トラブルシューティング ツール

ここでは、Unified Communications Managerの設定、監視、およびトラブルシューティングを行うために使用するツールやユーティリティについて説明し、テストの繰り返しや同一データの再収集を回避するためのデータ収集に関する一般的なガイドラインを提供します。

（注） このマニュアルにリストされているURLサイトの一部にアクセスするには、登録ユーザとしてログインする必要があります。

- Cisco Unified Serviceability トラブルシューティング ツール （1 ページ）
- コマンドライン インターフェイス （3 ページ）
- Kerneldump ユーティリティ （3 ページ）
- ネットワーク管理 （6 ページ）
- スニファ トレース （7 ページ）
- デバッグ （8 ページ）
- Cisco Secure Telnet （8 ページ）
- パケット キャプチャ （9 ページ）
- 一般的なトラブルシューティングのタスク、ツール、およびコマンド （16 ページ）
- トラブルシューティングのヒント （19 ページ）
- システム履歴ログ （21 ページ）
- 監査ロギング （24 ページ）
- Cisco Unified Communications Manager サービスが稼働しているかどうかの確認 （29 ページ）

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

Cisco Unified Serviceabilityには、さまざまなUnified Communications Managerシステムを監視および分析するために、次のような各種ツールが用意されています。これらのツールの詳細については、『*Cisco Unified Serviceability* アドミニストレーション ガイド』を参照してください。

表 *1 : Serviceability* ツール

用語	定義
Cisco Unified Real-Time Monitoring Tool（RTMT）	このツールは、Unified Communications Managerのデバイスとパフォーマンス カウンタに関するリアルタイムな情報を提供するとともに、トレースの収集を可能にします。 パフォーマンス カウンタは、システム固有か、またはUnified Communications Manager固有である場合があります。 オブジェクトは、Cisco Unified IP 電話 や Unified Communications Manager などの、特定のデバイスまたは機能に対する同等のカウンタの論理的なグループで構成されています。 カウンタによって、システム パフォーマンスのさまざまな側面が測定されます。 登録済み電話機の数、試行されたコール数、進行中のコール数などの統計が測定されます。
アラーム	管理者は、アラームを使用して、Unified Communications Manager システムの実行時のステータスや状態情報を取得します。アラームには、説明や推奨処置など、システムの問題に関する情報が含まれています。 管理者は、アラーム定義データベースでアラーム情報を検索します。アラーム定義には、アラームの説明と推奨処置が含まれています。
トレース	管理者とシスコのエンジニアは、トレース ファイルを使用して、Unified Communications Managerシステムの問題に関する特定の情報を取得します。Cisco Unified Serviceabilityは設定されたトレース情報をトレース ログファイルに送信します。 トレース ログ ファイルには、SDI と SDL の 2 種類があります。 各サービスには、デフォルトのトレース ログが含まれています。 システムによって、サービスからのシステム診断インターフェイス（SDI）情報がトレースされ、実行時のイベントとトレースがログ ファイルに記録されます。 SDL トレース ログ ファイルには、Cisco CallManager や Cisco CTIManager などのサービスからのコール処理情報が含まれています。システムによって、コールの信号配信レイヤ（SDL）がトレースされ、状態遷移がログ ファイルに記録されます。 （注） 通常は、Cisco Technical Assistance Center（TAC）の指示に従って、SDL トレースだけを収集することになります。
品質レポート ツール	この用語は、Cisco Unified Serviceability の音声品質と一般的な問題をレポートするユーティリティを示しています。

用語	定義
Serviceability Connector	Cisco Webex Serviceability サービスは、シスコのテクニカル サポート スタッフがより迅速にインフラストラクチャの問題を診断できます。診断ログや情報を検索、取得、保存するタスクを SR ケースに自動化します。 このサービスは、TAC がオンプレミスの機器の問題を効率的に特定し、解決できるよう、診断署名に対する分析をトリガーします。

コマンドライン インターフェイス

コマンドライン インターフェイス（CLI）を使用すると、Unified Communications Manager システムにアクセスし、基本的なメンテナンスや障害からの回復を行うことができます。ハードワイヤされた端末（システム モニタとキーボード）を使用するか、または SSH セッションを実行することによってシステムにアクセスします。

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

コマンドとは、システムに特定の機能を実行させるテキスト命令を表します。 コマンドは、単独で使用される場合と、必須または任意の引数を伴う場合があります。

レベルは、コマンドの集合で構成されます。たとえば、show はレベルを示し、show status はコマンドを示します。 また、各レベルとコマンドには、特権レベルが関連付けられています。ユーザは、適切な特権レベルを持っている場合にだけ、コマンドを実行できます。

Unified Communications Managerの CLI コマンド セットの詳細については、『*Cisco Unified* ソリューション コマンドライン インターフェイス リファレンス ガイド』を参照してください。

Kerneldump ユーティリティ

Kerneldump ユーティリティにより、セカンダリ サーバを要求することなしに、該当するマシンでクラッシュ ダンプ ログをローカルに収集できます。

Unified Communications Managerクラスタでは、Kerneldump ユーティリティがサーバで有効であることを確認するだけで、クラッシュ ダンプ情報を収集できます。

（注） シスコでは、より効果的なトラブルシューティングを実現するため、Unified Communications Managerのインストール後に、Kerneldump ユーティリティが有効であることを確認するよう推奨しています。 Kerneldump ユーティリティの設定をまだ行っていない場合は、Unified Communications Managerをサポート対象のアプライアンス リリースからアップグレードする前に行ってください。

重要 Kerneldump ユーティリティをイネーブル化またはディセーブル化を行うには、ノードのリブートが必要です。 リブートが許容されるウィンドウ以外では、enable コマンドを実行しないでください。

Cisco Unified Communications オペレーティング システムのコマンドライン インターフェイス（*CLI*）を使用すると、Kerneldump ユーティリティのイネーブル化、ディセーブル化、ステータス確認を実行できます。

