゲートウェイの数

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 本の線により、H.323 ゲートウェイの詳細（または Cisco Unified Communications Manager クラスタ構成のクラスタ全体の詳細）が示されます。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。

次の図は、Cisco 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。

図 *3*：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

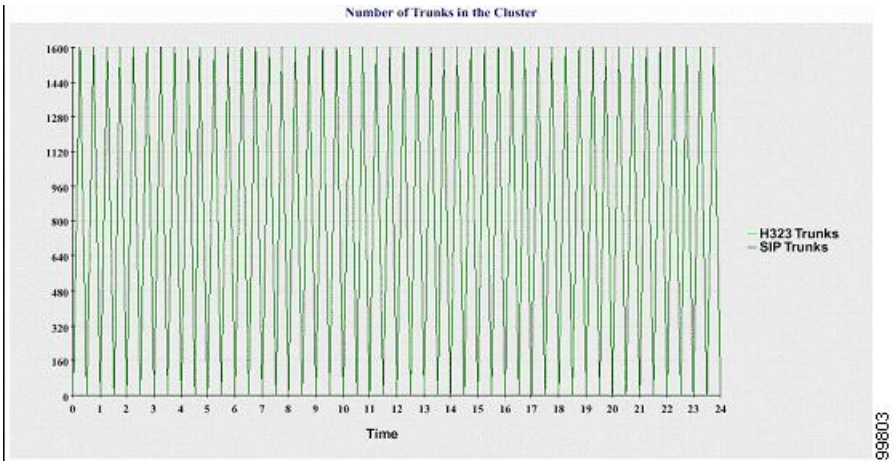


クラスタ内のトランクの数

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 本の線により、H.323 トランクおよび SIP トランクの詳細（または Cisco Unified Communications Manager クラスタ構成のクラスタ全体の詳細）が示されます。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。

次の図は、Cisco 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。

図 *4*：クラスタごとのトランクの数を示す折れ線グラフ



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 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 Cisco 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 Cisco 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 Cisco 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

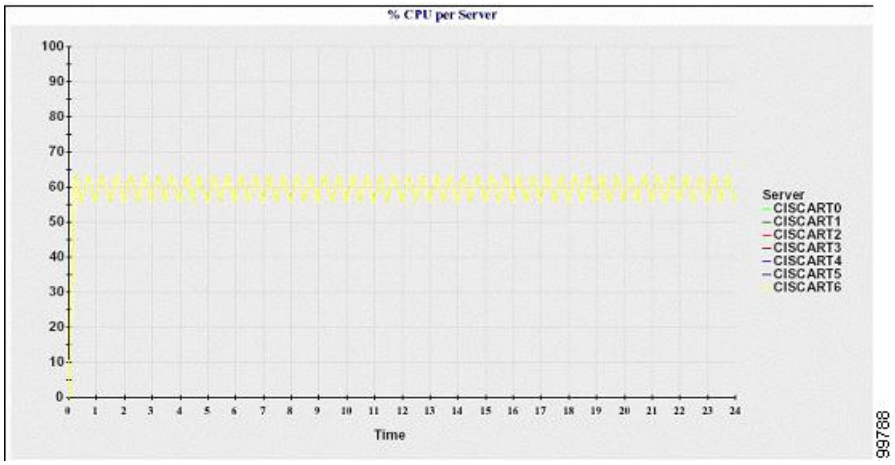
クラスタ固有の統計情報は、Cisco Unified Communications Manager および IM and Presence Service によってのみサポートされます。

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のデータを表します（または、クラスタ内のサーバごとに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（またはクラスタ内のいずれかのサーバ）のデータが存在しない場合、そのサーバ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。メッセージ「サーバ統計レポートのデータがありません（No data for Server Statistics report available）」が表示されます。

次の図は、Cisco 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。

図 *5*：サーバごとの *CPU* のパーセンテージを示す折れ線グラフ

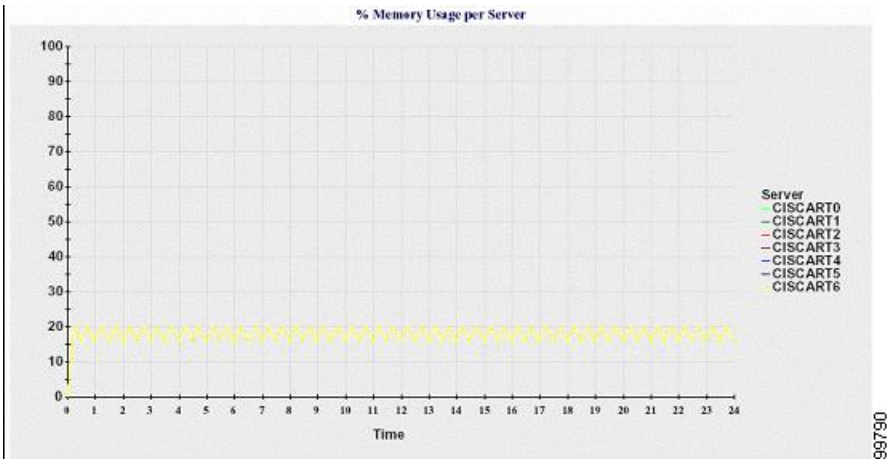


サーバごとのメモリ使用率のパーセンテージ

折れ線グラフには、Cisco Unified Communications Manager サーバのメモリ使用率のパーセンテージ（%MemoryInUse）が表示されます。Cisco 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のデータが存在しない場合、Reporter はそのサーバを表す線を生成しません。

次の図は、クラスタ構成で Cisco 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。

図 *6*：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

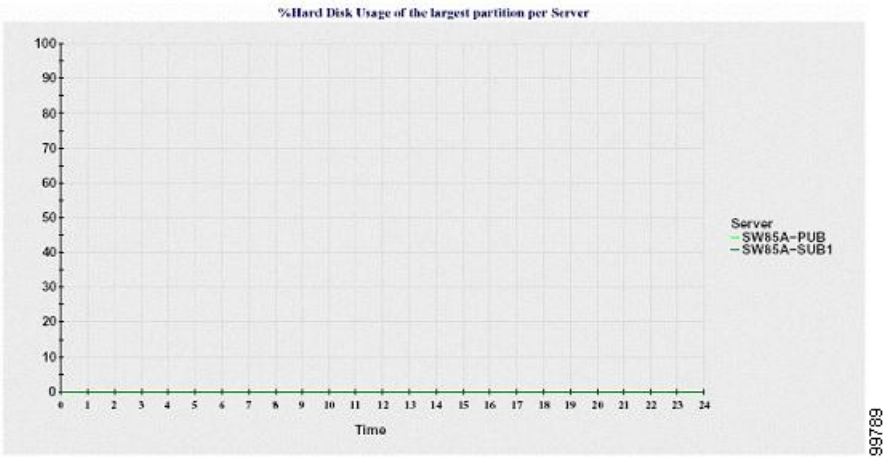


サーバごとの最大パーティションのハード ディスク使用率のパーセンテージ

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のデータが存在しない場合、Reporter はそのサーバを表す線を生成しません。

次の図は、Cisco 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。

図 *7*：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



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。

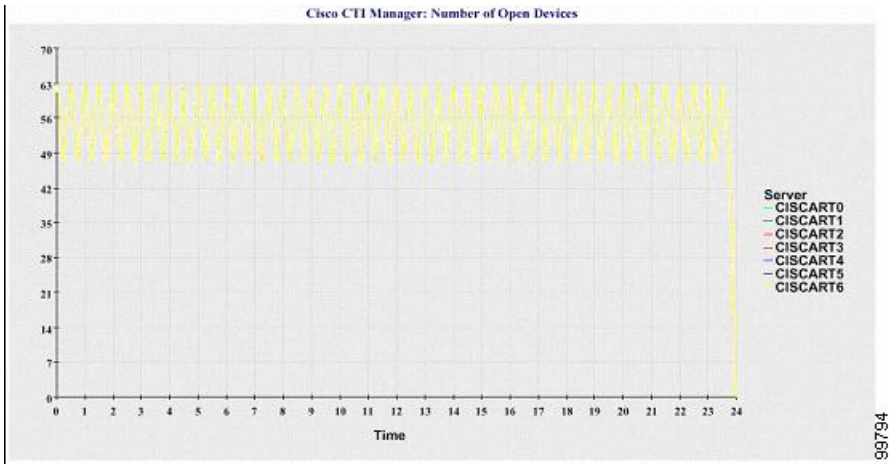
- Cisco CTI Manager：オープン デバイスの数
- Cisco CTI Manager：オープン回線の数
- Cisco TFTP：要求の数
- Cisco TFTP：中断された要求の数

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 Cisco 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 Cisco 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。Cisco Unified Communications Manager クラスタ構成でいずれかのサーバのデータが存在しない場合、Reporter はそのサーバを表す線を生成しません。メッセージ「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（No data for Service Statistics report available）」が表示されます。

次の図は、Cisco 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。

図 *8*：*Cisco CTI Manager*：オープン デバイスの数を示す折れ線グラフ

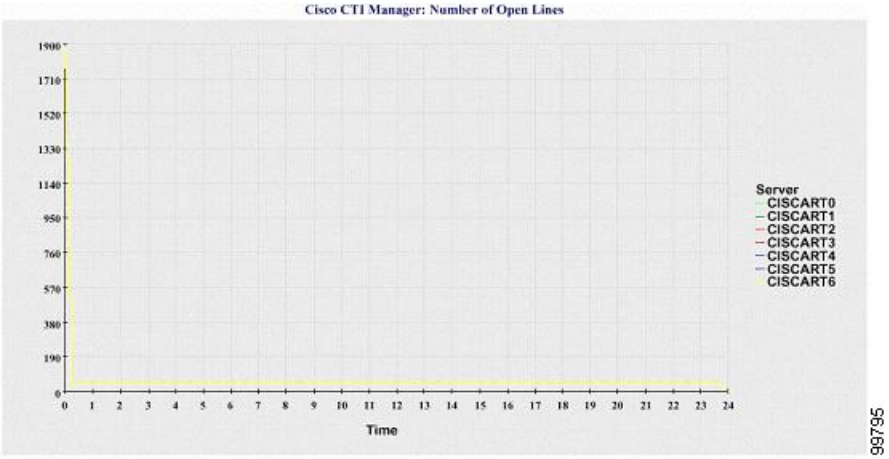


Cisco CTI Manager：オープン回線の数

折れ線グラフには、CTI Manager（または Cisco 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のデータを表します（または Cisco Unified Communications Manager クラスタ構成内のサーバごとに 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。Cisco Unified Communications Manager クラスタ構成でいずれかのサーバのデータが存在しない場合、Reporter はそのサーバを表す線を生成しません。

次の図は、Cisco 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。

図 *9*：*Cisco CTI Manager*：オープン回線の数を示す折れ線グラフ

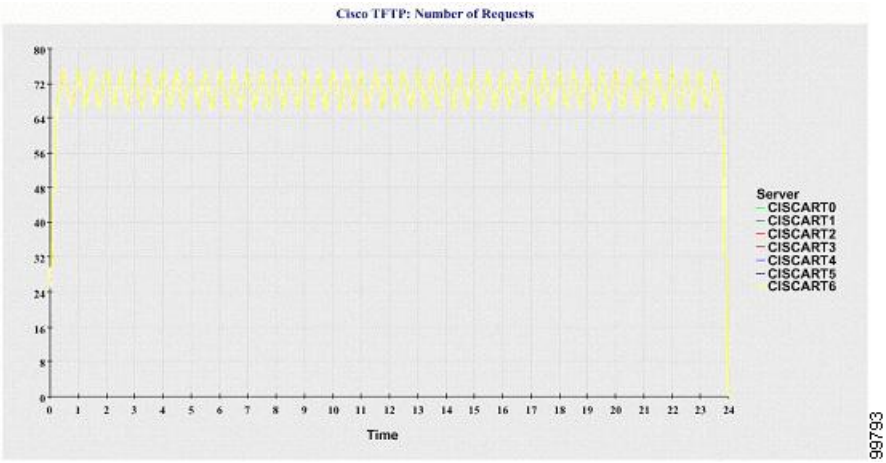


Cisco TFTP：要求の数

折れ線グラフには、TFTP サーバ（または Cisco Unified Communications Manager クラスタ構成内の TFTP サーバごと）の Cisco TFTP 要求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のデータを示します（または Cisco Unified Communications Manager クラスタ内のサーバごとに 1 本の線）。グラフ内の各データ値は、15 分間の TFTP 要求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。Cisco Unified Communications Manager クラスタ構成でいずれかのサーバのデータが存在しない場合、Reporter はそのサーバを表す線を生成しません。

