Cisco Unified Serviceability アドミニストレーション ガイド for Cisco Unified Presence

Release 6.0(1)

Text Part Number: OL-12729-01-J

CONTENTS

このマニュアルについて

ここでは、このマニュアルの目的、対象読者、構成、および表記法、そして関連資料の入手方法について説明します。

次のトピックについて取り上げます。

目的

『*Cisco Unified Serviceability アドミニストレーション ガイド for Cisco Unified Presence*』は、Cisco Unified Presence Serviceability プログラム（Real-Time Monitoring Tool（RTMT）など）に関する情報を提供します。

対象読者

『*Cisco Unified Serviceability アドミニストレーション ガイド for Cisco Unified Presence*』は、Cisco Unified Presence システムの管理とサポートを担当するネットワーク管理者を対象としています。ネットワーク技術者、システム管理者、または電気通信技術者は、このマニュアルを参照してリモート サービスアビリティの機能を理解し、その管理を行います。テレフォニーおよび IP ネットワーキング テクノロジーに関する知識が必要です。

マニュアルの構成

次の表は、このマニュアルの構成を示しています。

章番号	説明
第 1 章「概要」	Cisco Unified Presence Serviceability アプリケーションとリモート保守アプリケーション、レポート作成ツールの概要を説明します。
第 2 章「サービスの管理」	Cisco Unified Presence のサービスをアクティブ化、非アクティブ化、開始、および停止する手順について説明します。
第 3 章「アラームの設定」	Cisco Unified Presence のアラームを設定する手順について説明します。
第 4 章「アラーム定義」	Cisco Unified Presence のアラーム定義を検索および編集する手順について説明します。
第 5 章「トレースの設定」	Cisco Unified Presence のサービスのトレース パラメータを設定する手順について説明します。
第 6 章「トラブルシューティング トレース設定値の設定」	トラブルシューティング トレースの設定値を設定する手順について説明します。
第 7 章「Real-Time Monitoring の設定」	Real-Time Monitoring Tool を設定する手順について説明します。
第 8 章「RTMT でのアラート設定」	アラート プロパティの設定、アラート アクションの設定、アラート通知用の電子メールの設定など、Real-Time Monitoring Tool でアラートを操作する手順について説明します。
第 9 章「パフォーマンス モニタリングの設定と使用」	パフォーマンス カウンタやカウンタの説明の表示など、パフォーマンス モニタを操作する手順について説明します。
第 10 章「RTMT の トレース収集とログ集中管理」	Cisco Unified Presence のサービスとクラッシュ ダンプ ファイルのオンデマンド トレース収集を設定する方法、および適切なビューアでトレース ファイルを表示する方法について説明します。
第 11 章「RTMT SysLog Viewer の使用」	SysLog Viewer を使用する方法について説明します。
第 12 章「プラグインの使用」	Real-Time Monitoring Tool のプラグインをインストールおよび使用する方法について説明します。
第 13 章「Log Partition Monitoring の設定」	Log Partition Monitoring を設定して、特定のサーバ（またはクラスタ内のすべてのサーバ）のログ パーティションでのディスク使用状況をモニタする方法について説明します。
第 14 章「Serviceability Reports Archive の設定」	Serviceability Reporter サービスによって生成されるレポートを表示する手順について説明します。
第 15 章「SNMP V1/V2c の設定」	SNMP バージョン 1 および 2c を設定する手順について説明します。
第 16 章「SNMP V3 の設定」	SNMP バージョン 3 を設定する手順について説明します。
第 17 章「MIB2 システム グループの設定」	システムの連絡先およびシステムの場所のオブジェクトを MIB-II システム グループに設定する手順について説明します。

関連マニュアル

関連する Cisco IP テレフォニーのアプリケーションと製品の詳細については、『*Cisco Unified Presence Documentation Guide*』を参照してください。次の URL には、ドキュメント ガイドへのパスのサンプルが表示されます。

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/<release #>/doc_gd/index.htm

表記法

このマニュアルは、次の表記法を使用しています。

表記法	説明
太字	コマンドおよびキーワードは、**太字**で示しています。
イタリック体	ユーザが値を指定する引数は、*イタリック体*で示しています。
[ ]	角カッコの中の要素は、省略可能です。
{ x | y | z }	必ずどれか 1 つを選択しなければならない必須キーワードは、波カッコで囲み、縦棒で区切って示しています。
[x | y | z]	どれか 1 つを選択できる省略可能なキーワードは、角カッコで囲み、縦棒で区切って示しています。
ストリング	引用符を付けない一組の文字。ストリングの前後には引用符を使用しません。引用符を使用すると、その引用符も含めてストリングとみなされます。
`screen` フォント	システムが表示する端末セッションおよび情報は、`screen` フォントで示しています。
太字の **`screen`** フォント	ユーザが入力しなければならない情報は、**太字**の **`screen`** フォントで示しています。
イタリック体の `screen` フォント	ユーザが値を指定する引数は、*イタリック体の `screen`* フォントで示しています。
―→	例の中で重要なテキストを強調しています。
^	^ 記号は、Ctrl キーを表します。たとえば、画面に表示される ^D というキーの組み合せは、Ctrl キーを押しながら D キーを押すことを意味します。
< >	パスワードのように出力されない文字は、山カッコで囲んで示しています。

（注）は、次のように表しています。

（注） 「*注釈*」です。役立つ情報や、このマニュアル以外の参照資料などを紹介しています。

ワンポイント アドバイスは、次のように表しています。

ワンポイント・アドバイス *時間を節約する方法*です。ここに紹介している方法で作業を行うと、時間を短縮できます。

ヒントは、次のように表しています。

ヒント *便利なヒント*です。

注意は、次のように表しています。

注意 「*要注意*」の意味です。機器の損傷またはデータ損失を予防するための注意事項が記述されています。

警告は、次のように表しています。

警告 **「危険」の意味です。人身事故を予防するための注意事項が記述されています。装置の取り扱い作業を行うときは、電気回路の危険性に注意し、一般的な事故防止策をとるよう努めてください。**

技術情報の入手方法、サポートの利用方法、およびセキュリティ ガイドライン

技術情報の入手、サポートの利用、技術情報に関するフィードバックの提供、セキュリティ ガイドライン、推奨するエイリアスおよび一般的なシスコのマニュアルに関する情報は、月刊の『*What's New* in Cisco Product Documentation』を参照してください。ここには、新規および改訂版のシスコの技術マニュアルもすべて記載されています。次の URL からアクセスできます。

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

シスコ製品のセキュリティの概要

本製品には暗号化機能が備わっており、輸入、輸出、配布および使用に適用される米国および他の国での法律を順守するものとします。シスコの暗号化製品を譲渡された第三者は、その暗号化技術の輸入、輸出、配布、および使用を許可されたわけではありません。輸入業者、輸出業者、販売業者、およびユーザは、米国および他の国での法律を順守する責任があります。本製品を使用するにあたっては、関係法令の順守に同意する必要があります。米国および他の国の法律を順守できない場合は、本製品を至急送り返してください。

シスコでは、オンラインの Security Vulnerability Policy ポータル（英文のみ）を無料で提供しています。URL は次のとおりです。

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

PART 1

Cisco Unified Presence Serviceability

CHAPTER 1

概要

この章は、次の項で構成されています。

Cisco Unified Presence Serviceability の概要

Cisco Unified Presence の Web ベースのトラブルシューティング ツールである Cisco Unified Presence Serviceability は、次の機能を備えています。

- トラブルシューティングに備えて、Cisco Unified Presence の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。
- トラブルシューティングに備えて、Cisco Unified Presence の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、および表示を行うことができます。
- Real-Time Monitoring Tool（RTMT）を使用して、Cisco Unified Presence クラスタ内のコンポーネントの動作をリアルタイムにモニタします。
- Service Activation ウィンドウでアクティブ化、非アクティブ化、および表示できる機能サービスを提供します。
- 機能サービスとネットワーク サービスを開始および停止するインターフェイスを提供します。
- Cisco Unified Presence Serviceability のツールに関連付けられるレポートをアーカイブします。
- Cisco Unified Presence が SNMP リモート管理とトラブルシューティングのための管理対象デバイスとして機能できるようにします。
- 1 つのサーバ（またはクラスタ内のすべてのサーバ）上のログ パーティションのディスク使用状況をモニタします。

Cisco Unified Presence Serviceability へのアクセス

Cisco Unified Presence Serviceability にアクセスするには、次の手順を実行します。

手順

ステップ 1　Netscape 7.1（またはそれ以降）あるいは Internet Explorer 6.0（またはそれ以降）を使用して、Cisco Unified Presence Serviceability サービスが動作している Cisco Unified Presence を参照します。

ヒント　サポートされているブラウザで、**https://< サーバ名または IP アドレス >:8443** と入力します。ここで、「サーバ名または IP アドレス」は Cisco Unified Presence Serviceability サービスが動作しているサーバ、8443 は HTTPS のポート番号を表します。

ブラウザで http://< サーバ名または IP アドレス >:8080 と入力すると、HTTPS を使用するようにシステムによってリダイレクトされます。HTTP は、ポート番号 8080 を使用します。

ステップ 2　［**Cisco Unified Presence の管理**］リンクをクリックします。

ステップ 3　証明書に関するプロンプトが表示された場合は、P.1-3 の「Hypertext Transfer Protocol over Secure Sockets Layer（HTTPS）の使用」を参照してください。

ステップ 4　ユーザ名とパスワードの入力を求めるプロンプトが初めて表示されたときは、インストール中にユーザ名とパスワードとして指定したアプリケーション ユーザ名およびアプリケーション ユーザ パスワードをそれぞれ入力します。

ヒント　Standard CCMUsers 権限が割り当てられたユーザはすべて、Cisco Unified Presence Serviceability にアクセスできます。この権限をユーザに割り当てる方法の詳細については、『*Cisco Unified Presence アドミニストレーション ガイド*』を参照してください。

ステップ 5　Cisco Unified Presence の管理ページが表示されたら、ウィンドウの右上にある［ナビゲーション］ドロップダウン リスト ボックスで［**Cisco Unified サービスアビリティ**］を選択します。

Cisco Unified Presence Serviceability が表示されます。

ヒント　設定の途中で Cisco Unified Presence Serviceability のメイン ウィンドウに戻るには、アプリケーション ウィンドウの右上にある［Home］をクリックします。

追加情報

P.1-8 の「関連項目」を参照してください。

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

この項では、次のトピックについて取り上げます。

Hypertext Transfer Protocol over Secure Sockets Layer（SSL）は、ブラウザ クライアントと Tomcat Web サーバ間の通信をセキュリティで保護するためのプロトコルであり、証明書と公開鍵を使用し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 はサーバのアイデンティティを保証し、Cisco Unified Presence 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。

HTTPS の概要（Internet Explorer の場合）

Cisco Unified Presence のインストールまたはアップグレード後に、Cisco Unified Presence の管理ページまたはその他の Cisco Unified Presence 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、サーバを信頼するかどうかを確認するための［セキュリティの警告］ダイアログボックスが表示されます。このダイアログボックスが表示されたら、次のいずれかの操作を実行する必要があります。

- ［はい］をクリックして、現在の Web セッションに対してのみ証明書を信頼する。現在のセッションに対してのみ証明書を信頼すると、［セキュリティの警告］ダイアログボックスは、信頼できるフォルダに証明書をインストールするまで、アプリケーションにアクセスするたびに表示されます。
- ［証明書の表示］>［証明書のインストール］の順にクリックして証明書のインストール タスクを実行し、その証明書を常に信頼することを指定する。信頼できるフォルダ内に証明書をインストールした場合、Web アプリケーションにアクセスするたびに［セキュリティの警告］ダイアログボックスが表示されることはありません。
- ［いいえ］をクリックして、操作をキャンセルする。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、［はい］をクリックするか、または［証明書の表示］>［証明書のインストール］オプションで証明書をインストールします。

（注） システムは、ホスト名を使用して証明書を発行します。IP アドレスを使用して Web アプリケーションにアクセスしようとすると、クライアントに証明書をインストールした場合でも、［セキュリティの警告］ダイアログボックスが表示されます。

追加情報

P.1-8 の「関連項目」を参照してください。

信頼できるフォルダへの証明書の保存（Internet Explorer の場合）

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［セキュリティの警告］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　Tomcat Web サーバ上のアプリケーションを参照します。

ステップ 2　［セキュリティの警告］ダイアログボックスが表示されたら、**［証明書の表示］**をクリックします。

ステップ 3　［証明書］ペインで、**［証明書のインストール］**をクリックします。

ステップ 4　**［次へ］**をクリックします。

ステップ 5　**［証明書をすべて次のストアに配置する］**オプション ボタンを選択して、**［参照］**をクリックします。

ステップ 6　**［信頼されたルート証明機関］**を参照します。

ステップ 7　**［次へ］**をクリックします。

ステップ 8　**［完了］**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、**［はい］**をクリックします。

インポートが正常に行われたことを知らせる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　証明書を信頼し、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、**［はい］**をクリックします。

追加情報

P.1-8 の「関連項目」を参照してください。

信頼できるフォルダへの証明書の保存（Netscape の場合）

Netscape で HTTPS を使用する場合、証明書の資格情報を表示し、1 回のセッションに対して証明書を信頼する、期限が切れるまでその証明書を信頼する、または証明書を信頼しない、のいずれかを選択できます。

ヒント　1 回のセッションに対してのみ証明書を信頼する場合は、HTTPS がサポートされているアプリケーションにアクセスするたびに次の手順を繰り返す必要があります。証明書を信頼しない場合は、アプリケーションにアクセスできません。

信頼できるフォルダに証明書を保存するには、次の手順を実行します。

手順

ステップ 1　Netscape を使用して、アプリケーション（たとえば、Cisco Unified Presence Serviceability など）を参照します。

証明書に関するダイアログボックスが表示されます。

ステップ 2　次のいずれかのオプション ボタンをクリックします。

- ［この証明書をこのセッションのために一時的に受け入れる］
- ［この証明書を受け入れない / この Web サイトに接続しない］
- ［この証明書を永続的に受け入れる］

（注）　［この証明書を受け入れない / この Web サイトに接続しない］を選択した場合、アプリケーションは表示されません。

（注）　次に進む前に証明書の資格情報を表示する場合は、**［証明書を調査］**をクリックします。資格情報を確認し、**［閉じる］**をクリックします。

ステップ 3　**［OK］**をクリックします。

［セキュリティに関する警告］ダイアログボックスが表示されます。

ステップ 4　**［OK］**をクリックします。

追加情報

P.1-8 の「関連項目」を参照してください。

Cisco Unified Presence Serviceability のインターフェイスの使用

Cisco Unified Presence Serviceability では、トラブルシューティングやサービス関連の操作に加え、次の操作を実行できます。

- 1 つの特定ウィンドウに関するドキュメントを表示するには、Cisco Unified Presence Serviceability で［**Help**］>［**This page**］の順に選択します。
- このリリースの Cisco Unified Presence で利用できるマニュアルのリストを表示する（またはオンライン ヘルプの索引にアクセスする）には、Cisco Unified Presence Serviceability で［**Help**］>［**Contents**］>［**Contents and Index**］の順に選択します。
- 設定のウィンドウから Cisco Unified Presence Serviceability のホーム ページに直接移動するには、ウィンドウの右上にある［**Home**］リンクをクリックします。
- Cisco Unified Presence の管理ページまたは他のアプリケーションにアクセスするには、ウィンドウの右上にある［**Navigation**］ドロップダウン リスト ボックスで対象のアプリケーションを選択します。
- Cisco Unified Presence Serviceability でアイコンを使用するには、表 1-1 を参照してください。

表 1-1　Cisco Unified Presence Serviceability のアイコン

アイコン	目的
	新しい設定を追加します。
	操作を取り消します。
	指定した設定をクリアします。
	選択した設定を削除します。
	設定に関するオンライン ヘルプを表示します。
	ウィンドウを更新して最新の設定を表示します。
	選択したサービスを再起動します。

表 1-1　Cisco Unified Presence Serviceability のアイコン（続き）

アイコン	目的
	入力した情報を保存します。
	設定のデフォルトを定義します。
	選択したサービスを開始します。
	選択したサービスを停止します。

アクセシビリティ機能

Cisco Unified Presence Serviceability の管理ページには、ユーザがマウスを使用せずにウィンドウ上のボタンにアクセスできる機能が用意されています。これらのナビゲーション ショートカットにより、視覚障害を持つユーザにもアプリケーションが使用しやすくなります。

表 1-2 は、キーボード ショートカットでインターフェイスをナビゲーションする際のガイドです。

表 1-2　Cisco Unified Presence Serviceability のナビゲーション ショートカット

キーストローク	動作
Alt	ブラウザのメニュー バーにフォーカスを移動します。
Enter	項目（メニュー オプション、ボタンなど）をフォーカスして選択します。
Alt、矢印キー	ブラウザ メニュー間を移動します。
Space	チェックボックスのオン / オフなどのコントロールを切り替えます。
Tab	タブ順の次の項目または次のコントロール グループにフォーカスを移動します。
Shift+Tab	タブ順の前の項目または前のコントロール グループにフォーカスを移動します。
矢印キー	グループ内でコントロール間を移動します。
Home	1 画面分を超える情報が存在する場合、ウィンドウの一番上に移動します。また、ユーザが入力したテキストの行頭に移動します。
End	ユーザが入力したテキストの行末に移動します。 1 画面分を超える情報が存在する場合、ウィンドウの一番下に移動します。
Page Up	1 画面分だけ上にスクロールします。
Page Down	1 画面分だけ下にスクロールします。

参考情報

- *Cisco Unified Presence アドミニストレーション ガイド*

追加情報

P.1-8 の「関連項目」を参照してください。

関連項目

- Hypertext Transfer Protocol over Secure Sockets Layer（HTTPS）の使用（P.1-3）
- HTTPS の概要（Internet Explorer の場合）（P.1-3）
- 信頼できるフォルダへの証明書の保存（Internet Explorer の場合）（P.1-4）

PART 2

サービスの管理

CHAPTER 2

サービスの管理

この章は、次の項で構成されています。

機能サービスのアクティブ化と非アクティブ化

Cisco Unified Presence Serviceability では、［Service Activation］ウィンドウでサービスをアクティブまたは非アクティブにします。［Service Activation］ウィンドウに表示されているサービスは、アクティブにするまで開始されません。

Cisco Unified Presence では、機能サービスをアクティブおよび非アクティブにできます。必要な数のサービスを同時にアクティブまたは非アクティブにすることができます。一部の機能サービスは他のサービスに依存していますが、その場合は、対象の機能サービスがアクティブになる前に従属サービスがアクティブになります。

Cisco Unified Presence Serviceability で Cisco Unified Presence のサービスをアクティブまたは非アクティブにするには、次の手順を実行します。

手順

ステップ 1　**［Tools］** > **［Service Activation］**の順に選択します。

［Service Activation］ウィンドウが表示されます。

ステップ 2　［Server］ドロップダウン リスト ボックスでサーバを選択し、**［Go］**をクリックします。

選択したサーバのサービス名およびサービスのアクティブ化状況がウィンドウに表示されます。

ステップ 3　**［Set Default］**ボタンをクリックするか、またはアクティブにするサービスの横にあるチェックボックスをオンにして、使用するサービスをアクティブにします。

ステップ 4　必要な変更を加えたら、**［Save］**をクリックします。

ヒント　アクティブにしたサービスを非アクティブにするには、非アクティブにするサービスの横にあるチェックボックスをオフにし、**［Update］**をクリックします。

追加情報

P.2-4 の「関連項目」を参照してください。

Control Center におけるサービスの開始、停止、再起動、および状況更新

Cisco Unified Presence Serviceability の Control Center では、クラスタ内の特定のサーバについて、状況の表示、状況の更新、および Cisco Unified Presence のサービスの開始、停止、再起動を行うことができます。Cisco Presence のサービスを開始、停止、または再起動すると、その Cisco Presence のサービスに現在登録されているゲートウェイはすべて、セカンダリ Cisco Presence のサービスにフェールオーバーされます。別の Cisco Presence のサービスに登録できない場合にだけ、デバイスと電話機を再起動する必要があります。Cisco Presence のサービスを開始、停止、または再起動すると、その Cisco Unified Presence をホームとする他のインストール済みアプリケーション（Conference Bridge や Cisco Messaging Interface など）も同様に開始および停止します。

（注） Cisco Unified Presence をアップグレードした場合、システム上ですでに開始されていたサービスは、アップグレード後に開始されます。

クラスタ内の特定のサーバ上のサービスを開始、停止、または再起動したり、そのサービスの状況を表示したりするには、次の手順を実行します。一度に開始、停止、または更新できるサービスは、1 つだけです。

手順

ステップ 1　開始 / 停止 / 再起動 / 更新するサービス タイプに応じて、次のいずれかの操作を実行します。

- ［**Tools**］>［**Control Center - Feature Services**］の順に選択します。

ヒント 開始 / 停止 / 再起動できるのは、アクティブにされている機能サービスのみです。サービスをアクティブにするには、P.2-2 の「機能サービスのアクティブ化と非アクティブ化」を参照してください。

- ［**Tools**］>［**Control Center - Network Services**］の順に選択します。

ステップ 2　［Server］ドロップダウン リスト ボックスでサーバを選択し、［**Go**］をクリックします。

選択したサーバのサービス名、サービス タイプ、およびサービス状況がウィンドウに表示されます。ウィンドウには、サービスの状況（Started、Running、または Stopped）も表示されます。

ステップ 3　次のいずれかの操作を実行します。

- 開始するサービスの横にあるオプション ボタンをクリックし、［**Start**］ボタンをクリックします。
  更新された状況を反映して、ステータスが変更されます。
- 再起動するサービスの横にあるオプション ボタンをクリックし、［**Restart**］ボタンをクリックします。
  再起動に少し時間がかかることを示すメッセージが表示されます。［**OK**］をクリックします。
- 停止するサービスの横にあるオプション ボタンをクリックし、［**Stop**］ボタンをクリックします。

更新された状況を反映して、ステータスが変更されます。

- 最新のサービス状況を表示するには、［**Refresh**］ボタンをクリックします。
- ［Service Activation］ウィンドウやその他の［Control Center］ウィンドウに移動するには、［Related Links］ドロップダウン リスト ボックスでオプションを選択し、［**Go**］をクリックします。

追加情報

P.2-4 の「関連項目」を参照してください。

コマンドライン インターフェイスを使用したサービスの開始と停止

次のサービスは、コマンドライン インターフェイス（CLI）でコマンドを実行することで、開始および停止できます。

- システム NTP
- システム SSH
- サービス マネージャ
- Cisco DB
- Cisco Tomcat
- Cisco Database Layer Monitor

サービスを開始するには、**utils service start** < **サービス名** > と入力します。ここで、「サービス名」はサービスの完全な名前を表します。

サービスを停止するには、**utils service stop** < **サービス名** > と入力します。ここで、「サービス名」はサービスの完全な名前を表します。

ヒント　他のすべてのサービスは、Cisco Unified Presence Serviceability の Control Center から開始および停止する必要があります。

追加情報

P.2-4 の「関連項目」を参照してください。

関連項目

- Control Center におけるサービスの開始、停止、再起動、および状況更新（P.2-3）
- 機能サービスのアクティブ化と非アクティブ化（P.2-2）

PART 3

アラームの設定

CHAPTER 3

アラームの設定

Cisco Unified Presence Serviceability のアラームでは、管理者がアラームやイベントの設定およびアラーム メッセージの定義を行うことができるので、システム管理者やサポート担当者が Cisco Unified Presence の問題をトラブルシューティングするのに役立ちます。管理者は、アラームとトレースのパラメータを設定し、この情報を Cisco TAC のエンジニアに提供します。

管理者はアラームを使用することにより、システムの実行時の状況と状態を表示して、問題を解決する修正処置をとることができます。たとえば、電話機が登録済みで機能しているかどうかを判別できます。アラームには、説明や推奨処置などの情報が含まれています。また、アラームの情報には、アプリケーション名、マシン名、およびクラスタ名が含まれているため、ローカル以外で起こった Cisco Unified Presence の問題をトラブルシューティングするときに役立ちます。

クラスタ内の Cisco Unified Presence サーバ、および各サーバのサービスにアラームを設定できます。アラーム インターフェイスは、複数の宛先にアラーム情報を送信するように設定します。それぞれの宛先には、固有のアラーム イベント レベル（Debug から Emergency まで）を指定できます。アラームの収集および表示には、Real-Time Monitoring Tool を使用します。

サービスがアラームを発行すると、アラーム インターフェイスは、選択されたモニタ（たとえば SDI トレースや Cisco RIS Data Collector）にそのアラームを送信します。モニタは、アラームを転送するか、または最終的な宛先（ログ ファイルなど）に書き込みます。