次の手順を利用して Kerneldump ユーティリティをイネーブル化します。

ユーティリティによって収集されるファイルの処理

Kerneldump ユーティリティから送信されたクラッシュ情報を表示するには、*Cisco Unified Real-Time Monitoring Tool* またはコマンドライン インターフェイス（*CLI*）を使用します。 *Cisco Unified Real-Time Monitoring Tool* を使用して netdump ログを収集するには、[トレースおよびログ セントラル（Trace & Log Central）] の [ファイルの収集（Collect Files）] オプションを選択します。 [システム サービス/アプリケーションの選択（Select System Services/Applications）] タブで、[Kerneldump ログ（Kerneldump logs）] チェックボックスをオンにします。 *Cisco Unified Real-Time Monitoring Tool* を使用したファイルの収集の詳細については、『*Cisco Unified Real-Time Monitoring Tool Administration Guide*』を参照してください。

CLI を使用して kerneldump ログを収集するには、クラッシュ ディレクトリのファイルに対して「「file」」CLI コマンドを使用します。 これらは 「activelog」 のパーティションの下にあります。 ログ ファイル名は、kerneldump クライアントの IP アドレスで始まり、ファイルが作成された日付で終わります。 ファイル コマンドの詳細については、『*Command Line Interface Reference Guide for Cisco Unified Solutions*』を参照してください。

Kerneldump ユーティリティの有効化

次の手順を利用して Kerneldump ユーティリティをイネーブル化します。 カーネル クラッシュが発生した場合、ユーティリティは、クラッシュの収集とダンプのメカニズムを提供します。 ローカル サーバまたは外部サーバにログをダンプするユーティリティを設定できます。

手順

ステップ 1 コマンドライン インターフェイスにログインします。

ステップ 2 次のいずれかを実行します。

- ローカルサーバー上のカーネルクラッシュを破棄するには、`utils os kerneldump enable` CLI コマンドを実行します。
- 外部サーバにカーネルクラッシュをダンプするには、外部サーバの IP アドレスを指定して `utils os kerneldump ssh enable <ip_address>` CLI コマンドを実行します。

ステップ 3 サーバをリブートします。

例

（注） kerneldumpユーティリティを無効にする必要がある場合、`utils os kernelcrash disable` コマンドを実行してローカルサーバのコアダンプを無効にし、`utils os kerneldump ssh disable <ip_address>`CLIコマンドを実行して外部サーバ上のユーティリティを無効にします。

次のタスク

コア ダンプの指示に従ってリアルタイム モニタリング ツールで電子メール アラートを設定します。 詳細は、コア ダンプの電子メール アラートの有効化を参照してください。

kerneldumpユーティリティおよびトラブルシューティングについては、『*Troubleshooting Guide for Cisco Unified Communications Manager*』を参照してください。

コア ダンプの電子メール アラートの有効化

コア ダンプが発生するたびに管理者に電子メールを送信するようにリアルタイム モニタリング ツールを設定するには、次の手順を使用します。

手順

ステップ 1 **[システム（System）]**>**[ツール（Tools）]**>**[アラート（Alert）]**>**[アラートセントラル（Alert Central）]**の順に選択します。

ステップ 2 [CoreDumpFileFound]アラートを右クリックし、[アラート/プロパティの設定（Set Alert/Properties）]を選択します。

ステップ 3 ウィザードの指示に従って優先条件を設定します。

a) [アラート プロパティ：電子メール通知（Alert Properties: Email Notification）] ポップアップで、[電子メールの有効化（電子メールの有効化(Enable Email)）] がオンになっていることを確認し、[設定（Configure）]をクリックしてデフォルトのアラートアクションを設定します。これにより管理者に電子メールが送信されます。

b) プロンプトに従って、受信者電子メールアドレスを**[追加（Add）]**します。 このアラートがトリガーされると、デフォルトのアクションは、このアドレスへの電子メールの送信になります。

c) **[保存]** をクリックします。

ステップ 4 デフォルトの電子メールサーバーを設定します。

a) **[システム（System）] > [ツール（Tools）] > [アラート（Alert）] > [電子メールサーバーの設定（Config Email Server）]** の順に選択します。
b) 電子メールサーバーとポート情報を入力して、電子メールアラートを送信します。
c) **[送信するユーザー ID（Send User Id）]** を入力します。
d) **OK**をクリックします。

ネットワーク管理

Unified Communications Manager のリモート有用性には、ネットワーク管理ツールを使用します。

- システム ログ管理
- Cisco Discovery Protocol のサポート
- 簡易ネットワーク管理プロトコル（SNMP）のサポート

これらのネットワーク管理ツールの詳細については、それぞれの項に記載された URL にあるマニュアルを参照してください。

システム ログ管理

Resource Manager Essentials（RME）にパッケージされている Cisco Syslog Analysis は、他のネットワーク管理システムにも適応可能ですが、シスコ デバイスから送信される Syslog メッセージの管理に最適な方法を提供します。

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

これら 2 つの Cisco アプリケーションが連動し、Cisco Unified Communication ソリューションの集中型システム ログ サービスを提供します。

RME のマニュアルについては、次の URL を参照してください。
http://www.cisco.com/en/US/products/sw/cscowork/ps2073/products_tech_note09186a00800a7275.shtml

Cisco Discovery Protocol のサポート

Cisco Discovery Protocol がサポートされているため、 Unified Communications Managerサーバの検出および管理が可能です。

RME のマニュアルについては、次の URL を参照してください。
http://www.cisco.com/en/US/products/sw/cscowork/ps2073/products_tech_note09186a00800a7275.shtml

簡易ネットワーク管理プロトコル（SNMP）のサポート

ネットワーク管理システム（NMS）では、業界標準インターフェイスである SNMP を使用して、ネットワーク デバイス間で管理情報が交換されます。 TCP/IP プロトコル スイートの一部である SNMP を使用すると、管理者はリモートでネットワークのパフォーマンスを管理し、ネットワークの問題を検出および解決し、ネットワークの拡張計画を立てることができます。

