概要

この章では、Cisco CallManager Serviceability プログラム、リモート Serviceability ツール、および CDR Analysis and Reporting ツールの概要について説明します。システム管理者は、Cisco CallManager Administration の保守ツールを使用して、システムに関する問題をトラブルシューティングすることができます。これらのツールには、Serviceability、リモート Serviceability、および CDR Analysis and Reporting があります。

この章の構成は、次のとおりです。

Cisco CallManager Serviceability

Web ベースのツールである Serviceability は、次の保守機能を備えています。

- アラーム：トラブルシューティングに備えて Cisco CallManager サービスのアラームとイベントを保存します。また、アラーム メッセージの定義も提供します。
- トレース：トラブルシューティングに備えて、Cisco CallManager サービスのトレース情報を各種ログ ファイルに保存します。システム管理者は、トレース情報の設定、収集、および分析を行うことができます。
- リアルタイム モニタリング：Cisco CallManager クラスタ内のコンポーネントの動作をリアルタイムでモニタします。
- Service Activation：Cisco CallManager サービスのアクティベーション状況を表示します。システム管理者は、Service Activation を使用してサービスをアクティブまたは非アクティブにします。
- Control Center：Cisco CallManager サービス全体の状況を表示します。システム管理者は、Control Center を使用してサービスの開始と停止を行います。
- IP Phone Problem Reports Viewer：Quality Report Tool (QRT) によって生成される IP Phone Problem レポートを表示します。

Serviceability にアクセスするには、Cisco CallManager Administration ウィンドウのメニューバーから Applications を選択します。Serviceability は、Cisco CallManager ソフトウェアのインストール時に自動的にインストールされて使用可能になります。

リモート Serviceability

シスコ サービス エンジニア（CSE）は、Cisco CallManager システムの管理を補助するリモート保守ツールを使用できます。リモート側からトラブルシューティングや診断ヘルプを行う必要がある場合は、CSE はこれらのツールを使用してシステム情報とデバッグ情報を収集します。

お客様の承諾があれば、技術サポート エンジニアは Cisco CallManager サーバにログオンし、デスクトップやシェルを使用して、ローカル ログオン セッションから実行可能なあらゆる機能を実行できます。

リモート保守は、マルチホスト、マルチプラットフォームの Cisco IP Telephony ソリューション環境内で多種多様なアプリケーションをサポートします。ツールを使用して、大量に収集したローカルまたはリモートの Cisco CallManager の設定データとシステム情報を処理し、レポートを作成できます。

Cisco CallManager では、次のリモート保守機能をサポートしています。

- Cisco Secure Telnet：CSE は、お客様のリモート サイトにログオンして Cisco CallManager システムのトラブルシューティングを行います。
- Show コマンドラインインターフェイス：CSE は、お客様のネットワークに関する Cisco CallManager システムの統計を表示します。
- Microsoft Windows 2000 パフォーマンス モニタリング：システム管理者は、ローカルまたはリモート側にインストールされている Cisco CallManager のパフォーマンスをモニタします。
- ISDN トレース用の Message Translator：CSE は、Q931 Message Translator を使用して、ISDN レイヤ 3 プロトコルのメッセージをデバッグします。
- CiscoWorks2000 ネットワーク管理システム：Cisco CallManager クラスタのリモート ネットワーク管理を実行します。
- パス分析インターフェイス：ネットワーク上の指定された 2 ポイント間の接続性をトレースし、そのポイント間を流れるパケットの物理パスと論理パス（レイヤ 2 とレイヤ 3）の両方を分析します。
- システム ログ管理：集中システム ロギング サービスを Cisco IP Telephony ソリューションに提供します。
- SNMP インスツルメンテーション：システム管理者は、リモートからネットワーク パフォーマンスの管理、ネットワークの問題の検出と解決、およびネットワークの拡張計画を行うことができます。
- Cisco Discovery Protocol サポート：Cisco CallManager サーバを特定し、CiscoWorks2000 によるこれらのサーバの管理を可能にします。

関連項目

- CDR Analysis and Reporting（P.1-4）
- 参考情報（P.1-8）

CDR Analysis and Reporting

Cisco CallManager Serviceability 報告ツールである CDR Analysis and Reporting (CAR) は、次の機能を備えています。

- 複数レベルのユーザ：管理者（システム レポートの生成とシステム パラメータの設定を行う）、マネージャ（ユーザと各部門のレポートを生成する）、およびユーザ（個々の課金記録を生成する）。
- ユーザ レポートの生成：ユーザ レポートには、個人の課金情報、部門別の課金情報、top N by charge、top N by duration、top N by number of calls、CTI port enabled、および Cisco IP Phone サービスがあります。
- システム レポートの生成：システム レポートには、QoS の詳細、QoS の要約、ゲートウェイ別の QoS、コール タイプ別の QoS、トラフィックの要約、内線番号によるトラフィックの要約、システムの概要、CDR エラーが含まれます。
- デバイス レポートの生成：デバイス レポートには、ゲートウェイの詳細、ゲートウェイの要約、ゲートウェイの使用状況、ルート グループの使用状況、ルート リストの使用状況、ルート パターンの使用状況、Conference Bridge の使用状況、およびボイスメールの使用状況が含まれます。
- CDR 検索：CDR データベースを検索して、コール レッグの進行状況と品質の追跡に役立つ、コールの詳細情報を確認します。
- システム設定：管理者は、システム パラメータ、レポート スケジューラ、データベース オプション、およびエラーとイベントのログを設定します。
- レポート設定：管理者は、コールの基本料金と通話時間、係数オプション、QoS 値、および自動レポート生成またはアラートを設定します。