この章は、次の項で構成されています。

サービスに対するアラームの設定または更新

この項では、Cisco Unified Presence のサービスにアラームを設定する方法について説明します。

（注） SNMP トラップおよびカタログの設定は、変更しないことをお勧めします。

標準のレジストリ エディタの使用方法の詳細については、OS のオンライン マニュアルを参照してください。

手順

ステップ 1　［**Alarm**］>［**Configuration**］の順に選択します。

［Alarm Configuration］ウィンドウが表示されます。

ステップ 2　［Server］ドロップダウン ボックスから、アラームを設定する対象のサーバを選択し、［**Go**］をクリックします。

ステップ 3　［Service Group］ドロップダウン リスト ボックスから、アラームを設定する対象のサービスのカテゴリ（CUP など）を選択し、［**Go**］をクリックします。

ステップ 4　［Service］ドロップダウン　ボックスから、アラームを設定する対象のサービスを選択し、［**Go**］をクリックします。

（注） ドロップダウン リスト ボックスには、すべての（アクティブおよび非アクティブの）サービスが表示されます。

［Alarm Configuration］ウィンドウには、選択したサービスのアラーム モニタとイベント レベルのリストが表示されます。

ステップ 5　表 3-1 の説明に従って、使用するアラーム宛先のチェックボックス（1 つまたは複数）をオンにします。

ステップ 6　［Alarm Event Level］ドロップダウン リスト ボックスで、表 3-2 の説明に従って、必要なイベント レベルを選択します。

ステップ 7　選択したサービスの現在の設定値をクラスタ内のすべてのノードに適用するには、［**Apply to All Nodes**］チェックボックスをオンにします。

ステップ 8　［**Save**］ボタンをクリックして、設定を保存します。

（注） デフォルトを設定するには、［**Set Default**］ボタンをクリックした後で、［**Save**］をクリックします。

追加情報

P.3-4 の「関連項目」を参照してください。

アラーム宛先の設定値

表 3-1 では、アラーム宛先の設定値について説明します。

表 3-1　アラーム宛先

名前	宛先の説明
Enable Alarm for Local Syslogs	SysLog Viewer。Cisco Unified Presence のエラーは SysLog Viewer 内のアプリケーション ログに記録され、アラームの説明と推奨処置が提供されます。SysLog Viewer には、Serviceability の Real-Time Monitoring Tool からアクセスできます。 SysLog Viewer でログを表示する方法については、P.11-1 の「RTMT SysLog Viewer の使用」を参照してください。
Enable Alarm for Remote Syslogs	Syslog ファイル。Syslog メッセージを Syslog サーバに格納し、Syslog サーバ名を指定するには、このチェックボックスをオンにします。この宛先が有効になっていても、サーバ名が指定されていない場合、Cisco Unified Presence は Syslog メッセージを送信しません。 **（注）** CiscoWorks 2000 にアラームを送信する場合は、CiscoWorks 2000 のサーバ名を指定します。
Enable Alarm for SDI Trace	SDI トレース ライブラリ。 SDI トレース ログ ファイルにアラームを記録するには、このチェックボックスをオンにし、選択したサービスの Trace Configuration ウィンドウで Trace On チェックボックスをオンにします。 Trace Configuration ウィンドウの使用方法の詳細については、P.5-2 の「トレース パラメータの設定」を参照してください。

追加情報

P.3-4 の「関連項目」を参照してください。

アラーム イベント レベルの設定値

表 3-2 では、アラーム イベント レベルの設定値について説明します。

表 3-2　アラーム イベント レベル

名前	説明
Emergency	このレベルは、システムが使用不能であることを示します。
Alert	このレベルは、ただちに処置が必要であることを示します。
Critical	このレベルは、クリティカル条件が検出されたことを示します。
Error	このレベルは、エラー条件が存在することを示します。
Warning	このレベルは、警告条件が検出されたことを示します。
Notice	このレベルは、正常ではあるが重要な状況を示します。
Informational	このレベルは、情報メッセージだけを示します。
Debug	このレベルは、Cisco TAC のエンジニアがデバッグに使用するための詳細なイベント情報を示します。

追加情報

P.3-4 の「関連項目」を参照してください。

関連項目

- サービスに対するアラームの設定または更新（P.3-2）
- アラーム宛先の設定値（P.3-3）
- アラーム イベント レベルの設定値（P.3-4）

CHAPTER 4

アラーム定義

この章では、サービスアビリティ アラーム定義で使用するユーザ情報を検索、表示、および作成する手順について説明します。

この章は、次の項で構成されています。

アラーム定義には、アラーム メッセージの内容（メッセージの意味とその回復方法）が記述されます。

アラームに関する情報を入手するには、アラーム定義データベースを検索します。サービス固有のアラームをクリックすると、アラーム情報の説明とその推奨処置が表示されます。

Cisco Unified Presence では、アラーム定義と推奨処置が SQL サーバ データベースに保存されます。システム管理者は、すべてのアラーム定義をこのデータベースで検索できます。定義の内容には、アラーム名、記述、説明、推奨処置、重大度、パラメータ、モニタなどがあります。この情報は、システム管理者が Cisco Unified Presence に発生した問題をトラブルシューティングするときに役立ちます。

アラーム定義の表示およびユーザ指定の記述の追加

この項では、アラーム定義を検索し、その内容を表示する方法について説明します。

手順

ステップ 1　［**Alarm**］>［**Definitions**］を選択します。

［Alarm Message Definitions］ウィンドウが表示されます。

ステップ 2　［Equals］フィールドからアラーム定義のカタログを選択するか、［Enter Alarm Name］フィールドにアラーム名を入力します。

ステップ 3　［**Find**］ボタンをクリックします。

選択したアラーム カタログの定義リストが表示されます。

（注）　アラーム定義が複数のページにわたっている場合があります。別のページを表示するには、［Alarm Message Definitions］ウィンドウの下部にある適切なナビゲーション ボタンをクリックしてください。ウィンドウに表示するアラームの数を変更するには、［Rows Per Page］ドロップダウン リスト ボックスで別の値を選択します。

ステップ 4　表示されたリストの中から、アラームの詳細を表示する定義のハイパーリンクをクリックします。

［Alarm Details］ウィンドウが表示されます。

ステップ 5　アラームに情報を追加する場合は、［User Defined Text］ボックスにテキストを入力し、［**Update**］ボタンをクリックします。

ステップ 6　［Alarm Message Definitions］ウィンドウに戻るには、［Related Links］ドロップダウン リスト ボックスから［**Back to Find/List Alarms**］を選択し、［**Go**］をクリックします。

追加情報

P.4-3 の「関連項目」を参照してください。

アラーム定義のカタログ記述

表 4-1 では、アラーム定義のカタログ記述について説明します。

表 4-1　アラーム定義カタログ

名前	説明
CiscoUPSConfigAgent	設定エージェントに対するすべてのアラーム
CiscoUPSPresenceEngine	プレゼンス エンジンに対するすべてのアラーム
CiscoUPSSIPProxy	SIP プロキシに対するすべてのアラーム
CiscoUPSSoap	Cisco Unified Personal Communicator に対するすべての変更通知アラーム
CiscoUPSSyncAgent	同期エージェントに対するすべてのアラーム
DBAlarmCatalog	Cisco データベース（Aupair）に対するすべてのアラーム定義
DRFAlarmsCatalog	障害復旧フレームワークに対するすべてのアラーム定義
GenericAlarmCatalog	すべてのアプリケーションが共有するすべての汎用アラーム定義
JavaApplications	Cisco CallManager Java Applications に対するすべてのアラーム定義 **（注）** JavaApplications アラームは、アラーム設定のウィンドウからは設定できません。通常、これらのアラームには、これらのアラームをイベント ログに送信して、CiscoWorks2000 との統合に必要な SNMP トラップを生成するための設定を行います。アラーム定義およびパラメータを表示または変更するには、オペレーティング システムに付属のレジストリ エディタを使用してください。
LpmTctCatalog	Log Partition Monitor トレース収集ツールに対するすべてのアラーム
SystemAccessCatalog	プロセスおよびスレッド モニタリングに対するすべてのアラーム
TFTPAlarmCatalog	Cisco TFTP に対するすべてのアラーム定義

関連項目

- アラーム定義の表示およびユーザ指定の記述の追加（P.4-2）
- アラーム定義のカタログ記述（P.4-3）

関連項目

PART 4

トレースの設定

CHAPTER 5

トレースの設定

［Trace Configuration］ウィンドウでは、Cisco Unified Presence の問題をトラブルシューティングするときにトレースするパラメータを指定できます。トレースする情報のレベル（デバッグ レベル）、トレース対象の情報（トレース フィールド）、およびトレース ファイルに関する情報（サービスごとのファイル数、ファイル サイズなど）を設定できます。1 つのサービスに対してトレースを設定することも、そのサービスに対するトレース設定をクラスタ内のすべてのサーバに適用することもできます。

さまざまなサービスのトレース ファイルにどの情報を記録するかを設定した後、Real-Time Monitoring Tool（RTMT）で Trace & Log Central のオプションを使用してトレース ファイルを収集することができます。トレースを収集する方法の詳細については、P.10-1 の「RTMT の トレース収集とログ集中管理」を参照してください。

(注) トレースを有効にすると、システム パフォーマンスが低下します。このため、トラブルシューティングを行う場合にだけトレースを有効にしてください。トレースの使用方法については、Cisco TAC にお問い合せください。

この章は、次の項で構成されています。

トレース パラメータの設定

この項では、Cisco Presence のサービスに対してトレース パラメータを設定する方法について説明します。

手順

ステップ 1　［**Trace**］>［**Configuration**］を選択します。

［Trace Configuration］ウィンドウが表示されます。

ステップ 2　［Server］ドロップダウン リスト ボックスから、トレースを設定する対象のサービスが動作しているサーバを選択し、［**Go**］をクリックします。

ステップ 3　［Service Group］ドロップダウン リスト ボックスから、トレースを設定する対象のサービスのサービス グループを選択し、［**Go**］をクリックします。

ステップ 4　［Service］ドロップダウン　リスト　ボックスから、トレースを設定する対象のサービスを選択し、［**Go**］をクリックします。

（注）　ドロップダウン リスト ボックスに、すべての（アクティブおよび非アクティブの）サービスが表示されます。

選択したサービスのトレース パラメータが表示されます。

（注）　このサービスに対してトラブルシューティング トレースを設定した場合、トラブルシューティング トレースが設定されていることを示すメッセージがウィンドウの上部に表示されます。ウィンドウでは、［Output Settings］以外のすべてのフィールドが無効になります。［Output Settings］を設定するには、ステップ 10 に進みます。トラブルシューティング トレースをリセットするには、P.6-1 の「トラブルシューティング トレース設定値の設定」を参照してください。

ステップ 5　クラスタ内のすべての Cisco Unified Presence のサーバにトレースを適用する場合は、［**Apply to All Nodes**］チェックボックスをオンにします。

ステップ 6　［**Trace On**］チェックボックスをオンにします。

ステップ 7　［Debug Trace Level］ドロップダウン リスト ボックスから、P.5-4 の「デバッグ トレース レベルの設定値」の説明に従って、トレースする情報のレベルを選択します。

ステップ 8　選択したサービスの［Trace Field］チェックボックス（たとえば Cisco UPS SIP Proxy Trace Fields）をオンにします。

ステップ 9　選択したサービスに複数のトレース フィールドが存在する場合（Cisco UP SIP プロキシ サービスなどの場合）は、有効にするトレース フィールドの横にあるチェックボックスをオンにします。Cisco UP SIP プロキシ サービスのトレース フィルタ設定の詳細については、表 5-1 を参照してください。

ステップ 10　トレース ファイルの数とサイズを制限するには、トレース出力設定を指定します。説明とデフォルト値については、表 5-3 を参照してください。

ステップ 11　トレース パラメータの設定を保存するには、［**Save**］ボタンをクリックします。

Cisco Messaging Interface を除き、すべてのサービスに対するトレース設定の変更は、即時に有効になります。Cisco Messaging Interface に対するトレース設定の変更は、3 ～ 5 分以内に有効になります。

（注）　デフォルトを設定するには、［**Set Default**］ボタンをクリックします。

表 5-1　Cisco UP SIP プロキシ サービス パラメータのトレース フィルタの設定値

パラメータ	説明
Enable CTI Gateway Trace	このパラメータは、CTI ゲートウェイのトレースを有効にします。
Enable Parser Trace	このパラメータは、per-sipd チャイルド SIP パーサーの操作に関連するパーサー情報のトレースを有効にします。
Enable SIP TLS Trace	このパラメータは、TCP サービスによる SIP メッセージの TLS 転送に関連する情報のトレースを有効にします。
Enable Privacy Trace	このパラメータは、プライバシー要求に関連する PAI、RPID、および Diversion ヘッダーの処理についての情報のトレースを有効にします。
Enable Routing Trace	このパラメータは、Routing モジュールのトレースを有効にします。
Enable IPPM Trace	このパラメータは、IP Phone Messenger のトレースを有効にします。
Enable SIPUA Trace	このパラメータは、SIP UA アプリケーション モジュールのトレースを有効にします。
Enable SIP Message and State Machine Trace	このパラメータは、per-sipd SIP ステートマシンの操作に関連する情報のトレースを有効にします。
Enable SIP TCP Trace	このパラメータは、TCP サービスによる SIP メッセージの TCP 転送に関連する情報のトレースを有効にします。
Enable Authentication Trace	このパラメータは、Authentication モジュールのトレースを有効にします。
Enable Enum Trace	このパラメータは、ENUM モジュールのトレースを有効にします。
Enable Registry Trace	このパラメータは、Registry モジュールのトレースを有効にします。
Enable Method/Event Routing Trace	このパラメータは、Method/Event ルーティング モジュールのトレースを有効にします。
Enable CALENDAR Trace	このパラメータは、Calendar モジュールのトレースを有効にします。

追加情報

P.5-5 の「関連項目」を参照してください。

デバッグ トレース レベルの設定値

表 5-2 に、サービスのデバッグ トレース レベルの設定値を示します。

表 5-2　サービスのデバッグ トレース レベル

レベル	説明
Arbitrary	すべての Entry/Exit 状態に加えて、低いレベルのデバッグ情報をトレースします。 **（注）** Cisco UPS Presence Engine サービスまたは Cisco IP Voice Media Streaming Application サービスに対して、通常の運用中にこのトレース レベルを使用しないでください。
Debug	すべての State Transition 状態に加えて、通常の運用中に発生するメディア レイヤ イベントをトレースします。 すべてのログ記録をオンにするトレース レベルです。
Detailed	すべての Arbitrary 状態に加えて、詳細なデバッグ情報をトレースします。 **（注）** Cisco UPS Presence Engine サービスまたは Cisco IP Voice Media Streaming Application サービスに対して、通常の運用中にこのトレース レベルを使用しないでください。
Entry/Exit	すべての Significant 状態に加えて、ルーチンの Entry Point と Exit Point をトレースします。このトレース レベルを使用しないサービスもあります（たとえば、Cisco Presence は使用しません）。
Error	アラーム状態とイベントをトレースします。異常なパスで生成されたすべてのトレースに使用されます。最小限の CPU サイクルを使用します。
Fatal	アプリケーションの中止の原因となる、非常に重大なエラー イベントをトレースします。
Info	servlet の問題の大部分をトレースします。システムのパフォーマンスに対する影響は最小限です。
Significant	すべての State Transition 状態に加えて、通常の運用中に発生するメディア レイヤ イベントをトレースします。
Special	すべての Error 状態に加えて、プロセス メッセージとデバイス初期化メッセージをトレースします。
State Transition	すべての Special 状態に加えて、通常の運用中に発生するサブシステムの状態遷移をトレースします。
Warn	潜在的に有害な状況をトレースします。

追加情報

P.5-5 の「関連項目」を参照してください。

トレース出力設定値の説明とデフォルト値

表 5-3 に、トレース ログ ファイルの説明とデフォルト値を示します。

注意

Maximum No. of Files または Maximum File Size のいずれかのパラメータを変更すると、サービスが実行中の場合は、現在のファイルを除くすべてのサービス ログ ファイルが削除され、サービスがアクティブにされていない場合は、サービスが最初にアクティブにされたときにファイルが削除されます。ログ ファイルの記録を保存する場合は、Maximum No. of Files パラメータまたは Maximum File Size パラメータを変更する前に、必ずサービス ログ ファイルをダウンロードして別のサーバに保存してください。

表 5-3　トレース出力設定値

フィールド	説明
Maximum number of files	このフィールドには、特定のサービスに対するトレース ファイルの合計数を指定します。Cisco Unified Presence は、各ファイルを識別するために、ファイル名にシーケンス番号を自動的に追加します（例：esp000005）。シーケンスの最後のファイルが満杯になると、トレース データは最初のファイルに上書きされます。デフォルト値は、サービスによって異なります。
Maximum file size (MB)	このフィールドには、トレース ファイルの最大サイズを MB 単位で指定します。デフォルト値は、サービスによって異なります。

追加情報

P.5-5 の「関連項目」を参照してください。

関連項目

- トレース パラメータの設定（P.5-2）
- トレース出力設定値の説明とデフォルト値（P.5-5）
- デバッグ トレース レベルの設定値（P.5-4）

関連項目

CHAPTER 6

トラブルシューティング トレース設定値の設定

［Troubleshooting Trace Settings］ウィンドウでは、トラブルシューティング トレースの事前設定値を設定する対象の Cisco Unified Presence のサービスを選択できます。この章では、特定のサービスのトラブルシューティング トレース設定値を設定またはリセットする方法について説明します。

（注） 長時間にわたってトラブルシューティング トレースを有効にすると、トレース ファイルのサイズが増大し、サービスのパフォーマンスに影響を与える可能性があります。

手順

ステップ 1 ［**Trace**］>［**Troubleshooting Trace Settings**］の順に選択します。

ステップ 2 ［Server］ドロップダウン リスト ボックスから、トラブルシューティング トレース設定値を設定する対象のサーバを選択し、［**Go**］をクリックします。

（注） サービスのリストが表示されます。Cisco Unified Presence ノードでアクティブにされていないサービスは、N/A と表示されます。

ステップ 3 次のいずれかの操作を実行します。

- ［Server］ドロップダウン リスト ボックスで選択したノードの特定のサービスをチェックするには、［Database and Admin Services］ペイン、［Performance and Monitoring Services］ペイン、［Backup and Restore Services］ペインなどのサービスペインで、そのサービスのチェックボックスをオンにします。

  この操作は、［Server］ドロップダウン リスト ボックスで選択したノードにのみ影響します。
- 次のいずれかのチェックボックスをオンにします。
  - ［**Check All Services**］：［Server］ドロップダウン リスト ボックスで選択した現在のノード上にあるすべてのサービスのチェックボックスを自動的にオンにします。
  - ［**Check Selected Services on All Nodes**］：［TroubleshootingTrace Setting］ウィンドウで特定のサービスのチェックボックスをオンにします。この設定は、そのサービスがアクティブになっているクラスタ内のすべてのノードに適用されます。

— ［**Check All Services on All Nodes**］：クラスタ内のすべてのノードのすべてのサービスのチェックボックスを自動的にオンにします。このチェックボックスをオンにすると、［Check All Services］チェックボックスと［Check Selected Services on All Nodes］チェックボックスが自動的にオンになります。

ステップ 4　［**Save**］ボタンをクリックします。

ステップ 5　1 つ以上のサービスに対してトラブルシューティング トレースを設定した後は、元のトレース設定値を復元できます。元のトレース設定値を復元するには、次のいずれかのボタンをクリックします。

- ［**Reset Troubleshooting Traces**］：［Server］ドロップダウン リスト ボックスで選択したノード上のサービスに元のトレース設定値を復元し、クリック可能なアイコンとして表示します。
- ［**Reset Troubleshooting Traces On All Nodes**］：クラスタ内のすべてのノード上のサービスに元のトレース設定値を復元します。

［Reset］ボタンをクリックすると、ウィンドウが更新され、［Service］チェックボックスがオフの状態で表示されます。

（注）　［Reset Troubleshooting Traces］ボタンは、1 つ以上のサービスに対してトラブルシューティング トレースを設定した場合にのみ表示されます。

追加情報

P.6-2 の「関連項目」を参照してください。

関連項目

- トレースの設定（P.5-1）

PART 5

モニタリング ツールの設定

CHAPTER 7

Real-Time Monitoring の設定

この章では、Cisco Unified Presence Real-Time Monitoring Tool（RTMT）を設定する手順について説明します。

ヒント インストールされている RTMT のバージョンが、クラスタ内で動作している Cisco Unified CallManager のバージョンと互換性があることを確認してください。たとえば、Cisco Unified CallManager 5.X をサポートしている RTMT のバージョンは、Cisco Unified CallManager 6.X をサポートしていません。Cisco Unified CallManager 5.0 をサポートしている RTMT のバージョンは、Cisco Unified CallManager 5.1 をサポートしています。異なるバージョンの Cisco Unified CallManager が同時に動作しているクラスタをモニタするには、複数のバージョンの RTMT（Cisco Unified CallManager のリリースごとに 1 つのバージョン）をインストールする必要があります。複数のバージョンのプラグインをインストールする場合、そのバージョンが異なるフォルダに存在する限り、同じクライアント上に複数のバージョンをインストールできます。インストールによってフォルダ内に別のバージョンが検出された場合は、メッセージが表示されます。インストールを続行するには、そのバージョンを別のフォルダにインストールします。

ヒント アラート、パフォーマンス モニタリング、トレース収集、Syslog Viewer の設定については、P.7-13 の「参考情報」を参照してください。

Real-Time Monitoring Tool（RTMT）のインストール

RTMT は、800*600 以上の解像度で動作し、Windows 98、Windows XP、Windows 2000、または Red Hat Linux with KDE や Gnome クライアントにインストールできます。

（注） Microsoft Windows で稼働する Cisco Unified CallManager サーバと連携するように RTMT がすでにインストールされている場合、Cisco Unified Presence 対応の RTMT をローカル コンピュータの別のフォルダにインストールする必要があります。

ツールをインストールするには、次の手順を実行します。

手順

ステップ 1　Cisco Unified Presence の管理ページで、［**アプリケーション**］>［**プラグイン**］の順に選択します。

ステップ 2　［**検索**］ボタンをクリックします。

ステップ 3　Microsoft Windows オペレーティング システムを実行しているコンピュータに RTMT ツールをインストールする場合は、Cisco Unified Presence Real-Time Monitoring Tool-Windows の［**ダウンロード**］リンクをクリックします。Linux オペレーティング システムを実行しているコンピュータに RTMT ツールをインストールする場合は、Cisco Unified Presence Real-Time Monitoring Tool-Linux の［**ダウンロード**］リンクをクリックします。

ステップ 4　実行ファイルを適切な場所にダウンロードします。

ステップ 5　Windows バージョンをインストールするには、デスクトップに表示された RTMT アイコンをダブルクリックするか、ファイルのダウンロード先のディレクトリから RTMT インストール ファイルを実行します。抽出プロセスが開始されます。

Linux バージョンをインストールするには、たとえば **chmod +x CcmServRtmtPlugin.bin** というコマンド（大文字と小文字の区別あり）を入力して、ファイルに実行権限があることを確認します。

ステップ 6　［RTMT welcome］ウィンドウで［**Next**］をクリックします。

ステップ 7　ライセンス契約書に同意するには、［**Yes**］をクリックします。

ステップ 8　RTMT　　のインストール先を選択します。デフォルト以外の場所にインストールする場合は、［Browse］をクリックし、別の場所に移動します。［**Next**］をクリックします。

ステップ 9　インストールを開始するには、［**Next**］をクリックします。

設定状況に関するウィンドウが表示されます。［Cancel］をクリックしないでください。

ステップ 10　インストールを完了するには、［**Finish**］をクリックします。

追加情報

P.7-13 の「関連項目」を参照してください。

RTMT のアップグレード

ツール（RTMT）を使用すると、ユーザ プリファレンスやダウンロードされたモジュールの jar ファイルは、クライアント　　マシンにローカルに保存されます。システムはプロファイルを Cisco Unified Presence データベースに保存するので、RTMT のアップグレード後もこれらの項目に RTMT でアクセスできます。

ヒント　互換性を確保するため、クラスタ内のすべてのサーバ上で Cisco Unified Presence をアップグレードした後に RTMT をアップグレードすることをお勧めします。

RTMT をアップグレードするには、次の手順を実行します。

手順

ステップ 1　Cisco Unified Presence の管理ページで、［**アプリケーション**］>［**プラグイン**］の順に選択します。

ステップ 2　［**検索**］ボタンをクリックします。

ステップ 3　Microsoft Windows オペレーティング システムを実行しているコンピュータに RTMT ツールをインストールする場合は、Cisco Unified CallManager Real-Time Monitoring Tool-Windows の［**ダウンロード**］リンクをクリックします。Linux オペレーティング システムを実行しているコンピュータに RTMT ツールをインストールする場合は、Cisco Unified CallManager Real-Time Monitoring Tool-Linux の［**ダウンロード**］リンクをクリックします。