次の図は、TFTP サーバごとの Cisco TFTP 要求の数を表す折れ線グラフの例を示します。

図 *10*：*Cisco TFTP*：要求の数を示す折れ線グラフ

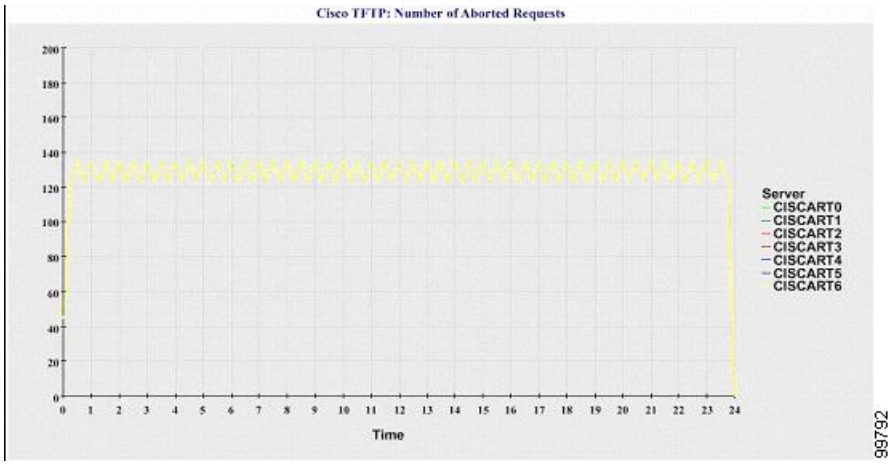


Cisco TFTP：中断された要求の数

折れ線グラフには、TFTP サーバ（または Cisco Unified Communications Manager クラスタ構成内の TFTP サーバごと）の中断された Cisco TFTP 要求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のデータを示します（または Cisco Unified Communications Manager クラスタ内のサーバごとに 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 要求の平均を表します。データが存在しない場合はグラフが生成されません。Cisco Unified Communications Manager クラスタ構成でいずれかのサーバのデータが存在しない場合、Reporter はそのサーバを表す線を生成しません。

次の図は、TFTP サーバごとに中断された Cisco TFTP 要求の数を表す折れ線グラフの例を示します。

図 *11*：*Cisco TFTP*：中断された要求の数を示す折れ線グラフ



サーバ（または Cisco 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 Cisco 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

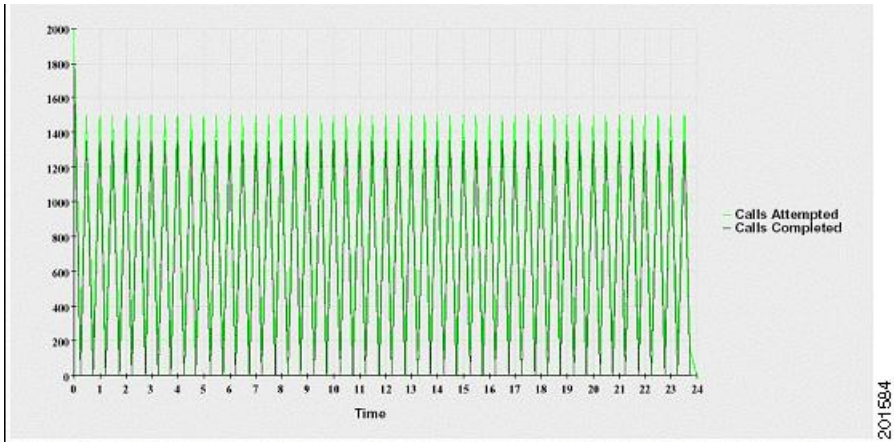
クラスタの Cisco Unified Communications Manager コール アクティビティ

折れ線グラフには、試行された Cisco Unified Communications Manager コールと完了したコールの数が表示されます。Cisco Unified Communications Manager クラスタ構成では、折れ線グラフに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が表示されます。グラフは 2 本の線で構成され、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。Cisco Unified Communications Manager クラスタ構成の場合、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 Cisco Unified Communications Manager 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 Cisco 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。Cisco Unified Communications Manager クラスタ構成では、クラスタ内のサーバに関するデータが存在しない場合、そのサーバで試行されたコールと完了したコールを表す線は生成されません。Cisco 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。メッセージ「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（No data for Call Activities report available）」が表示されます。

次の図は、Cisco 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。

図 *12*：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



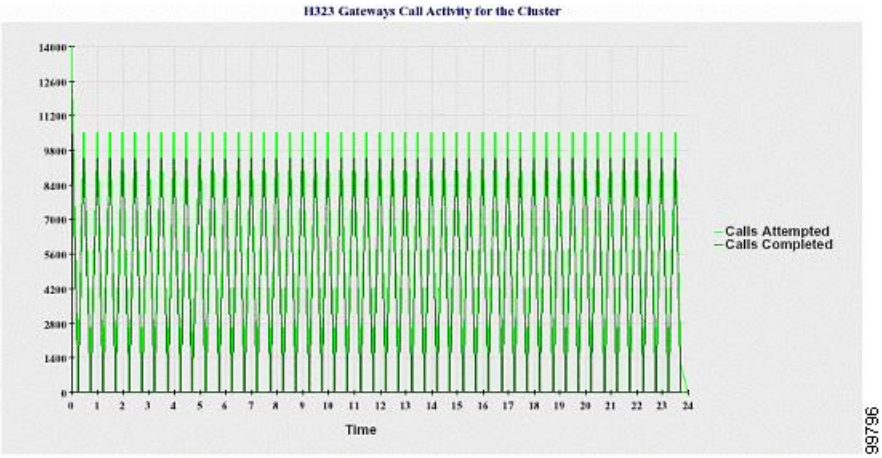
クラスタの H.323 ゲートウェイ コール アクティビティ

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。Cisco Unified Communications Manager クラスタ構成では、折れ線グラフに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が表示されます。グラフは 2 本の線で構成され、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。Cisco Unified Communications Manager クラスタ構成の場合、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の値の合計と同じ値です。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 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。Cisco Unified Communications Manager クラスタ構成では、クラスタ内のサーバに関するデータが存在しない場合、そのサーバで試行されたコールと完了したコールを表す線は生成されません。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。

次の図は、Cisco 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。

図 *13*：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

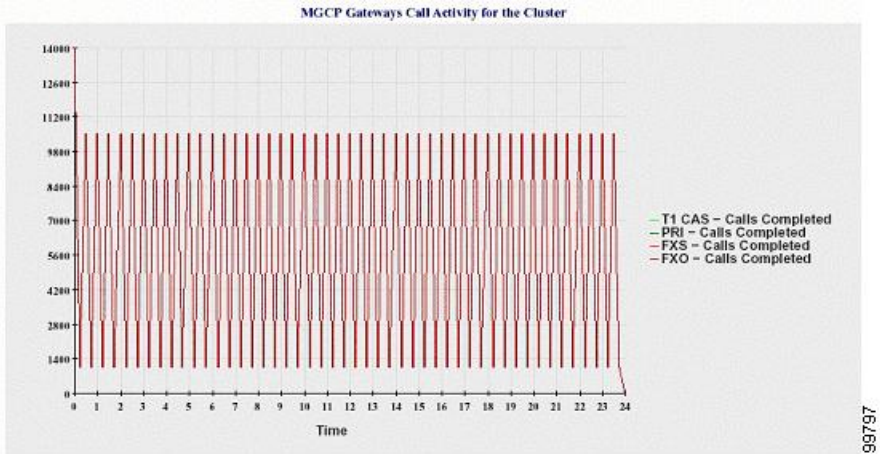


クラスタの MGCP ゲートウェイ コール アクティビティ

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。Cisco Unified Communications Manager クラスタ構成では、グラフには Cisco 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。

次の図は、Cisco 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。

図 *14*：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

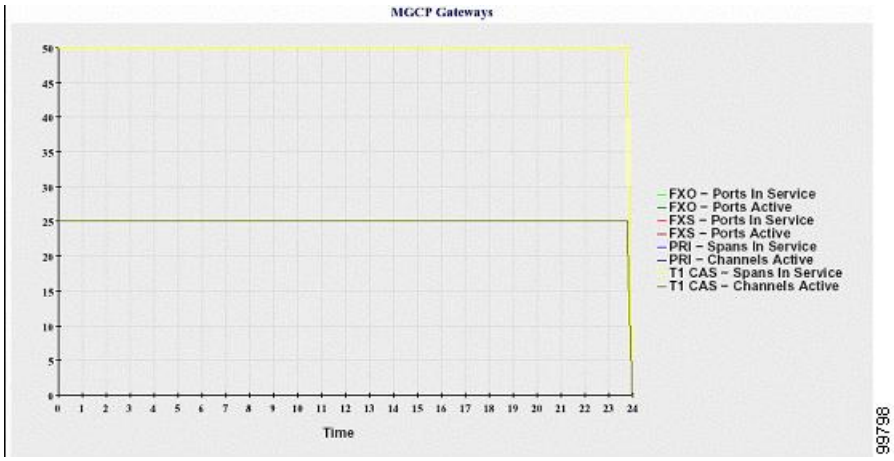


MGCP ゲートウェイ

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。Cisco Unified Communications Manager クラスタ構成の場合、グラフには Cisco 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。Cisco Unified Communications Manager クラスタ構成の場合、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。

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。

図 *15*：*MGCP* ゲートウェイを示す折れ線グラフ

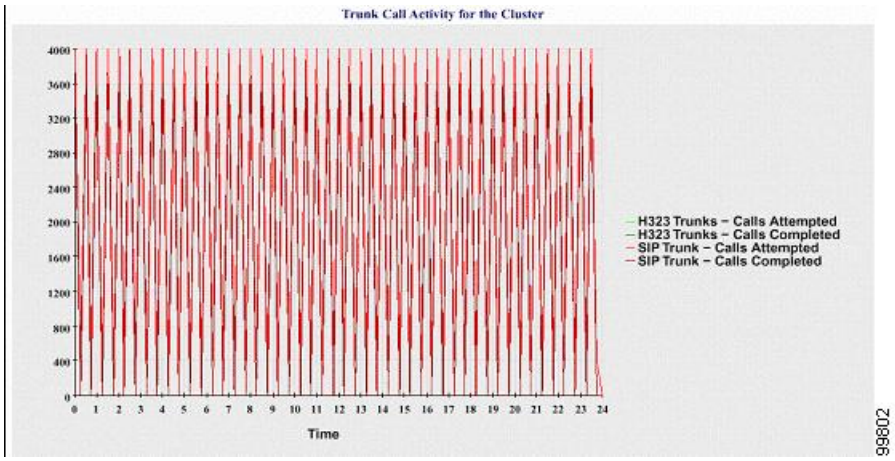


クラスタのトランク コール アクティビティ

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。Cisco Unified Communications Manager クラスタ構成の場合、グラフには Cisco 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、2 本は（データが利用できる）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。Cisco Unified Communications Manager クラスタ構成の場合、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。

次の図は、Cisco 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。

図 *16*：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



サーバ（または Cisco 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。

- Cisco Unified Communications Manager（または Cisco 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 Cisco Unified Communications Manager クラスタ内の各サーバのゲートウェイ）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 Cisco Unified Communications Manager クラスタ内の各サーバのゲートウェイ）の完了したコール
- （Cisco Unified Communications Manager クラスタ内の各サーバの）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

アラート要約レポート

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、Cisco 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

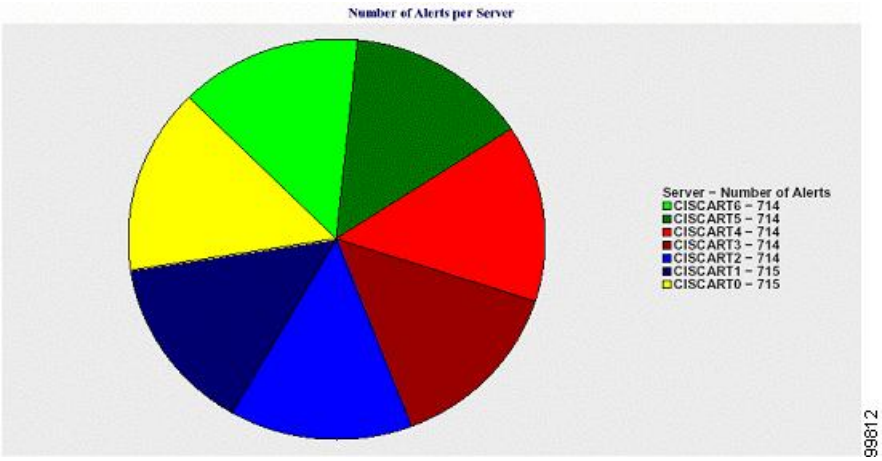
クラスタ内のノードごとのアラートの数が円グラフに表示されます。グラフには、生成されたアラートのサーバ全体の詳細が表示されます。円グラフの各領域は、クラスタの特定のサーバに対

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。あるサーバのデータがない場合、そのサーバを表すチャートの領域はありません。すべてのサーバのデータが存在しない場合はグラフが生成されません。メッセージ「その日はアラートが生成されませんでした（No alerts were generated for the day）」が表示されます。

Cisco Unity Connection のみ：円グラフには、サーバ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。サーバのデータが存在しない場合はグラフが生成されません。メッセージ「その日はアラートが生成されませんでした（No alerts were generated for the day）」が表示されます。

