



**Cisco Unified Presence Server**  
**サービスアビリティ**  
**アドミニストレーション ガイド**

Release 1.0(3)



このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザ側の責任になります。

対象製品のソフトウェア ライセンスおよび限定保証は、製品に添付された『Information Packet』に記載されています。見当たらない場合には、代理店にご連絡ください。

シスコが採用している TCP ヘッダー圧縮機能は、UNIX オペレーティング システムの UCB (University of California, Berkeley) パブリック ドメイン バージョンとして、UCB が開発したプログラムを最適化したものです。All rights reserved.Copyright © 1981, Regents of the University of California.

ここに記載されている他のいかなる保証にもよらず、すべてのマニュアルおよび上記各社のソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコおよび上記各社は、商品性や特定の目的への適合性、権利を侵害しないことに関する、または取り扱い、使用、または取り引きによって発生する、明示されたまたは黙示された一切の保証の責任を負わないものとします。

いかなる場合においても、シスコおよびその代理店は、このマニュアルの使用またはこのマニュアルを使用できないことによって起こる制約、利益の損失、データの損傷など間接的で偶発的に起こる特殊な損害のあらゆる可能性がシスコまたは代理店に知らされていても、それらに対する責任を一切負いかねます。

CCVP, the Cisco Logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, IQ Expertise, the IQ logo, IQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, *Packet*, PIX, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners.The use of the word partner does not imply a partnership relationship between Cisco and any other company.(0609R)

*Cisco Unified Presence Server サービスアビリティ アドミニストレーション ガイド*  
Copyright © 2006 Cisco Systems, Inc.  
All rights reserved.



<b>このマニュアルについて</b>	<b>ix</b>
目的	ix
対象読者	ix
マニュアルの構成	x
関連マニュアル	xi
表記法	xi
技術情報の入手方法	xii
Cisco.com	xii
Product Documentation DVD (英語版)	xiii
マニュアルの発注方法 (英語版)	xiii
シスコシステムズマニュアルセンター	xiii
シスコ製品のセキュリティの概要	xiv
シスコ製品のセキュリティ問題の報告	xiv
Product Alerts および Field Notices	xv
テクニカル サポート	xvi
Cisco Support Web サイト	xvi
Japan TAC Web サイト	xvii
サービス リクエストの発行	xvii
サービス リクエストのシビラティの定義	xvii
その他の資料および情報の入手方法	xviii

---

PART 1

---

**Cisco Unified Presence Server Serviceability**

---

CHAPTER 1

<b>概要</b>	<b>1-1</b>
Cisco Unified Presence Server Serviceability の概要	1-1
Cisco Unified Presence Server Serviceability へのアクセス	1-2
Hypertext Transfer Protocol over Secure Sockets Layer (HTTPS) の使用	1-3
HTTPS の概要 (Internet Explorer の場合)	1-3
信頼できるフォルダへの証明書の保存 (Internet Explorer の場合)	1-4
信頼できるフォルダへの証明書の保存 (Netscape の場合)	1-5
Cisco Unified Presence Server Serviceability のインターフェイスの使用	1-6

アクセシビリティ機能	1-8
参考情報	1-8
関連項目	1-8

PART 2

サービスの管理

CHAPTER 2

サービスの管理 2-1

機能サービスのアクティブ化と非アクティブ化	2-2
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	2-3
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	2-4
関連項目	2-4

PART 3

アラームの設定

CHAPTER 3

アラームの設定 3-1

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

CHAPTER 4

アラーム定義 4-1

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

PART 4

トレースの設定

CHAPTER 5

トレースの設定 5-1

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

CHAPTER 6

トラブルシューティングトレース設定値の設定 6-1

関連項目	6-2
------	-----

PART 5

モニタリングツールの設定

CHAPTER 7

Real-Time Monitoring の設定 7-1

Real-Time Monitoring Tool ( RTMT ) のインストール	7-2
--	-----

RTMT のアップグレード	7-3
RTMT のアンインストール	7-4
RTMT の使用	7-5
電子メール通知の設定	7-7
構成プロファイルの操作	7-8
デフォルトの構成プロファイルの使用	7-8
構成プロファイルの追加	7-8
プロファイルの復元	7-9
構成プロファイルの削除	7-9
事前定義オブジェクトの操作	7-10
事前定義オブジェクトの表示とモニタリング	7-11
デバイスの操作	7-13
電話機情報の表示	7-13
デバイスのプロパティの表示	7-13
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	7-13
カテゴリの操作	7-15
カテゴリの追加	7-15
カテゴリ名の変更	7-15
カテゴリの削除	7-16
参考情報	7-16
関連項目	7-16

## CHAPTER 8

<b>RTMT でのアラート設定</b>	<b>8-1</b>
アラートの操作	8-2
アラート プロパティの設定	8-4
Cisco Unified Presence Server ノードまたはクラスタ上のアラートの一時停止	8-7
アラート通知用電子メールの設定	8-8
アラート アクションの設定	8-8
関連項目	8-8

## CHAPTER 9

<b>パフォーマンス モニタリングの設定と使用</b>	<b>9-1</b>
パフォーマンス カウンタの表示	9-2
RTMT Performance Monitoring ペインからのカウンタの削除	9-4
カウンタ インスタンスの追加	9-5
カウンタのアラート通知の設定	9-6
カウンタの詳細表示	9-9
カウンタの説明の表示	9-10
サンプル データの設定	9-11

カウンタ データの表示	9-12
Perfmon カウンタによるローカルでのデータのログ記録	9-13
カウンタ ログの開始	9-13
カウンタ ログの停止	9-13
Perfmon Log Viewer でのログ ファイルの表示	9-14
拡大および縮小	9-16
関連項目	9-16

CHAPTER 10

<b>RTMT のトレース収集とログ集中管理</b>	10-1
証明書のインポート	10-2
RTMT での Trace & Log Central のオプションの表示	10-3
トレースの収集	10-4
Query Wizard の使用	10-7
トレース収集のスケジュール	10-11
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	10-14
クラッシュ ダンプの収集	10-15
Local Browse の使用	10-17
Remote Browse の使用	10-18
Q931 Translator の使用	10-20
QRT レポート情報の表示	10-20
Real Time Trace の使用	10-21
View Real Time Data	10-21
Monitor User Event	10-22
RTMT のトレース設定の更新	10-25
関連項目	10-25

CHAPTER 11

<b>RTMT SysLog Viewer の使用</b>	11-1
関連項目	11-2

CHAPTER 12

<b>プラグインの使用</b>	12-1
関連項目	12-2

CHAPTER 13

<b>Log Partition Monitoring の設定</b>	13-1
Log Partition Monitoring の有効化	13-1
Log Partition Monitoring の設定	13-2
関連項目	13-2

---

<b>PART 6</b>	<b>レポート ツールの設定</b>	
<b>CHAPTER 14</b>	<b>Serviceability Reports Archive の設定</b>	<b>14-1</b>
	関連項目	14-2
<b>PART 7</b>	<b>SNMP の設定</b>	
<b>CHAPTER 15</b>	<b>SNMP V1/V2c の設定</b>	<b>15-1</b>
	SNMP コミュニティ ストリングの設定	15-2
	SNMP 通知先	15-3
	SNMP 通知先の設定 (V1/V2c)	15-4
	関連項目	15-5
<b>CHAPTER 16</b>	<b>SNMP V3 の設定</b>	<b>16-1</b>
	SNMP ユーザの設定	16-2
	SNMP 通知先の設定 (V3)	16-4
	関連項目	16-5
<b>CHAPTER 17</b>	<b>MIB2 システム グループの設定</b>	<b>17-1</b>
	関連項目	17-2
<b>INDEX</b>	<b>索引</b>	







# 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 \(P.ix\)](#)
- [対象読者 \(P.ix\)](#)
- [マニュアルの構成 \(P.x\)](#)
- [関連マニュアル \(P.xi\)](#)
- [表記法 \(P.xi\)](#)
- [技術情報の入手方法 \(P.xii\)](#)
- [シスコ製品のセキュリティの概要 \(P.xiv\)](#)
- [Product Alerts および Field Notices \(P.xv\)](#)
- [テクニカル サポート \(P.xvi\)](#)
- [その他の資料および情報の入手方法 \(P.xviii\)](#)

## 目的

『Cisco Unified Presence Server サービスアビリティ アドミニストレーション ガイド』は、Cisco Unified Presence Server 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 Presence Server サービスアビリティ アドミニストレーション ガイド』は、Cisco Unified Presence Server 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 Server 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 Server 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 Server 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 Server 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 Server 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 Server 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 Server 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](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わせは、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