ステップ 4　実行ファイルを適切な場所にダウンロードします。

ステップ 5　デスクトップに表示された RTMT アイコンをダブルクリックするか、ファイルのダウンロード先のディレクトリから RTMT インストール ファイルを実行します。抽出プロセスが開始されます。

Linux バージョンをインストールするには、たとえば **chmod +x CcmServRtmtPlugin.bin** というコマンド（大文字と小文字の区別あり）を入力して、ファイルに実行権限があることを確認します。

ステップ 6　［RTMT welcome］ウィンドウで［**Next**］をクリックします。

ステップ 7　アップグレードの場合はインストール先を変更できないので、［**Next**］をクリックします。

設定状況に関するウィンドウが表示されます。［**Cancel**］をクリックしないでください。

ステップ 8　インストール完了ウィンドウで［**Finish**］をクリックします。

追加情報

P.7-13 の「関連項目」を参照してください。

RTMT のアンインストール

ヒント　RTMT を使用すると、ユーザ プリファレンスやモジュールの jar ファイル（キャッシュ）は、クライアント マシンにローカルに保存されます。サーバ データベースのキャッシュも保存されます。RTMT をアンインストールするときは、キャッシュを削除するか保存するかを選択します。

Windows クライアントで RTMT をアンインストールするには、［コントロール パネル］の**［アプリケーションの追加と削除］**を使用します（［スタート］>［設定］>［コントロール パネル］>［アプリケーションの追加と削除］）。

KDE や Gnome クライアントを使用した Red Hat Linux で RTMT をアンインストールするには、タスクバーから**［Start］**>**［Accessories］**>**［Uninstall Real-time Monitoring tool］**の順に選択します。

追加情報

P.7-13 の「関連項目」を参照してください。

RTMT の起動

開始する前に

RTMT を使用する前に、クラスタ内の各ノードで Cisco AMC Service をアクティブにする必要があります。Cisco Unified Presence Serviceability から［**Tools**］>［**Service Activation**］の順に選択し、［**Cisco AMC Service**］チェックボックスをオンにします。［**Update**］をクリックします。

手順

ステップ 1　プラグインをインストールした後、次のいずれかの操作を実行します。

- Windows デスクトップで、［**Cisco Unified CallManager Real-Time Monitoring Tool**］アイコンをダブルクリックします。
- ［**スタート**］>［**プログラム**］>［**Cisco CallManager Serviceability**］>［**Real-Time Monitoring Tool**］>［**Real-Time Monitoring Too**］**l** の順に選択します。

［Real-Time Monitoring Tool Login］ウィンドウが表示されます。

ステップ 2　［Host IP Address］フィールドに、ファースト ノードの IP アドレスまたはホスト名を入力します。

ステップ 3　［User Name］フィールドに、CCMAdministrator アプリケーションのユーザ名を入力します。たとえば、このユーザのデフォルトのユーザ名は、**CCMAdministrator** です。

ステップ 4　［Password］フィールドに、CCMAdministrator アプリケーションのユーザ名に対応するユーザ パスワードを入力します。

（注）　認証に失敗した場合、またはサーバに到達できない場合は、サーバと認証の詳細を再入力するように求められます。また、［Cancel］ボタンをクリックして、アプリケーションを終了することもできます。認証に成功した場合は、RTMT により、ローカル キャッシュまたはリモート ノードからモニタリング モジュールが起動されます。リモート ノードは、バックエンドの Cisco Unified Presence バージョンと一致するモニタリング モジュールがローカル キャッシュに含まれていない場合に使用されます。

ステップ 5　アプリケーションがサーバのリッスンに使用するポートを入力します。デフォルト設定は 8443 です。

ステップ 6　［**Secure Connection**］チェックボックスをオンにします。

ステップ 7　［**OK**］をクリックします。

ステップ 8　［**Yes**］をクリックして、証明書ストアを追加します。

追加情報

P.7-13 の「関連項目」を参照してください。

RTMT のナビゲーション

RTMT ウィンドウは、次の主要コンポーネントで構成されています。

- メニュー バーには、次のメニュー オプションがあります。
  - File：既存の RTMT プロファイルの保存、復元、および削除、Java ヒープ メモリ使用状況のモニタ、Cisco Unified サービスアビリティの［Serviceability Report Archive］ウィンドウへの移動、RTMT のログオフまたは終了を行います。
  - System：システム サマリーのモニタ、サーバ リソースのモニタ、パフォーマンス カウンタの操作、アラートの操作、トレースの収集、syslog メッセージの表示を行います。
  - CUP：サーバの Cisco Unified CallManager サマリー情報を表示します。
  - Edit：カテゴリの設定（表形式での表示用）、デバイスおよびパフォーマンス モニタリング カウンタのポーリング レートの設定、［Quick Launch Channel］の非表示、RTMT のトレース設定値の編集を行います。
  - Window：1 つまたはすべての RTMT ウィンドウを閉じます。
  - Application：管理ページおよびサービスアビリティの Web ページを参照します。
  - Help：RTMT のマニュアルのオンライン ヘルプにアクセスするか、RTMT のバージョンを参照します。
- ［Quick Launch Channel］：クリックするとサーバの情報やアプリケーションの情報が表示されるタブを持つ、RTMT ウィンドウの左側にあるペインです。タブには、クリックして各種オブジェクトをモニタできる複数のアイコンがあります。
- ［Monitor］ペイン：モニタリング結果を表示するペインです。

追加情報

P.7-13 の「関連項目」を参照してください。

構成プロファイルの操作

この項では、次のトピックについて取り上げます。

デフォルトの構成プロファイルの使用

RTMT を初めてロードすると、CM-Default という名前のデフォルト設定が適用されます。RTMT を初めて使用すると、CM-Default プロファイルが使用され、モニタ ペインに要約ページが表示されます。

独自の構成プロファイルを作成する方法については、P.7-7 の「構成プロファイルの追加」を参照してください。

追加情報

P.7-13 の「関連項目」を参照してください。

構成プロファイルの追加

RTMT で複数のモニタリング ウィンドウ（CPU & Memory やパフォーマンス カウンタなど）を開いた後、独自の構成プロファイルを作成すると、これらのウィンドウを個別に開かなくても 1 つの操作でこれらのモニタリング ウィンドウを復元できます。同じ RTMT セッションで複数の異なるプロファイルを切り替えたり、後続の RTMT セッションで同じプロファイルを使用したりすることもできます。

プロファイルを作成する手順は、次のとおりです。

手順

ステップ 1　［**System**］>［**Profile**］の順に選択します。

［Preferences］ダイアログボックスが表示されます。

ステップ 2　［**Save**］をクリックします。

［Save Current Configuration］ダイアログボックスが表示されます。

ステップ 3　［Configuration name］フィールドに、この構成プロファイルの名前を入力します。

ステップ 4　Configuration description フィールドに、この構成プロファイルの説明を入力します。

（注）　構成プロファイルの名前と説明は任意に入力できます。

新しい構成プロファイルが作成されます。

追加情報

P.7-13 の「関連項目」を参照してください。

プロファイルの復元

構成済みのプロファイルを復元するには、次の手順を実行します。

手順

ステップ 1　［**System**］>［**Profile**］の順に選択します。

［Preferences］ダイアログボックスが表示されます。

ステップ 2　復元するプロファイルをクリックします。

ステップ 3　［**Restore**］をクリックします。

復元された構成に対する、あらかじめ用意されている設定やパフォーマンス モニタリング カウンタのすべてのウィンドウが開きます。

追加情報

P.7-13 の「関連項目」を参照してください。

構成プロファイルの削除

構成済みのプロファイルを削除するには、次の手順を実行します。

手順

ステップ 1　［**System**］>［**Profile**］の順に選択します。

［Preferences］ダイアログボックスが表示されます。

ステップ 2　削除するプロファイルをクリックします。

ステップ 3　［**Delete**］をクリックします。

ステップ 4　［**Close**］をクリックします。

追加情報

P.7-13 の「関連項目」を参照してください。

事前定義オブジェクトの操作

ツール（RTMT）には、システムの状況をモニタするデフォルトのモニタリング オブジェクトのセットが用意されています。デフォルト　オブジェクトには、パフォーマンス　カウンタや Cisco Unified Presence でサポートされているサービスについての重要なイベント ステータスが含まれています。

この項では、次のトピックについて取り上げます。

- 事前定義オブジェクトの表示とモニタリング（P.7-9）
- ポーリング レート パフォーマンス モニタリング カウンタの設定（P.7-11）

事前定義オブジェクトの表示とモニタリング

カテゴリ（つまり、事前定義オブジェクト）のモニタリング ペインには、事前定義モニタリング オブジェクトのアクティビティが表示されます。カテゴリの情報を表示する手順は、次のとおりです。

ヒント　事前定義オブジェクトのモニタ上で拡大表示するには、マウスの左ボタンをクリックし、図の必要な領域上にドラッグします。領域を選択したら、マウスの左ボタンを放します。モニタリングしている表示が、RTMT により更新されます。モニタを縮小して最初のデフォルト表示にリセットするには、**R** キーを押します。

手順

ステップ 1　カテゴリを表示またはモニタするには、［Quick Launch Channel］で［System］または［CUP］をクリックします。

［Quick Laungh Channel］で［System］を選択すると、仮想メモリの使用状況など、事前定義のシステム オブジェクトに関する情報が表示されます。［Quick Launch Channel］で［CUP］を選択すると、PE Active Subscription など、事前定義の Cisco Unified Presense Server オブジェクトに関する情報がモニタリング ペインに表示されます。RTMT は、クラスタ内のすべてのノード上の事前定義オブジェクトをモニタします。

ステップ 2　［Summary］や［Server］などのカテゴリをクリックします。カテゴリのアイコンが表示されている場合は、アイコンをクリックして、モニタする情報を表示します。

（注）　現在のバージョンの RTMT にあるオプションには、Cisco Unified Presence に適用されないものもあります。

ステップ 3　表示するカテゴリに応じて、次の 表 7-1 から、いずれかのオプションを選択します。

表 7-1　モニタリング カテゴリ

カテゴリ	表示されるデータ
CUP Summary	PE Active Subscription、Proxy SIP Message Requests In、Proxy SIP Message Requests Out、Proxy SIP Register Requests In、Proxy SIP Subscribe Requests In、JVM Memory に関する情報を表示します。 事前定義のシステム オブジェクトに関する情報を表示するには、［**CUP**］>［**CUP Summary**］の順に選択します。
System Summary	仮想メモリの使用状況、CPU 使用状況、共通パーティションの使用状況、アラート履歴ログに関する情報を表示します。事前定義のシステム オブジェクトに関する情報を表示するには、［**System**］>［**System Summary**］の順に選択します。
Server	• CPU and Memory：各サーバの CPU 使用状況と仮想メモリの使用状況に関する情報を表示します。 CPU および仮想メモリの使用状況に関する情報を表示するには、［**System**］>［**Server**］>［**CPU and Memory**］の順に選択します。特定のサーバの CPU およびメモリの使用状況をモニタするには、［Host］ドロップダウン リスト ボックスからサーバを選択します。 • Process：各サーバ上で動作しているプロセスに関する情報を表示します。 システム上で動作しているプロセスに関する情報を表示するには、［**System**］>［**Server**］>［**Process**］の順に選択します。特定のサーバのプロセス使用状況をモニタするには、［Host］ドロップダウン リスト ボックスからサーバを選択します。 • Disk Usage：各サーバのディスク使用状況に関する情報を表示します。システム上のディスク使用状況に関する情報を表示するには、［**System**］>［**Server**］>［**Disk Usage**］の順に選択します。特定のサーバのディスク使用状況をモニタするには、［Host］ドロップダウン リスト ボックスからサーバを選択します。 • Critical Services：サーバ上で動作しているサービスのステータスに関する情報を表示します。重要なサービスに関する情報を表示するには、［**System**］>［**Server**］>［**Critical Services**］の順に選択します。 システムの重要なサービスを表示するには、［System］タブをクリックします。Cisco Unified Presense Server の重要なサービスを表示するには、［CUP］タブをクリックします。特定のサーバの重要なサービスをモニタするには、［Host］ドロップダウン リスト ボックスからサーバを選択します。
Performance	perfmon カウンタを表示します。 perfmon カウンタを表示するには、［System］>［Performance］>［Performance］の順に選択します。 perfmon カウンタの使用方法の詳細については、P.9-1 の「パフォーマンス モニタリングの設定と使用」を参照してください。

追加情報

P.7-13 の「関連項目」を参照してください。

ポーリング レート パフォーマンス モニタリング カウンタの設定

Cisco Unified Presence は、カウンタをポーリングしてステータス情報を収集します。［RTMT monitoring］ペインでは、パフォーマンス モニタリング カウンタのポーリング間隔を設定します。

（注） ポーリング レートの頻度を高くすると、Cisco Unified Presence のパフォーマンスに悪影響を及ぼすことがあります。図形式でパフォーマンス カウンタをモニタする場合、最小ポーリング レートは 5 秒です。表形式で パフォーマンス カウンタをモニタする場合、最小レートは 1 秒です。デフォルト値はいずれも 10 秒です。

デバイスのデフォルト値は 10 分です。

ポーリング レートを更新するには、次の手順を実行します。

手順

ステップ 1　［RTMT monitoring］ペインに、パフォーマンス モニタリング カウンタを表示します。

ステップ 2　デバイスをクリックし、［**Edit**］>［**Polling Rate**］の順に選択します。

ステップ 3　［Polling Interval］ペインで、使用する時間間隔を指定します。

ステップ 4　［**OK**］をクリックします。

追加情報

P.7-13 の「関連項目」を参照してください。

カテゴリの操作

カテゴリを使用すると、パフォーマンス モニタリング カウンタをモニタできます。たとえば、Cisco UP SIP Proxy カテゴリでは、SIP プロキシのパフォーマンス モニタリング カウンタをグラフ形式でモニタできます。それ以上のカウンタを使用する場合は、新しいカテゴリを設定して、データを表形式で表示できます。

カテゴリの追加

カテゴリを追加するには、次の手順を実行します。

手順

ステップ 1　パフォーマンス モニタリング ツリー階層を表示します。

ステップ 2　［**Edit**］>［**New Category**］の順に選択します。

ステップ 3　カテゴリ名を入力し、［**OK**］をクリックします。

ウィンドウの下部に、カテゴリのタブが表示されます。

追加情報

- P.7-13 の「関連項目」を参照してください。

カテゴリ名の変更

カテゴリ名を変更するには、次の手順を実行します。

手順

ステップ 1　次のいずれかの操作を実行します。

- 名前を変更するカテゴリのタブを右クリックし、［**Rename Category**］を選択します。
- 名前を変更するカテゴリのタブをクリックし、［**Edit**］>［**Rename Category**］の順に選択します。

ステップ 2　新しい名前を入力し、［**OK**］をクリックします。

ウィンドウの下部に、変更後のカテゴリ名が表示されます。

追加情報

- P.7-13 の「関連項目」を参照してください。

カテゴリの削除

カテゴリを削除するには、次のいずれかの操作を実行します。

- 削除するカテゴリのタブを右クリックし、［**Remove Category**］を選択します。
- 削除するカテゴリのタブをクリックし、［**Edit**］>［**Remove Category**］の順に選択します。

追加情報

P.7-13 の「関連項目」を参照してください。

参考情報

- RTMT でのアラート設定（P.8-1）
- パフォーマンス モニタリングの設定と使用（P.9-1）
- RTMT の トレース収集とログ集中管理（P.10-1）

追加情報

P.7-13 の「関連項目」を参照してください。

関連項目

- カテゴリの追加（P.7-12）
- カテゴリ名の変更（P.7-12）
- カテゴリの削除（P.7-13）
- パフォーマンス モニタリングの設定と使用（P.9-1）
- ポーリング レート パフォーマンス モニタリング カウンタの設定（P.7-11）
- ポーリング レート パフォーマンス モニタリング カウンタの設定（P.7-11）
- デフォルトの構成プロファイルの使用（P.7-7）
- プロファイルの復元（P.7-8）
- デフォルトの構成プロファイルの使用（P.7-7）
- 構成プロファイルの削除（P.7-8）
- 構成プロファイルの追加（P.7-7）
- 構成プロファイルの操作（P.7-7）
- 事前定義オブジェクトの操作（P.7-9）
- RTMT でのアラート設定（P.8-1）
- パフォーマンス モニタリングの設定と使用（P.9-1）
- RTMT SysLog Viewer の使用（P.11-1）
- Real-Time Monitoring Tool（RTMT）のインストール（P.7-2）
- RTMT のナビゲーション（P.7-6）
- RTMT のアンインストール（P.7-4）
- RTMT のアップグレード（P.7-3）
- RTMT の起動（P.7-5）

関連項目

CHAPTER 8

RTMT でのアラート設定

RTMT では、あらかじめ設定されているアラートとカスタム アラートの両方が Alert Central に表示されます。RTMT では、アラートは［System］タブ、［CUP］タブ、［Custom］タブに整理されます。どちらの種類のアラートも設定できますが、あらかじめ設定されているアラートは削除できません。あらかじめ設定されているアラートやユーザ定義のアラートを RTMT で無効にすることができます。

あらかじめ設定されているアラート、アラートのカスタマイゼーション、およびアラートを設定できるアラート アクション フィールドについては、『*Cisco Unified CallManager Serviceability システム ガイド*』の「アラート」を参照してください。

アクティブにされているサービスが稼働状態から停止状態になると、RTMT によりアラートが生成されます。Alert Central を使用して、RTMT によって生成されるアラートの状況と履歴を表示できます。

この章は、次の項で構成されています。

アラートの操作

次の手順を実行して、Alert Central へのアクセス、アラート情報のソート、アラートの有効化、無効化、削除、アラートのクリア、またはアラート詳細の表示などの操作を実行できます。

手順

ステップ 1　次のいずれかの操作を実行します。

- ［Quick Launch Channel］で、次の操作を実行します。
  - ［**System**］をクリックします。
  - ツリー階層で、［**Tools**］をダブルクリックします。
  - ［Alert Central］アイコンをクリックします。
- ［**System**］>［**Tools**］>［**Alert**］>［**Alert Central**］の順に選択します。

［Alert Central］モニタリング ウィンドウが表示され、アラートのステータスとシステムが生成したアラートの履歴が表示されます。

ステップ 2　次のいずれかの操作を実行します。

- アラートのプロパティを設定する場合は、P.8-4 の「アラート プロパティの設定」を参照してください。
- Cisco Unified Presence ノードのアラートを一時停止する場合は、P.8-7 の「Cisco Unified Presence ノードまたはクラスタ上のアラートの一時停止」を参照してください。
- アラートの電子メール通知を設定する場合は、P.8-8 の「アラート通知用電子メールの設定」を参照してください。
- アラート アクションを設定する場合は、P.8-8 の「アラート アクションの設定」を参照してください。
- ［Alert Status］ペイン内のアラート情報をソートする場合は、列見出しで上向き矢印または下向き矢印をクリックします。たとえば、［Enabled］列や［InSafeRange］列の上向き矢印または下向き矢印をクリックします。

  ［Alert History］ペインの列の上向き矢印または下向き矢印をクリックすると、アラート履歴情報をソートできます。ペインに表示されていないアラート履歴を表示するには、［Alert History］ペインの右側にあるスクロール バーを使用します。
- アラートを有効化、無効化、または削除するには、次のいずれかの操作を実行します。
  - ［Alert Status］ウィンドウで、アラートを右クリックし、目的の操作に応じて、［**Disable/Enable Alert**］（オプション トグル）または［**Remove Alert**］を選択します。
  - ［Alert Status］ウィンドウでアラートを強調表示し、［**System**］>［**Tools**］>［**Alert**］>［**Disable/Enable**（または **Remove**）**Alert**］の順に選択します。

ヒント　ユーザ定義のアラートに限り、RTMT から削除できます。あらかじめ設定されているアラートを選択すると、［Remove Alert］オプションがグレー表示されます。

- アラートを解決した後、アラートを個別に、またはまとめてクリアするには、次のいずれかの操作を実行します。
  - ［Alert Status］ウィンドウが表示されたら、アラートを右クリックし、［**Clear Alert**］（または［**Clear All Alerts**］）を選択します。
  - ［Alert Status］ウィンドウでアラートを強調表示し、［**System**］>［**Tools**］>［**Alert**］>［**Clear Alert**］（または［**Clear All Alerts**］）の順に選択します。

アラートをクリアすると、アラートの色が赤から黒に変わります。

- アラートの詳細を表示するには、次のいずれかの操作を実行します。
  - ［Alert Status］ウィンドウが表示されたら、アラートを右クリックし、［**Alert Details**］を選択します。
  - ［Alert Status］ウィンドウでアラートを強調表示し、［**System**］>［**Tools**］>［**Alert**］>［**Alert Details**］の順に選択します。

ヒント　アラートの詳細を確認したら、［**OK**］をクリックします。

追加情報

P.8-8 の「関連項目」を参照してください。

アラート プロパティの設定

アラート プロパティを設定する手順は、次のとおりです。

手順

ステップ 1　P.8-2 の「アラートの操作」の説明に従って、Alert Central を表示します。

ステップ 2　［Alert Status］ウィンドウで、アラート プロパティを設定するアラートをクリックします。

ステップ 3　次のいずれかの操作を実行します。

- アラートを右クリックし、［**Set Alert/Properties**］を選択します。
- ［**System**］>［**Tools**］>［**Alert**］>［**Set Alert/Properties**］の順に選択します。

（注）　Cisco Unified Presence のクラスタ全体のアラートの場合は、［Alert Properties］ウィンドウに［Enable/Disable this alert on following server(s):］ボックスが表示されません。クラスタ全体のアラートには、登録済みの電話機の数、ゲートウェイの数、メディア デバイスの数、すべて使用されたルート リスト、すべて使用されたメディア リスト、稼働していない MGCP D チャネル、悪意のあるコールのトレース、および限度を超えている品質レポートが含まれます。

ステップ 4　アラートを有効にするには、［**Enable Alert**］チェックボックスをオンにします。

ステップ 5　［Severity］ドロップダウン リスト ボックスから、アラートの重大度を選択します。

ステップ 6　［Enable/Disable this alert on following server(s)］ペインで、このアラートを有効にするサーバの［Enable］チェックボックスをオンにします。

あらかじめ設定されているアラートについては、［Description 情報］ペインにアラートの説明が表示されます。

ステップ 7　［**Next**］をクリックします。

ステップ 8　［Threshold］ペインに、システムがアラートをトリガーする条件を入力します。

ステップ 9　［Duration］ペインで、次のいずれかのオプション ボタンをクリックします。

- ［Trigger alert only when below or over....］オプション ボタン：特定の期間（秒単位）に常に値がしきい値を下回るまたは上回る場合に限り、アラートがトリガーされます。秒数を入力します。
- ［Trigger alert immediately］：アラートがすぐにトリガーされます。

ステップ 10　［**Next**］をクリックします。

ステップ 11　［Frequency］ペインで、次のいずれかのオプション ボタンをクリックします。

- ［trigger alert on every poll］：ポーリングのたびにアラートがトリガーされます。
- ［trigger up to <numbers> of alerts within <number> of minutes］：特定の期間（分単位）内に、特定の数のアラートがトリガーされます。アラートの数と分数を入力します。

ステップ 12［Schedule］ペインで、次のいずれかのオプション ボタンをクリックします。

- ［24-hours daily］：アラートが 1 日 24 時間トリガーされます。
- ［Start time/Stop time］：特定の開始時刻と終了時刻の間のみアラートがトリガーされます。開始時刻と終了時刻を入力します。

ステップ 13［**Next**］をクリックします。

ステップ 14 このアラートの電子メールを有効にする場合は、［Enable Email］チェックボックスをオンにします。

ステップ 15 このアラートでアラート アクションをトリガーするには、ドロップダウン リスト ボックスから、送信するアラート アクションを選択します。

ステップ 16 新しいアラート アクションを設定する場合、または既存のアラート アクションを編集する場合は、［**Configure**］をクリックします。

ステップ 17 新しいアラート アクションを追加するには、次の手順を実行します。

a. ［**Add**］をクリックします。

b. ［Name］フィールドに、アラート アクションの名前を入力します。

c. ［Description］フィールドに、アラート アクションの説明を入力します。

d. 電子メール受信者を追加するには、［**Add**］をクリックします。

e. ［Enter email/epage address］フィールドに、アラート アクションを受信する受信者の電子メールまたは電子ページのアドレスを入力します。

f. ［**OK**］をクリックします。

［Action Configuration］ウィンドウに、追加した受信者が表示され、その［Enable］チェックボックスがオンになっています。

ヒント　電子メールの受信者を削除するには、その受信者を強調表示し、［**Delete**］をクリックします。選択した受信者が、受信者リストから削除されます。

g. すべての受信者を追加したら、［**OK**］をクリックします。

ステップ 18 既存のアラート アクションを編集するには、次の手順を実行します。

a. アラート アクションを強調表示し、［**Edit**］をクリックします。

選択したアラート アクションの［Action Configuration］ウィンドウが表示されます。

b. 設定を変更し、［**OK**］をクリックします。

ステップ 19 アラート アクションの設定を終了したら、［**Close**］をクリックします。

ステップ 20　トレースのダウンロードが許可されていないアラートの場合は、［Alert Properties: Email Notification］ウィンドウで［**Activate**］をクリックします。

