トラブルシューティング ツール

ここでは、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 サービスアビリティ トラブルシューティング ツール

さまざまな Cisco Unified Communications Manager システムを監視および分析するために Cisco Unified サービスアビリティによって提供されている、次の各種ツールの詳細については、『*Cisco Unified Serviceability Administration Guide*』を参照してください。

表 *1*：サービスアビリティのツール

用語	定義
Cisco Unified Real-Time Monitoring Tool（RTMT）	このツールは、Cisco 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 Cisco 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 Phone や Cisco Unified Communications Manager システム パフォーマンスなどの、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、Cisco 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。

用語	定義
トレース（Trace）	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、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 サービスアビリティからトレース ログ ファイルに、設定済みトレース情報が送信されます。 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。
Quality Report Tool	この用語は、Cisco Unified サービスアビリティ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。

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、Cisco 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。

Cisco Unified Communications Manager の CLI コマンド セットの詳細については、『*Command Line Interface Reference Guide for Cisco Unified Solutions*』を参照してください。

netdump ユーティリティ

netdumpユーティリティを使用すると、ネットワーク上の1つのサーバからもう1つのサーバに、データおよびメモリ クラッシュ ダンプ ログを送信することができます。 netdump クライアントとして設定されているサーバから netdump サーバとして設定されているサーバにクラッシュログが送信されます。 ログ ファイルは、netdump サーバのクラッシュ ディレクトリに送信されます。

Cisco Unified Communications Manager クラスタでは、netdump サーバとして少なくとも 2 つのノードを設定し、第 1 ノードと後続ノードの間でクラッシュ ダンプ ログを互いに送信できるようにする必要があります。

たとえば、クラスタに 3 つのサーバ（1 つのプライマリ/第 1 ノードと 2 つの後続ノード）がある場合、第 1 ノードと後続ノード #1 を netdump サーバとして設定できます。 次に、第 1 ノードを後続ノード #1 の netdump クライアントとして設定し、すべての後続ノードを第 1 ノードの netdump クライアントとして設定できます。 第 1 ノードがクラッシュした場合、netdump が後続ノード #1 に送信されます。 後続ノードがクラッシュした場合は、netdump が第 1 ノードに送信されます。

Cisco Unified Communications Manager サーバを netdump サーバとして設定せずに、外部の netdump サーバを使用できます。 外部の netdump サーバの設定方法については、TAC にお問い合わせください。

（注） netdumpユーティリティの設定は、トラブルシューティングのための Cisco Unified Communications Manager をインストールしてから行うことを推奨します。 netdump ユーティリティの設定をまだ行っていない場合は、Cisco 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。

netdump のサーバとクライアントを設定するには、Cisco Unified Communications Operating System で利用可能なコマンドライン インターフェイス（CLI）を使用します。

関連トピック

netdump サーバの設定, （4 ページ）
netdump クライアントの設定, （5 ページ）
netdump サーバによって収集されるファイルの処理, （5 ページ）
netdump ステータスの監視, （6 ページ）

netdump サーバの設定

netdump サーバを設定するには、次の手順を実行します。

手順

1 netdump サーバとして設定するノードで、『*Command Line Interface Reference Guide for Cisco Unified Solutions*』の説明に従って CLI セッションを開始します。

2 **utils netdump server start** コマンドを実行します。

3 netdump サーバのステータスを表示するには、**utils netdump server status** コマンドを実行します。

4 netdump クライアントを設定します。

関連トピック

netdump クライアントの設定, （5 ページ）

netdump クライアントの設定

netdump クライアントを設定するには、次の手順を実行します。

手順

1 netdump クライアントとして設定するノードで、『*Command Line Interface Reference Guide for Cisco Unified Solutions*』の説明に従って CLI セッションを開始します。

2 **utils netdump client start** *ip-address-of-netdump-server* コマンドを実行します。

3 **utils netdump server add-client** *ip-address-of-netdump-client* を実行します。 netdump クライアントとして設定する各ノードで、このコマンドを繰り返します。

（注） 正しい IP アドレスが入力されていることを確認してください。 CLI では、IP アドレスの検証は行われません。

4 netdump クライアントのステータスを表示するには、**utils netdump client status** コマンドを実行します。

netdump サーバによって収集されるファイルの処理

netdump サーバ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、[Netdump ログ（Netdump 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 netdump 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。 ログ ファイル名は、netdump 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。

netdump ステータスの監視

Cisco Unified Real-Time Monitoring Tool で SyslogSearchStringFound アラートを設定すると、netdump ステータスを監視できます。 適切なアラートを設定するには、次の手順を実行します。

