トラブルシューティング ツール

この章では、Cisco Unified CallManager 5.0(2) の設定、監視、およびトラブルシューティングに使用するツールとユーティリティについて説明し、同じデータを何度もテストしたり再収集したりすることを避けるために、情報収集に関する一般的なガイドラインを示します。

（注） 本書に示す URL サイトの中には、登録ユーザとしてログインしないとアクセスできないものもあります。

この章では、次のトピックについて取り上げます。

Sniffer トレース

通常は、VLAN をスパンするように設定された Catalyst ポートまたはトラブル情報を含むポート（CatOS、Cat6K-IOS、XL-IOS）上で、ラップトップ、または sniffer を装備した他のデバイスを接続することにより、sniffer トレースを収集します。ポートが空いていない場合は、スイッチとデバイスの間に挿入されているハブ上で、sniffer を装備したデバイスを接続します。

ヒント　TAC では Sniffer Pro ソフトウェアが広く使用されているため、TAC エンジニアがトレースを簡単に読み取って解釈できるように、このソフトウェアを使用することをお勧めします。

関係するすべての機器（IP Phone、ゲートウェイ、Cisco Unified CallManager など）の IP アドレスと MAC アドレスを用意しておいてください。

トレースの収集

CallManager クラスタから Call Connection Manager（Unified CM）と Signal Distribution Layer（SDL）の基本的なトレースを収集する方法については、ここで説明するビデオで示しています。収集した情報は、TAC Service Request Tool で使用することができます。

このビデオを観た後は、次の作業ができるようになります。

- 問題を文書化する。
- 問題を再現し、必要な情報を収集する。
- 収集した情報を TAC エンジニアに提出する。

この Flash による説明ビデオは、次の Web サイトで閲覧できます。

www.cisco.com/warp/public/788/video_64826/callmanager-tool.html
（未登録のユーザ用）

www.cisco.com/warp/customer/788/video_64826/callmanager-tool.html
（登録済みユーザ用）

デバッグ

debug 特権 EXEC コマンドからの出力には、プロトコル ステータスやネットワーク アクティビティ全般に関連するさまざまなインターネットワーキング イベントについての診断情報が記載されています。

デバッグ出力をファイルに取り込むことができるように、ターミナル エミュレータ ソフトウェア（ハイパーターミナルなど）を設定します。ハイパーターミナルでは、［**転送**］をクリックし、［**テキストのキャプチャ**］をクリックして、適切なオプションを選択します。

IOS 音声ゲートウェイのデバッグを実行する前に、ゲートウェイ上で `service timestamps debug datetime msec` がグローバルに設定されていることを確認します。

（注） 営業時間中にライブ環境でデバッグを収集しないでください。

営業時間外にデバッグを収集することをお勧めします。ライブ環境でデバッグを収集する必要がある場合は、`no logging console` および `logging buffered` を設定します。デバッグを収集するには、**`show log`** を使用します。

デバッグは長くなることがあるため、コンソール ポート（デフォルト **`logging console`**）またはバッファ（**`logging buffer`**）でデバッグを直接収集します。Telnet セッションを介してデバッグを収集すると、デバイスのパフォーマンスが低下して、デバッグが不完全となり、デバッグを再収集する必要が生じることがあります。

デバッグを停止するには、**`no debug all`** または **`undebug all`** コマンドを使用します。**`show debug`** コマンドを使用して、デバッグがオフになっていることを確認してください。

パケット キャプチャ

この項では、次のトピックについて取り上げます。

パケット キャプチャの概要

メディアや TCP パケットをスニフィングするサードパーティ製トラブルシューティング ツールは、暗号化を有効にした後は機能しません。このため、問題が発生した場合は、Cisco Unified CallManager の管理ページを使用して次の作業を行う必要があります。

- Cisco Unified CallManager とデバイス（Cisco Unified IP Phone、Cisco Unified SIP IP Phone、Cisco IOS MGCP ゲートウェイ、H.323 ゲートウェイ、H.323/H.245/H.225 トランク、または SIP トランク）の間で交換されるメッセージのパケットを分析する。
- デバイス間で交換される Secure Real Time Protocol（SRTP）パケットをキャプチャする。
- メディア暗号鍵の材料をメッセージから抽出し、デバイス間で交換されるメディアを復号化する。

ヒント　この作業を複数のデバイスに対して同時に行うと、CPU の使用率が上昇し、コールの処理が妨げられる可能性があります。この作業を行うのは、コール処理への影響が最小限で済む時間帯にすることを強くお勧めします。

詳細については、『*Cisco Unified CallManager セキュリティ ガイド*』を参照してください。

パケット キャプチャ設定のチェックリスト

必要なデータを抽出し、分析するには、表 2-1 に示す作業を行います。

表 2-1　パケット キャプチャ設定のチェックリスト

設定のステップ		手順およびトピック
ステップ 1	エンド ユーザを Standard Packet Sniffer Users グループに追加します。	Standard Packet Sniffer Users グループへのエンド ユーザの追加（P.2-5）
ステップ 2	Cisco Unified CallManager の管理ページの［サービスパラメータ設定 (Service Parameter Configuration)］ウィンドウで、パケット キャプチャのサービス パラメータを設定します。たとえば、Packet Capture Enable サービス パラメータを設定します。	パケット キャプチャのサービス パラメータの設定（P.2-6）

表 2-1　パケット キャプチャ設定のチェックリスト（続き）

設定のステップ		手順およびトピック
ステップ 3	［電話の設定 (Phone Configuration)］、［ゲートウェイの設定 (Gateway Configuration)］、または［トランクの設定 (Trunk Configuration)］のウィンドウで、デバイスごとのパケット キャプチャの設定を行います。 （注）　パケット キャプチャは、複数のデバイスで同時には有効にしないことを強くお勧めします。この作業によって、ネットワークに含まれている CPU の使用率が上昇する可能性があるためです。	• 電話の設定（Phone Configuration）ウィンドウでのパケット キャプチャの設定（P.2-6） • ゲートウェイの設定 (Gateway Configuration) ウィンドウおよびトランクの設定 (Trunk Configuration) ウィンドウでのパケット キャプチャの設定（P.2-7） • パケット キャプチャの設定値（P.2-9）
ステップ 4	該当するデバイス間で Sniffer トレースを使用して、SRTP パケットをキャプチャします。	使用している Sniffer トレース ツールに対応したマニュアルを参照
ステップ 5	パケットをキャプチャしたら、Packet Capture Enable サービス パラメータを False に設定します。	• パケット キャプチャのサービス パラメータの設定（P.2-6） • パケット キャプチャの設定値（P.2-9）
ステップ 6	パケットの分析に必要なファイルを収集します。	キャプチャしたパケットの分析（P.2-10）
ステップ 7	Cisco Technical Assistance Center（TAC）がパケットを分析します。この作業については、TAC に直接ご依頼ください。	キャプチャしたパケットの分析（P.2-10）

Standard Packet Sniffer Users グループへのエンド ユーザの追加

Standard Packet Sniffer Users グループに所属するユーザは、パケット キャプチャをサポートしているデバイスについて、［パケットキャプチャモード (Packet Capture Mode)］と［パケットキャプチャ時間 (Packet Capture Duration)］を設定できます。ユーザが Standard Packet Sniffer Users グループに含まれていない場合、そのユーザはパケット キャプチャを開始できません。

次の手順では、エンド ユーザを Standard Packet Sniffer Users グループに追加する方法について説明します。この手順では、『*Cisco Unified CallManager アドミニストレーション ガイド*』の説明に従って、Cisco Unified CallManager の管理ページでエンド ユーザを設定したことを前提としています。