CriticalServiceDown や CodeYellow のようにトレースのダウンロードが許可されているアラートの場合は、次の手順を実行します。

a. ［**Next**］をクリックします。

b. ［Alert Properties: TCT Download］ウィンドウで、［Enable TCT Download］チェックボックスをオンにします。

c. ［SFTP Parameters Dialog］ウィンドウが表示されます。IP アドレス、ユーザ名、パスワード、ポート、およびトレースを保存するためのダウンロード ディレクトリ パスを入力します。SFTP サーバとの接続を確認するには、［**Test Connection**］をクリックします。**接続テストに失敗した場合、設定は保存されません。**

d. ［**OK**］をクリックして、設定を保存します。

e. ［TCT Download Parameters］ウィンドウに、ダウンロードの回数と頻度を入力します。ダウンロードの回数と頻度を設定すると、ダウンロードされるトレース ファイルを制限するのに役立ちます。設定されたポーリングが、頻度のデフォルト設定の基準となります。

注意　TCT Download を有効にすると、サーバ上のサービスに影響が生じることがあります。ダウンロード回数を多くすると、サーバのサービス品質に悪影響が生じます。

（注）　アラート アクションを削除するには、そのアクションを強調表示し、［**Delete**］をクリックして、［**Close**］をクリックします。

追加情報

P.8-8 の「関連項目」を参照してください。

Cisco Unified Presence ノードまたはクラスタ上のアラートの一時停止

特定の Cisco Unified Presence ノードまたはクラスタ全体で、一部のアラートまたはすべてのアラートを一時的に停止する必要が生じる場合があります。たとえば、Cisco Unified Presence を新しいリリースにアップグレードする場合、アップグレードが完了するまですべてのアラートを一時停止する必要があります。アラートを一時停止することにより、アップグレード中に電子メールや電子ページを受信しなくなります。Alert Central でアラートを一時停止する手順は、次のとおりです。

手順

ステップ 1　［**System**］>［**Tools**］>［**Alert**］>［Suspend cluster/node Alerts］の順に選択します。

（注）　サーバごとの一時停止状況は、Cisco Unified Presence クラスタ全体のアラートには適用されません。

ステップ 2　クラスタ内のすべてのアラートを一時停止するには、［Cluster Wide］オプション ボタンを選択し、［suspend all alerts］チェックボックスをオンにします。

ステップ 3　サーバごとにアラートを一時停止するには、［Per Server］オプション ボタンを選択し、アラートを一時停止するサーバの［Suspend］チェックボックスをオンにします。

ステップ 4　［**OK**］をクリックします。

（注）　アラートを再開するには、再び［**Alert**］>［**Suspend cluster/node Alerts**］の順に選択し、［Suspend］チェックボックスをオフにします。

追加情報

P.8-8 の「関連項目」を参照してください。

アラート通知用電子メールの設定

アラート通知用の電子メールを設定するには、次の手順を実行します。

手順

ステップ 1　［**System**］>［**Tools**］>［**Alert**］>［**Config Email Server**］の順に選択します。

［Mail Server Configuration］ウィンドウが表示されます。

ステップ 2　［Mail Server］フィールドに、電子メールの受信者の情報を入力します。

ステップ 3　［Port］フィールドに、メール サーバのポート番号を入力します。

ステップ 4　［**OK**］をクリックします。

追加情報

P.8-8 の「関連項目」を参照してください。

アラート アクションの設定

新しいアラート アクションを設定する手順は、次のとおりです。

手順

ステップ 1　P.8-2 の「アラートの操作」の説明に従って、Alert Central を表示します。

ステップ 2　［**Alert**］>［**Config Alert Action**］の順に選択します。

ステップ 3　P.8-4 の「アラート プロパティの設定」のステップ 17 ～ステップ 20 を実行して、アラート アクションを追加、編集、または削除します。

追加情報

P.8-8 の「関連項目」を参照してください。

関連項目

- アラートの操作（P.8-2）
- アラート プロパティの設定（P.8-4）
- Cisco Unified Presence ノードまたはクラスタ上のアラートの一時停止（P.8-7）
- アラート通知用電子メールの設定（P.8-8）
- アラート アクションの設定（P.8-8）

CHAPTER 9

パフォーマンス モニタリングの設定と使用

Cisco Unified Presence のパフォーマンスをモニタするには、RTMT を使用してオブジェクトのカウンタを選択します。フォルダを展開すると、各オブジェクトのカウンタが表示されます。

perfmon カウンタのログはコンピュータにローカルで記録することができ、RTMT の Performance Log Viewer を使用して、収集した perfmon CSV ログ ファイル、または Alert Manager and Collector（AMC）および Realtime Information Server Data Collection（RISDC）の perfmon ログを表示することができます。

トラブルシューティング用の perfmon データのログ記録を有効にし、システム状態に関する包括的な情報を備えた統計情報を一連の perfmon カウンタから自動的に収集することもできます。トラブルシューティング用の perfmon データのログ記録を有効にすると、サーバのシステム パフォーマンスに影響が生じることがあるので注意してください。

この章は、次の項で構成されています。

パフォーマンス カウンタの表示

RTMT は、perfmon カウンタを図形式または表形式で表示します。図形式では、線グラフを使用して perfmon カウンタ情報を表示します。作成したカテゴリ タブごとに、最大 6 つの図を［RTMT Perfmon Monitoring］ペインに表示できます。1 つの図には、最大 3 つのカウンタを表示できます。

ヒント　［RTMT Perfmon Monitoring］ペインの 1 つの図には、カウンタを 3 つまで表示できます。図に別のカウンタを追加するには、カウンタをクリックして［RTMT Perfmon Monitoring］ペインにドラッグします。この操作をもう一度繰り返して、最大 3 つのカウンタを追加します。

デフォルトでは、RTMT は perfmon カウンタを図形式で表示します。perfmon カウンタを表形式で表示するように選択することもできます。perfmon カウンタを表形式で表示するには、新しいカテゴリを作成するときに［**Present Data in Table View**］チェックボックスをオンにします。

機能ベースの一連のカウンタを表示するように perfmon カウンタを整理して、それをカテゴリに保存することができます。RTMT プロファイルを保存した後は、必要なカウンタにすばやくアクセスできます。カテゴリを作成した後に、図形式から表形式あるいはその逆に表示方法を変更することはできません。

手順

ステップ 1　次のいずれかの操作を実行します。

- ［Quick Launch Channel］で、次の操作を実行します。
  - ［**System**］をクリックします。
  - ツリー階層で、［**Performance**］をダブルクリックします。
  - ［**Performance**］アイコンをクリックします
- ［**System**］>［**Performance**］>［**Open Performance Monitoring**］の順に選択します。

ステップ 2　モニタするカウンタの追加先であるサーバの名前をクリックします。

ツリー階層が展開され、そのノードのすべての perfmon オブジェクトが表示されます。

ステップ 3　カウンタを表形式でモニタする場合は、ステップ 4 を参照してください。カウンタを図形式でモニタする場合は、ステップ 5 を参照してください。

ステップ 4　カウンタを表形式でモニタするには、次の手順を実行します。

a.　［**Edit**］>［**New Category**］の順に選択します。

b.　［Enter Name］フィールドにタブ名を入力します。

c.　perfmon カウンタを表形式で表示するには、［**Present Data in Table View**］チェックボックスをオンにします。

d.　［**OK**］をクリックします。

入力した名前の付いた新規タブが、ペインの下部に表示されます。

e.　モニタするカウンタを含むオブジェクト名の横にあるファイル アイコンをクリックします。

ヒント　カウンタを表形式で表示した後、図形式に変更するには、カテゴリ タブを右クリックし、［**Remove Category**］を選択します。カウンタが図形式で表示されます。

ステップ 5　カウンタを図形式でモニタするには、次の操作を実行します。

- モニタするカウンタを含むオブジェクト名の横にあるファイル アイコンをクリックします。カウンタのリストが表示されます。
- カウンタ情報を表示するには、カウンタを右クリックして［**Counter Monitoring**］をクリックするか、カウンタをダブルクリックするか、カウンタを［RTMT Perfmon Monitoring］ペインにドラッグ アンド ドロップします。

［RTMT Perfmon Monitoring］ペインにカウンタの図が表示されます。

追加情報

P.9-15 の「関連項目」を参照してください。

［RTMT Performance Monitoring］ペインからのカウンタの削除

カウンタが必要なくなったときは、［RTMT Perfmon Monitoring］ペインからカウンタを削除できます。この項では、ペインからカウンタを削除する方法について説明します。

次のいずれかの操作を実行します。

- 削除するカウンタを右クリックし、［**Remove**］を選択します。
- 削除するカウンタをクリックし、［**Perfmon**］>［**Remove Chart/Table Entry**］の順に選択します。

［RTMT Perfmon Monitoring］ペインからカウンタの図が消去されます。

追加情報

P.9-15 の「関連項目」を参照してください。

カウンタ インスタンスの追加

カウンタ インスタンスを追加するには、次の手順を実行します。

手順

ステップ 1　P.9-2 の「パフォーマンス カウンタの表示」の説明に従って、パフォーマンス モニタリング カウンタを表示します。

ステップ 2　次のいずれかの操作を実行します。

- パフォーマンス モニタリング ツリー階層で、パフォーマンス モニタリング カウンタをダブルクリックします。
- パフォーマンス モニタリング ツリー階層でパフォーマンス モニタリング カウンタをクリックし、［**System**］>［**Performance**］>［**Counter Instances**］の順に選択します。
- パフォーマンス モニタリング ツリー階層でパフォーマンス モニタリング カウンタを右クリックし、［**Counter Instances**］を選択します。

ステップ 3　［Select Instance］ウィンドウで、インスタンスをクリックし、［**Add**］をクリックします。

カウンタが表示されます。

追加情報

P.9-15 の「関連項目」を参照してください。

カウンタのアラート通知の設定

カウンタに関するアラート通知を設定する手順は、次のとおりです。

ヒント　カウンタのアラートを削除するには、カウンタを右クリックし、［Remove Alert］を選択します。アラートを削除すると、オプションがグレー表示されます。

手順

ステップ 1　P.9-2 の「パフォーマンス カウンタの表示」の説明に従って、パフォーマンス カウンタを表示します。

ステップ 2　カウンタの図または表で、アラート通知を設定する対象のカウンタを右クリックし、**［Set Alert/Threshold］**を選択します。

ステップ 3　**［Enable Alert］**チェックボックスをオンにします。

ステップ 4　［Severity］ドロップダウン リスト ボックスで、通知する重大度を選択します。

ステップ 5　［Description］ペインに、アラートの説明を入力します。

ステップ 6　**［Next］**をクリックします。

ステップ 7　表 9-1 を使用して、［Threshold］、［Value Calculated As］、［Duration］、［Frequency］、［Schedule］の各ペインの設定値を設定します。ウィンドウに設定値を入力したら、**［Next］**をクリックして次のペインに進みます。

表 9-1　カウンタのアラート設定パラメータ

設定値	説明
Threshold ペイン	
Trigger alert when following conditions met（Over、Under）	チェックボックスをオンにし、適切な値を入力します。 • Over：アラート通知がアクティブになる前に満たされている必要のある最大しきい値を設定するには、このチェックボックスをオンにします。Over value フィールドに値を入力します。たとえば、進行中のコール数の値を入力します。 • Under：アラート通知がアクティブになる前に満たされている必要のある最小しきい値を設定するには、このチェックボックスをオンにします。Under value フィールドに値を入力します。たとえば、進行中のコール数の値を入力します。 **ヒント**　これらのチェックボックスは、Frequency と Schedule の設定パラメータと組み合せて使用します。

表 9-1　カウンタのアラート設定パラメータ（続き）

設定値	説明
Value Calculated As ペイン	
Absolute、Delta、Delta Percentage	適切なオプション ボタンをクリックします。 • Absolute：一部のカウンタ値は累積値なので（例：CallsAttempted や CallsCompleted）、データの現在の状況を表示するには Absolute を選択します。 • Delta：現在のカウンタ値と直前のカウンタ値の差を表示するには、Delta を選択します。 • Delta Percentage：カウンタのパフォーマンスの変化をパーセントで表示するには、［Delta Percentage］を選択します。
Duration ペイン	
Trigger alert only when value constantly...、Trigger alert immediately	• Trigger alert only when value constantly...：特定の期間（秒単位）に常に値がしきい値を下回るまたは上回る場合に限りアラート通知が必要な場合は、このオプション ボタンを選択し、アラートを送信するまでの秒数を入力します。 • Trigger alert immediately：アラート通知をすぐに送信する場合は、このオプション ボタンをクリックします。
Frequency ペイン	
Trigger alert on every poll、trigger up to...	適切なオプション ボタンをクリックします。 • Trigger alert on every poll：しきい値に達したときにポーリングのたびにアラート通知をアクティブにする場合は、このオプション ボタンをクリックします。 進行中のコール数がしきい値を上回るか下回る状態が続いても、アラート通知は再び送信されません。しきい値が正常（進行中のコール数が 50 ～ 100）になると、アラート通知は非アクティブになります。ただし、しきい値が再びしきい値を上回るか下回ると、アラート通知は再度アクティブになります。 • Trigger up to...：特定の間隔でアラート通知をアクティブにする場合は、このオプション ボタンをクリックし、送信するアラート数、およびアラートの送信期間（分単位）を入力します。
Schedule ペイン	
24-hours daily、start/stop	適切なオプション ボタンをクリックします。 • 24-hours daily：1 日 24 時間アラートをトリガーする場合は、このオプション ボタンをクリックします。 • Start/Stop：特定の時間枠内でアラート通知をアクティブにする場合は、このオプション ボタンをクリックし、開始時刻と停止時刻を入力します。このチェックボックスをオンにした場合は、毎日の作業の開始時刻と停止時刻を入力します。たとえば、毎日午前 9:00 ～午後 5:00、または午後 9:00 ～午前 9:00 にカウンタがチェックされるように設定できます。

ステップ 8　システムがアラートとして電子メール メッセージを送信するように設定する場合は、［**Enable Email**］チェックボックスをオンにします。

ステップ 9　すでに設定されているアラート アクションをトリガーする場合は、［Trigger Alert Action］ドロップダウン リスト ボックスから目的のアラート アクションを選択します。

ステップ 10 アラートに新しいアラート アクションを設定する場合は、［**Configure**］をクリックします。

（注） 指定したアラートがトリガーされるたびに、そのアラート アクションが送信されます。

［Alert Action］ダイアログボックスが表示されます。

ステップ 11 新しいアラート アクションを追加するには、［**Add**］をクリックします。

［Action Configuration］ダイアログボックスが表示されます。

ステップ 12［Name］フィールドに、アラート アクションの名前を入力します。

ステップ 13［Description］フィールドに、アラート アクションの説明を入力します。

ステップ 14 アラート アクションの新しい電子メール受信者を追加するには、［**Add**］をクリックします。

［Input］ダイアログボックスが表示されます。

ステップ 15 アラート　アクション通知を受信する受信者の電子メールまたは電子ページのアドレスを入力します。

ステップ 16［**OK**］をクリックします。

Recipient リストに、受信者のアドレスが表示されます。［Enable］チェックボックスがオンになります。

ヒント 受信者のアドレスを無効にするには、［Enable］チェックボックスをオフにします。Recipient リストから受信者のアドレスを削除するには、そのアドレスを強調表示し、［**Delete**］をクリックします。

ステップ 17［**OK**］をクリックします。

ステップ 18 追加したアラート アクションが Action List に表示されます。

ヒント Action List からアラート アクションを削除するには、そのアラート アクションを強調表示し、［**Delete**］をクリックします。［**Edit**］をクリックして、既存のアラート アクションを編集することもできます。

ステップ 19［**Close**］をクリックします。

ステップ 20［User-defined email text］ボックスに、電子メール メッセージに表示するテキストを入力します。

ステップ 21［**Activate**］をクリックします。

追加情報

P.9-15 の「関連項目」を参照してください。

カウンタの詳細表示

perfmon カウンタの詳細を表示するには、［RTMT Perfmon Monitoring］ペインの perfmon モニタ カウンタを詳細表示します。

手順

ステップ 1　次のいずれかの操作を実行します。

- ［RTMT Performance Monitoring］ペイン内で、詳細表示するカウンタをダブルクリックします。カウンタのボックスが強調表示され、［Zoom］ウィンドウが自動的に表示されます。
- ［RTMT Performance Monitoring］ペイン内で、詳細表示するカウンタをクリックします。カウンタのボックスが強調表示されます。**［System］> ［Perfmon］> ［Zoom Chart］**の順に選択します。［Zoom］ウィンドウが自動的に表示されます。

カウンタのモニタリングが開始されてからの、カウンタの最小、最大、平均、および最新の値のフィールドが表示されます。

ステップ 2　**［OK］**をクリックして、ウィンドウを閉じます。

追加情報

P.9-15 の「関連項目」を参照してください。

カウンタの説明の表示

カウンタの説明を表示するには、次のどちらかの方法を使用します。

手順

ステップ 1　次のいずれかの操作を実行します。

- Perfmon ツリー階層でプロパティ情報を表示するカウンタを右クリックし、［**Counter Description**］を選択します。
- ［RTMT Performance Monitoring］ペインでカウンタをクリックし、［**System**］>［**Performance**］>［**Counter Description**］の順に選択します。

ヒント　カウンタの説明を表示し、データサンプリング パラメータを設定するには、P.9-10 の「サンプル データの設定」を参照してください。

［Counter Property］ウィンドウにカウンタの説明が表示されます。説明には、ホスト アドレス、カウンタが属するオブジェクト、カウンタ名、カウンタの機能の要旨などがあります。

ステップ 2　［**OK**］ボタンをクリックして、［Counter Property］ウィンドウを閉じます。

追加情報

P.9-15 の「関連項目」を参照してください。

サンプル データの設定

［Counter Property］ウィンドウには、カウンタのサンプル データを設定するためのオプションがあります。［RTMT Perfmon Monitoring］ペインに表示される perfmon カウンタには、緑のドットがあり、サンプル データがある期間存在していることを示します。収集するサンプル データの数と、図に表示されるデータ ポイント数を設定できます。サンプル データを設定した後、View All Data/View Current Data メニュー オプションを使用して情報を表示します。P.9-11 の「カウンタ データの表示」を参照してください。

この項では、カウンタに対して収集するサンプル データの数を設定する方法について説明します。

手順

ステップ 1　P.9-2 の「パフォーマンス カウンタの表示」の説明に従ってカウンタを表示します。

ステップ 2　次のいずれかの操作を実行します。

- サンプル データ情報を収集するカウンタを右クリックし、図形式を使用している場合は［**Monitoring Properties**］を、表形式を使用している場合は［**Properties**］を選択します。
- サンプル データ情報を収集するカウンタをクリックし、［**System**］>［**Performance**］>［**Monitoring Properties**］の順に選択します。

［Counter Property］ウィンドウに、カウンタの説明、およびサンプル データ設定用のタブが表示されます。説明には、ホスト アドレス、カウンタが属するオブジェクト、カウンタ名、カウンタの機能の要旨などがあります。

ステップ 3　カウンタのサンプル データ数を設定するには、［**Data Sample**］タブをクリックします。

ステップ 4　［No. of data samples］ドロップダウン リスト ボックスから、サンプル数（100 ～ 1000）を選択します。デフォルトは 100 です。

ステップ 5　［No. of data points shown on chart］ドロップダウン リスト ボックスから、図に表示するデータ ポイントの数（10 ～ 50）を選択します。デフォルトは 20 です。

ステップ 6　表 9-2 で説明されているパラメータのいずれかをクリックします。

表 9-2　サンプル データ パラメータ

パラメータ	説明
Absolute	一部のカウンタ値は累積値なので（例：CallsAttempted や CallsCompleted）、データの現在の状況を表示するには Absolute を選択します。
Delta	現在のカウンタ値と直前のカウンタ値の差を表示するには、Delta を選択します。
Delta Percentage	カウンタのパフォーマンスの変化をパーセントで表示するには、［Delta Percentage］を選択します。

ステップ 7　［**OK**］ボタンをクリックして、［Counter Property］ウィンドウを閉じ、［RTMT Perfmon Monitoring］ペインに戻ります。

追加情報

P.9-15 の「関連項目」を参照してください。

カウンタ データの表示

パフォーマンス カウンタに関する収集データを表示するには、次の手順を実行します。

手順

ステップ 1　［RTMT Perfmon Monitoring］ペイン内で、サンプル データを表示するカウンタの図を右クリックし、［**View All Data**］を選択します。

サンプリングされたデータはカウンタの図にすべて表示されます。緑のドットは密に表示されるため、ほとんど実線のように見えます。

ステップ 2　現在表示されているカウンタを右クリックし、［**View Current**］を選択します。

最後に設定および収集されたサンプル データが、カウンタの図に表示されます。サンプル データの設定手順については、P.9-10 の「サンプル データの設定」を参照してください。

追加情報

P.9-15 の「関連項目」を参照してください。

Perfmon カウンタによるローカルでのデータのログ記録

RTMT では、ローカルでログを記録する各種 perfmon カウンタを選択できます。その後、Performance Log Viewer を使用して perfmon CSV ログのデータを表示できます。P.9-13 の「Perfmon Log Viewer でのログ ファイルの表示」を参照してください。

カウンタ ログの開始

CSV ログ ファイルへの perfmon カウンタ データのログ記録を開始するには、次の手順を実行します。

手順

ステップ 1　P.9-2 の「パフォーマンス カウンタの表示」の説明に従って、パフォーマンス モニタリング カウンタを表示します。

ステップ 2　図形式で perfmon カウンタを表示する場合は、サンプル データ情報を収集するカウンタを右クリックし、［**Start Counter(s) Logging**］を選択します。画面（図形式と表形式の両方）のすべてのカウンタをログ記録する場合は、ウィンドウの下部にあるカテゴリ名のタブを右クリックし、［**Start Counter(s) Logging**］を選択します。

［Counter Logging Configuration］ダイアログボックスが表示されます。

ステップ 3　［Logger File Name］フィールドにファイル名を入力し、［OK］を選択します。

RTMT は、ユーザのホーム ディレクトリの下にある .jrtmt ディレクトリのログ フォルダに CSV ログ ファイルを保存します。たとえば、Windows のパスは D:\Documents and Settings\userA\.jrtmt\log、Linux のパスは /users/home/.jrtmt/log になります。

ファイルの数とサイズを制限するには、トレースの出力設定値で、最大ファイル サイズと最大ファイル数のパラメータを指定します。P.5-2 の「トレース パラメータの設定」を参照してください。

カウンタ ログの停止

perfmon カウンタ データのログ記録を停止するには、次の手順を実行します。

手順

ステップ 1　P.9-2 の「パフォーマンス カウンタの表示」の説明に従って、パフォーマンス モニタリング カウンタを表示します。

ステップ 2　図形式で perfmon カウンタを表示する場合は、カウンタのログ記録を開始した図を右クリックし、［**Stop Counter(s) Logging**］を選択します。画面（図形式と表形式の両方）のすべてのカウンタのログ記録を停止する場合は、ウィンドウの下部にあるカテゴリ名のタブを右クリックし、［**Stop Counter(s) Logging**］を選択します。

Perfmon Log Viewer でのログ ファイルの表示

Performance Log Viewer には、perfmon CSV ログ ファイルからのカウンタのデータがグラフィカル形式で表示されます。Performance Log Viewer を使用することにより、収集したローカル perfmon ログのデータを表示したり、Alert Manager and Collector（AMC）および Realtime Information Server Data Collection（RISDC）の perfmon ログのデータを表示したりすることができます。

ローカル perfmon ログは、ローカルのコンピュータで選択および保存したカウンタのデータで構成されています。カウンタの選択方法とローカルでのログ記録の開始および停止方法については、P.9-12 の「Perfmon カウンタによるローカルでのデータのログ記録」を参照してください。

AMC および RISDC の perfmon ログを有効にすると、Cisco Unified Presence は、Cisco Unified Presence に書き込まれているログの中からシステムの情報を収集します。AMC および RISDC の perfmon ログは、Cisco Unified Presence の管理ページで［**System**］>［**Service Management**］の順に選択することにより、有効または無効にすることができます。デフォルトでは、AMC perfmon のログ記録は有効になっており、RISDC perfmon のログ記録は無効になっています。RISDC perfmon のログ記録は、トラブルシューティング用の perfmon データのログ記録とも呼ばれます。RISDC perfmon のログ記録を有効にすると、問題のトラブルシューティングに使用するデータがサーバによって収集されます。Cisco Unified Presence は短時間のうちに大量のデータを収集するので、RISDC perfmon データのログ記録（トラブルシューティング用の perfmon データのログ記録）を有効にする時間を制限する必要があります。

