CHAPTER 2

トラブルシューティング ツール

この章では、Cisco Unified Communications Manager 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。

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

次に示す各種ツールの詳細については、『*Cisco Unified Serviceability アドミニストレーション ガイド*』を参照してください。これらのツールは、多様な Cisco Unified Communications Manager システムを監視および分析するために、Cisco Unified Serviceability により提供されます。

表 2-1　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 Communications Manager の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し、管理者がトレースを収集できる、サービスアビリティのプログラムを示します。 パフォーマンス カウンタは、システム固有のものも Cisco Unified Communications Manager 固有のものもあります。オブジェクトは、Cisco Unified IP Phone や Cisco Unified Communications Manager 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構成されます。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。
アラーム	管理者は、アラームを使用して、Cisco Unified Communications Manager 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、説明や推奨処置など、システムの問題に関する情報が含まれています。 管理者は、アラーム定義データベースを検索して、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処置が含まれています。
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 Unified Communications Manager サービスの問題に関する特定の情報を取得します。Cisco Unified Serviceability は、設定されているトレース情報をトレース ログ 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。 すべてのサービスには、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。 SDL トレース ログ ファイルには、Cisco CallManager や Cisco CTIManager などのサービスからのコール処理情報が含まれています。システムは、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。
品質レポート ツール	この用語は、Cisco Unified Serviceability 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。

コマンドライン インターフェイス

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 Communications Manager システムにアクセスするには、Command Line Interface（CLI; コマンドライン インターフェイス）を使用します。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、コマンドの集合で構成されます。たとえば、***show*** はレベルを表し、***show status*** はコマンドを表します。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 Communications Manager の CLI コマンド セットの詳細については、『*Cisco Unified Communications Operating System アドミニストレーション ガイド*』を参照してください。

CiscoWorks2000

CiscoWorks2000 は、Cisco Unified Communications Manager 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 Communications Manager 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、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 Communications Manager サーバからログ メッセージを収集します。

これら 2 つのシスコ アプリケーションは連動し、シスコ 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。

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 Communications Manager サーバを検出および管理できます。

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 Communications Manager と互換性があります。
  - CiscoWorks2000
  - HP OpenView
  - SNMP および Cisco Unified Communications Manager SNMP インターフェイスをサポートするサードパーティ製アプリケーション

スニファ 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、またはスニファを装備した他のデバイスを接続することにより、スニファ 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、スニファ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 Communications Manager 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。

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。

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 Communications Manager 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 Communications Manager ノードの監視およびトラブルシューティングをリモートで行うことができます。

（注）　シスコでは、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。

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 Communications Manager 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 Communications Manager 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。
- メディア暗号鍵関連情報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 Communications Manager セキュリティ ガイド*』を参照してください。

パケット キャプチャ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 2-2 に示す作業を行います。

表 2-2　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.2-7）
ステップ 2	Cisco Unified Communications Manager 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.2-8）
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.2-9） • 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.2-10） • パケット キャプチャの設定値（P.2-11）
ステップ 4	該当するデバイス間でスニファ トレースを使用して、SRTP パケットをキャプチャします。	使用しているスニファ トレース ツールに対応したマニュアルを参照
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.2-8） • パケット キャプチャの設定値（P.2-11）
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.2-12）
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.2-12）

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 Communications Manager アドミニストレーション ガイド*』の説明に従って、Cisco Unified Communications Manager 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 Communications Manager 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 Communications Manager 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 Communications Manager の管理ページで、**［システム］> ［サービスパラメータ］**を選択します。

ステップ 2　［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.2-9）
- 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.2-10）

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 Communications Manager 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.2-7 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 Communications Manager 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 2-3 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 Communications Manager 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スニファ トレースを使用して、SRTP パケットをキャプチャします。

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

P.2-12 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 Communications Manager 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.2-7 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 Communications Manager 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 Communications Manager 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 Communications Manager 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 Communications Manager 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 Communications Manager 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 2-3 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 Communications Manager 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スニファ トレースを使用して、SRTP パケットをキャプチャします。