手順

1. Cisco Unified Real-Time Monitoring Tool のクイック起動チャネルで、[ツール（Tools）]>[アラート セントラル（Alert Central）] を選択します。
2. SyslogStringMatchFound 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。
3. [次へ（Next）] を 3 回クリックします。
4. [SysLog アラート（SysLog Alert）] ウィンドウで、[追加（Add）] ボタンをクリックします。 [検索文字列の追加（Add Search String）] ダイアログボックスが表示されたら、**netdump: failed** と入力し、[追加（Add）] をクリックします。 次に、[次へ（Next）] をクリックします。

（注） 大文字と小文字、および構文が正確に一致していることを確認してください。

5. [電子メール通知（Email Notification）] ウィンドウで、適切なトリガー アラート アクションを選択し、ユーザ定義の電子メール テキストを入力して、[保存（Save）] をクリックします。

ネットワーク管理

Cisco Unified Communications Manager リモート サービスアビリティのために、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、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 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、Cisco 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 Cisco Unified Communications Manager と互換性を持っています。
  - CiscoWorks Common Services Software
  - 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

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、Cisco 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、service timestamps debug datetime msec 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 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 Cisco 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、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, （10 ページ）
Standard Packet Sniffer Users グループへのエンド ユーザの追加, （11 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 キャプチャの設定値, （15 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、Cisco Unified Communications Manager の管理を使用して次のタスクを行う必要があります。

- Cisco Unified Communications Manager とデバイス（Cisco Unified IP Phone（SIP および 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）との間で交換されるメッセージのパケットの分析。
- 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 Security Guide*』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 の管理の [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 グループへのエンド ユーザの追加, （11 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 キャプチャの設定値, （15 ページ）

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 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 Administration Guide*』の説明に従って、Cisco Unified Communications Manager の管理でエンド ユーザを設定したことを前提としています。

手順

1. 『*Cisco Unified Communications Manager Administration Guide*』の説明に従って、ユーザ 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. 『*Cisco Unified Communications Manager Administration Guide*』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. Cisco Unified CM の管理で、[システム（System）]>[サービス パラメータ（Service Parameters）] 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 CM の管理の [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 Administration Guide*』の説明に従って、SIP 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 の管理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，（10 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、Cisco Unified CM の管理でのパケット 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 Administration Guide*』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 Administration Guide*』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 Administration Guide*』の説明に従って、H.323/H.245/H.225 トランクを検索します。
   - 『*Cisco Unified Communications Manager Administration Guide*』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『*Cisco Unified Communications Manager Administration Guide*』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 の管理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，（10 ページ）

パケット キャプチャの設定値

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）	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にだけ使用します。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 ボックスで、次のいずれかのオプションを選択します。 • [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、Cisco 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）]：Cisco Unified Communications Manager が、復号化されたメッセージや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。 システムでは、毎日新しいファイルが新しい暗号キーを使用して作成されます。 Cisco Unified Communications Manager はファイルを 7 日間保存し、さらにファイルを暗号化するキーを安全な場所に保存します。 Cisco Unified Communications Manager は、PktCap 仮想ディレクトリにファイルを保存します。 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 つだけ要求します。 同様にこのツールでは、暗号化ファイルを復号化するためのキー情報を要求します。 **ヒント** 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する必要があります。

設定	説明
パケット キャプチャ時間（Packet Capture Duration）	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にだけ使用します。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（分単位）を指定します。 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。

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 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。
- ファイルのキー：**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 Security Guide*』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 アクセスがディセーブルになっている Cisco 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* のまとめ

情報	Linux コマンド	サービスアビリティの GUI ツール	CLI コマンド
CPU 使用率	top	RTMT [表示（View）] タブに移動し、[サーバ（Server）] > [CPU とメモリ（CPU and Memory）] を選択	プロセッサ CPU 使用率： show perf query class Processor すべてのプロセスのプロセス CPU 使用率： show perf query counter Process “% CPU Time” 個々のプロセス カウンタの詳細（CPU 使用率を含む） show perf query instance <Process task_name>
プロセスの状態	ps	RTMT [表示（View）] タブに移動し、[サーバ（Server）] > [プロセス（Process）] を選択	show perf query counter Process “Process Status”
ディスク使用量	df/du	RTMT [表示（View）] タブに移動し、[サーバ（Server）] > [ディスク使用量（Disk Usage）] を選択	show perf query counter Partition“% Used” または show perf query class Partition
メモリ	free	RTMT [表示（View）] タブに移動し、[サーバ（Server）] > [CPU とメモリ（CPU and Memory）] を選択	show perf query class Memory
ネットワーク ステータス	netstats		show network status