SNMP管理のネットワークは、管理対象デバイス、エージェント、およびネットワーク管理システムという 3 つの主要コンポーネントで構成されています。

- 管理対象デバイスは、SNMPエージェントを含み、管理対象ネットワークに存在するネットワーク ノードを指します。 管理対象デバイスには管理情報が収集および格納され、その情報は SNMP を使用することによって利用可能になります。
- エージェントは、ネットワーク管理ソフトウェアとして、管理対象デバイスに存在します。エージェントには、管理情報のローカルな知識が蓄積され、SNMP と互換性のある形式に変換されます。
- ネットワーク管理システムは、SNMP管理アプリケーションと、そのアプリケーションが実行されるコンピュータで構成されています。 NMS では、管理対象デバイスをモニタおよび制御するアプリケーションが実行されます。 ネットワーク管理に必要な処理とメモリリソースの大部分は、NMS によって提供されます。 次の NMS は Unified Communications Manager と互換性を持っています。
  - CiscoWorks Common Services Software
  - HP OpenView
  - SNMP および Unified Communications Manager SNMP インターフェイスをサポートしているサードパーティ製アプリケーション

スニファ トレース

通常、スニファ トレースは、VLANまたは問題の情報が含まれるポート（CatOS、Cat6K-IOS、XL-IOS）にまたがるように設定されたCatalystポートに、ラップトップやその他のスニファ搭載デバイスを接続することによって収集します。利用可能なポートが空いていない場合は、スニファ搭載デバイスを、スイッチとデバイスの間に挿入されるハブに接続します。

ヒント TAC のエンジニアがトレースを読解しやすいように、TAC で広く使用されている Sniffer Pro ソフトウェアを使用することを推奨します。

IP Phone、ゲートウェイ、Unified Communications Manager など、関連するすべての装置の IP/MAC アドレスを利用可能にしておいてください。

デバッグ

debug 特権 EXEC コマンドの出力は、プロトコルのステータスおよびネットワーク アクティビティ全般に関する、さまざまなネットワーク間イベントについての診断情報を提供します。

端末エミュレータ ソフトウェア（ハイパーターミナルなど）を設定し、デバッグ出力をファイルに取得できるようにしてください。 ハイパーターミナルで、**[転送（Transfer）]**をクリックし、**[テキストのキャプチャ（Capture Text）]**をクリックして、適切なオプションを選択します。

IOS 音声ゲートウェイ デバッグを実行する前に、**servicetimestampsdebugdatetimemsec** がゲートウェイでグローバルに設定されていることを確認してください。

（注） 運用時間中にライブ環境でデバッグを収集することは避けてください。

運用時間外にデバッグを収集することを推奨します。 ライブ環境でデバッグを収集する必要がある場合は、**no logging console** oy**loggingbuffered**を設定します。 デバッグを収集するには、**show log** を使用します。

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

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

Cisco Secure Telnet

シスコ サービス エンジニア（*CSE*）は、Cisco Secure Telnet を使用して、サイト上のUnified Communications Managerノードに対して透過的にファイアウォール アクセスを実行できます。*Cisco Secure Telnet* は、強力な暗号化を使用して、シスコ内の特別な Telnet クライアントを、ファイアウォールの内側にある Telnetデーモンに接続できます。 このセキュアな接続により、ファイアウォールを変更せずに、Unified Communications Managerノードの監視およびトラブルシューティングをリモートで行うことができます。

（注） シスコは、お客様の承諾を得た場合にだけこのサービスを提供します。 サイトに、このプロセスの開始を支援するネットワーク管理者を配置する必要があります。

パケット キャプチャ

ここでは、パケット キャプチャについて説明します。

関連トピック

パケット キャプチャの概要 （9 ページ）
パケット キャプチャの設定チェックリスト （9 ページ）
Standard Packet Sniffer Users アクセス コントロールグループへのエンドユーザの追加 （10 ページ）
パケット キャプチャのサービス パラメータの設定 （11 ページ）
[電話の設定（Phone Configuration）] ウィンドウでのパケット キャプチャの設定 （12 ページ）
[ゲートウェイの設定（Gateway Configuration）] ウィンドウおよび [トランクの設定（Trunk Configuration）] ウィンドウでのパケット キャプチャの設定 （13 ページ）
パケット キャプチャの構成設定 （14 ページ）
キャプチャしたパケットの分析 （16 ページ）

パケット キャプチャの概要

メディアや TCP パケットをスニフィングするサードパーティ製トラブルシューティング ツールは、暗号化をイネーブルにしたあとは機能しません。このため、問題が発生した場合は、Unified Communications Managerを使用して次のタスクを行う必要があります。

- Unified Communications Manager とデバイスとの間で交換されるメッセージのパケットの分析（Cisco Unified IP 電話[SIP と SCCP]、Cisco IOS MGCP ゲートウェイ、H.323 ゲートウェイ、H.323/H.245/H.225 トランク、または SIP トランク）。
- デバイス間の Secure Real Time Protocol（SRTP）パケットのキャプチャ。
- メッセージからのメディア暗号キー情報の抽出、およびデバイス間のメディアの復号化。

ヒント このタスクを複数のデバイスに対して同時に実行すると、CPU使用率が高くなり、コール処理が中断される可能性があります。 このタスクは、コール処理が中断される危険性が最も少ないときに実行することを強く推奨します。

詳細については、Cisco Unified Communications Manager セキュリティガイドを参照してください。

パケット キャプチャの設定チェックリスト

必要なデータを抽出し、分析するには、次の作業を実行します。

手順

1. エンド ユーザを Standard Packet Sniffer Users グループに追加します。
2. Cisco Unified Communications Manager Administrationの [サービス パラメータ設定（Service Parameter Configuration）] ウィンドウで、パケット キャプチャのサービス パラメータを設定します。たとえば、Packet Capture Enable サービス パラメータを設定します。
3. [電話の設定（Phone Configuration）]、[ゲートウェイの設定（Gateway Configuration）]、または [トランクの設定（Trunk Configuration）] の各ウィンドウで、デバイスごとのパケット キャプチャの設定を行います。