シスコの製品マニュアルやその他の資料は、Cisco.com でご利用いただけます。ここでは、シスコが提供する製品マニュアルについて説明します。

### Cisco.com

次の URL から、シスコ製品の最新資料を入手できます。

<http://www.cisco.com/techsupport>

シスコの Web サイトには、次の URL からアクセスしてください。

<http://www.cisco.com>

シスコの Web サイトの各国語版には、次の URL からアクセスしてください。

[http://www.cisco.com/public/countries\\_languages.shtml](http://www.cisco.com/public/countries_languages.shtml)

シスコ製品の最新資料の日本語版は、次の URL からアクセスしてください。

<http://www.cisco.com/jp>

## Product Documentation DVD (英語版)

Product Documentation DVD は、技術情報を包含する製品マニュアルをポータブルなメディアに格納したライブラリです。この DVD を使用することにより、シスコ製の各ハードウェアやソフトウェアのインストール、コンフィギュレーション、およびコマンドに関するマニュアルにアクセスすることができます。また、この DVD を使用すると、次の URL のシスコの Web サイトに掲載されている HTML マニュアルおよび PDF ファイルにアクセスすることができます。

<http://www.cisco.com/univercd/home/home.htm>

Product Documentation DVD は、定期的に作成されリリースされます。DVD は、1 回単位で入手することも、または定期購読することもできます。Cisco.com 登録ユーザの場合、Product Documentation Store の Cisco Marketplace から Product Documentation DVD ( Product Number DOC-DOCDVD= または DOC-DOCDVD=SUB ) を発注できます。次の URL にアクセスしてください。

<http://www.cisco.com/go/marketplace/docstore>

## マニュアルの発注方法 (英語版)

Cisco Marketplace にアクセスするには、Cisco.com ユーザ登録が必要です。登録ユーザの場合、Product Documentation Store からシスコ製品の英文マニュアルを発注できるようになっています。次の URL にアクセスしてください。

<http://www.cisco.com/go/marketplace/docstore>

ユーザ ID またはパスワードを取得していない場合は、次の URL にアクセスして登録手続きを行ってください。

<http://tools.cisco.com/RPF/register/register.do>

## シスコシステムズマニュアルセンター

シスコシステムズマニュアルセンターでは、シスコ製品の日本語マニュアルの最新版を PDF 形式で公開しています。また、日本語マニュアル、および日本語マニュアル CD-ROM もオンラインで発注可能です。ご希望の方は、次の URL にアクセスしてください。

<http://www2.hipri.com/cisco/>

また、シスコシステムズマニュアルセンターでは、日本語マニュアル中の誤記、誤植に関するコメントをお受けしています。次の URL の「製品マニュアル内容不良報告」をクリックすると、コメント入力画面が表示されます。

<http://www2.hipri.com/cisco/>

なお、技術内容に関するお問い合わせは、この Web サイトではお受けできませんので、製品を購入された各代理店へお問い合わせください。

## 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](http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html)

このサイトは、次の目的に利用できます。

- シスコ製品のセキュリティ脆弱性を報告する。
- シスコ製品に伴うセキュリティ事象についてサポートを受ける。
- シスコからセキュリティ情報を受け取るための登録をする。

シスコ製品に関するセキュリティ勧告、セキュリティ上の注意事項、およびセキュリティ対策の最新のリストには、次の URL からアクセスできます。

<http://www.cisco.com/go/psirt>

セキュリティ勧告、セキュリティ上の注意事項、およびセキュリティ対策がアップデートされた時点でリアルタイムに確認する場合は、次の URL から Product Security Incident Response Team Really Simple Syndication ( PSIRT RSS ) フィードに登録してください。PSIRT RSS フィードへの登録方法については、次の URL を参照してください。

[http://www.cisco.com/en/US/products/products\\_psirt\\_rss\\_feed.html](http://www.cisco.com/en/US/products/products_psirt_rss_feed.html)

## シスコ製品のセキュリティ問題の報告

シスコでは、セキュアな製品を提供すべく全力を尽くしています。製品のリリース前には内部でテストを行い、すべての脆弱性を早急に修正するよう努力しています。万一、シスコ製品に脆弱性が見つかった場合は、PSIRT にご連絡ください。

- 緊急の場合のみ: [security-alert@cisco.com](mailto:security-alert@cisco.com) ( 英語のみ )  
緊急とは、システムがアクティブな攻撃を受けている場合、または至急の対応を要する重大なセキュリティ上の脆弱性が報告されている場合を指します。これに該当しない場合はすべて、緊急でないと思なされます。
- 緊急でない場合: [psirt@cisco.com](mailto:psirt@cisco.com) ( 英語のみ )

緊急の場合は、電話で PSIRT に連絡することもできます。

- 1 877 228-7302 ( 英語のみ )
- 1 408 525-6532 ( 英語のみ )

**ヒント**

シスコに機密情報をお送りいただく際には、PGP (Pretty Good Privacy) または GnuPG などの互換製品を使用して、暗号化することをお勧めします。PSIRT は、PGP バージョン 2.x から 9.x と互換性のある暗号化情報に対応しています。

無効になった暗号鍵、または有効期限が切れた暗号鍵は絶対に使用しないでください。PSIRT に連絡する際に使用する正しい公開鍵には、Security Vulnerability Policy ページの Contact Summary セクションからリンクできます。次の URL にアクセスしてください。

[http://www.cisco.com/en/US/products/products\\_security\\_vulnerability\\_policy.html](http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html)

このページ上のリンクからは、現在使用されている最新の PGP 鍵の ID にアクセスできます。

PGP を持っていない、または使用していない場合は、機密情報を送信する前に PSIRT に問い合わせ、データ暗号化方法を確認してください。

## Product Alerts および Field Notices

シスコ製品に対する変更やアップデートは、Cisco Product Alerts および Cisco Field Notices で発表されます。Cisco.com のプロダクトアラートツールを使用すると、アナウンスを受け取ることができます。このツールを使用して、プロファイルを作成し、情報を受け取る製品を選択できます。

プロダクトアラートツールにアクセスするには、Cisco.com の登録ユーザとなる必要があります。登録ユーザは、次の URL でこのツールを使用できます。

<http://tools.cisco.com/Support/PAT/do/ViewMyProfiles.do?local=en>

Cisco.com にユーザ登録するには、次の URL にアクセスしてください。

<http://tools.cisco.com/RPF/register/register.do>

## テクニカル サポート

Cisco Technical Support では、24 時間テクニカル サポートを提供しています。Cisco.com の Cisco Support Web サイトでは、多数のサポート リソースをオンラインで提供しています。また、シスコと正式なサービス契約を交わしているお客様には、Cisco Technical Assistance Center (TAC) のエンジニアが電話でのサポートにも対応します。シスコと正式なサービス契約を交わしていない場合は、代理店にお問い合わせください。

## Cisco Support Web サイト

Cisco Support Web サイトでは、シスコ製品やシスコの技術に関するトラブルシューティングにお役立ていただけるように、オンラインでマニュアルやツールを提供しています。この Web サイトは、24 時間、いつでも利用可能です。URL は次のとおりです。

<http://www.cisco.com/en/US/support/index.html>

Cisco Support Web サイトのツールにアクセスするには、Cisco.com のユーザ ID とパスワードが必要です。サービス契約が有効で、ユーザ ID またはパスワードを取得していない場合は、次の URL にアクセスして登録手続きを行ってください。

<http://tools.cisco.com/RPF/register/register.do>



(注)

オンラインまたは電話でサービス リクエストを発行する前に、**Cisco Product Identification Tool** を使用して製品のシリアル番号を確認してください。Cisco Support Web サイトでこのツールを使用するには、**Get Tools & Resources** リンクをクリックし、**All Tools (A-Z)** タブをクリックした後、アルファベット順のリストから **Cisco Product Identification Tool** を選択します。このツールには、3 つの検索オプションがあります。製品 ID またはモデル名による検索、ツリー表示による検索、show コマンド出力のコピー アンド ペーストによる特定製品の検索です。検索結果では、製品が図示され、シリアル番号ラベルの位置が強調表示されます。ご使用の製品でシリアル番号ラベルを確認し、その情報を記録してからサービス コールをかけてください。



ヒント

### Cisco.com での表示および検索

ブラウザが Web ページをリフレッシュしていないと思われる場合は、Ctrl キーを押したまま F5 を押すことで強制的にブラウザに Web ページを更新させます。

技術情報を検索する場合は、Cisco.com の Web サイト全体ではなく、技術マニュアルに検索対象を絞り込みます。Cisco.com のホームページで Search ボックスを使用した後、検索結果ページの Search ボックスのとなりにある **Advanced Search** リンクをクリックし、**Technical Support & Documentation** オプション ボタンをクリックしてください。

Cisco.com の Web サイトまたは特定の技術マニュアルに関するフィードバックを送るには、Cisco.com のすべての Web ページの下部にある **Contacts & Feedback** をクリックします。