手順

ステップ 1　『*Cisco Unified CallManager アドミニストレーション ガイド*』の説明に従って、ユーザ グループを検索します。

ステップ 2　［ユーザグループの検索と一覧表示 (Find and List User Groups)］ウィンドウが表示されたら、**Standard Packet Sniffer Users** リンクをクリックします。

ステップ 3　**［グループにエンドユーザを追加］**ボタンをクリックします。

ステップ 4　『*Cisco Unified CallManager アドミニストレーション ガイド*』の説明に従って、エンド ユーザを追加します。

パケット キャプチャのサービス パラメータの設定

パケット キャプチャのパラメータを設定するには、次の手順を実行します。

手順

ステップ 1　Cisco Unified CallManager の管理ページで、［システム］>［サービスパラメータ］を選択します。

ステップ 2　［サーバ (Server)］ドロップダウン リスト ボックスから、Cisco Unified CallManager サービスをアクティブにした Active サーバを選択します。

ステップ 3　［サービス (Service)］ドロップダウン リスト ボックスから、**Cisco CallManager (Active)** サービスを選択します。

ステップ 4　TLS Packet Capture Configurations ペインまでスクロールして、パケット キャプチャを設定します。

ヒント　サービス パラメータについては、ウィンドウに表示されているパラメータ名または疑問符をクリックしてください。

（注）　パケット キャプチャを実行するには、Packet Capture Enable サービス パラメータを True に設定する必要があります。

ステップ 5　変更内容を有効にするには、［保存］をクリックします。

ステップ 6　パケット キャプチャの設定を続行する場合は、次のいずれかの項を参照してください。

- 電話の設定（Phone Configuration）ウィンドウでのパケット キャプチャの設定（P.2-6）
- ゲートウェイの設定 (Gateway Configuration) ウィンドウおよびトランクの設定 (Trunk Configuration) ウィンドウでのパケット キャプチャの設定（P.2-7）

電話の設定（Phone Configuration）ウィンドウでのパケット キャプチャの設定

［サービスパラメータ設定 (Service Parameter Configuration)］ウィンドウでパケット キャプチャを有効にしたら、Cisco Unified CallManager の管理ページの［電話の設定 (Phone Configuration)］ウィンドウで、デバイスごとにパケット キャプチャを設定することができます。

電話機ごとに、パケット キャプチャを有効または無効にします。パケット キャプチャのデフォルト設定は、None です。

ヒント　パケット キャプチャは、複数の電話機で同時には有効にしないことを強くお勧めします。この作業によって、ネットワークに含まれている CPU の使用率が上昇する可能性があるためです。

パケットをキャプチャしない場合、または作業が完了した場合は、Packet Capture Enable サービス パラメータを False に設定します。

電話機のパケット キャプチャを設定するには、次の手順を実行します。

手順

ステップ 1　パケット キャプチャを設定する前に、P.2-4 の「パケット キャプチャ設定のチェックリスト」を参照してください。

ステップ 2　『*Cisco Unified CallManager　アドミニストレーション　ガイド*』の説明に従って、SIP 電話機または SCCP 電話機を検索します。

ステップ 3　［電話の設定 (Phone Configuration)］ウィンドウが表示されたら、表 2-2 の説明に従って、トラブルシューティングの設定を行います。

ステップ 4　設定が完了したら、**［保存］**をクリックします。

ステップ 5　［デバイスリセット (Device Reset)］ダイアログボックスで、**［リスタート］**をクリックします。

ヒント　Cisco Unified CallManager の管理ページからデバイスをリセットするように求められますが、パケットをキャプチャするためにデバイスをリセットする必要はありません。

この他の手順

該当するデバイス間で Sniffer トレースを使用して、SRTP パケットをキャプチャします。

パケットをキャプチャしたら、Packet Capture Enable サービス パラメータを False に設定します。

P.2-10 の「キャプチャしたパケットの分析」を参照してください。

ゲートウェイの設定 (Gateway Configuration) ウィンドウおよびトランクの設定 (Trunk Configuration) ウィンドウでのパケット キャプチャの設定

次のゲートウェイおよびトランクは、Cisco Unified CallManager の管理ページでパケット キャプチャをサポートしています。

- Cisco IOS MGCP ゲートウェイ
- H.323 ゲートウェイ
- H.323 トランク、H.245 トランク、H.225 トランク
- SIP トランク

ヒント　パケット キャプチャは、複数のデバイスで同時には有効にしないことを強くお勧めします。この作業によって、ネットワークに含まれている CPU の使用率が上昇する可能性があるためです。

パケットをキャプチャしない場合、または作業が完了した場合は、Packet Capture Enable サービス パラメータを False に設定します。

［ゲートウェイの設定 (Gateway Configuration)］ウィンドウまたは［トランクの設定 (Trunk Configuration)］ウィンドウでパケット キャプチャの設定を行うには、次の手順を実行します。

手順

ステップ 1　パケット キャプチャを設定する前に、P.2-4 の「パケット キャプチャ設定のチェックリスト」を参照してください。

ステップ 2　次のいずれかの作業を行います。

- 『*Cisco Unified CallManager アドミニストレーション ガイド*』の説明に従って、Cisco IOS MGCP ゲートウェイを検索します。
- 『*Cisco Unified CallManager アドミニストレーション ガイド*』の説明に従って、H.323 ゲートウェイを検索します。
- 『*Cisco Unified CallManager アドミニストレーション ガイド*』の説明に従って、H.323、H.245、または H.225 トランクを検索します。
- 『*Cisco Unified CallManager アドミニストレーション ガイド*』の説明に従って、SIP トランクを検索します。

ステップ 3　設定ウィンドウが表示されたら、［パケットキャプチャモード (Packet Capture Mode)］設定値と［パケットキャプチャ時間 (Packet Capture Duration)］設定値を確認します。

ヒント　Cisco IOS MGCP ゲートウェイを見つけたら、Cisco IOS MGCP ゲートウェイ用のポートを『*Cisco Unified CallManager アドミニストレーション ガイド*』の説明に従って設定してあることを確認します。Cisco IOS MGCP ゲートウェイのパケット キャプチャ設定値は、エンドポイント識別子の［ゲートウェイの設定 (Gateway Configuration)］ウィンドウに表示されます。このウィンドウにアクセスするには、音声インターフェイス カードのエンドポイント識別子をクリックします。

ステップ 4　表 2-2 の説明に従って、トラブルシューティングの設定を行います。

ステップ 5　パケット キャプチャを設定したら、**［保存］**をクリックします。

ステップ 6　［デバイスリセット (Device Reset)］ダイアログボックスで、**［リスタート］**をクリックします。

ヒント　Cisco Unified CallManager の管理ページからデバイスをリセットするように求められますが、パケットをキャプチャするためにデバイスをリセットする必要はありません。

この他の手順

該当するデバイス間で Sniffer トレースを使用して、SRTP パケットをキャプチャします。

パケットをキャプチャしたら、Packet Capture Enable サービス パラメータを False に設定します。

P.2-10 の「キャプチャしたパケットの分析」を参照してください。

パケット キャプチャの設定値

［パケットキャプチャモード (Packet Capture Mode)］設定値および［パケットキャプチャ時間 (Packet Capture Duration)］設定値について説明した表 2-2 とともに、次の項も参照してください。

- 電話の設定（Phone Configuration）ウィンドウでのパケット キャプチャの設定（P.2-6）
- ゲートウェイの設定 (Gateway Configuration) ウィンドウおよびトランクの設定 (Trunk Configuration) ウィンドウでのパケット キャプチャの設定（P.2-7）