（注） パケット キャプチャは、複数のデバイスで同時にはイネーブルにしないことを強く推奨します。このタスクによって、ネットワークで使用されている CPU の使用率が上昇する可能性があるためです。

4. 該当するデバイス間でスニファ トレースを使用して、SRTP パケットをキャプチャします。使用しているスニファ トレースツールに対応したマニュアルを参照してください。
5. パケットをキャプチャしたら、Packet Capture Enable サービス パラメータを False に設定します。
6. パケットの分析に必要なファイルを収集します。
7. Cisco Technical Assistance Center（TAC）がパケットを分析します。 このタスクについては、TAC に直接お問い合わせください。

関連トピック

Standard Packet Sniffer Users アクセス コントロールグループへのエンド ユーザの追加 （10 ページ）
キャプチャしたパケットの分析 （16 ページ）
[ゲートウェイの設定（Gateway Configuration）] ウィンドウおよび [トランクの設定（Trunk Configuration）] ウィンドウでのパケット キャプチャの設定 （13 ページ）
[電話の設定（Phone Configuration）] ウィンドウでのパケット キャプチャの設定 （12 ページ）
パケット キャプチャのサービス パラメータの設定 （11 ページ）
パケット キャプチャの構成設定 （14 ページ）

Standard Packet Sniffer Users アクセス コントロールグループへのエンド ユーザの追加

Standard Packet Sniffer Users グループに所属するユーザは、パケット キャプチャをサポートしているデバイスについて、パケット キャプチャ モードとパケット キャプチャ時間を設定できます。 ユーザが Standard Packet Sniffer Users アクセス コントロール グループに含まれていない場合、そのユーザはパケット キャプチャを開始できません。

次の手順では、エンドユーザを Standard Packet Sniffer アクセス制御グループに追加する方法について説明します。この手順では、『Administration Guide for Cisco Unified Communications Manager』の説明に従って、Cisco Unified Communications Manager Administrationでエンド ユーザを設定したことを前提としています。

手順

1. 『Administration Guide for Cisco Unified Communications Manager』の説明に従って、アクセス制御グループを検索します。
2. [検索/リスト（Find/List）] ウィンドウが表示されたら、[標準パケット スニファ ユーザ（Standard Packet Sniffer Users）]リンクをクリックします。
3. [グループにユーザを追加（Add Users to Group）]ボタンをクリックします。
4. 『Administration Guide for Cisco Unified Communications Manager』の説明に従って、エンド ユーザを追加します。
5. ユーザを追加したら、[保存（Save）]をクリックします。

パケット キャプチャのサービス パラメータの設定

パケット キャプチャのパラメータを設定するには、次の手順を実行します。

手順

1. Unified Communications Managerで、**[システム]** > **[サービス パラメータ]** を選択します。
2. [サーバ（Server）] ドロップダウン リスト ボックスで、Cisco CallManager サービスをアクティブにした Active サーバを選択します。
3. [サービス（Service）]ドロップダウン リスト ボックスで、[Cisco CallManager（アクティブ）（Cisco CallManager (Active)）] サービスを選択します。
4. [TLS パケット キャプチャ設定（TLS Packet Capturing Configuration）] ペインまでスクロールして、パケット キャプチャを設定します。

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

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

5. 変更内容を有効にするには、[保存（Save）]をクリックします。
6. パケット キャプチャの設定を続行できます。

関連トピック

[ゲートウェイの設定（Gateway Configuration）] ウィンドウおよび[トランクの設定（Trunk Configuration）] ウィンドウでのパケット キャプチャの設定 （13 ページ）

[電話の設定（Phone Configuration）] ウィンドウでのパケット キャプチャの設定 （12 ページ）

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

[サービス パラメータ（Service Parameter）] ウィンドウでパケット キャプチャをイネーブルにしたら、Cisco Unified Communications Manager Administrationの [電話の設定（Phone Configuration）] ウィンドウで、デバイスごとにパケット キャプチャを設定できます。

電話機ごとに、パケットキャプチャをイネーブルまたはディセーブルにします。パケットキャプチャのデフォルト設定は、None です。

注意 パケットキャプチャは、複数の電話機で同時にはイネーブルにしないことを強く推奨します。このタスクによって、ネットワークで使用されている CPU の使用率が上昇する可能性があるためです。

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

電話機のパケット キャプチャを設定するには、次の手順を実行します。

手順

1. パケット キャプチャを設定する前に、パケット キャプチャの設定に関するトピックを参照してください。
2. Cisco Unified Communications Manager システム設定ガイドの説明に従って、SIP 電話機または SCCP 電話機を検索します。
3. [電話の設定（Phone Configuration）] ウィンドウが表示されたら、「パケット キャプチャの設定値」の説明に従って、トラブルシューティングの設定を行います。
4. 設定が完了したら、[保存（Save）]をクリックします。
5. [リセット（Reset）] ダイアログボックスで、[OK]をクリックします。

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

この他の手順

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

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

関連トピック

キャプチャしたパケットの分析 （16 ページ）
パケット キャプチャの設定チェックリスト （9 ページ）

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

次のゲートウェイおよびトランクは、Unified Communications Managerでのパケット キャプチャをサポートしています。

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

ヒント パケット キャプチャは、複数のデバイスで同時にはイネーブルにしないことを強く推奨します。このタスクによって、ネットワークで使用されている CPU の使用率が上昇する可能性があるためです。

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

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

手順

1. パケット キャプチャを設定する前に、パケット キャプチャの設定に関するトピックを参照してください。
2. 次のいずれかの作業を実行します。
   - Cisco Unified Communications Manager システム設定ガイドの説明に従って、Cisco IOS MGCP ゲートウェイを検索します。
   - Cisco Unified Communications Manager システム設定ガイドの説明に従って、H.323 ゲートウェイを検索します。