次のグラフは、Cisco Unified Communications Manager クラスタ内のサーバごとのアラート数を表す円グラフの例を示しています。

図 *17*：サーバごとのアラート数を示す円グラフ

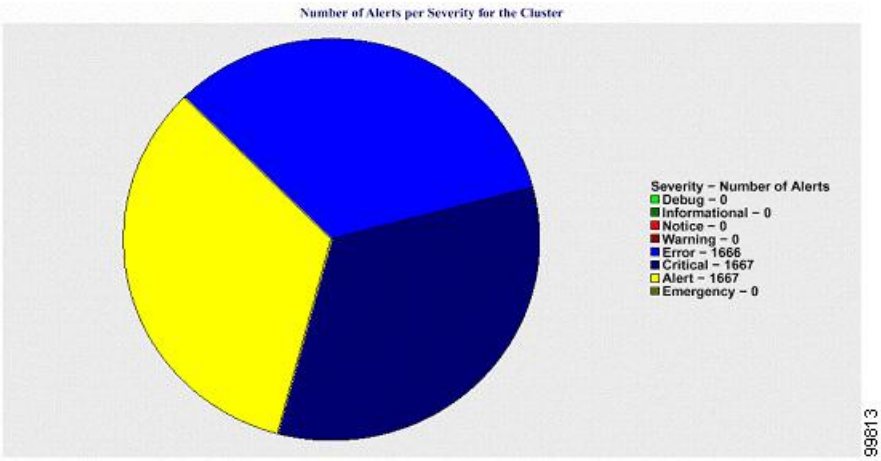


クラスタの重大度ごとのアラート数

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。

次のグラフは、Cisco Unified Communications Manager クラスタの重大度ごとのアラート数を表す円グラフの例を示しています。

図 *18*：クラスタの重大度ごとのアラート数を示す円グラフ

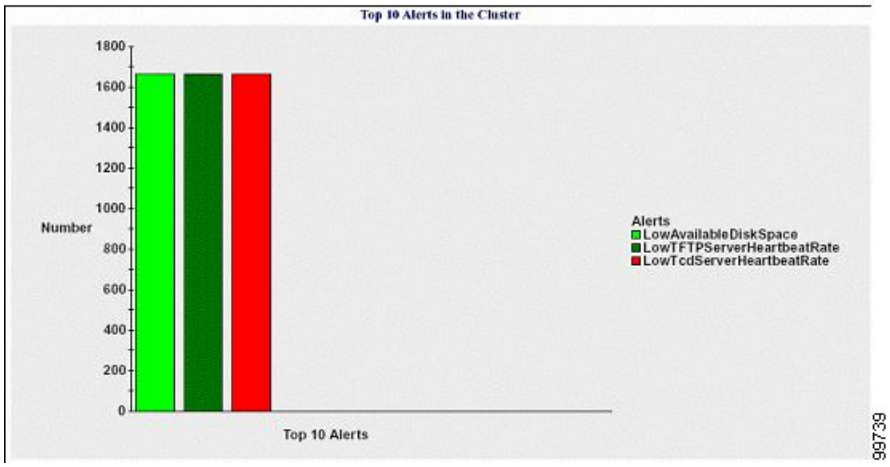


クラスタ内の上位 10 のアラート

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。

次のグラフは、Cisco 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 *19*：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。Cisco Unified Communications Manager のクラスタ構成では、クラスタ内の各サーバのデータについて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。Cisco 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 Cisco 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。Cisco 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 Cisco 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。

サービスアビリティ レポートのアーカイブのセットアップの概要

次の手順では、サービスアビリティ レポートのアーカイブ機能を設定する方法について説明します。

手順

ステップ 1 Cisco Serviceability Reporter サービスをアクティブ化します。

ステップ 2 Cisco Serviceability Reporter サービスのパラメータを設定します。

ステップ 3 Cisco Serviceability Reporter サービスが生成するレポートを表示します。

関連トピック

機能サービスのアクティブ化, （112 ページ）
Serviceability Reporter のサービス パラメータ, （118 ページ）

サービスアビリティ レポートのアーカイブのセットアップ

Cisco Serviceability Reporter サービスは、Cisco Unified Serviceability の日次レポートを生成します。各レポートには、特定のレポートの統計を示すさまざまなチャートを構成す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。

ここでは、[サービスアビリティ レポートのアーカイブ（Serviceability Reports Archive）] ウィンドウの使用方法について説明します。

はじめる前に

Cisco Serviceability Reporter サービスをアクティブ化します。このサービスをアクティブ化すると、CPU に高い負荷がかかります。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。

Cisco Unified Communications Manager の場合のみ：このサービスはコール処理を行わないサーバでアクティブ化することを推奨します。

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。
[サービスアビリティ レポートのアーカイブ（Serviceability Reports Archive）] ウィンドウにレポートを確認できる月と年が表示されます。

ステップ 2 [年月（Month-Year）] ペインから、レポートを表示する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 レポートを表示するには、レポートが生成された日に対応するリンクをクリックします。
選択した日のレポート ファイルが表示されます。

ステップ 4 特定の PDF レポートを表示するには、表示したいレポートのリンクをクリックします。

ヒント ブラウザでノード名を使用して Cisco Unified Serviceability を表示した場合は、レポートを表示する前に Cisco Unified Serviceability にログインする必要があります。

ネットワークでネットワーク アドレス変換（NAT）を使用しているときに NAT の内側にあるサービスアビリティ レポートにアクセスする場合は、ブラウザの URL に NAT に関連付けられたプライベート ネットワークの IP アドレスを入力します。NAT の外側にあるレポートにアクセスする場合は、パブリック IP アドレスを入力すると、NAT によってプライベート IP アドレスに適切に変換/マッピングされます。

PDF 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、[サービスアビリティ レポートのアーカイブ（Serviceability Reports Archive）] ウィンドウの下部にあるリンクをクリックします。

ウィンドウが開き、選択したレポートの PDF ファイルが表示されます。

サービスアビリティ レポートのアーカイブへのアクセス

サービスアビリティ レポートのアーカイブのアクティブ化

手順

ステップ 1 [ツール（Tools）] > [サービスの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）] リスト ボックスで、必要なサーバを選択し、[移動（Go）] を選択します。

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）] ペインに移動します。

ステップ 4 [Cisco Serviceability Reporter サービス（Cisco Serviceability Reporter service）] チェックボックスをオンにして、[Save（保存）] を選択します。

ステップ 5 [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。

ステップ 6 [サーバ（Server）] リスト ボックスで、必要なサーバを選択し、[移動（Go）] を選択します。

ステップ 7 [パフォーマンスおよびモニタリング サービス（Performance and Monitoring services）] に移動し、Cisco Serviceability Reporter を探します。

ステップ 8 Cisco Serviceability Reporter のステータスが [起動済み（Started）] かつ [アクティブ化（Activated）] になっていることを確認します。Cisco Serviceability Reporter が動作していない場合は、Cisco Serviceability Reporter を選択し、[開始（Start）] を選択します。

次の作業

ブラウザでサーバ名を入力して Cisco Unified IM and Presence Serviceability を開いた場合は、レポートを表示する前に Cisco Unified IM and Presence Serviceability にサインインする必要があります。

Cisco Unified IM and Presence Serviceability 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、必ず最初のノードでレポートを生成します。

サービスアビリティ レポートのアーカイブへのアクセス

はじめる前に

Cisco Serviceability Reporter サービスをアクティブ化します。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。

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 [年月（Month-Year）] セクションで、レポートを表示する月と年を選択します。

ステップ 3 レポートが生成された日に対応するリンクを選択し、必要なレポートを表示します。

ステップ 4 表示するレポートのリンクを選択し、特定の PDF レポートを表示します。
[トレースフィルタ設定（Trace Filter Settings）] 領域のデバイスに関係するセクションは、IM and Presence には関係しません。

ヒント ブラウザでサーバ名を入力して Cisco Unified IM and Presence Serviceability を開いた場合は、レポートを表示する前に Cisco Unified IM and Presence Serviceability にサインインする必要があります。

CDR Repository Manager

この項の内容は、IM and Presence Service には適用されません。

[CDRの管理設定（CDR Management Configuration）] ウィンドウを使用して、呼詳細レコード（CDR）ファイルと呼管理レコード（CMR）ファイルに割り当てるディスク領域の容量、ファイルを削除するまでの保存日数、およびCDRの送信先となる最大3つの課金アプリケーションサーバを設定します。CDR Repository Manager サービスは、CDR ファイルと CMR ファイルが正常に送信されるか、[CDRの管理設定（CDR Management Configuration）] ウィンドウで課金アプリケーションサーバが変更または削除されるか、ファイルが保存期間を過ぎて削除されるまで、[CDRの管理設定（CDR Management Configuration）] ウィンドウに設定されている課金サーバに対して、これらのファイルの送信を繰り返し試行します。

（注） [エンタープライズ パラメータ設定（Enterprise Parameters Configuration）] ウィンドウにアクセスするには、Cisco Unified Communications Manager Administration を開き、[システム（System）] > [エンタープライズ パラメータ（Enterprise Parameters）] の順に選択します。**CDR File Time Interval** パラメータは、CDR データを収集する際の間隔を指定します。たとえば、この値を 1 に設定すると、各ファイルには1分間のCDRデータ（有効になっている場合はCDR と CMR）が含まれます。外部課金サーバと CAR データベースは、この間隔が経過するまで各ファイルのデータを受信しません。そのため、このパラメータに設定する間隔を決める際には、どのくらい早く CDR データにアクセスする必要があるかを考慮してください。たとえば、このパラメータを60に設定すると、各ファイルには60分間のデータが含まれますが、60分が経過し、レコードが CAR データベースに書き込まれ、CDR ファイルが設定済みの課金サーバに送信されるまで、そのデータは使用できません。デフォルト値は 1 です。最小値は 1 で、最大値は 1440 です。この必須フィールドの測定単位は分です。

CDR Agent と CDR Repository Manager の両方により、CDR File Time Interval に依存しない間隔でファイルが処理されます。CDR Repository Manager は、課金アプリケーション サーバに既存のすべての CDR ファイルを送信し、6 秒間スリープしてから送信する新しいファイルを確認して、この 6 秒間隔の動作を継続して行います。宛先（外部課金アプリケーション サーバ）が応答しない場合、スリープ間隔の 2 倍の長さ（12 秒）でプロセスが再試行されます。配信が失敗するたびにスリープ時間が倍増し（6、12、24、48 秒というように）、これは2分間に達するまで続きます。それ以降は配信が成功するまで 2 分間隔になります。配信が成功すると、自動的に 6 秒間隔に戻ります。

ユーザは、6 秒の処理間隔および障害時に倍増するスリープ間隔を設定できません。ユーザが設定できるのは、**CDR File Time Interval** エンタープライズ パラメータだけです。最初のファイル配信失敗後はアラートは送信されません。デフォルトでは、任意の課金アプリケーション サーバにファイルを配信する Cisco CDR Repository Manager サービスが 2 回目に配信に失敗した後に、CDRFileDeliveryFailed アラートが生成されます。電子メールを送信したり、ポケットベルなどで通知するようにアラートを設定できます。アラートの設定の詳細については、『*Cisco Unified Real-Time Monitoring Tool Administration Guide*』の「Working with Alerts」の章を参照してください。

それ以降に課金アプリケーション サーバにファイルを配信できなかった場合は、CDRFileDeliveryFailureContinues の syslog アラームが生成されます。

CDR Agent はほぼ同じように動作します。まず、パブリッシャに既存のすべての CDR ファイルを送信します。送信する追加ファイルがない場合、CDR Agent は 6 秒間スリープしてから新しいファイルを確認します。配信が失敗するとすぐにスリープ間隔が 1 分間に変更され、配信が成功するまで 1 分間隔になります。ファイルの配信が成功すると、6 秒間隔に戻ります。

CDR Agent が最初にファイル配信に失敗した後は、アラートは送信されません。デフォルトでは、CDR Agent が 2 回目に配信に失敗した後に、CDRAgentSendFileFailed アラートが生成されます。電子メールを送信したり、ポケットベルなどで通知するようにアラートを設定できます。アラートの設定の詳細については、『*Cisco Unified Real-Time Monitoring Tool Administration Guide*』の「Working with Alerts」の章を参照してください。

それ以降にファイルを配信できなかった場合は、CDRAgentSendFileFailedContinues の syslog アラームが生成されます。

ファイル転送タイマーを起動または再起動する必要がある場合は、[Cisco Unified Serviceability] ウィンドウに移動し、[ツール（Tools）] > [コントロール センター（Control Center）] > [ネットワーク サービス（Network Services）] を選択すると、Cisco CDR Repository Manager または CDR Agent プロセスを再開できます。

High Water Mark パラメータに基づいてファイルの削除を有効にすると、CDR Repository Manager サービスは、CDR ファイルと CMR ファイルが使用するディスク領域の容量をモニタします。ディスク使用率が設定されている上限を超えると、ディスク領域が下限値に達するか、正常に配信されたファイルがすべて削除されるまで、すべての宛先に正常に配信され、（CAR がアクティブな場合は）CAR データベースにロードされた CDR ファイルおよび CMR ファイルがパージされます。正常に配信されたファイルがすべて削除された後もディスク使用率が上限を超えている場合は、ディスク使用率が設定されているディスク割り当て量を超えていない限り、それ以上ファイルは削除されません。ディスク使用率が設定されているディスク割り当て量を超える場合は、ファ

イルが保存期間内であるかどうか、または正常に配信されたかどうかに関係なく、ディスク使用率が上限を下回るまで、最も古いファイルからパージされます。

（注） High Water Mark パラメータに基づくファイルの削除を有効にするかどうかに関係なく、ディスク使用率が設定されているディスク割り当て量を超える場合は、CDR Repository Manager サービスによって、ディスク使用率が上限を下回るまで、最も古いファイルから CDR ファイルおよび CMR ファイルが削除されます。

Cisco Log Partition Monitoring Tool サービスは、CDR Repository Manager に配信されていない CDR フラット ファイルおよび CMR フラット ファイルのディスク使用率をモニタします。

Cisco Unified Communications Manager のみ：サーバのログ パーティションのディスク使用率が設定されている上限を超過し、サービスによって他のログファイルとトレースファイルがすべて削除されている場合は、ログ パーティション モニタ サービスによって、CDR Repository Manager に配信されていない後続ノードの CDR/CMR ファイルが削除されます。

ログ パーティション モニタリングの詳細については、『*Cisco Unified Real-Time Monitoring Tool Administration Guide*』を参照してください。

一般パラメータのセットアップ

CDR のディスク使用およびファイル保存パラメータを設定するには、次の手順を実行します。

手順

ステップ 1 [ツール（Tools）] > [CDR管理（CDR Management）] を選択します。
[CDR管理（CDR Management）] ウィンドウが表示されます。