表 2-2　パケット キャプチャの設定値

設定値	説明
［パケットキャプチャモード (Packet Capture Mode)］	この設定値は、暗号化のトラブルシューティングを行う場合のみ使用します。パケット キャプチャを実行すると、CPU の使用率が上昇して、コール処理が妨げられる可能性があります。ドロップダウン リスト ボックスから、次のいずれかのオプションを選択します。 • **None**：このオプションは、パケット キャプチャが発生しないことを示します（デフォルト設定）。パケット キャプチャが完了すると、Cisco Unified CallManager は［パケットキャプチャモード (Packet Capture Mode)］を None に設定します。 • **Batch Processing Mode**：Cisco Unified CallManager は、復号化された（暗号化されていない）メッセージをファイルに書き込み、システムが各ファイルを暗号化します。システムは、毎日新しい暗号鍵を使用して、新しいファイルを作成します。Cisco Unified CallManager はファイルを 7 日間保管し、ファイルを暗号化する鍵も安全な場所に格納します。ファイルの格納先は、/var/pktCap です。1 つのファイルの中に、タイム スタンプ、送信元 IP アドレス、送信元 IP ポート、宛先 IP アドレス、パケットのプロトコル、メッセージの長さ、およびメッセージが保持されます。TAC のデバッグ ツールでは、HTTPS、管理者のユーザ名とパスワード、および指定された日付を使用して、キャプチャされたパケットを保持している暗号化済みファイルを 1 つのみ要求します。同様に、暗号化されているファイルを復号化するための鍵情報も要求します。 **ヒント**　TAC にお問い合せいただく前に、該当するデバイス間で Sniffer トレースを使用して、SRTP パケットをキャプチャする必要があります。
［パケットキャプチャ時間 (Packet Capture Duration)］	この設定値は、暗号化のトラブルシューティングを行う場合のみ使用します。パケット キャプチャを実行すると、CPU の使用率が上昇して、コール処理が妨げられる可能性があります。 このフィールドには、1 つのパケット キャプチャ セッションに割り当てる時間の上限を分単位で指定します。デフォルト設定は 0 で、範囲は 0 ～ 300 分です。 パケット キャプチャを開始するには、このフィールドに 0 以外の値を入力します。パケット キャプチャが完了すると、値 0 が表示されます。

キャプチャしたパケットの分析

Cisco Technical Assistance Center（TAC）は、デバッグ ツールを使用してパケットを分析します。TAC にお問い合せいただく前に、該当するデバイス間で Sniffer トレースを使用して、SRTP パケットをキャプチャしてください。次の情報を収集したら、TAC まで直接お問い合せください。

- パケット キャプチャ ファイル：**https://<IP アドレスまたはサーバ名 >/pktCap/pktCap.jsp?file=mm-dd-yyyy.pkt**。サーバを参照し、西暦年と日付（mm-dd-yyyy）別のパケット キャプチャ ファイルを見つけます。
- ファイルの鍵：**https://<IP アドレスまたはサーバ名 >/pktCap/pktCap.jsp?key=mm-dd-yyyy.pkt**。サーバを参照し、西暦年と日付（mm-dd-yyyy）別の鍵を見つけます。
- Standard Packet Sniffer Users グループに所属しているエンド ユーザのユーザ名とパスワード。

詳細については、『*Cisco Unified CallManager セキュリティ ガイド*』を参照してください。

Cisco Unified CallManager のトラブルシューティング ツール

さまざまな Cisco Unified CallManager システムを監視および分析するために Cisco Unified CallManager のサービスアビリティ ページが提供する、次の各種ツールの詳細については、『*Cisco Unified CallManager Serviceability アドミニストレーション ガイド*』および『*Cisco Unified CallManager Serviceability システム ガイド*』を参照してください。

表 2-3　サービスアビリティ ツール

用語	定義
Real-Time Monitoring Tool（RTMT）	この用語は、Cisco Unified CallManager デバイスおよびパフォーマンス カウンタに関するリアルタイム情報を提供する、サービスアビリティ ページ内のプログラムを示します。
アラーム	管理者は、アラームを使用して、Cisco Unified CallManager システムの実行時のステータスや状態を確認します。アラームには、説明や推奨される処置など、システムの問題に関する情報が含まれています。
アラーム カタログ	この用語は、Cisco Unified CallManager サービスのすべてのアラーム定義を含むファイルを示します。サービスアビリティは、アラーム タイプに固有の複数のアラーム カタログをサポートしています。
アラーム定義	管理者は、アラーム定義データベースを検索して、アラーム情報を見つけます。アラーム定義には、アラームの説明および推奨される処置が含まれています。
アラーム イベント レベル	管理者は、アラームに含まれる情報のレベルを決定します。レベルの範囲は、システムに関する一般的な情報から、デバッグだけを目的とした情報にまで及びます。
アラーム フィルタ	管理者は、アラームに含まれる情報のレベル、およびアラーム 情報が保存される場所を決定します。
アラーム モニタ	Cisco Unified CallManager のサービスアビリティ ページでは、モニタと呼ばれるさまざまな宛先（ローカルの syslog、リモートの syslog、SDI トレース、および SDL トレース）にアラームを送信できます。
アラート通知	管理者は、Real-Time Monitoring Tool を使用して、パフォーマンス カウンタおよびゲートウェイ ポート（チャネル）のアラート通知を設定します。リアルタイム モニタリングでは、電子メールまたはシステム通知（ポップアップ）ウィンドウで管理者にアラートが送信されます。
カテゴリ タブ	管理者は、トラブルシューティングの目的で、リアルタイム モニタリングに特定のモニタリング ウィンドウを設定します。管理者は、カテゴリ タブを使用して、その特定のウィンドウを作成します。
チャート ビュー	パフォーマンス モニタリング ウィンドウでは、デフォルトで、チャート ビューにパフォーマンス カウンタが表示されます。チャート ビューでは、カウンタ情報がグラフィカルに表示されます。
Cisco CallManager サービス	Cisco Unified CallManager は、TFTP、CTI、Music On Hold（MOH; 保留音）など、特定の機能を実行するソフトウェアの形で、多くのサービスをサポートしています。
コントロール センタ	サービスアビリティ ページのコントロールセンタ ツールを使用すると、管理者は、Cisco Unified CallManager サービスのステータスを表示したり、このサービスを開始および停止できます。
デバッグ トレース レベル	管理者は、トレースに含まれる情報のレベルを決定します。レベルの範囲は、一般的なエラーから、デバッグを目的とした詳細なエラーにまで及びます。