- Cisco Unified Communications Manager システム設定ガイドの説明に従って、H.323、H.245、または H.225 トランクを検索します。
- Cisco Unified Communications Manager システム設定ガイドの説明に従って、SIP トランクを検索します。

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

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

4. 「パケット キャプチャの設定値」の説明に従って、トラブルシューティングを設定します。
5. パケット キャプチャを設定したら、[保存（Save）]をクリックします。
6. [リセット（Reset）] ダイアログボックスで、[OK]をクリックします。

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

この他の手順

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

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

関連トピック

キャプチャしたパケットの分析 （16 ページ）
パケット キャプチャの設定チェックリスト （9 ページ）

パケット キャプチャの構成設定

次の表に、ゲートウェイ、トランク、および電話機にパケット キャプチャを設定する際の [パケット キャプチャ モード（Packet Capture Mode）] 設定と [パケット キャプチャ時間（Packet Capture Duration）] 設定について説明します。

設定	説明
[パケットキャプチャモード(Packet Capture Mode)]	暗号化のトラブルシューティング専用の設定。パケット キャプチャリングは、高い CPU 使用率およびコール処理中断の原因となります。 ドロップダウン リスト ボックスから、次のオプションのいずれかを選択します。 • [なし（None）]：このオプションは、パケット キャプチャが発生しないことを示します（デフォルト設定）。 パケット キャプチャが完了すると、Unified Communications Manager は [パケット キャプチャ モード（Packet Capture Mode）] を [なし（None）] に設定します。 • **[バッチ処理モード（Batch Processing Mode）]**：Unified Communications Managerが復号化または非暗号化されたメッセージをファイルに書き込み、システムが各ファイルを暗号化します。 システムは毎日、新しい暗号キーを持つ新しいファイルを作成します。 Unified Communications Manager は 7 日間ファイルを保存しますが、ファイルを暗号化するキーも安全な場所に保存します。Unified Communications Manager はファイルを PktCap 仮想ディレクトリに保存します。 単一のファイルには、タイムスタンプ、送信元 IP アドレス、送信元 IP ポート、宛先 IP アドレス、パケット プロトコル、メッセージ長、およびメッセージが含まれます。 TAC デバッグ ツールは、HTTPS、管理者のユーザ名とパスワード、および指定日を使用して、キャプチャされたパケットを含む単一の暗号化されたファイルを要求します。 さらにキー情報も要求し、暗号化されたファイルを復号化します。 **ヒント** TAC に連絡する前に、該当するデバイス間でスニファ トレースを使用して、SRTP パケットをキャプチャする必要があります。
[パケットキャプチャ時間(Packet Capture Duration)]	暗号化のトラブルシューティング専用の設定。パケット キャプチャリングは、高い CPU 使用率およびコール処理中断の原因となります。 このフィールドには、パケット キャプチャリングの 1 つのセッションに割り当てる最大分数を指定します。 デフォルト設定は 0 です。 ただし、0 ～ 300 分の範囲で指定できます。 パケット キャプチャリングを開始するには、このフィールドに 0 以外の値を入力します。 パケット キャプチャリングの完了後、0 が表示されます。

関連トピック

[ゲートウェイの設定（Gateway Configuration）] ウィンドウおよび [トランクの設定（Trunk Configuration）] ウィンドウでのパケット キャプチャの設定 （13 ページ）

[電話の設定（Phone Configuration）] ウィンドウでのパケット キャプチャの設定 （12 ページ）

キャプチャしたパケットの分析

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

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

詳細については、Cisco Unified Communications Manager セキュリティガイド を参照してください。

一般的なトラブルシューティングのタスク、ツール、およびコマンド

この項では、ルート アクセスが無効にされた Unified Communications Manager サーバのトラブルシューティングに役立つコマンドやユーティリティのクイック リファレンスを提供します。次の表に、システムのさまざまな問題をトラブルシューティングするための情報収集に使用できる CLI コマンドと GUI をまとめます。

表 *2 : CLI* コマンドと *GUI* 選択のまとめ

情報	Linux コマンド	サービスアビリティの GUI ツール	CLI コマンド
CPU 使用率	top	RTMT [表示（View）] タブに移動し、**[サーバ（Server）] > [CPU とメモリ（CPU and Memory）]** を選択	プロセッサ CPU 使用率： show perf query class Processor すべてのプロセスのプロセス CPU 使用率： show perf query counter Process 「% CPU Time」 個々のプロセス カウンタの詳細（CPU 使用率を含む） show perf query instance <Process task_name>
プロセスの状態	ps	RTMT [表示（View）] タブに移動し、**[サーバ（Server）] > [プロセス（Process）]** を選択	show perf query counter Process 「Process Status」
ディスク使用量	df/du	RTMT [表示（View）] タブに移動し、**[サーバ（Server）] > [ディスク使用量（Disk Usage）]** を選択	show perf query counter Partition「% Used」 または show perf query class Partition
メモリ	free	RTMT [表示（View）] タブに移動し、**[サーバ（Server）] > [CPU とメモリ（CPU and Memory）]** を選択	show perf query class Memory
ネットワーク ステータス	netstats		show network status
サーバのリブート	リブート（reboot）	サーバの [プラットフォーム（Platform）] Web ページにログイン **[サーバ（Server）] > [現在のバージョン（Current Version）]** に移動	utils system restart

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
トレース/ログの収集	Sftp、ftp	RTMT [ツール（Tools）] タブに移動し、**[トレース（Trace）] > [トレースおよびログ セントラル（Trace & Log Central）]** を選択	ファイルのリスト：file list ファイルのダウンロード：file get ファイルの表示：file view