## Japan TAC Web サイト

Japan TAC Web サイトでは、利用頻度の高い TAC Web サイト (<http://www.cisco.com/tac>) のドキュメントを日本語で提供しています。Japan TAC Web サイトには、次の URL からアクセスしてください。

<http://www.cisco.com/jp/go/tac>

サポート契約を結んでいない方は、「ゲスト」としてご登録いただくだけで、Japan TAC Web サイトのドキュメントにアクセスできます。Japan TAC Web サイトにアクセスするには、Cisco.com のログイン ID とパスワードが必要です。ログイン ID とパスワードを取得していない場合は、次の URL にアクセスして登録手続きを行ってください。

<http://www.cisco.com/jp/register>

## サービス リクエストの発行

オンラインの TAC Service Request Tool を使用すると、S3 と S4 のサービス リクエストを短時間でオープンできます (S3: ネットワークに軽微な障害が発生した、S4: 製品情報が必要である)。状況を入力すると、その状況を解決するための推奨手段が検索されます。これらの推奨手段で問題を解決できない場合は、シスコのエンジニアが対応します。TAC Service Request Tool には、次の URL からアクセスできます。

<http://www.cisco.com/techsupport/servicerequest>

S1 または S2 のサービス リクエストの場合、またはインターネットにアクセスできない場合は、Cisco TAC に電話でお問い合わせください (S1: ネットワークがダウンした、S2: ネットワークの機能が著しく低下した)。S1 および S2 のサービス リクエストには、シスコのエンジニアがすぐに割り当てられ、業務を円滑に継続できるようサポートします。

Cisco TAC の連絡先については、次の URL を参照してください。

<http://www.cisco.com/techsupport/contacts>

## サービス リクエストのシビラティの定義

シスコでは、報告されるサービス リクエストを標準化するために、シビラティを定義しています。

シビラティ 1 (S1): 既存のネットワークが「ダウン」した状態か、業務に致命的な損害が発生した場合。お客様およびシスコが、24 時間体制でこの問題を解決する必要があると判断した場合。

シビラティ 2 (S2): 既存のネットワーク動作が著しく低下したか、シスコ製品が十分に機能しないため、業務に重大な影響を及ぼした場合。お客様およびシスコが、通常の業務中の全時間を費やして、この問題を解決する必要があると判断した場合。

シビラティ 3 (S3): ネットワークの動作パフォーマンスが低下しているが、ほとんどの業務運用は継続できる場合。お客様およびシスコが、業務時間中にサービスを十分なレベルにまで復旧させる必要があると判断した場合。

シビラティ 4 (S4): シスコ製品の機能、インストレーション、コンフィギュレーションについて、情報または支援が必要な場合。業務の運用には、ほとんど影響がありません。

## その他の資料および情報の入手方法

シスコの製品、テクノロジー、およびネットワーク ソリューションに関する情報について、さまざまな資料をオンラインおよび印刷物で入手できます。

- Cisco Online Subscription Center は、さまざまなシスコのメールマガジンや他のコミュニケーションを申し込むことができる Web サイトです。プロフィールを作成して、受け取る製品を選択できます。購入を希望される場合は、次の URL にアクセスしてください。  
<http://www.cisco.com/offer/subscribe>
- 『Cisco Product Quick Reference Guide』は手軽でコンパクトな参照ツールです。チャネルパートナー経由で販売される多くのシスコ製品に関する簡単な製品概要、主要な機能、サンプル部品番号、および簡単な技術仕様を記載しています。年 2 回の更新の際には、シスコの最新情報が収録されます。『Cisco Product Quick Reference Guide』の注文方法および詳細については、次の URL にアクセスしてください。  
<http://www.cisco.com/go/guide>
- Cisco Marketplace では、シスコの書籍やリファレンス ガイド、マニュアル、ロゴ製品を数多く提供しています。購入を希望される場合は、次の URL にアクセスしてください。  
<http://www.cisco.com/go/marketplace/>
- Cisco Press では、ネットワーク全般、トレーニング、および認定資格に関する出版物を幅広く発行しています。これらの出版物は、初級者にも上級者にも役立ちます。Cisco Press の最新の出版情報などについては、次の URL からアクセスしてください。  
<http://www.ciscopress.com>
- 『Internet Protocol Journal』は、インターネットおよびイントラネットの設計、開発、運用を担当するエンジニア向けに、シスコが発行する季刊誌です。『Internet Protocol Journal』には、次の URL からアクセスしてください。  
<http://www.cisco.com/ipj>
- シスコが提供するネットワーク製品、および各種のカスタマー サポート サービスは、次の URL から入手できます。  
<http://www.cisco.com/en/US/products/index.html>
- Networking Professionals Connection は対話形式の Web サイトです。このサイトでは、ネットワーク製品やテクノロジーに関する質問、提案、および情報をネットワーク担当者がシスコの専門家や他のネットワーク担当者と共に共有できます。次の URL にアクセスしてディスカッションに参加してください。  
<http://www.cisco.com/discuss/networking>
- 「What's New in Cisco Documentation」は、シスコ製品の最新のマニュアル リリースに関する情報を提供するオンライン出版物です。このオンライン出版物は毎月更新され、製品カテゴリ別に編成されているため、製品のマニュアルを簡単に検索できます。次の URL で「What's New in Cisco Documentation」の最新リリースを見ることができます。  
<http://www.cisco.com/univercd/cc/td/doc/abtnicd/136957.htm>
- シスコは、国際的なレベルのネットワーク関連トレーニングを実施しています。最新情報については、次の URL からアクセスしてください。  
<http://www.cisco.com/en/US/learning/index.html>



## **PART 1**

# **Cisco Unified Presence Server Serviceability**







## 概要

この章は、次の項で構成されています。

- [Cisco Unified Presence Server Serviceability の概要 \( P.1-1 \)](#)
- [Cisco Unified Presence Server Serviceability へのアクセス \( P.1-2 \)](#)
- [Hypertext Transfer Protocol over Secure Sockets Layer \( HTTPS \) の使用 \( P.1-3 \)](#)
- [Cisco Unified Presence Server Serviceability のインターフェイスの使用 \( P.1-6 \)](#)
- [アクセシビリティ機能 \( P.1-8 \)](#)
- [参考情報 \( P.1-8 \)](#)

## Cisco Unified Presence Server Serviceability の概要

Cisco Unified Presence Server 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 Server 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 Server 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 Server 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 Server 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 Server 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 Server 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 Server Serviceability へのアクセス

Cisco Unified Presence Server 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 Server Serviceability が動作している Cisco Unified Presence Server 1.0 サーバを参照します。



**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 Server 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 Server Administration 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、ユーザ名に CCMAdministrator と入力し、パスワードには、インストール中に指定したアプリケーション ユーザパスワードを入力します。



**ヒント** Standard CCMUsers ロールが割り当てられたユーザはすべて、Cisco Unified Presence Server Serviceability にアクセスできます。このロールをユーザに割り当てる方法の詳細については、『Cisco Unified Presence Server 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 Server 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 Presence Server のサービスアビリティ] を選択します。

Cisco Unified Presence Server Serviceability が表示されます。



**ヒント** 設定の途中で Cisco Unified Presence Server Serviceability 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。

- [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 \(Internet Explorer の場合\) \(P.1-4\)](#)

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 Server 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 Server 1.0 のインストールまたはアップグレード後に、Cisco Unified Presence Server の管理ページまたはその他の Cisco Unified Presence Server 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、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 Server 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 Server Serviceability のインターフェイスの使用

Cisco Unified Presence Server 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 Server Serviceability で **Help > This page** の順に選択します。
- このリリースの Cisco Unified Presence Server 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 Server 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 Server 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** をクリックします。
- Cisco Unified Presence Server 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 Server 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 Server Serviceability のアイコン


アイコン	目的
	新しい設定を追加します。
	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。

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

アイコン	目的
	選択したサービスを再起動します。
	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 Server 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 Server 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。
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 Server 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







## 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 \(P.2-2\)](#)
- [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 \(P.2-3\)](#)
- [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 \(P.2-4\)](#)

## 機能サービスのアクティブ化と非アクティブ化

Cisco Unified Presence Server 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 Server 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 Server Serviceability で Cisco Unified Presence Server 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 Server 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 Server 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 Server のサービスを開始、停止、または再起動すると、その Cisco Presence Server 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 Server のサービスにフェールオーバーされます。別の Cisco Presence Server 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 Server のサービスを開始、停止、または再起動すると、その Cisco Unified Presence Server 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 Server 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。

## ■ 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

- 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 Server 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







## アラームの設定

Cisco Unified Presence Server 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 Server 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 Server 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 Server 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 \(P.3-2\)](#)
- [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 \(P.3-4\)](#)