ステップ 2 変更する CDR Manager 一般パラメータ値をクリックします。

ステップ 3 適切な CDR Repository Manager 一般パラメータの設定を入力します。

ステップ 4 [更新（Update）] をクリックします。

ヒント いつでも [デフォルトの設定（Set Default）] をクリックしてデフォルト値を指定できます。デフォルトの設定後、[更新（Update）] をクリックしてデフォルト値を保存します。

関連トピック

一般パラメータの設定, （143 ページ）

一般パラメータの設定

次の表では、[CDRの管理設定（CDR Management Configuration）] ウィンドウの [一般パラメータ（General Parameters）] セクションでの設定について説明します。

表 *46*：*CDR Repository Manager* の一般パラメータの設定

フィールド	説明
ディスク割り当て (MB)（Disk Allocation (MB)）	CDR および CMR フラット ファイル ストレージに割り当てる数値をメガバイトで選択します。 デフォルトのディスクの割り当てと範囲は、サーバのハードドライブのサイズによって変わります。 （注） CAR データベースの最大サイズは、Cisco Unified Communications Manager サーバの場合は 3328 MB です。 ディスク使用率が CDR ファイルに割り当てられた最大ディスク容量を超えると、システムによって CDRMaximumDiskSpaceExceeded アラートが生成され、正常に処理されたファイル（課金サーバに送信され、CAR にロードされたもの）がすべて削除されます。ディスク使用率が依然として割り当てられているディスク容量を超えている場合は、ディスク使用率の上限を下回るまで、未配信ファイルと保存期間内のファイルが最も古いものから削除されます。 大規模なシステムで十分なディスク領域が割り当てられていない場合は、CAR Scheduler が CAR データベースにファイルをロードする前に、システムによって CDR ファイルと CMR ファイルが削除される場合があります。たとえば、CAR Scheduler が 1 日に 1 回実行されるよう設定した場合に、ディスク割り当ての設定が 1 日に生成される CDR ファイルおよび CMR ファイルを保存するには不十分な大きさであると、これらのファイルが CAR データベースにロードされる前にシステムによって削除されます。

フィールド	説明
上限(%)（High Water Mark (%)）	このフィールドには、CDR ファイルおよび CMR ファイルに割り当てられるディスク容量の最大割合を指定します。たとえば、[ディスク割り当て（Disk Allocation）] フィールドから 2000 メガバイトを選択し、[上限(%)（High Water Mark (%)）] フィールドから 80% を選択した場合、上限は 1600 メガバイトになります。上限の割合に加えて、CAR データベースの CDR 数は 1 つの Cisco Unified Communications Manager サーバで 2,000,000 レコードを超えることはできません。 ディスク使用率が指定した割合を超えた場合、または CDR の総数が上限を超えた場合で、[HWMに基づくCDRまたはCMRファイルの削除の無効化（Disable CDR/CMR Files Deletion Based on HWM）] チェックボックスがオフにされている場合には、正常に処理された CDR ファイルおよび CMR ファイル（課金サーバに送信され、CAR にロードされたもの）が、最も古いファイルから自動的に消去され、ディスク使用率が [下限(%)（Low Water Mark (%)）] ドロップダウン リスト ボックスで指定した量になるまで減らされます。 ディスク使用率が依然として下限または上限を超えている場合、ディスク使用率がディスク割り当ての値を超えていなければ、未配信のファイルまたはアンロードされたファイルは削除されません。 [HWMに基づくCDRまたはCMRファイルの削除の無効化（Disable CDR/CMR Files Deletion Based on HWM）] チェックボックスをオンにした場合は、CDR と CMR がこのフィールドで指定した割合に基づいて削除されることはありません。 （注） CDR のディスク領域が上限を超えると、システムによって CDRHWMExceeded アラートが生成されます。
下限(%)（Low Water Mark (%)）	このフィールドには、常に使用可能な CDR ファイルおよび CMR ファイルに割り当てるディスク容量の割合を指定します。たとえば、[ディスク割り当て（Disk Allocation）] フィールドから 2000 メガバイトを選択し、[下限(%)（Low Water Mark (%)）] フィールドから 40% を選択した場合、下限は 800 メガバイトになります。
CDRまたはCMRファイルの保持期間(日数)（CDR / CMR Files Preservation Duration (Days)）	CDR ファイルおよび CMR ファイルを保持する日数を選択します。CDR Repository Manager は保持期間を過ぎたファイルを削除します。 （注） CDRMaximumDiskSpaceExceeded アラームが繰り返し発生する場合は、ディスク割り当てを増やすか、または保持日数を短くしてください。

フィールド	説明
HWMに基づくCDRまたはCMRファイルの削除の無効化（Disable CDR/CMR Files Deletion Based on HWM）	（注） 上限のパラメータに基づく削除を有効化しているかどうかに関係なく、ディスク使用率が設定されているディスク割り当て、最大データベース サイズ、またはインストール環境の最大レコード数を超過した場合は、ディスク使用率が上限を下回るまで CDR Repository Manager サービスによって CDR ファイルおよび CMR ファイルが古いものから削除されます。 ディスク使用率が [上限(%)（High Water Mark (%)）] フィールドで指定した割合を超えた場合でも CDR と CMR を削除したくない場合は、この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されているため、ディスク使用率が上限を超過するとシステムによって CDR と CMR が削除されます。
CDR Repository Managerのホスト名（CDR Repository Manager Host Name）	このフィールドには、CDR Repository Manager サーバのホスト名が一覧されます。
CDR Repository Managerのホストアドレス（CDR Repository Manager Host Address）	このフィールドには、CDR Repository Manager サーバの IP アドレスが一覧されます。

アプリケーション課金サーバのセットアップ

CDR の送信先となるアプリケーション課金サーバを設定するには、次の手順を使用します。最大 3 台の課金サーバを設定できます。

手順

ステップ 1 [ツール（Tools）] > [CDRの管理設定（CDR Management Configuration）] の順に選択します。
[CDR の管理設定（CDR Management Configuration）] ウィンドウが表示されます。

ステップ 2 次のいずれかの作業を実行します。

- 新しいアプリケーション課金サーバを追加するには、[新規追加（Add New）] ボタンをクリックします。
- 既存のアプリケーション課金サーバを更新するには、サーバのホスト名/IP アドレスをクリックします。

ステップ 3 アプリケーション課金サーバのパラメータ設定を入力します。

ステップ 4 [追加（Add）] または [更新（Update）] をクリックします。

関連トピック

アプリケーション課金サーバのパラメータ設定, （146 ページ）

アプリケーション課金サーバのパラメータ設定

次の表に、[CDRの管理設定（CDR Management Configuration）] ウィンドウの [課金アプリケーションサーバのパラメータ（Billing Application Server Parameters）] セクションで使用可能な設定について説明します。

表 47 : アプリケーション課金サーバのパラメータ設定

フィールド	説明
ホスト名/IP アドレス（Host Name/IP Address）	CDR の送信先となるアプリケーション課金サーバのホスト名または IP アドレスを入力します。 このフィールドの値を変更すると、新しい宛先に未配信のファイルを送信するかどうかを尋ねるプロンプトが表示されます。 次のいずれかの作業を実行します。 • 新しいサーバにファイルを配信する場合は、[はい（Yes）] をクリックします。 • 未配信ファイルを送信せずにサーバのホスト名/IPアドレスを変更するには、[いいえ（No）] をクリックします。CDR 管理サービスによって CDR および CMR ファイルは正常に配信されたものとしてマークされます。
ユーザ名（User Name）	アプリケーション課金サーバのユーザ名を入力します。
プロトコル（Protocol）	設定済みの課金サーバへCDR ファイルを送信するために使用するプロトコルを FTP または SFTP から選択します。

フィールド	説明
ディレクトリ パス（Directory Path）	CDR の送信先となるアプリケーション課金サーバ上のディレクトリ パスを入力します。指定するパスは、アプリケーション課金サーバで動作しているオペレーティング システムによって、「“/”」または「“\”」で終了する必要があります。 （注） FTP ユーザにディレクトリに対する書き込み権限があることを確認します。
パスワード（Password）	アプリケーション課金サーバへのアクセスに使用するパスワードを入力します。
障害時に再送（Resend on Failure）	[障害時に再送（Resend on Failure）] ボックスをオンにすると、FTP または SFTP 接続が復旧した後に古い CDR および CMR ファイルを課金サーバに送信するように CDRM に通知されます。ボックスをオンにすると、Resend on Failure フラグが True に設定されます。チェックボックスをチェックしない場合、Resend on Failure フラグが False に設定されます。 さまざまなシナリオが発生する可能性があります。課金サーバの Resend on Failure フラグが True に設定されている場合、すべての CDR ファイルが課金サーバに移動されます。Resend On Failure フラグが False に設定されている場合、課金サーバのシャットダウン中に生成された CDR ファイルが処理済みのフォルダに移動されますが、課金サーバには移動されません。Resend on Failure フラグが最初に True に設定された後で何度か変更された場合、[障害時に再送（Resend on Failure）] ボックスがオンになるたびに CDR ファイルが課金サーバに移動されます。
新しいキーの生成（Generate New Key）	新しいキーを生成し、SFTP サーバへの接続をリセットするには、[リセット（Reset）] ボタンをクリックします。

アプリケーション課金サーバの削除

アプリケーション課金サーバを削除するには、次の手順を使用します。

手順

ステップ 1 [ツール（Tools）] > [CDR管理（CDR Management）] を選択します。
[CDR の管理設定（CDR Management Configuration）] ウィンドウが表示されます。

ステップ 2 削除するアプリケーション課金サーバの隣にあるチェックボックスをオンにして、[選択項目の削除（Delete Selected）] をクリックします。
このサーバを削除すると、このサーバにまだ送信されていない CDR ファイルまたは CMR ファイルがこのサーバに送信されず、正常に送信されたファイルとして処理されることを示すメッセージが表示されます。

ヒント サーバを削除するとき、システムはそのサーバに送信されないファイルに対して CDRFileDeliveryFailed アラートを生成しません。

ステップ 3 削除を完了するには、[OK] をクリックします。

ロケーション

この項の内容は、IM and Presence Service には適用されません。

ここでは、Cisco Unified Serviceability のロケーション機能（[ツール（Tools）] > [ロケーション（Locations）]）について説明します。この機能を使用すると、管理者は企業内の設定済みロケーションの詳細を表示し、リンクおよびロケーション内の不一致を把握し、2 つのロケーション間の有効なパスを確認し、ロケーションの切断されたグループを識別することができます。

ロケーション トポロジ

Cisco Unified Serviceability のロケーション トポロジは、企業で設定されているロケーションの詳細を提供します。ロケーション トポロジとは、ネットワーク内でのメディアのフローを表すモデル化されたトポロジを意味します。

よく用いられる用語とその定義を以下に示します。

アサーション

アサーションとは、クラスタで設定されているロケーション、リンクの帯域幅、および重みの値を意味します。アサートされた値は、別のクラスタに複製することができます。

不一致

不一致は、さまざまなクラスタ間でアサートされたロケーションの帯域幅の値やリンクの帯域幅、重みの値に違いがある場合に発生します。

有効なパス

有効なパスとは、2 つのエンド ロケーションを接続する一連の中間ロケーションであり、隣り合うロケーション間の各リンクには重みが割り当てられます。有効なパスは累積した重みが最も少ないものとして決定され、任意の 2 つのエンド ロケーション間で帯域幅の差し引きに使用される唯一のパスです。

ロケーション トポロジの表示

Cisco Unified Serviceability のロケーション トポロジは、管理者がグラフィカルなロケーション トポロジを表形式で表示する上で役立ちます。管理者は、[検索（Find）] フィルタを使用して必要なロケーションの名前をフィルタリングできます。ロケーショントポロジデータには、選択したロケーションのロケーション内の詳細やリンクの詳細が含まれます。
ここでは、Cisco Unified Serviceability でロケーション トポロジを検索して表示する方法について説明します。

手順

ステップ 1 Cisco Unified Serviceability で、[ツール（Tools）] > [ロケーション（Locations）] > [トポロジ（Topology）] の順に選択します。
[ロケーショントポロジ（Locations Topology）] ウィンドウが表示されます。

ステップ 2 [ロケーション名でロケーションを検索（Find Locations Where Location Name）] ドロップダウンボックスから、フィルタ条件を選択します。

ステップ 3 [ロケーション名でロケーションを検索（Find Locations Where Location Name）] フィールドに検索文字列を入力し、[検索（Find）] をクリックします。
（注） [ロケーション名でロケーションを検索（Find Locations Where Location Name）] フィールドでは、大文字と小文字は区別されません。
選択したフィルタ条件でロケーションのリストが表示されます。

ステップ 4 リスト内で任意のロケーションをクリックして展開し、ロケーション内の詳細とリンクの詳細を表示します。
ロケーション内の詳細には音声、ビデオ、イマーシブ帯域幅が含まれ、リンクの詳細には 2 つのロケーションを接続するリンクの詳細（重み付け、音声、ビデオ、イマーシブ帯域幅など）が含まれます。

ヒント ロケーションのリストが長くなる場合は、複数のページになることがあります。別のページを表示するには、[ロケーショントポロジ（Locations Topology）] ウィンドウの下部にある適切なナビゲーション ボタンをクリックするか、[ページ（Page）] フィールドにページ番号を入力します。ウィンドウに表示されるロケーション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 ボックスから別の値を選択します。

ヒント ロケーションが注意記号で強調表示されている場合は、不一致があることを意味します。この不一致の詳細を表示するには、[アサーションの詳細を表示（View Assertion Details）] リンクをクリックします。