手順

ステップ 1　次のいずれかの操作を実行します。

- ［Quick Launch Channel］で、次の操作を実行します。
  - ［**System**］をクリックします。
  - ツリー階層で、［**Performance**］をダブルクリックします。
  - ［**Performance Log Viewer**］アイコンをクリックします。
- ［**System**］>［**Performance**］>［**Open Performance Log Viewer**］の順に選択します。

ステップ 2　表示する perfmon ログのタイプを選択します。

- AMC または RISDC の perfmon ログの場合は、次の手順を実行します。
  a. ［AMC Perfmon Logs］または［Perfmon Logs］のどちらかをクリックし、［Select a node］ドロップダウン ボックスからノードを 1 つ選択します。
  b. ［**Open**］をクリックします。
     ［File Selection］ダイアログボックスが表示されます。
  c. ファイルを選択し、［**Open File**］をクリックします。
     ［Select Counters］ダイアログボックスが表示されます。
  d. カウンタの横にあるチェックボックスをオンにして、表示するカウンタを選択します。
  e. ［**OK**］をクリックします。
- ローカルで保存されたデータの場合は、次の手順を実行します。
  a. ［Local Perfmon Logs］をクリックします。

b. ［**Open**］をクリックします。

［File Selection］ダイアログボックスが表示されます。RTMT は、ユーザのホーム ディレクトリの下にある .jrtmt ディレクトリのログ フォルダに perfmon CSV ログ ファイルを保存します。Windows のパスは D:\Documents and Settings\userA\.jrtmt\log、Linux のパスは /users/home/.jrtmt/log になります。

c. ファイルのディレクトリを参照します。

d. 表示する対象のファイルを選択するか、ファイル名フィールドにファイル名を入力します。

e. ［**Open**］をクリックします。

［Select Counters］ダイアログボックスが表示されます。

f. カウンタの横にあるチェックボックスをオンにして、表示するカウンタを選択します。

g. ［**OK**］をクリックします。

Performance Log Viewer には、選択したカウンタからのデータによる図が表示されます。下部のペインには、選択したカウンタ、それらのカウンタの色凡例、表示オプション、平均値、最小値、および最大値が表示されます。

表 9-3 に、Performance Log Viewer で使用できるボタンの機能を示します。

ヒント　列見出しをクリックすると、各列をソートできます。最初に列見出しをクリックすると、レコードは昇順に表示されます。小さな上向きの三角は、昇順であることを示しています。列見出しをもう一度クリックすると、レコードは降順に表示されます。小さな下向きの三角は、降順であることを示しています。列見出しをさらにもう一度クリックすると、レコードはソートされていない状態で表示されます。

表 9-3　Performance Log Viewer

ボタン	機能
Select Counters	Performance Log Viewer に表示するカウンタを追加できます。カウンタが表示されないようにするには、カウンタの横にある Display 列のチェックマークを外します。
Reset View	Performance Log Viewer を初期のデフォルト表示にリセットします。
Save Downloaded File	ログ ファイルをローカル コンピュータに保存できます。

拡大および縮小

Performance Log Viewer には拡大縮小機能があり、図の領域を拡大することができます。拡大するには、マウスの左ボタンをクリックし、必要な領域が選択されるまでドラッグします。

図を初期のデフォルト表示にリセットするには、［**Reset View**］をクリックするか、または図をマウスで右クリックして［**Reset**］を選択します。

関連項目

- パフォーマンス カウンタの表示（P.9-2）
- ［RTMT Performance Monitoring］ペインからのカウンタの削除（P.9-3）
- カウンタのアラート通知の設定（P.9-5）
- カウンタの詳細表示（P.9-8）
- カウンタの説明の表示（P.9-9）
- サンプル データの設定（P.9-10）
- カウンタ データの表示（P.9-11）
- Perfmon カウンタによるローカルでのデータのログ記録（P.9-12）
- Perfmon Log Viewer でのログ ファイルの表示（P.9-13）

関連項目

CHAPTER 10

RTMT の トレース収集とログ集中管理

Cisco Unified Presence Real-Time Monitoring Tool（RTMT）の Trace and Log Central 機能を使用すると、特定の日付範囲または絶対時間におけるオンデマンドのトレース収集を設定できます。指定した検索条件を含むトレース ファイルを収集して後で使用するためにトレース収集条件を保存したり、定期的なトレース収集をスケジュールしてトレース ファイルをネットワーク上の SFTP サーバにダウンロードしたり、クラッシュ ダンプ ファイルを収集したりすることができます。ファイルを収集したら、Real-Time Monitoring Tool 内の適切なビューアにそのファイルを表示できます。

(注) RTMT から、指定されたノードのトレースに関するトレースの設定を編集することもできます。トレースの設定を有効にするとシステム パフォーマンスが低下します。このため、トラブルシューティングを行う場合にだけトレースを有効にしてください。

(注) RTMT で Trace and Log Central 機能を使用するには、RTMT が Network Access Translation（NAT）を使用せずにクラスタ内のすべてのノードに直接アクセスできることを確認する必要があります。デバイスにアクセスするように NAT を設定した場合は、IP アドレスではなくホスト名を使用して Cisco Unified Presence を設定し、ホスト名とそのルータブル IP アドレスが DNS サーバ内またはホスト ファイル内にあることを確認します。

(注) 暗号化をサポートするデバイスの場合、SRTP 鍵関連情報はトレース ファイルに表示されません。

この章は、次の項で構成されています。

証明書のインポート

クラスタ内のサーバごとに認証局が提供するサーバ認証証明書をインポートできます。Trace & Log Central のオプションを使用する前に、証明書をインポートすることをお勧めします。証明書をインポートしない場合、RTMT にログインして Trace & Log Central のオプションを使用するたびに、クラスタ内のノードごとのセキュリティ証明書が表示されます。証明書に表示されるデータは変更できません。

証明書をインポートするには、[**System**] > [**Tools**] > [**Trace**] > [**Import Certificate**] の順に選択します。

サーバ証明書のインポートが完了したことを示すメッセージが表示されます。[**OK**] をクリックします。

RTMT での Trace & Log Central のオプションの表示

開始する前に、P.10-2 の「証明書のインポート」の説明に従って、セキュリティ証明書がインポートされていることを確認します。

Trace & Log Central のツリー階層を表示するには、次のいずれかの操作を実行します。

- ［Quick Launch Channel］で［**System**］をクリックし、ツリー階層構造で［**Tools**］をダブルクリックしてから、［**Trace & Log Central**］アイコンをクリックします。
- ［**System**］>［**Tools**］>［**Trace**］>［**Open Trace & Log Central**］の順に選択します。

ヒント　ツリー階層に表示される任意のオプションから、トレースする対象のサービス / アプリケーションの指定、使用するログとサーバの指定、収集の時刻と日付のスケジュール、ファイルのダウンロード機能の設定、zip ファイルの設定、および収集したトレース ファイルの削除を行うことができます。

Real-Time Monitoring Tool で Trace & Log Central のオプションが表示されたら、次のいずれかの操作を実行します。

- クラスタ内の 1 台以上のサーバについて、サービス、アプリケーション、システム ログのトレースを収集します。P.10-4 の「トレースの収集」を参照してください。
- 指定した検索条件を含むトレース ファイルを収集してダウンロードし、トレース収集条件を後で使用するために保存します。P.10-7 の「Query Wizard の使用」を参照してください。
- 定期的なトレース収集をスケジュールし、トレース ファイルをネットワーク上の SFTP サーバにダウンロードします。P.10-11 の「トレース収集のスケジュール」を参照してください。
- 1 台以上のサーバについて、クラッシュ ダンプ ファイルを収集します。P.10-15 の「クラッシュ ダンプの収集」を参照してください。
- 収集したトレース ファイルを表示します。P.10-18 の「Local Browse の使用」を参照してください。
- サーバ上のすべてのトレース ファイルを表示します。P.10-19 の「Remote Browse の使用」を参照してください。
- アプリケーションごとに、サーバ上で現在書き込まれているトレース ファイルを表示します。トレース ファイルに検索文字列が書き込まれた場合、指定したアクションを実行できます。P.10-23 の「Real Time Trace の使用」を参照してください。

トレースの収集

Trace and Log Central 機能の Collect Traces オプションを使用すると、クラスタ内の 1 台以上のサーバについて、サービス、アプリケーション、システム ログのトレースを収集できます。トレースを収集する日時の範囲、トレース ファイルのダウンロード先のディレクトリ、収集したファイルをサーバから削除するかどうかなどを指定します。Trace and Log Central 機能を使用してトレースを収集する手順は、次のとおりです。

（注） アクティブにしていないサービスも表示されるため、そのサービスのトレースを収集できます。

指定した検索条件を含むトレース ファイルを収集する場合、または後で使用するために保存したトレース収集条件を使用する場合は、P.10-7 の「Query Wizard の使用」を参照してください。

開始する前に

次の 1 つ以上の操作を実行します。

- ［Trace Configuration］ウィンドウで、さまざまなサービスのトレース ファイルに含める情報を設定します。詳細については、P.5-1 の「トレースの設定」を参照してください。
- アラームをトレース ファイルに送信する場合は、［Alarm Configuration］ウィンドウで、アラームの宛先として SDI トレース ファイルを選択します。詳細については、P.3-1 の「アラームの設定」を参照してください。

手順

ステップ 1　P.10-3 の「RTMT での Trace & Log Central のオプションの表示」の説明に従って、Trace & Log Central のオプションを表示します。

ステップ 2　ツリー階層で、**［Collect Files］**をダブルクリックします。

［Select CUP Services/Applications］タブが表示されます。

（注） クラスタ内に使用できないサーバがある場合は、使用できないサーバを特定するメッセージがダイアログボックスに表示されます。使用できないサーバは、Trace & Log Central のウィンドウには表示されません。

ステップ 3　次のいずれかの操作を実行します。

- クラスタ内のすべてのサーバ上の、すべてのサービスおよびアプリケーションのトレースを収集するには、**［Select All Services on All Servers］**チェックボックスをオンにします。
- 特定のサーバ上の、すべてのサービスおよびアプリケーションのトレースを収集するには、サーバの IP アドレスの横にあるチェックボックスをオンにします。
- 特定のサーバ上の、特定のサービスまたはアプリケーションのトレースを収集する場合は、該当するチェックボックスをオンにします。
- サービスまたはアプリケーションのトレースを収集せずにトレース収集ウィザードを続行する場合は、ステップ 4 に進みます。

（注） アクティブにしていないサービスも表示されるため、そのサービスのトレースを収集できます。

（注） リストされている一部のサービス / アプリケーションは、クラスタ内の特定のノードにのみインストールできます。これらのサービス / アプリケーションのトレースを収集する場合は、必ず、サービス / アプリケーションをアクティブにしたサーバからトレースを収集してください。

ステップ 4　［**Next**］をクリックします。

［Select System Services/Applications］タブが表示されます。

ステップ 5　次のいずれかの操作を実行します。

- クラスタ内のすべてのサーバ上の、すべてのシステム ログを収集する場合は、［**Select All Logs on all Servers**］チェックボックスをオンにします。
- 特定のサーバ上の、すべてのシステム ログのトレースを収集する場合は、サーバの IP アドレスの横にあるチェックボックスをオンにします。
- 特定のサーバ上の、特定のシステム ログのトレースを収集する場合は、該当するチェックボックスをオンにします。

  たとえば、CSA ログを収集するには、［Select System Logs タブで［Cisco Security Agent］チェックボックスをオンにします。ログインおよびログアウトするユーザについての情報を記録するユーザ ログにアクセスするには、［Select System Logs］タブで［Security Logs］チェックボックスをオンにします。
- システム ログのトレースを収集せずにトレース収集ウィザードを続行する場合は、ステップ 6 に進みます。

ステップ 6　［**Next**］をクリックします。

ステップ 7　［Collection Time］グループ ボックスで、トレースを収集する時間範囲を指定します。次のいずれかのオプションを選択します。

- **Absolute Range**：トレースを収集する対象のサーバのタイム ゾーンと時間範囲（開始日時と終了日時）を指定します。

  クライアント マシンのタイム ゾーンは、［Select Reference Server Time Zone］フィールドのデフォルト設定値です。Daylight Savings 設定値を持つすべてのタイム ゾーンの個別のエントリセットとともに、すべての標準タイム ゾーンが、［Select Time Zone］ドロップダウン リスト ボックスに表示されます。

  選択したタイム ゾーンがサーバ（たとえば、Server 1）のタイム ゾーン設定と一致する場合は、その日付範囲内（開始日付と終了日付の間）の修正されたトレース ファイルが収集されます。同じ Cisco Unified Presence クラスタ内に別のサーバ（Server 2）が存在し、そのサーバが別のタイム ゾーンである場合、Server 2 の対応する日付範囲内の修正されたトレース ファイルが Server 2 から収集されます。

  トレースを収集する日付範囲を設定するには、［From Date/Time］フィールドと［To Date/Time］フィールドのドロップダウン リスト ボックスから選択します。
- **Relative Range**：現在時刻から遡ってトレースを収集する時間を（分、時間、日、週、月のいずれかの単位で）指定します。

ステップ 8　［Select Partition］ドロップダウン リスト ボックスから、トレースを収集する対象のログを含むパーティションを選択します。

Cisco Unified Presence Serviceability では、Cisco Unified Presence の最大 2 つの Linux ベースのバージョンについてログを保存します。Cisco Unified Presence Serviceability は、ユーザがログインしているバージョンの Cisco Unified Presence のログをアクティブなパーティションに保存し、他のバージョンの Cisco Unified Presence（インストールされている場合）のログをアクティブでないディレクトリに保存します。

したがって、Linux プラットフォームで実行されている Cisco Unified Presence のバージョンを別のバージョンにアップグレードし、Linux プラットフォームで実行されている新しいバージョンの Cisco Unified Presence にログインすると、Cisco Unified Presence Serviceability は前バージョンのログをアクティブでないパーティションに移動し、新しいバージョンのログをアクティブなパーティションに保存します。ユーザが古いバージョンの Cisco Unified Presence にログインすると、Cisco Unified Presence Serviceability は新しいバージョンの Cisco Unified Presence のログをアクティブでないパーティションに移動し、古いバージョンのログをアクティブなディレクトリに保存します。

（注）　Cisco Unified Presence Serviceability では、Windows プラットフォームで実行されている Cisco Unified Presence のバージョンのログは保存されません。

ステップ 9　トレース ファイルのダウンロード先ディレクトリを指定するには、［Download File Directory］フィールドの横にある［**Browse**］ボタンをクリックし、該当するディレクトリに移動して［**Open**］をクリックします。デフォルトでは、C:\Program Files\Cisco\Presence Serviceability\jrtmt\< サーバ IP アドレス >\< ダウンロード時刻 > が指定されます。

ステップ 10　収集するトレース ファイルの zip ファイルを作成するには、［**Zip File**］オプション ボタンを選択します。トレース ファイルを zip 圧縮せずにダウンロードするには、［**Do Not Zip Files**］オプション ボタンを選択します。

ステップ 11　収集したログ ファイルをサーバから削除するには、［**Delete Collected Log Files from the server**］チェックボックスをオンにします。

ステップ 12　［**Finish**］をクリックします。

ウィンドウにトレース収集の進行状況が表示されます。トレース収集を中止する場合は、［**Cancel**］をクリックします。

トレース収集プロセスが完了すると、ウィンドウの下部に「Completed downloading for node <IP アドレス >」というメッセージが表示されます。

ステップ 13　収集したトレース ファイルを表示するには、トレース収集機能の Local Browse オプションを使用します。詳細については、P.10-18 の「Local Browse の使用」を参照してください。

追加情報

P.10-27 の「関連項目」を参照してください。

Query Wizard の使用

Trace Collection Query Wizard を使用すると、指定した検索条件を含むトレース ファイルを収集してダウンロードし、後で使用するためにトレース収集条件を保存することができます。Trace Collection Query Wizard を使用するには、次の手順を実行します。

開始する前に

次の 1 つ以上の操作を実行します。

- ［Trace Configuration］ウィンドウで、さまざまなサービスのトレース ファイルに含める情報を設定します。詳細については、P.5-1 の「トレースの設定」を参照してください。
- アラームをトレース ファイルに送信する場合は、［Alarm Configuration］ウィンドウで、アラームの宛先として SDI トレース ファイルを選択します。詳細については、P.3-1 の「アラームの設定」を参照してください。

手順

ステップ 1　P.10-3 の「RTMT での Trace & Log Central のオプションの表示」の説明に従って、Trace & Log Central のオプションを表示します。

ステップ 2　ツリー階層で、［**Query Wizard**］をダブルクリックします。

（注）　クラスタ内に使用できないサーバがある場合は、使用できないサーバを特定するメッセージがダイアログボックスに表示されます。使用できないサーバは、Trace & Log Central のウィンドウには表示されません。

ステップ 3　開いたウィンドウで、次のいずれかのオプション ボタンをクリックします。

- Saved Query

  ［**Browse**］ボタンをクリックして、使用するクエリーに移動します。クエリーを選択し、［**Open**］をクリックします。

  Single Node Generic Query を選択した場合は、RTMT の接続先のノードが［Browse］ボタンの横にチェックマーク付きで表示されます。追加のノードの横にチェックマークを入れると、該当するサーバに関するクエリーを実行できます。

  All Node Generic Query を選択した場合は、すべてのノードが［Browse］ボタンの横にチェックマーク付きで表示されます。クエリーを実行する対象に含まれないサーバがある場合は、そのチェックマークを外すことができます。

  Regular Query を選択した場合は、クエリーを保存するときに選択したすべてのノードがチェックマーク付きで表示されます。リストに表示される任意のサーバについて、チェックを入れるか外すことができます。新しいサーバを選択する場合は、ウィザードを使用してそのノードのサービスを選択する必要があります。

  変更せずにクエリーを実行するには、［**Run Query**］をクリックし、ステップ 17 に進みます。クエリーを変更するには、ステップ 4 に進みます。
- Create Query

ステップ 4　［**Next**］をクリックします。

［Select CUP Services/Applications］タブが表示されます。

ステップ 5　［Saved Query］オプション ボタンをクリックしてクエリーを選択した場合は、クエリーに指定した条件が表示されます。必要に応じて、トレースを収集する対象のサービス / アプリケーションのリストを変更します。［Create Query］オプション ボタンをクリックした場合は、トレースを収集するすべてのサービス / アプリケーションを選択する必要があります。

ヒント　クラスタ内のすべてのサーバ上の、すべてのサービスおよびアプリケーションのトレースを収集するには、**［Select All Services on All Servers］**チェックボックスをオンにします。特定のサーバ上の、すべてのサービスおよびアプリケーションのトレースを収集するには、サーバの IP アドレスの横にあるチェックボックスをオンにします。

（注）　アクティブにしていないサービスも表示されるため、そのサービスのトレースを収集できます。

（注）　リストされている一部のサービス / アプリケーションは、クラスタ内の特定のノードにのみインストールできます。これらのサービス / アプリケーションのトレースを収集する場合は、必ず、サービス / アプリケーションをアクティブにしたサーバからトレースを収集してください。

ステップ 6　**［Next］**をクリックします。

ステップ 7　［Select System Services/Applications］タブで、該当するすべてのチェックボックスをオンにします。

ヒント　クラスタ内のすべてのサーバ上の、すべてのサービスおよびアプリケーションのシステム ログのトレースを収集するには、**［Select All Logs on All Servers］**チェックボックスをオンにします。特定のサーバ上の、すべてのサービスおよびアプリケーションのトレースを収集するには、サーバの IP アドレスの横にあるチェックボックスをオンにします。

ステップ 8　**［Next］**をクリックします。

ステップ 9　［Query Time Options］グループ ボックスで、トレースを収集する時間範囲を指定します。次のいずれかのオプションを選択します。

- **All Available Traces**：このオプションは、選択したサーバ上のサービスに関するすべてのトレースを収集する場合に選択します。
- **Absolute Range**：トレースを収集する対象のサーバのタイム ゾーンと時間範囲（開始日時と終了日時）を指定します。

  クライアント マシンのタイム ゾーンは、［Select Reference Server Time Zone］フィールドのデフォルト設定値です。Daylight Savings 設定値を持つすべてのタイム ゾーンの個別のエントリセットとともに、すべての標準タイム ゾーンが、［Select Time Zone］ドロップダウン リスト ボックスに表示されます。

選択したタイム ゾーンがサーバ（たとえば、Server 1）のタイム ゾーン設定と一致する場合は、その日付範囲内（開始日付と終了日付の間）の修正されたトレース ファイルが収集されます。同じ Cisco Unified Presence クラスタ内に別のサーバ（Server 2）が存在し、そのサーバが別のタイム ゾーンである場合、Server 2 の対応する日付範囲内の修正されたトレース ファイルが Server 2 から収集されます。

トレースを収集する日付範囲を設定するには、［From Date/Time］フィールドと［To Date/Time］フィールドのドロップダウン リスト ボックスから選択します。

- **Relative Range**：現在時刻から遡ってトレースを収集する時間を（分、時間、日、週、月のいずれかの単位で）指定します。

ステップ 10　トレース ファイルに含まれる単語や句で検索するには、［Search String］フィールドに該当する単語または句を入力します。このツールは、入力した単語または句の完全一致を検索します。

ステップ 11　［Call Procession Impact Options］ドロップダウン リスト ボックスから、文字列検索アクティビティがコール処理に与える影響のレベルを指定します。指定できるオプションには、Low、Medium、High があります。Low を選択すると、コール処理への影響は最小になりますが、時間がかかります。High を選択すると、コール処理への影響は最大になりますが、時間は短縮されます。

ステップ 12　次のいずれかのオプションを選択します。

- クエリーを実行する場合は、［**Run Query**］をクリックします。

  Query Results フォルダが表示されます。クエリーが完了すると、クエリーの実行が完了したことを示すダイアログボックスが表示されます。［**OK**］をクリックし、ステップ 17 に進みます。
- クエリーを保存する場合は、［**Save Query**］ボタンをクリックし、ステップ 13 に進みます。

ステップ 13　作成するクエリー タイプの横にあるチェックボックスをオンにします。

- **Generic Query**：このオプションは、クエリーを作成したノード以外のノードで実行できるクエリーを作成する場合に選択します。Generic Query を作成できるのは、選択したサービスがシングル ノード上に存在する場合のみです。複数のノード上のサービスを選択すると、メッセージが表示されます。この場合は、クエリーを Regular Query として保存するか、シングル ノード上のサービスを選択します。

  次に、Single Node Query または All Node Query のいずれかのオプションを選択します。Single Node Query を選択すると、トレース収集ツールは、クエリーを実行するときに、クエリーを作成したサーバをデフォルトで選択します。All Node Query オプションを選択すると、トレース収集ツールは、クエリーを実行するときに、クラスタ内のすべてのサーバをデフォルトで選択します。

（注）　クエリーを実行する前に、デフォルト以外のサーバを選択できます。

- **Regular Query**：このオプションは、クエリーを作成したノードまたはクラスタ上でクエリーを実行する場合にのみ選択します。

ステップ 14　［**Finish**］をクリックします。

ステップ 15　クエリーを保存する場所に移動し、［File Name］フィールドにクエリーの名前を入力し、［**Save**］をクリックします。

ステップ 16　次のいずれかの操作を実行します。

- 保存したクエリーを実行する場合は、［**Run Query**］をクリックし、ステップ 17 に進みます。
- 作成したクエリーを実行せずに Query Wizard を終了する場合は、［**Cancel**］をクリックします。

ステップ 17　クエリーの実行が完了したら、次の 1 つ以上の操作を実行します。

- 収集したファイルを表示する場合は、Query Results をダブルクリックし、<node> フォルダ（<node> はウィザードで指定したサーバの IP アドレスまたはホスト名を表す）をダブルクリックし、表示するファイルが含まれているフォルダをダブルクリックしてファイルに移動します。ファイルの場所に移動したら、そのファイルをダブルクリックします。ファイル タイプに対応した既定のビューアに、ファイルが表示されます。
- トレース ファイルとクエリーで収集したトレース ファイルのリストを含む結果のファイルをダウンロードします。そのためには、ダウンロードするファイルを選択して［**Download**］をクリックし、ダウンロードの条件を指定して［**Finish**］をクリックします。
  - トレース ファイルと結果のファイルをダウンロードするディレクトリを指定する場合は、［Download all files］フィールドの横にある［**Browse**］ボタンをクリックし、該当するディレクトリを表示して［**Open**］をクリックします。デフォルトでは、C:\Program Files\Cisco\Presence Serviceability\jrtmt\< サーバ IP アドレス >\< ダウンロード時刻 > が指定されます。
  - 収集するトレース ファイルの zip ファイルを作成するには、［**Zip File**］チェックボックスをオンにします。
  - 収集したログ ファイルをサーバから削除するには、［**Delete Collected Log Files from Server**］チェックボックスをオンにします。