## 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 Server 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ます。

**ステップ 3** 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。

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 4** 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 5** Alarm Event Level ドロップダウン リスト ボックスの下向き矢印をクリックします。

イベント レベルを含むリストが表示されます。

**ステップ 6** 表 3-2 の説明に従って、使用するアラーム イベント レベルをクリックします。

**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	<p>SysLog Viewer。Cisco Unified Presence Server 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。</p> <p>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。</p>
Enable Alarm for Remote Syslogs	<p>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 Server は Syslog メッセージを送信しません。</p> <p> (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。</p>
Enable Alarm for SDI Trace	<p>SDI トレース ライブラリ。</p> <p>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。</p> <p>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。</p>

## 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 \(P.3-4\)](#)





## 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atalog記述 \(P.4-3\)](#)

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 Server 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 Server 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atalog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 Catalog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atalog記述

表 4-1 では、アラーム定義のカatalog記述について説明します。

表 4-1 アラーム定義カatalog

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   <b>(注)</b> 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atalog記述 \(P.4-3\)](#)





## PART 4

### トレースの設定







## トレースの設定

Trace Configuration ウィンドウでは、Cisco Unified Presence Server 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 にお問い合わせください。

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 \(P.5-2\)](#)
- [デバッグトレース レベルの設定値 \(P.5-4\)](#)
- [トレース出力設定値の説明とデフォルト値 \(P.5-5\)](#)

## トレースパラメータの設定

この項では、Cisco Presence Server 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ます。

**ステップ 3** 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 9](#)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 4** クラスタ内のすべての Cisco Unified Presence Server 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 5** Trace On チェックボックスをオンにします。

**ステップ 6** 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 7** 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 8** 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 UPS 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 UPS 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 9** 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 10** 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 UPS 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。



### 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	<p>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。</p> <p> (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。</p>
Debug	<p>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。</p> <p>すべてのログ記録をオンにするトレース レベルです。</p>
Detailed	<p>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。</p> <p> (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。</p>
Entry/Exit	<p>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 Server は使用しません)。</p>
Error	<p>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。</p>
Fatal	<p>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。</p>
Info	<p>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。</p>
Significant	<p>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。</p>
Special	<p>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。</p>
State Transition	<p>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。</p>
Warn	<p>潜在的に有害な状況をトレースします。</p>

### 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 Server 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 \(P.5-4\)](#)





# 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 Server 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** 次のいずれかの操作を実行します。

- トラブルシューティング トレースを設定するには、各ノードのサービス リストで、サービスのチェックボックスをオンにします。特定のノードにおいて、すべてのサービスをチェックにする場合は、そのノードの下にある **Check all Services for a Node** チェックボックスをオンにします。すべてのノードのすべてのサービスをチェックする場合は、サービス リストで **Check all Services for a Node** チェックボックスをオンにします。

次に、**Apply Troubleshooting Traces** ボタンをクリックします。



(注) Cisco Unified Presence Server 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。

- クラスタ内のサービスの、元のトレース設定値を復元するには、**Reset Troubleshooting Traces** をクリックします。



(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**









## Real-Time Monitoring の設定

---

この章では、Cisco Unified Presence Server Real-Time Monitoring Tool (RTMT) を設定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。



(注)

---

現在のバージョンの Cisco Real-Time Monitoring Tool で使用可能なオプションの一部は、Cisco Unified Presence Server Release 1.0 (3) に適用されません。

---

- [Real-Time Monitoring Tool \(RTMT\) のインストール \(P.7-2\)](#)
- [RTMT のアップグレード \(P.7-3\)](#)
- [RTMT のアンインストール \(P.7-4\)](#)
- [RTMT の使用 \(P.7-5\)](#)
- [電子メール通知の設定 \(P.7-7\)](#)
- [構成プロファイルの操作 \(P.7-8\)](#)
- [事前定義オブジェクトの操作 \(P.7-10\)](#)
- [デバイスの操作 \(P.7-13\)](#)
- [参考情報 \(P.7-16\)](#)



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.7-16](#) 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 Server 1.0 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 Server 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** Cisco Unified Presence Server Real-Time Monitoring Tool 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。
- 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.7-16 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 Server 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 Server 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 Server 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。
- ステップ 6** [ Real Time Monitoring Tool の InstallShield ウィザードへようこそ ] 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.7-16 の「[関連項目](#)」を参照してください。

## RTMT のアンインストール

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.7-16 の「[関連項目](#)」を参照してください。

## RTMT の使用

### 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 Server 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 Tool 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 Server 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。

**ステップ 9** RTMT で実行できる操作については、次のリストを参照してください。

- 電子メール アラートのためのメール サーバを設定する場合は、P.7-7 の「電子メール通知の設定」を参照してください。
- 構成プロファイルを作成する場合は、P.7-8 の「構成プロファイルの追加」を参照してください。
- 事前定義オブジェクトをモニタする場合は、P.7-10 の「事前定義オブジェクトの操作」を参照してください。

- デバイスを操作する場合は、P.7-13 の「[デバイスの操作](#)」を参照してください。
- アラートを操作する場合は、P.8-1 の「[RTMT でのアラート設定](#)」を参照してください。
- パフォーマンス モニタリング オブジェクトを操作する場合は、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。
- トレースを収集して表示する場合は、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。
- SysLog Viewer を使用する場合は、P.11-1 の「[RTMT SysLog Viewer の使用](#)」を参照してください。
- RTMT のトレース設定値を設定する場合は、**Edit > Trace Setting** の順に選択します。適切なオプション ボタンをクリックします。
- ウィンドウの左側に表示される Quick Launch Channel ペインを非表示にするには、**Edit > Hide Quick Launch Channel** の順に選択します。  
一度非表示にした Quick Launch Channel を表示するには、**Edit > Hide Quick Launch Channel** の順に選択します。
- 1 つのモニタリング ウィンドウを閉じるには、**Window > Close** の順に選択します。表示されているすべてのモニタリング ウィンドウを閉じるには、**Window > Close All Windows** の順に選択します。
- RTMT ウィンドウから Cisco Unified Presence Server の管理ページまたは Cisco Unified Presence Server Serviceability にアクセスするには、**Application > CCMAdmin webpage** (または **CCM Serviceability webpage**) の順に選択します。
- RTMT から Serviceability Report Archive オプションにアクセスするには、**System > Report Archive** の順に選択します。[セキュリティの警告] ウィンドウが表示されたら、[はい] をクリックします。サーバの管理ユーザ名とパスワードを入力し、**OK** をクリックします。
- インストールされている RTMT のバージョンを確認するには、**Help > About** の順に選択します。バージョン情報がウィンドウに表示されます。情報を確認したら、**OK** をクリックします。
- RTMT のマニュアルにアクセスするには、**Help > Help Topics** (または **For this Window**) の順に選択します。RTMT または Cisco Unified Presence Server Serviceability の詳細については、『*Cisco Unified CallManager Serviceability システムガイド*』および『*Cisco Unified Presence Server サービスアビリティ アドミニストレーションガイド*』を参照してください。
- JVM 情報をモニタするには、**System > JVM Information** の順にクリックします。JAVA ヒープメモリの使用状況がウィンドウに表示されます。**OK** をクリックします。
- RTMT からログアウトするには、**System > Log Off** の順に選択します。この操作を実行すると、現在のユーザがログオフされ、Real-Time Monitoring Tool Login ウィンドウが表示されます。
- アプリケーションを終了するには、**System > Exit** の順に選択します。この操作を実行すると、アプリケーションが終了します。

### 追加情報

P.7-16 の「[関連項目](#)」を参照してください。

## 電子メール通知の設定

電子メール通知を設定するには、次の手順を実行します。

### 手順

- 
- ステップ 1** 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 2** 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 3** OK をクリックします。
- 

### 追加情報

P.7-16 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 \(P.7-8\)](#)
- [構成プロファイルの追加 \(P.7-8\)](#)
- [プロファイルの復元 \(P.7-9\)](#)
- [構成プロファイルの削除 \(P.7-9\)](#)

### 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.7-8 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.7-16 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.7-16 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.7-16 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.7-16 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 Server 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 \(P.7-11\)](#)
- [デバイスの操作 \(P.7-13\)](#)

## 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。

### 手順

**ステップ 1** カテゴリを表示またはモニタするには、次のいずれかの操作を実行します。

- Quick Launch Channel で **View** タブをクリックします。次に、Summary、Server、Call Process 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 にあるオプションの一部は、Cisco Unified Presence Server に適用されません。