ステップ 5 任意のロケーションのアサーションの詳細を表示するには、展開した詳細セクションの下部にある [アサーションの詳細を表示（View Assertion Details）] リンクをクリックします。
[アサーションの詳細（Assertion Details）] ウィンドウが表示されます。

ステップ 6 [ロケーショントポロジ（Locations Topology）] ウィンドウに戻るには、[閉じる（Close）] をクリックします。

（注） ロケーション トポロジ データを XML 形式でダウンロードするには、[ロケーショントポロジ（Locations Topology）] ウィンドウの下部にある [トポロジのダウンロード（Download Topology）] または上部のツールバーにある [トポロジのダウンロード（Download Topology）] アイコンをクリックします。

XML 形式のトポロジ データの詳細については、『*Cisco Unified Communications Manager XML Developers Guide*』を参照してください。

アサーションの詳細の表示

次のアサーションの詳細を表示するには、Serviceability GUI を使用します。

- ロケーション内設定のアサーション：[クラスタでアサート（Asserted by Cluster）]、[オーディオ（Audio）]、[ビデオ（Video）]、[イマーシブ帯域幅（Immersive bandwidth）] など、ロケーション内のアサーションの詳細が含まれます。[クラスタでアサート（Asserted by Cluster）] カラムには、特定のロケーションをアサートするすべてのクラスタの名前が表示されます。
- リンクのアサーション：[クラスタでアサート（Asserted by Cluster）]、[重み付け（Weight）]、[オーディオ（Audio）]、[ビデオ（Video）]、[イマーシブ帯域幅（Immersive bandwidth）] など、2 つのロケーションを接続するリンクのアサーションの詳細が含まれます。

手順

ステップ 1 [ツール（Tools）] > [ロケーション（Locations）] > [ロケーショントポロジ（Locations Topology）] の順に選択します。

ステップ 2 [ロケーショントポロジ（Locations Topology）] ウィンドウで、[アサーションの詳細を表示（View Assertion Details）] リンクをクリックします。

ロケーションの不一致

[ロケーションの不一致（Locations Discrepancy）] 画面には、さまざまなロケーション設定のアサーションにおける競合が表示されます。

次の詳細情報が表示されます。

- [リンク設定の不一致（Link Configuration Discrepancy）]：重み、音声、ビデオ、イマーシブ帯域幅などの、2 つのロケーションを接続するリンクの不一致の詳細が表示されます。
- [ロケーション内設定の不一致（Intralocation Configuration Discrepancy）]：音声、ビデオ、イマーシブ帯域幅などの、ロケーション内の不一致の詳細が表示されます。

ロケーションの不一致の表示

ここでは、Cisco Unified Serviceability でロケーションの不一致を表示する方法について説明します。

手順

ステップ 1 Cisco Unified Serviceability で、[ツール（Tools）] > [ロケーション（Locations）] > [不一致（Discrepancy）] の順に選択します。
[ロケーションの不一致（Location Discrepancy）] ウィンドウが表示されます。

ステップ 2 リンク設定の不一致とロケーション内設定の不一致のリストが表示されます。
（注） [リンク設定の不一致（Link Configuration Discrepancy）] セクションには、不一致が検出されたリンク名だけが表示されます。リンク名は、*<Location Name 1>* <--> *<Location Name 2>* の形式でリストされます。[ロケーション内設定の不一致（Intralocation Configuration Discrepancy）] セクションには、不一致が検出されたロケーションの名前だけが表示されます。リスト内の要素は辞書順にソートされます。
不一致が検出されなかった場合、次のステータス メッセージが表示されます。

「不一致が見つかりません（`No discrepancies found`）」

ステップ 3 リストで、リンク名またはロケーション名をクリックして展開し、異なるクラスタによってアサートされている設定の詳細を表形式で表示します。
下の行には、音声、ビデオ、イマーシブ帯域幅プールおよび重み付けのために考慮される有効値が表示されます（リンクの場合）。有効値と一致しない値は赤で強調表示されます。

（注） 有効値は、特定のカラムの最小値です。たとえば、音声帯域幅の有効値は [音声帯域幅（Audio Bandwidth）] カラムの最小値です。

有効なパス

Cisco Unified Serviceability の [有効なパス（Effective Path）] 画面には、管理者が指定する 2 つのロケーション間で確立される音声、ビデオ、またはイマーシブ コールにメディアが使用する有効なパスの詳細が表示されます。この画面には、有効なパスの各リンクおよび内部ロケーションで使用可能な帯域幅と設定された帯域幅が表示されます。管理者は、コールの発信で帯域幅の問題が生じた場合に、このレポートを使用してリンクと内部ロケーションでの帯域幅の可用性を判断することができます。また、コールの発信時の帯域幅の問題を修復し、帯域幅の可用性が低い場所を検索するためにも Cisco Unified Serviceability の [有効なパス（Effective Path）] を使用できます。

Cisco Unified Serviceability の [有効なパス（Effective Path）] 画面には、選択した 2 つのロケーション間について次の詳細が表示されます。

- [クイックパスの概要（Quick Path Overview）]：累積的な重みと、有効なパス全体の設定済みおよび使用可能な音声、ビデオ、イマーシブ帯域幅の値の一部が表示されます。

- [詳細パスビュー（Detailed Path View）]：有効なパスを構成するロケーションとリンクに対する音声、ビデオ、イマーシブ コールの重みと帯域幅の値（使用可能および設定済み）が表示されます。発信元のロケーションが上位、宛先のロケーションが下位という順序で表形式で表示されます。

（注） レポートに表示される使用可能な帯域幅の値は、有効なパスを表示した時点での値です。Cisco Unified Real-Time Monitoring Tool ではリアルタイムの値を表示できます。

有効なパスの表示

手順

ステップ 1 Cisco Unified Serviceability で、[ツール（Tools）] > [ロケーション（Locations）] > [有効なパス（Effective Path）] の順に選択します。
[有効なパス（Effective Path）] ウィンドウが表示されます。

ステップ 2 [ロケーション（Locations）] ドロップダウン ボックスから、有効なパスが必要な任意の 2 つのロケーションを選択し、[検索（Find）] をクリックします。
または、入力ボックスにロケーション名を入力し、一致するロケーション名が表示されたら、[検索（Find）] をクリックします。

[クイックパスの概要（Quick Path Overview）] セクションや [詳細パスビュー（Detailed Path View）] セクションなどの有効なパスに関する詳細が表示されます。選択した 2 つのロケーション間にパスが存在しない場合、次のステータス メッセージが表示されます。

「`<From_Location>`と`<To_Location>`の間にパスが存在しません。（`No path exists between <From_Location> and <To_Location>.`）」

切断されたグループ

Cisco Unified Serviceability の [切断されたグループ（Disconnected Groups）] 画面では、管理者がトポロジの一部であるロケーション間の切断を確認し、分析することができます。この画面には切断されたグループのロケーションの一覧が表示され、接続が必要なロケーションを管理者が理解するのに役立ちます。

トポロジ内での切断は、2 つのロケーション間にリンクが設定されていないか、共有ロケーション名のスペルが間違っている場合に発生します。

（注） [切断されたグループ（Disconnected Groups）] 画面には、切断されたロケーションのグループだけが表示され、比較することができます。接続されたロケーションの詳細については、『*Administration Guide for Cisco Unified Communications Manager*』のロケーション設定に関するトピックを参照してください。

切断されたグループの表示

ここでは、Cisco Unified Serviceability で切断されたグループを表示する方法について説明します。

手順

Cisco Unified Serviceability で、[ツール（Tools）] > [ロケーション（Locations）] > [切断されたグループ（Disconnected Groups）] の順に選択します。
[切断されたグループ（Disconnected Groups）] 画面が表示されます。

以下の表に、[切断されたグループ（Disconnected Groups）] 画面に表示される設定の詳細を示します。

表 *48*：*[切断されたグループ（Disconnected Groups）] 画面の設定*

設定	説明
切断されたグループのリスト	
選択（Select）	切断されたグループを選択して別の切断されたグループと比較する場合に、このボックスをオンにします。 **注意** 比較する際はグループを 2 つだけ選択できます。
グループ ID（Group ID）	選択したグループの自動生成された一意の ID 番号が表示されます。
説明（Description）	グループ内の最初と最後のロケーションの名前が（アルファベット順に）表示されます。 （注） 切断されたグループに 1 つのノードだけが存在する場合、そのノードの名前だけがここに表示されます。
ロケーションの数（No of Locations）	グループ内のロケーションの数が表示されます。

設定	説明
選択したグループの比較（Compare Selected Groups）	選択したグループを表示および比較するには、このボタンをクリックします。このボタンをクリックすると、選択したグループに関する詳細が表示されます。 選択したすべてのグループについて、そのグループに含まれるロケーションの名前と、ロケーションをアサートする対応するクラスタが表示されます。次の「選択したグループの比較ビュー」を参照してください。
選択したグループの比較ビュー	
ロケーション名（Location Name）	グループに含まれているすべてのロケーションの名前がこのカラムに表示されます。
クラスタでアサート（Asserted by Cluster）	特定のロケーションをアサートするすべてのクラスタの名前がこのカラムに表示されます。

切断されたグループにロケーションが存在しない場合、次のステータス メッセージが表示されます。

「切断されたグループのロケーションが見つかりません（`No disconnected groups of locations found`）」

（注） 切断されたグループのリストは、どのカラムでもソートできます。デフォルトでは、グループは [ロケーションの数（No of Locations）] カラムでソートされます。

第 7 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、ユーザが行った、またはユーザ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。

  次に、アラームを送信するために Cisco Unified Communications Manager のコンポーネントが使用できる 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。（Cisco 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

Cisco Unified Communications Managerの標準イベント 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

Cisco Unified Communications Manager Administration のさまざまなコンポーネントについて、次のイベントが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 Cisco Unified Communications Manager サーバの追加または削除）

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（Cisco 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

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

Cisco Unified Communications Manager IM and Presence Administration のさまざまなコンポーネントについて、次のイベントがログに記録されます。

- 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 IM and Presence サーバの追加または削除）

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 ユーザのログイン（ユーザのログイン/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。

監査ログ タイプ

システム監査ログ

システム監査ログでは、Linux OS ユーザの作成、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、ユーザによる、またはユーザ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, （162 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, （162 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 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の設定, （163 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, （163 ページ）	これはオプションです。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。。

監査ロギングのセットアップ

はじめる前に

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 [サーバ名（Server Name）] フィールドに、リモート syslog サーバの 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。

次の作業

リモート監査ログの転送プロトコルの設定, （162 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、TCP 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。

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 Cisco Unified Communications Manager と IM and Presence サービスのクラスタ ノードでこの手順を繰り返します。

次の作業

アラート通知用の電子メール サーバの設定, （163 ページ）

アラート通知用の電子メール サーバの設定

アラート通知用の電子メール サーバ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 サーバ設定（Mail Server Configuration）] ポップアップで、メール サーバの詳細を入力します。

ステップ 4 [OK] をクリックします。

次の作業

電子メール アラートの有効化, （163 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 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、**TCPRemoteSyslogDeliveryFailed** 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。

監査ログの構成時の設定

はじめる前に

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。Cisco Cisco Unified Communications Manager の場合、デフォルトでは、新規インストールまたはアップグレードの後で、CCMAdministrator に監査ロールが与えられます。CCMAdministrator は、Cisco Cisco Unified Communications Manager Administration の [ユーザグループ設定（User Group Configuration）] ウィンドウで標準監査ユーザ グループに監査権限を持つユーザ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を標準監査ユーザ 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 Cisco Unified Communications Manager のロール、ユーザ、ユーザ グループの詳細については、『*Administration Guide for Cisco Unified Communications Manager*』を参照してください。

Cisco Unity Connection のロールとユーザの詳細については、『*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 グループの詳細については、『*Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager*』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 *49*：監査ログの構成時の設定

フィールド	説明
サーバの選択	
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。 Cisco Cisco Unified Communications Manager の場合、アプリケーションの監査ログは Cisco Cisco Unified Communications Manager Administration、Cisco Unified RTMT、Cisco Cisco Unified Communications Manager CDR Analysis and Reporting、Cisco Unified Serviceability などの Cisco Cisco Unified Communications Manager ユーザ インターフェイスの設定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 Cisco Unified Communications Manager IM and Presence Administration、Cisco Unified IM and Presence Real-Time Monitoring Tool、Cisco Unified IM and Presence Serviceability などの IM and Presence ユーザ 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 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。Cisco Cisco 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ないため、Cisco Cisco Unified Communications Manager ノードを宛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 ～ 10 MB 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 Cisco Cisco Unified Communications Manager および Cisco Unity Connection データベースに対して作成されます。[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（Administrative Tasks）] : Cisco Cisco Unified Communications Manager システムのすべての管理上の変更（たとえば、システムを維持するための変更）、および [スキーマ（Schema）] のすべての変更を追跡します。 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（Database Reads）] : システムのすべての読み取りと、[スキーマ（Schema）]、[管理タスク（Administrative Tasks）]、および [データベースの更新（Database Updates）] のすべての変更を追跡します。 ヒント　Cisco Cisco Unified Communications Manager、IM and Presence Service、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（Database Reads）] 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。

フィールド	説明
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。
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 8 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。

（注） 任意の SFTP サーバ製品を使用できますが、Cisco Technology Developer Partner Program（CTDP）を介してシスコが認定する SFTP 製品を使用することをシスコでは推奨します。CTDP パートナー（GlobalSCAPE など）は、特定のバージョンの Cisco Unified Communications Manager で自社製品を認定しています。ご使用のバージョンの Cisco Unified Communications Manager と自社製品の互換性を保証しているベンダーについては、次の URL を参照してください。

http://www.cisco.com/pcgi-bin/ctdp/Search.pl

サポートされている Cisco Unified Communications バージョンで GlobalSCAPE を使用する方法の詳細については、次の URL を参照してください。

http://www.globalscape.com/gsftps/cisco.aspx

シスコでは社内テストに次のサーバを使用しています。いずれかのサーバを使用できますが、サポートについては各ベンダーにお問い合わせください。

- Open SSH（http://sshwindows.sourceforge.net/）
- Cygwin（http://www.cygwin.com/）
- Titan（http://www.titanftp.com/）