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

表 *3 : CLI* コマンドおよび *GUI* 選択オプションによる一般的な問題のトラブルシューティング

タスク	GUI ツール	CLI コマンド
データベースにアクセスする	なし	admin としてログインし、次のいずれかの **show** コマンドを使用します。 • show tech database • show tech dbinuse • show tech dbschema • show tech devdefaults • show tech gateway • show tech locales • show tech notify • show tech procedures • show tech routepatterns • show tech routeplan • show tech systables • show tech table • show tech triggers • show tech version • show tech params* SQL コマンドを実行するには、**run** コマンドを使用します。 • run sql <sql command>

タスク	GUI ツール	CLI コマンド
ディスクの空き容量を増やす （注） Log パーティションにあるファイルだけ、削除できます。	RTMT クライアントアプリケーションを使用して、[ツール（Tools）]タブに移動し、**[トレースおよびログセントラル（Trace & Log Central）]** > **[ファイルの収集（Collect Files）]** を選択します。 収集するファイルの選択基準を選択し、[ファイルの削除（Delete Files）]オプションのチェックボックスをオンにします。 この操作を実行すると、ファイルが PC にダウンロードされ、Unified Communications Manager サーバ上のファイルは削除されます。	file delete
コア ファイルを表示する	コアファイルは表示できませんが、RTMT アプリケーションを使用して **[Trace & Log Central]** > **[クラッシュ ダンプの収集（Collect Crash Dump）]** を選択すると、コア ファイルをダウンロードできます。	utils core [options]
Unified Communications Manager サーバをリブートする	サーバの [プラットフォーム（Platform）]ページにログインし、**[リスタート（Restart）]** > **[現在のバージョン（Current Version）]** に移動します。	utils system restart
トレースのデバッグレベルを変更する	*Cisco Unity Connection Serviceability* Administration（`https://<server_ipaddress>:8443/ccmservice/`）にログインして、**[トレース（Trace）]** > **[設定（Configuration）]**を選択します。	set trace enable [Detailed, Significant, Error, Arbitrary, Entry_exit, State_Transition, Special] [syslogmib, cdpmib, dbl, dbnotify]
ネットワークのステータスを表示する	なし	show network status

トラブルシューティングのヒント

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

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

ヒント　デバイスの登録先を確認します。

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

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

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

ヒント　問題のおおよその時刻を確認します。

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

Cisco Unified IP 電話 79xx の電話機統計情報は、**i** または **?** ボタンをアクティブ コール中に 2 回押すと取得できます。

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

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

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

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

ヒント ログ ファイルを保存して、上書きされないようにします。

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

システム履歴ログ

システム履歴ログを使用すると、システムの初期インストール、システムのアップグレード、Cisco オプションのインストール、DRS バックアップと DRS 復元、バージョン切り替えとリブート履歴などの情報の概要を中央からすばやく把握できます。

関連トピック

システム履歴ログの概要 （21 ページ）
システム履歴ログのフィールド （22 ページ）
システム履歴ログへのアクセス （23 ページ）

システム履歴ログの概要

システム履歴ログは、**system-history.log** という単純な ASCII ファイルとして保管され、そのデータはデータベース内には保持されません。サイズが膨大ではないため、ローテーションされることはありません。

システム履歴ファイルには、次の機能があります。

- サーバ上のソフトウェアの初期インストールを記録します。
- ソフトウェアの各アップデート（Cisco オプション ファイルおよびパッチ）の成功、失敗、またはキャンセルを記録します。
- 実行される各 DRS バックアップと復元を記録します。
- CLI または GUI によって発行されるバージョン切り替えの各呼び出しを記録します。
- CLI または GUI によって発行される再起動およびシャットダウンの各呼び出しを記録します。
- システムの各ブートを記録します。 再起動エントリまたはシャットダウン エントリと関連付けられていない場合のブートは、手動リブート、電源サイクル、またはカーネル パニックの結果として発生したものです。

- 初期インストール以降、または機能が利用可能になって以降のシステム履歴を単一ファイルに保持します。
- インストール フォルダに存在します。 **file** コマンドか、または Real Time Monitoring Tool（RTMT）を使用して、CLI からログにアクセスできます。

システム履歴ログのフィールド

ログには、製品名、製品バージョン、およびカーネルイメージに関する情報を含む、次のような共通のヘッダーが表示されます。

```
==================================

Product Name - Unified Communications Manager

Product Version - 7.1.0.39000-9023

Kernel Image - 2.6.9-67.EL

==================================
```

システム履歴ログの各エントリには、次のようなフィールドがあります。

timestamp userid action description start/result

システム履歴ログのフィールドには、次のような値が含まれます。

- *timestamp*：サーバ上のローカルな日付と時刻が *mm/dd/yyyy hh:mm:ss* の形式で表示されます。
- *userid*：アクションを呼び出したユーザの名前が表示されます。
- *action*：次のいずれかのアクションが表示されます。
  - インストール
  - Windows アップグレード
  - インストール時のアップグレード
  - アップグレード
  - Cisco オプションのインストール
  - バージョン切り替え
  - システム再起動
  - Shutdown
  - Boot
  - DRS バックアップ
  - DRS 復元
- *description*：次のいずれかのメッセージが表示されます。

- *Version*：基本インストール、Windows アップグレード、インストール時のアップグレード、アップグレードの各アクションが表示されます。
- *Cisco Option file name*：Cisco オプションのインストールのアクションが表示されます。
- *Timestamp*：DRS バックアップと DRS 復元の各アクションが表示されます。
- *Active version to inactive version*：バージョン切り替えのアクションが表示されます。
- *Active version*：システム再起動、シャットダウン、およびブートの各アクションが表示されます。