表 2-3　サービスアビリティ ツール（続き）

用語	定義
デバイス モニタリング	リアルタイム モニタリングでは、電話機やゲートウェイなど、Cisco Unified CallManager デバイスに関するリアルタイム情報が表示されます。
デバイス モニタリング ウィンドウ	Real-Time Monitoring Tool がデバイスのパフォーマンスを監視しているときに、Real-Time Monitoring Tool ウィンドウの右側にデバイスのパフォーマンス情報が表示されます。
デバイス名に基づくトレース モニタリング	管理者は、Cisco CallManager および Cisco CTIManager サービスのトレース パラメータを設定することにより、選択したデバイスに関するトレース情報を取得します。
モニタリング　オブジェクト ウィンドウ	Real-Time Monitoring Tool ウィンドウの左側には、クラスタに対応する、Cisco Unified CallManager 関連のオブジェクトおよびカウンタまたはデバイスが表示されます。表示される情報は、ウィンドウでアクティブになっているタブによって異なります。
オブジェクトとカウンタ	システムは、さまざまなオブジェクトおよびカウンタに関する情報を含むパフォーマンス データを提供します。オブジェクトとは、Cisco Unified IP Phone や Cisco Unified CallManager System Performance など、特定のデバイスまたは機能に関する同様のカウンタを論理グループにまとめたものです。カウンタは、システム パフォーマンスのさまざまな側面を測定します。カウンタは、登録されている電話機の数、試行されたコール、進行中のコールなど、統計情報を測定します。Real-Time Monitoring Tool は、これらのカウンタによって生成されるリアルタイムの統計情報を監視します。
パフォーマンス モニタリング	Real-Time Monitoring Tool には、パフォーマンス カウンタに関するリアルタイム情報が表示されます。パフォーマンス カウンタは、システム固有のものも Cisco Unified CallManager 固有のものもあります。
パフォーマンス モニタリング ウィンドウ	Real-Time Monitoring Tool がカウンタを監視しているときに、Real-Time Monitoring Tool ウィンドウの右側にカウンタの統計情報が表示されます。
CCM トレース ログ ファイル（以前は SDI トレース）	すべての Cisco CallManager サービスには、デフォルトのトレース ログ ファイルが含まれています。システムは、サービスからの system diagnostic interface（SDI）情報をトレースし、実行時のイベントおよびトレースをログ ファイルに記録します。
品質レポート ツール	この用語は、Cisco Unified CallManager のサービスアビリティ ページに含まれる、音声品質および一般的な問題を報告するユーティリティを示します。
SDL トレース ログ ファイル	このファイルには、Cisco CallManager や Cisco CTIManager などのサービスからのコール処理情報が含まれています。システムは、コールの signal distribution layer（SDL）をトレースし、状態遷移をログ ファイルに記録します。 **（注）** ほとんどの場合は、Cisco Technical Assistance Center（TAC）から要求された場合にだけ、SDL トレースを収集します。
サービスのステータスを示すアイコン	Control Center には、サーバ上のサービスのステータスが表示されます。
トレース	管理者およびシスコのエンジニアは、トレース ファイルを使用して、Cisco CallManager サービスの問題に関する特定の情報を取得します。

表 2-3　サービスアビリティ ツール（続き）

用語	定義
トレース ログ ファイル	Cisco Unified CallManager のサービスアビリティ ページは、設定されているトレース情報をこのファイルに送信します。SDI と SDL という 2 つのタイプのトレース ログ ファイルがあります。
ウィンドウ ステータス バー	Real-Time Monitoring Tool ウィンドウの右下隅には、ウィンドウ ステータス バーが表示されます。このステータス バーには、Preferences、Cluster Information、Resource Usage、About、および Help という 5 つのアイコンが表示されます。

Cisco Secure Telnet

Cisco Secure Telnet を使用すると、Cisco Service Engineer（CSE; シスコ サービス エンジニア）は、ファイアウォールを介してお客様のサイトの Cisco Unified CallManager ノードに透過的にアクセスできます。Cisco Secure Telnet は、強力な暗号化を使用して、シスコシステムズ内の特別な Telnet クライアントを、お客様のファイアウォールの内側にある Telnet デーモンに接続できます。このセキュアな接続により、ファイアウォールを変更せずに、お客様の Cisco Unified CallManager ノードの監視およびトラブルシューティングをリモートで行うことができます。

（注）　シスコでは、お客様の承諾を得た場合にだけこのサービスを提供します。作業を開始する場合は、お客様のサイトでネットワーク管理者のご協力をお願いしています。

コマンドライン インターフェイス

コマンドライン インターフェイス（CLI）は、基本的なメンテナンスおよび障害からの回復を目的として、Cisco Unified CallManager システムにアクセスするために使用します。システムには、物理的に接続された端末（システム モニタおよびキーボード）を使用してアクセスすることも、SSH セッションを実行してアクセスすることもできます。

インストール中に、アカウント名とパスワードが作成されます。パスワードはインストール後に変更できますが、アカウント名は一切変更できません。

コマンドは、システムで何らかの機能を実行するための、テキストによる命令文です。コマンドは、スタンドアロンで実行することも、必須または省略可能な引数やオプションを指定して実行することもできます。

レベルは、コマンドの集合です。たとえば、***show*** はレベルであり、***show status*** はコマンドです。レベルおよびコマンドには、それぞれ特権レベルも関連付けられています。ユーザがコマンドを実行できるのは、十分な特権レベルを持っている場合に限られます。

Cisco Unified CallManager の CLI コマンド セットの詳細については、『*Cisco Unified Communications Operating System Administration Guide, Release* 5.0(2)』の「Appendix A」を参照してください。

トラブルシューティング用 perfmon データのロギング

注意　トラブルシューティング用 perfmon データのロギング機能を有効にすると、有効にしたノード上ではシステムのパフォーマンスが低下します。このパラメータは、Cisco Technical Assistance Center（TAC）からの指示がない限り有効にしないでください。

トラブルシューティング用 perfmon データのロギング機能は、システムの問題点を特定する際に、Cisco TAC が利用します。トラブルシューティング用 perfmon データのロギングを有効にすると、有効にしたノード上では、Cisco Unified CallManager およびオペレーティング システムのパフォーマンスに関する、一連の統計情報の収集が開始されます。収集される統計情報には、システムの診断に利用できる包括的な情報、および現在の事前設定済みカウンタ セットに含まれていない、一連のカウンタからの情報が含まれています。

大量の情報が短時間で収集されるため、トラブルシューティング用 perfmon データのロギングは、長時間にわたって有効にしないことを強くお勧めします。また、有効にしている間は、Log Partitioning Monitor を有効にしてディスクの使用状況を監視してください。

トラブルシューティング用 perfmon データのロギング機能をアクティブな電話コールが発生しないシステム上で有効にし、このロギングのパラメータをデフォルト設定のまま使用した場合、シスコによる見積りでは、システムでの CPU 使用率の上昇は 5 % 未満であり、使用メモリ量の増加はわずかなもので、ログ ファイルには 1 日あたり約 50 MB の情報が書き込まれます。

トラブルシューティング用 perfmon データのロギング機能については、次の管理タスクを実行できます。

- トラブルシューティング用 perfmon データのロギングのトレース フィルタを有効または無効にする。
- 各サーバ上で、事前定義済みの一連の System パフォーマンス オブジェクトおよび Cisco Unified CallManager パフォーマンス オブジェクト、およびカウンタを監視する。
- ローカル サーバ上のアクティブなログ パーティションと cm/log/ris/csv ディレクトリに、監視対象のパフォーマンス データを CSV ファイル形式で記録する。ログ ファイルの命名規則は、PerfMon_<node>_<month>_<day>_<year>_<hour>_<minute>.csv です。たとえば、PerfMon_172.19.240.80_06_15_2005_11_25.csv のようになります。
- ポーリングのレートを指定する。このレートは、パフォーマンス データを収集し、ログに記録するレートです。設定できるポーリング レートは、最短で 5 秒です。デフォルトのポーリング レートは 15 秒です。
- ディスクに格納するログ ファイルの最大数を指定する。この制限値を超えると、ログ ファイルが自動的に消去されます（最も古いログ ファイルが削除されます）。
- ファイルの最大サイズ（MB 単位）に基づいて、ログ ファイルのロールオーバー基準を指定する。デフォルト値は 2 MB です。
- TCT/SOAP トレース収集ツール（TCT）またはコマンドライン インターフェイスを使用して、ログ ファイルを収集する。
- Microsoft Windows のパフォーマンス ツールを使用して、ログ ファイルをグラフ形式で表示する。