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

P.2-12 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 2-3 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.2-9）
- 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.2-10）

表 2-3　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 Communications Manager 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 Communications Manager 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 Communications Manager 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。ファイルの保管先は、PktCap 仮想ディレクトリです。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スニファ トレースを使用して、SRTP パケットをキャプチャする必要があります。
［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スニファ トレースを使用して、SRTP パケットをキャプチャしてください。次の情報を収集したら、TAC 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 Communications Manager セキュリティ ガイド*』を参照してください。

一般的なトラブルシューティングの作業、ツール、およびコマンド

この項は、ルート アクセスが無効になっている Cisco Unified Communications Manager 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。表 2-4 に、システムのさまざまな問題をトラブルシューティングするための情報収集に使用できる CLI コマンドおよび GUI 選択オプションの要約を示します。

表 2-4　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 <プロセスのタスク名>
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］を選択	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

表 2-5 に、一般的な問題と、そのトラブルシューティングに使用するツールのリストを示します。

表 2-5　CLI コマンドおよび GUI 選択オプションによる一般的な問題のトラブルシューティング

作業	GUI ツール	CLI コマンド
データベースにアクセスする。	なし	admin としてログインし、次のいずれかの **show** コマンドを使用します。 • show tech database • show tech dbinuse • show tech dbschema • show tech devdefaults • show tech gateway • show tech locales • show tech notify • show tech procedures • show tech routepatterns • show tech routeplan • show tech systables • show tech table • show tech triggers • show tech version • show tech params* SQL コマンドを実行するには、**run** コマンドを使用します。 • run <SQL コマンド>
ディスクの空き容量を増やす。 （注） Log パーティションにあるファイルのみ、削除することができます。	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。 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 Communications Manager サーバ上のファイルは削除されます。	file delete
コア ファイルを表示する。	コア ファイルは表示できませんが、RTMT アプリケーションを使用して［**Trace & Log Central**］>［**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。	Core［options..］
Cisco Unified Communications Manager サーバをリブートする。	サーバ上でプラットフォームの管理ページにログインし、［**Restart**］ > ［**Current Version**］に移動します。	utils system restart

表 2-5　CLI コマンドおよび GUI 選択オプションによる一般的な問題のトラブルシューティング（続き）

作業	GUI ツール	CLI コマンド
トレースのデバッグ レベルを変更する。	Cisco Unified Serviceability（https://<サーバの IP アドレス >:8443/ ccmservice/）にログインし、**[Trace] > [Configuration]** を選択します。	set trace enable［Detailed, Significant, Error, Arbitrary, Entry_exit, State_Transition, Special］［syslogmib, cdpmib, dbl, dbnotify］
ネットワークのステータスを表示する。	なし	show network status

トラブルシューティングのヒント

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

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

ヒント　デバイスの登録先を確認します。

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

デバイスがサブスクライバ サーバに登録されているにも関わらず、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 Communications Manager からの両方のトレースが必要となります。

ヒント　問題のおおよその時刻を認識します。

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**］または［**?**］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 Communications Manager サーバからコピーすることです。

ヒント　ログ ファイルを保存して、上書きされないようにします。

ファイルは、時間が経つと上書きされます。ログが記録されているファイルを調べる唯一の方法は、メニューバーで［**表示**］>［**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 Communications Manager 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 Communications Manager の管理ページから、**［ナビゲーション］>［Cisco Unified 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　［Server］カラムから、サーバを選択します。

選択したサーバが Current Server というタイトルの隣に表示され、設定済みのサービスを示す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のままになっています。

［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サービスがアクティブになりました。

Cisco CallManager サービスがアクティブであるかどうか、およびサービスが現在動作しているかどうかを確認するには、次の手順を実行します。

手順

ステップ 1　Cisco Unified Communications Manager の管理ページから、**［ナビゲーション］>［Cisco Unified サービスアビリティ］**を選択します。

［Cisco Unified Communications Manager 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　［Server］カラムから、サーバを選択します。

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

［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。