- *result*：次の結果が表示されます。
  - 開始
  - 成功または失敗
  - キャンセル（Cancel）

次に、システム履歴ログの例を示します。

```
admin:file dump install system-history.log=======================================
 Product Name - Cisco Unified Communications Manager Product Version -
6.1.2.9901-117 Kernel Image - 2.4.21-47.EL.cs.3BOOT
======================================= 07/25/2008 14:20:06 | root: Install
6.1.2.9901-117 Start 07/25/2008 15:05:37 | root: Install 6.1.2.9901-117 Success
 07/25/2008 15:05:38 | root: Boot 6.1.2.9901-117 Start 07/30/2008 10:08:56 |
root: Upgrade 6.1.2.9901-126 Start 07/30/2008 10:46:31 | root: Upgrade
6.1.2.9901-126 Success 07/30/2008 10:46:43 | root: Switch Version 6.1.2.9901-117
 to 6.1.2.9901-126 Start 07/30/2008 10:48:39 | root: Switch Version
6.1.2.9901-117 to 6.1.2.9901-126 Success 07/30/2008 10:48:39 | root: Restart
6.1.2.9901-126 Start 07/30/2008 10:51:27 | root: Boot 6.1.2.9901-126 Start
08/01/2008 16:29:31 | root: Restart 6.1.2.9901-126 Start 08/01/2008 16:32:31
| root: Boot 6.1.2.9901-126 Start
```

システム履歴ログへのアクセス

システム履歴ログにアクセスするには、CLI または RTMT を使用できます。

CLI の使用

次のように CLI の **file** コマンドを使用すると、システム履歴ログにアクセスできます。

- **file view install system-history.log**
- **file get install system-history.log**

CLI **ファイル** コマンドの詳細については、『*Command Line Interface Reference Guide for Cisco Unified Communications Solutions*』を参照してください。

RTMT の使用

RTMT を使用してシステム履歴ログにアクセスすることもできます。 [Trace and Log Central] タブで、[インストール ログの収集（Collect Install Logs）]を選択します。

RTMT の使用の詳細については、『*Cisco Unified Real-Time Monitoring Tool Administration Guide*』を参照してください。

監査ロギング

一元化された監査ロギングにより、Unified Communications Manager システムへの設定変更を監査用の別のログ ファイルに記録できます。 監査イベントは、記録する必要があるすべてのイベントを指します。 次の Unified Communications Manager コンポーネントによって監査イベントが生成されます。

- Cisco Unified Communications Manager Administration
- Cisco Unified Serviceability
- *Unified Communications Manager CDR Analysis and Reporting*
- *Cisco Unified Real-Time Monitoring Tool*
- *Cisco Unified Communications Operating System*
- *Disaster Recovery System*
- データベース
- コマンドライン インターフェイス
- Remote Support Account Enabled（テクニカル サポート チームによって発行される CLI コマンド）

Cisco Business Edition 5000 では、次のCisco Unity Connectionコンポーネントによっても監査イベントが生成されます。

- Cisco Unity Connection の管理
- *Cisco Personal Communications Assistant* (Cisco PCA)
- Cisco Unity Connection サービスアビリティ
- Representational State Transfer（REST）API を使用する Cisco Unity Connection クライアント

次に、監査イベントの例を示します。

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

監査イベントに関する情報が含まれている監査ログは、共通のパーティションに書き込まれます。 これらの監査ログのページは、トレース ファイルと同様に、Log Partition Monitor（LPM）によって管理されます。 デフォルトでは、LPM によって監査ログがパージされますが、監査ユーザは Cisco Unified Serviceability の [Audit User Configuration] ウィンドウからこの設定を変更できます。 共通パーティションのディスク使用量がしきい値を超えると、LPM によってアラートが送信されますが、アラートには、ディスクが監査ログまたはトレース ファイルによっていっぱいであるかどうかに関する情報は含まれていません。

ヒント　監査ログをサポートするネットワーク サービスである Cisco Audit Event Service は、Cisco Unified Serviceability のコントロール センターのネットワーク サービスに表示されます。 監査ログへの書き込みが行われない場合は、 Cisco Unified Serviceabilityで **[Tools]** > **[Control Center-Network Services]** を選択し、このサービスを停止してから開始します。

監査ログはすべて、*Cisco Unified Real-Time Monitoring Tool* の Trace and Log Central から収集、表示、および削除されます。 RTMT の Trace and Log Central で監査ログにアクセスします。 **[システム]** > **[リアルタイム トレース]** > **[監査ログ]** > **[ノード]** に移動します。 ノードを選択したら、別のウィンドウに **[システム]** > **[Cisco 監査ログ]** が表示されます。

RTMT には、次のタイプの監査ログが表示されます。

- アプリケーション ログ
- データベース ログ
- オペレーティング システム ログ
- リモート SupportAccEnabled ログ

アプリケーション ログ

RTMT の AuditApp フォルダに表示されるアプリケーション監査ログには、Cisco Unified Communications Manager Administration、Cisco Unified Serviceability、*CLI*、*Cisco Unified* リアルタイム監視ツール（*RTMT*）、ディザスタ リカバリ システム、およびCisco Unified CDR Analysis and Reporting（CAR）の設定変更が記録されます。 *Cisco Business Edition 5000* の場合、アプリケーション監査ログにはCisco Unity Connectionの管理、*Cisco Personal Communications Assistant*（Cisco PCA）、Cisco Unity Connectionのサービスアビリティ、および Representational State Transfer（REST）API を使用するクライアントに対する変更も記録されます。

アプリケーション ログはデフォルトでは有効になっていますが、Cisco Unified Serviceabilityで **[Tools]** > **[Audit Log Configuration]** を選択することによって設定を変更できます。 設定可能な監査ログの設定については、『*Cisco Unified Serviceability Administration Guide*』を参照してください。