ヒント　トレース ファイルをダウンロードしたら、Trace and Log Central 機能の Local Browse オプションを使用してそれらのファイルを表示できます。詳細については、P.10-18 の「Local Browse の使用」を参照してください。

- クエリーを保存する場合は、［**Save Query**］をクリックし、ステップ 13 ～ステップ 15 を実行します。

追加情報

P.10-27 の「関連項目」を参照してください。

トレース収集のスケジュール

Trace and Log Central 機能の Schedule Collection オプションを使用すると、同時に最大 6 件の定期的なトレース収集をスケジュールしたり、ネットワーク上の SFTP サーバにトレース ファイルをダウンロードしたり、保存された別のクエリーを実行したり、syslog ファイルを作成したりすることができます。スケジュールされた収集をシステムに入力した後で変更するには、そのスケジュールされた収集を削除して新しい収集イベントを追加する必要があります。トレース収集をスケジュールするには、次の手順を実行します。

（注） 最大 10 件のトレース収集をスケジュールできますが、同時に実行できるのは 6 件までです。つまり、同時に実行中の状態にできるのは 6 件までです。

開始する前に

次の 1 つ以上の操作を実行します。

- ［Trace Configuration］ウィンドウで、さまざまなサービスのトレース ファイルに含める情報を設定します。詳細については、P.5-1 の「トレースの設定」を参照してください。
- アラームをトレース ファイルに送信する場合は、［Alarm Configuration］ウィンドウで、アラームの宛先として SDI トレース ファイルを選択します。詳細については、P.3-1 の「アラームの設定」を参照してください。

手順

ステップ 1　P.10-3 の「RTMT での Trace & Log Central のオプションの表示」の説明に従って、Trace & Log Central のオプションを表示します。

ステップ 2　ツリー階層で、［**Schedule Collection**］をダブルクリックします。

［Select CUP Services/Applications］タブが表示されます。

（注） クラスタ内に使用できないサーバがある場合は、使用できないサーバを特定するメッセージがダイアログボックスに表示されます。使用できないサーバは、Trace & Log Central のウィンドウには表示されません。

ステップ 3　次のいずれかの操作を実行します。

- クラスタ内のすべてのサーバ上の、すべてのサービスおよびアプリケーションのトレースを収集するには、［**Select All Services on All Servers**］チェックボックスをオンにします。
- 特定のサーバ上の、すべてのサービスおよびアプリケーションのトレースを収集するには、サーバの IP アドレスの横にあるチェックボックスをオンにします。
- 特定のサーバ上の、特定のサービスまたはアプリケーションのトレースを収集する場合は、該当するチェックボックスをオンにします。
- サービスまたはアプリケーションのトレースを収集せずにトレース収集ウィザードを続行する場合は、ステップ 4 に進みます。

（注） アクティブにしていないサービスも表示されるため、そのサービスのトレースを収集できます。

（注） リストされている一部のサービス / アプリケーションは、クラスタ内の特定のノードにのみインストールできます。これらのサービス / アプリケーションのトレースを収集する場合は、必ず、サービス / アプリケーションをアクティブにしたサーバからトレースを収集してください。

ステップ 4　［**Next**］をクリックします。

［System Services/Applications］タブが表示されます。

ステップ 5　システム ログのトレースを収集するには、次のいずれかの操作を実行します。

- クラスタ内のすべてのサーバ上の、すべてのシステム ログを収集する場合は、［**Select All Logs on all Servers**］チェックボックスをオンにします。
- 特定のサーバ上の、すべてのシステム ログのトレースを収集する場合は、サーバの IP アドレスの横にあるチェックボックスをオンにします。
- 特定のサーバ上の、特定のシステム ログのトレースを収集する場合は、該当するチェックボックスをオンにします。
- システム ログのトレースを収集せずにトレース収集ウィザードを続行する場合は、ステップ 6 に進みます。

ステップ 6　［**Next**］をクリックします。

ステップ 7　トレースを収集する対象のサーバのタイム ゾーンと時間範囲を指定します。

クライアント マシンのタイム ゾーンは、［Select Reference Server Time Zone］フィールドのデフォルト設定値です。Daylight Savings 設定値を持つすべてのタイム ゾーンの個別のエントリ セットとともに、すべての標準タイム ゾーンが、［Select Time Zone］ドロップダウン リスト ボックスに表示されます。

ステップ 8　トレース収集を開始する日時を指定するには、［Schedule Start Date/Time］フィールドの横にある下向き矢印ボタンをクリックします。［Date］タブで、適切な日付を選択します。［Time］タブで、適切な時刻を選択します。

ステップ 9　トレース収集を終了する日時を指定するには、［Schedule End Date/Time］フィールドの横にある下向き矢印ボタンをクリックします。［Date］タブで、適切な日付を選択します。［Time］タブで、適切な時刻を選択します。

（注） トレース収集は、設定した終了時刻を過ぎても完了しますが、Trace and Log Central 機能はこの収集をスケジュールから削除します。

ステップ 10　［Scheduler Frequency］ドロップダウン リスト ボックスから、設定されたトレース収集を実行する頻度を選択します。

ステップ 11　［**Collect Files generated in the last**］ドロップダウン リスト ボックスから、現在時刻から遡ってトレースを収集する時間を（分、時間、日、週、月のいずれかの単位で）指定します。

ステップ 12　トレース ファイルに含まれる単語や句で検索するには、［**Search String**］フィールドに該当する単語または句を入力します。このツールは、入力した単語または句の完全一致を検索し、検索条件に一致するファイルのみを収集します。

ステップ 13　収集するトレース ファイルの zip ファイルを作成するには、［**Zip File**］チェックボックスをオンにします。

ステップ 14　収集したログ ファイルをサーバから削除するには、［**Delete Collected Log Files from the Server**］チェックボックスをオンにします。

ステップ 15　次の 1 つ以上のアクションを選択します。

- Download Files
- Run Another Query
- Generate Syslog

ステップ 16　次のいずれかの操作を実行します。

- Download Files または Run Another Query を選択した場合は、ステップ 17 に進みます。
- Generate Syslog を選択した場合は、ステップ 19 に進みます。

ステップ 17　［SFTP Server Parameters］グループ ボックスで、Trace and Log Central 機能が結果をダウンロードするサーバの資格情報を入力し、［**Test Connection**］をクリックします。Trace and Log Central 機能が SFTP サーバへの接続を検証したら、［**OK**］をクリックします。

（注）　［**Download Directory Path**］フィールドに、Trace and Log Central 機能が収集ファイルを保存するためのディレクトリを指定します。デフォルトでは、トレース収集機能は、SFTP パラメータのフィールドに指定したユーザ ID を持つユーザのホーム ディレクトリ（/home/<ユーザ >/Trace）に収集ファイルを保存します。

ステップ 18　Run Another Query オプションを選択した場合は、［**Browse**］ボタンをクリックして実行するクエリーを選択し、［**OK**］をクリックします。

（注）　Trace and Log Central 機能は、第 1 のクエリーの結果が生成された場合にのみ、指定されたクエリーを実行します。

ステップ 19　［**Finish**］をクリックします。

スケジュールされたトレースが正常に追加されたことを示すメッセージが表示されます。

（注）　Real-Time Monitoring Tool が SFTP サーバにアクセスできない場合は、メッセージが表示されます。IP アドレス、ユーザ名、およびパスワードを正しく入力したことを確認してください。

ステップ 20　［**OK**］をクリックします。

ステップ 21　スケジュールされた収集のリストを表示するには、［Quick Launch Channel］の［**Job Status**］アイコンをクリックします。

ヒント　スケジュールされた収集を削除するには、収集イベントを選択し、［**Delete**］をクリックします。確認メッセージが表示されます。［**OK**］をクリックします。

追加情報

P.10-27 の「関連項目」を参照してください。

トレース収集状況の表示とスケジュールされた収集の削除

トレース収集イベントの状況を表示し、スケジュールされたトレース収集を削除するには、次の手順を実行します。

手順

ステップ 1　P.10-3 の「RTMT での Trace & Log Central のオプションの表示」の説明に従って、Trace & Log Central のオプションを表示します。

ステップ 2　［Quick Launch Channel］で、［**Job Status**］アイコンをクリックします。

ステップ 3　［Select a Node］ドロップダウン リスト ボックスから、トレース収集イベントを表示または削除する対象のサーバを選択します。

スケジュールされたトレース収集のリストが表示されます。

ジョブ タイプには、Scheduled Job、OnDemand、RealTimeFileMon、RealTimeFileSearch があります。

状況には、Pending、Terminated、Running、Cancel、Terminated があります。

ステップ 4　スケジュールされた収集を削除するには、削除するイベントを選択し、［**Delete**］をクリックします。

（注）　削除できるのは、状況が「Pending」または「Running」で、ジョブ タイプが「ScheduleTask」のジョブのみです。

追加情報

P.10-27 の「関連項目」を参照してください。

クラッシュ ダンプの収集

トレース ファイルのコア ダンプを収集するには、次の手順を実行します。

手順

ステップ 1　P.10-3 の「RTMT での Trace & Log Central のオプションの表示」の説明に従って、Trace & Log Central のツリー階層を表示します。

ステップ 2　［**Collect Crash Dump**］をダブルクリックします。

（注）　アクティブにしていないサービスも表示されるため、そのサービスのトレースを収集できます。

（注）　クラスタ内に使用できないサーバがある場合は、使用できないサーバを特定するメッセージがダイアログボックスに表示されます。使用できないサーバは、Trace & Log Central のウィンドウには表示されません。

（注）　リストされている一部のサービス / アプリケーションは、クラスタ内の特定のノードにのみインストールできます。これらのサービス / アプリケーションのトレースを収集する場合は、必ず、サービス / アプリケーションをアクティブにしたサーバからトレースを収集してください。

ステップ 3　［Select CUP Services/Applications］タブで、次のいずれかの操作を実行します。

- クラスタ内のすべてのサーバ上の、すべてのサービスおよびアプリケーションのトレースを収集するには、［**Select All Services on All Servers**］チェックボックスをオンにします。
- 特定のサーバ上の、すべてのサービスおよびアプリケーションのトレースを収集するには、サーバの横にあるチェックボックスをオンにします。
- 特定のサーバ上の、特定のサービスまたはアプリケーションのトレースを収集する場合は、該当するチェックボックスをオンにします。
- サービスまたはアプリケーションのトレースを収集せずにクラッシュ　ダンプ収集ウィザードを続行する場合は、ステップ 4 に進みます。

ステップ 4　［**Next**］をクリックします。

ステップ 5　［Select System Services/Applications］タブで、次のいずれかの操作を実行します。

- すべてのサーバ上の、すべてのシステム　ログを収集する場合は、［Select All Services on all Servers］チェックボックスをオンにします。
- 特定のサーバ上の、すべてのシステム ログのトレースを収集する場合は、サーバの IP アドレスの横にあるチェックボックスをオンにします。
- 特定のサーバ上の、特定のシステム ログのトレースを収集する場合は、該当するチェックボックスをオンにします。
- システム ログのトレースを収集せずにクラッシュ ダンプ収集ウィザードを続行する場合は、ステップ 6 に進みます。

ステップ 6　［Collection Time］グループ ボックスで、トレースを収集する時間範囲を指定します。次のいずれかのオプションを選択します。

- **Absolute Range**：トレースを収集する対象のサーバのタイム ゾーンと時間範囲（開始日時と終了日時）を指定します。

  クライアント マシンのタイム ゾーンは、［Select Reference Server Time Zone］フィールドのデフォルト設定値です。Daylight Savings 設定値を持つすべてのタイム ゾーンの個別のエントリセットとともに、すべての標準タイム ゾーンが、［Select Time Zone］ドロップダウン リスト ボックスに表示されます。

  選択したタイム ゾーンがサーバ（たとえば、Server 1）のタイム ゾーン設定と一致する場合は、その日付範囲内（開始日付と終了日付の間）の修正されたクラッシュ ファイルが収集されます。同じ Cisco Unified Presence クラスタ内に別のサーバ（Server 2）が存在し、そのサーバが別のタイム ゾーンである場合、Server 2 の対応する日付範囲内の修正されたクラッシュ ファイルが Server 2 から収集されます。

  クラッシュ ファイルを収集する日付範囲を設定するには、［From Date/Time］フィールドと［To Date/Time］フィールドのドロップダウン リスト ボックスから選択します。
- **Relative Range**：現在時刻から遡ってクラッシュ ファイルを収集する時間を（分、時間、日、週、月のいずれかの単位で）指定します。

ステップ 7　［Select Partition］ドロップダウン リスト ボックスから、トレースを収集する対象のログを含むパーティションを選択します。

Cisco Unified Presence Serviceability では、Cisco Unified Presence の最大 2 つの Linux ベースのバージョンについてログを保存します。Cisco Unified Presence Serviceability は、ユーザがログインしているバージョンの Cisco Unified Presence のログをアクティブなパーティションに保存し、他のバージョンの Cisco Unified Presence（インストールされている場合）のログをアクティブでないディレクトリに保存します。

したがって、Linux プラットフォームで実行されている Cisco Unified Presence のバージョンを別のバージョンにアップグレードし、Linux プラットフォームで実行されている新しいバージョンの Cisco Unified Presence にログインすると、Cisco Unified Presence Serviceability は前バージョンのログをアクティブでないパーティションに移動し、新しいバージョンのログをアクティブなパーティションに保存します。ユーザが古いバージョンの Cisco Unified Presence にログインすると、Cisco Unified Presence Serviceability は新しいバージョンの Cisco Unified Presence のログをアクティブでないパーティションに移動し、古いバージョンのログをアクティブなディレクトリに保存します。

（注）　Cisco Unified Presence Serviceability では、Windows プラットフォームで実行されている Cisco Unified Presence のバージョンのログは保存されません。

ステップ 8　トレース ファイルのダウンロード先ディレクトリを指定するには、［Download File Directory］フィールドの横にある［**Browse**］ボタンをクリックし、該当するディレクトリに移動して［**Open**］をクリックします。デフォルトでは、C:\Program Files\Cisco\Presence Serviceability\jrtmt\< サーバ IP アドレス >\< ダウンロード時刻 > が指定されます。

ステップ 9　収集するクラッシュ ダンプ ファイルの zip ファイルを作成するには、［**Zip File**］オプション ボタンを選択します。クラッシュ ダンプ ファイルを zip 圧縮せずにダウンロードするには、［**Do Not Zip Files**］オプション ボタンを選択します。

（注） クラッシュ ダンプの zip ファイルが 2 ギガバイトを超える場合、そのファイルはダウンロードできません。

ステップ 10 収集したクラッシュ ダンプ ファイルをサーバから削除するには、［**Delete Collected Log Files from Server**］チェックボックスをオンにします。

ステップ 11 ［**Finish**］をクリックします。

コア ダンプを収集しようとしていることを示すメッセージが表示されます。［**Yes**］をクリックして続行します。

（注） ［**Zip File**］オプション ボタンを選択し、クラッシュ ダンプ ファイルが 2 ギガバイトを超えた場合、［**Zip File**］オプション ボタンを選択した状態ではこのサイズのクラッシュ ダンプ ファイルを収集できないことを示すメッセージが表示されます。［**Do Not Zip Files**］オプション ボタンを選択してから、もう一度収集してください。

追加情報

P.10-27 の「関連項目」を参照してください。

Local Browse の使用

トレース ファイルを収集して PC にダウンロードしたら、UNIX 系の行末記号を処理できる WordPad のようなテキスト エディタを使用して、PC 上でトレース ファイルを表示できます。Real-Time Monitoring Tool 内のビューアで表示することもできます。

（注） 収集したトレース ファイルを表示するのに、NotePad を使用しないでください。

Trace and Log Central 機能で収集したログ ファイルを表示するには、次の手順を実行します。トレース ファイルを PC にダウンロードするときに zip 圧縮した場合は、これを解凍してから Real-Time Monitoring Tool 内のビューアで表示する必要があります。

開始する前に

次のいずれかの項の説明に従って、トレース ファイルを収集します。

- トレースの収集（P.10-4）
- Query Wizard の使用（P.10-7）
- トレース収集のスケジュール（P.10-11）

手順

ステップ 1　P.10-3 の「RTMT での Trace & Log Central のオプションの表示」の説明に従って、Trace & Log Central のオプションを表示します。

ステップ 2　［**Local Browse**］をダブルクリックします。

ステップ 3　ログ ファイルを保存したディレクトリを参照し、表示するファイルを選択します。

ステップ 4　結果を表示するには、ファイルをダブルクリックします。

ステップ 5　ファイルの表示に使用するプログラム（ビューア）をクリックします。プログラムがリストにない場合は、［**Other**］ボタンをクリックして別のプログラムを選択します。このプログラムをデフォルトのビューアとして使用する場合は、［**Always use this program to open these files**］チェックボックスをオンにします。Real-Time Monitoring Tool により、ファイル タイプに適したビューアにファイルが表示されます。他に適切なビューアがない場合は、Generic Log Viewer でファイルが開きます。

追加情報

P.10-27 の「関連項目」を参照してください。

Remote Browse の使用

システムがトレース ファイルを生成したら、サーバで Real-Time Monitoring Tool 内のビューアにそのファイルを表示できます。Remote Browse 機能を使用して、トレースを PC にダウンロードすることもできます。

Trace and Log Central 機能でサーバ上のログ ファイルを表示またはダウンロードするには、次の手順を実行します。

開始する前に

次のいずれかの項の説明に従って、トレース ファイルを収集します。

- トレースの収集（P.10-4）
- Query Wizard の使用（P.10-7）
- トレース収集のスケジュール（P.10-11）

手順

ステップ 1　P.10-3 の「RTMT での Trace & Log Central のオプションの表示」の説明に従って、Trace & Log Central のオプションを表示します。

ステップ 2　［**Remote Browse**］をダブルクリックします。

ステップ 3　適切なオプション ボタンを選択し、［**Next**］をクリックします。Trace Files を選択する場合は、ステップ 4 に進みます。Crash Dump を選択する場合は、ステップ 9 に進みます。

（注）　アクティブにしていないサービスも表示されるため、そのサービスのトレースを選択できます。

（注）　リストされている一部のサービス / アプリケーションは、クラスタ内の特定のノードにのみインストールできます。これらのサービス / アプリケーションのトレースを選択する場合は、必ず、サービス / アプリケーションをアクティブにしたサーバからトレースを選択してください。

ステップ 4　［Select CUP Services/Applications］タブで、次のいずれかの操作を実行します。

- クラスタ内のすべてのサーバ上の、すべてのサービスおよびアプリケーションのトレースを選択する場合は、［**Select All Services on All Servers**］チェックボックスをオンにします。
- 特定のサーバ上の、すべてのサービスおよびアプリケーションのトレースを選択する場合は、サーバの IP アドレスの横にあるチェックボックスをオンにします。
- 特定のサーバ上の、特定のサービスまたはアプリケーションのトレースを選択する場合は、該当するチェックボックスをオンにします。
- サービスまたはアプリケーションのトレースを選択せずにリモート ブラウズ ウィザードを続行する場合は、ステップ 5 に進みます。

（注） アクティブにしていないサービスも表示されるため、そのサービスのトレースを選択できます。

（注） リストされている一部のサービス / アプリケーションは、クラスタ内の特定のノードにのみインストールできます。これらのサービス / アプリケーションのトレースを選択する場合は、必ず、サービス / アプリケーションをアクティブにしたサーバからトレースを選択してください。

ステップ 5　［**Next**］をクリックします。

［System Services/Applications］タブが表示されます。

ステップ 6　次のいずれかの操作を実行します。

- クラスタ内のすべてのサーバ上の、すべてのサービスおよびアプリケーションのシステム ログを選択する場合は、［**Select All Logs on all Servers**］チェックボックスをオンにします。
- 特定のサーバ上の、すべてのシステム ログのトレースを選択する場合は、サーバの IP アドレスの横にあるチェックボックスをオンにします。
- 特定のサーバ上の、特定のシステム ログのトレースを選択する場合は、該当するチェックボックスをオンにします。
- システム ログのトレースを収集せずにリモート ブラウズ ウィザードを続行する場合は、ステップ 13 に進みます。

ステップ 7　［**Next**］をクリックします。

ステップ 8　ステップ 13 に進みます。

ステップ 9　［CUP Applications/Services］タブで、次のいずれかの操作を実行します。

- クラスタ内のすべてのサーバ上の、すべてのサービスおよびアプリケーションのクラッシュ ダンプ ファイルを選択する場合は、［**Select All Services on All Servers**］チェックボックスをオンにします。
- 特定のサーバ上の、すべてのサービスおよびアプリケーションのクラッシュ ダンプ ファイルを選択する場合は、サーバの IP アドレスの横にあるチェックボックスをオンにします。
- 特定のサーバ上の、特定のサービスまたはアプリケーションのクラッシュ ダンプ ファイルを選択する場合は、該当するチェックボックスをオンにします。

ステップ 10　［**Next**］をクリックします。

ステップ 11　［Select System Services/Applications］タブで、次のいずれかの操作を実行します。

- すべてのサーバのクラッシュ ダンプ ファイルを選択する場合は、［**Select All Services on all Servers**］チェックボックスをオンにします。
- 特定のサーバ上の、すべてのシステム ログのクラッシュ ダンプ ファイルを選択する場合は、サーバの IP アドレスの横にあるチェックボックスをオンにします。
- 特定のサーバ上の、特定のシステム ログのクラッシュ ダンプ ファイルを選択する場合は、該当するチェックボックスをオンにします。

- クラッシュ　ダンプ　ファイルを収集せずにクラッシュ　ダンプ収集ウィザードを続行する場合は、ステップ 12 に進みます。

ステップ 12　［**Next**］をクリックします。

ステップ 13　［**Finish**］をクリックします。

ステップ 14　トレースが選択可能になると、メッセージが表示されます。［**Close**］をクリックします。

ステップ 15　次のいずれかの操作を実行します。

- 結果を表示するには、ツリー階層でファイルに移動します。ウィンドウの右側のペインにログ ファイル名が表示されたら、マウスを右クリックしてファイルの表示に使用するプログラムのタイプを選択するか、ファイルをダブルクリックしてデフォルトのビューアでファイルを表示できます。

ヒント　ペインに表示されるファイルをソートするには、列見出しをクリックします。たとえば、名前でファイルをソートする場合は、［Name］の列見出しをクリックします。

Real-Time Monitoring Tool では、ファイル タイプに対応したビューアでファイルが表示されます。他に適切なビューアがない場合は、Generic Log Viewer でファイルが開きます。

- トレース ファイルをダウンロードするには、ダウンロードするファイルを選択して［**Download**］をクリックし、ダウンロードの条件を指定して［**Finish**］をクリックします。
  - トレース ファイルをダウンロードするディレクトリを指定する場合は、［Download all files］フィールドの横にある［**Browse**］ボタンをクリックし、該当するディレクトリを表示して［**Open**］をクリックします。デフォルトでは、C:\Program Files\Cisco\Presence Serviceability\jrtmt\< サーバ IP アドレス >\< ダウンロード時刻 > が指定されます。
  - 収集するトレース ファイルの zip ファイルを作成するには、［**Zip File**］チェックボックスをオンにします。
  - 収集したログ ファイルをサーバから削除するには、［**Delete Files on server**］チェックボックスをオンにします。
- トレース ファイルをノードから削除するには、ウィンドウの右側のペインに表示された対象のファイルをクリックし、［**Delete**］ボタンをクリックします。
- 特定のサービスまたはノードを更新するには、サーバ名またはサービスをクリックし、［**Refresh**］ボタンをクリックします。Remote Browse の準備ができたことを示すメッセージが表示されたら、［**Close**］をクリックします。
- ツリー階層に表示されるすべてのサービスとノードを更新するには、［**Refresh All**］ボタンをクリックします。Remote Browse の準備ができたことを示すメッセージが表示されたら、［**Close**］をクリックします。

ヒント　トレース ファイルをダウンロードしたら、Trace and Log Central 機能の Local Browse オプションを使用してそれらのファイルを表示できます。詳細については、P.10-18 の「Local Browse の使用」を参照してください。

追加情報

P.10-27 の「関連項目」を参照してください。

Q931 Translator の使用

（注）　Cisco Unified Presence は Q931 Translator をサポートしていません。

QRT レポート情報の表示

（注）　Cisco Unified Presence は QRT レポート情報をサポートしていません。

Real Time Trace の使用

RTMT の Trace and Log Central 機能の Real Time Trace オプションを使用すると、アプリケーションごとに、サーバ上で現在書き込まれているトレース ファイルを表示できます。システムがトレース ファイルへの書き込みを開始すると、リアルタイム トレースはトレース ファイルの先頭からではなく、モニタリングを開始したポイントからこのファイルの読み取りを開始します。以前の内容を読み取ることはできません。