トラブルシューティング用 perfmon データのロギング機能では、次の perfmon オブジェクトに含まれている次のカウンタから情報を収集します。各カウンタについては、『*Cisco Unified CallManager Serviceability システム ガイド*』の「パフォーマンス オブジェクトとパフォーマンス カウンタ」の章を参照してください。

- Cisco CallManager オブジェクト：
  - CallManagerHeartBeat
  - CallsActive
  - CallsAttempted
  - CallsCompleted
  - InitializationState
  - RegisteredHardwarePhones
  - RegisteredMGCPGateway
- Cisco CallManager System パフォーマンス オブジェクト：
  - QueueSignalsPresent 1-High
  - QueueSignalsPresent 2-Normal
  - QueueSignalsPresent 3-Low
  - QueueSignalsPresent 4-Lowest
  - QueueSignalsProcessed 1-High
  - QueueSignalsProcessed 2-Normal
  - QueueSignalsProcessed 3-Low
  - QueueSignalsProcessed 4-Lowest
  - QueueSignalsProcessed Total
- Cisco TFTP：
  - BuildAbortCount
  - BuildCount
  - BuildDeviceCount
  - BuildDialruleCount
  - BuildDuration
  - BuildSignCount
  - BuildSoftkeyCount
  - BuildUnitCount
  - ChangeNotifications
  - DeviceChangeNotifications
  - DialruleChangeNotifications
  - EncryptCount
  - GKFoundCount
  - GKNotFoundCount
  - HeartBeat
  - HttpConnectRequests
  - HttpRequests
  - HttpRequestsAborted
  - HttpRequestsNotFound
  - HttpRequestsOverflow
  - HttpRequestsProcessed
  - HttpServedFromDisk
  - LDFoundCount
  - LDNotFoundCount

  - MaxServingCount
  - Requests
  - RequestsAborted
  - RequestsInProgress
  - RequestsNotFound
  - RequestsOverflow
  - RequestsProcessed
  - SegmentsAcknowledged
  - SegmentsFromDisk
  - SegmentsSent
  - SEPFoundCount
  - SEPNotFoundCount
  - SIPFoundCount
  - SIPNotFoundCount
  - SoftkeyChangeNotifications
  - UnitChangeNotifications
- Process オブジェクト：
  - PID
  - STime
  - %CPU Time
  - Page Fault Count
  - VmData
  - VmSize
  - Thread Count
- Memory オブジェクト：
  - Used Kbytes
  - Free Kbytes
  - Total Kbytes
  - Shared Kbytes
  - Buffers Kbytes
  - Cached Kbytes
  - Free Swap Kbytes
  - Total Swap Kbytes
  - Used Swap Kbytes
  - Pages Input
  - Pages Output
  - Pages
  - % Page Usage
  - % VM Used
  - % Mem Used
- Processor オブジェクト：
  - Irq Percentage
  - Softirq Percentage

  - IOwait Percentage
  - User Percentage
  - Nice Percentage
  - System Percentage
  - Idle Percentage
  - %CPU Time
- Thread オブジェクト（トラブルシューティング用 perfmon データのロギング機能で記録されるのは、CCM スレッドのみ）：
  - PID
  - %CPU Time
- Partition オブジェクト：
  - Used Mbytes
  - Total Mbytes
  - %Used
  - % Wait in Read Time
  - % Wait in Write Time
  - %CPU Time
  - Read Bytes Per Sec
  - Write Bytes Per Sec
  - Queue Length
- IP オブジェクト：
  - In Receives
  - InHdr Errors
  - In Unknown Protos
  - In Discards
  - In Delivers
  - Out Requests
  - Out Discards
  - Reasm Reqds
  - Reasm Oks
  - Reasm Fails
  - Frag OKs
  - Frag Fails
  - Frag Creates
  - InOut Requests
- TCP オブジェクト：
  - Active Opens
  - Passive Opens
  - Attempt Fails
  - Estab Resets
  - Curr Estab
  - In Segs
  - Out Segs
  - Retrans Segs

- InOut Segs

- Network Interface オブジェクト：
  - Rx Bytes
  - Rx Packets
  - Rx Errors
  - Rx Dropped
  - Rx Multicast
  - Tx Bytes
  - Tx Packets
  - Tx Errors
  - Tx Dropped
  - Total Bytes
  - Total Packets
  - Tx QueueLen
- System オブジェクト：
  - Allocated FDs
  - Freed FDs
  - Being Used FDs
  - Max FDs
  - Total Processes
  - Total Threads
  - Total CPU Time

次に、トラブルシューティング用 perfmon データのロギング機能を使用する手順を示します。

手順

ステップ 1　Cisco RIS Data Collector サービスの Troubleshooting Perfmon Data Logging パラメータを設定します。

P.2-19 の「トラブルシューティング用 perfmon データのロギングの設定」を参照してください。

ステップ 2　ログ パーティションの監視が有効になっていることを確認します。

『*Cisco Unified CallManager アドミニストレーション ガイド*』を参照してください。

ステップ 3　トラブルシューティング用 perfmon データのロギングを有効にしたサーバ上で、Cisco RIS Data Collector サービスのログ ファイルを収集します。

- ログ ファイルを RTMT を使用してダウンロードする場合は、『*Cisco Unified CallManager Serviceability アドミニストレーション ガイド*』を参照してください。
- ログ ファイルを CLI を使用してダウンロードする場合は、『*Cisco Unified Communications Operating System Administration Guide*』を参照してください。

ステップ 4　Microsoft Windows のパフォーマンス ツールを使用して、ログ ファイルを表示します。

P.2-20 の「Microsoft パフォーマンス ツールでの perfmon ログ ファイルの表示」を参照してください。

ステップ 5　必要なファイルをすべて収集したら、Enable Logging パラメータを False に設定して、トラブルシューティング用 perfmon データのロギングを無効にします。

トラブルシューティング用 perfmon データのロギングの設定

ここでは、トラブルシューティング用 pefmon データのロギング機能を設定する手順について説明します。

手順

ステップ 1　Cisco Unified CallManager の管理ページで、［システム］>［サービスパラメータ］を選択します。

［サービスパラメータ設定 (Service Parameter Configuration)］ウィンドウが表示されます。

ステップ 2　［サーバ (Server)］ドロップダウン リスト ボックスから、サーバを選択します。

ステップ 3　［サービス (Service)］ドロップダウン リスト ボックスから、Cisco RIS Data Collector を選択します。

ステップ 4　表 2-4 の説明に従って、適切な設定値を入力します。

ステップ 5　［保存］をクリックします。

表 2-4　トラブルシューティング用 perfmon データのロギングのパラメータ

フィールド	説明
Enable Logging	ドロップダウン リスト ボックスから、**True** を選択してトラブルシューティング用 perfmon データのロギングを有効にします。または、**False** を選択して無効にします。
Polling Rate	ポーリング レート（間隔）を秒単位で入力します。5（最小）～ 300（最大）の値を入力できます。デフォルト値は 15 です。
Maximum No. of Files	ディスクに格納するトラブルシューティング用 perfmon データのロギング ファイル数の上限を入力します。1（最少）～ 100（最大）の値を入力できます。デフォルト値は 50 です。 Maximum No. of Files パラメータおよび Maximum File Size パラメータを設定するときは、ストレージ容量を考慮に入れてください。Maximum No. of Files 値に Maximum File Size 値を掛けたときに、値が 100 MB を超えないようにすることをお勧めします。 ファイル数がこのフィールドで指定したファイル数上限値を超えると、タイムスタンプの最も古いログ ファイルが削除されます。 ⚠ **注意**　このパラメータを変更する場合は、事前にログ ファイルを別のマシンに保存しておかないと、ログ ファイルが失われる恐れがあります。