CTDP プロセスでまだ認定されていないサードパーティ製品で問題が発生した場合、サポートについてはそのサードパーティ ベンダーに問い合わせてください。

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 Cisco Unified Communications Manager 4.X で指定した SNMP 設定パラメータは、Cisco 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。

CISCO-CCM-MIB には IPv6 アドレス、プリファレンスなどのカラムとストレージが含まれますが、SNMP は IPv4 をサポートしています。

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 要求に関連する認証、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。

  Cisco Unified Communications Manager サブエージェントは、ローカルの Cisco Unified Communications Manager とのみ対話します。Cisco 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 Cisco 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

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。

- Cisco Unified Communications Manager では CISCO-UNITY-MIB はサポートされません。
- 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に常駐し、サーバ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 *50*：***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。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)。この値は、このアプリケーションインスタンスの実行要素の評価（sysApplElmRunState を参照）および sysApplInstallElmtRole で定義されたロールに基づきます。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。

- system
- interfaces
- at
- ip
- icmp
- tcp
- udp
- snmp

表 *51*：*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 *52* : ***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施されているかを確認するのに便利です。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 *53*：*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	syslog のどの重大度レベルを処理するかを示します。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、Cisco Unified Communications Manager と、それに関連する電話やゲートウェイなどの Cisco Unified Communications Manager ノードで確認でき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（静的な）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。

CISCO-CCM-MIB には IPv6 アドレス、プリファレンスなどのカラムとストレージが含まれますが、SNMP は IPv4 をサポートしています。

（注） Cisco Unified Communications Manager は Cisco Unified Communications Manager システムでこの 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

廃止オブジェクトも含めて Cisco Unified Communications Manager 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（Cisco Unified Communications Manager クラスタ構成の場合はローカルの Cisco CallManager サービス）が起動され、実行中の場合にのみ入力されます。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 *54*：*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 Cisco 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、ローカル Cisco Unified Communications Manager が認識するクラスタ内のすべての Cisco 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 Cisco Unified Communications Manager がダウンした場合は、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 Phone の場合、ccmPhoneTable の登録済み電話の数は、Cisco 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 Phone 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、Cisco Unified Communications Manager MIB の ccmRegisteredCTIDevices、ccmUnregisteredCTIDevices、ccmRejectedCTIDevices の各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、Cisco Unified Communications Manager（クラスタ構成の場合はローカル Cisco Unified Communications Manager）に情報が含まれる H.323 デバイスのリストが格納されます。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、Cisco Unified Communications Manager には登録されません。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、Cisco 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。

テーブル	コンテンツ
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き、Cisco Unified Communications Manager MIB の ccmRegisteredVoiceMailDevices、ccmUnregisteredVoiceMailDevices、ccmRejectedVoiceMailDevices の各カウンタが更新されます。
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。 Cisco 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 Cisco Unified Communications Manager へ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、Cisco Unified Communications Manager クラスタの Cisco Unified Communications Manager グループが格納されます。
ccmGroupMapping	このテーブルは、クラスタのすべての Cisco Unified Communications Manager を Cisco Unified Communications Manager グループにマッピングします。ローカル Cisco Unified Communications Manager ノードがダウンしている場合、このテーブルは空のままになります。

表 *55*：*CISCO-CCM-MIB* の静的テーブル

テーブル	目次
ccmProductType	このテーブルには、Cisco Unified Communications Manager（Cisco Unified Communications Manager クラスタ構成の場合はクラスタ）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、ボイス 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、Cisco Unified Communications Manager クラスタの地理的リージョン ペアのリストが格納されます。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、Cisco Unified Communications Manager 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格納されます。
ccmDevicePool	このテーブルには、Cisco Unified Communications Manager クラスタ内のすべてのデバイス プールのリストが格納されます。デバイス プールは、リージョン、日付/時刻グループ、Cisco 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。Cisco Unified Communications Manager および IM and Presence Service ではこの 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 *56*：***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 のセットアップ

SNMP を設定する手順の概要を次に示します。

はじめる前に

10 個を超える同時ポーリング クエリーは許可されません。推奨する最大トラップ宛先は 8 個です。それ以上はCPUの性能に影響します。この要件は、使用するOVAテンプレートに関係なく、すべてのインストールに適用されます。

手順

ステップ 1 SNMP NMS をインストールし、設定します。

ステップ 2 [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、SNMP サービスが起動されたことを確認します。

ステップ 3 Unified Communications Manager：[サービスの開始（Service Activation）] ウィンドウで、Cisco CallManager SNMP サービスをアクティブ化します。Cisco Unity Connection のみ：自動的に Connection SNMP Agent サービスがアクティブになります。

ステップ 4 SNMP V1/V2c を使用している場合は、コミュニティ ストリングを設定します。

ステップ 5 SNMP V3 を使用している場合は、SNMP ユーザを設定します。

ステップ 6 トラップまたはインフォームの通知先を設定します。

ステップ 7 MIB2 システム グループのシステム コンタクトとロケーションを設定します。

ステップ 8 CISCO-SYSLOG-MIB のトラップ設定を行います。

ステップ 9 Unified Communications Manager のみ：CISCO-CCM-MIB のトラップ設定を行います。

ステップ 10 マスター エージェント サービスをリスタートします。

ステップ 11 NMS で、Cisco Unified Communications Manager のトラップ パラメータを設定します。

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。

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 *57*：*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（Community String）]
V3 コミュニティ ストリング	[SNMP] > [V3] > [ユーザ（User）]
MIB2 のシステム コンタクトおよびロケーション	[SNMP] > [システム グループ（SystemGroup）] > [MIB2 システム グループ（MIB2 System Group）]
トラップ通知先（V1/V2c）	[SNMP] > [V1/V2c] > [通知先（Notification Destination）]
トラップ通知先（V3）	[SNMP] > [V3] > [通知先（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 が要求を発行し、管理対象デバイスから応答が返されます。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 から応答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（要求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（要求された操作がユーザ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（要求されたオブジェクトにユーザ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。

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 ユーザを使用します。

Serviceability GUI では、[V3の設定（V3 Configuration）] ウィンドウで SNMP v3 の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 *58*：*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。

MIB	サービス	ウィンドウ
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 Unified IM 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 Cisco 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。

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 ユーザを使用します。SNMP ユーザ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） Cisco Unified Communications Manager は、Cisco 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ています。

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。

次に、設定済みのトラップ通知先に送信される、Cisco Unified Communications Manager の SNMP のトラップおよびインフォーム メッセージを示します。

- Cisco Unified Communications Managerで障害が発生しました（Cisco Unified Communications Manager failed）
- 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 59：*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 Administration では Cisco ATA 186 デバイスを電話機として設定できますが、Cisco Unified Communications Manager が SNMP トラップを Cisco ATA デバイスに送信するときには、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。
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。

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
ccmQualityReportAlarmEnable	True	このトラップは、Cisco Extended Functions サービスがサーバ上、または、クラスタ設定の場合には（Cisco Unified Communications Manager のみ）ローカル Cisco Unified Communications Manager サーバ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	Warning	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。

関連トピック

CISCO-CCM-MIB トラップ パラメータ，（223 ページ）
CISCO-SYSLOG-MIB トラップ パラメータ，（222 ページ）

SNMP トレースの設定

Cisco 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（Trace Configuration）] 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（Performance and Monitoring Services）] サービス グループの [Cisco CallManager SNMPサービス（Cisco CallManager SNMP Service）] 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 V1 および V2c の設定

ここでは、SNMP V1/V2c の SNMP 管理対象デバイスを設定する方法について説明します。

コミュニティ ストリングの検索

コミュニティ ストリングを検索するには、次の手順を実行します。

はじめる前に

SNMP をセットアップするための手順の概要のタスクを確認します。

手順

ステップ 1 [Snmp] > [V1/V2c] > [コミュニティ ストリング（Community String）] を選択します。

ステップ 2 [次の名前のコミュニティストリングを検索（Find Community Strings where Name）] リスト ボックスから、コミュニティ ストリングに対して使用する検索条件を選択します。

ステップ 3 検索するコミュニティ ストリングを入力します。

ステップ 4 コミュニティ ストリングが存在するサーバのホスト名または IP アドレスを、[サーバ（Server）] リスト ボックスから選択します。

ステップ 5 [検索（Find）] を選択します。

ステップ 6 （任意） 検索結果のいずれかのオプションの設定をクラスタのすべてのノードに適用するには、そのオプションの名前の隣にあるチェックボックスをオンにし、[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。
この手順は、Unified Communications Manager および IM and Presence Service のクラスタにのみ適用されます。

ステップ 7 結果のリストから表示するコミュニティ ストリングを選択します。

ヒント [新規追加（Add New）] ボタンは、[検索（Find）] ボタンを選択するまで [SNMP コミュニティ ストリング設定（SNMP Community String Configuration）] ウィンドウに表示されません。コミュニティ ストリングが存在せず、コミュニティ ストリングを追加する場合は、[検索（Find）] ボタンを選択し、ウィンドウが更新されるのを待ちます。[新規追加（Add New）] ボタンが表示されます。

ステップ 8 結果のリストから、表示するコミュニティ ストリングをクリックします。

コミュニティ ストリングのセットアップ

SNMP エージェントはコミュニティ ストリングを使用してセキュリティを提供するため、SNMP 管理対象デバイスのシステムで管理情報ベース（MIB）にアクセスするには、コミュニティ ストリングを設定する必要があります。SNMP 管理対象デバイスのシステムへのアクセスを制限する

には、コミュニティストリングを変更します。コミュニティストリングを追加、変更、削除するには、[SNMP コミュニティ ストリング設定（SNMP Community String Configuration）] ウィンドウにアクセスします。

手順

ステップ 1 [Snmp] > [V1/V2c] > [コミュニティ ストリング（Community String）] を選択します。

ステップ 2 [サーバ（Server）] リスト ボックスで必要なサーバを選択し、[検索（Find）] を選択します。

ステップ 3 次のいずれかの作業を実行します。

- 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。

  ヒント [新規追加（Add New）] ボタンは、[検索（Find）] ボタンを選択するまで [SNMP コミュニティ ストリング設定（SNMP Community String Configuration）] ウィンドウに表示されません。コミュニティ ストリングが存在せず、コミュニティ ストリングを追加する場合は、[検索（Find）] ボタンを選択し、ウィンドウが更新されるのを待ちます。[新規追加（Add New）] ボタンが表示されます。

- 既存のコミュニティ ストリングを変更するには、結果リストで、編集するコミュニティ ストリングの名前をクリックします。

  コミュニティ ストリングまたはサーバの名前は変更できません。

ステップ 4 コミュニティ ストリングの構成時の設定を入力します。

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 5 設定が完了したら、新しいコミュニティ ストリングを保存する場合は [新規追加（Add New）] をクリックし、既存のコミュニティ ストリングへの変更を保存する場合は [保存（Save）] をクリックします。

SNMP マスター エージェントをリスタートするまで変更内容が有効にならないことを示すメッセージが表示されます。

ステップ 6 次のいずれかの操作を実行します。

- [OK] を選択して SNMP マスター エージェント サービスを再起動し、変更を有効にします。
- [キャンセル（Cancel）] を選択し、SNMP マスター エージェントをリスタートせずに設定を続行します。

  （注） SNMP の設定をすべて終えてから SNMP マスター エージェント サービスをリスタートすることを推奨します。

  システムが更新され、[SNMP コミュニティ ストリング設定（SNMP Community String Configuration）] ウィンドウが表示されます。作成したコミュニティ ストリングがウィンドウに表示されます。

関連トピック

コミュニティ ストリングの構成時の設定, （200 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, （113 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 *60*：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。
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）	指定したホストからのみ SNMP 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。 **ヒント** [ホスト IP アドレス（Host IP Address）] フィールドに、パケットを受け入れるホストを入力し、[挿入（Insert）] をクリックします。パケットを受け入れるホストごとにこの手順を繰り返します。ホストを削除するには、そのホストを [ホスト IP アドレス（Host IP Address）] 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。 なし（**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、Cisco Unified Communications Manager および IM and Presence Service のクラスタにのみ適用されます。

関連トピック

コミュニティ ストリングの検索, （198 ページ）

コミュニティ ストリングの削除

コミュニティ ストリングを削除するには、次の手順を実行します。

手順

ステップ 1 コミュニティ ストリングを探します。

ステップ 2 一致するレコードのリストから削除するコミュニティ ストリングをオンにします。

ステップ 3 [選択項目の削除（Delete Selected）] を選択します。このコミュニティ ストリングに関連する通知エントリが削除されることを示すメッセージが表示されます。

ステップ 4 削除を続行するには、[OK] を選択します。SNMP マスターエージェントをリスタートするまで変更内容が有効にならないことを示すメッセージが表示されます。

ステップ 5 次のいずれかの操作を実行します。

- [キャンセル（Cancel）] を選択し、SNMP マスター エージェントをリスタートせずに設定を続行します。
- [OK] を選択して SNMP マスター エージェント サービスをリスタートします。