情報	Linux コマンド	サービスアビリティの GUI ツール	CLI コマンド
サーバのリブート	reboot	サーバの [プラットフォーム（Platform）] Web ページにログイン [サーバ（Server）] > [現在のバージョン（Current Version）] に移動	utils system restart
トレース/ログの収集	Sftp、ftp	RTMT [ツール（Tools）] タブに移動し、[トレース（Trace）] > [トレースおよびログ セントラル（Trace & Log Central）] を選択	ファイルのリスト：file list ファイルのダウンロード：file get ファイルの表示：file view

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

表 *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、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[トレースおよびログセントラル（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]
Cisco Unified Communications Manager サーバの再起動	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	`https://<server_ipaddress>:8443/ccmservice/` で [Cisco Unity Connection サービスアビリティの管理（Cisco Unity Connection Serviceability Administration）] ページにログインして、[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、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 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 Phone 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 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（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, （22 ページ）
システム履歴ログのフィールド, （23 ページ）
システム履歴ログへのアクセス, （24 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 - Cisco 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
  - シャットダウン
  - ブート

- 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（Start）
  - 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

集中型監査ロギングによって、Cisco Unified Communications Manager システムの設定の変更が個別の監査ログ ファイルに記録されます。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 Cisco 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
- Cisco Unified Communications Manager CDR Analysis and Reporting
- Cisco Unified Real-Time Monitoring Tool
- Cisco Unified Communications Operating System
- ディザスタ リカバリ システム
- 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 の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パージは、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 サービスアビリティの [監査ユーザ設定（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 監査ロギン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 サービスアビリティのコントロール 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 サービスアビリティで [ツール（Tools）]>[コントロール センターのネットワーク サービス（Control Center-Network Services）] を選択し、このサービスを停止してから開始します。

すべての監査ログは、Cisco Unified Real-Time Monitoring Tool の Trace and Log Central から収集、表示、および削除します。 RTMT の Trace and Log Central で監査ログにアクセスします。 [システム（System）]>[リアルタイム トレース（Real-Time Trace）]>[監査ログ（Audit Logs）]>[ノード（Nodes）] 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（System）]>[Cisco 監査ログ（Cisco Audit Logs）] 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 の管理、Cisco Unified サービスアビリティ、CLI、Cisco Unified Real-Time Monitoring Tool（RTMT）、ディザスタ リカバリ システム、および Cisco Unified CDR Analysis and Reporting（CAR）の設定変更が示されます。 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イネーブルになっていますが、Cisco Unified サービスアビリティで [ツール（Tools）] > [監査ログ設定（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 サービスアビリティで監査ログがディセーブルになると、新しい監査ログは作成されません。

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。

Cisco Unified Communications Manager では、1 つのアプリケーション監査ログ ファイルが作成され、設定済みの最大ファイル サイズに到達すると、そのファイルが閉じられて新しいアプリケーション監査ログ ファイルが作成されます。 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は、Cisco Unified Communications Manager によって設定済みの数のファイルが保存されます。 ログ イベントの一部は、RTMT SyslogViewer を使用して表示できます。

Cisco Unified Communications Manager 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。
- 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 サービスアビリティでは、次のイベントが記録されます。

- サービスアビリティ ウィンドウからの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。
- 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。

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

- CDR ローダのスケジュール
- 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、デフォルトではイネーブルになっていませんが、Cisco Unified サービスアビリティで [ツール（Tools）] > [監査ログ設定（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。

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 サービスアビリティ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、『*Command Line Interface Reference Guide for Cisco Unified Solutions*』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 CM の管理から、[ナビゲーション（Navigation）] > [Cisco Unified サービスアビリティ（Cisco Unified Serviceability）] を選択します。
2. [ツール（Tools）] > [サービスの開始（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 CM の管理から、[ナビゲーション（Navigation）] > [Cisco Unified サービスアビリティ（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の機能サービス（Control Center – Feature Services）] を選択します。

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。