- 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 カテゴリのメニューパス

カテゴリ	メニューパス	表示されるデータ
Summary	Monitor > Summary	<p><b>(注)</b> 現在のバージョンの RTMT にあるオプションの一部は、Cisco Unified Presence Server に適用されません。</p> <p>メモリと CPU の使用状況を表示します。</p>
Server	Monitor > Server > CPU and Memory (または Process、Disk Usage、Critical Services)	<ul style="list-style-type: none"> <li>CPU and Memory：メモリと CPU の使用状況を表示します。</li> <li>Process：プロセス名、プロセス ID (PID) に加え、プロセス、常駐メモリ、共有メモリ、および Nice (レベル) によって使用されている CPU とメモリの割合を表示します。</li> <li>Disk Usage：各ホストの最大パーティションで使用されているディスク容量の割合を表示します。</li> <li>Critical Services：特定のサーバのサービスを表示します。</li> </ul>
Service	Monitor > Service > Cisco TFTP (または Heartbeat、Database Summary)	<ul style="list-style-type: none"> <li>Cisco TFTP：クラスタ内の各 Cisco Unified Presence Server サーバの Cisco TFTP ステータスを表示します。TFTP 要求合計、検出された TFTP 要求合計、中止された TFTP 要求合計などの項目が含まれます。</li> <li>Heartbeat：Cisco Unified Presence Server、Cisco TFTP、Cisco Presence Server Attendant Console サービスのハートビート情報を表示します。</li> <li>Database Summary：Cisco Unified Presence Server 上のデータベースに関する要約情報を表示します。データベースのキューに登録された接続要求、メモリのキューに登録された接続要求、接続されたクライアントの合計数、およびキュー登録中にリセットされたデバイスの数などの項目が含まれます。</li> </ul>
Performance	Performance > Open Performance	<p>perfmon カウンタを表示します。</p> <p>perfmon カウンタの使用方法の詳細については、<a href="#">P.9-1</a> 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。</p>

**ステップ 2** 一部のカテゴリでは、特定のサーバやデバイス タイプを選択してモニタできます。特定のサーバやデバイス タイプを選択してモニタするには、表示されたペインで次のいずれかの操作を実行します。

- CPU and Memory Usage ペイン：特定のサーバの CPU や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。
- Disk Usage ペイン：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 ボックスの Disk Usage からサーバを選択します。
- Critical Services ペイン：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 ボックスの Critical Services からサーバを選択します。



**(注)** 現在のバージョンの RTMT にあるオプションの一部は、Cisco Unified Presence Server に適用されません。

#### 追加情報

P.7-16 の「[関連項目](#)」を参照してください。

## デバイスの操作



(注) 現在のバージョンの RTMT にある Device のオプションは、Cisco Unified Presence Server に適用されません。

## 電話機情報の表示



(注) 現在のバージョンの RTMT にある Phone Information のオプションは、Cisco Unified Presence Server に適用されません。

## デバイスのプロパティの表示



(注) 現在のバージョンの RTMT にある Device Properties のオプションは、Cisco Unified Presence Server に適用されません。

## 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



(注) 現在のバージョンの RTMT にあるオプションの一部は、Cisco Unified Presence Server に適用されません。

Cisco Unified Presence Server 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 Server 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。

## ■ デバイスの操作

**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.7-16 の「[関連項目](#)」を参照してください。

## カテゴリの操作



(注) 現在のバージョンの RTMT にあるオプションの一部は、Cisco Unified Presence Server に適用されません。

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 UPS 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** Performance Monitoring または Devices ツリー階層を表示します。

**ステップ 2** Edit > Add 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.7-16 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.7-16 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.7-16 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.7-16 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 \(P.7-15\)](#)
- [カテゴリ名の変更 \(P.7-15\)](#)
- [カテゴリの削除 \(P.7-16\)](#)
- [パフォーマンス モニタリングの設定と使用 \(P.9-1\)](#)
- [デバイスの操作 \(P.7-13\)](#)
- [デバイスのプロパティの表示 \(P.7-13\)](#)
- [電話機情報の表示 \(P.7-13\)](#)
- [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 \(P.7-13\)](#)
- [デフォルトの構成プロファイルの使用 \(P.7-8\)](#)
- [プロファイルの復元 \(P.7-9\)](#)
- [デフォルトの構成プロファイルの使用 \(P.7-8\)](#)
- [構成プロファイルの削除 \(P.7-9\)](#)
- [構成プロファイルの追加 \(P.7-8\)](#)
- [構成プロファイルの操作 \(P.7-8\)](#)
- [事前定義オブジェクトの操作 \(P.7-10\)](#)
- [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 の使用 \(P.7-5\)](#)





## RTMT でのアラート設定

---

RTMT には、あらかじめ設定されているアラートとユーザ定義のアラートという 2 つの種類のアラートがあります。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 \(P.8-2\)](#)
- [アラート プロパティの設定 \(P.8-4\)](#)
- [Cisco Unified Presence Server 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 \(P.8-8\)](#)

## 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、Tools タブ、Alert タブの順にクリックし、Alert Central アイコンをクリックします。
- Tools > Alert > Alert Central の順に選択します。

RTMT が Cisco Unified Presence Server クラスタ内で生成したアラートの状況と履歴を示す Alert Central モニタリングウィンドウが表示されます。

**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 Server 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 Server 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、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、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、**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。
- Tools > Alert > Set Alert/Properties の順に選択します。



**(注)** Cisco Unified Presence Server 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、Config Alert Action 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 Server 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 Server 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ある場合があります。たとえば、Cisco Unified Presence Server 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** 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 Server 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** 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 Server 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)





# パフォーマンス モニタリングの設定と使用

Cisco Unified Presence Server 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 \(P.9-2\)](#)
- [RTMT Performance Monitoring ペインからのカウンタの削除 \(P.9-4\)](#)
- [カウンタ インスタンスの追加 \(P.9-5\)](#)
- [カウンタのアラート通知の設定 \(P.9-6\)](#)
- [カウンタの詳細表示 \(P.9-9\)](#)
- [カウンタの説明の表示 \(P.9-10\)](#)
- [サンプル データの設定 \(P.9-11\)](#)
- [カウンタ データの表示 \(P.9-12\)](#)
- [Perfmon カウンタによるローカルでのデータのログ記録 \(P.9-13\)](#)
- [Perfmon Log Viewer でのログ ファイルの表示 \(P.9-14\)](#)

## パフォーマンス カウンタの表示

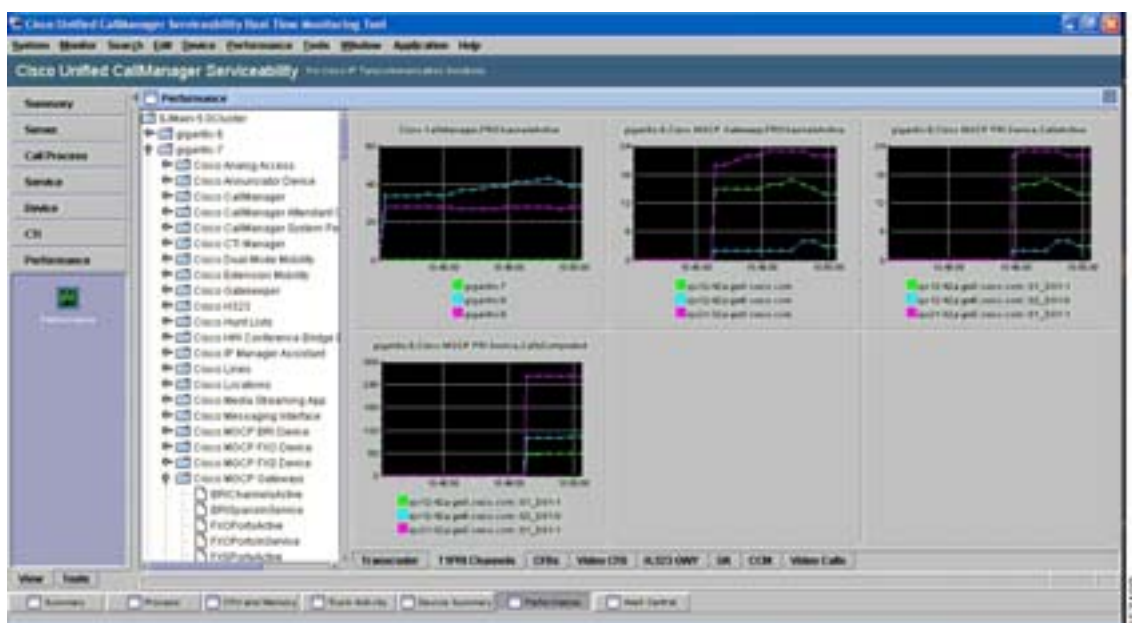
RTMT は、perfmon カウンタを図形式または表形式で表示します。図形式では、図 9-1 に示すように、線グラフを使用して perfmon カウンタ情報を表示します。作成したカテゴリ タブごとに、最大 6 つの図を RTMT Perfmon Monitoring ペインに表示できます。1 つの図には、最大 3 つのカウンタを表示できます。