表 2-4　トラブルシューティング用 perfmon データのロギングのパラメータ（続き）

フィールド	説明
Maximum File Size	perfmon ログ ファイルに格納するときの最大ファイル サイズを MB 単位で入力します。このサイズに達すると、新しいファイルが作成されます。1（最小）～ 500（最大）の値を入力できます。デフォルト値は 2 です。 Maximum No. of Files パラメータおよび Maximum File Size パラメータを設定するときは、ストレージ容量を考慮に入れてください。Maximum No. of Files 値に Maximum File Size 値を掛けたときに、値が 100 MB を超えないようにすることをお勧めします。

Microsoft パフォーマンス ツールでの perfmon ログ ファイルの表示

Microsoft のパフォーマンス ツールを使用してログ ファイルを表示するには、次の手順に従います。

手順

ステップ 1　［スタート］> ［設定］> ［コントロール パネル］> ［管理ツール］> ［パフォーマンス］を選択します。

ステップ 2　アプリケーションのウィンドウで、マウスの右ボタンをクリックし、［プロパティ］を選択します。

ステップ 3　［システム モニタのプロパティ］ダイアログボックスで、［ソース］タブをクリックします。

ステップ 4　perfmon ログ ファイルをダウンロードしたディレクトリを参照し、perfmon の csv ファイルを選択します。ログ ファイルの命名規則は、PerfMon_<node>_<month>_<day>_<year>_<hour>_<minute>.csv です。たとえば、PerfMon_172.19.240.80_06_15_2005_11_25.csv のようになります。

ステップ 5　［適用］をクリックします。

ステップ 6　［時間の範囲］ボタンをクリックします。表示する perfmon ログ ファイルについて期間を指定するには、バーを適切な開始時刻および終了時刻にドラッグします。

ステップ 7　［カウンタの追加］ダイアログボックスを開くには、［データ］タブをクリックし、［追加］をクリックします。

ステップ 8　［パフォーマンス オブジェクト］ドロップダウン リスト ボックスから、perfmon オブジェクトを選択します。オブジェクトに複数のインスタンスがある場合は、［すべてのインスタンス］を選択するか、表示するインスタンスのみ選択します。

ステップ 9　［すべてのカウンタ］を選択するか、表示するカウンタのみ選択します。

ステップ 10　選択したカウンタを追加するには、［追加］をクリックします。

ステップ 11　カウンタの選択が終了したら、［閉じる］をクリックします。

CiscoWorks2000

CiscoWorks2000 は、Cisco Unified CallManager を含め、すべてのシスコ デバイスに最適なネットワーク管理システムとして機能します。CiscoWorks2000 は Cisco Unified CallManager にバンドルされていないため、別途購入する必要があります。次のツールを CiscoWorks2000 と併用すると、リモート サービスアビリティが得られます。

- システム ログの管理
- シスコ検出プロトコル（CDP）のサポート
- 簡易ネットワーク管理プロトコルのサポート

CiscoWorks2000 の詳細については、『*Cisco Unified CallManager Serviceability アドミニストレーション ガイド*』、および次の URL にある CiscoWorks2000 のマニュアルを参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/index.htm

システム ログの管理

システム ログ管理プロセスは他のネットワーク管理システムに適合させることもできますが、シスコ デバイスからの Syslog メッセージの管理には、CiscoWorks2000 Resource Manager Essentials に付属の Cisco Syslog Analysis が最適です。

Cisco Syslog Analyzer は、Cisco Syslog Analysis のコンポーネントとして機能し、複数のアプリケーションのシステム ログの共通ストレージおよび分析を提供します。もう 1 つの主要コンポーネントである Syslog Analyzer Collector は、Cisco Unified CallManager サーバからログ メッセージを収集します。

これら 2 つのシスコ アプリケーションは連動し、Cisco ユニファイド コミュニケーション ソリューション用の集中システム ロギング サービスを提供します。

詳細については、『*Cisco Unified CallManager Serviceability アドミニストレーション ガイド*』を参照してください。

シスコ検出プロトコル（CDP）のサポート

シスコ検出プロトコル（CDP）のサポートにより、CiscoWorks2000 で、Cisco Unified CallManager サーバを検出および管理できます。

CiscoWorks2000 の詳細については、『*Cisco Unified CallManager Serviceability アドミニストレーション ガイド*』、および次の URL にある CiscoWorks2000 のマニュアルを参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/index.htm

簡易ネットワーク管理プロトコルのサポート

Network Management System（NMS; ネットワーク管理システム）は、業界標準のインターフェイスである SNMP を使用して、ネットワーク デバイス間で管理情報を交換します。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 パフォーマンスを管理し、ネットワークの問題を検出して解決し、ネットワークの拡張を計画できます。

SNMP で管理されるネットワークは、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ます。

- 管理対象デバイスとは、SNMP エージェントを含み、管理対象ネットワークに常駐するネットワーク ノードです。管理対象デバイスは、管理情報を収集して格納し、SNMP を使用してその情報を使用できるようにします。
- エージェントは、ネットワーク管理ソフトウェアとして、管理対象デバイスに常駐します。エージェントは、管理情報をローカルで認識し、その情報を SNMP と互換性のある形式に変換します。
- ネットワーク管理システムは、SNMP 管理アプリケーションと、そのアプリケーションを実行するコンピュータで構成されます。NMS は、管理対象デバイスを監視および制御するアプリケーションを実行します。NMS は、ネットワーク管理に必要な処理リソースおよびメモリ リソースの大部分を提供します。次の NMS は Cisco Unified CallManager と互換性があります。
  - CiscoWorks2000
  - HP OpenView
  - SNMP および Cisco Unified CallManager SNMP インターフェイスをサポートするサードパーティ製アプリケーション

詳細については、『*Cisco Unified CallManager Serviceability アドミニストレーション ガイド*』および『*Cisco Unified CallManager Serviceability システム ガイド*』を参照してください。

ルート アクセスを使用しないサーバのトラブルシューティング

この項は、ルート アクセスが無効になっている Cisco Unified CallManager サーバをトラブルシューティングするためのコマンドおよびユーティリティのクイック リファレンスです。この項では、次のトピックについて取り上げます。

よく使用される Linux コマンドに対応するサービスアビリティ ページの GUI および CLI コマンド

Real Time Monitoring Tool（RTMT）は、管理者の PC にインストールできるクライアント アプリケーションです。インストールするには、RTMT クライアントを次の URL でサーバからダウンロードします。

https://<server_ipaddress>:8443/ccmadmin/pluginsFindList.do

手順

ステップ 1　Cisco Unified CallManager にログインします。

ステップ 2　**［アプリケーション］>［プラグイン］**を選択します。

［プラグインの検索と一覧表示 (Find and List Plugins)］画面が表示されます。

ステップ 3　選択ボックスを**［名前］［が次の文字列を含む］**に設定し、**tool** と入力します。

ステップ 4　**［かつプラグインタイプが次に等しい］**選択ボックスを **Installation** に設定します。

ステップ 5　**［検索］**をクリックします。

［検索結果 (Search Results)］ボックスに、Cisco Unified CallManager の Real-Time Monitoring Tool の Windows バージョンおよび Linux バージョンへのリンクが表示されます。