Cisco Unified Serviceabilityで監査ログが無効になると、監査ログ ファイルは新規で作成されなくなります。

ヒント　監査のロールを割り当てられたユーザだけが監査ログの設定を変更する権限を持っています。新規のインストールまたはアップグレード後には、デフォルトで CCMAdministrator に監査のロールが割り当てられます。 CCMAdministrator は、監査のために作成した新規ユーザを「「Standard Audit Users」」グループに割り当てることができます。 その後、CCMAdministrator を監査ユーザ グループから削除できます。 「「Standard Audit Log Configuration」」ロールには、監査ログを削除する権限と、*Cisco Unified Real-Time Monitoring Tool*、Trace Collection Tool、RTMT Alert Configuration、[コントロール センターのネットワーク サービス（Control Center - Network Services）] ウィンドウ、RTMT Profile Saving、[監査の設定（Audit Configuration）] ウィンドウ、および Audit Traces という新規リソースへの読み取り/更新権限が与えられます。 *Cisco Business Edition 5000* のCisco Unity Connectionの場合、インストール時に作成されたアプリケーション管理アカウントは、Audit Administrator ロールに割り当てられます。このアカウントは、他の管理者ユーザをこのロールに割り当てることができます。

Unified Communications Manager は、設定された最大ファイル サイズに達するまで、1 つのアプリケーション監査ログ ファイルを使用します。最大ファイル サイズに達すると、そのファイルを閉じ、新規アプリケーション監査ログ ファイルを作成します。 システムでログ ファイルのローテーションが指定されている場合、Unified Communications Manager は設定されている数のファイルを保存します。 ログ イベントの一部は、RTMT SyslogViewer を使用して表示できます。

以下の Cisco Unified Communications Manager Administrationのイベントは、ログに記録されます。

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

以下の Cisco Unified Serviceabilityのイベントは、ログに記録されます。

- Serviceability ウィンドウからのサービスのアクティベーション、非アクティブ化、開始、または停止。
- トレース設定およびアラーム設定の変更。
- SNMP 設定の変更。
- CDR 管理の変更。
- サービスアビリティ レポートのアーカイブのレポートの参照。 このログはレポーター ノードで表示します。

RTMT では、次のイベントが監査イベント アラームとともに記録されます。

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

Unified Communications Manager CDR Analysis and Reporting では、次のイベントが記録されます。

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

ディザスタ リカバリ システムでは、次のイベントが記録されます。

- 開始に成功または失敗したバックアップ
- 開始に成功または失敗した復元
- 正しくキャンセルされたバックアップ
- 完了に成功または失敗したバックアップ

- 完了に成功または失敗した復元
- バックアップ スケジュールの保存、更新、削除、イネーブル化、ディセーブル化
- バックアップの宛先デバイスの保存、更新、削除

Cisco Business Edition 5000 の場合、Cisco Unity Connectionの管理では、次のイベントが記録されます。

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

Cisco Business Edition 5000 の場合、Cisco PCA では、次のイベントが記録されます。

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

Cisco Business Edition 5000 の場合、Cisco Unity Connectionのサービスアビリティ ログでは、次のイベントが記録されます。

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

Cisco Business Edition 5000 の場合、REST API を使用するクライアントでは、次のイベントが記録されます。

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

データベース ログ

RTMT の informix フォルダに表示されるデータベース監査ログでは、データベースの変更がレポートされます。 このログは、デフォルトでは有効になっていませんが、 Cisco Unified Serviceabilityで **[Tools]** > **[Audit Log Configuration]** を選択することによって設定を変更できます。 設定可能な監査ログの設定については、Cisco Unified Serviceabilityを参照してください。

このログは、アプリケーションの設定変更を記録するアプリケーション監査ログとは異なり、データベースの変更を記録します。 Cisco Unified Serviceability でデータベース監査がイネーブルに設定されるまで、informix フォルダは RTMT に表示されません。

オペレーティング システム ログ

RTMT の vos フォルダに表示されるオペレーティング システム監査ログでは、オペレーティング システムによってトリガーされるイベントがレポートされます。 デフォルトでは、イネーブルになっていません。 **utils auditd** CLI コマンドによって、イネーブルまたはディセーブルにしたり、イベントのステータスを提供したりできます。

CLI で監査がイネーブルに設定されるまで、vos フォルダは RTMT に表示されません。

CLI の詳細については、『*Cisco Unified Solutions* コマンドライン インターフェイス リファレンス ガイド』を参照してください。

リモート サポート アカウント イネーブル化ログ

RTMT の vos フォルダに表示されるリモート サポート アカウント イネーブル化ログでは、テクニカル サポート チームによって発行される CLI コマンドがレポートされます。 このログの設定は変更できません。このログは、テクニカル サポート チームによってリモート サポート アカウントがイネーブルに設定された場合にだけ作成されます。

Cisco Unified Communications Manager サービスが稼働しているかどうかの確認

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

手順

1. Cisco Unified Communications Manager Administrationの **[ナビゲーション] メニューで、** > **[Cisco Unified Serviceability]** を選択します。
2. **[ツール（Tools）]** > **[サービス アクティベーション（Service Activation）]** を選択します。
3. [サーバ（Server）] カラムから必要なサーバを選択します。

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

   Cisco CallManager 行の [アクティベーション ステータス（Activation Status）] カラムに、[アクティブ化（Activated）] または [非アクティブ（Deactivated）] と表示されます。

   [アクティブ化（Activated）]というステータスが表示されている場合、選択したサーバ上で、指定した Cisco CallManager サービスがアクティブのままになっています。

   [非アクティブ（Deactivated）]というステータスが表示されている場合は、引き続き次のステップを実行します。
4. 目的の Cisco CallManager サービスのチェックボックスをオンにします。
5. [更新（Update）]ボタンをクリックします。

指定した Cisco CallManager サービス行の [アクティベーション ステータス（Activation Status）] カラムに [アクティブ化（Activated）]と表示されます。

これで、選択したサーバ上の指定したサービスがアクティブになります。

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

手順

1. Cisco Unified Communications Manager Administrationの **[ナビゲーション] メニューで、> [Cisco Unified Serviceability]** を選択します。

   [Cisco Unified サービスアビリティ（Cisco Unified Serviceability）] ウィンドウが表示されます。

2. **[ツール（Tools）] > [コントロール センター - 機能サービス（Control Center - Feature Services）]** の順に選択します。

3. [サーバ（Server）] カラムからサーバを選択します。

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

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

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。