関連項目

- Cisco CallManager Serviceability（P.1-2）
- 参考情報（P.1-8）

Hypertext Transfer Protocol over Secure Sockets Layer（HTTPS）の使用方法

この項は、次の内容で構成されています。

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

HTTPS の概要

ブラウザ クライアントと IIS サーバ間の通信を保護する Hypertext Transfer Protocol over Secure Sockets Layer（HTTPS）は、証明書と公開鍵を使って、インターネット上で転送されるデータを暗号化します。HTTPS はサーバの ID を検証し、Cisco CallManager Serviceability などのアプリケーションをサポートします。また、ユーザ ログイン パスワードが Web を介して安全に送信されるようにします。

Cisco CallManager 4.1 のインストールまたはアップグレード後に、Cisco CallManager Administration またはその他の Cisco CallManager SSL 対応の仮想ディレクトリに管理者またはユーザが初めてアクセスすると、Security Alert ダイアログボックスが開き、サーバを信用するかどうか確認します。このダイアログボックスが表示されたら、以下のいずれかの操作を実行する必要があります。

- Yes をクリックして、現在の Web セッションの証明書だけを信用する。現在のセッションの証明書だけを信用した場合、信頼できるフォルダに証明書がインストールされるまで、アプリケーションにアクセスするたびに Security Alert ダイアログボックスが表示されます。
- View Certificate > Install Certificate をクリックして、常に証明書を信用するように、証明書のインストール タスクを実行する。信頼できるフォルダに証明書をインストールすると、Web アプリケーションにアクセスするたびに Security Alert ダイアログボックスが表示されることはありません。

- No をクリックして、操作を中止する。認証は行われず、Web アプリケーションにアクセスできません。Web アプリケーションにアクセスするには、Yes をクリックするか、または View Certificate > Install Certificate オプションで証明書をインストールします。

（注）　ホスト名を使用して Web アプリケーションにアクセスし、信頼できるフォルダに証明書をインストールしてから、ローカル ホストまたは IP アドレスを使用してそのアプリケーションにアクセスしようとすると、セキュリティ証明書の名前がサイトの名前と一致しないことを示す Security Alert ダイアログボックスが表示されます。

ローカル ホスト、IP アドレス、または URL のホスト名を使用してアプリケーションにアクセスする場合は、各タイプ（ローカル ホスト、IP アドレスなど）ごとに信頼できるフォルダに証明書を保存する必要があります。

（注）　Netscape 4.79 およびアンダースコア（_）を含むホスト名を使用してアプリケーションをブラウズする場合、HTTPS は HTTPS 対応アプリケーションには機能しません。「The computer name <xxxx> contains one or more non-standard characters. Standard characters include letters (A-Z), digits (0-9), and hyphens (-).Using a nonstandard name will prevent others from finding the computer on the network, unless your network is using the Microsoft DNS Server. Do you want to use this nonstandard name?」というエラー メッセージが表示された場合は、**No** をクリックします。このエラーが発生するのは、HTTPS サービスを使用可能にする証明書で、証明書の件名にホスト名が使用されているためです。Netscape 4.79 は件名に含まれるアンダースコアを無効な文字とみなすため、HTTPS は機能しません。HTTPS のサポートが必要な場合は、Internet Explorer を使用してください。Netscape 4.79 とホスト名を使用してアプリケーションにアクセスするには、HTTPS を無効にしてください（『*Cisco CallManager セキュリティ ガイド*』を参照）。

関連項目

- Hypertext Transfer Protocol over Secure Sockets Layer（HTTPS）の使用方法（P.1-5）
- 信頼できるフォルダへの証明書の保存（P.1-7）

信頼できるフォルダへの証明書の保存

信頼できるフォルダに CA ルート証明書を保存して、Web アプリケーションにアクセスするたびに Security Alert ダイアログボックスが表示されないようにするには、次の手順を実行します。

手順

ステップ 1　IIS サーバでアプリケーションをブラウズします。

ステップ 2　Security Alert ダイアログボックスが表示されたら、**View Certificate** をクリックします。

ステップ 3　Certificate ペインで、**Install Certificate** をクリックします。

ステップ 4　**Next** をクリックします。

ステップ 5　**Place all certificates in the following store** オプション ボタンを選択して、**Browse** をクリックします。

ステップ 6　**Trusted Root Certification Authorities** をブラウズします。

ステップ 7　**Next** をクリックします。

ステップ 8　**Finish** をクリックします。

ステップ 9　証明書をインストールするには、**Yes** をクリックします。

インポートが成功したというメッセージが表示されます。**OK** をクリックします。

ステップ 10　ダイアログボックスの右下にある **OK** をクリックします。

ステップ 11　証明書を信用し、ダイアログボックスが再び表示されないようにするには、**Yes** をクリックします。

（注）　URL にローカル ホスト、IP アドレス、またはホスト名を使用して Cisco CallManager Administration にアクセスする場合は、各タイプ（ローカル ホスト、IP アドレスなど）ごとに信頼できるフォルダに証明書を保存する必要があります。保存しない場合、タイプごとに Security Alert ダイアログボックスが表示されます。

関連項目

- Hypertext Transfer Protocol over Secure Sockets Layer（HTTPS）の使用方法（P.1-5）
- HTTPS の概要（P.1-5）

参考情報

- *Cisco CallManager アドミニストレーション ガイド*
- *Cisco CallManager システム ガイド*
- *Cisco CallManager Serviceability System Guide*
- *Cisco CallManager セキュリティ ガイド*
- CiscoWorks2000 ユーザ マニュアル
  http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/index.htm