ステップ 6　適切な RTMT インストール プラグイン（Windows バージョンまたは Linux バージョン）をダウンロードします。

ステップ 7　RTMT クライアント アプリケーションを PC またはワークステーションにインストールします。

表 2-5 に、以降の各項で説明する CLI コマンドおよび GUI 選択オプションの要約を示します。

表 2-5　CLI コマンドおよび GUI 選択オプションの要約

情報	Linux コマンド	サービスアビリティの GUI ツール	CLI コマンド
CPU 使用率	top	RTMT View タブに移動し、Server > CPU and Memory を選択	プロセッサの CPU 使用率： show perf query class Processor プロセスの CPU 使用率（すべてのプロセス）： show perf query counter Process "% CPU Time" 個々のプロセスのカウンタの詳細（CPU 使用率含む）： show perf query instance <Process task_name>
プロセスの状態	ps	RTMT View タブに移動し、Server > Process を選択	show perf query counter Process "Process Status"
ディスクの使用状況	df/du	RTMT View タブに移動し、Server > Disk Usage を選択	show perf query counter Partition"% Used" または show perf query class Partition
メモリ	free	RTMT View タブに移動し、Server > CPU and Memory を選択	show perf query class Memory
ネットワークのステータス	netstats		show network status
サーバのリブート	reboot	サーバのプラットフォームの管理 Web ページにログイン Restart >Current Version に移動	utils system restart
トレースとログの収集	Sftp、ftp	RTMT Tools タブに移動し、Trace > Trace & Log Central > Collect Files の順に選択	ファイル一覧の表示：file list ファイルのダウンロード：file get ファイル内容の表示：file view

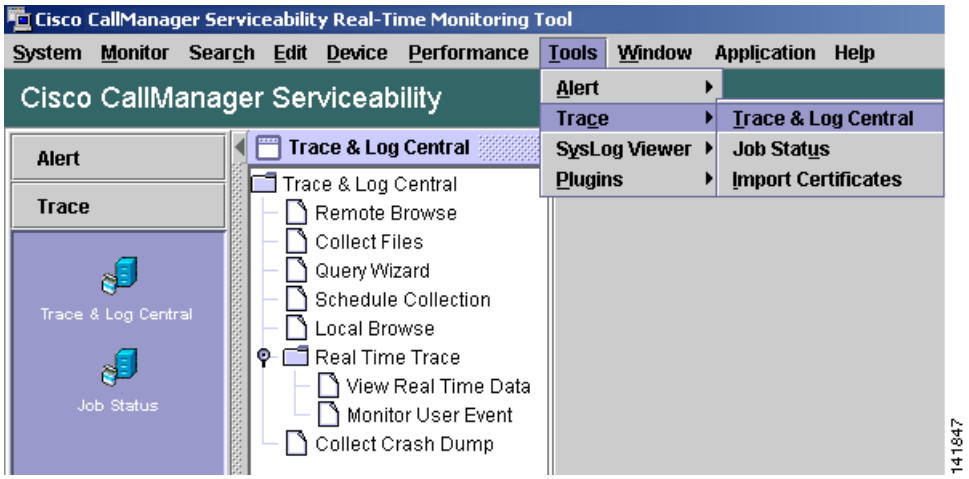
一般的なトラブルシューティング作業

ログおよびトレース ファイルを収集する方法

GUI

RTMT クライアント アプリケーションを使用して、**Tools** タブに移動し、**Trace & Log Central** を選択して、各種のトレース ユーティリティを表示します。

図 2-1　Cisco Unified CallManager RTMT の Trace & Log Central



CLI

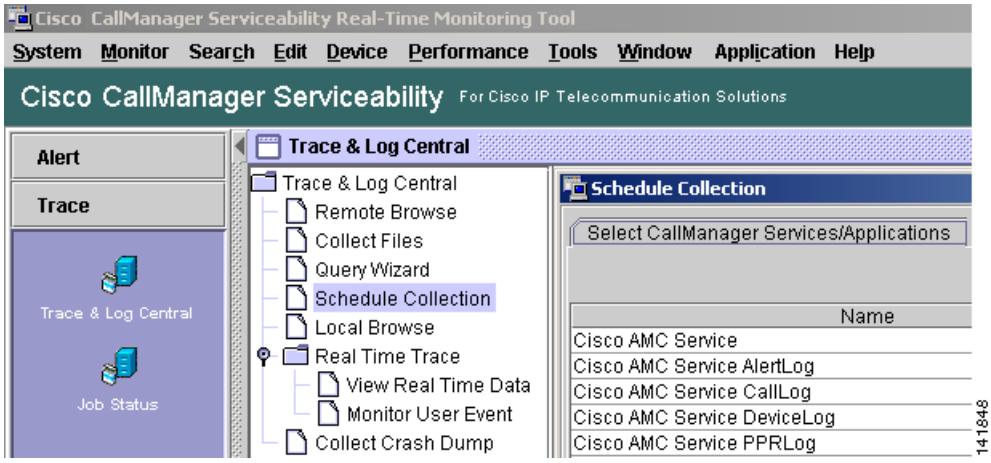
- file list
- file get
- file view

ログおよびトレース ファイルの収集スケジュールを設定する方法

GUI

RTMT クライアント アプリケーションを使用して、**Tools** タブに移動し、**Trace & Log Central** > **Schedule Collection** を選択します。

図 2-2　Cisco Unified CallManager RTMT の Schedule Collection



データベースにアクセスする方法

CLI

admin としてログインし、次のいずれかの **show** コマンドを使用します。

- show tech database
- show tech dbinuse
- show tech dbschema
- show tech devdefaults
- show tech gateway
- show tech locales
- show tech notify
- show tech procedures
- show tech routepatterns
- show tech routeplan
- show tech systables
- show tech table
- show tech triggers
- show tech version
- show tech params*

SQL コマンドを実行するには、**run** コマンドを使用します。

- run <sql command>

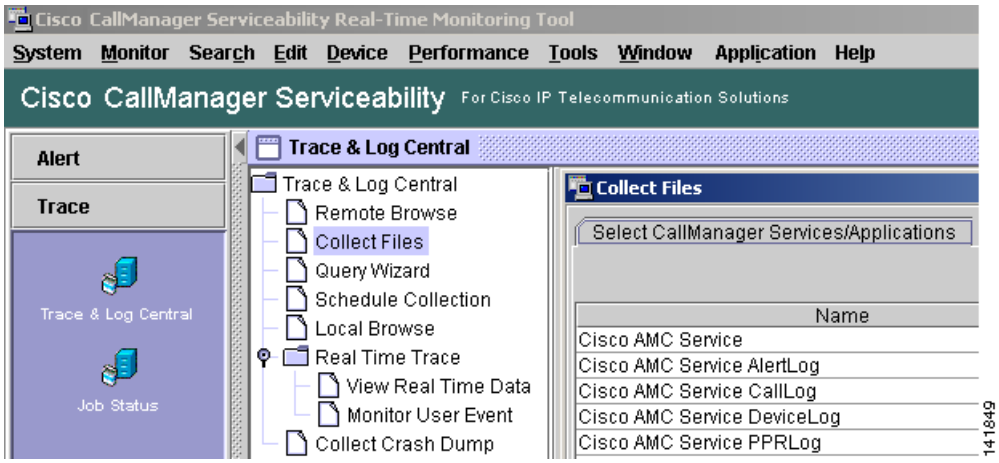
ハードディスクの空き容量を増やす方法

Log パーティションにあるファイルのみ、削除することができます。

GUI

RTMT クライアント アプリケーションを使用して、**Tools** タブに移動し、**Trace & Log Central** > **Collect Files** を選択します。