リアルタイム トレースには、次のオプションがあります。

- View Real Time Data（P.10-23）
- Monitor User Event（P.10-24）

View Real Time Data

Trace and Log Central 機能の View Real Time Data オプションを使用すると、システムがデータを書き込むと同時にトレース ファイルを表示できます。Generic Log Viewer には、最大 10 個のサービスのリアルタイム トレース データを表示できます。シングル ノードについては 5 つのサービスまでです。ログ ビューアは 5 秒ごとに更新されます。トレースが新しいファイルに切り替わると、Generic Log Viewer はその内容をビューアに追加します。

（注） サービスが書き込むトレースの頻度によっては、View Real Time Data オプションを選択した場合に、Generic Log Viewer にデータを表示できるようになるまで遅延が発生することがあります。

手順

ステップ 1　P.10-3 の「RTMT での Trace & Log Central のオプションの表示」の説明に従って、Trace & Log Central のツリー階層を表示します。

ステップ 2　［**Real Time Trace**］をダブルクリックします。

（注） クラスタ内に使用できないサーバがある場合は、使用できないサーバを特定するメッセージがダイアログボックスに表示されます。使用できないサーバは、Trace & Log Central のウィンドウには表示されません。

ステップ 3　［**View Real Time Data**］をダブルクリックします。

［Real Time Data］ウィザードが表示されます。

ステップ 4　［**Nodes**］ドロップダウン リスト ボックスから、リアルタイム データを表示する対象のノードを選択し、［**Next**］をクリックします。

ステップ 5　リアルタイム データを表示する対象のサービスとトレース ファイル タイプを選択し、［**Finish**］をクリックします。

（注） アクティブにしていないサービスも表示されるため、そのサービスのトレースを収集できます。

選択したサービスのリアルタイム データが Generic Log Viewer に表示されます。

ステップ 6　カーソルをウィンドウの末尾に固定し、新しいトレースが生成されたときにそのトレースを表示する場合は、［**Show New Data**］チェックボックスをオンにします。新しいトレースが表示されるときにカーソルをウィンドウの最下部に移動しない場合は、［**Show New Data**］チェックボックスをオフにします。

ステップ 7　その他のサービスについても、この手順を繰り返します。最大 10 個のサービスのデータを表示できます。ただし、シングル ノードについては 5 つのサービスまでです。データを表示する対象のサービスが多すぎる場合、またはシングル ノード上のサービスが多すぎる場合は、メッセージが表示されます。

ステップ 8　リアルタイム データの表示を完了する場合は、Generic Log Viewer で［**Close**］をクリックします。

追加情報

P.10-27 の「関連項目」を参照してください。

Monitor User Event

Trace and Log Central 機能の Monitor User Event オプションを使用すると、リアルタイム トレース ファイルがモニタされ、トレース ファイル内に検索文字列が見つかったときに、指定されたアクションが実行されます。システムは、トレース ファイルを 5 秒ごとにポーリングします。ポーリング間隔内に検索文字列が複数回発生しても、システムがアクションを実行するのは 1 回だけです。イベントごとに、1 つのノード上の 1 つのサービスをモニタできます。

開始する前に

モニタ対象のトレース ファイル内に指定の検索文字列があるときにアラームを生成する場合は、TraceCollectionToolEvent アラートを有効にします。アラートを有効にする方法の詳細については、P.8-4 の「アラート プロパティの設定」を参照してください。

手順

ステップ 1　P.10-3 の「RTMT での Trace & Log Central のオプションの表示」の説明に従って、Trace & Log Central のツリー階層を表示します。

ステップ 2　［**Real Time Trace**］をダブルクリックします。

（注） クラスタ内に使用できないサーバがある場合は、使用できないサーバを特定するメッセージがダイアログボックスに表示されます。使用できないサーバは、Trace & Log Central のウィンドウには表示されません。

ステップ 3　［**Monitor User Event**］をダブルクリックします。

［Monitor User Event］ウィザードが表示されます。

ステップ 4　次のいずれかの操作を実行します。

- すでに設定されているモニタリング イベントを表示する場合は、［**View Configured Events**］オプション ボタンを選択し、ドロップダウン リスト ボックスからサーバを選択し、［**Finish**］をクリックします。

  選択したサーバ用に設定されたイベントが表示されます。

（注）　イベントを削除する場合は、イベントを選択し、［**Delete**］をクリックします。

- 新しいモニタリング イベントを設定する場合は、［**Create Events**］オプション ボタンを選択し、［**Next**］をクリックして ステップ 5 に進みます。

ステップ 5　［**Nodes**］ドロップダウン リスト ボックスから、システムがモニタするノードを選択し、［**Next**］をクリックします。

ステップ 6　システムがモニタするサービスとトレース ファイル タイプを選択し、［**Next**］をクリックします。

（注）　アクティブにしていないサービスも表示されるため、そのサービスのトレースを収集できます。

ステップ 7　［**Search String**］フィールドに、トレース ファイル内でシステムが検索する単語または句を指定します。このツールは、入力した単語または句の完全一致を検索します。

ステップ 8　システムがトレース ファイルをモニタする対象のサーバの、タイム ゾーンと時間範囲（開始日時と終了日時）を指定します。

クライアント マシンのタイム ゾーンは、［Select Reference Server Time Zone］フィールドのデフォルト設定値です。Daylight Savings 設定値を持つすべてのタイム ゾーンの個別のエントリ セットとともに、すべての標準タイム ゾーンが、［Select Time Zone］ドロップダウン リスト ボックスに表示されます。

選択したタイム ゾーンがサーバ（たとえば、Server 1）のタイム ゾーン設定と一致する場合は、その日付範囲内（開始日付と終了日付の間）の修正されたトレース ファイルがモニタされます。同じ Cisco Unified Presence クラスタ内に別のサーバ（Server 2）が存在し、そのサーバが別のタイム ゾーンである場合、Server 2 の対応する日付範囲内の修正されたトレース ファイルが Server 2 からモニタされます。

トレースをモニタする日付範囲を設定するには、［From Date/Time］フィールドと［To Date/Time］フィールドのドロップダウン リスト ボックスから選択します。

ステップ 9　［Search String］フィールドに指定した検索文字列が見つかった場合にシステムが実行するアクションとして、次の 1 つ以上のアクションを選択します。

- Alert：このオプションは、指定した検索文字列が見つかったときにアラームを生成する場合に選択します。システムがアラームを生成するには、TraceCollectionToolEvent アラートを有効にする必要があります。アラートを有効にする方法の詳細については、P.8-4 の「アラート プロパティの設定」を参照してください。
- Local Syslog：このオプションは、システムがアプリケーション ログ領域のエラーを SysLog Viewer に記録する場合に選択します。システムは、アラームと推奨処置に関する説明を記録します。SysLog Viewer には、RTMT からアクセスできます。
- Remote Syslog：このオプションは、システムが syslog メッセージを syslog サーバに保存できるようにする場合に選択します。［**Server Name**］フィールドに、syslog サーバ名を指定します。
- Download File：このオプションは、指定した検索文字列を含むトレース ファイルをダウンロードする場合に選択します。［SFTP Server Parameters］グループ ボックスに、トレース ファイルをダウンロードするサーバの資格情報を入力し、［**Test Connection**］をクリックします。Trace and Log Central 機能が SFTP サーバへの接続を検証したら、［**OK**］をクリックします。

（注）　［Download Directory Path］フィールドには、Trace and Log Central 機能が収集ファイルを保存するためのディレクトリを指定します。デフォルトでは、トレース収集機能は、SFTP パラメータのフィールドに指定したユーザ ID を持つユーザのホーム ディレクトリ（/home/<ユーザ >/Trace）に収集ファイルを保存します。

（注）　システムはトレース ファイルを 5 秒ごとにポーリングし、検索文字列が見つかった場合は指定されたアクションを実行します。ポーリング間隔内に検索文字列が複数回発生しても、システムがアクションを実行するのは 1 回だけです。

ステップ 10　［**Finish**］をクリックします。

追加情報

P.10-27 の「関連項目」を参照してください。

RTMT のトレース設定の更新

Real-Time Monitoring プラグインのトレース設定を編集するには、［**Edit**］>［**Trace Settings**］の順に選択し、該当するオプション ボタンをクリックします。RTMT プラグインをインストールしたログ ディレクトリ（たとえば、C:\Program Files\Cisco\Presence Serviceability\jrtmt\log）に rtmt.log ファイルが保存されます。

ヒント　Error オプション ボタンはデフォルト設定です。

追加情報

P.10-27 の「関連項目」を参照してください。

関連項目

- Query Wizard の使用（P.10-7）
- Local Browse の使用（P.10-18）
- トレースの収集（P.10-4）
- トレース収集のスケジュール（P.10-11）
- RTMT での Trace & Log Central のオプションの表示（P.10-3）
- クラッシュ ダンプの収集（P.10-15）
- Local Browse の使用（P.10-18）
- トレースの設定（P.5-1）
- RTMT でのアラート設定（P.8-1）

関連項目

CHAPTER 11

RTMT SysLog Viewer の使用

SysLog Viewer にメッセージを表示するには、次の手順を実行します。

手順

ステップ 1 次のいずれかの操作を実行します。

- ［Quick Launch Channel］で［**Tools**］タブをクリックし、［**SysLog Viewer**］および［**SysLog Viewer**］アイコンをクリックします。
- ［**System**］>［**Tools**］>［**SysLog Viewer**］>［**Open SysLog Viewer**］の順に選択します。

ステップ 2 ［Select a Node］ドロップダウン リスト ボックスから、表示するログが保存されているサーバを選択します。

ステップ 3 表示するログのタブをクリックします。

ステップ 4 ログが表示されたら、ログ アイコンをダブルクリックして、同じウィンドウにファイル名のリストを表示します。

ステップ 5 ウィンドウの下部にファイルの内容を表示するには、ファイル名をクリックします。

ステップ 6 表示するエントリをクリックします。

ステップ 7 syslog メッセージ全体を表示するには、syslog メッセージをダブルクリックします。表 11-1 で説明するボタンを使用して、syslog メッセージを表示することもできます。

ヒント 列の幅を広くしたり狭くしたりするには、列見出しの間にカーソルを置いたときに表示される矢印をドラッグします。

ヒント 列見出しをクリックすると、メッセージをソートできます。最初に列見出しをクリックすると、レコードは昇順に表示されます。小さな上向きの三角は、昇順であることを示しています。列見出しをもう一度クリックすると、レコードは降順に表示されます。小さな下向きの三角は、降順であることを示しています。列見出しをさらにもう一度クリックすると、レコードはソートされていない状態で表示されます。

ヒント　［Filter By］ドロップダウン リスト ボックスのオプションを選択すると、結果をフィルタリングすることができます。フィルタを削除するには、Clear Filter をクリックします。フィルタを削除すると、すべてのログが表示されます。

表 11-1　Syslog Viewer のボタン

ボタン	機能
Refresh	Syslog Viewer に表示されている現在のログの内容を更新します。 **ヒント**　Auto Refresh ボタンをチェックすると、Syslog Viewer で syslog メッセージの自動更新が有効になります。
Clear	現在のログの表示をクリアします。
Filter	選択する一連のオプションに基づいて、表示するメッセージを制限します。
Clear Filter	表示するメッセージのタイプを制限するフィルタを削除します。
Find	現在のログに含まれる特定の文字列を検索できます。
Save	現在選択しているログを PC に保存します。

追加情報

P.11-2 の「関連項目」を参照してください。

関連項目

- Real-Time Monitoring の設定（P.7-1）

CHAPTER 12

プラグインの使用

Voice Log Translator（VLT）アプリケーションなどのアプリケーション プラグインをインストールすると、RTMT の機能を拡張できます。RTMT ビューアの最新プラグインは、Cisco.com からダウンロードできます。プラグインをインストールした後は、RTMT ビューアでアプリケーションにアクセスできます。

プラグインをダウンロードするには、次の手順を実行します。

手順

ステップ 1 ［**Application**］>［**CCO Webpage**］の順に選択します。

ステップ 2 Login Prompt が表示されます。Cisco.com のユーザ名とパスワードを入力し、［OK］をクリックします。

ステップ 3 ファイルを PC にダウンロードします。

ステップ 4 インストールを開始するには、ダウンロード ファイルをダブルクリックします。

ステップ 5 インストールの指示に従います。

プラグインにアクセスするには、次の手順を実行します。

手順

ステップ 1 次のいずれかの操作を実行します。

- ［Quick Launch Channel］で、［**Tools**］タブ、［**Plugins**］タブの順にクリックし、目的のアプリケーションのアイコンをクリックします。
- ［**System**］>［**Tools**］>［**Plugin**］から、起動するプラグインを選択します。

プラグイン ウィンドウにアプリケーションが表示されます。

使用方法については、アプリケーションのマニュアルを参照してください。

関連項目

Cisco Voice Log Translator の詳細については、『*Cisco Voice Log Translator User Guide*』を参照してください。

CHAPTER 13

Log Partition Monitoring の設定

Log Partition Monitoring は、次に示す設定済みのしきい値を使用して、1 台のサーバ（またはクラスタ内のすべてのサーバ）上のログ パーティションのディスク使用状況を 5 分ごとにモニタします。

- LogPartitionLowWaterMarkExceeded（ディスク使用率 %）：ディスク使用率が指定のパーセンテージを超えると、LPM はすべてのアラーム メッセージを syslog に送信し、RTMT Alert Central にアラートを送信します。ログ ファイルを保存し、ディスク スペースを回復するには、RTMT で Trace & Log Central のオプションを使用できます。
- LogPartitionHighWaterMarkExceeded（ディスク使用率　%）：ディスク使用率が指定のパーセンテージを超えると、LPM はすべてのアラーム メッセージを syslog に送信し、RTMT Alert Central にアラートを送信します。

Log Partition Monitoring の有効化

Log Partition Monitoring を有効にするには、次の手順を実行します。

手順

ステップ 1　Cisco Unified Presence Serviceability で、［**Tools**］>［**Control Center**］>［**Network Services**］の順に選択します。

ステップ 2　［Servers］ドロップダウン リスト ボックスから、ディスク使用状況をモニタする対象のサーバを選択し、［**Go**］をクリックします。

ステップ 3　［Performance and Monitoring Services］から、Cisco Log Partition Monitoring Tool（LPM）の状況を確認します。

ステップ 4　LPM が実行されていない場合は、Cisco LPM の横にあるオプション ボタンをクリックしてから、［**Start**］ボタンをクリックします。

Log Partition Monitoring の設定

Log Partitioning Monitoring を設定するには、Alert Central で、LogPartitionLowWaterMarkExceeded アラートおよび LogPartitionHighWaterMarkExceeded アラートのアラート プロパティを設定します。P.8-4 の「アラート プロパティの設定」を参照してください。

追加情報

P.13-2 の「関連項目」を参照してください。

関連項目

- 『*Cisco Unified CallManager Serviceability アドミニストレーション ガイド*』の「Log Partition Monitoring」
- RTMT の トレース収集とログ集中管理（P.10-1）

PART 6

レポート ツールの設定

CHAPTER 14

Serviceability Reports Archive の設定

［Serviceability Reports Archive］ウィンドウでは、Serviceability Reporter サービスによって生成されたレポートを表示できます。Serviceability Reporter サービスは、Cisco Unified Presence の管理ページにある Serviceability Reporter サービスのパラメータで指定された時刻にレポートを生成します。

この項では、［Serviceability Reports Archive］ウィンドウの使用方法について説明します。

開始する前に

Cisco Serviceability Report サービスをアクティブにします。Serviceability Reporter サービスは CPU を集中的に使用するので、コール処理を実行していないサーバ上でアクティブにすることをお勧めします。

手順

ステップ 1 **［Tools］>［Serviceability Reports Archive］**の順に選択します。

［Serviceability Reports Archive］ウィンドウに、レポートを表示できる月と年が表示されます。

ステップ 2 ［Month-Year］グループ ボックスから、レポートを表示する月を選択します。

選択した月と年が表示されます。

ステップ 3 レポートを表示するには、RTMT がレポートを生成した日に対応するリンクをクリックします。

選択した日のレポート ファイルが表示されます。

ステップ 4 特定の PDF レポートを表示するには、表示するレポートのリンクをクリックします。

ウィンドウが開き、選択したレポートの PDF ファイルが表示されます。

（注） PDF レポートを表示するには、Acrobat ® Reader をマシンにインストールする必要があります。Acrobat Reader をダウンロードするには、ウィンドウの右下隅のリンクをクリックします。

追加情報

P.14-2 の「関連項目」を参照してください。

関連項目

- Real-Time Monitoring の設定（P.7-1）
- 『*Cisco Unified CallManager Serviceability システム ガイド*』の「Real-Time Monitoring Tool」
- 『*Cisco Unified CallManager Serviceability システム ガイド*』の「Serviceability Reports Archive」

PART 7

SNMP の設定

CHAPTER 15

SNMP V1/V2c の設定

この章では、ネットワーク管理システムで Cisco Unified CallManager をモニタできるように SNMP バージョン 1 および 2c を設定する方法について説明します。この章は、次の項で構成されています。

ヒント SNMP バージョン 3 を使用する場合は、P.16-1 の「SNMP V3 の設定」を参照してください。

コミュニティ ストリングの検索

ヒント　［Add New］ボタンは、［Find］ボタンをクリックするまで［SNMP Community String Configuration］ウィンドウに表示されません。コミュニティ ストリングが存在しない場合、コミュニティ ストリングを追加するには、**［Find］**ボタンをクリックして、ウィンドウが更新されるのを待ちます。［Add New］ボタンが表示されます。

コミュニティ ストリングを検索するには、次の手順を実行します。

手順

ステップ 1　**［Snmp］**>**［V1/V2c］**>**［Community String］**の順に選択します。

［Find/List］ウィンドウが表示されます。

ステップ 2　［Find Community Strings where Name］ドロップダウン リスト ボックスから、コミュニティ ストリングに使用する特定の検索条件を選択します。

ステップ 3　検索するコミュニティ ストリングを入力します。

ステップ 4　［Server］フィールドに、コミュニティ ストリングが存在するサーバのホスト名または IP アドレスを入力します。

ステップ 5　**［Find］**をクリックします。

［Find］ボタンをクリックすると、［Add New］ボタンが表示されます。検索結果が表示された後、［Apply to All Nodes］チェックボックスが表示されます。

ステップ 6　検索結果のオプションの 1 つから、クラスタ内のすべてのノードに設定を適用する場合は、オプション名の横にあるチェックボックスをオンにしてから、**［Apply to All Nodes］**チェックボックスをオンにします。

ステップ 7　検索結果のリストから、表示するコミュニティ ストリングをクリックします。

ステップ 8　コミュニティ ストリングの追加方法または更新方法については、P.15-3 の「コミュニティ ストリングの設定」を参照してください。

追加情報

P.15-10 の「関連項目」を参照してください。

コミュニティ ストリングの設定

SNMP エージェントはコミュニティ ストリングを使用してセキュリティを提供するので、Cisco Unified CallManager システムで、管理情報ベース（MIB）にアクセスするためのコミュニティ ストリングを設定する必要があります。Cisco Unified CallManager システムへのアクセスを制限するには、コミュニティ ストリングを変更します。コミュニティ ストリングを追加、変更、削除するには、［SNMP Community String Configuration］ウィンドウにアクセスします。

手順

ステップ 1　P.15-2 の「コミュニティ ストリングの検索」の手順を実行します。

ステップ 2　次のいずれかの操作を実行します。

- 新しいコミュニティ ストリングを追加する場合は、［**Add New**］ボタンをクリックし、ステップ 3 に進みます。
- 既存のコミュニティ ストリングを変更する場合は、P.15-2 の「コミュニティ ストリングの検索」の説明に従ってコミュニティ ストリングを見つけ、編集するコミュニティ ストリング名をクリックしてから、ステップ 3 に進みます。

  コミュニティ ストリング名やコミュニティ ストリングのサーバを変更することはできません。
- コミュニティ ストリングを削除する方法については、P.15-6 の「コミュニティ ストリングの削除」を参照してください。

ステップ 3　表 15-1 の説明に従って、設定値を入力します。

ヒント　新しいコミュニティ ストリングを追加する場合、いつでも［**Clear All**］ボタンをクリックして、すべての設定値に入力したすべての情報を削除することができます。

ステップ 4　設定が完了したら、［**Add New**］をクリックして新しいコミュニティ ストリングを保存するか、［**Save**］をクリックして既存のコミュニティ ストリングへの変更を保存します。

ステップ 5　SNMP マスター エージェントを再起動するまで変更が有効にならないことを示すメッセージが表示されます。SNMP マスター エージェントを再起動せずに設定を続行するには、［**Cancel**］をクリックします。SNMP マスター エージェント サービスを再起動するには、［**OK**］をクリックします。

（注）　すべての SNMP 設定が終了するのを待ってから、SNMP マスター エージェント サービスを再起動することをお勧めします。サービスを再起動する方法については、P.2-3 の「Control Center におけるサービスの開始、停止、再起動、および状況更新」を参照してください。

［SNMP Community String Configuration］ウィンドウの表示が更新されます。作成したコミュニティ ストリングがウィンドウに表示されます。

追加情報

P.15-10 の「関連項目」を参照してください。

コミュニティ ストリングの設定値

表 15-1 に、コミュニティ ストリングの設定値を示します。関連する手順については、P.15-10 の「関連項目」を参照してください。

表 15-1　コミュニティ ストリングの設定値

フィールド	説明
Server	P.15-2 の「コミュニティ ストリングの検索」の手順を実行したときにサーバを指定したので、［Community String Configuration］ウィンドウでは、この設定値は読み取り専用として表示されます。 コミュニティ ストリングのサーバを変更する場合は、P.15-2 の「コミュニティ ストリングの検索」の手順を実行します。
Community String	コミュニティ ストリング名を入力します。名前には、英数字、ハイフン（-）、アンダースコア（_）の任意の組み合せで、最大 32 文字を指定できます。 **ヒント**　外部者にわかりにくいコミュニティ　ストリング名を選択してください。 コミュニティ ストリングを編集するときに、コミュニティ ストリング名を変更することはできません。
Accept SNMP Packets from any host	すべてのホストから SNMP パケットを受け入れる場合は、このオプション ボタンをクリックします。
Accept SNMP Packets only from these hosts	指定したホストから SNMP パケットを受け入れる場合は、このオプション ボタンをクリックします。 **ヒント**　［Host IP Address］フィールドに、パケットの送信元のホストを入力し、［**Insert**］をクリックします。パケットの送信元のホストごとに、このプロセスを繰り返します。ホストを削除するには、［Host IP Addresses］リスト ボックスからホストを選択し、［**Remove**］をクリックします。

表 15-1　コミュニティ ストリングの設定値（続き）

フィールド	説明
Access Privileges	ドロップダウン リスト ボックスから、次に示す適切なアクセス レベルを選択します。 • **ReadOnly**：コミュニティ ストリングは、MIB オブジェクト値の読み取りのみが可能です。 • **ReadWrite**：コミュニティ ストリングは、MIB オブジェクト値の読み取りと書き込みが可能です。 • **ReadWriteNotify**：コミュニティ ストリングは、MIB オブジェクト値の読み取りと書き込みに加えて、MIB オブジェクト値のトラップおよび通知メッセージの送信が可能です。 • **NotifyOnly**：コミュニティ ストリングは、MIB オブジェクト値のトラップおよび通知メッセージの送信のみが可能です。 • **None**：コミュニティ ストリングは、読み取り、書き込み、トラップ情報送信のいずれも不可能です。 **ヒント**　Cisco Unified Presence トラップの設定パラメータを変更するには、NotifyOnly 特権または ReadWriteNotify 特権を持つコミュニティを使用する必要があります。
Apply To All Nodes	コミュニティ ストリングをクラスタ内のすべてのノードに適用する場合は、このチェックボックスをオンにします。

コミュニティ ストリングの削除

コミュニティ ストリングを削除するには、次の手順を実行します。

手順

ステップ 1　P.15-2 の「コミュニティ ストリングの検索」の説明に従って、コミュニティ ストリングを見つけます。

ステップ 2　一致レコードのリストから、削除するコミュニティ ストリングの横にあるチェックボックスをオンにします。

ステップ 3　［**Delete Selected**］をクリックします。

ステップ 4　このコミュニティ　ストリングに関連する通知エントリが削除されることを示すメッセージが表示されます。削除を続行する場合は、［**OK**］をクリックします。

ステップ 5　SNMP マスター エージェントを再起動するまで変更が有効にならないことを示すメッセージが表示されます。SNMP マスター エージェントを再起動せずに設定を続行するには、［**Cancel**］をクリックします。SNMP マスター エージェント サービスを再起動するには、［**OK**］をクリックします。