ヒント SNMP の設定をすべて終えてから SNMP マスター エージェント サービスをリスタートすることを推奨します。

関連トピック

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, （113 ページ）

SNMP V1 および V2c 通知先の検索

V1/V2c の通知先を検索するには、次の手順を実行します。

手順

ステップ 1 [Snmp] > [V1/V2c] > [通知先（Notification Destination）] を選択します。
[検索/リスト（Find/List）] ウィンドウが表示されます。

ステップ 2 [通知先 IP の検索（Find Notification where Destination IP）] ドロップダウン リスト ボックスから、通知先を検索するために使用する検索条件を選択します。

ステップ 3 検索する通知先を入力します。

ステップ 4 通知先をサポートするサーバのホスト名または IP アドレスを [サーバ（Server）] リスト ボックスに入力し、[検索（Find）] をクリックします。
[検索（Find）] をクリックすると、[新規追加（Add New）] ボタンが表示されます。検索結果が表示された後、[すべてのノードに適用（Apply to All Nodes）] チェックボックスが表示されます。

ステップ 5 （任意） 次の 1 つまたは複数の操作を実行します。

- 検索結果のいずれかのオプションの設定をクラスタのすべてのノードに適用するには、そのオプションの名前のチェックボックスをオンにし、[すべてのノードに適用（Apply to All Nodes）] をオンにします。

  この手順は、Cisco Unified Communications Manager および IM and Presence Service クラスタにのみ適用されます。

- 項目の設定を表示するには、検索結果のその項目を選択します。

  （注） [新規追加（Add New）] ボタンは、[検索（Find）] ボタンを選択するまで [SNMP 通知先設定（Notification Destination Configuration）] ウィンドウに表示されません。通知先が存在せず、通知先を追加する場合は、[検索（Find）] を選択し、ウィンドウが更新されるのを待ちます。[新規追加（Add New）] ボタンが表示されます。

SNMP V1 および V2c の通知先の設定

V1/V2c の通知先（トラップまたはインフォームの受信者）を設定するには、次の手順を実行します。

手順

ステップ 1 [Snmp] > [V1/V2c] > [通知先（Notification Destination）] を選択します。

ステップ 2 [サーバ（Server）] リスト ボックスで必要なサーバを選択し、[検索（Find）] を選択します。

ステップ 3 次のいずれかの作業を実行します。

- 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。

  [検索/リスト（Find/List）] ウィンドウの [サーバ（Server）] ドロップダウン リスト ボックスで選択したサーバの通知先を設定します。

  （注） [新規追加（Add New）] ボタンは、[検索（Find）] ボタンを選択するまで [SNMP 通知先設定（Notification Destination Configuration）] ウィンドウに表示されません。通知先がなく、通知先を追加する場合は、[検索（Find）] を選択し、ウィンドウが更新されるのを待ちます。[新規追加（Add New）] ボタンが表示されます。

- 既存の SNMP 通知先を変更するには、編集する通知先を検索し、[検索/リスト（Find/List）] ウィンドウの結果リストで SNMP 通知先の名前をクリックします。

ステップ 4 通知先の設定を入力します。

ヒント 設定を保存する前であれば、[クリア（Clear）] 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 5 次のいずれかの操作を実行します。

- [挿入（Insert）] を選択して通知先を保存します。
- [保存（Save）] を選択して既存の通知先に対する変更を保存します。SNMP マスター エージェントをリスタートするまで変更内容が有効にならないことを示すメッセージが表示されます。

ステップ 6 [OK] を選択して SNMP マスター エージェントを再起動するか、または [キャンセル（Cancel）] を選択して SNMP マスター エージェントを再起動せずに設定を続行します。

（注） SNMP の設定を終えてから SNMP マスター エージェント サービスをリスタートすることを推奨します。

関連トピック

SNMP V1 および V2c 通知先の検索, （202 ページ）
SNMP V1 および V2c の通知先の設定, （204 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, （113 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 *61*：*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 IP アドレス（Host IP 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 IP 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、トラップ通知先の IP 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。

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	[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。

関連トピック

コミュニティ ストリングの検索, （198 ページ）
SNMP V1 および V2c 通知先の検索, （202 ページ）
コミュニティ ストリングのセットアップ, （198 ページ）
SNMP V1 および V2c の通知先の設定, （203 ページ）

SNMP V1 および V2c 通知先の削除

SNMP V1/V2c の通知先を削除するには、次の手順を実行します。

手順

ステップ 1 削除する通知先を検索します。

ステップ 2 [検索/リスト（Find/List）] ウィンドウの一致するレコードのリストから、削除する通知先の隣にあるチェックボックスをオンにします。

ステップ 3 [選択項目の削除（Delete Selected] をクリックします。通知先エントリを削除するかどうか確認するメッセージが表示されます。

ステップ 4 削除を続行するには、[OK] をクリックします。SNMP マスターエージェントをリスタートするまで変更内容が有効にならないことを示すメッセージが表示されます。

ステップ 5 次のいずれかを実行します。

- SNMP マスター エージェント サービスを再起動するには、[OK] をクリックします。
- SNMP マスター エージェントを再起動せずに設定を続行するには、[キャンセル（Cancel）] をクリックします。

ヒント SNMP の設定をすべて終えてから SNMP マスター エージェント サービスをリスタートすることを推奨します。

ウィンドウが更新されると、削除した通知先が結果に表示されなくなっています。

関連トピック

SNMP V1 および V2c 通知先の検索, （202 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, （113 ページ）

SNMP V3 の設定

ここでは、SNMP V3 の SNMP 管理対象デバイスを設定する方法について説明します。

SNMP V3 ユーザの検索

ヒント [新規追加（Add New）] ボタンは、[検索（Find）] ボタンをクリックするまで [SNMP ユーザ設定（SNMP User Configuration）] ウィンドウに表示されません。ユーザが存在せず、ユーザを追加する場合は、[検索（Find）] ボタンをクリックし、ウィンドウが更新されるのを待ちます。[新規追加（Add New）] ボタンが表示されます。

SNMP ユーザを検索するには、次の手順を実行します。

手順

ステップ 1 [Snmp] > [V3] > [ユーザ（User）] を選択します。

ステップ 2 ユーザを検索するために使用する検索条件（たとえば [が次の文字列で始まる（begins with）]）を選択します。

ステップ 3 検索するユーザ名を入力します。

ステップ 4 ユーザにアクセスするサーバのホスト名または IP アドレスを、[サーバ（Server）] リスト ボックスから選択し、[検索（Find）] をクリックします。

ステップ 5 （任意） 検索結果のいずれかのオプションの設定をクラスタのすべてのノードに適用するには、そのオプションの名前の隣にあるチェックボックスをオンにし、[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。
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。

ステップ 6 結果のリストから表示するユーザを選択します。

SNMP V3 ユーザの設定

SNMP V3 のユーザを設定するには、次の手順を実行します。

手順

ステップ 1 [Snmp] > [V3] > [ユーザ（User）] を選択し、設定する SNMP V3 のユーザを見つけます。
詳細については、SNMP V3 のユーザを検索する手順を参照してください。

ステップ 2 次のいずれかの作業を実行します。

- 新しい SNMP ユーザを追加するには、SNMP ユーザ設定の [検索/リスト（Find/List）] ウィンドウの [新規追加（Add New）] ボタンをクリックします。

- IM and Presence のみ：新しい SNMP ユーザを追加するには、[Snmp] > [V3] > [ユーザ（User）] > [新規追加（Add New）] を選択します。

  （注） [新規追加（Add New）] ボタンは、[検索（Find）] ボタンを選択するまで [SNMP ユーザ設定（SNMP User Configuration）] ウィンドウに表示されません。ユーザが存在せず、ユーザを追加する場合は、[検索（Find）]ボタンを選択し、ウィンドウが更新されるのを待ちます。[新規追加（Add New）] ボタンが表示されます。

- 既存の SNMP ユーザを変更するには、SNMP ユーザ設定の [検索/リスト（Find/List）] ウィンドウでユーザを検索し、検索結果のリストから変更する SNMP ユーザの名前をクリックします。

ステップ 3 SNMP V3 ユーザの設定を入力します。

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 4 新しいユーザを追加するには、[挿入（Insert）] をクリックするか、[保存（Save）] をクリックして既存のユーザに対する変更を保存します。
SNMP マスター エージェントをリスタートするまで変更内容が有効にならないことを示すメッセージが表示されます。

ステップ 5 次のいずれかを実行します。

- SNMP マスター エージェント サービスを再起動するには、[OK] をクリックします。
- SNMP マスター エージェントを再起動せずに設定を続行するには、[キャンセル（Cancel）] をクリックします。

ヒント SNMP の設定を終えてから SNMP マスター エージェント サービスをリスタートすることを推奨します。

（注） 設定したユーザが存在するこのサーバにアクセスするには、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を設定してください。

関連トピック

SNMP V3 ユーザの検索, （207 ページ）
SNMP V3 のユーザ構成時の設定, （208 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, （113 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 *62* : ***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を変更するには、SNMPユーザの検索手順を実行します。
ユーザ名（User Name）	このフィールドには、アクセスを提供するユーザ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を入力します。 既存の SNMP ユーザの場合、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。
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 IP アドレス（Host IP Address）] フィールドに、SNMP パケットを受け入れるホストを入力し、[挿入（Insert）] をクリックします。SNMP パケットを受け入れるホストごとにこの手順を繰り返します。ホストを削除するには、そのホストを [ホスト IP アドレス（Host IP Address）] ペインから選択し、[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。 なし（**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 権限でユーザを設定します。
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、Cisco Unified Communications Manager および IM and Presence Service クラスタにのみ適用されます。

関連トピック

SNMP V3 ユーザの検索, （207 ページ）

SNMP V3 ユーザの削除

SNMP のユーザを削除するには、次の手順を実行します。

手順

ステップ 1 [Snmp] > [V3] > [ユーザ（User）] を選択し、削除する SNMP V3 ユーザを検索します。
詳細については、SNMP V3 のユーザを検索する手順を参照してください。

ステップ 2 一致するレコードのリストから、削除するユーザの隣にあるチェックボックスをオンにします。

ステップ 3 [選択項目の削除（Delete Selected）] をクリックします。
このユーザに関連する通知エントリが削除されることを示すメッセージが表示されます。

ステップ 4 削除を続行するには、[OK] をクリックします。
SNMP マスター エージェントをリスタートするまで変更内容が有効にならないことを示すメッセージが表示されます。

ステップ 5 次のいずれかの操作を実行します。

- [OK] を選択して SNMP マスター エージェント サービスをリスタートします。
- [キャンセル（Cancel）] を選択し、SNMP マスター エージェントをリスタートせずに設定を続行します。

SNMP の設定をすべて終えてから SNMP マスター エージェント サービスをリスタートすることを推奨します。

ウィンドウが更新されると、削除したユーザが結果に表示されなくなっています。

関連トピック

SNMP V3 ユーザの検索, （207 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, （113 ページ）

SNMP V3 通知先の検索

ヒント [新規追加（Add New）] ボタンは、[検索（Find）] ボタンをクリックするまで [SNMP 通知先設定（Notification Destination Configuration）] ウィンドウに表示されません。ユーザが存在せず、ユーザを追加する場合は、[検索（Find）] ボタンをクリックし、ウィンドウが更新されるのを待ちます。[新規追加（Add New）] ボタンが表示されます。

V3 の通知先を検索するには、次の手順を実行します。

手順

ステップ 1 [Snmp] > [V3] > [通知先（Notification Destination）] を選択します。

ステップ 2 [通知先 IP の検索（Find Notification where Destination IP）] ドロップダウン リスト ボックスから、通知先を検索するために使用する検索条件（たとえば [が次の文字列で始まる（begins with）]）を選択します。

ステップ 3 検索する通知先の IP アドレスまたはホスト名を入力します。

ステップ 4 [サーバ（Server）] フィールドに、通知先をサポートするサーバのホスト名または IP アドレスを選択し、[検索（Find）] をクリックします。
[検索（Find）] をクリックすると、[新規追加（Add New）] ボタンが表示されます。検索結果が表示された後、[すべてのノードに適用（Apply to All Nodes）] チェックボックスが表示されます。

ステップ 5 （任意） 検索結果のいずれかのオプションの設定をクラスタのすべてのノードに適用するには、そのオプションの名前の隣にあるチェックボックスをオンにし、[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。
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。

ステップ 6 結果のリストから表示する通知先を選択します。

SNMP V3 の通知先の設定

トラップまたはインフォームの受信者を設定するには、次の手順を実行します。

手順

ステップ 1 [Snmp] > [V3] > [通知先（Notification Destination）] の順に選択し、設定する SNMP V3 の通知先を検索します。
詳細については、SNMP V3 の通知先を検索する手順を参照してください。

ステップ 2 次のいずれかの作業を実行します。

- 新しい SNMP 通知先を追加するには、検索結果ウィンドウの [新規追加（Add New）] ボタンをクリックします。
- 既存の SNMP 通知先を変更するには、検索結果ウィンドウで、編集する SNMP 通知先の名前をクリックします。

ステップ 3 SNMP V3 通知先の構成時の設定を行います。
ヒント 設定を保存する前であれば、[クリア（Clear）] 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 4 通知先を保存するには、次のいずれかの操作を実行します。

- [挿入（Insert）] を選択して通知先を追加します。
- [保存（Save）] を選択して既存の通知先に対する変更を保存します。

SNMP マスター エージェントをリスタートするまで変更内容が有効にならないことを示すメッセージが表示されます。

ステップ 5 次のいずれかの操作を実行します。

- SNMP マスター エージェント サービスを再起動するには、[OK] をクリックします。
- SNMP マスター エージェントを再起動せずに設定を続行するには、[キャンセル（Cancel）] をクリックします。