図 2-3　Cisco Unified CallManager RTMT の Collect Files



収集するファイルの選択基準を選択し、**Delete Files** オプションのチェックボックスをオンにします。この操作を実行すると、ファイルが PC にダウンロードされ、Cisco Unified CallManager サーバ上のファイルは削除されます。

CLI

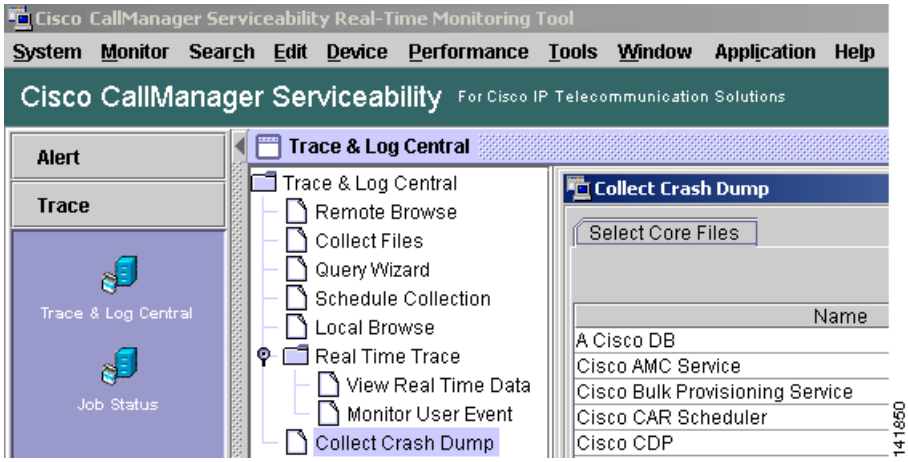
- file delete

コア ファイルを表示する方法

GUI

コア ファイルは表示できませんが、RTMT アプリケーションを使用して **Trace & Log Central > Collect Crash Dump** を選択すると、コア ファイルをダウンロードできます。

図 2-4　Cisco Unified CallManager RTMT の Collect Crash Dump



CLI

- Core［options..］

Cisco Unified CallManager サーバをリブートする方法

GUI

サーバ上でプラットフォームの管理 Web ページにログインし、**Restart > Current Version** に移動します。

CLI

- utils system restart

トレースのデバッグ レベルを変更する方法

GUI

サービスアビリティの Web ページ（https://<server_ipaddress>:8443/ccmservice/）にログインし、**Trace > Configuration** に移動します。

CLI

- set trace enable [Detailed, Significant, Error, Arbitrary, Entry_exit, State_Transition, Special] [syslogmib, cdpmib, dbl, dbnotify]

ネットワークのステータスを表示する方法

GUI

なし

CLI

- show network status

トラブルシューティングのヒント

次のヒントは、Cisco Unified CallManager のトラブルシューティングに役立ちます。

ヒント　Cisco Unified CallManager のリリース ノートで既知の問題を確認します。リリース ノートには、既知の問題の説明と対応策が記載されています。

ヒント　デバイスの登録先を確認します。

各 Cisco Unified CallManager ログはファイルをローカルでトレースします。電話機またはゲートウェイが特定の Cisco Unified CallManager に登録されている場合、コールがそこで開始されると、コール処理がその Cisco Unified CallManager で実行されます。問題をデバッグするには、その Cisco Unified CallManager 上のトレースを取り込む必要があります。

デバイスがサブスクライバ サーバに登録されているにも関わらず、パブリッシャ サーバ上のトレースを取り込むという間違いがよくあります。そのトレース ファイルはほとんど空です（そのファイルには目的のコールがまったく含まれていません）。

デバイス 1 を CM1 に登録し、デバイス 2 を CM2 に登録しているために問題が生じることも多くあります。デバイス 1 がデバイス 2 をコールすると CM1 でコール トレースが実行され、デバイス 2 がデバイス 1 をコールすると CM2 でトレースが実行されます。双方向のコール問題のトラブルシューティングを行う場合は、トラブルシューティングに必要なすべての情報を得るために、両方の Cisco Unified CallManager からの両方のトレースが必要となります。

ヒント　問題のおおよその時刻を認識します。

複数のコールが発信された可能性があるため、コールのおおよその時刻を認識していると、TAC が問題を迅速に特定するのに役立ちます。

アクティブなコール中に **i** ボタンを 2 回押すと、Cisco Unified IP Phone 79xx 上で統計情報を取得できます。

テストを実行して問題を再現し、情報を生成する場合は、問題を理解するために不可欠な次のデータを確認してください。

- 発信側の番号または着信側の番号
- 特定のシナリオに関係する他の番号
- コールの時刻

（注）　トラブルシューティングには、すべての機器の時刻が同期化されていることが重要であることに注意してください。

問題を再現している場合は、ファイルの変更日付とタイムスタンプを調べて、その時間枠のファイルを選択します。適切なトレースを収集する最良の方法は、問題を再現してからすぐに最新のファイルを見つけ、そのファイルを Cisco Unified CallManager サーバからコピーすることです。

ヒント　ログ ファイルを保存して、上書きされないようにします。

ファイルは、時間が経つと上書きされます。ログが記録されているファイルを調べる唯一の方法は、メニューバーで[**表示**]>[**最新の情報に更新**]を選択し、ファイルの日付と時刻を確認することです。

Cisco Unified CallManager サービスが動作していることの確認

サーバ上で Cisco CallManager サービスがアクティブであることを確認するには、次の手順を実行します。

手順

ステップ 1　Cisco Unified CallManager の管理ページの［**ナビゲーション**］で［**Cisco Unified CallManager のサービスアビリティ**］を選択します。

ステップ 2　**Tools > Service Activation** を選択します。

ステップ 3　Servers カラムから、サーバを選択します。

選択したサーバが Current Server というタイトルの隣に表示され、設定済みのサービスを示す一連のボックスが表示されます。

Cisco CallManager 行の Activation Status カラムに、Activated または Deactivated と表示されます。

Activated　というステータスが表示されている場合、選択したサーバ上で、指定した Cisco CallManager サービスがアクティブです。

Deactivated というステータスが表示されている場合は、引き続き次のステップを実行します。

ステップ 4　目的の Cisco CallManager サービスのチェックボックスをオンにします。

ステップ 5　**Update** ボタンをクリックします。

指定した Cisco CallManager サービス行の Activation Status カラムに **Activated** と表示されます。

これで、選択したサーバ上の指定した Cisco CallManager サービスがアクティブになりました。

Cisco CallManager が使用されているかどうか、および現在動作しているかどうかを確認するには、次の手順を実行します。

手順

ステップ 1　Cisco Unified CallManager の管理ページの［**ナビゲーション**］で［**Cisco Unified CallManager のサービスアビリティ**］を選択します。

Cisco Unified CallManager Serviceability ウィンドウが表示されます。

ステップ 2　**Tools > Control Center – Feature Services** を選択します。

ステップ 3　Servers カラムから、サーバを選択します。

選択したサーバが Current Server というタイトルの隣に表示され、設定済みのサービスを示すボックスが表示されます。

Status カラムに、選択したサーバでどのサービスが動作しているかが表示されます。

その他の情報

参考資料

- *Cisco Unified CallManager Serviceability アドミニストレーション ガイド*
- *Cisco Unified CallManager Serviceability システム ガイド*
- *Cisco Unified CallManager アドミニストレーション ガイド*
- *Cisco Unified CallManager セキュリティ ガイド*
- *Cisco Unified CallManager インストレーション ガイド*