ヒント　すべての SNMP 設定が終了するのを待ってから、SNMP マスター エージェント サービスを再起動することをお勧めします。サービスを再起動する方法については、P.2-3 の「Control Center におけるサービスの開始、停止、再起動、および状況更新」を参照してください。

ウィンドウが更新されると、削除したコミュニティ ストリングは結果に表示されなくなります。

追加情報

P.15-10 の「関連項目」を参照してください。

通知先の検索

ヒント　［Add New］ボタンは、［Find］ボタンをクリックするまで［SNMP Notification Destination Configuration］ウィンドウに表示されません。通知先が存在しない場合、通知先を追加するには、**［Find］**ボタンをクリックして、ウィンドウが更新されるのを待ちます。［Add New］ボタンが表示されます。

V1/V2c の通知先を検索するには、次の手順を実行します。

手順

ステップ 1　**［Snmp］**>**［V1/V2c］**>**［Notification Destination］**の順に選択します。

［Find/List］ウィンドウが表示されます。

ステップ 2　［Find Notification where Destination IP］ドロップダウン リスト ボックスから、通知先の検索に使用する特定の検索条件を選択します。

ステップ 3　検索する通知先を入力します。

ステップ 4　［Server］フィールドに、通知先をサポートするサーバのホスト名または IP アドレスを入力します。

ステップ 5　**［Find］**をクリックします。

［Find］ボタンをクリックすると、［Add New］ボタンが表示されます。検索結果が表示された後、［Apply to All Nodes］チェックボックスが表示されます。

ステップ 6　検索結果のオプションの 1 つから、クラスタ内のすべてのノードに設定を適用する場合は、オプション名の横にあるチェックボックスをオンにしてから、**［Apply to All Nodes］**チェックボックスをオンにします。

ステップ 7　検索結果のいずれかの項目の設定を表示するには、その項目をクリックします。

ステップ 8　通知先の追加方法または更新方法については、P.15-8 の「V1/V2c の通知先の設定」を参照してください。

追加情報

P.15-10 の「関連項目」を参照してください。

V1/V2c の通知先の設定

V1/V2c の通知先（トラップ / 通知の受信者）を設定するには、次の手順を実行します。

手順

ステップ 1　P.15-7 の「通知先の検索」の手順を実行します。

ステップ 2　次のいずれかの操作を実行します。

- 新しい SNMP 通知先を追加する場合は、［**Add New**］ボタンをクリックし、ステップ 3 に進みます。

  ［Find/List］ウィンドウの［Server］ドロップダウン リスト ボックスで選択したサーバの通知先を設定します。
- 既存の SNMP 通知先を変更する場合は、P.15-7 の「通知先の検索」の説明に従って通知先を見つけ、編集する SNMP 通知先名をクリックしてから、ステップ 3 に進みます。
- SNMP 通知先を削除する方法については、P.15-10 の「通知先の削除」を参照してください。

ステップ 3　表 15-2 の説明に従って、設定値を入力します。

ヒント　新しい通知先を追加する場合、いつでも［**Clear**］ボタンをクリックして、すべての設定値に入力したすべての情報を削除することができます。

ステップ 4　［**Insert**］をクリックして通知先を保存するか、［**Save**］をクリックして既存の通知先への変更を保存します。

ステップ 5　SNMP マスター エージェントを再起動するまで変更が有効にならないことを示すメッセージが表示されます。SNMP マスター エージェントを再起動せずに設定を続行するには、［**Cancel**］をクリックします。SNMP マスター エージェントを再起動するには、［**OK**］をクリックします。

（注）　SNMP 設定が終了するのを待ってから、SNMP マスター エージェント サービスを再起動することをお勧めします。サービスを再起動する方法については、P.2-3 の「Control Center におけるサービスの開始、停止、再起動、および状況更新」を参照してください。

追加情報

P.15-10 の「関連項目」を参照してください。

V1/V2c の通知先の設定値

表 15-2 に、V1/V2c の通知先の設定値を示します。関連する手順については、P.15-10 の「関連項目」を参照してください。

表 15-2　V1/V2c の通知先の設定値

フィールド	説明
Server	P.15-7 の「通知先の検索」の手順を実行したときに、サーバを指定したので、この設定値は、読み取り専用として表示されます。 通知先のサーバを変更する場合は、P.15-2 の「コミュニティ ストリングの検索」の手順を実行します。
Host IP Addresses	ドロップダウン リスト ボックスからトラップ宛先のホスト IP アドレスを選択するか、［**Add New**］を選択します。［Add New］を選択した場合は、トラップ宛先の IP アドレスを入力します。 既存の通知先の場合は、ホスト IP アドレスの設定は変更できません。
Port Number	このフィールドに、SNMP パケットを受信する通知先サーバが通知を受信するポート番号を入力します。
V1 or V2C	［SNMP Version Information］ペインで、該当する SNMP バージョンのオプション ボタンである V1 または V2C のいずれか（使用する SNMP のバージョンによって異なる）をクリックします。 • V1 を選択した場合は、コミュニティ ストリングの設定値を設定します。 • V2C を選択した場合は、通知タイプの設定値を設定してから、コミュニティ ストリングを設定します。
Community String	ドロップダウン リスト ボックスから、このホストが生成する通知メッセージで使用するコミュニティ ストリング名を選択します。 最下位の通知特権（ReadWriteNotify または Notify Only）を持つコミュニティ ストリングのみが表示されます。このような特権を持つコミュニティ ストリングを設定していない場合、ドロップダウン リスト ボックスにオプションは表示されません。必要に応じて［**Create New Community String**］ボタンをクリックし、P.15-3 の「コミュニティ ストリングの設定」の説明に従ってコミュニティ ストリングを作成します。
Notification Type	ドロップダウン リスト ボックスから、適切な通知タイプを選択します。
Apply To All Nodes	通知先の設定をクラスタ内のすべてのノードに適用する場合は、このチェックボックスをオンにします。

通知先の削除

通知先を削除するには、次の手順を実行します。

手順

ステップ 1　P.15-7 の「通知先の検索」の説明に従って、通知先を見つけます。

ステップ 2　一致レコードのリストから、削除する通知先の横にあるチェックボックスをオンにします。

ステップ 3　［**Delete Selected**］をクリックします。

ステップ 4　通知先のエントリを削除するかどうかを尋ねるメッセージが表示されます。削除を続行する場合は、［**OK**］をクリックします。

ステップ 5　SNMP マスター エージェントを再起動するまで変更が有効にならないことを示すメッセージが表示されます。SNMP マスター エージェントを再起動せずに設定を続行するには、［**Cancel**］をクリックします。SNMP マスター エージェント サービスを再起動するには、［**OK**］をクリックします。

ヒント　すべての SNMP 設定が終了するのを待ってから、SNMP マスター エージェント サービスを再起動することをお勧めします。サービスを再起動する方法については、P.2-3 の「Control Center におけるサービスの開始、停止、再起動、および状況更新」を参照してください。

ウィンドウが更新されると、削除した通知先は結果に表示されなくなります。

追加情報

P.15-10 の「関連項目」を参照してください。

関連項目

- コミュニティ ストリングの設定（P.15-3）
- V1/V2c の通知先の設定（P.15-8）
- SNMP V3 の設定（P.16-1）
- MIB2 システム グループの設定（P.17-1）

CHAPTER 16

SNMP V3 の設定

この章では、ネットワーク管理システムで Cisco Unified CallManager をモニタできるように SNMP v3 を設定する方法について説明します。この章は、次の項で構成されています。

ヒント SNMP v1 または v2c を使用する場合は、P.15-1 の「SNMP V1/V2c の設定」を参照してください。

SNMP ユーザの検索

ヒント　［Add New］ボタンは、［Find］ボタンをクリックするまで［SNMP User Configuration］ウィンドウに表示されません。ユーザが存在しない場合、ユーザを追加するには、**［Find］**ボタンをクリックして、ウィンドウが更新されるのを待ちます。［Add New］ボタンが表示されます。

SNMP ユーザを検索するには、次の手順を実行します。

手順

ステップ 1　**［Snmp］**>**［V3］**>**［User］**の順に選択します。

［SNMP User Configuration］ウィンドウが表示されます。

ステップ 2　［Find User where Name］リスト ボックスから、ユーザの検索に使用する特定の検索条件（［begin with］など）を選択します。

ステップ 3　検索するユーザ名を入力します。

ステップ 4　［Server］ドロップダウン リスト ボックスから、ユーザにアクセスするサーバのホスト名または IP アドレスを選択します。

ステップ 5　**［Find］**をクリックします。

［Find］ボタンをクリックすると、［Add New］ボタンが表示されます。検索結果が表示された後、［Apply to All Nodes］チェックボックスが表示されます。

ヒント　［Apply to All Nodes］チェックボックスは、Cisco Unified Communications Managar Business Edition システムには適用されません。

ステップ 6　検索結果のオプションの 1 つから、クラスタ内のすべてのノードに設定を適用する場合は、オプション名の横にあるチェックボックスをオンにしてから、**［Apply to All Nodes］**チェックボックスをオンにします。

ステップ 7　検索結果のリストから、表示するユーザをクリックします。

ステップ 8　ユーザの追加方法または更新方法については、P.16-3 の「SNMP ユーザの設定」を参照してください。

追加情報

P.16-10 の「関連項目」を参照してください。

SNMP ユーザの設定

SNMP のユーザを設定するには、次の手順を実行します。

手順

ステップ 1　P.16-7 の「通知先の検索」の手順を実行します。

ステップ 2　次のいずれかの操作を実行します。

- 新しい SNMP ユーザを追加する場合は、[SNMP User Configuration Find/List] ウィンドウで [**Add New**] ボタンをクリックし、ステップ 3 に進みます。
- 既存のユーザを変更する場合は、P.16-7 の「通知先の検索」の説明に従ってユーザを見つけ、編集する SNMP ユーザ名をクリックしてから、ステップ 3 に進みます。
- SNMP ユーザを削除する方法については、P.16-6 の「SNMP ユーザの削除」を参照してください。

ステップ 3　表 16-1 の説明に従って、設定値を入力します。

ヒント　いつでも［**Clear All**］ボタンをクリックして、すべての設定値に入力したすべての情報を削除できます。

ステップ 4　［**Insert**］をクリックして新しいユーザを追加するか、［**Save**］をクリックして既存のユーザへの変更を保存します。

ステップ 5　SNMP マスター エージェントを再起動するまで変更が有効にならないことを示すメッセージが表示されます。SNMP マスター エージェントを再起動せずに設定を続行するには、［**Cancel**］をクリックします。SNMP マスター エージェント サービスを再起動するには、［**OK**］をクリックします。

ヒント　SNMP 設定が終了するのを待ってから、SNMP マスター エージェント サービスを再起動することをお勧めします。サービスを再起動する方法については、P.2-1 の「サービスの管理」を参照してください。

（注）　設定したユーザを使用してこの Cisco Unified CallManager サーバにアクセスするには、このユーザを、NMS 上で適切な認証とプライバシーの設定値で設定したことを確認します。

追加情報

P.16-10 の「関連項目」を参照してください。

SNMP ユーザの設定値

表 16-1 に、V3 の SNMP ユーザの設定値を示します。関連する手順については、P.16-10 の「関連項目」を参照してください。

表 16-1　V3 の SNMP ユーザの設定値

フィールド	説明
Server	P.16-7 の「通知先の検索」の手順を実行したときにサーバを指定したので、この設定値は、読み取り専用として表示されます。 アクセス権を与える対象となるサーバを変更するには、P.16-2 の「SNMP ユーザの検索」の手順を実行します。
User Name	このフィールドに、アクセス権を与える対象となるユーザの名前を入力します。名前には、英数字、ハイフン（-）、アンダースコア（_）の任意の組み合せで、最大 32 文字を指定できます。 **ヒント**　ネットワーク管理システム（NMS）に対してすでに設定されているユーザを入力します。 既存の SNMP ユーザの場合、この設定値は読み取り専用として表示されます。
Authentication Required	認証を要求する場合は、このチェックボックスをオンにして、［Password］フィールドと［Reenter Password］フィールドにパスワードを入力し、適切なプロトコルを選択します。パスワードは、8 文字以上にする必要があります。
Privacy Required	［Authentication Required］チェックボックスをオンにした場合は、プライバシー情報を指定できます。プライバシーを要求する場合は、このチェックボックスをオンにして、［Password］フィールドと［Reenter Password］フィールドにパスワードを入力し、適切なプロトコルのチェックボックスをオンにします。パスワードは、8 文字以上にする必要があります。 **ヒント**　［Privacy Required］チェックボックスをオンにすると、［DES（Data Encryption Standard）］チェックボックスも自動的にオンになります。DES プロトコルを使用すると、パケットが解読されるのを防止できます。
Accept SNMP Packets from any host	すべてのホストから SNMP パケットを受け入れる場合は、このオプション ボタンをクリックします。
Accept SNMP Packets only from these hosts	特定のホストから SNMP パケットを受け入れる場合は、このオプション ボタンをクリックします。［Host IP Address］フィールドに、SNMP パケットの送信元のホストを入力し、**［Insert］**をクリックします。SNMP パケットの送信元のホストごとに、このプロセスを繰り返します。ホストを削除する場合は、［Host IP Addresses］ペインからホストを選択し、**［Remove］**をクリックします。

表 16-1　V3 の SNMP ユーザの設定値

フィールド	説明
Access Privileges	ドロップダウン リスト ボックスから、アクセス レベルに関する次のオプションのいずれかを選択します。 • **ReadOnly**：ユーザは、MIB オブジェクト値の読み取りのみが可能です。 • **ReadWrite**：ユーザは、MIB オブジェクト値の読み取りと書き込みが可能です。 • **ReadWriteNotify**：ユーザは、MIB オブジェクト値の読み取りと書き込みに加えて、MIB オブジェクト値のトラップおよび通知メッセージの送信が可能です。 • **NotifyOnly**：ユーザは、MIB オブジェクト値のトラップおよび通知メッセージの送信のみが可能です。 • **None**：ユーザは、読み取り、書き込み、トラップ情報送信のいずれも不可能です。 トラップの設定パラメータを変更するには、NotifyOnly 特権または ReadWriteNotify 特権を持つユーザを設定する必要があります。
Apply To All Nodes	ユーザをクラスタ内のすべてのノードに適用する場合は、このチェックボックスをオンにします。

SNMP ユーザの削除

SNMP のユーザを削除するには、次の手順を実行します。

手順

ステップ 1　P.16-2 の「SNMP ユーザの検索」の説明に従って、SNMP ユーザを特定します。

ステップ 2　一致レコードのリストから、削除するユーザの横にあるチェックボックスをオンにします。

ステップ 3　［**Delete Selected**］をクリックします。

ステップ 4　このユーザに関連する通知先エントリが削除されることを示すメッセージが表示されます。削除を続行する場合は、［**OK**］をクリックします。

ステップ 5　SNMP マスター エージェントを再起動するまで変更が有効にならないことを示すメッセージが表示されます。SNMP マスター エージェントを再起動せずに設定を続行するには、［**Cancel**］をクリックします。SNMP マスター エージェント サービスを再起動するには、［**OK**］をクリックします。

ヒント　すべての SNMP 設定が終了するのを待ってから、SNMP マスター エージェント サービスを再起動することをお勧めします。サービスを再起動する方法については、P.2-1 の「サービスの管理」を参照してください。

ウィンドウが更新されると、削除したユーザは結果に表示されなくなります。

追加情報

P.16-10 の「関連項目」を参照してください。

通知先の検索

ヒント　［Add New］ボタンは、［Find］ボタンをクリックするまで［SNMP Notification Destination Configuration］ウィンドウに表示されません。ユーザが存在しない場合、ユーザを追加するには、**［Find］**ボタンをクリックして、ウィンドウが更新されるのを待ちます。［Add New］ボタンが表示されます。

V3 の通知先を検索するには、次の手順を実行します。

手順

ステップ 1　**［Snmp］** > **［V3］** > **［Notification Destination］**の順に選択します。

ステップ 2　［Find Notification where Destination IP］ドロップダウン リスト ボックスから、通知先の検索に使用する特定の検索条件（［begin with］など）を選択します。

ステップ 3　検索対象とする通知先の IP アドレスまたはホスト名を入力します。

ステップ 4　［Server］フィールドで、通知先をサポートするサーバのホスト名または IP アドレスを選択します。

ステップ 5　**［Find］**をクリックします。

［Find］ボタンをクリックすると、［Add New］ボタンが表示されます。検索結果が表示された後、［Apply to All Nodes］チェックボックスが表示されます。

ステップ 6　検索結果のオプションの 1 つから、クラスタ内のすべてのノードに設定を適用する場合は、オプション名の横にあるチェックボックスをオンにしてから、**［Apply to All Nodes］**チェックボックスをオンにします。

ステップ 7　検索結果のリストから、表示する通知先をクリックします。

ステップ 8　通知先の追加方法または更新方法については、P.16-8 の「SNMP V3 の通知先の設定」を参照してください。

追加情報

P.16-10 の「関連項目」を参照してください。

SNMP V3 の通知先の設定

トラップ / 通知の受信者を設定するには、次の手順を実行します。

手順

ステップ 1　P.16-7 の「通知先の検索」の手順を実行します。

ステップ 2　次のいずれかの操作を実行します。

- 新しい SNMP 通知先を追加する場合は、検索結果ウィンドウで［**Add New**］ボタンをクリックし、ステップ 3 に進みます。
- 既存の　SNMP　通知先を変更する場合は、検索結果ウィンドウで通知先を見つけ、編集する SNMP 通知先名をクリックしてから、ステップ 3 に進みます。
- SNMP 通知先を削除する方法については、P.16-10 の「SNMP V3 の通知先の削除」を参照してください。

ステップ 3　表 16-2 の説明に従って、設定値を入力します。

ヒント　いつでも［**Clear**］ボタンをクリックして、設定値に入力したすべての情報を削除できます。

ステップ 4　［**Insert**］をクリックして通知先を保存するか、［**Save**］をクリックして既存の通知先への変更を保存します。

ステップ 5　SNMP マスター エージェントを再起動するまで変更が有効にならないことを示すメッセージが表示されます。SNMP マスター エージェントを再起動せずに設定を続行するには、［**Cancel**］をクリックします。SNMP マスター エージェント サービスを再起動するには、［**OK**］をクリックします。

ヒント　SNMP 設定が終了するのを待ってから、SNMP マスター エージェント サービスを再起動することをお勧めします。サービスを再起動する方法については、P.2-1 の「サービスの管理」を参照してください。

追加情報

P.16-10 の「関連項目」を参照してください。

SNMP V3 の通知先の設定値

表 16-2 に、V3 の通知先の設定値を示します。関連する手順については、P.16-10 の「関連項目」を参照してください。

表 16-2　V3 の通知先の設定値

フィールド	説明
Server	P.16-7 の「通知先の検索」の手順を実行したときにサーバを指定したので、この設定値は、読み取り専用として表示されます。 通知先のサーバを変更する場合は、P.16-7 の「通知先の検索」の手順を実行します。
Host IP Addresses	ドロップダウン リスト ボックスからホスト IP アドレスを選択するか、［**Add New**］を選択します。［Add New］を選択した場合は、ホストの IP アドレスを入力します。
Port Number	このフィールドに、通知先サーバが通知を受信するポート番号を入力します。
Notification Type	ドロップダウン リスト ボックスから、［**Inform**］または［**Trap**］を選択します。 **ヒント**　Inform オプションを選択することをお勧めします。Inform 機能では、確認応答されるまでメッセージが再送信されます。したがって、Inform は Trap よりも信頼性が高くなります。
Remote SNMP Engine Id	［Notification Type］ドロップダウン リスト ボックスで［Inform］を選択した場合は、この設定値が表示されます。 ドロップダウン リスト ボックスからエンジン ID を選択するか、［**Add New**］を選択します。［Add New］を選択した場合は、［Remote SNMP Engine Id］フィールドにエンジン ID を 16 進数で入力します。
Security Level	ドロップダウン リスト ボックスから、適切なセキュリティ レベルを選択します。 • **noAuthNoPriv**：認証もプライバシーも設定されません。 • **authNoPriv**：認証は設定されますが、プライバシーは設定されません。 • **authPriv**：認証とプライバシーが設定されます。
User Information pane	このペインから次のいずれかの操作を実行して、通知先をユーザに関連付けたり、関連付けを解除したりします。 • 新しいユーザを作成する場合は、［**Create New User**］ボタンをクリックし、P.16-3 の「SNMP ユーザの設定」を参照してください。 • 既存のユーザを変更する場合は、そのユーザのオプション ボタンをクリックし、［**Update Selected User**］をクリックします。P.16-3 の「SNMP ユーザの設定」を参照してください。 • ユーザを削除する場合は、そのユーザのオプション　ボタンをクリックし、［**Delete Select User**］をクリックします。 表示されるユーザは、通知先に設定したセキュリティ レベルによって異なります。
Apply To All Nodes	通知先の設定をクラスタ内のすべてのノードに適用する場合は、このチェックボックスをオンにします。

SNMP V3 の通知先の削除

通知先を削除するには、次の手順を実行します。

手順

ステップ 1　P.16-7 の「通知先の検索」の説明に従って、SNMP 通知先を見つけます。

ステップ 2　一致レコードのリストから、削除する通知先の横にあるチェックボックスをオンにします。

ステップ 3　［**Delete Selected**］をクリックします。

ステップ 4　通知先を削除するかどうかを尋ねるメッセージが表示されます。削除を続行する場合は、［**OK**］をクリックします。

ステップ 5　SNMP マスター エージェントを再起動するまで変更が有効にならないことを示すメッセージが表示されます。SNMP マスター エージェントを再起動せずに設定を続行するには、［**Cance**］**l** をクリックします。SNMP マスター エージェント サービスを再起動するには、［**OK**］をクリックします。

ヒント　すべての SNMP 設定が終了するのを待ってから、SNMP マスター エージェント サービスを再起動することをお勧めします。サービスを再起動する方法については、P.2-3 の「Control Center におけるサービスの開始、停止、再起動、および状況更新」を参照してください。

ウィンドウが更新されると、削除した通知先は検索結果ウィンドウに表示されなくなります。

追加情報

P.16-10 の「関連項目」を参照してください。

関連項目

- SNMP V1/V2c の設定（P.15-1）
- SNMP ユーザの設定（P.16-3）
- MIB2 システム グループの設定（P.17-1）
- SNMP V3 の通知先の設定（P.16-8）

CHAPTER 17

MIB2 システム グループの設定

Cisco Unified Presence Serviceability の［MIB2 System Group Configuration］ウィンドウでは、MIB-II システム グループについて、システムの連絡先とシステムの場所のオブジェクトを設定できます。たとえば、システムの連絡先として Administrator, 555-121-6633、システムの場所として San Jose, Bldg 23, 2nd floor のように入力できます。この章は、次の項で構成されています。

MIB2 システム グループの設定

MIB-II システム グループについて、システムの連絡先とシステムの場所を設定するには、次の手順を実行します。

ヒント　この手順は、SNMP v1、v2c、および v3 の設定をサポートしています。

手順

ステップ 1　［**Snmp**］>［**System Group**］>［**MIB2 System Group**］の順に選択します。

ステップ 2　表 17-1 の説明に従って、設定値を入力します。

ステップ 3　［**Save**］をクリックします。

ステップ 4　SNMP マスター エージェントを再起動するまで変更が有効にならないことを示すメッセージが表示されます。SNMP マスター エージェント サービスを再起動せずに設定を続行するには、［**Cancel**］をクリックします。SNMP マスター エージェント サービスを再起動するには、［**OK**］をクリックします。

（注）　［System Contact］フィールドと［System Location］フィールドをクリアするには、［**Clear All**］ボタンをクリックします。システム設定を削除するには、［**Clear All**］ボタンをクリックしてから、［**Save**］ボタンをクリックします。

追加情報

P.17-3 の「関連項目」を参照してください。

MIB2 システム グループの設定値

表 17-1 に、MIB2 システム グループの設定値を示します。関連する手順については、P.17-3 の「関連項目」を参照してください。

表 17-1　MIB2 システム グループの設定値

フィールド	説明
Server	このドロップダウン リスト ボックスから、連絡先を設定する対象のサーバを選択し、［**Go**］をクリックします。
System Contact	このフィールドに、問題が発生したときに通知する個人を入力します。
System Location	このフィールドに、システムの連絡先として指定した個人の場所を入力します。
Apply To All Nodes	このシステム設定をクラスタ内のすべてのノードに適用する場合は、このチェックボックスをオンにします。

関連項目

- SNMP V1/V2c の設定（P.15-1）
- SNMP V3 の設定（P.16-1）

関連項目

INDEX

A

C

H

L

M

N

Q

R

S

あ

え

か

き

こ

さ

し

せ

つ

て

と

ね

は

ふ

ほ

も

ゆ