ヒント SNMP の設定を終えてから SNMP マスター エージェント サービスをリスタートすることを推奨します。

関連トピック

SNMP V3 ユーザの検索, （207 ページ）
SNMP V3 のユーザ構成時の設定, （208 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, （113 ページ）

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 *63*：*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、別のサーバを選択します。
ホスト IP アドレス（Host IP Addresses）	ドロップダウン リスト ボックスからホストの IP アドレスを選択するか、[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、ホストの IP アドレスを入力します。
ポート番号（Port Number）	フィールドに、宛先サーバ上の通知を受け取るポート番号を入力します。

フィールド	説明
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。
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** 新しいユーザを作成するには、[新規ユーザの作成（Create New User）] をクリックします。 **2** 既存のユーザを変更するには、ユーザのオプション ボタンをクリックしてから、[選択したユーザの更新（Update Selected User）] をクリックします。 **3** ユーザを削除するには、ユーザのオプション ボタンをクリックしてから、[選択したユーザの削除（Delete Selected User）] をクリックします。 表示されるユーザは、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。

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。

関連トピック

SNMP V3 ユーザの検索, （207 ページ）

SNMP V3 通知先の削除

SNMP V3 通知先を削除するには、次の手順を実行します。

手順

ステップ 1 [Snmp] > [V3] > [通知先（Notification Destination）] を選択し、削除する通知先を検索します。詳細については、SNMP V3 の通知先を検索する手順を参照してください。

ステップ 2 一致するレコードのリストから、削除する通知先の隣にあるチェックボックスをオンにします。

ステップ 3 [選択項目の削除（Delete Selected）] を選択します。通知先を削除するかどうかを確認するメッセージが表示されます。

ステップ 4 削除を続行するには、[OK] を選択します。SNMP マスターエージェントをリスタートするまで変更内容が有効にならないことを示すメッセージが表示されます。

ステップ 5 次のいずれかの操作を実行します。

- [OK] を選択して SNMP マスター エージェント サービスをリスタートします。
- [キャンセル（Cancel）] を選択し、SNMP マスター エージェントをリスタートせずに設定を続行します。

（注） SNMP の設定を終えてから SNMP マスター エージェント サービスをリスタートすることを推奨します。

関連トピック

SNMP V3 通知先の検索, （211 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, （113 ページ）

MIB2 システム グループ

SNMP MIB-II システム グループのシステム コンタクト オブジェクトとシステム ロケーション オブジェクトを設定するには、Serviceability GUI を使用します。たとえば、システム コンタクトとして Administrator, 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 と入力できます。

MIB2 システム グループのセットアップ

MIB-II システム グループのシステム コンタクトとシステム ロケーションを設定するには、次の手順を実行します。

ヒント　この手順では、SNMP v1、v2c、および v3 の構成がサポートされます。

手順

ステップ 1　[Snmp] > [システム グループ（SystemGroup）] > [MIB2 システム グループ（MIB2 System Group）] を選択します。

ステップ 2　SNMP MIB2 システム グループの設定を構成します。

ステップ 3　[保存（Save）] をクリックします。SNMP マスター エージェントをリスタートするまで変更内容が有効にならないことを示すメッセージが表示されます。

ステップ 4　[OK] を選択して SNMP マスター エージェント サービスを再起動するか、または [キャンセル（Cancel）] を選択して SNMP マスター エージェントを再起動せずに設定を続行します。

ステップ 5　次のいずれかの操作を実行します。

- [すべてクリア（Clear All）] を選択し、[システム コンタクト（System Contact）] フィールドと [システム ロケーション（System Location）] フィールドをクリアします。
- [すべてクリア（Clear All）]、[保存（Save）] の順に選択して、システム設定を削除します。

関連トピック

MIB2 システム グループの設定, （216 ページ）

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 *64* : *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、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 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 トラップのセットアップ

SNMP トラップ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 Serviceability にログインし、次の手順を実行して Cisco CallManager SNMP サービスと SNMP Master Agent がアクティブ化され実行されていることを確認します。

a) [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、Cisco CallManager SNMP サービスが開始されていることを確認します。

b) [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、SNMP Master Agent が開始されていることを確認します。

ステップ 2 SNMP V1 または V2 を実行する場合は、次の手順を実行してコミュニティ ストリングと通知先がセットアップされていることを確認してください。

a) コミュニティ ストリングのセットアップ手順に従い、アクセス権限が ReadWriteNotify、NotifyOnly、ReadNotify のいずれかに設定されていることを確認します。

b) 通知先のセットアップ手順に従ってください。

ステップ 3 SNMP V3 を実行する場合は、次の手順を実行してユーザと通知先がセットアップされていることを確認してください。

a) SNMP ユーザのセットアップ手順に従い、アクセス権限が ReadWriteNotify、NotifyOnly、ReadNotify のいずれかに設定されていることを確認します。

b) 通知先のセットアップ手順に従ってください。

ステップ 4 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 5 「SNMP トラップの生成」の記述に従い、特定の SNMP トラップを生成します（ccmPhoneFailed または MediaResourceListExhausted トラップなど）。

ステップ 6 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 7 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 トラップのセットアップ，（217 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 *65* : ***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 Cisco Unified Communications Manager Administration にログインします。 **3** 使用中で Cisco Unified Communications Manager に登録されている電話の場合は、電話をリセットします。 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 Administration 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 Administration で、電話を再登録します。 **4** TFTP サーバ A を指すように電話を設定し、別のサーバに電話をつなぎます。
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 Administration 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 Administration 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 Administration 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（Phone Configuration）] ウィンドウで、[メディアリソースグループリスト（Media Resource Group List）] フィールドを作成したメディア 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	ccmCallManagerFailed トラップをトリガーするには： **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>` クラッシュ CLI コマンドを実行します。 **3** `utils core active list` 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 サーバの停止、タイマーの問題などがあります。 （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。
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。例：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。例：snmpset -c <Community String> -v 2c <transmitter ip address> 1.3.6.1.4.1.9.9.41.1.1.3.0 i <value>

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> 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：警報
  - 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，（222 ページ）

第 9 章

Call Home

Call Home

この章では、Cisco Unified Communications Manager Call Home サービスの概要と Cisco 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

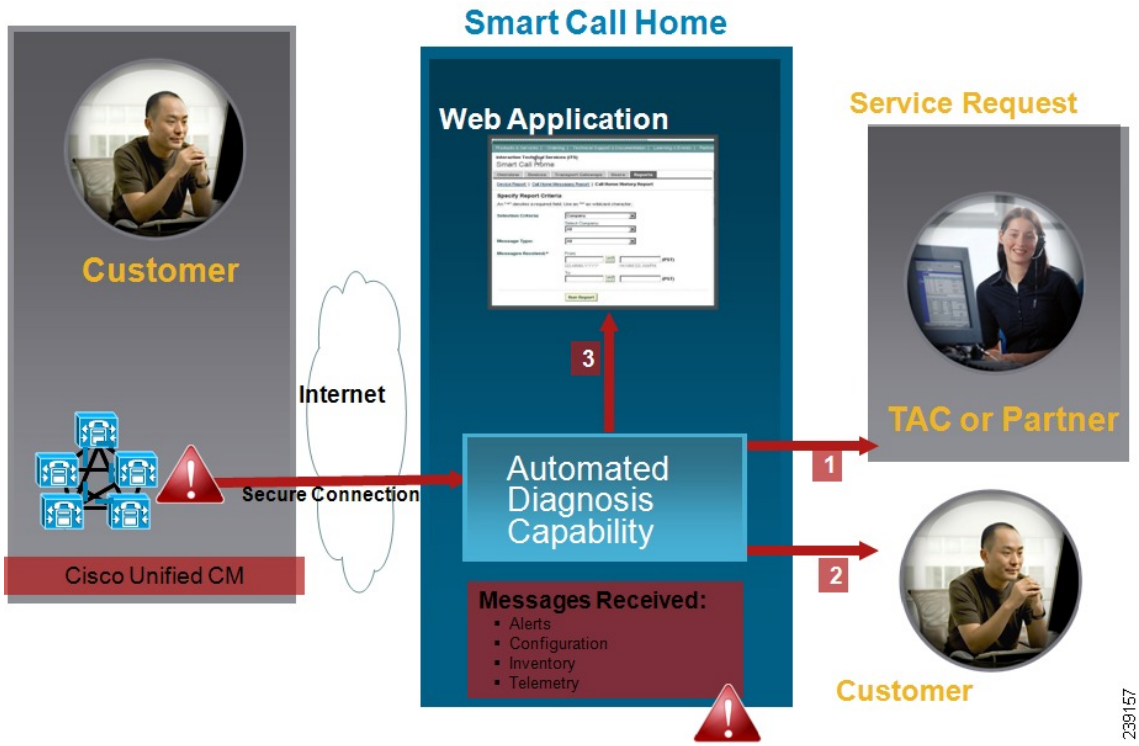
Smart Call Home は、さまざまなシスコ デバイスを対象として予防的診断、リアルタイム アラート、および修復を実行し、ネットワークの可用性と運用効率を向上させます。Smart Call Home が有効化された Cisco Unified Communications Manager から診断アラート、インベントリ、その他のメッセージを受け取り分析することでも同様のことを達成します。Cisco Unified Communications Manager の特定の機能は Cisco Unified Communications Manager Call Home と呼ばれます。

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 *20*：*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

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。

- Cisco 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 CM 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（Include Trace logs and Diagnostic Information）] 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 *66*：*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	適用不可能
連絡先電話番号（Contact Phone Number）	適用可能	適用不可能
住所（Street Address）	適用可能	適用不可能
サーバ名（Server Name）	適用可能	適用不可能
サーバの IP アドレス（Server IP Address）	適用可能	適用不可能
ライセンス サーバ（Licence Server）	適用可能	適用不可能
OS のバージョン（OS Version）	適用可能	適用可能
モデル（Model）	適用可能	適用可能

インベントリ メッセージ	Smart Call Home	匿名 Call Home
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	適用不可能
パブリッシャ IP（Publisher IP）	適用可能	適用不可能
製品 ID（Product ID）	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、Cisco Unified Communication 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 *67*：*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	N/A
連絡先電話番号（Contact Phone Number）	適用可能	N/A
住所（Street Address）	適用可能	N/A
サーバ名（Server name）	適用可能	N/A
CM ユーザ数（CM User Count）	適用可能	N/A
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	N/A
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	N/A
アップグレードの履歴（Upgrade history）	適用可能	N/A
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

シスコ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 Cisco Unified Communications Manager を登録できます。Smart Call Home は、Cisco 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することで、システムの問題を迅速に解決します。

Cisco Unified Communications Manager Call Home 機能では、Smart Call Home バックエンド サーバ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についてアラート情報が含まれています。アラートは Cisco Unified Communications Manager クラスタ内のノードから生成されることがあります。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（Cisco 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には、Smart Call Home によって処理されません。

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、CUCM パブリッシャがプライマリ AMC サーバです。

- **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。

関連トピック

Call Home の前提条件

Cisco Unified Communications Manager Call Home サービスをサポートするには、次が必要です。

- 対応する Cisco Unified Communications Manager サービス契約に関連付けられた Cisco.com ユーザ ID。
- ドメイン ネーム システム（DNS）と Simple Mail Transfer Protocol（SMTP）の両サーバを Cisco 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

Cisco Unified Communications Manager Call Home にアクセスするには、Cisco Unified Serviceability Administrationに移動し、[CallHome]（[Cisco Unified Serviceability] > [CallHome] > [Call Homeの設定（Call Home Configuration）]）を選択します。

Call Home の設定

次の表に、Cisco Cisco Unified Communications Manager Call Home のデフォルト設定を示します。

表 *68*：*Call Home* のデフォルト設定

パラメータ	デフォルト
Call Home	有効
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） Cisco Cisco Unified Communications Manager のインストール中に、Cisco Smart Call Home を設定できます。

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（None）] を選択すると、通知メッセージは Cisco Cisco Unified Communications Manager Administration にログインしたときに表示されます。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、Cisco Cisco Unified Communications Manager Call Home の設定について説明します。

表 *69*：*Cisco Cisco Unified Communications Manager Call Home* の構成時の設定

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（None）]： 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。Smart Call Home を設定するか、リマインダを無効にするには、[Cisco Unified Serviceability] > [Call Home] に移動するか、ここをクリックしてください（Smart Call Home is not configured.To configure Smart Call Home or disable the reminder, please go to Cisco Unified Serviceability > Call Home or click here）」というリマインダメッセージが管理者ページに表示されます。 • [無効（Disabled）]：Call Home を無効にする場合は、このオプションを選択します。 • [有効（Smart Call Home）（Enabled (Smart Call Home)）]：インストール中に Smart Call Home を選択した場合には、このオプションが有効になります。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）（Enabled (Anonymous 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	

フィールド名	説明
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。
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）（Secure 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には、このオプションを選択します。 • [電子メール（Email）]：電子メールを使用して 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。電子メールの場合は、SMTP サーバを設定する必要があります。設定された SMTP サーバのホスト名または 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/ホスト名（HTTPS Proxy IP/Hostname）]*：プロキシIP/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。

フィールド名	説明
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。
トレースログと診断情報を含める（Include Trace logs and Diagnostics Information）	ログと診断情報を収集するために Cisco Cisco Unified Communications Manager をアクティブ化するには、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。

制限事項

次の制限事項は、Cisco Unified Communications Manager や Cisco Unified Presence サーバがダウンしているか到達不能である場合に適用されます。

- Smart Call Home は、サーバ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を次に示します。

- **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 **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

索 引

C

H

M

N

R

S

T

あ

い

え

く

こ

さ

し

せ

て

と

ね

は

ま

ゆ

れ