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。

図 9-1 図形式のパフォーマンス カウンタ



デフォルトでは、RTMT は perfmon カウンタを図形式で表示します。図 9-2 に示すように、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。



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.9-16 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

カウンタがなくなってきたときは、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.9-16 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、**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.9-16 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カウンタを右クリックし、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 の各ペインの設定を行います。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
<b>Threshold ペイン</b>	
Trigger alert when following conditions met ( Over、 Under )	<p>チェックボックスをオンにし、適切な値を入力します。</p> <ul style="list-style-type: none"> <li>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。</li> <li>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。</li> </ul>
	<p> <b>ヒント</b> 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わせて使用します。</p>

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
<b>Value Calculated As</b> <b>ペイン</b>	
Absolute、Delta、% Delta	適切なオプション ボタンをクリックします。 <ul style="list-style-type: none"> <li>• 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。</li> <li>• 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。</li> <li>• % Delta: 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 を選択します。</li> </ul>
<b>Duration</b> <b>ペイン</b>	
Trigger alert only when value constantly...、Trigger alert immediately	<ul style="list-style-type: none"> <li>• 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。</li> <li>• 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。</li> </ul>
<b>Frequency</b> <b>ペイン</b>	
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。 <ul style="list-style-type: none"> <li>• 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。</li> <li>• 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。</li> </ul>
<b>Schedule</b> <b>ペイン</b>	
24-hours daily、start/stop	適切なオプション ボタンをクリックします。 <ul style="list-style-type: none"> <li>• 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。</li> <li>• 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。</li> </ul>

**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.9-16 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。**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.9-16 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、**Perfmon > 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.9-11](#) 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.9-16](#) 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.9-12 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、**Perfmon > 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	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 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.9-16 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.9-11 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.9-16 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.9-14 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.9-13 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 Server は、Cisco Unified Presence Server サーバに書き込まれているログの中からシステムの情報収集します。AMC および RISDC の perfmon ログは、Cisco Unified Presence Server 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 Server 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、**Performance** をクリックしてから **Performance Log Viewer** をクリックします。
- **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 \(P.9-4\)](#)
- [カウンタのアラート通知の設定 \(P.9-6\)](#)
- [カウンタの詳細表示 \(P.9-9\)](#)
- [カウンタの説明の表示 \(P.9-10\)](#)
- [サンプル データの設定 \(P.9-11\)](#)
- [カウンタ データの表示 \(P.9-12\)](#)
- [Perfmon カウンタによるローカルでのデータのログ記録 \(P.9-13\)](#)
- [Perfmon Log Viewer でのログ ファイルの表示 \(P.9-14\)](#)





# RTMT の トレース収集とログ集中管理

Cisco Unified Presence Server 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 Server 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 \(P.10-2\)](#)
- [RTMT での Trace & Log Central のオプションの表示 \(P.10-3\)](#)
- [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 \(P.10-11\)](#)
- [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 \(P.10-14\)](#)
- [クラッシュ ダンプの収集 \(P.10-15\)](#)
- [Local Browse の使用 \(P.10-17\)](#)

## ■ 証明書のインポート

- [Remote Browse の使用 \( P.10-18 \)](#)
- [Q931 Translator の使用 \( P.10-20 \)](#)
- [QRT レポート情報の表示 \( P.10-20 \)](#)
- [Real Time Trace の使用 \( P.10-21 \)](#)
- [RTMT のトレース設定の更新 \( P.10-25 \)](#)

## 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、**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 **Tools** タブをクリックし、**Trace** および **Trace & Log Central** アイコンをクリックします。
- **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.10-17 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.10-18 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.10-21 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 Presence Server 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 4** Next をクリックします。

Select System Logs 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 Server 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 Server Serviceability では、Cisco Unified Presence Server 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 Server Serviceability は、ユーザがログインしているバージョンの Cisco Unified Presence Server 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 Server (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 Server 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 Server にログインすると、Cisco Unified Presence Server 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 Server にログインすると、Cisco Unified Presence Server Serviceability は新しいバージョンの Cisco Unified Presence Server 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 Server Serviceability では、Windows プラットフォームで実行されている Cisco Unified Presence Server 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 Server 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.10-17 の「Local Browse の使用」](#)を参照してください。

#### 追加情報

[P.10-25 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 Cisco Presence Server 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 6** Next をクリックします。

**ステップ 7** Select System Logs 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** 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。

- **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 Server 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** Select Impact Level 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 Server 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.10-17 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.10-25 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 Presence Server 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。

## ■ トレース収集のスケジュール



(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 4** Next をクリックします。

System Logs 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せん。

**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。

## ■ 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

**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.10-25 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.10-25 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)** 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** Select Core Files タブで、該当するサーバの Core Files チェックボックスをオンにします。

**ステップ 4** Next をクリックします。

**ステップ 5** 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 Server 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 6** 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 Server Serviceability では、Cisco Unified Presence Server 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 Server Serviceability は、ユーザがログインしているバージョンの Cisco Unified Presence Server 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 Server (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。

## ■ クラッシュ ダンプの収集

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 Server 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 Server にログインすると、Cisco Unified Presence Server 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 Server にログインすると、Cisco Unified Presence Server Serviceability は新しいバージョンの Cisco Unified Presence Server 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 Server Serviceability では、Windows プラットフォームで実行されている Cisco Unified Presence Server のバージョンのログは保存されません。

**ステップ 7** 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 Server 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 8** 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 9** 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 10** **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.10-25 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 ファイルは、NotePad を使用して表示しないでください。

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するか、Finish 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。

### 追加情報

[P.10-25 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 8](#)に進みます。

**ステップ 4** 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 Logs 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 9**に進みます。

**ステップ 7** **ステップ 9**に進みます。

**ステップ 8** 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 9** **Finish** をクリックします。

**ステップ 10** 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 11** 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の名前が表示されたら、そのファイルをダブルクリックします。



**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、名前で見出し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 Server 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。

## ■ Q931 Translator の使用

- 特定のサービスまたはノードをリフレッシュするには、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リフレッシュするには、**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.10-17 の「Local Browse の使用」](#)を参照してください。

---

**追加情報**

[P.10-25 の「関連項目」](#)を参照してください。

## Q931 Translator の使用



---

**(注)**    Cisco Unified Presence Server 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 Server 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。以前のコンテンツ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 \( P.10-21 \)](#)
- [Monitor User Event \( P.10-22 \)](#)

### 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せん。

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.10-25 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 Server 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.10-25 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 Server Serviceability\jrtmt\log）に rtmt.log ファイルが保存されます。



Error オプション ボタンはデフォルト設定です。

### 追加情報

P.10-25 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 \( P.10-17 \)](#)
- [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 \( P.10-17 \)](#)
- [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



# 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。
- **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。
	 <p><b>ヒント</b> 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。</p>
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 \( P.7-1 \)](#)



## 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。
    - 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。



## 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（またはクラスター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 Server Serviceability で、**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ます。
  - ステップ 3** CCM Services の下で、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、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 システム ガイド』の「[Log Partition Monitoring](#)」
- 『Cisco Unified CallManager Serviceability システム ガイド』の「[RTMT でのアラート設定](#)」
- [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







# 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 Server 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







## 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 Presence Server 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。

- [SNMP コミュニティ スtring の設定 \(P.15-2\)](#)
- [SNMP 通知先の設定 \(V1/V2c\) \(P.15-4\)](#)



### 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。

---

## SNMP コミュニティ スtring の設定

SNMP エージェントはコミュニティ スtring を使用してセキュリティを提供するので、Cisco Unified Presence Server 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tring を設定する必要があります。Cisco Unified Presence Server システムへのアクセスを制限するには、コミュニティ スtring を変更します。コミュニティ スtring 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** Smp > V1/V2c Configuration > Community String を選択します。
- ステップ 2** Server ドロップダウン リスト ボックスから、コミュニティ スtring を設定する対象のサーバを選択します。
- ステップ 3** 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tring を追加する場合は、Add New ボタンをクリックし、[ステップ 4](#) に進みます。
  - 既存のコミュニティ スtring を変更する場合は、編集するコミュニティ スtring の名前をクリックし、[ステップ 5](#) に進みます。
  - コミュニティ スtring を削除する場合は、削除するコミュニティ スtring (複数可) の横にあるチェックボックスをオンにし、Delete Selected をクリックします。このコミュニティ スtring 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。削除を続行するには、OK をクリックし、[ステップ 9](#) に進みます。
- ステップ 4** Community String Name フィールドに、コミュニティ スtring 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 (\_) の任意の組み合わせで、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tring 名を選択してください。

- ステップ 5** Host IP Addresses Information グループ ボックスで、SNMP パケットの送信元のホストを指定します。次のいずれかのオプションをクリックします。
- すべてのホストから SNMP パケットを受信する場合は、Accept SNMP Packets from any host オプション ボタンをクリックします。
  - 指定したホストからのみ SNMP パケットを受信する場合は、Accept SNMP Packets only from these hosts 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、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。
- ステップ 6** 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tring 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tring 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tring 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tring 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tring 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。



(注) Cisco Unified Presence Server 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。

- ステップ 7** コミュニティ スtring をクラスタ内のすべてのサーバに適用するには、**Apply To All Nodes** チェックボックスをオンにします。
- ステップ 8** Insert をクリックして新しいコミュニティ スtring を保存するか、Save をクリックして既存のコミュニティ スtring への変更を保存します。
- ステップ 9** 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.2-1 の「サービスの管理」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tring がウィンドウに表示されます。

#### 追加情報

P.15-5 の「関連項目」を参照してください。

## SNMP 通知先

次のうち適切なトピックを参照してください。

- [SNMP 通知先の設定 \( V1/V2c \) \(P.15-4\)](#)
- [SNMP 通知先の設定 \( V3 \) \(P.16-4\)](#)

## SNMP 通知先の設定 (V1/V2c)

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** Smp > V1/V2c Configuration > Notification Destination 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、通知先を設定する対象のサーバを選択します。

**ステップ 3** 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 4](#) に進みます。
- 既存の SNMP 通知先を変更する場合は、編集する SNMP 通知先の名前をクリックし、[ステップ 5](#) に進みます。
- SNMP 通知先を削除する場合は、削除する SNMP 通知先 (複数可) の横にあるチェックボックスをオンにし、Delete Selected をクリックします。[ステップ 11](#) に進みます。

**ステップ 4** 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 Host 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、IP アドレスを入力します。

**ステップ 5** Port Number 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。

**ステップ 6** SNMP Version Information Group 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、[ステップ 8](#) に進みます。V2C を選択した場合は、[ステップ 7](#) に進みます。

**ステップ 7** 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。

**ステップ 8** 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名を選択します。



### ヒント

最下位の通知特権 (ReadWriteNotify または Notify Only) を持つコミュニティ スtring 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tring 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 ボタンをクリックしてコミュニティ スtring を作成します。コミュニティ スtring を作成する方法については、[P.15-2 の「SNMP コミュニティ スtring の設定」](#)を参照してください。

**ステップ 9** クラスタ内のすべてのノードに通知先を適用するには、Apply To All Nodes チェックボックスをオンにします。

**ステップ 10** 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 11** 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.2-1 の「サービスの管理」](#)を参照してください。

### 追加情報

[P.15-5 の「関連項目」](#)を参照してください。

## 関連項目

- [SNMP コミュニティ スtring の設定 \(P.15-2\)](#)
- [SNMP V3 の設定 \(P.16-1\)](#)
- [MIB2 システム グループ の設定 \(P.17-1\)](#)
- 『Cisco Unified CallManager Serviceability システム ガイド』の「SNMP」
- [SNMP 通知先 の設定 \(V1/V2c\) \(P.15-4\)](#)





## 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 Presence Server 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。

- [SNMP ユーザの設定 \(P.16-2\)](#)
- [SNMP 通知先の設定 \(V3\)\(P.16-4\)](#)



### 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** Smp > V3 Configuration > User 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、アクセスする対象のサーバを選択します。

**ステップ 3** 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、Add New ボタンをクリックし、**ステップ 4** に進みます。
- 既存の SNMP ユーザを変更する場合は、編集する SNMP ユーザの名前をクリックし、**ステップ 5** に進みます。
- SNMP ユーザを削除する場合は、削除する SNMP ユーザ (複数可) の横にあるチェックボックスをオンにし、Delete Selected をクリックします。**ステップ 11** に進みます。

**ステップ 4** User Name 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 (\_) の任意の組み合わせで、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。

**ステップ 5** 認証を要求するには、Authentication Required 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。

**ステップ 6** 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には、Privacy Required 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。

**ステップ 7** Host IP Addresses Information グループ ボックスで、SNMP パケットの送信元のホストを指定します。次のいずれかのオプションを選択します。

- すべてのホストから SNMP パケットを受信する場合は、Accept SNMP Packets from any host オプション ボタンをクリックします。
- 特定のホストから SNMP パケットを受信する場合は、Accept SNMP Packets only from these hosts 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。

- ステップ 8** Access Privileges ドロップダウン リスト ボックスで、適切なアクセス レベルを選択します。
- ステップ 9** クラスタ内のすべてのノードにユーザ設定を適用するには、**Apply To All Nodes** チェックボックスをオンにします。
- ステップ 10** **Insert** をクリックして新しいユーザを保存するか、**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 11** 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 Presence Server 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.16-5 の「関連項目」](#)を参照してください。

## SNMP 通知先の設定 (V3)

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** Smp > V3 Configuration > Notification Destination 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、通知先を設定する対象のサーバを選択します。

**ステップ 3** 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 4](#) に進みます。
- 既存の SNMP 通知先を変更する場合は、編集する SNMP 通知先の名前をクリックし、[ステップ 5](#) に進みます。
- SNMP 通知先を削除する場合は、削除する SNMP 通知先 (複数可) の横にあるチェックボックスをオンにし、Delete Selected をクリックします。[ステップ 12](#) に進みます。

**ステップ 4** 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、IP アドレスを入力します。

**ステップ 5** Port Number 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。

**ステップ 6** 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。

Inform を選択する場合は、[ステップ 7](#) に進みます。Trap を選択する場合は、[ステップ 8](#) に進みます。



### 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。

**ステップ 7** Remote SNMP Engine Id 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 を入力します。

**ステップ 8** 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 : 認証もプライバシーも設定されます。

**ステップ 9** User Information グループ ボックスで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.16-2 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、該当するユーザのチェックボックスをオンにし、Updated Select User をクリックします。[P.16-2 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、ユーザのチェックボックスをオンにし、**Delete Select User** をクリックします。



(注) 表示されるユーザは、前のステップで選択したセキュリティ レベルによって異なります。

**ステップ 10** クラスタ内のすべてのノードに通知先を適用するには、**Apply To All Nodes** チェックボックスをオンにします。

**ステップ 11** **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 12** 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。

SNMP v.3 Notification Destination ウィンドウに、通知先の IP アドレス、ポート番号、セキュリティ モデルバージョン、セキュリティ名、レベル、および通知タイプが表示されます。

#### 追加情報

[P.16-5 の「関連項目」](#)を参照してください。

## 関連項目

- [SNMP V1/V2c の設定 \(P.15-1\)](#)
- [MIB2 システム グループの設定 \(P.17-1\)](#)
- [SNMP ユーザの設定 \(P.16-2\)](#)
- [SNMP 通知先の設定 \(V3\)\(P.16-4\)](#)
- 『Cisco CallManager Serviceability システム ガイド』の「SNMP」





## MIB2 システム グループの設定

Cisco Unified Presence Server 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。

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 > SystemGroup Configuration > MIB2 System Group Configuration 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、連絡先を設定する対象のサーバを選択します。
- ステップ 3** Contact 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。
- ステップ 4** System Location 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。
- ステップ 5** クラスタ内のすべてのノードにこのシステム設定を適用するには、Apply To All Nodes チェックボックスをオンにします。
- ステップ 6** Save 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。
- ステップ 7** 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) Contact フィールドと System Location フィールドをクリアするには、Clear 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 ボタンをクリックし、Save ボタンをクリックします。

#### 追加情報

P.17-2 の「[関連項目](#)」を参照してください。

## 関連項目

- 『Cisco CallManager Serviceability システム ガイド』の「SNMP」
- [SNMP V1/V2c の設定 \( P.15-1 \)](#)
- [SNMP V3 の設定 \( P.16-1 \)](#)



<p><b>A</b></p> <p>Alert Central、アクセス 8-2</p> <p><b>C</b></p> <p>Cisco Unified CallManager、サービス 5-2</p> <p>CLI</p> <ul style="list-style-type: none"> <li>サービスの開始 2-4</li> <li>サービスの停止 2-4</li> </ul> <p>Control Center</p> <ul style="list-style-type: none"> <li>サービスの開始 2-3</li> <li>サービスの停止 2-3</li> <li>状況の表示 2-3</li> </ul> <p><b>H</b></p> <p>HTTPS</p> <ul style="list-style-type: none"> <li>概要 (IE) 1-3</li> <li>信頼できるフォルダへの証明書の保存 (IE) 1-4</li> <li>信頼できるフォルダへの証明書の保存 (Netscape) 1-5</li> </ul> <p><b>L</b></p> <p>Log Partition Monitoring</p> <ul style="list-style-type: none"> <li>設定 12-1, 13-1</li> </ul> <p><b>M</b></p> <p>MIB2</p> <ul style="list-style-type: none"> <li>システムグループの設定 17-1</li> </ul> <p><b>N</b></p> <p>NT イベント ビューア 3-3</p>	<p><b>Q</b></p> <p>Q931 Translator、使用 10-20</p> <p><b>R</b></p> <p>Real-Time Monitoring Tool</p> <ul style="list-style-type: none"> <li>Local Browse オプションを使用したトレース ファイルの表示 10-17</li> <li>Query Wizard を使用したトレースの収集 10-7</li> <li>Real Time Trace オプションの使用 10-21</li> <li>Real Time Trace オプションの使用、Monitor User Event 10-22</li> <li>Real Time Trace オプションの使用、View Real Time Data 10-21</li> <li>Remote Browse オプションを使用したトレース ファイルの表示 10-18</li> <li>Schedule Collection オプションを使用したトレースの収集 10-11</li> <li>SysLog Viewer 11-1</li> <li>Trace &amp; Log Central のオプションの表示 10-3</li> <li>アップグレード 7-3</li> <li>アラート <ul style="list-style-type: none"> <li>Alert Central へのアクセス 8-2</li> <li>アラート アクションの設定 8-8</li> <li>一時停止 8-7</li> <li>電子メールの設定 8-8</li> <li>プロパティの設定 8-4</li> </ul> </li> <li>アラート通知 <ul style="list-style-type: none"> <li>カウンタ用の設定 9-6</li> </ul> </li> <li>アンインストール 7-4</li> <li>インストール 7-2</li> <li>カウンタ <ul style="list-style-type: none"> <li>サンプルデータ 9-11</li> <li>詳細表示 9-9</li> <li>データの表示 9-12</li> <li>プロパティの説明の表示 9-10</li> </ul> </li> <li>カウンタの詳細表示 9-9</li> </ul>
--	---

- カテゴリ
    - 削除 7-16
    - 追加 7-15
    - 名前の変更 7-15
  - クラッシュ ダンプの収集 10-15
  - 構成プロファイル
    - 削除 7-9
    - 使用、デフォルト 7-8
    - 追加 7-8
    - 復元 7-9
  - サンプル データ 9-11
  - 事前定義オブジェクトのモニタリング 7-10
    - 使用 7-5
  - スケジュールされた収集の削除 10-14
  - 電子メール通知、設定 7-7
  - トレース収集状況の表示 10-14
  - トレース収集の関連項目 10-25
  - トレース設定の更新 10-25
  - トレースの収集 10-4
  - 表示
    - デバイスのプロパティ 7-13
    - 電話機情報 7-13
  - ポーリング レート、設定 7-13
  - モニタリング
    - CTIManager 7-10
    - コール処理 7-10
    - サーバ 7-10
    - サービス 7-10
    - 事前定義オブジェクト 7-10
    - デバイス 7-10
    - 要約 7-10
  - モニタリングの要約 7-10
  - ロード 7-5
- S**
- Serviceability
    - アイコン (表) 1-6
    - アクセス 1-2
    - エラー コードへのアクセス 1-6
    - 概要 1-1
    - バージョンの確認 1-6
  - Serviceability Reports Archive
    - 設定 14-1
  - SNMP
    - MIB2 システム グループの設定 17-1
    - コミュニティ スtring の設定 15-2
    - 通知 (V1/V2) 15-4
    - 通知先 (V1/V2) 15-4
    - 通知先 (V3) 16-4
    - トラップ (V1/V2) 15-4
    - ユーザの設定 (V3) 16-2
  - SysLog Viewer 11-1
- あ**
- アクセシビリティ機能 1-8
  - アラート
    - Alert Central へのアクセス 8-2
    - アクションの設定 8-8
    - 一時停止 8-7
    - 電子メールの設定 8-8
    - プロパティの設定 8-4
  - アラート通知
    - カウンタの電子メール 9-6
    - カウンタのパラメータの設定 (表) 9-6
    - しきい値 9-6
    - スケジュール 9-6
    - メッセージ 9-6
  - アラート通知、設定 8-8
  - アラーム
    - SDI トレース ライブラリ 3-3
    - SDL トレース ライブラリ 3-3
    - Syslog 3-3
    - 宛先 3-3
    - 宛先の設定値 3-3
    - イベント ビューア 3-3
    - イベント レベル 3-4
    - イベント レベルの設定値 3-4
    - 更新、手順 3-2
    - 設定、手順 3-2
  - アラーム定義
    - カタログ記述 4-3
    - 検索 4-2
    - 検索と表示
      - 手順 4-2
    - 説明 4-1
    - 表示 4-2
    - ユーザ指定、作成 4-2
  - アラームのイベント レベル 3-4
  - アラームの設定、説明 3-1

- え
- エラー コード 1-6
- か
- 概要
- Serviceability 1-1
  - インターフェイスのアイコン (表) 1-6
  - インターフェイスへのアクセス 1-2
  - エラー コードへのアクセス 1-6
  - オンライン ヘルプへのアクセス 1-6
  - バージョンの確認 1-6
- カウンタ
- アラート通知の設定 9-6
  - アラート通知パラメータ (表) 9-6
  - サンプル データ、設定 9-11
  - サンプル データ パラメータ (表) 9-11
  - 詳細表示 9-9
  - データの表示 9-12
- カウンタの詳細表示 9-9
- カテゴリ
- 削除 7-16
  - 追加 7-15
  - 名前の変更 7-15
- 簡易ネットワーク管理プロトコル
- MIB2 システム グループの設定 17-1
  - コミュニティ スtring の設定 15-2
  - 通知 (V1/V2) 15-4
  - 通知先 (V1/V2) 15-4
  - 通知先 (V3) 16-4
  - トラップ (V1/V2) 15-4
  - ユーザの設定 (V3) 16-2
- き
- 機能サービス
- アクティブ化 2-2
  - 開始 2-3
  - 状況の表示 2-3
  - 停止 2-3
  - 非アクティブ化 2-2
- こ
- 構成プロファイル
- 削除 7-9
  - 使用、デフォルト 7-8
  - 追加 7-8
  - 復元 7-9
- コミュニティ スtring 15-2
- さ
- サーバ認証証明書
- トレース収集オプションを使用したインポート 10-2
- サービス
- アクティブ化 2-2
  - 開始 2-3
  - 状況の表示 2-3
  - 停止 2-3
  - 非アクティブ化 2-2
  - モニタリング 7-10
- サービスのアクティブ化
- アクティブ化 2-2
  - 非アクティブ化 2-2
- サンプル データ
- パラメータの設定 (表) 9-11
- し
- 事前定義オブジェクト
- モニタリング 7-10
- せ
- セキュリティ
- HTTPS (IE の場合) 1-4
  - HTTPS (Netscape の場合) 1-5
- つ
- 通知
- V1/V2 15-4
  - V3 16-4
- 通知先
- V1/V2 15-4
  - V3 16-4

- て
  - デバッグトレース レベル
    - 定義 5-4
  - 電子メールの設定
    - アラート 8-8
- と
- トラップ
  - V1/V2 15-4
  - V3 16-4
- トラブルシューティング トレース設定値
  - 設定 6-1
- トレース
  - サービスのデバッグ トレース レベル 5-4
  - 収集
    - Local Browse オプションの使用 10-17
    - Query Wizard オプションの使用 10-7
    - Real Time Trace オプションの使用 10-21
    - Real Time Trace オプションの使用、Monitor User Event 10-22
    - Real Time Trace オプションの使用、View Real Time Data 10-21
    - Remote Browse オプションの使用 10-18
    - Schedule Collection オプション 10-11
    - オプションの表示 10-3
    - 関連項目 10-25
    - クラッシュ ダンプの収集オプション 10-15
    - 状況の表示 10-14
    - スケジュールされた収集の削除 10-14
    - 設定、説明 10-1
    - トピックのリスト 10-1
    - ファイルの収集オプション 10-4
  - 設定 5-2
    - 説明 5-1
    - トピックのリスト 5-1
  - デバイス名に基づくトレース モニタリング 5-2
  - ログファイル
    - 出力設定値 5-5
- 停止 2-3
- は
  - パフォーマンス カウンタ
    - カウンタ インスタンスの追加 9-5
    - 削除 9-4
    - 図形式での表示 9-2
    - 表形式での表示 9-2
  - パフォーマンス モニタリング
    - カウンタ データの表示 9-12
    - カウンタのアラート通知の設定 9-6
- ふ
- プラグイン
  - アクセス 12-1
  - ダウンロード 12-1
- ほ
- ポーリング レート 7-13
- も
- モニタリング
  - サービス 7-10
  - 事前定義オブジェクト 7-10
- ゆ
- ユーザ指定のアラーム記述 4-2
- ね
- ネットワーク サービス
  - 開始 2-3
  - 状況の表示 2-3